QUANTITATIVE MODEL OF A FACILITY-LEVEL RADIOLOGICAL SECURITY RISK INDEX

by

Shraddha Vishwas Rane

A Dissertation

Submitted to the Faculty of Purdue University
In Partial Fulfillment of the Requirements for the degree of

Doctor of Philosophy

School of Health Sciences
West Lafayette, Indiana
August 2020

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Jason. T. Harris, Chair

School of Health Sciences

Dr. Linda Nie

School of Health Sciences

Dr. Jim Schweitzer

School of Health Sciences

Dr. C**raig Mariannoro**

Department of Nuclear Engineering
Texas A&M University

Approved by:

Dr. Aaron Bowman

Dedicated to my papa.

ACKNOWLEDGMENTS

Research reported in this dissertation is based upon work partially supported by the U.S. Department of Energy, Pacific Northwest National Laboratory, under Contract Number 368096 and Purdue Research Foundation, under Grant Number 60000029. The content is solely the responsibility of the author and does not necessarily represent the official views of the U.S. Department of Energy or Purdue University.

I would like to acknowledge the IUPUI Radiation Safety staff for being so accommodating in providing me with numerous tours, explanations, and healthcare facility security details for this research. I specially would like to thank Dr. Michael Martin, CHP (the Radiation Safety Officer for IU Medical center/IUPUI) for getting me evaluated under the trustworthiness and reliability (T&R) determination process so quickly and efficiently. The initiative from Dr. Martin to get the survey approval from the medical, HP and MP staff at IUPUI assisted me tremendously to effectively perform my research and acquire survey participants for the nuclear security culture assessment. I would like to also especially thank Dr. Jianxi Su (Assistant Professor of Statistics and Associate Director of Actuarial Science) who helped me discover the probabilistic approach towards terrorism risk analysis. The statics graduate department staff and the PhD graduate student Daniel Vasquez were very helpful in the thought process of devising statistical mechanism for this research. I would like to thank my lab group undergraduate members Courtney Sheffield and Naomi German who helped with the data collection process.

I would like to thank Dr. John Lanza (MD, PhD) who has been my mentor and my good friend for taking the time to review my dissertation drafts and making edits. I would like to express my deep and sincere gratitude to my research advisor Dr. Jason Harris (Advisor), who I have known for about a decade now, for always encouraging and uplifting me to reach higher goals in career and life. Dr. Harris has also always supported my spirit of adventure and creativity in regard to the research. Despite his busy schedule he has always managed to sit with me and discuss the problems in research and has thus guided me through the completion of this dissertation. I offer my sincere appreciation to my committee members Dr. Linda Nie, Dr. Jim Schweitzer, and Dr. Craig Marianno

for encouraging words, thoughtful criticism, and time and attention throughout my time here at Purdue.

I would like to also thank my fiancée, Dustin Glossic, who helped me explain complex economic models and utility functions. He has been very instrumental in valuable discussions regarding game theory models, utility functions and cost benefit analysis. His contributions have really helped me get my research completed on time. He has been my motivator, my friend, and my ESA at times. Appreciation is extended to my dearest friend Marcia Robinson and Madelina for being a part of this journey. Finally, I would like to thank my wonderful parents (Anita and Vishwas Rane), and my beautiful sister (Shruti Rane) for believing in me and helping me keep my sanity and balance through this PhD journey. I hope this work makes you proud mummy and papa.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

The safety and security of a radiological facility shares a common objective which is to ensure the protection of the population and the environment from an undue radiological hazard. Adapting and extending risk assessment to security applications has been limited because of the adaptive nature of the sub-state actors and the lack of historical data of terrorist attacks on radiological facilities. Currently, no broad risk index exists for radiological facilities, such as healthcare centers and universities. This study develops a quantitative risk-based methodology that radiological facilities can employ to conduct self-assessments and gain better understanding of the threat they face. The computation of the Potential Facility Risk Index (PFRI) is based on the triplet definition (threat, vulnerability, and consequences) of risk. The threat component of the PFRI is devised as a utility function weighing the threat group attributes and asset preference. The principles of probabilistic risk assessment and pathway analysis are implemented to account for radioactive material theft probabilities in different attack scenarios. Locational hazards and nuclear security culture are measured as a function of radiological facility vulnerability. The consequences of loss of life and economic loss are computed, as a result of an attack from the radiological dispersal device (RDD). The methodology is applied to a hypothetical healthcare facility a single radioactive with three material assets (^{60}Co, ^{137}Cs, ^{192}Ir). The representation of the PFRI value on a qualitative scale-ranging from "very low risk" (1) to "very high risk" (10) presents a holistic view of the state of the facility risk to RDD. The PFRI may be used by decision makers to evaluate any security upgrades and justify security investments. The RDD game, developed as an extension to PFRI, provides the healthcare facility (defender) with strategic options to budget scarce security resources and make optimal choices under severe uncertainty about the terrorist adversary (attacker) theat.

CHAPTER 1. INTRODUCTION

1.1 Background

On September 11, 2001, the United States (U.S.) was attacked, not by a rival State, but by a terrorist network. The single attack galvanized the world into widespread concerted action, profoundly changing the way Americans see themselves, their government, and their national security. The ability to cause mass harm has dispersed from nation states to amorphous groups and even to individuals with improvised weapons of mass destruction and nontraditional usage of common weaponry. Subsequent tragic terrorist attacks in places such as Bali (October 2002 bombings), Madrid (March 2004 bombings), Mumbai (attacks of November 2008) and Istanbul (June 2016 bombings), including the increasing number of mass shootings in the US and elsewhere, make it hard to envision a world without terrorism. Chemical, biological, radiological, nuclear, and explosive (CBRNE) agents are the weapons of terror that have prompted the international community to re-evaluate the threats posed by terrorism.

The risk of nuclear terrorism appears larger than ever before in the United States. To a terrorist, civilian populations, targets of historical, cultural, and national significance, and the infrastructure that underpins the US way of life, are all 'fair game'(Garrick et al., 2004). A leading question in American society today is the ability to protect our stockpile of nuclear materials and weapons as well as radioactive materials against theft and sabotage by terrorist groups. Given the availability of radioactive materials and the sub state actors' familiarity with conventional explosives, the development of a radiological dispersal device (RDD), also known as a "dirty bomb", or radiation exposure device (RED) seems to be a more probable form of mass disruption weapon than other forms of nuclear terrorism.

In the recent past, terrorist groups like Al Qaeda and Chechen rebels have shown some interest in RDDs. To meet the challenges of radiological terrorism, strengthening the protection of radioactive material (RAM) in domestic use, storage, and transport seems the best way to counter the threat. The responsibility of securing nuclear and radiological materials rests entirely with the States, many of which are members of the International Atomic Energy Agency (IAEA). Recommendations and guidance documents issued by organizations like, the IAEA assist the IAEA member States to meet their obligations under international legal instrument and discharge their responsibilities for nuclear security within the State. Domestically, federal and state governments are taking steps to prevent an RDD attack. In the U.S., the Nuclear Regulatory Commission (NRC) has issued regulations to secure radioactive sources. The U.S. National Nuclear Security Administration (NNSA) has recovered thousands of disused or abandoned sources and the Department of Homeland Security (DHS) supports efforts to detect radioactive material by emergency responders. The Nuclear Threat Initiative (NTI), a nongovernmental organization, maintains a Nuclear Materials Security Index (NMSI) that measures the level of security for weapons grade nuclear materials globally (US GAO, 2019).

While international and national regulatory bodies have been quite comprehensive in assisting the IAEA member States to prevent, detect, and respond to radiological terrorism, they, however, do not quantify the radiological security risk at the facility level. Given the evolving threat environment, it is imperative for radiological facilities to have the means to fully understand the gravity of radiological terrorism and evaluate security measures based on threat and risk assessments. Such is the purpose of the subject radiological security risk methodology study with the intention to lay the foundation for quantitative risk assessments of terrorist inspired catastrophes with application in both public and private sectors utilizing radioactive materials.

The central objective of this dissertation is to present a framework for assessing radiological security risk at the facility level. The study establishes a potential facility risk index (PFRI) by identifying and assessing the threats, weighing the vulnerabilities, and evaluating the consequences, specific to the radiological facility. The PFRI metric is a quantitative value that not only reflects the challenges the facility would face from the current radiological security threats, but also assists with appropriate allocation of resources by providing a linkage between understanding risk and making better radiological security upgrade decisions.

1.1.1 The Four faces of Nuclear Terrorism

Nuclear terrorism is defined as the actual or potential use of nuclear or radiological materials, or attacks on nuclear facilities or transportation carrying nuclear materials, by an individual or a sub-state group to generate fear or destruction in the pursuit of political objectives(Mærli, 2010). Terrorists have essentially four mechanisms by which they can exploit military and civilian nuclear asset around the globe to serve their destructive ends. These four threats, as described by the IAEA, highlight the four ‘faces’ of nuclear terrorism:

- The theft and detonation of an intact nuclear weapon;
- The theft or purchase of fissile material leading to the fabrication and detonation of a crude nuclear weapon, i.e., an improvised nuclear device (IND);
- Attacks against and sabotage of nuclear facilities, in particular nuclear power plants, causing the release of large amounts of radioactivity; or,
- The unauthorized acquisition of radioactive materials contributing to the fabrication and detonation of a RDD (a “dirty bomb’) or a RED (Ferguson et al, 2005; Myers 2012).

The first incident, which is concerned with a sub-state group stealing a nuclear weapon, only affects a small number of countries, since possessing a nuclear weapon is a prerequisite to this threat. Taking possession of an intact nuclear weapon is the most appealing option for a terrorist group intent upon acquiring considerable nuclear capability and resources, given the many hurdles they would have to overcome to produce their own device. However, nuclear weapons are considered the “crown jewels” and are among the State’s most heavily protected assets, making it very unlikely for the terrorist group to steal it successfully (Myers, 2012). Even if a terrorist organization was able to acquire a nuclear weapon, they could not simply detonate it, as State-controlled weapons are equipped with strict control measures, like permissive action links (PALs), that render the weapon useless without authorization codes (Grant 2005; Pomper & Tarini, 2017). Today, the nuclear arsenals of the nine nations known or believed to possess nuclear weapons (China, France, India, Israel, North Korea, Pakistan, Russia, the United Kingdom, and the United States) contain more than 13,000 nuclear weapons (Korda & Kristensen, 2019)From the perspective of guarding against nuclear terrorism, certain categories of the world’s nuclear weapons are more vulnerable to terrorist acquisition than others. This system classifies nuclear warheads into strategic and non-strategic weapons (tactical weapons) based on the range and military application of the delivery systems for which they were designed or on which they are deployed. Strategic weapons include intercontinental ballistic missiles, ballistic missile submarines, and heavy bombers, which can travel over intercontinental distances. Tactical nuclear weapons are typically limited to distances of less than intercontinental range (Ferguson et al., 2005; Myers, 2012). These weapons pose special risks of theft and diversion, as they have never been covered in arms control treaties and are much more portable than strategic warheads. Stealing and scrapping the tactical weapons to remove the fissile material and other useful components is another option for the non-state actors to accomplish this heinous act (Ferguson et al., 2005; Myers, 2012). However, this is not an attractive pathway for the terrorist group as there are likely other sources of special nuclear material (SNM) within the State that are less heavily protected and easier to exploit.

Of the four threats, developing an IND is the most complicated task. An attack involving an IND not only requires broad knowledge and resource base but also a secure location center to develop and construct the weapon. An IND is similar to a nuclear weapon which requires utilizing supercritical configurations of fissile material to produce a nuclear explosion. Experts seem to agree that the most difficult challenge for a terrorist organization wanting to construct an IND is finding the fissile material and engaging scientists to develop the device itself. For a gun-type weapon, about a barely critical mass of very highly enriched uranium (HEU) is needed. For an implosion-type device, approximately half a barely critical mass of highly enriched uranium or plutonium is required. Both the enrichment of uranium and the production of plutonium in a nuclear reactor are technically complex and expensive for even advanced States, and as such is well beyond the plausible capabilities of terrorist groups. Thus, obtaining fissile material for a bomb through purchase or theft, though still extremely difficult, is the most realistic option for a terrorist. It is more difficult to maintain strict control over fissile materials than over nuclear weapons. Since fissile materials are difficult to measure and handle in its bulk form, it is likely to introduce uncertainties and mask repeated diversions of minuscule quantities of HEU or plutonium from processing centers or storage areas (Ferguson et al., 2005).

The third type of nuclear terrorism involves nuclear sabotage, where a terrorist group acts premeditatedly against a nuclear facility or a vehicle containing or transporting nuclear material to cause the release of radioactive materials (Myers, 2012). The scenario complexity for this threat ranges from simply identifying and attacking a potentially vulnerable nuclear power plant (NPP) and detonating nuclear or radioactive material in place with conventional explosives, to disabling and destroying enough vital components at the facility with the intent to cause a core meltdown and a radiological release. Both Al Qaeda and Chechen terrorist groups have repeatedly considered sabotaging nuclear reactors. The Fukushima Daiichi accident in Japan provides a compelling example of the scale of terror such an attack might cause. As opposed to a nuclear accident, a terrorist attack could damage more than one plant system in a short time. Thus, protecting against a terrorist threat might be extremely challenging than defending against nuclear accidents (Ferguson et al, 2005).

The final threat of nuclear terrorism is an RDD where radioactive sources are combined with conventional explosives to disperse radioactive contamination over a wide area (Myers, 2012). Of course, a failed IND would also be classified as an RDD if the device exploded. In contrast, REDs which do not use explosives, emit radiation over a concentrated area. With radioactive materials being commonly available than nuclear weapons-usable fissile material and with conventional explosives also relatively easy to find, it is more likely that terrorists would construct and use an RDD or RED than an improvised nuclear device. Unlike an IND, neither a RDD nor a RED would typically cause damage or fatalities on the scale associated with weapons of mass destruction (WMD). However, radiological devices could potentially provoke mass hysteria causing mass disruption. This disruption and stigma could incite the universal fear in public similar to Chernobyl, Three Mile Island, and Fukushima (Ferguson et al, 2005).

These four threats of nuclear terrorism not only pose different risks based on their requisite characteristics, but also differ in the types, capabilities, and the motivational orientation of the terrorist organizations willing to engage in this particular type of violence.

Table 1.1 summarizes the general attributes of terrorist organizations, the criteria for pursuing the threats, and the number of groups that fit each description as of 2004 (Ferguson et al., 2005; Myers, 2012) .

Table 1.1 Terrorist traits and criteria for the four threats of nuclear terrorism(Ferguson et al., 2005, Myers, 2012).

Traits	Steal Nuclear Device	Steal Nuclear Material for IND	Sabotage Nuclear Facility	Steal Radioactive Material for RDD
Motivation	Extreme; desire to cause mass deaths, destruction; likely limited to apocalyptic and politico-religious groups	Extreme; desire to cause mass deaths, destruction; likely limited to apocalyptic and politico-religious groups	Very high; desire to cause great property damage, disruption, some loss of life	Very high; desire to cause great property damage, disruption, some loss of life
Organizational Skills	Very high	Very high	Very high	Moderate
Financial Resources	High	High	Moderate to high	Moderate
Technical Skills	High	High; moderate for some scenarios	Moderate to high	Moderate
Number of groups (in 2004)	Few (possibly none currently able to meet all criteria for foreign country incident)	Few (possibly none currently able to meet all criteria for foreign country incident)	10+	1-100's

While terrorists may have strategic reasons and tactical opportunities to pursue nuclear terrorism, few in fact have contemplated such an incident. In particular, the Japanese cult group Aum Shinrikyo and the militant Islamic organization al Qaeda and its associates (notably the Egyptian Islamic Jihad, Jemaah Islamiya and Lashkar al Tayyib), are the most prominent groups that have manifested some degree of intent, experimentation, and programmatic efforts to acquire a WMD. Fortunately, as of this writing, no detonations of illicitly obtained nuclear weapons or INDs have occurred, nor have there been any dirty bomb attacks. Nuclear facilities have faced some terrorist attacks, but none of these has resulted any radioactivity being released off-site (Ferguson et al, 2005). Nuclear terrorism experts generally agree that the threats with highest consequences, (i.e., nuclear weapon and IND) are least likely to occur because they are the most difficult to accomplish. Conversely, those acts with the least damaging consequences are the most likely to take place because they are the easiest to accomplish (Ferguson et al, 2005).

Considering the magnitude of potential consequences, the relative difficulty of execution, and the probability of occurrence, all four faces of nuclear terrorism pose potentially grave and imminent dangers since all the options are in the hands of the terrorist and always with the possibility of an attack without warning. The question, however, to be asked is “Why has a nuclear attack not happened since 9/11?” Well, some factors that influence terrorists to not resort to nuclear terrorism are implementation challenges, fears of reprisal, philosophical and moral issues, and insufficient capability. Implementation challenges are the primary barriers to any type of nuclear terrorism, even for terrorist groups set on mass destruction, such as al Qaeda, but it would be foolish to discount the possibility that such an incident will not occur in the future. Yet, WMD terrorism skeptics abound who believe that nuclear terrorism is another phony threat being hyped for political purposes and to stoke fears amongst the public. On the other side of the spectrum, ardent believers in this threat argue that considering the unlikelihood of the 9/11 plot, analysts may have concluded that it never could have happened; at the time, it was simply hard to envision that any terrorist group could have implemented such an elaborate plot using unpredictable weapons that were so difficult to acquire. While there is no consensus among experts about the intentions and capabilities of sub-state groups with respect to nuclear terrorism, and given a sustained and ferocious counterterrorist response to 9/11, we must continue to disrupt and deny the terrorists a safe haven to reestablish the ability to launch a major strike on the U.S. homeland, or elsewhere in the world (Mowatt-Larssen, 2010)

1.2 Understanding Radiological Terrorism

A radiological weapon is not a nuclear weapon. Unlike a nuclear weapon explosion, use of an RDD would not involve a nuclear chain reaction or a massive release of energy. The blast effect of a radiological bomb is therefore the same as that of a conventional bomb using the same amount of explosive. While an RDD can, of course, take the crude form of dynamite strapped to a radioactive source, radiation or radiological weapons can use dispersal methods other than conventional explosives to spread radioactivity. Depending on the chemical composition of the radioactive source, non-explosive methods could result in more effective dispersal than explosive methods.

Radioactive materials in the form of commercial radioactive sources are used in various applications such as cancer treatment, industrial radiography, oil well logging, and scientific research. The accelerator-produced radioactive materials tend to be short lived and generally do not pose an RDD threat. In contrast, nuclear reactors produce long-lived, bulk quantities of radioactive material that pose a high security concern. Spent fuel assemblies from research and commercial nuclear reactors could potentially be used to make an effective terrorism device. In a study, researchers at the Center for Nonproliferation Studies (CNS) identified seven reactor produced radionuclides as posing the greatest security concern and (Meyer et al, 2018)shown in Table 1.2. All these isotopes have half-lives ranging from months to decades, emitting most or essentially all of their radioactivity during a typical human lifespan, thus presenting the greatest risk to human health. Aside from half-life, radioactive sources containing a large amount of radioactivity obviously have the potential to create a more harmful RDD than a small source. Industrial radiography equipment, blood irradiators, radiosurgery devices, and teletherapy machines are among the highest category security concern sources, according to the IAEA.

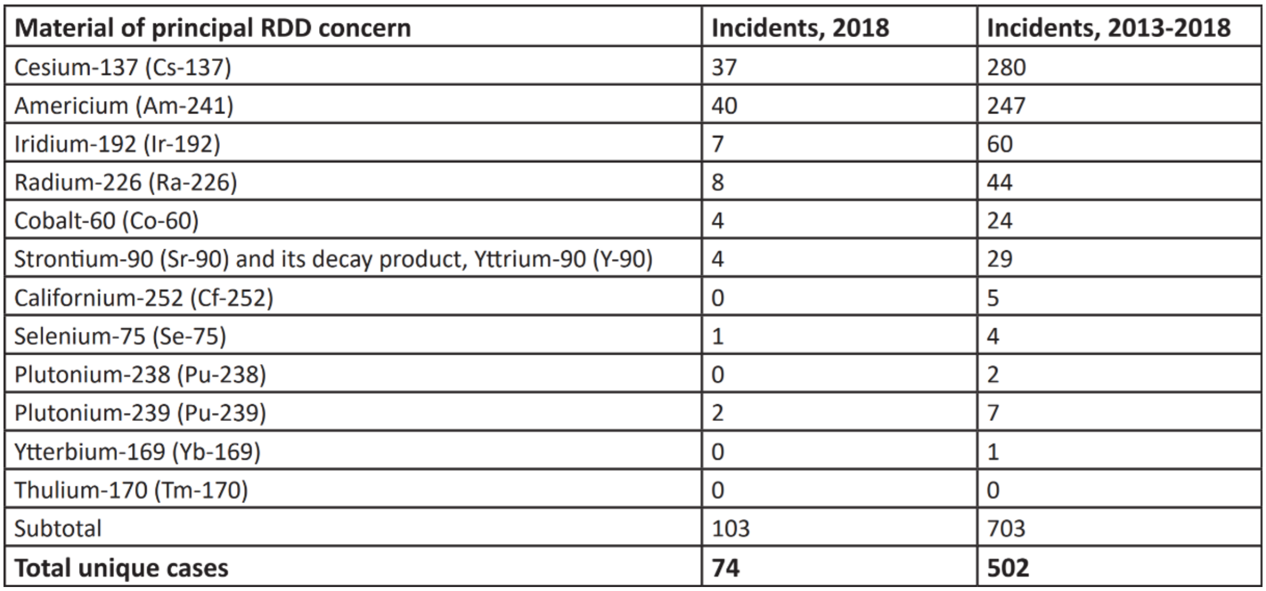
Table 1.2 Radionuclides that pose the greatest security risk (Medalia, 2012)

Radionuclides	Half-life	Specific activity (Ci/g)	High energy alpha emissions	High energy beta emission	High energy gamma emissions
Cobalt-60	5.3 years	1100	N/A	Low energy	Yes
Cesium-137 (Barium-137m)	30 years, (2.6 min)	88, (5.4 x 10^7)	N/A	Low energy	N/A, Yes
Iridium-192	74 days	>450	N/A	Yes	N/A, Low energy
Strontium-90 (Yttrium-90)	29 years, (64 hours)	140, (5.5×10^5)	N/A	Yes	Low energy
Americum-241	433 years	3.4	Yes	No	Low energy
Californium-252	2.7 years	536	Yes	No	Low energy
Plutonium-238	88 years	17.2	Yes	No	Low energy
Radium-226	1600 years	1	Yes	No	Low energy

From cradle to grave, every part of a radioactive source's life cycle presents potential security risks. After the production of the radionuclides in the reactor, the processed radioactive sources get distributed to dozens of subsidiaries and thousands of users. The security practices at users' facilities vary depending on the application and type of source. Some facilities, like hospitals and universities, by their very nature can present security challenges.

The next stage in a source's life cycle occurs when a source is no longer needed by the user. Such disused sources are either returned to the manufacturer for disposal or sent to a State sponsored disposal site. Competent governmental regulatory authorities around the world exercise control over most radioactive sources for civilian use. The sources are usually subjected to a system of registration, licensing, authorization, and regular inspection. However, some disused sources around the world become abandoned and orphaned. These orphaned sources may have been initially regulated but eventually get abandoned, lost, misplaced, stolen, or removed without authorization. The CNS Global Incidents and Trafficking Database funded by the NTI maintains detailed information drawn from open sources on incidents involving loss of regulatory control over nuclear and other radioactive materials. Loss of control refers to both unintentional acts (such as loss or misrouting), and intentional acts (such as theft or attempted trafficking). The Incident and Trafficking Database (ITDB), maintained by IAEA help participating States and selected organization to combat illicit nuclear trafficking and strengthen nuclear security. The CNS database is generated from publicly available data and news reports which is freely available to the public. Between 2013 and 2018, roughly 50% of cases in the CNS database involved at least one material of principal RDD concern. A little over 70 such cases were reported to have occurred in 2018 alone (Meyer et al, 2018). Table 1.3 reports incidents by material type across the globe.

Table 1.3 Reported incidents by material type ((Meyer et al, 2018)



Material of principal RDD concern	**Incidents, 2018**	**Incidents, 2013-2018**
Cesium-137 (Cs-137)	37	280
Americium (Am-241)	40	247
Iridium-192 (Ir-192)	7	60
Radium-226 (Ra-226)	8	44
Cobalt-60 (Co-60)	4	24
Strontium-90 (Sr-90) and its decay product, Yttrium-90 (Y-90)	4	29
Californium-252 (Cf-252)	0	5
Selenium-75 (Se-75)	1	4
Plutonium-238 (Pu-238)	0	2
Plutonium-239 (Pu-239)	2	7
Ytterbium-169 (Yb-169)	0	1
Thulium-170 (Tm-170)	0	0
Subtotal	103	703
Total unique cases	**74**	**502**

The CNS database includes a total of 1,040 incidents, which occurred in 58 countries during the 2013 to 2018 reporting period. The 2018 database had 156 incidents. Trends remain consistent with the data collected between 2013 and 2017:

- 58 losses were recorded, constituting 37% of all incidents,
- 45 thefts were recorded, constituting 29% of all incidents, and,

- 64 incidents occurred during transport, constituting 41% of all incidents

The regional case breakdown is shown in Figure 1.1.

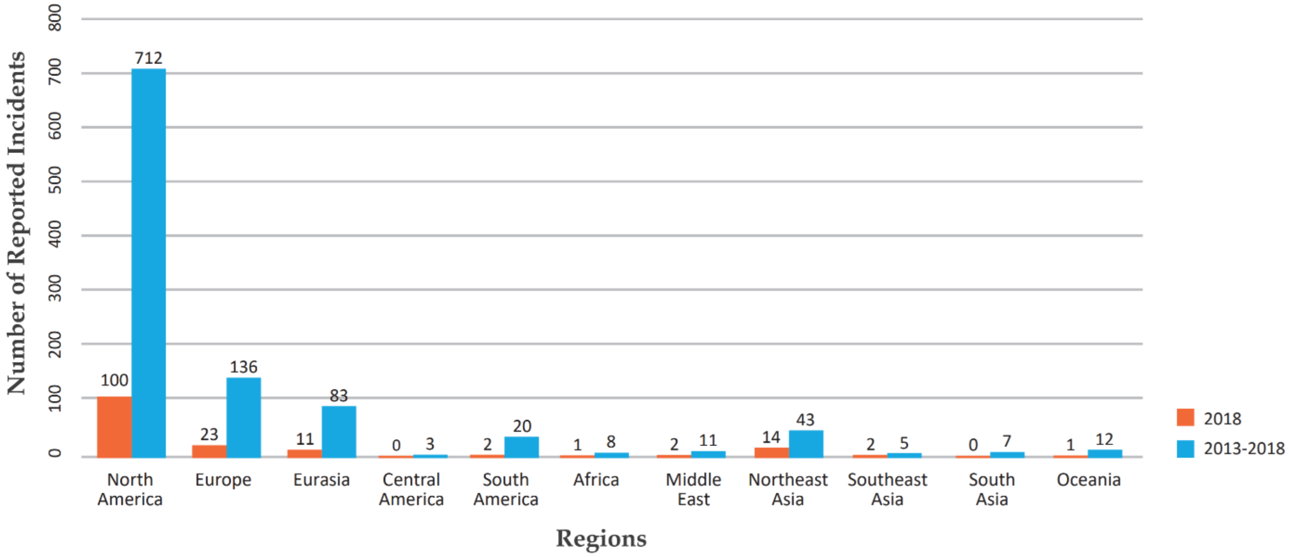


Figure 1.1 Number of reported incidents per region, (Meyer et al., 2018)

As seen from Figure 1.1, there is a drastic difference in the number of incidents reported across countries, with the U.S. disproportionately reporting the highest numbers. This says much more about the variations in reporting requirements across countries than it does about the actual number of incidents in each country. United States and Canada have two of the most robust and transparent reporting systems in the world. The level of global reporting has wide regional variance and presents an incomplete picture. Certain countries with fewer nuclear and other radioactive materials are expected to have fewer incidents. However, in other cases, governments may not catch incidents occurring in their jurisdiction, and if they do, they may choose to not report them. Some countries report incidents to the IAEA confidentially, but choose not to inform the public. In addition, several countries have different standards of reporting, making it difficult to definitively account for the total number of nuclear or radiological incidents. Many IAEA member States categorize radioactive materials using the IAEA categorization system, but still do not participate in the ITDB, including countries of concern for trafficking and terrorism, such as Angola, Egypt, Myanmar, North Korea, Syria, and Turkmenistan. A former senior analyst in the office of Nuclear Security at the IAEA, has noted that, “There is no binding international instrument that requires States to report the loss of regulatory control over hazardous or significant amounts of radioactive materials”(IAEA, 2001).

Establishing a mandatory reporting standard for Category 1 and 2 radioactive materials across all countries and member States, would not only improve reporting transparency but would also facilitate the development of better security policies.

The IAEA has identified radioactive materials as being most vulnerable to loss or theft while in transport. Theft cases as per the CNS database is categorized into, theft from a vehicle or an individual, theft from a fixed site, and theft under unknown circumstances. Of the 259 thefts recorded between 2013 and 2018, 140 occurred when the device involved was in transit, 77 occurred at fixed location, and 42 occurred under unknown circumstances. A majority of confirmed thefts involved unattended vehicles, suggesting that the presence of an individual is a strong deterrent and security measure. The two following incidents, stated in the 2018 CNS annual report, illustrated how even basic physical security measures on the part of end users can make all the difference.

- (Incident #1) A truck carrying a radiography camera with a Category 2 ^{192}Ir source was stolen during a fill-up at a gas station in West Virginia. The truck was, however, recovered by the state police later. The camera was found to be intact without any signs of intrusion because the camera was properly secured, making it difficult for the adversary to steal it.
- (Incident #2) In contrast, a piece of radiographic equipment was either lost or stolen from the back of a pickup truck while in transit between cities in Malaysia. When the vehicle arrived at the destination, the tailgate was found to have been lowered and the radioactive source was missing. Although there is no evidence that the source was used for malicious purpose, adequate security measures could have prevented the loss of the radioactive material.

Reports of incidents involving definitive cases of intentional trafficking of nuclear and other radioactive materials were also recorded in 2018. For example, four scrap metal dealers in the Netherlands were arrested after authorities determined they were illegally selling radioactive scrap metal used in ballast blocks on ships. In addition, Ukrainian security services arrested six individuals believed to be part of an international radioactive materials smuggling ring. The individuals were arrested after attempting to sell police an unspecified quantity of ^{226}Ra (Ra-226) in a sting operation. It is unclear how the individuals acquired the material. While the end use is unknown in these cases, the primary motivation behind most trafficking cases appears to be profit.

Human factors were found to be another key contributing factor towards security risk. In 2018, 87 incidents (58% of total incidents) included cases of theft where carelessness and inattention to appropriate procedures led to nuclear and radioactive material falling outside of regulatory control.

The real history of radioactive source security started with a non-criminal security breach of a ^{137}Cs (cesium-137) source capsule in Goiania, Brazil on 13 September 1987. Although this case study is a result of a radiological accident and not an intentional terrorist act, the actual extent of the accidental dispersal of radioactive material could be similar to a terrorist situation. Two scavengers looking for a scrap metal to sell broke into an abandoned medical clinic in Goiania and discovered a canister filled with 1,375 curies of ^{137}Cs in powdered form. They breached the canister and distributed the components to a junkyard as well as to family and friends. Since the radioactive material was in easy dispersible form, the contamination spread quickly. The accident sparked panic among the local population, resulting in more than 110,000 people demanding to be monitored for contamination.

More than 200 people were actually contaminated, with at least half of them experiencing significant internal doses from inhalation and ingestion of ^{137}Cs. Four people died from acute radiation dose and many experienced severe radiation burns. As mentioned previously, although this was a non-criminal activity, the end result demonstrated many of the consequences expected in an actual RDD or RED incident. The November 2006 death of Alexander Litvinenko through the ingestion of ^{210}Po (Polonium-210) reignited the debate concerning the possibility of future malicious use of radioactive materials. The alleged perpetrators who made two failed attempts to administer polonium to Litvinenko before the final and successful one, had stayed in three different hotels, and had carried the container of ^{210}Po to several different public places, thus leaving trails of ^{210}Po contamination. They left more significant traces of polonium than Litvinenko, indicating that they handled the radioactive material directly but did not ingest it. The contamination was also identified in member of the public who had inadvertently come in contact with ^{210}Po. Thus, what began as a targeted ^{210}Po assassination mushroomed into a radiological exposure incident. In London, before authorities could control the ^{210}Po contamination, it had already fanned out to expose large numbers of people. In an article from *The Guardian*, a group of scientist argued that if the terrorists try to replicate the murder of Litvinenko on a larger scale, or contrive other means to place radioactive sources inside, or in direct contact with their victims, it could kill several hundred, maybe upwards of a thousand, and without a doubt would paralyze a city (*The Guardian, 2007)*.

Both incidents demonstrated the widespread psychological and social effects that can grip a populace. The stigma that the Goiania incident has associated with it even to this day shows that the psychological burden can last for many years. Given the potential for significant societal disruption, and the large number of annual materials losses that could be used to make radiological devices, would lead to the conclusion that radiological attacks pose a serious societal threat.

1.3 Literature Review

Nuclear safety and security share a common purpose in protecting workers, members of the public, and the environment (IAEA, 2007). The primary difference between safety and security is that safety is concerned with actions taken to prevent unintentional, unforeseen, or unplanned events that can lead to hazards such as exposure to radiation or limit their consequences, whereas nuclear security is associated with the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer, or other malicious acts involving nuclear material, and other radioactive substances or their associated facilities. Essentially, safety protects against accidents, and security protects against malicious acts (U.S. NRC, 1975).

During the last 30 years we have seen a rapid and extensive development of principles, methods, and models for the analysis and management of risks caused by accidents. Probabilistic risk analysis (PRA), which is a systematic process that integrates information about design, operational practices, historical information, human interaction, and component reliability has been utilized to determine the likelihood and severity ratings for potential adverse events. PRA has been a major tool for assessing risk in areas as diverse as environmental protection, industrial safety, and even medical decision making. The nuclear power industry has clearly championed the development and application of quantitative methods more than any other industry or sector. PRA was first applied to study the reliability of nuclear reactors in the reactor safety study (RSS) released in 1974 (WASH-1400), to identify every single accident sequence, estimate the probability of the given accident sequence, and the consequences of these events. The “WASH-1400” report aimed for estimates “as realistic as is reasonably attainable.” The PRA methodology became generally followed as part of the safety-assessment of all modern nuclear power plants (NPPs). In the 1990s, all U.S. nuclear power plants submitted PRAs to the NRC under the “individual plant examination program”, and five of these commercial NPPs with different designs became the basis for the 1991 U.S, Nuclear Regulatory Commission Regulation (NUREG) - 1150. The RSS indicated that the probabilities of such reactor accidents were higher than previously believed but that the offsite consequences were significantly lower. The product of probability and consequences (a measure of the risk of severe accidents) was estimated to be quite low relative to other man-made and naturally occurring risks. The risk curve in Figure 1.2. compares the annual risk of deaths due to various man-made systems(U.S. NRC, 1975).

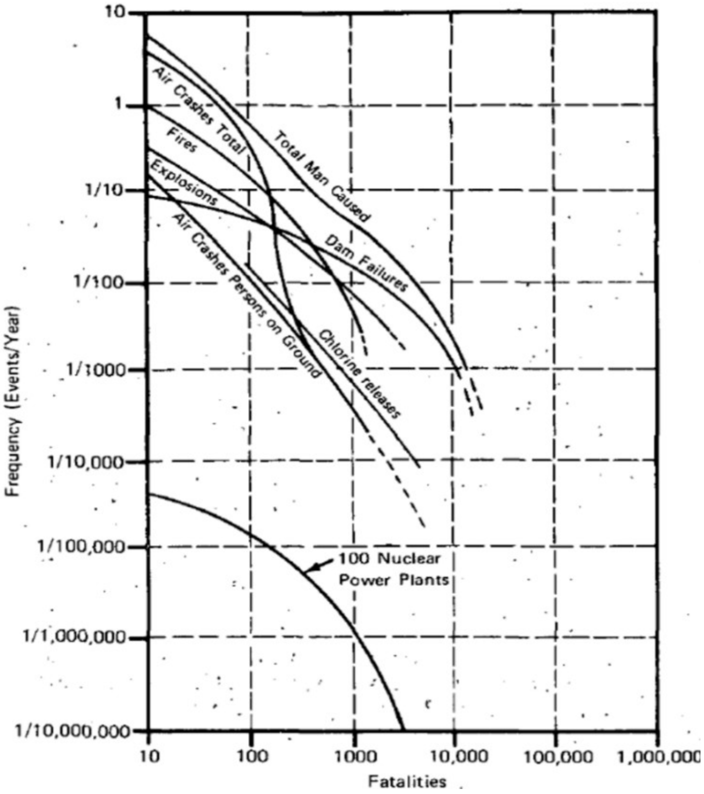


Figure 1. 2 WASH-1400 results comparing nuclear power plants and man-made events (Yang, 2012)

While NPPs are designed to be safe in their operation and safe during any malfunction or accident, no industrial activity can be represented as entirely risk-free. In avoiding such reactor accidents, the industry has been very successful. In over 17,000 cumulative reactor-years of commercial operation in 33 countries, there have been only three major accidents in the 50-year history of civil nuclear power generation:

Three Mile Island (USA 1979) where the reactor was severely damaged, but radiation was contained and there were no adverse health or environmental consequences;

Chernobyl (Ukraine 1986) where the destruction of the reactor by steam explosion and fire killed two people initially, followed by 28 from radiation poisoning within three months, and had significant health and environmental consequences internationally.

Fukushima (Japan 2011) where three old reactors (together with a fourth) were severely damaged after the effects of the loss of cooling due to a huge tsunami. There were no deaths or serious injuries due to radioactivity, though about 19,000 people were killed by the tsunami.

In 2007, the U.S. NRC launched a research program to assess the possible consequences of serious reactor accident. The State-of-the-Art Reactor Consequences Analysis (SOARCA) showed that a severe accident at a US nuclear power plant (either pressurized water reactor (PWR) or boiling water reactor (BWR)) would not be likely to cause any immediate deaths, and the risk of fatal cancers would be vastly less than the general risks of cancer. Two state-of-the-art computer codes have proven particularly useful in analyzing potential accidents. The codes especially examine the progression of an accident, response to the accident's severity based on human action, and estimate the potential public health effects and other types of consequence resulting from the radioactive material reaching the environment. Both codes have been reviewed by experts in several related fields to help validate their effectiveness. Many other studies have been performed and various models have been developed using the PRA to assess risks to the public from potential accidents in NPPs. Cho et al., (2018) extended the PRA structure from a single unit NPP risk to a multi-unit level 2 PRA method.

Probabilistic Safety Assessment (PSA), another name for PRA, was re-considered and improved after the Fukushima accident in Japan in 2011. Korea Atomic Energy Research Institute (KAERI) has researched the development of an integrated risk assessment framework that covered the internal PSA model and external PSA model in the full-power and low power shutdown modes. It also integrated level 1, 2, and 3 PSA to quantify the risk of nuclear facilities more efficiently and consistently (Willis, 2007). Kyne & Harris (2015) examined and constructed a potential risk index for the 65 U.S-based commercial NPP sites in relation to their surrounding population. The communities that host a NPP face various kinds of risks associated with them and thus the study focused on two distance areas, one within 50 miles, and the other being outside a 50-mile radius. Risk was categorized into four levels, where a greater percentage of minority groups were found to be exposed to the highest level of risk from the NPP.

The safety risk assessment includes the vulnerability of the system and the consequences of an adverse event, but the security risk, on the other hand, requires the intent to cause the adverse event by some threat. Security risk, therefore, exists at the intersection of threat, vulnerability, and consequences (Figure 1.3).

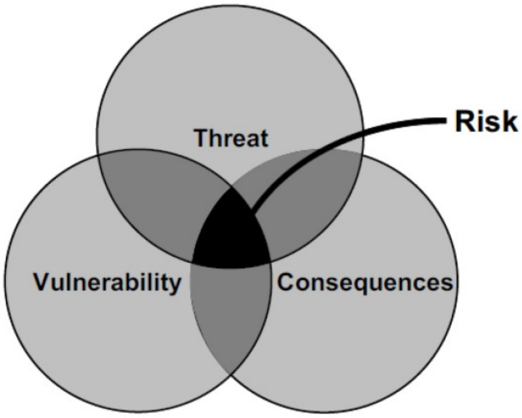


Figure 1. 3 Security risk is the intersection of threat, vulnerability, and consequences (McGill et al., 2007; Willis et al., 2018)

Nuclear security is not a new subject. Faced with increased security concerns, in the 1990s, there was an international reaction to the problem. International standards were approved by the Board of the IAEA in 1996, which was the first time that the security of radioactive sources was introduced explicitly as a regulatory obligation into international standards. President Obama and the United States brought nuclear security to the forefront of international awareness by hosting leaders from

47 countries at the inaugural Nuclear Security Summit. At the summit, Obama singled out nuclear terrorism as the most serious threat to international security (Myers, 2012).

Currently, the international nuclear security regime is made up of several international agreements that are binding or non-binding. The *Convention on Physical Protection of Nuclear Materials* (CPPNM) is the only international legally binding agreement focused on the physical protection of nuclear material. The *International Convention for the Suppression of Acts of Nuclear Terrorism* (ICSANT) is a binding legal agreement that requires States to define acts of nuclear terrorism as criminal offenses. Moreover, the United Nations Security Council adopted two resolutions that address the threat of nuclear terrorism and nuclear proliferation. Resolutions *1373* (2001), and *1540* (2004) also call for national, regional, and international cooperation to strengthen the global response to these challenges and threats to international security.

In addition to these legal agreements, a number of non-binding agreements exist that encompass nuclear security. The Physical Protection of Nuclear Materials and Nuclear Facilities (INFCIRC/225) provides guidance for States in establishing physical protection systems and covers the physical protection of nuclear materials in use, storage, and transport. With a long-established role in brokering international standards in nuclear safety and security, the IAEA has, in recent years, extended its oversight from protection of nuclear power plants and other nuclear facilities to the protection of radioactive sources and their associated facilities. The major international conference of Buenos Aires, Argentina (December 2000) was devoted to safety and security of radioactive materials. The *Code of Conduct (CoC) on the Safety and Security of Radioactive Sources*, despite being non-binding, has received political support from more than 130 member States. The Code of Conduct document serves as a guide to governments to point them towards better safety and security practices. It describes the components of an effective regulatory system. The *Guidance on the Import and Export of Radioactive Sources* supplements the Code and aims to provide for an adequate transfer of responsibility when a source is being transferred from one State to another (IAEA, 2001). The *Guidance on the Management of Disused Radioactive Sources* provides further guidance regarding the establishment of a national policy and strategy for the management of disused sources, and on the implementation of management options such as recycling and reuse, long term storage pending disposal, and return to a supplier.

Underpinning the work of the IAEA and their CoC is a suite of documents (the Nuclear Security Series) and services that provide capacity building in member States. Secondly, the World Institute for Nuclear Security (WINS) provides a range of guidance documents on radioactive source security that is designed to be used by practitioners more than governments or regulatory bodies. The International Radiation Protection Association (IRPA) is another noteworthy organization that has recently started its work in this area. It does not aspire to generate its own guidance documents but to assist in the dissemination of extant best practice information.

Progress in adapting risk analysis to security applications has been slow and does not yet have consensus level agreement from professional standards organizations. Quantifying risk presents many difficulties, especially when there is a paucity of information about the occurrence or likelihood of an event. From the perspective of risk analysis, this minimal data set significantly constrains the ability to perform a quantitative risk assessment (Garrick et al, 2004). Qualitative methods can be used to screen the risks of terrorist attacks, but much more is required to quantify the risk of genuine threats that have potentially catastrophic consequences. A major challenge in risk analysis of terrorism is the fact that terrorists, unlike nature or engineered systems, are intelligent adversaries and may adapt to the defensive measures.

Garrick et al. (2004) advocates the use of PRA for assessing terrorism risk. The paper offers a systematic methodology of assessing the likelihood of terrorist attacks and emphasizes the nature of terrorism and the information requirements to fight it for effective planning and decision making. The authors illustrate and discuss their methodology with examples from various large critical infrastructures that need to be protected against terrorist threats. Willis et al. (2018) and other researchers operationalize terrorism risk as the product of threat, vulnerability, and consequences. More specifically, threat is usually defined as the probability of an attack (weapon, delivery mode, target, etc.), vulnerability as the probability of an attack's success given that it occurs, and consequences as the losses that occur (fatalities, injuries, direct and indirect economic impacts, among others) given a successful attack. Event trees and fault trees have been used by some researchers to decompose terrorism scenarios in a number of efforts. Rosoff and von Winterfeldt (2007) use event trees to track the paths to failure or success of an RDD attack (Hubbard, 2010). Pate-Cornell and Guikema, (2002) present a model for setting priorities among threats and countermeasures based on probabilistic risk analysis, decision analysis, and elements of game theory. Drawing upon the several recommendations, guidance documents and the past studies, we understand terrorism to be a multicausal phenomenon, and no single method is likely to meet this challenge. Thus, as put forward by Ezell et al. (2010), applying a pluralistic method to quantify the security risk of radioactive materials would efficiently address the entire landscape of radiological terrorism.

1.4 Research Motivations and Objectives

Understanding the true nature of the radiological terror threat is the first order of business for States, policymakers, and the end users. Managing the security of radioactive materials is, however, challenging. Conceptually, the security risk lies at the intersection of threat, vulnerability, and consequences (Figure.1.3), which not only provides an approach for comparing and aggregating terrorism risk, but also provides a clear mapping between risk and methods of managing or reducing risk.

Radioactive materials find extensive use in medicine, industry, agriculture, and research. There are more than 2000 radiation therapy facilities which make use of radiation sources for radiotherapy and nuclear medicine in the United States. Medical facilities, housing radiation devices and radioactive materials are necessarily public places that pose easy targets to an unauthorized access in the absence of rigorous controls. The most widespread medical uses of large radioactive sources (Table1.2.) that pose a greater threat of unauthorized loss, theft or transfer are, the multibeam (gamma knife) units, high dose rate (HDR) brachytherapy seeds, nuclear medicine sources, and blood irradiators. While the sources are in regular full-time use, a determined adversary with the necessary tools could access the sources for malevolent purposes. The daunting question is how do you protect radioactive sources held in a hospital, university, or similar institution with high levels of public access and how do you secure a hospital that may have dozens of entrances/exists? While neither of these challenges are easy, they and others are manageable if they are approached with a right mindset.

Medical facilities, and other similar institutions need to believe that a credible threat exists and clearly understand who their potential adversaries are, their capabilities, and intentions. A key step in achieving the correct mindset is to liaise with international colleagues, who have been though the process and learned the lessons about how to overcome the challenges. The international organizations like the IAEA and the WINS, can be identified as having the resources and the potential to assist with knowledge transfer, they, however, are non-binding where the member States may or may not implement radioactive source security standards or participate in the reporting systems of illicit trafficking of radioactive materials. The United States is one of the member States that has fully implemented a radioactive source security system. The U.S. NRC has been instrumental in regulating low-risk and high-risk radioactive materials from unauthorized access, removal, or theft. In March 2013, the NRC finalized a rule amending the regulations to establish security requirements for the use of risk significant radioactive materials. These amendments were codified as Part 37 of Title 10 of the *Code of Federal Regulations* (CFR). Part 37 addresses topics such as physical security, access controls, monitoring and detection, incident response, co-ordination with local enforcement authorities, and employee trustworthiness and reliability.

Despite U.S. NRC's effective implementation of a graded approach to ensure adequate protection of radioactive materials, the non-partisan congressional Government Accountability Office (GAO) recently reported on the weaknesses in NRC and DHS policies and procedure towards assessing the risks of radioactive materials appropriately. As per the 2019 report, recommendations put forth by GAO to the agency included: (1) Considering socioeconomic consequences along with prompt fatalities and deterministic health effects, when assessing the risk of an RDD; and, (2) Requiring of additional security measures for smaller quantities of radioactive material and circumstances in which multiple small quantities of radioactive material are collected (U.S. GAO, 2019).

In regard to GAO's draft report and the NRC's response to the recommendations, the methodology presented in this study evaluates risk based on socio-economic impacts, along with the fatalities and injuries resulting from the blast, and the deterministic and stochastic effects of the radiation dose. It also accounts for probability of an event, credible adversary capabilities, the protection or safeguards afforded by the existing regulatory framework, and vulnerability hazards of the facility. The States and the competent authority exist to ensure that the security of radioactive material is effective and in compliance within its jurisdiction. The facility operators or licensees are authorized entities that exercise the competent authority's regulations to ensure their security programs meet these requirements and materials remain secure. While the U.S. NRC remains vigilant, it must be difficult for the agency's security experts to co-ordinate with the federal agency and intelligence community to counter any threat that may arise, based on the type and location of the facility.

The proposed methodology, thus, suggests an independent approach for the licensee to evaluate the adversary's objectives or intentions, and to make the decision to attack based on the formulation of utility functions and aspects of game theory. Human failure, another parameter generally attributed towards many nuclear and radiological security related incidents, was identified as a key issue by the CNS 2018 open source report. Human errors, although sometimes unavoidable can be diminished in frequency and severity through a robust nuclear security culture. The IAEA recognizes the importance of instilling a strong security culture in facilities with nuclear and radioactive materials, but it is still yet to be fully discovered by the State governments and the competent authorities. A culture is hard to impose or cultivate but it can be assessed periodically and fostered through positive reinforcement, training, and the sharing of good practices. Like traditional performance audits, security culture self-assessment surveys can help an organization, or a facility learn about nuclear security requirements and understand how culture influences security performance.

The proposed methodology incorporates the human factor related gaps in security systems by measuring multiple nuclear security culture characteristics and performance indicators through self-assessment surveys that are unique to the facility. Cultural change is a long-term process in which tracking and assessing the progress in a continuous basis is essential for improvement. The PFRI metric promotes to institutionalize this activity, preventing complacency from compromising overall security objectives. The risk index model also accounts for deterrence by calculating the payoffs for the attacker and defender as a measure of loss of life and economic consequences, the success probability of the theft or sabotage, and the expected tactics of the adversaries. Deterrence 'by denial', which means persuading the adversary to not attack based on the robust defensive measures and hardened targets, is also integrated in the model through principles of pathway analysis and game theory.

Reinforcing the above-mentioned weaknesses and gaps, the method of quantitative risk assessment presented in this study is one way of doing the analysis. Given that the use of quantitative methods is quite limited, this model is a suggested ‘think tank’ to counter a terrorist RDD threat. To summarize, the focus of this research is the overarching PFRI model with the following objectives:

- Identifying the threats by bringing together the mass of information regarding different types of threat scenarios, different groups of perpetrators, their objectives, intentions, and capabilities;
- Managing risks through vulnerability by integrating the impact of facility locational hazards and human behavior; and,
- Compounding the consequences from blast effects, deterministic and stochastic radiation effects, and socio-economic effects.

This research includes all the relevant criteria for the assessment of risk from an RDD attack.

Additionally, this model gives the operators and the regulators the ability to determine each facility’s performance through a facility level risk index, that can be used as a justification when directing funding to a facility where funds would have the maximum impact. Lastly, a methodology of this sort, could also help overcome the inertia at the political level by equipping the influencers of the state and national government with enough information to better understand the impacts of risk transfer when modifications are made to security systems.

CHAPTER 2. GENERAL RISK FRAMEWORK

2.1 Decomposing risk

Our first challenge is to define the nature of the problem we are trying to solve, i.e., what is risk? To better understand the concept of risk, it is necessary to make a clear distinction between risk and uncertainty. Risk refers to a state of uncertainty where some of the possibilities involve a loss, catastrophe, or other undesirable outcome. Typically, the outcome in risk is unknown, but the probability distribution governing that outcome is known. Uncertainty, on the other hand, is characterized by both an unknown outcome and an unknown probability distribution (Hubbard, 2010). Understanding how to measure uncertainty is a key to measuring risk. Understanding risk, in a quantitative sense, is key to understanding how to compute the value of information. Hubbard (2010) in his book of "*How to Measure Anything",* states that for all practical purposes, the concept of measurement can be defined as a quantitatively expressed reduction of uncertainty based on one or more observation. Even when a more useful concept of measurement is adopted, some things seem immeasurable, because of the lack of an identified *object* of measurement.

To clarify this thought better, let us consider the example of Nobel laureate physicist Enrico Fermi who had a well-developed knack of intuitive measurements. At the first detonation of the atom bomb at the Trinity site, on July 16, 1945, he was one of the atomic scientists observing the blast from base camp. While other scientists were making final adjustments to instruments used to measure the yield of the blast, Fermi was making confetti out of a page of a notebook paper. As the wind from the initial blast wave began to blow through the camp, he slowly dribbled the confetti into the air, observing how far back it was scattered by blast (taking the farthest scattered pieces as being the peak of the pressure wave). Fermi concluded that the yield must be greater than 10 kilotons. This initial assessment was crucial, since other observers did not know that lower limit, and after much analysis of the instrument readings, the final yield estimated was determined to be 18.6 kilotons. Along the lines of Fermi, in ancient Greece, a man named Eratosthenes estimated the circumference of Earth by looking at the different lengths of shadow in various cities at noon and by applying simple geometry. He did not use accurate survey instruments and he certainly did not have lasers or satellites; he instead made a clever calculation on some simple observations. Modern attempts to replicate Eratosthenes's calculations using advanced equipment, resulted in an answer of only 3% short of the actual value. Like Eratosthenes, Fermi was also aware of a rule relating one simple observation (the scattering of confetti in the wind) to a quantity he wanted to measure. These two examples show us that if a thing can be observed in any way at all, then it lends itself to some type of measurement method, and the concept of measurement itself means reduction of uncertainty but not necessarily the elimination of uncertainty. Although this may seem a paradox, all exact science is based on the idea of approximation. As Bertrand Russell, a British mathematician, famously states, *"If a man tells you he knows a thing exactly, then you can be safe in inferring that you are speaking to an inexact man"*. Risk, an uncertain variable is measured as a set of possibilities each with quantified probabilities and quantified losses. Symbolically, risk can be written as:

$$risk = uncertainty + damage \qquad (2.1)$$

Many measurements start by decomposing an uncertain variable into constituent parts to identify directly observable components that are easier to measure. This research decomposes risk as a derived value of threat, vulnerability, and consequences. Kaplan and Garrick (1981) also suggested risk to be quantitively defined as a "set of triplets". Risk, a function of safeguards, can be reduced to as small as possible by increasing safeguards, but it may never, as a matter of principle, be brought to zero.

This research utilizes an established and a standardized approach of Factor Analysis of Information Risk (FAIR) to outline the triplet definition of risk as the probable Loss Event (LE) and probable Loss Magnitude (LM) of future loss. LE is a measure of how often loss is likely to happen. It is the probability, within a given timeframe, that loss will materialize from an individual's action or behavior. LE can either be estimated directly or derived from 'Threat' and 'Vulnerability'. The LM factor in this framework offers a logical breakdown of the consequences into the probable loss of life and the probable economic loss (Figure.2.1.).

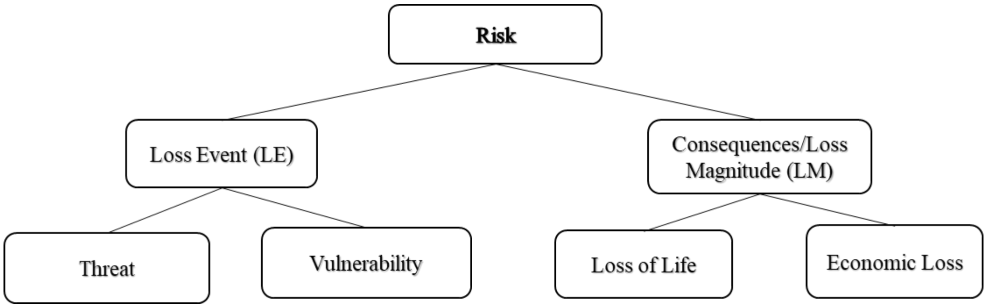


Figure 2.1 General risk decomposition framework

Figure 2.1. gives a basic risk framework, which is refined and enlarged in the later sections. Risk assessments are performed on actions or systems to identify the adverse events that could occur and the frequency with which they are expected to occur. Fundamentally, a risk analysis seeks to answer the following three questions:

i. What can go wrong?
ii. How likely is it?
iii. If it does happen, what are the consequences?

The answer to the first question of risk assessment is given by the component of ‘threat’. A threat is defined as ‘an indication of something impending, or an expression of intention to inflict evil, injury, or damage.’ This definition is extended in this research to the intention of a terrorist to inflict harm or damage to a specific asset or target by a specific means or weapon (Garrick et al., 2004). Identification of threats require technical knowledge of the possible detrimental outcomes of a given activity or action. Analysis techniques can be thought of as using either an inductive (bottom up) or deductive (top down) logical method. Deductive reasoning is where the future behavior is drawn from a set of premises, either true or false. Inductive reasoning is where the future behavior is based on hypothetical experience. This research uses inductive approach to characterize threat by developing a set of plausible attack scenarios and by estimating the probability of theft or sabotage.

Terrorists, unlike natural disasters, are intentional actors who continually evaluate, plan, and seek to exploit the weakest targets. Because of the presence of an intelligent adversary, the assessments of threat are facilitated by the development of attack scenarios, which are bounded in terms of the intentions and capabilities of the terrorist. Developing statistically valid estimates of attack frequencies or success probabilities based on historical data is difficult, as terrorists observe and respond to defenses and to changing political conditions in unpredictable ways. The subject matter experts (SME) and their knowledge base (i.e., the supporting evidence for their opinions), become the basis for assigning an objective probability distribution to the frequency of the attack. Intelligence community and expert elicitation is used to monitor behavior and model the decision process of intelligent adversaries in various security threats.

The answer to the second question of risk assessment is somewhat difficult to answer, as the phrase "*How likely is it?"* can be interpreted in many different ways. In principle, the term likelihood is a measure of probability and frequency, which means that the likelihood of a threat event to materialize into a loss event depends on the probable frequency of the threat agent to come into contact with the asset and the probability of the threat agent to act upon an asset once contact has occurred. This research equates likelihood to vulnerability of the radioactive material that is under regulatory control to fall out of regulatory control and into the wrong hands. Since adversaries are likely to seek out facilities or activities where the material is more vulnerable, this research uses a deterministic approach to identify the factors pertaining to an increase in the vulnerability of the theft of radioactive materials. It recognizes and accounts for all the perturbations and hazards that would directly or indirectly change the probability of success and subsequently affect the likelihood of the adversary choosing a path to their advantage.

The final question of risk assessment introduces the factors that drive the loss magnitude when events occur. Due to the inherent complexity within a loss, it is generally difficult to evaluate loss probability. Assets generally have more than one value or liability characteristic and hence it becomes challenging to put a precise value on assets at risk. In the realm of security risk, the adversary adds additional complexity to the problem. For instance, let us consider a ^{60}Co teletherapy source that is fixed and is enclosed in a heavily shielded container. The potential safety consequences from exposure to such a source is straight forward; the consequence analysis has to only consider the effectiveness of well-defined safety features against a bounded set of potential accident scenarios. Conversely, the security risks of the same source are much more complex to analyze. In the security context, the consequences depend on the type of source stolen, delivery method, capabilities of the adversary to weaponize the source, size of the blast weapon, and the detonation location. This requires the analysis of an essentially unbounded set of attack scenarios, all of which have very different consequences. Measuring the intangible and secondary effects of a terrorist incident is also a challenge. The PFRI consequence analysis conducted in this research measures primary and secondary effects of an RDD attack, including deaths and injuries from the blast effects, physical damage, deaths and injuries from deterministic and stochastic radiation effects, first-order economic effects, such as business interruptions, real estate, and household income ramifications.

Combatting terrorism effectively, therefore, requires an objective and preferably quantitative evaluation of risks, including a firm understanding of threat, reliable information, team work on the part of many segments of society, dimensions of vulnerabilities in the region of interest, and the magnitude of loss. Risk communications, the dissemination of risk information to stakeholders in an understandable form, is an essential part of decision making. Exchanging information to facilitate an understanding of risks enhances the process of developing consensus on issues and taking action in the context of risk management 'best practices' (Garrick et al., 2004). The PFRI model communicates risk to the facility and the stakeholders using a risk chart with a scale of 1-10 with a score of 1 meaning "very low risk" and a score of 10 meaning "very high risk".

The main advantage of the PFRI methodology (described in detail in the later sections) is that, it uses a risk-based approach. The risk informed approach is an iterative process that identifies and assesses threats and risks, and develops, evaluates, and implement alternatives, and monitors and manages the resulting actions for relevance and effectiveness (IAEA, 2015b). The calculated score, unique to the facility, allows the licensee to independently determine the list of physical protection measures that will protect the radioactive sources from a malevolent act. This metric can be used in parallel to the prescriptive approach, where the security measures are fixed and does not quickly adapt to changing threats. The PFRI framework gives the licensee and the regulator the flexibility to incorporate the advantages of the two approaches and assesses the adequacy of the applied physical protection measures.

2.2 Loss Event (LE) – Threats

In order for a threat event to be a loss event, an action must occur, and every action has to have an actor to carry it out. Considering this approach, the PFRI model identifies threats in terms of 'threats to' and 'threats from'. Identification of 'threats to' considers the 'What' element that describes the assets, asset characteristics, and its strategic locations. Identification of 'threats from' is based on the consideration of the ‘Who/Why’ element that describes the type of adversary, their intentions, motivations, and capabilities to a successful attempt of a malicious act (IAEA, 2015b). Sections 2.2.1 and 2.2.2 describes the ‘What’ and ‘Who/Why’ elements in greater detail.

2.2.1 Threats ‘TO’

The ‘What’ component identifies the assets targeted by an adversary. Assets usually have an intrinsic value, are fungible in some way, or create potential liability. In this risk analysis, assets imply radioactive material and devices containing radioactive sources found in the healthcare facility. These assets have certain characteristics that make them more vulnerable to theft and sabotage such as attractiveness, dispersibility, half-life, and portability. In recognition of the fact that human health is of paramount importance, the IAEA has developed a system of categorization of radioactive materials based on their potential to cause deterministic health effects. The concept of ‘dangerous sources’ (which are quantified in terms of ‘D values’) is applied in categorizing the radioactive sources. The D value is the radionuclide specific activity of a source which, if not under control, could cause severe deterministic effects, including both external exposure from an unshielded source and internal exposure following dispersal of the source material. The activity of the radioactive material, denoted by symbol A, varies over many orders of magnitude; D values are therefore used to normalize the range of activities in order to provide a reference in comparing risks. The A/D values are used to provide an initial ranking of relative risk for sources. The A/D values for a range of commonly used sources are given in Appendix I (IAEA, 2005a). The categorization system has five categories and within this categorization system, sources in Category 1-3 may pose a significant risk to individuals, society, and environment. An exposure of only a few minutes to an unshielded Category 1 source may be fatal. Sources in Category 5, on the other hand are the least dangerous; however, even these sources could cause to exceed the dose limits if not properly controlled. Table 2.1. outlines the recommended categories for sources used in common practices.

Table 2.1 Recommended categories for sources used in common practices (IAEA, 2005a)

Category	Source and practice	Activity ratio (A/D)
1	Radioisotope thermoelectric generator (RTGs) Irradiators Teletherapy sources Fixed, multi-beam teletherapy (gamma knife) sources	$A/D \geq 1000$
2	Industrial gamma radiography sources, High/medium dose rate brachytherapy sources	$1000 > A/D \geq 10$
3	Fixed industrial gauges, well logging gauges	$10 > A/D \geq 1$
4	Low dose rate brachytherapy sources, bone densitometers, static eliminators	$1 > A/D \geq 0.01$
5	X ray fluorescence (XRF) devices, electron capture devices, positron emission tomography (PET) check sources.	$0.01 > \frac{A}{D} and$ $A > exempt$

Ranking radiation sources based on their radioactivity content is not sufficient to classify the threat or hazard posed by their presence or use. In particular, the form of the material will have an influence on the exposure scenarios in accident or terrorist attack situations. Material that is dispersible, or in a dispersible form within a sealed source, poses a greater hazard than material that is not dispersible in situations where the source integrity is breached.

A list of sealed radioactive sources (assets) found in the healthcare facility are commonly used in radiosurgery devices, teletherapy machines, brachytherapy, and blood irradiators for the treatment of malignant disease and for blood irradiation. Some well-known examples of such sources that qualify as RDD candidates are given below:

Blood Irradiator

Device category: Category 1, extremely dangerous to the person, if not properly controlled.

Typical range of mass: 1500-3500 kg.

Source and activity: *^{60}Co*, 700Ci (25 TBq); ^{137}Cs, 7000Ci (259 TBq)

Decay mode: Beta decay – 0.512 MeV, 1.176 MeV, gamma decay- 0.662 MeV.

Physical form: Cesium-chloride (CsCl), a salt with chemical properties similar of sodium chloride (NaCl). It is also soluble in water like the common table salt.

Use and characteristics**:** Medical facilities use the blood irradiators to irradiate blood prior to blood transfusions to prevent Graft-Versus-Host-Disease (GVHD)-an immune-related complication caused by white blood cells in donor blood attacking tissues in the body of the recipient, which nearly always prove fatal. Blood irradiation using CsCl is carried out with self-shielded or self-contained irradiators. The shielded chambers are normally shipped, with the sources preloaded, from the manufacturer to the user in a special shipping canister or overpack. When the sources are depleted, they are returned to the manufacturer for service and source replacement, also in a special shipping overpack. The moderate level γ-ray energy emissions lead the shielding requirements to not be so thick as to become impractical.

Multibeam radiosurgery device (Gamma Knife®)

Device category: Category 1, extremely dangerous to the person, if not properly controlled.

Typical range of mass: Shielded spheroidal head containing sources: 1.8-2m diameter spheroid.

Source and activity: 201 encapsulated sources of ^{60}Co, with 30 Ci (1.11TBq) each.

Decay mode: Gamma rays with energies 1.17 MeV and 1.33 MeV, beta decay-0.315 MeV.

Physical form: Metallic

Use and characteristics: Gamma Knife ® is a non-invasive stereotactic radiosurgery instrument used to treat tumors, vascular malformations and other abnormalities in the brain. A control unit allows collimated beams from selected sources in the array to focus on well-defined treatment areas. The shielded cell and cask containing the sources are shipped separately. Depleted sources are unloaded from the machine and returned to a source manufacturer for recycling or disposal.

Remote after-loading high dose rate brachytherapy machine (HDR)

Device category: Category 2, very dangerous to the person, if not properly controlled.

Typical range of mass: Device: 300-600 mm length × 300-600 mm width × 800-1500 mm height, 50-250 kg.

Source and activity: ^{192}Ir, 20 sources of 14 Ci each (500 GBq)

Decay mode: Gamma ray with energy 0.38 MeV

Physical form: Sources are very small 1 mm in diameter; metal pellets.

Use and characteristics: These devices typically use multiple ^{137}Cs, ^{192}Ir or ^{60}Co sources. They are used for cancer therapy by automatically transporting the sources from their shielding in the container into a catheter type tube which has been positioned previously in a tumor site. A radiation dose can be administered directly to the site remotely, maximizing the dose to the tumor with minimal dose to healthy tissue of the patient and no dose to the medical staff. The radioactive sources are stored in a shielded canister in the brachytherapy machine. The unit is mounted on wheels and may be stored in a restricted access area and brought into the treatment area only when in use. The used sources are discharged into a special portable canister, which also delivers the new sources to and from the machine. The canister is used to transport sources between the manufacturer's site and the machine in the hospital. Figure 2.2. presents an overview of the typical ranges of source activity for various uses of radioactive sealed sources.

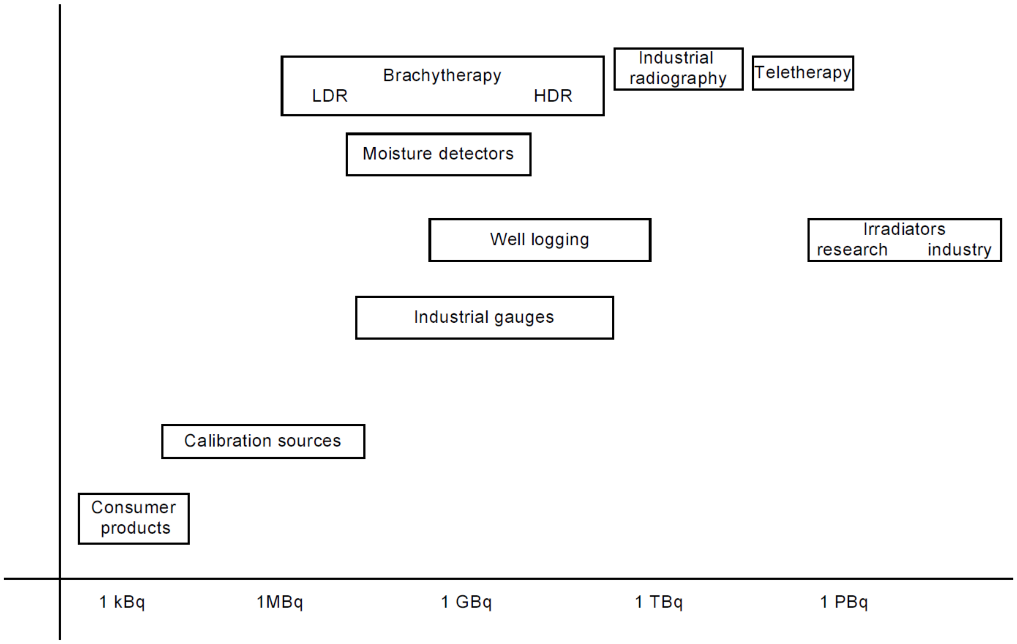


Figure 2.2 Activity ranges for some important applications of sealed sources (IAEA, 2001).

This study limits the asset list to the highest value targets (i.e., high likelihood of success and high impact) available, rather than all the potential targets in the medical facility. The asset characteristics like activity, dispersibility, half-life, and portability make them more vulnerable to theft and sabotage. The attributes of the target, in the shape of relative attractiveness (the A/D ratio) and the physical form are formulated as material utility functions to model facility's uncertainty with regards to the adversary's target preference and its value tradeoffs. Identified targets are prioritized in the PFRI model based on the estimated likelihood of being chosen, on their attractiveness to the adversary, or on the potential consequences of an attack. Characterizing and ranking of the radioactive material (target) with respect to its utility to the adversary, can thus provide a fundamental and internationally harmonized basis for risk-informed decision making.

2.2.2 Threats 'FROM'

The 'threat from' (who) identifies and describes the adversaries who may attempt criminal or intentional unauthorized acts. Identification of 'threats from' (why/how) also considers the tactics and route pathways the adversary may use to seek access to the vital area.

In this risk analysis, the threat agents or attackers are classified into threat communities to effectively estimate the attack strategies. Each of the threat communities are characterized based on their motivations, resources, and capabilities as shown in Table 2.2.

Table 2.2 Modeled adversary groups, motivations and capabilities

Threat Groups	Description	Potential Threat Agents	Motivations	Resources/ Capabilitie s
Group 1 (G1)	Outsiders: External to the targeted facility, highly opportunistic, no authorized access	Extremists, Nationalists, Criminals, Vandals	Apocalyptic beliefs, war on nations, to induce fear and panic	Low-Moderate
Group 2 (G2)	Semi-insiders: May or may not directly be employed by the targeted facility, authorized or escorted access to vital areas	Maintenance crew, third party contractors, security personnel	To induce fear and panic, revenge, religious conflicts	High-Very high
Group 3 (G3)	Insiders: Directly employed by the targeted facility, vetted individuals, have authorized access to vital areas	Technologists, physicians, physicists, hospital staff	Disgruntled employee, personal disappointments , antisocial behavior	Moderate-High

Outsiders or Group 1 (G1) comprise of external actors who prepare and commit a crime by opportunity and against a command structure. An insider or Group 3 (G3) is defined as anyone with knowledge of operations or security systems with authorized access to the vital areas. Insiders, as trusted and vetted personnel, are capable of methods of defeat that may not be available to the outsiders. A full range of insider threats would include an individual or individuals who are passive (e.g., provide information), active nonviolent (e.g., facilitate entrance and exit, disable alarms and communications), or active violent (participate in a violent attack) (Garcia, 2007). Group 2 (G2) are the semi-insiders, who are not directly related to the facility of interest but are employed by the targeted facility as third-party contractors. G2 individuals primarily have the highest capability to abuse system and maximize their chance of success to have access to critical areas and commit a malevolent act. G2 attackers could be anyone from the maintenance crew to the camera and surveillance personnel, law enforcement personnel, students, and other third-party contractors. Most G2 individuals should have undergone a strict background check before having the privilege of an authorized access. Depending on the facility, they may or may not have an escorted access to the vital areas.

The likelihood of stealing or sabotaging the asset depends on the capabilities, motivations, and the resources of the threat community. When considering the threat from different adversarial groups, it must be recognized that even though insiders and semi-insiders from G2 and G3 can have the same motivations as outsiders. Of utmost concern to the theft and sabotage of RAM is the capability and resource of the potential adversary. Although different group of adversaries are expected to use different combinations of tactics, including force, stealth, and deceit to increase their chances of achieving their objective, G2 and G3 actors benefit most through the use of deceit, that is, they bear legitimate credentials and authorization to be near the asset. G1actors, on the contrary, may possess the highest motivation to cause harm, but may lack the capability to get to the source. Some of the motivations that might prompt potential adversaries to undertake criminal actions against a facility may be linked to ideological, economical and, or personal incentives (Garcia, 2007).

This research incorporates the concept of utility functions to include each adversarial group's intent. In addition to drawing on political science and sociology, this study attempts to integrate terrorist ideology and motivations from a psychological perspective. The psychological mindset of an individual who become a terrorist or joins a terrorist groups (explained in further detail in later chapters) and commits public acts of shocking violence are heavily driven by factors such as, political, social, religious, and economical motives. In order to examine each adversarial group's own distinctive mindset, our study measures the intent as symbolism (i.e., sign or object representing a deliberate act of terror), casualties or life loss from the attack, and economic damage from the attack. These three attributes underscore the terrorist groups' goals and their ideological imperatives that distort their ability to see the world with a reasonable amount of objectivity. Swing weights are assigned to each attribute, reflecting the psychological implications from best (high) to worst (low). The overall objective of a terrorist attack is a complex interaction of the attributes with the reputation and goals of the particular terrorist group, e.g., a terrorist seeking to make a political statement without being perceived as evil would be modeled by a low swing weight on loss of life and high swing weights on symbolism and economic loss.

The threat profiling is followed by the development of exhaustive sets of attack scenarios, which emphasize the ‘how/where’ component of ‘threats from’ and describes the characteristics of the particular tactic. Given that the malicious intent of theft and sabotage has unique pathways, developing attack scenarios dictated the potential possibilities that the threat groups must take to execute the task as planned. Pathway analysis, a security assessment evaluation method, forms the basis for the standard Design Basis Threat (DBT) adversarial scenarios. The DBT is a tool used to help establish performance requirements for the design of physical protection systems for specific types of facilities or activities. The scenario development, specific to an asset, comprises specific attributes and characteristics of DBT, including the number of adversaries, type of attack plan, probability of detection, number of entry and exit points, and adversary task times.

Specific to the threat group, this research develops plausible attack scenarios evaluating each asset separately. The path interruption analysis for each asset attack scenario requires detection inputs as probabilities that the total detection function will be successful, delay inputs as mean times for each element and a value for the response force to arrive. The output is the probability of interruption, or the probability that the adversary gets intercepted before any theft or sabotage occurs. The Estimate of Adversary Sequence Interruption (EASI) program is used to analyze a specific path for a single adversary. In order to calculate the overall success probability of theft, the pathway model is followed by the development of a probabilistic model delineating various initiating events, depending on the type of asset and capability of the threat group of interest. The concept of initiating event, famously used in the safety PRA models, is defined as a state that would perturb the steady state operation of the facility and would likely add to the vulnerability and accessibility of radioactive sources from the threat groups. With PRA in a security application, the initiating event proves to be a formidable obstacle since there is no historical evidence of a theft or sabotage attempt of a radioactive material in the United States. Specific to the asset and the attack scenario, this research chooses to identify initiating incidents as mandatory maintenance days, radiation device repair days, source replacement durations, security feature failures, and other equipment unavailability times. Depending on the incident frequency, number of trials and the rate of occurrence, the probability model of binomial, Poisson and normal distribution functions are applied accordingly to estimate the final success probability of theft.

2.3 Loss Event (LE) – Vulnerability

The component of vulnerability integrates the degree of impact of facility locational hazards and human behavior assessed in the context of radiological security. Facility locational hazards include natural hazards, crime, and power outages which may induce a change in the control systems causing a negation of some portions of the safeguard system, making the security ineffective when the threat is real. Human behavior is another key failure that allows the attackers to inflict damage or loss. Downplaying or neglecting locational hazards or human behavior can lead to physical weaknesses or gaps in security that adversaries can exploit.

2.3.1 Locational hazard indicators

Vulnerability described through locational hazard indicators is comprised of natural disasters, neighborhood crime, and the effects of power loss. Physical Protection Systems are intended to protect assets and facilities. A naturally occurring disaster can, however, cause serious damage to the critical infrastructures making it not only susceptible to the damaging effects of a hazard, but also posing a danger to the national security domestically and internationally. Radioactive source security specifically depends on the robust layers of protection, external and internal intrusion alarm systems and sensors, response force communications, and most importantly, an uninterrupted power supply. External events like earthquakes, hurricanes, tsunami or floods accompanied by power loss may cause the security readiness of a facility to be compromised making it more susceptible to crime. This inter-play between human activities and natural events manifests the hazards to be specifically manmade. As the visibility of disruption precipitated by such calamities has escalated in recent years, inclusion of locational hazards in security analysis has become particularly urgent.

Natural hazards

Natural disasters in many ways serve as lightning rods for national and international security problems. More specifically, this research predominately combines event types into three broad categories of natural hazards: meteorological, geological and hydrological disasters. Geological event type identifies, earthquakes, landslides, debris flows, dust devils, dust storms, etc. as the environmental phenomena of this category. Floods, tsunami, heavy rain, heavy snow, waterspouts, and other sudden and destructive distributions or movements of water on land or in atmosphere shapes the hydrological event type. Meteorological disaster comprises blizzards, hurricane, ice storms, tornadoes, droughts, and other major weather-related phenomena. Potential hazard combinations can be very site specific. This study uses the National Oceanic and Atmospheric Administration (NOAA) event database as a comprehensive list of external natural hazards. The database tracks the characteristics of major storms and weather events in the United States, including the state and counties. This risk framework compiles its own database of county specific natural hazards by mining severe weather-related phenomena from the NOAA storm event database.

Crime data

The crime rate in the neighborhood area is another external indicator that is considered in this study, which adds to the component of vulnerability in the model. Crime as a hazard increases fear, rate of victimization, insecurity, and social disorder. In mapping out the geography of crime, many studies have identified the locations, within the larger city for the crime to be more common. Different social and economic histories of every region across the country may also influence the level and type of crime that occurs there. The crime data published by the Federal Bureau of Investigation (FBI) from its Uniform Crime Reporting (UCR) program is used to examine the impact of the neighborhood crime on the radiological security of the healthcare facility. The UCR crime data contains a compilation of the volume and rate of violent and property offenses for the nation, by state and city. The violent crime rate includes the total number of reported homicides, rapes, robberies and aggravated assaults per 100,000 people. The property crime reports offenses of burglary, larceny-theft, and motor vehicle theft per 100,000 inhabitants. The crime trend is collected first by city and subsequently compiled into county, to match the county weather data.

Power disruptions

A variety of events, both natural and manmade, can cause power outages. Power outages can mirror vulnerability for various reasons, such as by intrusion by external agents, which can also significantly impact the security of radioactive material and be problematic for larger facilities like hospitals. Even a small interruption can impede the safety and security of any radiological facility. Widespread outages or power shortages lasting several months, or more are unlikely unless significant components of the bulk power system (generation and transmission) are damaged. Natural disasters could damage any electric power system components, causing widespread outages over a long period of restoration and recovery. The most notable incidents (in South Carolina after Hurricane Hugo; New York City in 1977, or almost the entire Northeast in 1965) have demonstrated that blackouts are very expensive and entail considerable disruption to society (Crane, 1990). Power disruption data used in this analysis details fifteen years of region-based data across the United States. The report uses the compilation of region and facility specific power outage data from the Department of Energy (DOE) driven database. This model accounts for outages from only the major electricity providers and operators.

Correlation between the locational hazard indicators

Considering all the locational hazard factors that have the potential to threaten critical infrastructure, the possibility of physical distortion and social disruption of societies and their larger subsystems can exert an influence on vulnerability. Several studies have found significant correlations between natural disasters, power disruption, and crime incidence (Beccari, 2016; Kwanga et al., 2017). The damages and loses on infrastructure shift the attention of formal and informal security institutions from maintaining social order to coping and recovery measures, thus increasing the vulnerability of affected communities to criminal activities. On a NPR radio interview, the senior vice president of a security intelligence firm had mentioned that natural disasters make major cities vulnerable to national security threats. Power disruption and heightened crime levels occurring in the aftermath of a natural disaster significantly reduce the capacity of emergency response personnel and law enforcement to respond to a potential RDD attack (Crane, 1990).

Natural disasters with the potential to cause extended blackouts include earthquakes, hurricanes, tornadoes, and severe thunderstorms. Each affects the power system differently. In general, earthquakes could damage all types of power system equipment, and are the most likely to cause power interruptions lasting more than a few days. Hurricanes primarily affect transmission and local distribution systems, but the resultant flooding could damage generating equipment (Crane, 1990). As an example, the only hurricane in recorded history to hit the west coast of United States left parts of Oregon and Washington without power for up to two weeks. Tornadoes, most prevalent in the central and southern part of the US, kill hundreds, destroy properties and wipe out substations or generating plants. U.S. electric power systems may not necessarily be attractive to the terrorist, but the disruption of the power system, as a result of natural disasters, can be viewed as an opportunity to attack other critical infrastructures. Healthcare facilities may experience disabled physical security systems during a power outage, and facility security personnel may be less vigilant during emergency evacuations prompted by natural disasters.

Acknowledging that the vulnerability of any healthcare facility varies geographically, the collection of data of the chosen indicators would also vary accordingly. In order to fully assess the "big picture", this research uses a single composite locational vulnerability index emphasizing the screening of hazards based on the site and regional data, and its influence on the facility vulnerability. With each external event indicator being measured in different scales and units, normalization of indicators is performed to ensure that they are comparable. The Minmax normalization method initially developed for the calculation of the Human Development Index (HDI) is used to make data comparable across indicators[1]. Indicator standardization is followed by summarizing the indicators into composite indices and assigning weights based on their degree of influence on vulnerability. For the purpose of this study, a statistical method of Factor Analysis (FA) is applied to aid in selecting appropriate weights. A maximum likelihood estimation (MLE) is used to find factors that maximize the likelihood of producing the correlation matrix. Weights are computed from the factor loading results, which is further applied to summarize all weighted indicators into a single composite metric of vulnerability index.

[1] Minmax normalization is a normalization strategy which linearly transforms x to y= (x-min)/(max-min), where min and max are the minimum and maximum values in X, where X is the set of observed values of x.
UNDP Human Development Report Office, Training Material for Producing National Human Development Report, Occasional paper, March 2015. Available at http://hdr.undp.org/sites/default/files/hdi_training.pdf, Accessed on May 3, 2020.

2.3.2 Human factor - Nuclear/Radiological security culture

Nuclear or radiological security culture, defined as an assembly of characteristics, attitudes, and behaviors of individuals and organizations, is one such indicator that reflects the synergy between the threat and vulnerability (IAEA, 2008). The human factor, including management leadership, is generally a contributor to all nuclear security related incidents as well as malfunctions related to activities involving radioactive material. While both nuclear safety and nuclear security consider the risk of unintentional human error, nuclear security places additional emphasis on deliberate acts that are intended to cause harm. Since security deals with deliberate acts, security culture requires assessment of different attitudes and behavior and an understanding of all individuals engaged in any activity which has an impact on the security of nuclear or radiological activities. For safety culture, all individuals are prevailed upon to share information openly because of this field's necessity for transparency and dialogue. Security culture, on the other hand, restricts communication to authorized persons with a need to know basis but requires that individuals respond immediately to confirmed or perceived threats and incidents. Only personnel that have security culture imbued in them as second nature can continuously evaluate security systems and predict the performance of adversaries against changing scenarios to stay ahead of the threat. Radioactive source users may be technically competent but are still vulnerable if they discount the role of security culture. This study includes security culture as a vulnerability component to recognize the importance of adhering to security practices that can support or hinder any organization's ability to achieve its goals.

An effective nuclear security culture depends on proper planning, training, awareness, competence, knowledge, operations, and maintenance, as well as attitudes and behaviors of all people in the organization. A major reason for the focus on nuclear security culture is increasing incidence of security breaches directly attributable to deficiencies in human performance. One of the case studies for example, which highlights weak security culture, happened at the Y-12 Nuclear Security Complex in July 2012. Three elderly anti-nuclear activists made an incursion into the Y-12 facility, triggering multiple sensors in the process, and gained access to the Highly Enriched Uranium Materials Facility (HEUMF) protected area, where they proceeded to spray paint the side of the building and hang banners. The protestors remained and roamed around in the protected area for some time but did not gain access to the building itself. Cultural issues were apparent in the inadequate initial response to the incident-showcasing the importance that individuals can play in enhancing or undermining nuclear security. In a letter to the security contractor, the NNSA noted that "contributing and direct causes of the security event include an inappropriate Y-12 cultural mindset, as well as a severe lapse of discipline and performance". Since nuclear infrastructure, such a HEUMF, is a highly regulated sector, its security culture model according to IAEA is a combination of top down and bottom up approaches when both practices introduced from the top and attitudes from the bottom are contributing to a culture build-up process. Some of the issues highlighted by the Y-12 event can be attributed to beliefs, attitudes, and approaches at a higher level. Limited levels of oversight of contractor activities and fractured management structure appeared to have led to conflicting priorities.

The Y-12 security event also depicted the relevance to understanding common mechanisms of nuclear security culture and overall organizational culture where the roles in detecting, interpreting, and managing departures from norms and expectations is crucial. The thing that differentiates one organization from another is the extent to which people agree on what is appropriate and how strongly they feel about the appropriateness of the attitude and behavior. If under Y-12's security culture, most people (first responder, security guard, management) would have felt strongly about the importance of certain values related to security, there would have been little latitude for deviation, and slight departures from the norms would have been addressed swiftly and as a matter of priority (Khripunov, 2006).

To investigate and identify the nuclear security culture at a healthcare facility is to understand the perceptions, views, and behavior at all levels of staff and management. This risk analysis uses the organizational-culture model developed by Professor Edgar Schein of the Massachusetts Institute of Technology (MIT), also followed by the IAEA security culture design. Schein proposes that culture in organizations can be considered to exist in layers comprised of underlying assumptions, espoused values, and artifacts. Some of the layers are directly observable while other are invisible and must be deduced from what can be observed in the organization (Khripunov, 2006). This risk framework chooses a survey as a self-assessment tool to help quantify current perceptions and to establish a baseline for comparisons over time. The underlying assumptions and the espoused values of the Schein model is built on the beliefs, values, behaviors, and attitudes of the senior managers and the workforce and is drafted as general questionnaire survey. The third and the most observable layer of artifacts of Schein's model shapes the technical survey questionnaire, involving key characteristics of security functions and component subsystems of deterrence, detection, delay, and response. Respondents' perceptions pertaining to training of personnel in policies, procedures, and operation of equipment is also assessed as a part of understanding those components effectiveness in the facility. Both surveys are tailored to the medical facility environment. A descriptive analysis of both the survey responses gauges the degree of the nuclear and radiological security culture at the facility, which subsequently contributes to the risk index of the radiological facility.

2.4 Loss Magnitude (LM) – Consequences

An RDD is primarily an economic and a psychological weapon. However, depending on the amount of conventional explosive used, the physical damage could be significant and radioactive material is dispersed producing local or greater contamination of the environment. Quantification of risk includes measuring these consequences. While assessing the LM, the study assumes that the theft and detonation of radioactive material as an RDD was successful, regardless of the theft scenario used. The consequences of the RDD attack is mainly divided into two categories: 1) loss of life, resulting from immediate fatalities from the blast, acute radiation exposure, and lifetime cancer risk caused by airborne dispersal of radioactive material; and, 2) economic loss, resulting from lost human capital, decontamination costs, evacuation costs, business losses, lost wages, and property losses.

2.4.1 Loss of life

The type of dirty bomb constructed can vary in sophistication depending on the quantity and type of radioactive material used. The fatalities and injuries from the detonation's blast effects also depend on the type and amount of explosive material used and the population density in the area near the detonation site. When explosives are combined with radioactive materials and detonated, the result is both radioactive and nonradioactive shrapnel, and a radioactive plume. Most injuries and immediate fatalities from an RDD would probably occur from the heat, debris, radiological dust, and force of the conventional explosion used to disperse the radioactive material, mainly affecting only individuals close to the site of the explosion. It is unlikely that an RDD detonation would expose a significant number of persons to critical radiation doses. However, misinterpretation of the explosion as a nuclear detonation may produce fear similar to that produced from a true nuclear detonation. These psychological effects may be significant as mass psychosomatic symptoms due to fear of the effects of radioactive material may be pervasive and severely overload medical support operations. This risk analysis calculates the severity of the life loss consequence (C_{LL}) variable as a function of the casualties from the blast, mortality and morbidity from deterministic effects, and mortality and morbidity from stochastic effects, like cancer, caused by the airborne dispersal of radioactive material.

Blast casualties

Explosives are the most popular choice of terrorists to harm or kill people and damage property. As military explosives become more difficult to obtain, terrorists may choose to make their own conventional explosives using chemicals and precursor materials available to them. Conventional explosive devices used in terrorist attacks are called improvised explosive devices (IED). An IED is a homemade device that is usually unique in nature because its builder has had to improvise by creating it with the materials at hand. These materials could be explosives alone or used in combination with toxic chemicals, biological, or radiological materials. This risk framework assumes the terrorist using a vehicle borne improvised explosive device (VBIED) of different shapes and sizes, depending upon the type of package, container, and means of delivery used for explosive. The addition of radioactive materials (i.e., powder or pellet) to an IED creates an RDD. For explosives, it is common to express the explosive energy as an equivalent weight of trinitrotoluene (TNT) for the detonating materials by relating the explosive energy of the "effective charge weight" of those materials to that of an equivalent weight of TNT (U.S. NRC, 2015). The PFRI risk framework uses hypothetical case examples of different activities of radionuclides combined with various size TNT equivalent explosives. For personnel not directly exposed to an unabated air blast shock wave, human tolerance of blast effects can be considered as relatively high.

The impact of explosives on humans can be classified as primary, secondary, and tertiary. This risk analysis considers and calculates primary effects from direct exposure to the blast-induced pressure wave. The model utilizes effects of various long duration blast overpressures and blast wind on structures and the human body to calculate fatalities and injuries from the primary effects. Primary fragmentation originating from the casing or shielding of the radioactive pellet or the high explosive charge, along with secondary fragmentation from the surrounding structures affected by the detonation, such as glass or masonry, can prove to be dangerous and even lethal to human target. Considering fragmentation is a major source of injuries and owing to the number of known unknowns, i.e., number of fragments produced, impact energy and exact shape and weight of each fragment, a few assumptions are made to calculate the cumulative effects of fragmentation on the human body. Hazard Fragment distance (HFD) for the explosive quantity in kg TNT equivalent is computed to assess fragmentation hazards. In order to calculate the effectiveness of the explosion against a given target area, the risk framework calculates the 'hit probability' from the fragmentation as a function of distance (GICHD, 2017). Structures making significant use of glass-increasingly commonplace in urbanized areas-can be particularly sensitive to the effects of high explosive detonations. Findings from the Oklahoma City bombing is extrapolated to fit the TNT equivalent and the population density of the hypothetical facility under study to help predict the types of injuries resulting from flying glass, debris and ceiling collapse. The nature of explosion and the blast physics model (described in Chapter 3) is thus considered in detail in this risk analysis to account for fatalities and injuries resulting from the explosion.

Deterministic effects

A health effect from radiation for which, generally, a threshold level of dose exists above which the severity of the effect is greater for a higher dose is described as a 'severe deterministic effect'. It may be fatal, life threatening, or result in a permanent injury that reduces the quality of life. As with the other modes of attack, it is very difficult to cause serious deterministic health effects for large numbers of people with an RDD, even a very large RDD (Harper et al., 2007; Rosoff & von Winterfeldt, 2007). It is likely that a Category 1 or 2 source RED could cause serious deterministic effects from external exposures if people are exposed for longer times, at a closer proximity, and with less shielding material between the source and the subject. Internal contamination with a detonated Category 1 or 2 radionuclide increases lifetime cancer risk and can potentially cause acute radiation syndrome (ARS) if enough material is ingested or inhaled. For reference, individuals exposed during the Goiania incident suffered a range of acute injuries, including hematopoietic injuries (HI), gastrointestinal injuries (abdominal pain and diarrhea), as well as a host of prodromal symptoms (fever, nausea, and vomiting) (Adams & Casagrande, 2019) .

Hematopoietic radiation syndrome (H-ARS) is an acute radiation subsyndrome caused by the death of hematopoietic stem and progenitor cells in the red bone marrow. Subclinical depressed blood cell counts may occur at whole-body doses as low as 0.3 Gy but is not life threatening until approximately 2 Gy. Like all acute radiation subsyndromes, the severity of H-ARS increases with dose. At very high whole-body doses (>6-8 Gy), complete ablation of the hematopoietic stem cell pool can occur. Gastrointestinal radiation syndrome (GI-ARS) is caused by the death of crypt and epithelial cells in the small intestine and colon. The threshold for GI-ARS is approximately 6 Gy. If the dose is received to the whole body, GI-ARS would be accompanied by severe H-ARS, and GI hemorrhaging would be complicated by depressed platelet counts (Adams & Casagrande, 2019).

It is expected, therefore, that prompt doses (those coming directly from external radioactive material-above 25 rem (0.25 Gy)) are exceedingly unlikely for most RDD scenarios. Possible exceptions might be a lethal dose from contaminated shrapnel from an explosively driven RDD or from a large gamma source secretly emplaced to irradiate unwitting victims. Other, quite serious and potentially lethal, deterministic injuries from high doses of radiation will occur if the victim ingests or inhales significant amounts of radioactive material. (Zimmerman & Loeb, 2004).

To model the physiological effects and acute radiation injury, the consequence component of this risk framework uses the hazard function concept proposed by Scott (Scott, 1980; Scott & Hahn, 1980), later modified by the IAEA in order to develop emergency response criteria that met the international standards. This hazard function models the characteristics of target organ or tissue (radiosensitivity, potential for repairing injury, etc.) and the exposure scenario (dose, dose rate, quality of radiation etc.). The risk model uses the modified hazard function to calculate the risk of developing deterministic effect from a fragment shrapnel, assuming a contamination of 1% or less of the initially detonated activity of a metallic radioactive material pellet, hitting and wounding an individual. The PFRI framework also calculates the risk of developing deterministic effects in the population within the inner perimeter of ground zero, assuming they may inhale or ingest an activity of detonated radionuclide ten times greater than the respective inhalation and oral annual limit of intake (ALI) . In particular, the model makes use of biokinetic retention functions published by the International Commission on Radiological Protection (ICRP) (ICRP, 2016; ICRP 2017) to compute the effective dose rate of the exposed population, per radionuclide.

Stochastic effects

Stochastic effects are the effects that are, as the name implies, probabilistic. They may or may not occur in any given exposed individual. These effects generally manifest many years, even decades, after the radiation exposure. The fact that ionizing radiation causes cancer is well established. Cancer risk in this study is modeled using the linear no threshold (LNT) model, where there is no lower threshold at which stochastic effects start and assumes a linear relationship between dose and the stochastic health risk. The risk coefficients published by the United States Environmental Protection Agency (EPA) in the Federal Guidance Report (FGR) No. 13 are used in this model to estimate the risk of cancer from exposure to external and internal radiation from the detonated radionuclide. The mortality and morbidity risk per unit intake (Bq^{-1}) and per unit external exposure of the radionuclide is used to estimate radiogenic cancer at low doses. The HOTSPOT atmospheric dispersion model, designed for near-surface short range dispersion, is used to estimate the Total Effective Dose Equivalent (TEDE) values, including the inhalation, submersion, groundshine and resuspension component of the TEDE during the plume passage.

The projection of latent cancer risk due to radiation exposure is estimated from the TEDE values. As in the Biological Effects of Ionizing Radiation (BEIR) VII report(BEIR, 2006), the cancer risk estimate presented here uses a linear function of effective dose and age at exposure. The mathematical model for relative risk (RR), which is the increase in incidence rate associated with exposure, is adjusted for all solid cancers except thyroid and breast cancer as well as leukemia. Since it is difficult to determine if the cause of cancer is entirely due to radiation induction, the concept of the probability of causation (PC), developed by the U.S. National Institute of Health (NIH), is introduced. Probability of causation provides a calculation of excess relative risk (ERR) as a function of radiation dose for each exposure. The stochastic risk estimates are developed based on the population density of the hypothetical detonation site within the inner perimeter of the incident area.

2.4.2 Economic loss

The economic loss consequence severity value (C_{EL}) is comprised of human capital loss, decontamination cost, evacuation cost, business interruption cost, lost household income, and impaired real estate value.

The value of a statistical life (VSL), currently used by the U.S. Department of Transportation from Viscusi & Masterman (2017) methodology is used to assess the loss of human capital in this study. The distribution of casualties from the Oklahoma City bombing is used to estimate the cost of medical care and the value of lost income, amounting to losses from injuries and disabilities (Mallonee et al., 1996). Business interruption losses are a measure of the reduction in the flow of goods and services, representing lost sales revenue in gross terms. The extent of business sale declines would correspond to the established contamination deposition contours and the required amount of time governing the cleanup to the existing standards and protective action guidelines. In addition to the stigmatization of businesses in the contaminated region, property values in the plume area will also experience a significant reduction in the real estate figures. The business disruptions may even have a ripple effect on the household income and the employment rate statistics, temporarily or permanently, especially if a majority of businesses relocate outside of the region or cease to exist (Rosoff & von Winterfeldt, 2007).

The response to an RDD incident requires decontaminating and remediating a large portion of the contaminated area. The cleanup standard applied in this study was based on NRC regulations (U.S. NRC, 1991). According to the regulations, the TEDE to individual members of the public in unrestricted areas should not exceed $1\ mSv\ yr^{-1}$ or $0.02\ mSv\ hr^{-1}$. The ICRP also recommends that the long-term goal for people living in a contamination zone should be to reduce the contamination to a level at or below $1\ mSv\ yr^{-1}$, an additional dose over and above the background terrestrial dose but also within the range of a typical background annual dose. Studies have indicated that RDDs would likely produce heterogeneous patterns of contamination (U.S. EPA, 2016). Decontamination techniques, including scrubbing and flushing of surfaces with uncontaminated water and the disposal of contaminated soil, would be applied to reduce surface contamination to the required limit of $5000\ dpm\ 100cm^{-2}$ for beta-gamma emitters (U. S. NRC, 1982). Because the decontamination time for most RDD scenarios is difficult to predict, studies have analyzed scenarios ranging from short (15 days) to long (1 year) time frames (Rosoff and Von Winterfeldt, 2007).

The amount of effort required for decontamination will be a function of how much contamination exists relative to the allowed residual contamination, which in this risk model is assumed as $1\ mSv\ yr^{-1}$. Reducing the dose level to $1\ mSv$ may require demolition or waiting years for physical decay and weathering to reduce the dose. The data from Fukushima indicate that areas contaminated with ^{137}Cs were particularly difficult to decontaminate because of its chemistry and that even the surface removing technologies, such as scabbling, were only able to achieve a decontamination factor (DF) of around 2-3. This relatively low DF may not even be possible to satisfactorily cleanup those areas where the initial contamination exceeds $3\ mSv\ yr^{-1}$. The methodology from Reichmuth, Short, & Wood (2005) of developing unit cost factors ($\$\ km^{-2}$) for the cleanup of areas having different levels of population density, where population density is a surrogate for economic activity, is used to estimate the costs of decontamination services and the replacement of contaminated structures (Reichmuth et al., 2005). The total economic consequence estimate is calculated to be a numerical value between 0 and 1 that represented the severity of the monetary loss directly or indirectly resulting from an executed RDD threat incident.

Combining the inputs from the loss event (LE) and loss magnitude (LM) yields the Potential Facility Risk Index (PFRI) as shown in Figure2.3.

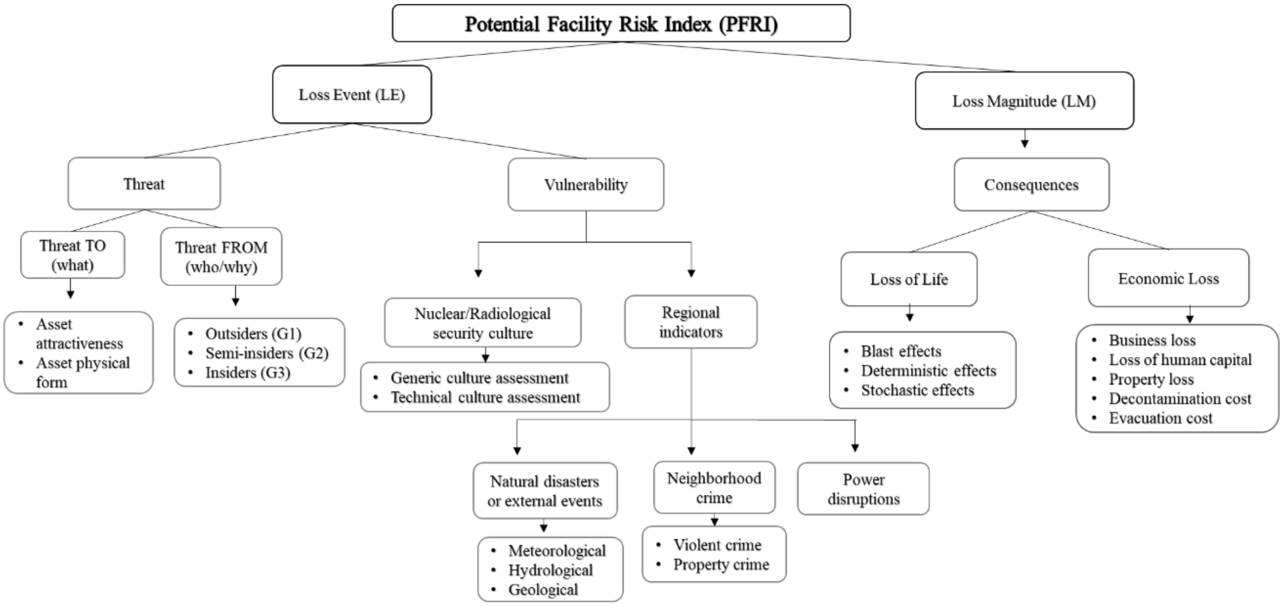


Figure 2.3 The complete Potential Facility Risk Index (PFRI) framework

2.5 The Potential Facility Risk Index (PFRI)

The PFRI risk framework presented in this dissertation is strictly a facility based approach, meaning the risk is unique to the facility, depending on the type of radiological facility, location of the facility, number and types of devices available at the facility, the radiological security culture found at the facility and so on. The PFRI index framework tree (Figure2.3.) gives a clear visualization of the multi-dimensional inputs of threat, vulnerability and consequences, hence being the premise of a quantitative evaluation of risk. The PFRI in this research is mathematically represented as the exponential product of the maximum expected utility among the threat groups, the sum of the geographic vulnerability and cultural vulnerability, and the net consequences of loss of life and economic loss.

The PFRI risk metric is one composite number that effectively and succinctly communicates risk to the decision makers. Quantitative values are viewed as a good thing, as it demonstrates estimates based on your underlying scientific and data-intensive approach but is sometimes harder to follow or implement than its qualitative counterpart. A combined approach is, therefore, unquestionably stronger. This research conducts qualitative and quantitative risk analysis in tandem, where the psychology of a terrorist mindset, its motivations along with the attributes and symbolism of the malevolent act is subjectively assessed to be numerically presented in the form of utility functions. The final PFRI metric is also qualitatively defined on the scale: high, medium, or low. A three-dimensional matrix (threat, vulnerability, consequences), presented using heat maps, gives a holistic visual of an entity wide security risk. Heatmap color bands effectively translate between the quantitative results and the qualitative levels. The facility radiological risk is thus quantified using a qualitative scale of “very low risk” to “very high risk”.

As an extension to the PFRI, this research uses game theoretical models to consider how players with conflicting interest interact in situations of interdependence, the strategies they choose, and how they assess the values of outcomes by choosing those strategies. The reason behind mapping the PFRI risk assessment to game theory is to construct a well-defined decision rule that let us find the best decision when the outcome is uncertain.

CHAPTER 3. THEORY AND METHODOLOGY

3.1 Preferences and Utility functions

The notion of preference has a central role in many disciplines, including economics, social science, moral philosophy and decision theory. The idea of preference and its analysis varies among the disciplines. This research incorporates the economic theory of preference and utility function to solve for the RDD asset preference in the threat component of security risk assessment.

3.1.1 Preferences

Let us define a consumption bundle as a combination of quantities of the various goods (and services) that are available, which is represented as X and Y. The consumer has preferences over consumption bundles. The consumer can compare the bundles and decide which one is better, or decide they are equally good. The symbol $\succ$ represents this consumer's preference relation. That is, $X \succ$Y means that consumer prefers bundle X over bundle Y. We assume that if $X \succ$Y, then $Y \succ$X cannot be true; therefore the $\succ$ relation is sometimes also called the strict preference relation rather than the preference relation, because $X \succ Y$ means the consumer definitely, unambiguously, prefers X to Y, or strictly prefers X to Y. If the consumer likes X and Y equally well, we say she is indifferent between them, which is represented as $X \sim Y$ in this case, and $\sim$ is called the indifference relation. We assume that if $X \sim Y$, then $Y \sim X$ must be true. If the consumer is either preferring X to Y, or being indifferent between the two, then Y is said to be weakly preferred to X, represented as $X \succcurlyeq Y$.

The four axioms of completeness, transitivity, reflexivity, and monotonicity enable the preference relations to realistically model the behavior of what we would consider a rational consumer.

Completeness: For all consumption bundles X and Y, either $X \succcurlyeq Y$ or $Y \succcurlyeq X$ or both. The rationale for this axiom is that all consumers have well-defined preference for the consumption of goods. That is, the consumer must like one better than the other, or like them equally well.

Transitivity: if $X \succ Y$ and $Y \succ Z$, then $X \succ Z$. For any three outcomes X, Y, and Z, if X is preferred to Y, and Y is preferred to Z, then X must be preferred to Z. This assumption implies a number of other transitivity results, such as, if $X \sim Y$ and $Y \sim Z$, then $X \sim Z$; and if $X \succ Y$ and $Y \sim Z$, then $X \succ Z$, and finally if $X \sim Y$ and $Y \succ Z$, then $X \succ Z$.

Reflexivity: Any bundle X is always at least as preferred as itself, i.e. $X \succcurlyeq X$

Monotonicity: If X is a bundle of goods and Y is a bundle of goods with at least as much of both goods and more of at least one, then $Y \succ X$, meaning the consumer prefers consuming more of a good to consuming less (Varian, 1992).

The first two axioms of completeness and reflexivity are straightforward and hardly objectionable. The third axiom of transitivity is more problematic. The assumption that preferences are transitive does not seem compelling on grounds of pure logic alone. Transitivity is a hypothesis about people's choice behavior, and not a statement of pure logic. The assumption of monotonicity is saying that the situation will be examined before any satiation sets in-while more still is better. This whole theory of consumer choice, also known as "Rational Choice Theory" (RCT), postulates the individual as the subject of analysis that is assumed to possess preferences and act rationally to allow for preferences to satisfy the basic axioms.

3.1.2 Utility functions

The preferences of the consumer are the fundamental description useful for analyzing choices, and utility is simply a way of describing preferences. Utility theory is a foundation for the theory of choice under uncertainty. In economics, the term utility refers to the happiness, benefit or value a consumer gets from a good or service (Varian, 2010). A utility function mathematically characterizes every possible consumption bundle such that more-preferred bundles get assigned larger numbers than less-preferred bundles. Let bundle $X = (x_1, x_2)$ and $Y = (y_1, y_2)$, such that

- A bundle (x_1, x_2) is preferred to a bundle (y_1, y_2) if and only if the utility of (x_1, x_2) is larger than the utility of (y_1, y_2) : Symbolically, $(x_1, x_2) \succ (y_1, y_2)$ if and only if $u(x_1, x_2) > u(y_1, y_2)$.
- Secondly, $u(x_1, x_2) = u(y_1, y_2)$, whenever $(x_1, x_2) \sim (y_1, y_2)$.

Based on the preferences, the utility function can be classified as either a cardinal utility function or an ordinal utility function. Cardinal utility functions reflect the preferences of decision makers on the bundles as values measured in units of "utils" defined as the exact amount of satisfaction from consumption of the bundle realized by the decision maker. Ordinal utility functions show the ordinality of preference for the decision maker between the available bundles without giving the exact magnitude of satisfaction realized by the decision maker from any given bundle. The only feature of a utility function that is necessary to model most decision processes is the ordinality of preferences, as it is more practical and sensible to rank utility on the basis of 'satisfaction' than measurement units of 'utils', and the ordinality of preferences is the basis for deciding between bundles. Utility can also be graphically represented using indifference curves. An indifference curve is a set of consumption bundles which the consumer thinks are all equally good; she is indifferent among them. Figure 3.1. shows two consumption bundles, X and Y, and an indifference curve. The two bundles are on the same indifference curve, and therefore the consumer likes them equally well.

$$Indifferent\ Curve = \{x \in X | u(x) = const\}$$

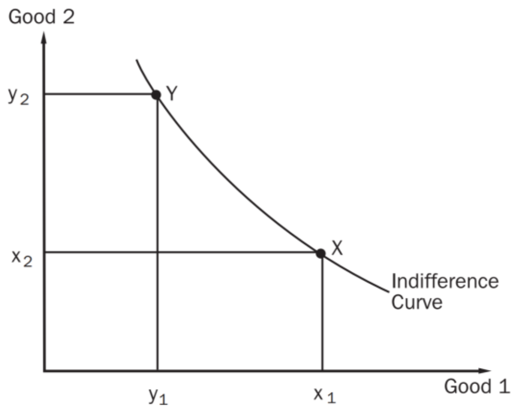


Figure 3.1 An indifference curve, where X and Y are on one indifference curve, the agent is indifferent between them.

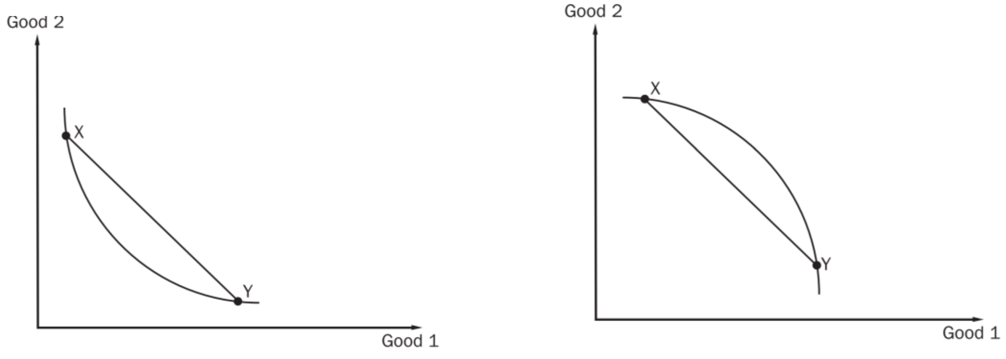
The slope of the indifference curve measures the rate at which the agent is willing to substitute one good for another. This slope is called the marginal rate of substitution or MRS. Mathematically,

$$MRS = -\frac{dx_2}{dx_1}|_{u(x_1,x_2)=const} \tag{3.1}$$

The MRS can be related to the agent's utility function through the idea of marginal utility, where the agent's utility changes as we give her a little more of good 1. The assumption of monotonicity of preferences (discussed in 3.1.1) implies the shape of the indifference curves into convexity and concavity.

Convexity for indifference curves mean that averages of consumption bundles are preferred to extremes. For any two distinct points on the same indifference curve, the line segment connecting them lies above the indifference curve, as shown in Fig. 3.2(a). In other words, if we take a weighted average of two distinct points, between which the consumer is indifferent, she prefers the weighted average to the original points.

Concavity for indifference curves: In reality, of course, indifference curves are sometimes concave, where a consumer might like two goods, but not in combination. For example, you may like classical music and hip-hop, but not in the same evening or you may like sushi and chocolate ice cream, but not together in the same dish. In a concave curve, the slope of the curve decreases as we move to the right along the graph, implying the concept of diminishing marginal rate of substitution. Figure 3.2(b) shows the concave indifference curve.



(a) (b)

Figure 3.2 (a) A convex indifference curve (b) A concave indifference curve.

For a typical utility function satisfying the monotonicity axiom, "more is better", meaning that total utility increases monotonically with the quantity of goods consumed. However, utility functions typically have diminishing marginal utility for the sake of realism. Most goods have a threshold level of consumption where the consumer reaches satiation, so it is reasonable to model the consumer's marginal utility as decreasing up to the point of satiation, e.g. the quantity of water drunk at a meal offers increasing utility (and decreasing marginal utility) to the consumer up to a satiation point, after which additional water makes the consumer feel bloated or even experience water poisoning. Figure3.3 shows the total utility vs the marginal utility.

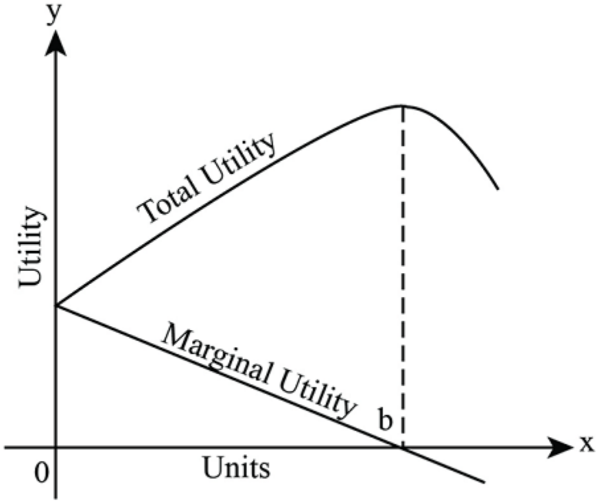


Figure 3.3. Total utility vs Marginal utility, showing the threshold level where the consumer reaches satiation.

In an uncertain environment it becomes necessary to ascertain how different individuals will react to risky situations. The von Neumann-Morgenstern utility function, an extension of the theory of consumer preferences or RCT, incorporates a theory of behavior toward risk variance. We use the von Neumann-Morgenstern utility function to explain risk averse, risk-neutral, and risk-loving behavior.

Before discussing the properties of risk variance, it is important to understand the concepts of utility maximization and expected utility. Utilitarian moral theory postulates that individuals should maximize the utility resulting from their actions.

The *Utility Maximization rule*, states that $\frac{MU_x}{P_x} = \frac{MU_y}{P_y}$, where MU_x is the marginal utility derived from good x, P_x is the price of good x, MU_y is the marginal utility derived from good y, P_y is the price of good y. A consumer should spend their limited money income on the goods which give her the most marginal utility per dollar. Only when the ratio $\frac{MU}{P}$ is equal for all goods is a consumer maximizing their total utility.

The theory of utility maximization gives a complete account of rational choice under certainty, but under uncertainty it seems intuitive to assign a probability to each of the states of nature and that individuals would maximize expected utility (EU). *Expected utility* could, more precisely, be called "probability-weighted utility theory", where each alternative is assigned a weighted average of its utility values under different states of nature, and the probabilities of these states are used as weights.

$$E(U) = \sum_i^n U(\,w_i)P_i \qquad (3.2)$$

where,

$E(U)$ is the expected utility

$U(w_i)$ is the utility of the ith outcome w_i; and

P_i is the probability of the ith outcome

The expected utility theory ranks events which have an uncertain outcome and captures the different risk attitudes of individuals. Risk averse individuals tend to prefer safe activities to risky ones. In other words, their utility for a risky activity is always lower than the utility derived from an activity with the same expected value but without risk. A concave utility function represents a risk-averse individual. By contrast, a risk-seeker always derives higher utility from a risky activity than from a riskless activity with the same expected value; risk is a positive characteristic for a risk-seeker. If an individual's utility function is linear, then she would be risk-neutral, as she is indifferent between accepting a known certain outcome or accepting a risky activity that has the same expected value.

3.1.3 Asset utility

This research uses the RCT concept of methodological individualism to explain the collective behavior of an adversary group. In this view the collective actors such as terrorist groups are said to behave as unitary actors reflecting one stable configuration of preferences and consistent goals. This study develops material utility functions $U[mat]$ to rank the relative attractiveness of each asset to a group of terrorists. For a set of radionuclides $I = \{Co, Cs, Ir\}$, the terrorist group ranks their preferences based on the amount of utility associated with the radioactive source material such that $U[Cs] \succ U[Co] \succ U[Ir]$.

The material utility function $U[mat]$ is a product of the attractiveness utility function ($U_i[attractiveness]$) and the form utility function ($U_i[form]$) (Eq. (3.4) and Eq (3.5)). $U[mat]$ incorporates two attributes: the relative attractiveness of the radiological material based on the IAEA categorization system, and the physical form (e.g., metallic, powdered salt) of the radionuclide. $U_i[attractiveness]$ is defined using the activity ratio (A/D), where A is the activity of the radionuclide (TBq) and D is the radionuclide-specific normalizing factor or the danger value (TBq) (Eq. (3.4)). $U_i[attractiveness]$ increases monotonically with the $\frac{A}{D}$ ratio, which measures a broad range of deterministic health effects but excludes stochastic health effects and economic consequences (Harper et al., 2007).$U_i[form]$ ranks the asset's dispersibility effect (Eq. (3.5)). For any level of radionuclide attractiveness, the physical form can make a significant difference in the aerosolization potential of the radionuclide (Harper et al., 2007). Terrorist adversaries would typically perceive materials with greater attractiveness and dispersibility to be more lethal, so it is reasonable to model their total utility of material, $U[mat]$, as the product of utility functions that increase monotonically with the A/D ratio or the physical form of the material(Myers et al., 2012).

$$U[mat] = U_i[attractiveness] \times U_i[form] \qquad (3.3)$$

$$U_i[attractiveness] = 1 - e^{(-\left[\frac{\frac{A}{D}}{m_r}\right]^3)} \qquad (3.4)$$

$$U_i[form] = 1 - e^{(-[F_r]^3)} \qquad (3.5)$$

where

i is the index of the radionuclide (weapon chosen as a dispersal device).

A is activity of the radionuclide in TBq.

D is the danger value of the radionuclide in TBq.

m_r is the mass of the radionuclide in kg; and

F_r is the physical form index of the radionuclide

(metal = 1, powdered salt = 2)

3.1.4 The psychology of a terrorist

In this study, the nouns “terrorist or “terrorists” do not necessarily refer to everyone within a terrorist organization. Members from previously defined threat groups, G1, G2, and G3 may play only a passive role and may not personally carry out a group’s terrorism strategy. Terrorist activists or operatives who carry out orders to perpetrate a malicious act have generally been recruited into the organization. Thus, their motives for joining may vary. New recruits are often isolated and alienated young people who want to join not only because they identify with the cause and idolize the group’s leader, but also because they want to belong to a group for a sense of self-importance and companionship (Morris et al., 1987).

If one accepts the proposition that political terrorists are made, not born, then the question is: what makes a terrorist? The psychological approach to terrorist radicalization is concerned with characterizing at-risk groups for radicalization, their recruitment and induction into terrorist groups, and their personalities, beliefs, attitudes, motivations, and careers as terrorists. Although the scholarly literature on the psychology of terrorism has large gaps, many anthropologists and other social scientists have found frustration-aggression, negative identity, and narcissistic rage to be the most widely recognized psychoanalytic behaviors that explain terrorist radicalization (Bruneau, 2016).

The Olson hypothesis suggests that participants in revolutionary violence predicate their behavior on a rational cost-benefit calculus concluding that violence is the best available course of action given the social conditions. The notion that a group rationally chooses a terrorism strategy is questionable and is further discussed in Section 3.2.2.

3.1.5 Motivations and Behavior

This study draws on the disciplines of psychology and sociology in an attempt to explain terrorists' motivation and to address their mindset. The risk analyst needs the help of the social scientists who are most able to shed some light on issues of terrorist objectives, including the possible shift in preferences with changes in the availability of means. Although it may be comforting to think of terrorists as people unlike us, Dr. Bruneau argues that this belief belies an uncomfortable reality: that the psychological processes that drive an individual to engage in terrorism are deeply human, common across cultures and are traits that likely reside in us all. Dr. Bruneau, in his article of "Understanding Terrorist Minds", offers some insight into the mind of a terrorist by looking at what lies in the human mind more generally. Expounding from his studies, below is a list of some behavioral factors that make individuals commit public acts of shocking violence (Um, 2009).

<u>Social factors</u> – Evolution has shaped within us a deep desire to belong to groups. In modern times, social belonging remains a major psychological need which we fill by connecting with others thorough a variety of 'social identities. From this perspective, the appeal of 'terrorist groups' is completely unremarkable. Just as a fraternity, club, team, or a gang can provide a deep social connection with others, so too can ISIS, Al-Qaeda, or white nationalist groups. The people who are at risk for joining the terrorist group are not those who are poor or violent, but those who are alienated and thus are drawn to the offer of brotherhood, camaraderie, and sense of purpose.

<u>Ideology brain </u>– Terrorist groups believe in their strict adherence to an ideology. Terror groups which are composed of an aggrieved minority often have their ideology centered around a narrative of victimhood. Whether about victimhood or not, ideologies are incredibly persistent. Part of what gives them momentum is a set of cognitive filters that help process incoming information to support and enhance the in-group's ideological narrative. Confirmation bias, for instance, describes the tendency to uncritically accept information that confirms the group's beliefs and scrutinize anything that runs counter to their ideological leaning. Another critical bias concerns the way that we construe the deviant actions of others. If I find myself doing something wrong (e.g., cutting late into a merging lane), it is easy for me to justify this by external circumstances (e.g., "I was late for an important meeting"). But when I see others doing the same, I tend to attribute this to their internal characteristics (e.g., "they are selfish jerks"). As was famously expressed by the comedian George Carlin, "Have you ever noticed that anybody driving slower than you is a moron, and everybody

driving faster than you is a maniac?” Terrorists view the world within the narrow lens of their own ideology, whether it be Marxism-Leninism, anarchism, nationalism, Islamic fundamentalism, or some other ideology. Most researchers also agree that terrorists generally do not regard themselves as terrorists but rather as soldiers, liberators, freedom fighters or martyrs. They are parochial altruists who are willing to die on the behalf of their group’s ideology.

Violence brain – Perceived injustice has long been recognized as a central factor in understanding violence. Our brains are structured with the capability to care deeply, but also to kill. This ambivalence deeply rooted in brain structure is potentially problematic. It is not difficult to imagine that one of the strongest motivations behind terrorism is vengeance, particularly the desire to avenge not oneself but others. Economic, ethnic, racial, legal, political, religious, or social grievances are important precipitant causes of terrorism.

Identity and belonging – An individual’s search for identity may draw him or her to extremist or terrorist organizations in a variety of ways. The absolutist, “black and white” nature of most extremist ideologies is often attractive to those who feel overwhelmed by the complexity and stress of navigating a complicated world. In radical extremist groups, many prospective terrorists find not only a sense of meaning, but also a sense of belonging. Some analysts even have suggested that the synergistic effect of injustice, identity and belonging forms the real “root cause” of terrorism, regardless of ideology (Selten, 2001).

A principal reason for the lack of psychometric studies of terrorism is that researchers have little, if any, direct access to terrorists, even imprisoned ones. From the perspective of risk analysts trying to anticipate these behaviors, they require estimating the potential perpetrators’ utilities of the possible outcomes of different types of attacks, and their expectations about their chances of success. In this study we try to quantify the perpetrators’ actions and their motivations with respect to the following attributes: loss of life, economic loss and symbolism.

3.1.6 Bounded rationality

Scholars of terrorism studies have long struggled to agree on a common understanding of what terrorism is if the behavior of terrorists can be characterized as rational (Simon, 1957). Translating the decisions of instrumentally rational individuals into economic terms and applying these decisions to the issue of terrorism, terrorists are assumed to maximize utility over time. They will use violent means as long as the expected benefits outweigh the expected costs. Perceiving individuals as fully informed, utility maximizing actors has received widespread criticism in the academic debate. "Fully rational man is a mythical hero who knows the solutions of all mathematical problems and can immediately perform all computations, regardless of how difficult they are"(Etzioni, 2010).

A widely known alternative to rationality is the idea of *bounded (limited) rationality* that was introduced by Herbert Simon (Ruby, 2002) to account for the cognitive limitations of the decision maker. The theory of subjective expected utility underlying neo-classical economics postulates that choices are made: (1) among a given, fixed set of alternatives; (2) with (subjectively) known probability distributions of outcomes for each alternative; and (3) in such a way as to maximize the expected value of a given utility function (Crenshaw, 2000). Bounded rationality deviates from these assumptions by recognizing that people are hardly capable of estimating all possible consequences of their actions. The "bounds" on rationality limit the decision criteria to what are perceived to be most crucial aspects of the outcome. Bounded rationality is understood to be a flawed decision process because consequences might be misjudged or ignored. Furthermore, even the most rational actor is assumed to make decisions under uncertainty and without the ability to eliminate all possible side effects. According to Simon, people do not maximize their utility but rather satisfice to achieve an acceptable level of utility, which stands in contrast to the utility maximizing concept of RCT. Bounded rationality needs to be further distinguished from irrationality.

Irrationality may actually come in many shapes and would not necessarily have to reflect individuals violating all of the axioms of RCT. Studies have at times proposed to consider terrorist actions to be rather bounded rational or even irrational.

Psychological analyses were formerly thought of as providing an adequate answer to the roots of terrorism based on the idea that terrorists were mentally abnormal or disturbed. Empirical research and interviews conducted with former terrorists, however, have widely rejected the idea that terrorists are mentally ill or psychotic or that they feature common mental defects or disorders (Crenshaw, 2000). Instead, there is good reason to believe that "the outstanding common characteristic of terrorists is their normality and that terrorists, by and large, are not insane at all" (Wasson & Bluesteen, 2017). These findings suggest terrorists to be rational actors. Still, it should not be left unmentioned that most psychological hypotheses about terrorist behavior are based on speculation or are derived from such a small number of cases that the findings cannot be considered reliable. In contrast to the prevailing view in the psychological literature of terrorist behavior generally not being explained by mental pathologies, a psychological study analyzing the personalities of five so-called lone-wolf terrorists[2] revealed that three of them suffered from personality disorders such as schizophrenia, anxiety disorder and obsessiveness.

While the concept of instrumental rationality clearly lacks explanatory power for at least parts of terrorist behavior, neither does the concept of irrational behavior explain all terrorist actions. Bounded rationality might provide the missing link to account both for apparently irrational behavior but also for thoroughly calculated means to reach political goals. While bounded rationality provides the underlying model, deciphering its significance for non-strategic deterrence requires understanding the psychology of human cognition. Daniel Kahneman explains the major cognitive processes generally agreed to be operating: System 1 (intuition) is passionate, reflexive, involuntary, and hard to change; while System 2 (reasoning) is purposeful, conscientious, and malleable. There is a substantial body of empirical research in psychology that has identified numerous System 1 biases. They include accessibility, where humans are unable to collect and recall every piece of relevant information for any particular activity, and because of this inability prejudice creates a selection effect in which choices available to an actor do not represent the true population but rather a truncated sample. Other System 1 biases include availability, representativeness, and relativity. Availability has to do with how people estimate the frequency or probability of something. Instead of making objective evaluations on the basis of fact, humans tend to give greater weight to those impressions that are more readily available mentally. Representativeness refers to the propensity of the human mind to evaluate the probability or value of something based on its similarity to archetype (prototype heuristics) as opposed to using base-rates and accounting for uncertainty. Related to representativeness is a fourth category of bias,

[2] Lone-wolf terrorists are individually acting terrorists who do not belong to an organized group and act without the influence of a leader or hierarchy,

relativity. Relativity biases arise because human beings do not make absolute value judgements but instead assess everything relative to something else.

The aforementioned biases are just some ways that the bias of intuition can cause human beings to systematically deviate from what might objectively be considered optimal behavior (Keeney, 1977). By shaping how information is presented, defenders may be able to take advantage of threat actor's biases to induce deterrence in the RDD game, discussed in Chapter 6.

3.2 Adversary utility

The objectives or intentions of the previously discussed threat groups (Table. 2.2) are also formulated using utility functions. Since terrorism is a multicausal phenomenon, each adversarial intent is measured using a set of attributes X_k. Attributes are any measurable characteristic that may influence a decision. The attributes of the adversary are defined as the symbolism of the attack (X_{SY}), the life loss caused from the attack (X_{LL}), and degree of economic damage from the attack (X_{ED}). Adversity utility uses a *multi-attribute utility function (MUF)* to quantify preferences.

3.2.1 Multi-attribute utility functions

Let us designate our set of attributes as x_1, $x_2 \ldots . x_n$. With this convention, the consequence of any alternative is $x = (x_1, x_2, \ldots x_n)$. For each alternative A_j, a probability distribution $P_j(x)$ indicates which consequences might occur and its likelihood. The preferences are quantified by assessing the decision maker's utility function $u(x) = u(x_1, x_2, \ldots x_n)$. The argument of the utility function is a vector indicating levels of the several attributes. The multi-attribute utility function has two properties which make it useful in addressing the issues of uncertainty and tradeoffs between objectives. These properties are:

- $u(x') > u(x'')$ if an only if x' is preferred to x'', and
- In situations with uncertainty, the expected value of u is the appropriate guide to making decisions, i.e., the alternative with the highest expected value is the most preferred. The second property follows directly from the axioms of utility theory postulated first by von Neumann and Morgenstern (Keeney, 1977).

The study of terrorism is further complicated by the fact that it is difficult to identify terrorist leader preferences. Collecting data on terrorist leaders' values and beliefs is a formidable task given the sensitive nature of the information and the restricted public availability of intelligence information. This study describes the construction of an adversary utility function based on the threat group profile swing weights on the attributes X_{LL}, X_{EL}, and X_{SY}.

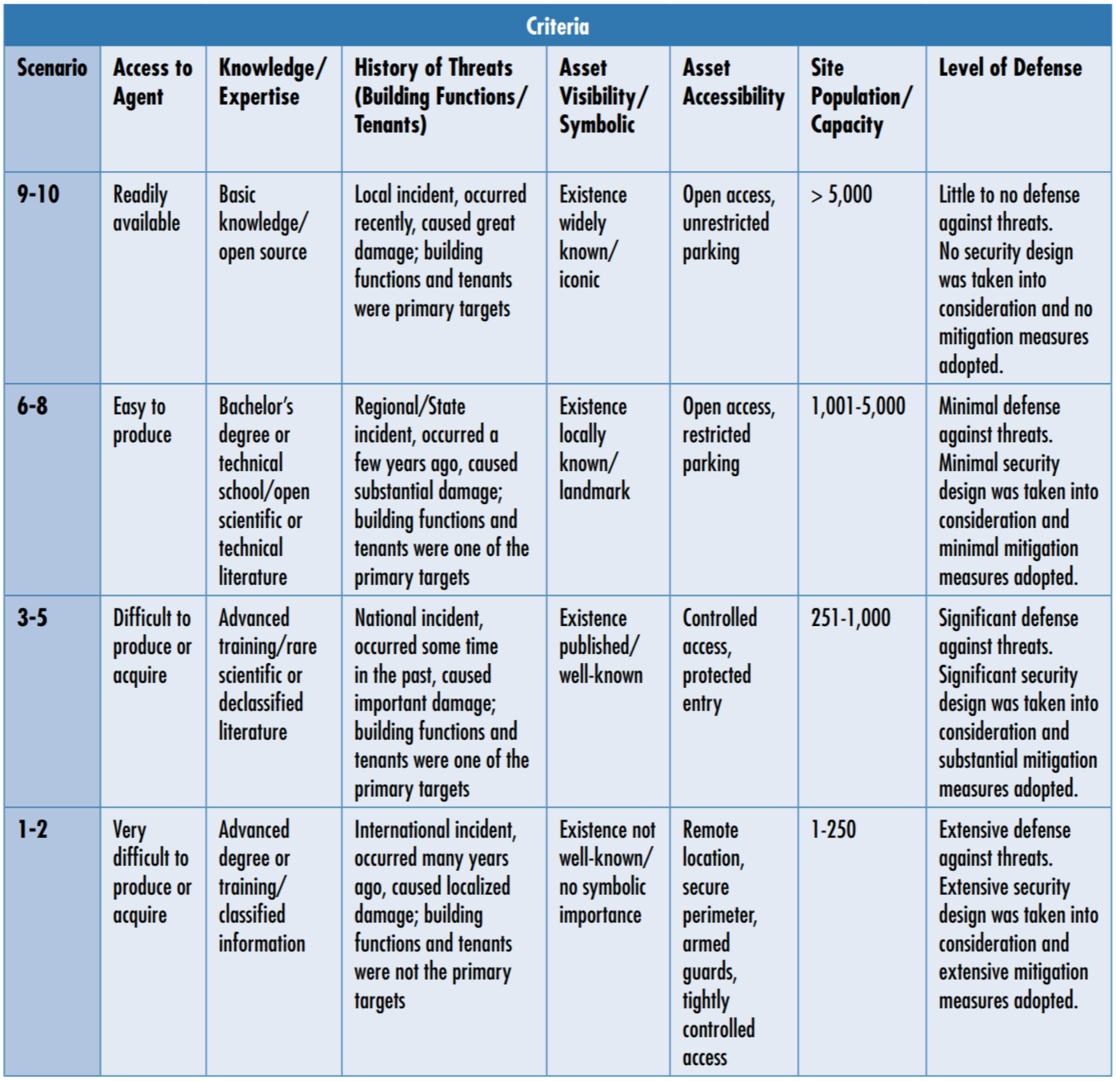
Loss of Life (X_{LL}): Determining which terrorist groups are the most active and responsible for the most deaths can be difficult due to the complexity of terrorist networks. Terrorist groups often have regional affiliates, and alliances between terrorist groups may result in overlapping and unstable chains of command. For the purposes of this study, loss of life is considered as a preference attribute for the terrorist who is interested in optimizing the number of fatalities resulting from a successful RDD attack. Violent true believers (VTBs) devoted to an ideology or belief system championing massacre and suicide as logical means of advancing their cause make good examples of threat groups that place a high swing weight on X_{LL}. Terrorists like Timothy McVeigh, Major Nidal Hasan and Andres Behring Breivik were notable VTBs.

Economic loss (X_{EL}): For a specific terrorist action, if causing economic damage is the group's primary intent, then the swing weight on X_{EL} would be high. Economically motivated terrorism represents one of the conceivable attributes that goes beyond political motivation. Economically motivated terrorism can meet political objectives, simultaneously causing economic disruption and inflicting human casualties. For some terrorists, causing economic damage might also constitute an end in itself, replacing political goals as the ultimate object. Potentially, a terrorist group may have some financial instrument or other business interest that would enable them to enrich themselves from the expected economic consequences of a terrorist attack.

Symbolism (X_{SY}) – As a particular method of communication, symbolism has the objective to channel information between a sender and a receiver. A symbol can be a material object, a concept, an action, or an event that represents something other than itself. The meaning of symbolism in this research is open ended and is not based on a literal or physical cause and effect relationships because mental processes may interpret symbols metaphorically. Rather, it depends on how meaning is constituted by the sender, on the environment in which it is produced, and how the receiver interprets the meaning. Symbolism can be the RDD itself or the type of facility chosen by the terrorist. Since symbolic communication is mostly visual, symbols play a pivotal role in communication of terrorism. Terrorism has been personified through extreme violence against public (federal) buildings (e.g., the Oklahoma City bombing), public transportation (e.g., the Aum Shinrikyo subway attack), historic landmarks (e.g., the attack on the Grand Mosque in Mecca, 20 November 1979), economic symbols (e.g., the attacks on the World Trade Center in 1993 and 2001). The RDD terrorist attack itself would be perceived as a symbol of intimidation and prestige. Children's hospitals, if attacked by a depraved terrorist organization, can be perceived to have a higher symbolic value relative to the standard healthcare facility.

The symbolic importance of the targeted facility is rated as per Federal Emergency Management Agency (FEMA) selection of primary threats criteria (FEMA, 2018) (Table 3.1). The economic damage and loss of life attributes are quantified in terms relative to 9/11.

Table 3.1 Criteria to select the symbolic value (FEMA, 2018)



Criteria							
Scenario	Access to Agent	Knowledge/ Expertise	History of Threats (Building Functions/ Tenants)	Asset Visibility/ Symbolic	Asset Accessibility	Site Population/ Capacity	Level of Defense
9-10	Readily available	Basic knowledge/ open source	Local incident, occurred recently, caused great damage; building functions and tenants were primary targets	Existence widely known/ iconic	Open access, unrestricted parking	> 5,000	Little to no defense against threats. No security design was taken into consideration and no mitigation measures adopted.
6-8	Easy to produce	Bachelor's degree or technical school/open scientific or technical literature	Regional/State incident, occurred a few years ago, caused substantial damage; building functions and tenants were one of the primary targets	Existence locally known/ landmark	Open access, restricted parking	1,001-5,000	Minimal defense against threats. Minimal security design was taken into consideration and minimal mitigation measures adopted.
3-5	Difficult to produce or acquire	Advanced training/rare scientific or declassified literature	National incident, occurred some time in the past, caused important damage; building functions and tenants were one of the primary targets	Existence published/ well-known	Controlled access, protected entry	251-1,000	Significant defense against threats. Significant security design was taken into consideration and substantial mitigation measures adopted.
1-2	Very difficult to produce or acquire	Advanced degree or training/ classified information	International incident, occurred many years ago, caused localized damage; building functions and tenants were not the primary targets	Existence not well-known/ no symbolic importance	Remote location, secure perimeter, armed guards, tightly controlled access	1-250	Extensive defense against threats. Extensive security design was taken into consideration and extensive mitigation measures adopted.

Terrorists pursue goals recognizing that the consequences might be grim, yet they have a practical determination, and under this pretense terrorist leaders make logical and strategic decisions based on our argument above in Section 3.2.2. Given the lack of biographical database, or a more accurate sociological profile of terrorist groups not being readily available, this research constructs an adversary utility $U[adv]$ profile (see Chapter 4) specific to each threat group based on the attributes (X_k). This study uses a value-focused thinking first developed by Keeney & von Winterfeldt (2011). This technique was further developed in Rosoff (Rosoff & John, 2011). We use value focused thinking, where adversary's profile is modeled by examining their own objectives and then choosing alternatives that fulfill those objectives The form of utility function, $U[adv]$, depends on the terrorist adversary's fundamental objectives and their interrelationships. Let there be n fundamental objectives (threat group profile) indexed by j from $0\ to\ n-1$. Each fundamental objective is measured using the attribute X_k, the metric for that particular objective. Each attribute has an associated single attribute utility function, $u(X_k)_j$ Eq (3.6) and Eq (3.8). When a complete set of fundamental objectives is identified, a simplifying assumption is that multiattribute utility function is linearly additive (Levine, 2012):

$$U[adv] = \sum_{j=0}^{n-1} w_{jk} u(X_k)_j \ \ j = 0\ to\ n-1, k = 0\ to\ 2 \qquad (3.6)$$

where,

j is the index for threat group (objective profile of the threat group).

k is the index of different attack attributes;

w_{jk} is the value tradeoff in the form of swing weights ;

$u(X_k)_j$ is the utility function of attribute k for threat group j; and

$U[adv]$ is the adversary utility function.

The uncertainty in the swing weights (w_{jk}) is parameterized via a probability density function (pdf) of beta distribution, $f(w_{jk})$. Beta distribution (discussed below) is assessed over attribute scale scores to represent the beliefs of the analyst (or the SME's) regarding the terrorist adversary's tradeoffs.

Beta distribution:

The Beta distribution is a continuous probability distribution having two parameters (i.e. constants). One of its most common uses is to model one's uncertainty about the probability of success of an experiment. The Beta distribution is characterized as follows: Suppose a probabilistic experiment can have only two outcomes, either success, with probability X, or failure, with probability $1 - X$. Also suppose that X is unknown and all its possible values are deemed equally likely. This uncertainty can be described by assigning to X a uniform distribution on the interval [0,1].

Now, suppose that we perform n independent repetitions of the experiment and we observe α success and β failures. In order to properly account the information provided by the observed outcomes, the distribution initially assigned to X needs to be revised. The result of this calculation is a Beta distribution. In particular, the conditional distribution of X, conditional on having observed α successes out of n trials, is a Beta distribution with parameters $\alpha + 1$ and $\beta + 1$.

The probability density function for x probability of success on any single trial is given by Eq (3.7).

$$f(x) = \frac{(n-1)!}{(\alpha-1)!(\beta-1)!} x^{\alpha-1} (1-x)^{\beta-1}, if\ x \in [0,1] \qquad (3.7)$$

Beta distribution is estimated using excel BETA.DIST function for each attribute using shape parameters $\alpha = 1$ and $\beta = 2$. The pdfs for these swing weights are independent; in other words, the uncertainties in the value tradeoffs for the different attributes are uncorrelated.

The single attribute utility function captures the terrorist adversary's attitude toward risk. A concave function is used to reflect the risk averse attitude of the terrorist, $u(X_k)_j$, Eq (3.8). While the threat groups (or individuals) may share similar attack attribute, their perspectives towards these are not always in agreement. This study assumes all three-threat group to have a risk averse attitude, shown in Eq (3.8). The utility u is not only increasing but is also concave in the outcome X_k, which implies that the marginal utility of preference of attribute is decreasing with the attribute.

$$u(X_k) = sqrt(X_k),\ k = 0\ to\ 2 \qquad (3.8)$$

The total utility of each asset $U[tot]$ to the threat group equals the product of the material input $U[mat]$(Eq(3.3)) and adversary's utility as a function of the attributes, $U[adv]$ (Eq(3.6)). In addition to describing the utility function of the asset and the terrorist adversary the overall objective of a terrorist attack is described as a complex interaction of the attributes with the reputation and goals of a profiled terrorist group. The Peircean semiotic three-part (representamen-object-interpretant) model is utilized to define the adversary utility function, $U[adv]$, assigning appropriate swing weights for the overall symbolic impact desired by each profiled threat group.

3.2.2 Pierces triangle

Peirce's semiotic framework consists of a three part model of signification: (1) the **representamen (**i.e., the sign itself; what something is), (2) the **object** (i.e., the "referent", what the sign refers to or symbolizes), and (3) the **interpretant** (i.e., the audience's interpretation or the effect in the mind of the interpreter) (Matusitz, 2015). This framework is referred to as Peirce's "representamen-object-interpretant" model (Fig.3.4)

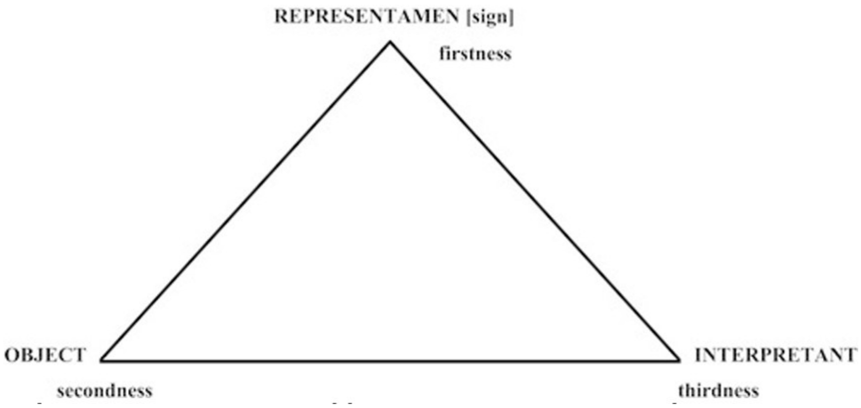


Figure 3. 4 Peirce's Representamen-Object-Interpretant semiotic triangle

Representamen is the sign – that is, "something that is". To illustrate, if we consider the case study of 9/11, the destruction of Twin Towers by airlines-a passenger plane hitting a skyscraper and the footage of a burning 110-story building constituted a categorical and incontestable image that represented the horrific act. In our research the RDD attack, itself, is considered a representamen. Since RDD is primarily an economic weapon a swing weight of high, medium, or low on the attribute of economic loss (X_{EL}) would reflect terrorist adversary's preference score of doing an economic damage with the RDD weapon.

The *object* is the meaning or concept which comes into play when the sign represents a deliberate act of terror. The object is reflected in the idea that the image symbolizes an extremely violent terrorist act. The Twin Towers were deliberately obliterated because they symbolized power (i.e., economic, political and cultural power). The WTC symbolized American success, sovereignty, capitalism, globalization, and modernity. The RDD attack on a “soft target”, such as a healthcare facility, which is relatively unprotected and vulnerable, would symbolize an attack towards humanity, an attack towards the expression of shared values and an overall unparalleled public loss. The loss is compounded if the healthcare facility attacked is a children’s hospital or has a religious affiliation. For instance, Mount Sinai Medical Center a major hospital in New York City is a Jewish entity, located only a few miles to the Subway station (Kamen et al., 2019). According to many historical data, terrorist attacks on Jewish entities has been commonplace, triggered by strong commitments and resistance to change the unbending religious beliefs. Among the possibilities, sadly, is the potential for an RDD attack targeted against a healthcare facility with humanitarian or religious affiliation -the softest of “soft targets” and the most potentially provocative in terms of public reaction. Based on maximizing or minimizing the “referent” or the object symbolism, the attribute preference of symbolism (X_{SY}) is assigned a swing weight of high, medium, or low. Lastly, the attribute of loss of life (X_{LL}) is reflected in the mind of the interpreter.

The *interpretant* in the 9/11 attack was the physical damage and loss of human life and the temporary disruption of financial and social routines. The power, success, and the future of the United States (symbolized by Twin Towers) were perceived as threatened. An RDD attack, though unlikely to cause mass death, would expose civilian populaces to radiation, engendering anxiety, stress and panic out of all proportion to the modest number of casualties. Among those who are indirectly affected by the RDD attack, may suffer ripple effects such as economic downturn. The news media and the movie industry can, accidentally or intentionally, act as a powerful multiplier of the harmful psychological consequences of an event, expanding its scope to the national level.

Pierce’s semiotic three-part triangle is one way to venture in an illustrative measurement of shaping terrorist adversary’s profile, without the SME or the intelligence. The triadic relationship of communicating between the perpetrators and the audiences is achieved by assigning swing weights to attributes of life loss, economic loss, and symbolism. By way of an example, a terrorist adversary seeking to produce social transformation by performing symbolic acts of violence will be modeled low on X_{EL}, high on X_{LL} and high on X_{SY}.

The threat group profiling is followed by the development of exhaustive sets of attack scenarios. To capture the dynamic relationship between the adversary attack strategy and the security safeguards of the facility, a combination of mathematical models is developed and employed. Principles of PRA and pathway analysis are implemented to quantify genuine threats and to analyze their overall theft success probabilities.

3.3 Pathway analysis

Theft and sabotage may be prevented in two ways: by *deterring* the adversary or by *defeating* the adversary. Deterrence occurs by implementing a physical protection system (PPS) that is seen by potential adversaries as too difficult to defeat; it makes the facility an unattractive target. Deterrence in this research is incorporated in the attacker defender game discussed later in Chapter 6. Defeating the adversary refers to the actions taken by the protective or response force to prevent an adversary from accomplishing her goal once she begins a malevolent action against a facility. The three major functions that the PPS must perform include (Whitehead et al., 2007):

- *Detection*: Detection is the discovery of an adversary action. It includes sensing of covert or overt actions. The measures of effectiveness for the detection function are the probability of sensing adversary action and the time required for reporting and assessing the alarm. The probability of assessed detection for a particular sensor captures both of these measures. Detection can be achieved by several means, including visual observation, video surveillance, electronic sensors, accountancy records, seals and other tamper indicating devices. Adversary awareness of detection measures can also serve as a deterrent. Guards at fixed posts or on patrol may serve a vital role in sensing an intrusion.
- *Delay*: Delay slows down an adversary's process by impeding its attempt to gain unauthorized access or to remove or sabotage a radioactive source, generally through barriers or other physical means. A measure of delay is the factor of time, after detection, that is required by an adversary to bypass each delay element.
- *Response*: Response encompasses the actions undertaken following detection to prevent an adversary from succeeding or to mitigate potentially severe consequences. Response can include both interruption and neutralization. Interruption is defined as a sufficient number of response force personnel arriving at the appropriate location to stop the adversary's progress. Interruption includes communication and deployment of the response force. Neutralization describes the actions and effectiveness of the responders after interruption.

Response time is the primary measure because responders must be at the correct location in order to neutralize the adversary.

As explained by Whitehead et al. (2007), these functions must be performed in a period of time that is less than the time required for the adversary to complete his tasks. Figure3.5 shows the relationship between adversary task time and the time required for the PPS to do its job. The total time required for the adversary to accomplish its goal has been labeled "adversary task time". It is dependent upon the delay provided by the PPS. The adversary may begin his task at some time before the first alarm occurs T_0. The adversary task time is shown by a dotted line before this point because delay is not effective before detection. After that alarm, the alarm information must be reported and assessed to determine whether the alarm is valid. The time at which the alarm is assessed to be valid is labeled T_A, and at this time the location of the alarm must be communicated to the members of the response force (Whitehead et al., 2007). The response time requires the response force to respond in adequate numbers and with adequate equipment to interrupt and neutralize the adversary actions. The time at which the response force interrupts adversary actions is labeled T_I and adversary task completion time is labeled T_C. The detection (i.e. T_0 and T_A) and response (i.e., T_I) should occur as early as possible; in other words, these events should be as far to the left on the time axis as possible (Garcia, 2007).

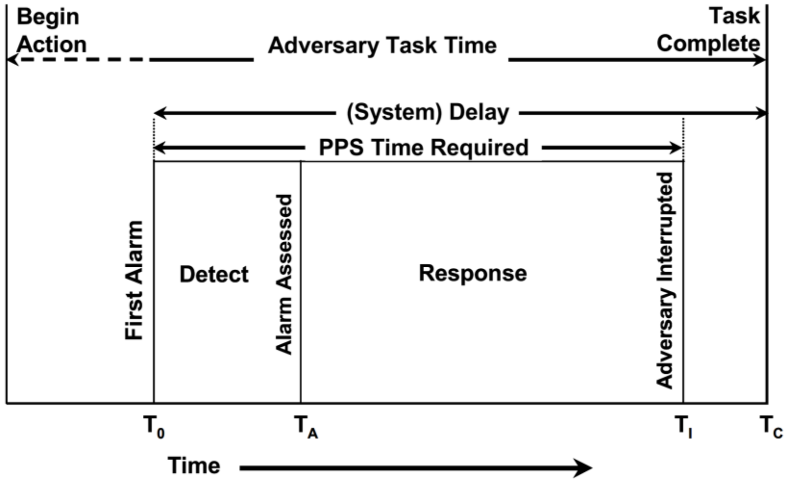


Figure 3.5 Interrelationship among physical protection system functions (Whitehead et al., 2007)

Pathway analysis involves identifying and examining the paths (through a facility) that an adversary might take during his theft or sabotage attempt. An adversary path is an ordered series of actions against a target that, if completed, results in successful theft or sabotage. Protection elements along the path detect and delay the adversary (Garcia, 2007). Path interruption analysis tool of "Estimate of Adversary Sequence Interruption" (EASI) is used to quantitatively illustrate the effect of changing physical protection parameters along a specific path for a single adversary. Detection and communication inputs are inputs in the form of probabilities and the delay and response inputs are in the form of mean times and standard deviations for each protection layer or element. The probability of detection P_D (Eq (3.9)) for each sensor encountered by an adversary is computed as a product of the probability of the sensor or detector sensing abnormality (P_S), the probability that an alarm will be transmitted to an evaluation point (P_T), and the probability of accurate assessment of the alarm (P_A) (Whitehead et., 2007).

$$P_D = P_S \times P_T \times P_A \tag{3.9}$$

An evaluation performed by Sandia National Laboratories found that most systems operate with a probability of guard communication (P_C) of 0.95. The delay time required by an adversary to travel a given path was computed as the sum of the times required to perform certain tasks or travel distinct path segments. Response force time (RFT), which is a measure of the time it takes to receive, assess and respond to an alarm is incorporated in the computation in the form of single mean time and standard deviation. The time data input, including the RFT and adversary task times is entered in the units of seconds. The response force time and the adversary task time standard deviations are approximated as 30% of the corresponding mean values. The reason to use standard deviation for RFT and delay times is to allow for the fact that guards will not always act in exactly the same time, and the adversaries may take some extra time to penetrate barriers. The output of the probability of interruption (P_I), in the case of a single detection sensor is given by Eq (3.10) (Garcia, 2007).

$$P_I = P(R|A)P(A) \tag{3.10}$$

$P(R|A)$ is the probability of response force arrival prior to the end of the adversary's action sequence, given an alarm, $P(A)$ is the probability of alarm.

EASI allows specification of where the detection sensors are located with respect to the respective task delays. If T_R is the time remaining for the adversary to reach the terminal point when a sensor triggers, and RFT is the response time of the security force, then for adversary interruption it requires that

$$T_R - RFT > 0 \tag{3.11}$$

The random variables T_R and RFT are assumed to be independent and normally distributed and thus the random variable. The equations below are adapted from Garcia (2007).

$$X = T_R - RFT \tag{3.12}$$

is normally distributed with mean

$$\mu_X = E(T_R - RFT) = E(T_R) - E(RFT) \tag{3.13}$$

variance

$$\sigma_X^2 = Var(T_R - RFT) = Var(T_R) + Var(RFT) \tag{3.14}$$

and

$$P(R|A) = P(X > 0) = \int_0^{\infty} \frac{1}{\sqrt{2\pi\sigma_X^2}} \exp\left[\frac{(X-\mu_X)^2}{2\sigma_X^2}\right] dx \tag{3.15}$$

In EASI, $P(R|A)$ is approximated using the NormSDist function found in Excel®. Because the method is concerned with the time remaining in the sequence, evaluation of $E(T_R)and\ E(RFT)$ at point p along a path of interest must be with respect to the terminal point. For two or more sensors, P_I is determined by finding the joint probability of detection for each PPS layer outside the critical detection point.

$$P_I = P_{D1}P_{C1}P(R|A_1) + \sum_{i=2}^{n} P(R|A_i)P(C_i)P(D_i) \prod_{i=1}^{i-1}(1 - P(D_i)) \tag{3.16}$$

P_I represents timely detection, it serves as one measure of system effectiveness. Timely detection is the minimum cumulative probability of detecting the adversary while there is enough time remaining to the response force to intercept the adversary. Figure3.6. illustrates the timely detection measure of effectiveness. The delay elements along the path determine the point by which the adversary must be detected. That point is where the minimum delay along the remaining portion of the path (T_R) just exceeds the guard response time (T_G); i.e., the sum of the individual delay times associated with each delay element just exceeds T_G. This point is the critical detection point (CDP). Minimum cumulative probability of interruption (P_I) is defined as the cumulative probability of detection from the start of the path up to CDP. To calculate P_I, an assumption is made, where the adversary tries to minimize detection before the CDP and minimize delay after the CDP (Whitehead et al., 2007; Garcia, 2007). For the adversary to minimize detection, careful movement is required up to the CDP. This careful movement may include stealth or deceit. After the CDP, not enough delay time remains for the response force to respond and detection is less impactful. After the CDP, the adversary is assumed to change strategies and minimize delay. This is accomplished by moving quickly and with least detection concerns (Whitehead et al., 2007).

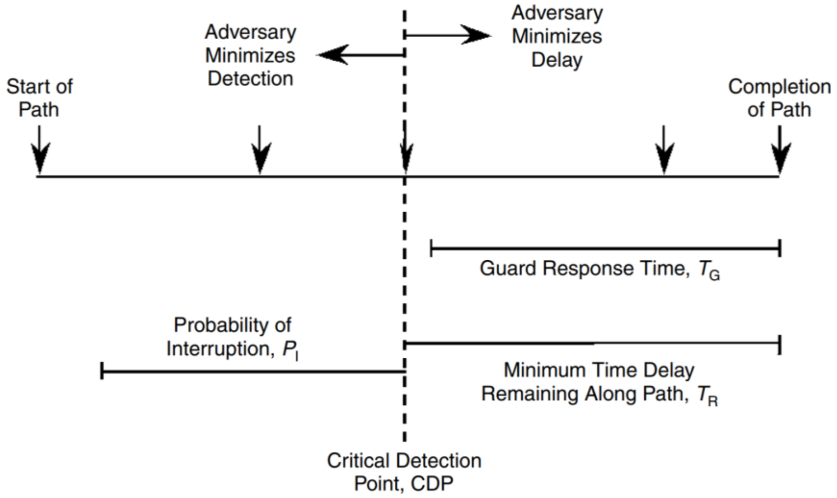

Adversary Minimizes Detection
Adversary Minimizes Delay
Start of Path
Completion of Path
Guard Response Time, T_G
Probability of Interruption, P_I
Minimum Time Delay Remaining Along Path, T_R
Critical Detection Point, CDP

Figure 3.6 Timely detection as a measure of effectiveness(Whitehead et al., 2007)

Timely detection considers only detection, delay, and guard response time. The force-on-force conflict is not considered between the law enforcement response forces and terrorist adversaries. It is unlikely that any healthcare facility will engage in use of deadly force against an adversary, so these aspects are not considered in this risk model. The major power of this approach is that all of the values used to determine the probability of interruption,P_I, can be based on measured data. All detectors can be tested to determine the probability of detecting an adversary passing that detector, barriers can be tested to determine how long it takes to breach each barrier, and the response force and adversary force can be modeled to simulate RFT and T_R. While Garcia's (2007), pathway methodology calculates the probability of adversary getting interdicted by the response force, given an attack; it does not incorporate the initiating events that trigger the vulnerability of an attack.

3.4 Probabilistic risk assessment (PRA)

PRA is a systematic process that integrates information about design, operational practices, historical information, human interaction, and component reliability to determine likelihood and severity ratings for potential adverse events (US NRC, 1975). The RSS (WASH-1400) contributed significantly to the state-of-the art PRA applications for nuclear power plants (U.S. NRC, 1975). The RSS established that the fault tree/event tree methodology could be used credibly to identify risk-significant accident sequences. PRA in this research is used in conjunction with the pathway analysis to calculate the overall success probability of theft.

The first technical step in PRA, performed at the beginning of the system modeling activity, is the identification of potential initiating events. The initiating events in this research, as described in Chapter 2 (Section 2.2.2), are undesired events which present a challenge to the security of the facility in that if taken advantage of by an opportunistic adversary, a theft or sabotage may occur. Unlike safety PRA, where an initiating event is a random uncontrollable event, initiating events in security PRA are the result of strategic and planned decisions made by an adversary (U.S. NRC, 2003). The adversary can purposely act in deceptive or unpredictable ways and can alter their attack strategy based on countermeasures taken by the defender. Because an intelligent adversary can make strategic decisions, the likelihood they decide to attack will depend to some degree on the likelihood they will succeed. Depending on the asset and the asset specific attack scenario the initiating events of scheduled maintenance days, random repair days and source reload days are assumed to represent the change of state in the normal operation of these assets or radioactive devices.

The study uses this frequency of device unavailability and other initiating events as an opportune time for a malevolent act. Determining an appropriate probability model to represent the initiating event is the next step in PRA towards calculating the success probability. These probability models typically have one or more parameters, whose estimation is based on the most applicable and available data. Table 3.2 shows the models considered in the study.

Table 3.2 Probability distributions and initiating events for different scenarios

Assets (radioactive material or devices)	Initiating events	Probability model	Parameter to estimate
Iridium	Source exchange and device not in use	Poisson distribution	Initiating event rate λ, number of occurrences *x* in fixed time *t*
Cobalt	Maintenance and repair days	Binomial distribution	Number of occurrences *X* in some fixed number of trials *n*
Cesium	Propped open door and device not in use	Poisson and Binomial distribution	Initiating event rate λ, number of occurrences *x* in fixed time *t,* number of occurrences *X* in some fixed number of trials *n*

A random parameter variation is used to randomly generate *n* inputs depending on the parameters of the probability model. A Monte Carlo simulation is run for each of the *n* inputs for each attack scenario. In general terms, the Monte Carlo method can be used to describe any technique that approximates solutions to quantitative problems through statistical sampling. It is a type of simulation that explicitly and quantitatively represents uncertainties. Monte Carlo simulation in this study explicitly represents uncertainties by specifying input as probability distributions. That is, the result of any analysis based on inputs represented by probability distributions is itself a probability distribution. The probability of interruption (P_I) calculated from the pathway model represents the single estimate of a particular outcome. Instead of calculating the P_I many times, a Monte Carlo simulation is used to simulate the terrorist adversary attacking the asset 1000 times. A random normal probability distribution with mean $(\mu = P_I)$, 95% confidence interval (1.96σ standard deviation) and n=1000 iterations gives a much more comprehensive view of the outcome. The output is further assessed by taking the mean of the pdf, which is then used in binomial or the Bayes theorem, depending on the probability model used, to calculate the final probability of theft.

3.4.1 Binomial distribution

The probability of theft $(X = 1)$ or no theft$(X = 0)$ of ^{60}Co and ^{137}Cs assets assume that the number of failures have a binomial distribution. The binomial distribution describes the number of failures X in *an* independent trials. The random variable X has a binomial distribution if:

- The number of random trials is one or more and is known in advance.
- Each trial results in one of two outcomes, usually called success and failure.
- The outcomes for different trials are statistically independent.
- The probability of failure, p, is constant across trials.

Equal to the number of failures in the *n* trials, a binomial random variable X can take on any integer value from 0 to *n*. The probability associated with each of these possible outcomes, *x*, is defined by the binomial (n, p) pdf as

$$\Pr(X = x) = \binom{n}{x} p^x (1 - p)^{n-x} \tag{3.17}$$

where the binomial coefficient is defined as

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{3.18}$$

The binomial coefficient has two parameters, *n* and *p*, of which *n* is known. For *^{60}Co*, *n* is the number of maintenance and repair days of Gamma Knife® in a year. For *^{137}Cs*, *n* is number of times the door to blood irradiator room is left propped open and number of hours the device (*CsCl* blood irradiator) is unused. The number of trials are randomly generated using poison random number generator (poissrnd) in MATLAB. The mean and variance of a binomial *(n,p)* random variable *X* are

$$E(X) = np \tag{3.19}$$

and

$$Var(X) = np(1-p) \qquad (3.20)$$

3.4.2 Poisson distribution

The Poisson distribution describes the total number of events occurring in some interval of time *t*. The probability distribution function of a Poisson random variable X, with parameter $\mu = \lambda t$, is

$$\Pr(X = x) = \frac{e^{-\mu}\mu^{x}}{x!} \qquad (3.21)$$

$$\Pr(X = x) = \frac{e^{-\lambda t}(\lambda t)^{x}}{x!} \qquad (3.22)$$

for $x = 0,1,2, \ldots n$ and $x! = x(x-1)(x-2) \ldots (x-n)$

The Poisson distribution has a single parameter μ, denoted Poisson (μ). If X denotes the number of events that occur during some time period of length *t*, then X is often assumed to have a Poisson distribution with parameter $\mu = \lambda t$. The mean of the Poisson distribution is equal to the parameter of the distribution, which is why μ is often used to represent the parameter. The variance of the Poisson distribution is also equal to the parameter of the distribution (US NRC, 2003)). Therefore, for a Poisson (μ) random variable X,

$$E(X) = Var(X) = \mu = \lambda t \qquad (3.23)$$

The Poisson distribution provides a discrete probability model that is appropriate for many random phenomena that involve counts. A common use of the Poisson distribution is to describe the behavior of many rare occurrences (US NRC, 2003). It is standard to assume that the event count has a Poisson distribution, given the assumptions below:

The probability that an event will occur in any specified short exposure time period is approximately proportional to the length of the time period.

Exactly simultaneous events do not occur.

Occurrences of events in disjoint exposure time periods are statistically independent (US NRC, 2003).

For ^{137}Cs, if we assume that in a large university setting medical center 50 to 60 blood units get irradiated per day, with 2 blood bags per irradiation cycle. The main door to the blood irradiator room gets accessed 150 times in a working day (8 hours) by approximately 5 nurses or technicians. Assuming the main door to the blood irradiator is left propped open 2% of the time, the rate parameter is then calculated to be $\lambda = 3/day$. Therefore, the probability that the door is never $(x = 0)$ left propped open in a given working day is calculated using the Poisson distribution function $poisspdf(x, lamda)$ in MATLAB. The rate parameter is generated using the Poisson random generator.

Similarly, for ^{192}Ir, let's assume that the HDR treats 10 patients in a week, so 2 patients in a day. Each patient takes an hour approximately to get treated. The ^{192}Ir also undergoes source exchange quarterly so 4 times a year (~1 working day every 3 months). The average number of times that the HDR device is undergoing source exchange or is unused is given by the mean parameter $\mu = 89$, the probability that the device is vulnerable to theft in a given working year $(x = 250)$ is calculated using the Poisson distribution function.

3.4.3 Bayes **theorem**

It is frequently desired to calculate the probability of an event A given than another event B has occurred at some prior point in time (US NRC, 2003). It can also be of interest to calculate the probability that a state of nature exists, given that a certain sample is observed or measured. The basic theorem applied to point probabilities states:

$$P(A|B) = \frac{P(B|A)P(B)}{P(A)} \qquad (3.24)$$

The $P(A|B)$ is the posterior probability for the event A, meaning the probability of A once B is known. The $P(A)$ is the prior probability of event A before experimentation or observation. The event B is the observation. The $P(B|A)$ is the probability of the observation given A is true. The denominator serves as a normalizing constant.

Bayes' theorem is applied to calculate the posterior probability of loss of ^{192}Ir source as an intentional or unintentional mail delivery failure. Event A is the prior probability of the number of radioactive material delivery failures according to the CNS global incident and trafficking report (Meyer et al, 2018) in North America. Event B is the number of mis-deliveries from the mail carriers (FedEx or the United Postal Service). Given that a package was misdelivered by the mailman ($P(B)$), the probability that the misdelivered package is a radioactive package ($P(A|B)$) is calculated using Bayes theorem. The CNS global incident and trafficking 2018 database also reports 3 theft cases of ^{192}Ir source which is used as a prior distribution towards calculation of success probability of theft in attack scenario two, given the probability of the source being unsafe or vulnerable in a year is known.

3.5 Factor analysis

This research chooses factor analysis as a preferred statistical tool to investigate patterns of relationship among many dependent variables, with the goal of discovering something about the nature of the independent variables that affect them. These independent variables are referred to as latent variables or so-called factors. The emphasis in factor analysis is the identification of underlying "factors" that might explain the dimensions associated with data variability. There are two main types of factor analysis: Principal component analysis (PCA) and common factor analysis (FA). PCA and FA tackles the same problem with different approaches. They are related, but not identical.

In PCA, from the observed original dimensions, $x_i, i = 1, \ldots, d,$ we form new variables that are linear combinations of x_i. It replaces a large set of variables by a smaller set which best summarizes the larger set. In other words, the goal of PCA is to replicate the correlation matrix using a set of *principal components* that are fewer in number and linear combinations of the original set of items. PCA assumes that there is no unique variance, the total variance is equal to common variance. Eigenvalues, which represent the total amount of variance, help decide the number of factors that need extraction (Kassim et al., 2013).

Unlike PCA, FA assumes that variance can be partitioned into common and unique. Common variance, also known as communality (h^2) is the amount of variance that is shared among a set of items. It ranges between 0 and 1. Unique variance (1-h^2) is any portion of variance that is not common. Specific and error form the two types of unique variance that is specific to a particular item and comes from errors of measurement and basically anything unexplained by common or specific variance. Figure3.7. shows how these concepts are related. In FA, the factor model postulates that all p observable variables in a data set is linearly dependent on m unobservable, common factors $F_1, F_2, \dots, F_m$ and additional sources of variation, specific to a variable, $\varepsilon_1, \varepsilon_2, \dots \varepsilon_p, i.e.,$

$$X_k - \mu_k = l_{k1}F_1 + l_{k2}F_2 + \cdots + l_{km}F_m + \varepsilon_k, k = 1,2, . . , p$$

The weights l_{kj} is known as the loading of the k^{th}variable on the j^{th} factor. The portion of the variance of the k^{th}variable contributed by the m common factors is known as the k^{th} communality. It is the sum of squared factor loadings and denoted as

$$h_k^2 = l_{k1}^2 + l_{k2}^2 + \cdots . + l_{km}^2 \tag{3.25}$$

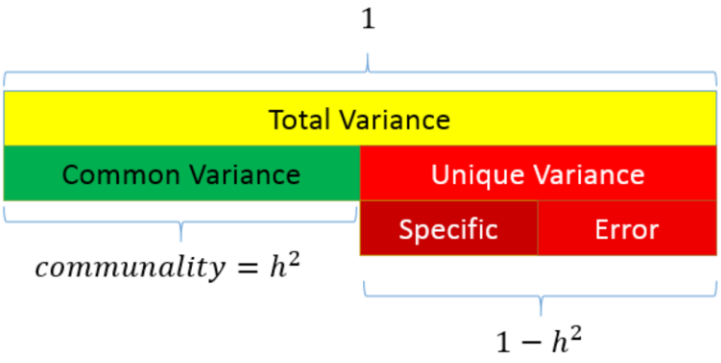


Figure 3.7 Common and unique variance used in factor analysis

Since the objective of this research is to find a latent construct (vulnerability) underlying the locational hazard variables, FA is used as a preferred method of analysis. In extracting the factors, FA repackages the variance that is common (shared) among variables only; variance due to the unique factors is excluded from the analysis. There are several estimating techniques in FA such as unweighted least squares, principal axis factoring, and maximum likelihood.

Extraction of factors

_Maximum likelihood estimation (MLE) is one of the many methods used for estimating factors from data. Research has shown than MLE produces almost identical factor solution as to the other estimation technique, like principal axis factoring (Kassim et al., 2013). The reason that this research uses MLE as a technique to extract factors is because it uses the known probability distributions (like the normal distribution) and compares data sets to those distributions in order to find a suitable match for the data.

In MLE it is assumed that the data are independently sampled from a multivariate normal distribution with mean vector μ, and variance-covariance matrix of the form $\Sigma = LL' + \Psi$, where L is the matrix of factor loadings and Ψ is the diagonal matrix of specific variances and L' denotes the vector of latent factors. The MLE procedure involves the estimation of μ, the matrix of factor loadings L, and specific variance Ψ from the log likelihood function. It is often easier to work with the natural log of the likelihood function. Since ln(x) is an increasing function, the maxima of the likelihood and log likelihood coincide.

$$l(\mu, L, \Psi) = -\frac{np}{2} log 2\pi - \frac{\mathrm{n}}{2} \log|LL' + \Psi| - \frac{1}{2}(X_i - \mu)^T(LL' + \Psi)(X_i - \mu) \qquad (3.26)$$

By maximizing the above log likelihood function, the maximum likelihood estimators for $\mu, L\ and\ \Psi$ are obtained.

<u>Factor rotation</u>

Once the initial factor loadings have been calculated, the factors are rotated. Factor rotations help in interpretation of the factor loadings. There are two types of rotation method, orthogonal and oblique. In orthogonal rotation the rotated factors are independent or uncorrelated with each other and in oblique rotation the factors are not independent and are correlated. Varimax, developed by Kaiser (Kaiser, 1960), is indubitably the most popular orthogonal rotation method. The total amount of variation explained by factors remains the same. The total amount of variation explained by the rotated factor model is the same, but the contributions are not the same from the individual factors. Since the amount of variation of the data set in this research is explained by only 1 factor, the data interpretation remains the same, regardless of what rotation is used.

This study uses $factoran(lambda, Psi, T)$ function in MATLAB, where observed data X is standardized to zero mean and unit variance before estimating the loadings $lambda$. The function returns the MLE estimates of the specific variances as a column vector psi. By default, $factoran$ calls the function $rotatefactors$ to rotate the estimated factor loadings using the varimax option.

Weights computed from the factor loading results ($lambda$) is applied to summarize all weighted indicators into a single composite metric, following a vulnerability index methodology shown in Eq (3.27) (Gbetibouo, 2009; Žurovec et al., 2017)

$$V = \sum_{y=1}^{n} (\frac{w_e(X_{ey} - \bar{x}_e}{s_{ey}}) \qquad y = 1, \ldots n; \qquad (3.27)$$

where,

V is the vulnerability value;

w_e is the weight of the *e*th locational hazard indicator;

$\overline{x_e}$ is the mean value of the eth locational hazard indicator; and

s_{ey} is the standard deviation of the eth locational hazard indicator

in the yth year.

X_{ey} is the minmax normalized value of eth locational hazard indicator for the yth year.

Each indicator (x_{ey}) is rescaled from 0 to 1 using the HDI minmax normalization methodology.

$$X_{ey} = \frac{x_{ey} - Min\, x_e}{Max\, x_e - Min\, x_e} \qquad (3.28)$$

where,

x_{ey} is the value of eth locational hazard indicator for the yth year;

$Min\ x_e$ is the minimum value of the eth indicator among all the prior years; and

$Max\ x_e$is the maximum value of the eth indicator among all the prior years.

3.6 Self-assessment tool-A Survey

The characteristics of an effective nuclear security culture is shown in Figure3.8. This three-layer model is based on the organizational culture model developed by Professor Edgar Schein of the Massachusetts Institute of Technology (MIT) (IAEA, 2008; Khripunov, 2006). Schein's model is broadly applicable to nuclear facilities and organizations, like nuclear power plants, fuel cycle facilities, research reactors, radioactive source users, and other entities that handle /store radioactive materials (IAEA, 2008).

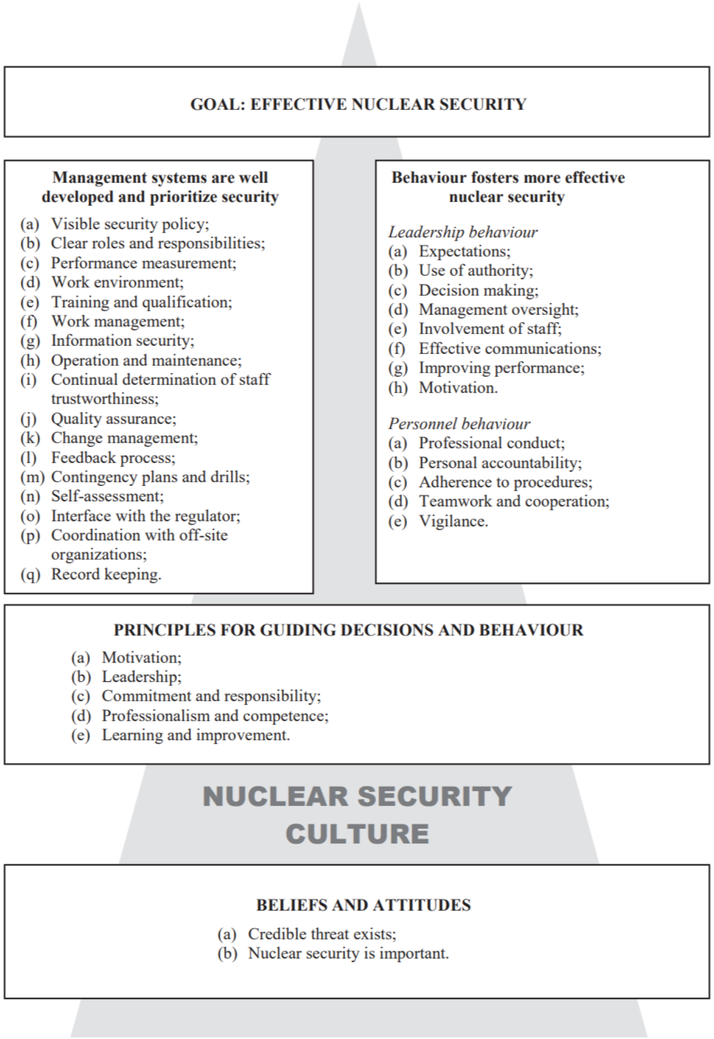

GOAL: EFFECTIVE NUCLEAR SECURITY
Management systems are well developed and prioritize security
(a) Visible security policy;
(b) Clear roles and responsibilities;
(c) Performance measurement;
(d) Work environment;
(e) Training and qualification;
(f) Work management;
(g) Information security;
(h) Operation and maintenance;
(i) Continual determination of staff trustworthiness;
(j) Quality assurance;
(k) Change management;
(l) Feedback process;
(m) Contingency plans and drills;
(n) Self-assessment;
(o) Interface with the regulator;
(p) Coordination with off-site organizations;
(q) Record keeping.
Behaviour fosters more effective nuclear security
Leadership behaviour
(a) Expectations;
(b) Use of authority;
(c) Decision making;
(d) Management oversight;
(e) Involvement of staff;
(f) Effective communications;
(g) Improving performance;
(h) Motivation.
Personnel behaviour
(a) Professional conduct;
(b) Personal accountability;
(c) Adherence to procedures;
(d) Teamwork and cooperation;
(e) Vigilance.
PRINCIPLES FOR GUIDING DECISIONS AND BEHAVIOUR
(a) Motivation;
(b) Leadership;
(c) Commitment and responsibility;
(d) Professionalism and competence;
(e) Learning and improvement.
NUCLEAR SECURITY CULTURE
BELIEFS AND ATTITUDES
(a) Credible threat exists;
(b) Nuclear security is important.

Figure 3.8 Characteristics of nuclear culture(IAEA, 2008).

The purpose of the security culture self-assessment is to present a clear picture of nuclear security as part of an organization's culture. This involves evaluating the key indicators of security culture in the organization and comparing them to reference level indicators that would correspond to an optimal security culture. Surveys are the primary tool used for initially assessing the security culture in the facility. The reasons of using surveys as a self-assessment tool for an initial screening are to discover an individual's attitude towards nuclear security, measure deficiencies in policies or procedures, and identify relationships between certain security indicators and individual parameters (Rane et al., 2018).

The overall culture of an organization is rarely homogenous and subcultures exist within the group. To analyze the relationship between them a cultural analysis should therefore be performed. This research drafts "general" and "technical" survey to account for the difference in perceptions and attitudes between personnel who are not radioactive users and those who use radioactive material on a daily basis. The general survey questions are drafted to deduce the layers of intangible human behavioral artifacts, that ultimately manifest into observable forms and are taken for granted as a radiological facility operates at a compliance level. Similar to our previous publication, the resulting survey contains 23 questions across four broad categories broken into awareness of policies, enforcement of policies, leadership behavior and involvement, and individual belief and attitude (Rane et al., 2018). A list of general and technical survey questions is included in Appendix A.

3.6.1 General survey categories

The first category of the general survey consists of policy knowledge, coined as "Policy" for future reference, and was comprised of six questions. The "Policy" category is used to assess how well the participants know the policies that are in place at the healthcare facility and communication of dissemination of policies. It is important to note that these questions inquire about person's ability to know the policies but not exactly cite it. The survey also does not attempt to determine that person's actual understanding of the policies. An example of this type of question is "I am aware of the policy at the healthcare center on nuclear and radioactive material security". An individual could strongly agree with that statement; however, if asked, the individual may not be able to actually cite the correct document (Rane et al., 2018).

The second category in general survey is enforcement of policies (“Enforcement”). The “Enforcement” category contains seven questions with the goal to determine the beliefs of individuals with regard to how the healthcare facility handles problems with security matters. An example question from this category is: “Regular meeting briefs at the healthcare facility covers significant security related items?”. Procedures embody the organization’s collective knowledge and experience, and they must be enforced and followed to ensure that tasks are performed correctly (Rane et al., 2018).

Leadership involvement (“Leadership”) is the third category of general survey. It consists of 6 questions. This area explores the beliefs of all participants in how leadership helps encourage nuclear and radioactive material security through communication and inspections. Several of the questions focuses on the idea of leadership giving subordinates the ability to exercise critical thinking. An example question from this area is: “Management (lab manager, physicians, etc.) frequently inspects my work to ensure that procedures are being followed in accordance with expectations” or “Management (lab manager, physicians, etc.) involves staff members in the risk assessment and decision making process and other activities that affect them”.

The final category or area explored by this survey is labeled individual involvement (“Belief and Attitude”). This area contains 4 questions and is the area of the survey that elicits personal opinions about nuclear and radioactive material security. “I consider myself personally responsible for security in my role at the healthcare facility” is an example question in this area. The beliefs and attitudes held by individuals are influenced by the actions that others take or do not take and also by what others (managers) say or do not say. In this way, beliefs and attitudes spread and replicate themselves within organizations.

3.6.2 Technical survey categories

The technical survey questionnaire involved evaluating the key characteristics of security functions and component subsystems of deterrence, detection, delay, and response. Respondents’ perceptions pertaining to training of personnel in policies, and accountability and awareness of procedures is also assessed as a part of understanding the operational effectiveness of the facility.

“Detect and Deter” asks about facility’s means of detecting loss of radioactive sources/equipment through verification (standard operating procedures) and surveillance. With deterrence effort being difficult to measure or predict, the questions concern more on possessing the measures to prevent the theft from occurring and deploying passive and active barriers to delay the adversary.

“Response” category comprises of four questions addressing a continuous state of readiness to handle security events at any time. An important element of the system is the set of contingency plans used to respond to attempted or successful malicious acts. This category of the survey investigates if appropriate drills or exercises are conducted periodically and if, provisions are in place at the healthcare facility to ensure if the security can be adjusted in response to an increased threat.

“Accountability and Security awareness” category refers to the personal dedication and accountability and understanding of all individuals engaged in any activity which has a bearing on the security of nuclear activities. “Each radioactive source periodically inventoried and accounted for, would not go unnoticed if it is missing or stolen?”, is an example question in this area. Accountable behavior means that all workers know their specific assigned tasks related to nuclear security and that they either execute these tasks as expected or report their inability to do so to their supervisor. Basic nuclear security awareness, such as, “I clearly known the difference between safety and nuclear and radioactive material security” will help broaden the thinking of people within the organization. Monitoring security awareness may also make staff and management pay more attention to the beliefs, attitudes and other cultural factors that underlie security performance.

The last two categories of the technical survey include “Transport” and “Training”. Questions, such as, “Training is provided towards secure use, storage and disposal of radioactive materials”, and if “Rewards and incentives are in place to recognize staff members contribution towards improving security?” provides clues if training program places adequate emphasis on security as it does to safety. Members of all organizations also need a clear understanding of who is responsible for what in order to achieve the desired result. With radioactive material being extremely vulnerable during transport, staff having necessary knowledge and skills should be effectively trained on secure movement of radioactive packages and evaluated periodically assuring comprehension of policies and procedures.

The survey responses were recorded from an actual medical facility to replicate the results realistically. Twenty-six respondents (16.2% participation) completed the general survey and fifteen respondents (9.37% participation) completed the technical survey. Each of the survey questions were formatted with a choice of seven levels of agreement from "strongly agree" to "strongly disagree"; a numerical value was given to each answer choice ranging from 1 to 7, 1 being "strongly agree" and 7 being "strongly disagree". The performance of a nuclear security regime ultimately hinges on how people behave. A workforce made up of individuals who are vigilant, question irregularities, execute their work diligently, and exhibit high standards of personal collective behavior will maintain tight security. Management must also do its part and apprise workers of what is expected of them, dole out rewards and punishments to shape their behavior.

To accentuate the observed security pattern of the healthcare facility, results of the two survey types were presented in three score ranges: weak (score > 4), neutral (score = 4), and strong (score < 4). The equally weighted categorical average, respective to its survey type, was totaled to emphasize the cumulative impact of the strengths and weaknesses of the healthcare facility's radiological security culture. The weighted sum, Z_{gen} and Z_{tech} obtained from the positive respondents (strength) found in either general or the technical survey reflected the impact of the security culture on the threat groups G1 and G3. A subset of questionnaires, highlighting the interactions between staff, personnel from external entities (mail services), and with the physical environment within the facility (visitors or students) were selected from the two survey types to compute Z_{sub}. . The weighted sum obtained from Z_{sub} is used to reflect the impact of security culture on the facility's vulnerability to attack from the G2 threat group. The rationale behind relating a security-minded nuclear and radiological culture to the expected utility of the threat group was to harness the impact of the changing espoused values (patterns of attitudes and beliefs, security protocol implementation, ineptitude in responding to alarms, poor communication etc.) on the value tradeoffs of the adversaries and the overall success probability of theft.

3.7 Blast basics and effects

The impact of explosive weapons can be broken down into the principal damage mechanism and their primary effects, and the secondary and tertiary effects occasioned by these. The study focuses on mostly the principal damage mechanism and their primary effects. Secondary and the tertiary effects which may be the result of secondary fragmentation from objects that have been affected by detonation are not thoroughly considered in the calculation of the blast effects. Tertiary effects, like the loss of electrical and gas services or lack of clean water caused by damage to water mains and sewers due to the blast, are beyond the scope of this dissertation.

Primary effects of explosive weapons are defined as those caused directly by the destructive effects that radiate from a point of detonation, including blast overpressure, fragmentation and heat and light (Ngo et al., 2007, GICHD, 2017)). The term ‘blast’ refers to a high-pressure blast wave moving at supersonic speed, referred to as the shockwave, which is followed by blast winds (US NRC, 2015). Primary fragmentation comprises of fragments that originate directly from the explosive weapon.

An explosion is defined as a large-scale, rapid, and sudden release of energy. Solid explosives are mainly high explosives for which blast effects are best known. They can be classified on the basis of their sensitivity to ignition. Materials such as mercury fulminate and lead azide are explosives that can be easily detonated by simple ignition from a spark, flame, or impact. Explosives like TNT and ANFO when detonated create blast (shock) waves which can result in widespread damage to the surroundings. The detonation of a condensed high explosive generates hot gases under pressure up to 300 kilo bar and a temperature of about 3000-4000C^{o}. The hot gas expands forcing out the volume it occupies. As a consequence, a layer of compressed air (blast wave) forms in front of this gas volume containing most of the energy released by the explosion. Blast wave instantaneously increases to a value of pressure above the ambient atmospheric pressure. This is referred to as the side-on overpressure that decays as the shock wave expands outward from the explosion source. After a short time, the pressure behind the front ay drop below the ambient pressure (Fig.3.9). During such a negative phase, a partial vacuum is created, and air is sucked in. This is also accompanied by high suction winds that carry the debris for long distances away from the explosion source (FEMA, 2003). When the shock wave encounters a surface that is in line-of sight of the explosion, the wave is reflected, resulting in a tremendous amplification of pressure. Unlike acoustical waves, which reflect with an amplification of two, shock waves can reflect with an amplification factor of up thirteen, due to supersonic velocity of the shock wave at impact[3].

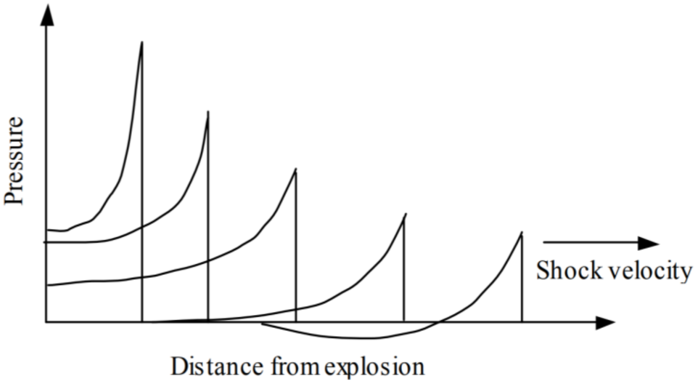


Figure 3. 9 Blast wave propagation (Ngo et al., 2007)

The threat from a conventional bomb is defined by two equally important elements, the bomb size, or charge weight W, and the standoff distance R between the blast source and the target. The Oklahoma City bomb in 1995, for instance had a charge weight of 1814 Kg (~4000 lbs..) at a standoff distance of 4.5m (Ngo et., 2007). The observed characteristics of air blast waves are found to be affected by the physical properties of the explosion source. Figure3.10 shows a typical blast pressure profile. At the arrival time t_A, following the explosion, pressure at that position suddenly increases to a peak value of overpressure, P_{so}, over the ambient pressure, P_o. The pressure then decays to ambient level at time t_d, then decays further to an under pressure P_{so-} (creating a partial vacuum) before eventually returning to ambient conditions at time $t_{d+} + t_{d-}$. The quantity P_{so} is usually referred to as the peak side-on overpressure, incident peak overpressure or merely peak overpressure. The negative pressure phase moves less quickly than the positive phase ad it generally lasts approximately three times as long.

[3] The physics of blast waves is a complex subject. More precise knowledge of blast behavior in different circumstances and environments requires advanced computer modelling. This study predicts the basic overpressure and stand off distance of a small size conventional explosives for purposes of calculating the fatalities and injuries from the blast.

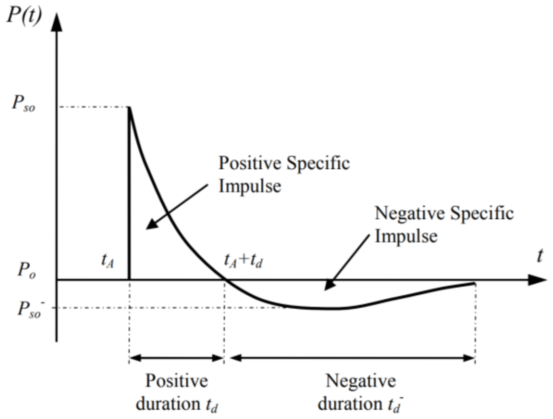


Figure 3. 10 Blast wave showing pressure changes (FEMA, 2003)

Vehicle bombs are able to deliver a sufficiently large quantity of explosives to cause potentially devasting structural damage. Another explosive attack threat is the small bomb that is hand delivered. Small weapons can cause the greatest damage when brought into vulnerable, unsecured areas of the building interior, such as building lobby, or retail spaces. Hand carried explosives are typically on the order of five to ten pounds of TNT equivalent. However, larger charge weights, in the 50 to 100 pounds TNT equivalent range, can be readily carried in rolling cases. This research considers the blast effects for a 150 pounds (68.04 kg) suitcase bomb and a 2000 pounds (907.18 kg) VBIED (FEMA, 2003). Table 3.3 gives a list of the type of container or vehicle in which the explosive is delivered.

Table 3. 3 Explosive capacity of typical bomb delivery methods ((Marchand & Alfawakhiri, 2004))

Delivery Method	Explosive Capacity (pounds/kilograms)
Mail bomb	5/2.3
Suitcase bomb	50/23
Automobile	500-1,000/225-450
Van	4,000/1,800

Truck	10,000-30,000/4,500-13,500
Semitrailer	40,000/18,000

3.7.1 Blast wave scaling laws

All blast parameters are primarily dependent on the amount of energy released by a detonation in the form of a blast wave and the distance from the explosion. A universal normalized description of the blast effect can be given by scaling distance relative to $\left(\frac{E}{P_o}\right)^{1/3}$ and scaling pressure relative to P_o, where E is the energy release (kJ) and $P_o$the ambient pressure. For convenience, however, it is general practice to express the basic explosive input or charge weight Was an equivalent mass of TNT. Two different weight TNT explosives will generate the same overpressure, but they will do so at a different distance from the explosive center. For a target to experience the same overpressure with a smaller bomb, the target will need to be much closer to the bomb than with a more massive explosive. This is the basic idea behind explosive scaling. Since the same overpressures will be generated by different weight explosives, the weight of the bomb can be combined with distance from the explosive to create a scaled distance parameter. The blast data from 1 kg of TNT is used as a reference explosion. Eq (3.29) was used to calculate the scaled distance parameter for the explosive weights of 150 lb. and 2000 lb. TNT equivalent.

$$Z = \frac{R}{W^{1/3}} \tag{3.29}$$

where

Z is the scaled distance parameter (m kg^{-1} TNT equivalent)

R is the radius from the center of the blast (m)

W is the equivalent weight of the explosive in TNT (kg).

Estimation of peak overpressure due to spherical blast based on scaled distance Z were introduced by Brode (1955) as:

$$P_{so} = \frac{6.7}{Z^3} + 1\ bar\ (P_{so} > 10\ bar) \tag{3.30}$$

$$P_{so} = \frac{0.975}{Z} + \frac{1.455}{Z^2} + \frac{5.85}{Z^3} - 0.019\ bar \qquad (3.31)$$

$$(0.1\ bar < P_{so} < 10\ bar)$$

where

P_{so} is the peak overpressure

Z is the scaled distance parameter (m kg-1 TNT equivalent)

For conversion purposes, 1bar = 14.50 psi=100 kPa. This research calculates the peak pressure as a function of the 150 lbs.-TNT equivalent and 2000 lbs.-TNT equivalent weapon yield, and the cube of the distance. Figure3.11 provides a quick method for predicting the expected overpressure (expressed in psi) on a building for a specific explosive weight and stand-off distance.

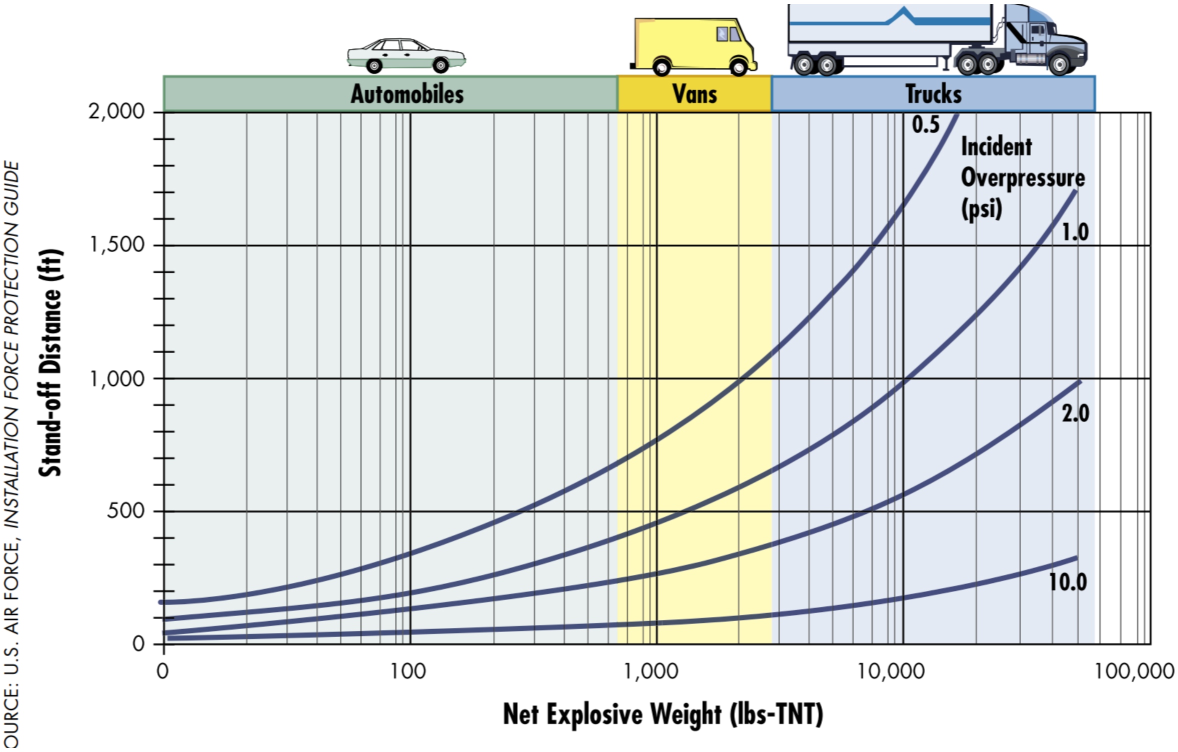
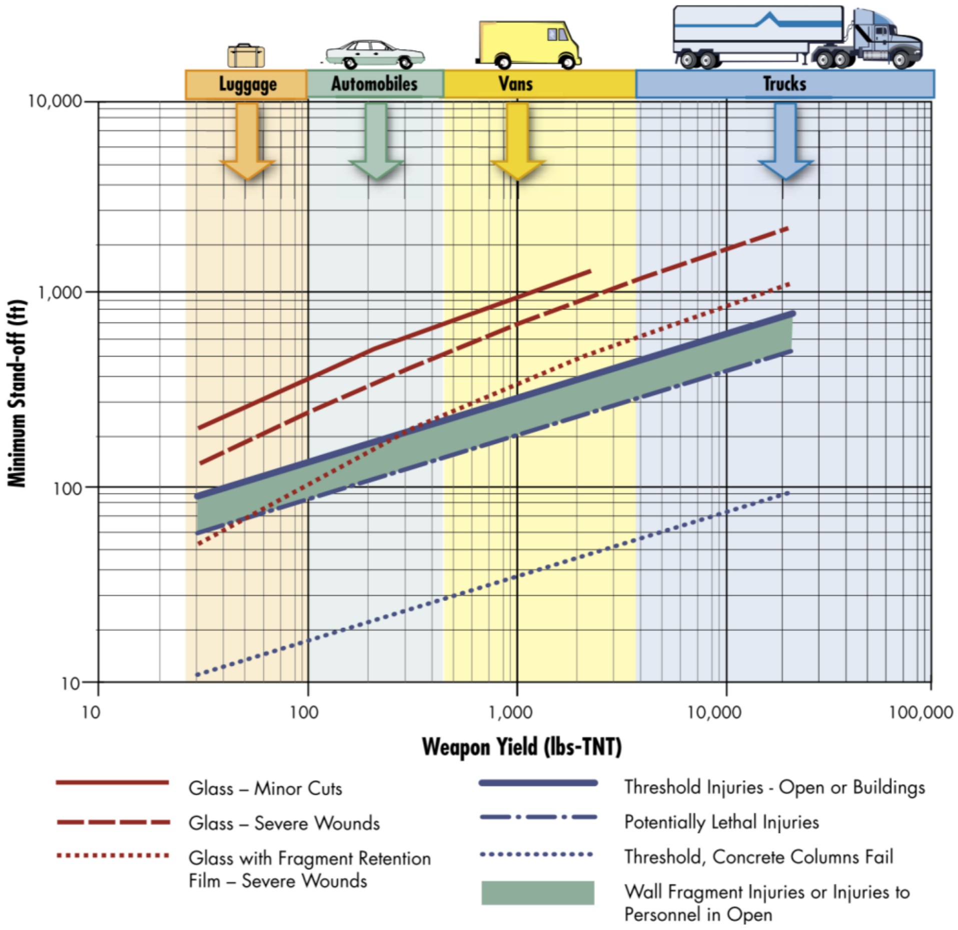


Figure 3.11 Incident overpressure measured in pounds per square inch (psi), as a function of standoff distance and net explosive weight (pounds-TNT) (FEMA, 2003)

3.7.2 Blast effects on structures

Figure3.11 can be used to predict damage for nominal buiding construction. Buildings experiences the effects of explosions in several stages: (1) The initial blast wave typically shatters windows and causes other damage to the building façade. It also exerts pressure on the roof and walls that are not direcly facing the blast, sometimes damaging them as well. (2) In the second stage, the blast wave enters the building and exerts pressure on the structure. When directed upward, this pressure may be extremely damging to slabs and columns because it acts counter to the desing used to resist gravity loads. Air-blast pressurs within a building can actually increase as the presure waves reflect from surfaces and can cause injuries to the occupants direcly by means of physical translation, ear, lung, and other organ damage, or debris from building elements and contents. (3) Finally, the building frame is loaded globally and responds a it would to a short duration, high intensity earthquake. In particular, the pressure experienced by a building increases with bomb size, but decreases very quickly with increasing distance between the building and the bomb.

As seen from Figure3.12, large explosive devices detonated at relatively greater standoff distances will produce a large but uniform pressure over the surface of the building. At lesser standoff distances, even a small explosive device can produce locally intense effecs, such as shattering load-bearing columns. The standoff distance is vital in the design of blast resistant structures since it is the key paramter that determines, for a given bomb size or charge weight, the blast overpressures that load the building cladding and its structural elements.



E: DEFENSE THREAT REDUCTION AGENCY

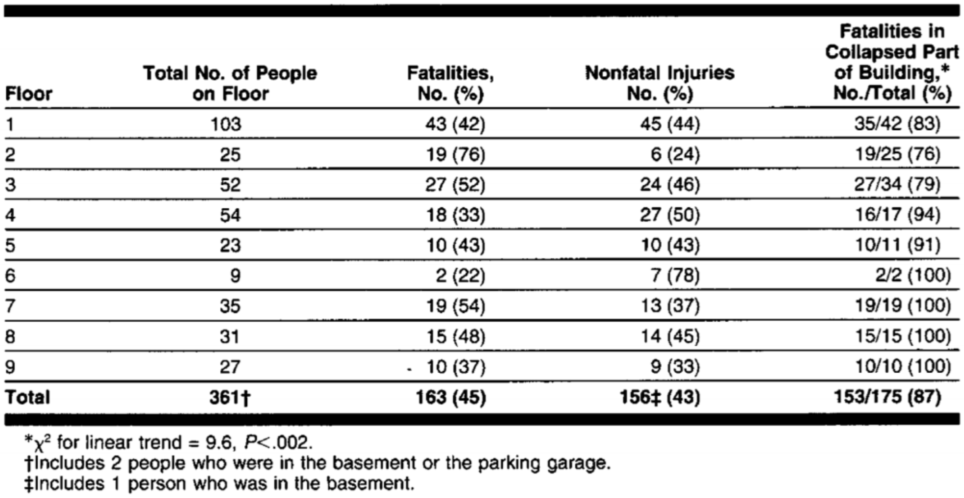
Figure 3. 12 Explosives environments – blast range to effects (Marchand & Alfawakhiri, 2004)

If a large explosive device is detonated close to the structure, global damage and the size of the resulting ground crater may be increased to the point that the structure, foundation, or both will be overwhelmed and a catastrophic collapse may ensue. The extent of damage due to progressive collapse was seen in the Oklahoma City bombing, where the short distance between the explosive laden truck and the transfer grider column line caused a 7-ft deep by 30 ft diameter crater to be framed in the pavement and subsurface material[4].

[4] Progressive collapse defined as “the spread of an initial local failure from element to element, eventually resulting in the collapse of an entire structure or a dispropotionately part of it”

Progressive collapse is a relatively rare event in the United States and other Western nations, as it requires both an abnormal loading to initate the local damage and a structure that lacks adequate continuity, ductility, and redundancy to resist the spread of damage. These abnormal loads can occur as errors or problems during construction, as accidental impacts of energy releases anytime during the structure's life, or as intentional attacks by terrorists or other aggresors. (GICHD, 2017). However the loads are generated, significant casualties can result when collapse occurs. Majority of the 168 fatalities were due to the partial collapse of the structure and not due to direct blast effects at the Alfred P. Murrah Federal building in Oklahoma City bombing. Table 3.4. shows the number of fatalities in the collapsed area of the Murrah building (U.S. Department of the Army, 2011).

Table 3.4 Fatal and nonfatal injuries by floor and building collapse in the Murrah building (Mallonee et al., 1996)



Floor	Total No. of People on Floor	Fatalities, No. (%)	Nonfatal Injuries No. (%)	Fatalities in Collapsed Part of Building,* No./Total (%)
1	103	43 (42)	45 (44)	35/42 (83)
2	25	19 (76)	6 (24)	19/25 (76)
3	52	27 (52)	24 (46)	27/34 (79)
4	54	18 (33)	27 (50)	16/17 (94)
5	23	10 (43)	10 (43)	10/11 (91)
6	9	2 (22)	7 (78)	2/2 (100)
7	35	19 (54)	13 (37)	19/19 (100)
8	31	15 (48)	14 (45)	15/15 (100)
9	27	10 (37)	9 (33)	10/10 (100)
Total	**361†**	**163 (45)**	**156‡ (43)**	**153/175 (87)**

*χ^2 for linear trend = 9.6, P<.002.
†Includes 2 people who were in the basement or the parking garage.
‡Includes 1 person who was in the basement.

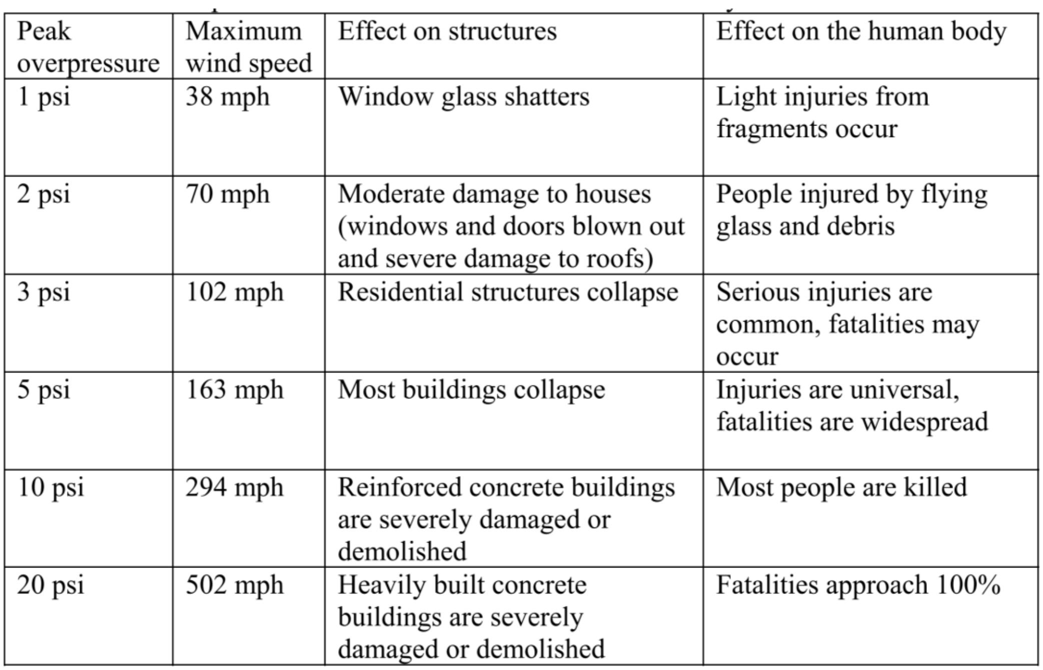
It is rather difficult to determine the number of deaths that would have occurred if the Murrah building had not collapsed. The medical examiner's office was unable to clearly distinguish deaths caused by primary blast effects and those caused by building collapse. However, the large risk ratio of 16 for persons in the collapsed area vs those in the uncollapsed area of the Murrah building leads us to regard the collapse as a major risk factor. Also, historically more building damage has been due to collateral effects than direct attack. In the PFRI model, the results of fatal and nonfatal injuries from Oklahoma City bombing are used and extrapolated to fit the 150 (pounds-TNT) and 2000 (pounds-TNT) explosives and the population density of the hypothetical healthcare facility. This method conservatively estimates the fatalities and injuries due to the blast. The calculation of explosion damage is mainly based on empirically derived criteria. With the help of charts and table, a more or less rough description of the damage to certain types of structures for each increment level of overpressure are drawn.

3.7.3 Blast effects on people

For personnel not directly exposed to an unabated air blast shock wave, human tolerance of blast effects can be considered relatively high. A TNT explosion can generate an audible sound and an expanding sphere of hot dense gas that can have a pressure of over $6.9 \times 10^{10} N/m^2$ $(10^7 psi)$. This pressure when transmitted into the surrounding medium creates a blast wave. The peak overpressure, P_{so} (Figure3.10.), propagating radially at velocities 3000 to 8000 meters per second can exert extreme force on objects and humans in its path and can reflect off solid object at 2 to 9 times the initial pressure, P_o. During the negative phase (Figure3.10), which lasts 3 times longer than the positive phase, the pressure passes back through the structure and the direction of the energy is reversed. The underpressure created by the negative phase and the blast wind from the overpressure leads to severe penetration or laceration type injuries, eardrum damage, lung collapse, blunt force trauma and even deaths. Injuries usually affect the head, neck, and extremities, suggesting a protective effect of clothing (U.S. NRC, 1993). Perforated tympanic membranes are common as a result of the blast and can result in conductive, neurosensory, or mixed type of hearing loss. The onset of lung hemorrhage begins in the range of 30 to 40 *psi*, with severe damage occurring above 8 *psi* and death in the range of 100 to 120 psi.

A 5 *psi* blast overpressure will rupture eardrums in about 1% of subjects, and a 45 *psi* overpressure will cause eardrum rupture in about 99% of all subjects(U.S. Department of the Army, 2011). A 35-45 psi overpressure may cause 1% fatalities, and 55 to 65 psi overpressure may cause 99% fatalities. Table 3.5. summarizes the effect of increasing blast pressure on various structures and the human body. This data originates from weapons tests and blast studies to assess the effect of blast overpressure on structures and people (Mazonka, 2012).

Table 3.5 Effect of various long duration blast overpressures and the associated maximum wind speed on various structures and the human body (Mazonka, 2012).



Peak overpressure	Maximum wind speed	Effect on structures	Effect on the human body
1 psi	38 mph	Window glass shatters	Light injuries from fragments occur
2 psi	70 mph	Moderate damage to houses (windows and doors blown out and severe damage to roofs)	People injured by flying glass and debris
3 psi	102 mph	Residential structures collapse	Serious injuries are common, fatalities may occur
5 psi	163 mph	Most buildings collapse	Injuries are universal, fatalities are widespread
10 psi	294 mph	Reinforced concrete buildings are severely damaged or demolished	Most people are killed
20 psi	502 mph	Heavily built concrete buildings are severely damaged or demolished	Fatalities approach 100%

While it is impossible to determine the exact correlation between blast wave overpressure and fatality rate for personnel in a blast explosion, the data in Table 3.5. appears to provide useful guidance.

3.8 Fragmentation effects

Primary fragmentation originates from the casing of the typically metallic warhead surrounding the high explosive charge. The remnants of the RDD weapon (shielded casing surrounding the radioactive material), in a similar manner, may fragment into shrapnel, radioactive metal projectiles and pieces of explosive’s casing, which may accelerate outwards and impact targets at high velocity. Primary fragments (projectiles) are normally small, high-speed fragments that cause injury by penetration and perforation of vital areas of the body. Secondary fragments are normally larger and have less velocity upon impact and cause non-penetrating blunt trauma. The secondary fragments which are not produced by the explosive device itself but are generated by air blast pressures or primary fragments impacting local objects are not considered in this risk model.

Primary fragments being another blast parameter are expected to injure the person in the vicinity to some extent. However, there is no guarantee that the target or the person hit by a fragment projectile will be killed or incapacitated. There are too many factors involved that may alter the outcome of the engagement. Thus, it makes sense to talk of damage in terms of probabilities. Hit probability is defined as the probability of a hit or hits being made on a target (person) out of a given number of projectiles directed at the target. In this research, the number of projectiles reference the number of fragments from the blast (N_{hits}). A hit is a blow or impact by a radioactive shrapnel or other projectile. Kill probability is defined as the conditional probability that a projectile will kill a target given that the projectile hits the target. This research defines the probability of kill (P_k) as a measure of the likelihood that the target will be either killed or incapacitated given that the fragment hits the target.

Owing to the many unknown variables of the exact shape, weight, impact energy and the aerodynamic performance of each fragment; few assumptions are made to predict upon the effects of fragmentation on the human targets. The incapacitation of the human target by fragment is attributed to the kinetic energy of metallic fragments. It is accepted that the probable lethal effect of fragments on a random person can be achieved in few seconds if that person is hit by at least one fragment that has a kinetic energy not less than 78 Joules. The research assumes the explosive casing and the radioactive material pellet casing to break into N_o fragments. The human target presenting a frontal area, A, to the fragment, is assumed to sustain a moderate level damage to the body, where many functions are lost but the person hit is still capable of operation ($P_{k|hit} = 0.2$). The expected number of hits (N_{hits}) is given by:

$$N_{hits} = A(\frac{N_0}{4\pi R^2}) \qquad (3.32)$$

Where

N_0 is the initial number of fragments from the explosion;

R is the range of fragment to the human target (m);

A is the frontal area of the fragment hitting the human target (m^2);

N_{hits} is the expected number of fragments

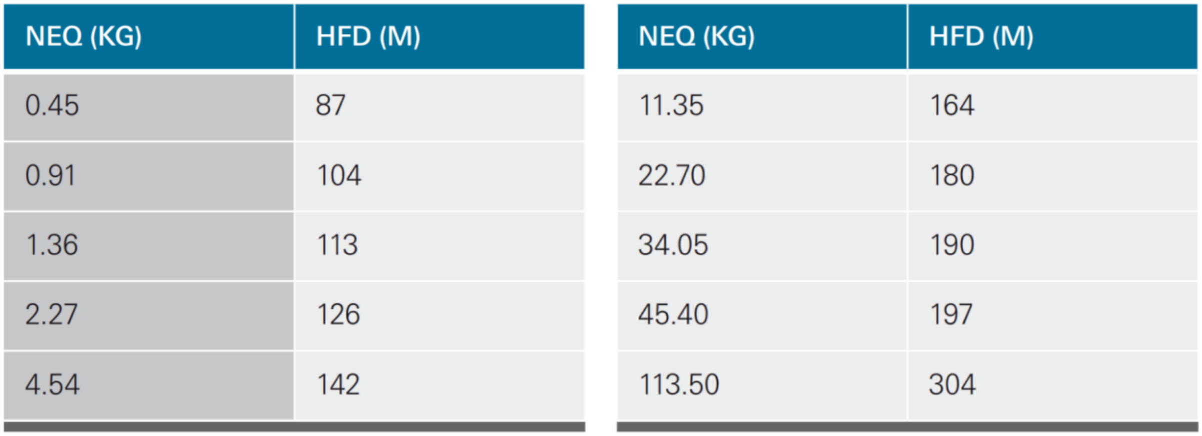
The study computes the hazardous fragment distance (HFD) as the distance measured from the point of explosion to the point at which the density of hazardous fragments generated by the explosion has decreased to where people in the open are not expected to be seriously injured. The HFD represents the distance at which the density of fragments in the air will likely reduce to 1 per 55.7 m^2 (U.S. DoT, 2011). The HFD distance, given by Eq (3.33) is one with a low probability of being hit by a hazardous fragment, and if one were hit after all, the impact would not be lethal

If $W \geq 100\ lb$:

$$HFD\ (ft) = -1133.9 + [389 \ln(W)] \tag{3.33}$$

Table 3.6 gives the HFD in meters for a nominal munition with a given net explosive quantity (NFQ in kg TNT equivalent (GICD, 2017).

Table 3.6 Hazardous fragment distances for a given net explosive quantity



NEQ (KG)	HFD (M)	NEQ (KG)	HFD (M)
0.45	87	11.35	164
0.91	104	22.70	180
1.36	113	34.05	190
2.27	126	45.40	197
4.54	142	113.50	304

Knowing the probability of human target surviving ($P_{k|hit}$) after N_{hits} hits, the total probability of a kill given N fragmentation hits can be calculated using the following equation (Deeney, 1970):

$$P_k = 1 - \left(1 - P_{K|hit}\right)^{N_{hits}} \tag{3.34}$$

where.

N_{hits} is the expected number of fragments hitting the target

$P_{K|hit}$ is the level of damage to the human target

The level of damage ($P_{k|hit}$) can range from 0.1 to 0.9, with 0.1 being light damage and 0.9 being heavy damage to the human target (Federal American Scientist, 1997; Denney, 1970).

The probability that a given human target is hit by at least one fragment reduces with distance. The further a target is from the point of detonation, the less likely it is to be hit by the fragmentation produced. Many projectiles inflict damage to a target without having to impact the target directly. The blast or explosion effect of a fragment or shrapnel may cause damage to the target if the target is within a lethal area from the burst point of the fragment. Lethal area of a given fragment is called the region A_L around the center of explosion inside which the incapacitation or kill probability is equal to 1 ($P_k = 1$) whereas outside A_L the probability approaches 0. Lethal area A_L lies within the HFD and can be written as (Myers, 1963; Mazonka, 2012):

$$A_L = \pi R_L^2 \tag{3.35}$$

$$R_L = R_D\sqrt{P_k} \tag{3.36}$$

where

A_L is the lethal area

R_L is the lethal range

R_D is the radius of the border where $P_k(x_{HFD}, y_{HFD}) = 0$

The expected number of casualties can be estimated as:

$$E_k = nA_L \tag{3.37}$$

where

E_k is the expected number of casualties from primary fragmentation effects

n is the number of people in the area ($population\ density\ km^{-2}$)

As per the Geneva International Center of Humanitarian Demining (GICHD, 2017), warheads utilizing pre-formed fragmentation or pre-fragmented munitions casings are easier to predict, generating more consistent fragmentation effects. Due to the greater variation in the size and number of fragments caused by the explosion, natural fragmentation is more difficult to predict and model (GICHD, 2017). When examining the effects of fragmentation on the human body, it is important to note that these vary significantly based on the amount of body area exposed to the fragmentation and the posture of the victim when struck. With every person's unique physiology and the location of impact, it is likely that one person would be killed but another would only be injured with the similar sized piece of fragmentation. With most people suffering multiple injuries on various part of their bodies indicate a variation in the aerodynamic drag followed by a variation in the velocity of each fragment. This research, however, considers all fragments to be of the same velocity and hence same kinetic energy.

The risk of injury from blast overpressure is represented by a smaller radius than the risk of fragment injury, as blast pressure drops much more rapidly than the rate that fragments lose velocity (GICHD, 2017). For explosions that occur in open spaces, the majority of injuries will be caused by fragmentation. Buildings can provide a level of protection from primary fragmentation. An urban environment, composed of brick, stone and concrete structures, would provide a much greater amount of protection from primary fragmentation as majority of the fragment's energy would likely be absorbed in the initial impact than the weaker structures. Studies have found that detonations in enclosed area had significantly higher morbidity and mortality than those in open space attacks. The reflection and the consequent intensification of blast waves within the confined space can cause significant primary blast and fragmentation injuries than those that occur in open.

Although the targeted building is at greatest risk of collapse, other nearby buildings may also collapse and for the buildings that remain standing, flying debris generated by exterior cladding may cause severe injuries. In the Oklahoma City bombing, a total of nine adjacent buildings collapsed and several persons lost their lives after being stuck by structural debris generated by infill walls of a concrete frame building across the street from Murrah building. In Khobar Towers bombing in 1996, most of the U.S. servicemen who lost their lives were impacted by high velocity projectiles created by failure exterior cladding on the wall that faced the weapon (FEMA, 2003). Oklahoma City bombing mortality and morbidity rates from buildings other than the targeted one are extrapolated to account for the collateral damage on other structures surrounding the hypothetical facility in the present PFRI model.

3.9 Deterministic effects of radiation

Among the three causes of early death from radiation exposure, hematopoietic syndrome (H-ARS) will be the dominant cause of early fatalities following brief whole-body exposures to external gamma rays (IAEA, 2005b; U.S. NRC, 2003). Scientific understanding of the biological nature of early effects indicates that most are threshold effects i.e., in any individual the effect will not be experienced unless a threshold dose is exceeded. However, for many effects the available data are too weak to permit precise identification of population thresholds. The median lethal dose for humans is not precisely known for H-ARS. Several estimates have been published, ranging from 2.4 to 5.1 Gy to the bone marrow.

The limited human evidence on the effects of doses of low-LET radiation received at low dose rates also suggests that these doses may be less effective than the same doses received at high dose rates. An anecdotal evidence is found in the experience of 23 Japanese fishermen exposed to fallout, seven were estimated to have received doses greater than 4 Gy and all of them survived. Scott & Hahn (1980) have proposed mathematical models that quantitatively express the dependence of the median lethal dose on the dose rate of low-LET radiation. For the purpose of this research, 4.5 Gy is used as the LD_{50} (dose that produces lethality in 50% of the population) for estimating the risks of hematopoietic syndrome mortality.

In pulmonary syndrome, the lungs may be irradiated from external sources, e.g., cloudshine and groundshine, and by radionuclides that are inhaled. Acute radiation pneumonitis may occur following such exposures. Because large doses are required to induce this effect (LD_{50}~$10.4\ Gy$), early fatalities from pulmonary injury are not expected to occur as a result of the RDD exposure or uniform external whole-body irradiation. Irradiation of the abdomen may lead to the gastrointestinal syndrome (GI-ARS). In animal experiments, the gamma or X-ray doses required to cause death from the GI-ARS have been in the range of 10 to 50 Gy. These are much higher than the doses necessary to cause death due to bone marrow syndrome. In RDD attack, the GI-ARS is unlikely to be induced by exposure to amounts of radioactivity found in groundshine or cloudshine.

Deterministic effects such as epilation, dry and moist desquamation, blister formation, ulceration and necrosis are the non-fatal effects which do not lead to death but reduce the quality of life.

The biophysical model used for evaluating onset of severe deterministic effects was proposed by Scott & Hahn (1980). The model connects the characteristics of acute exposure with the onset of deterministic effect. Its mathematical formulation is given by the IAEA (2005b):

$$P_{T,S} = 1 - e^{-H_{T,S}} \tag{3.38}$$

where

$P_{T,S}$ is the probability of the onset of irreversible injury of critical tissue which leads to a particular deterministic effect or syndrome S in organ or tissue T ; and

$H_{T,S}$ is the hazard function describing syndrome S of irreversible injury in organ or tissue T.

The non-linear sigmoid dose-effect dependence for onset of radiation health effect is a defining characteristic of severe deterministic effects. In the case of high dose extended irradiation of an organ or tissue any additional dose increment leads to an increment in risk which depends not only on dose growth value but also on the previously accumulated dose (IAEA, 2005b). Taking this into account, the PFRI risk approach used the principle that the start of a deterministic effect in a particular organ depends on the distribution of relative biological effectiveness (RBE) weighted absorbed dose rate over the exposure period. The cumulative hazard functions used to predict early effects was proposed as a two-parameter Weibull functions of the form (Scott & Hahn, 1980):

$$H = \ln(2) \times \left(\frac{D}{LD_{50}}\right)^{V} \tag{3.39}$$

where

H is the hazard lethality, $D$is the dose received in Gy,

LD_{50} is the dose that produces lethality in 50% of the population, and;

V is the shape parameter.

Subsequently this approach was developed in the NUREG/CR-4214 reports using the available literature data on animal experiments and investigation of human exposures (U.S. NRC, 1993). The model uses the concept of 'adjusted dose' to describe exposure conditions in order to assess the onset of deterministic effects. The IAEA modified the hazard function equation to develop emergency response criteria that met the international requirements for emergency preparedness and response. The modified model uses the concept of RBE-weighted dose (IAEA, 2005b; V Kutkov et al., 2011). The RBE-weighted absorbed dose in organ or tissue, AD_T, is defined as a product of average dose in organ or tissue, and relative biological effectiveness given by Eq (3.40):

$$AD_T = \sum_R D_{T,R} \times RBE_{T,R} \qquad (3.40)$$

where, $D_{T,R}$ is an average dose of radiation R in organ or tissue T, and $RBE_{T,R}$ is the relative biological effectiveness of the radiation R in producing the particular deterministic effect in organ or tissue T.

The modified model used in such an approach is based on the concept of irreversible injury as a precursor of deterministic effect. An irreversible injury is a level of cell death in an organ or tissue that cannot be compensated and determinately leads to failure of function or/and structure of the organ or tissue, which is diagnosed as a deterministic effect or syndrome S (V Kutkov et al., 2011). The hazard function $H_{T,S}(\tau)$ is the probability that irreversible injury, S, will not be developed in organ or tissue T during a time shorter than a period τ of exposure. The hazard function is defined by:

$$H_{T,S}(\tau) = \ln(2)\left[\int_0^{\tau} \frac{AD_{T,\dot{S}}(t)}{\theta_T^{\infty} + \theta_T^{1}\left(AD_{T,\dot{S}}(t)\right)^{-1}} dt\right]^{V_T} \quad A\dot{D}_{T,S}(t) > TD_{T,S} \qquad (3.41)$$

where,

$H_{T,S}(\tau)$ is the hazard function of syndrome S in tissue T, $A\dot{D}_{T,S}(t)$ is the adjusted dose rate (Gy h-1) of tissue T at time t after beginning of initial exposure, θ_T^{∞} is a parameter characterizing the radiosensitivity of a given organ or tissue and is equal to the asymptotic value of the median dose that results in affecting 50% of those exposed for a very high dose rate exposure (Gy), θ_T^1 is a parameter characterizing the effectiveness of repair of the radiation injury and accounts for the influence of dose rate on the development of a deterministic effect in organ or tissue T; V_T is a parameter characterizing the variability of radiosensitivity or organ or tissue T and the ability to compensate for its radiation-induced injury. $TD_{T,S}$ is the threshold dose for a given syndrome S and tissue T (Gy) (IAEA, 2005b; V Kutkov, 2011).

The basic scenario of external emergency exposure assumes an acute exposure with a constant dose rate $A\dot{D}_T$ during time τ. The hazard function which follows from Eq (3.41) for the external exposure scenarios is given by Eq (3.42) (Adams & Casagrande, 2019).

$$H_{T,S}(\tau) = \ln(2)\left[\frac{A\dot{D}_T \times \tau}{\theta_{T,S}^{\infty} + \theta_{T,S}^{1}(A\dot{D}_T)^{-1}}\right]^{V_T} \qquad (3.42)$$

Each parameter in Eq (3.41) and Eq (3.42) changes how the hazard function reacts with changing dose or dose rate. Perhaps the most important is $\theta_{T,S}^{\infty}$, which defines when the risk of developing the syndrome is 50% with an infinite dose rate. In other contexts, $\theta_{T,S}^{\infty}$ is frequently called the LD_{50}, or the dose that cause the effect in 50% of the population. ARS is a deterministic effect with a threshold below which the syndrome does not occur. As the risk of developing the syndrome of interest asymptotically approaches zero as dose decreases, defining an exact threshold is impossible. Instead, the threshold used in this work was the dose that causes the syndrome in 5% of the population (LD_{05}). Values for $\theta_{T,S}^{\infty}$, $\theta_{T,S}^{1}$, $V_{T,S}$ and $TD_{T,S}$ for each syndrome along with target organs are listed in Table 3.7 (Bland & Potter, 2018).

Table 3. 7 Hazard function parameters for H-ARS, GI-ARS and P-ARS. Threshold dose,$TD_{T,S}$, is the dose that causes the syndrome in 5% of the population (ICRP, 2000, 2006, 2016)

Syndrome	Target organ	RBE (β or γ)	$\theta_{T,S}^{\infty}[Gy]$	$\theta_{T,S}^{1}[Gy\ h^{-1}]$	$V_{T,S}$	$TD_{T,S}$
Hematopoietic syndrome	Red bone marrow	1	4.5[a]	0.1	6	3.0[a]
GI syndrome	Small intestine and colon	1	15	4	10	12
Radiation-induced pneumonitis	Lung (specifically alveolar interstitial [AI] region)	1	10	30	5	8

[a] Assuming medical treatment. Without medical intervention, $\theta_{T,S}^{\infty}$ for hematopoietic syndrome decreases to 3.0 *Gy* and the $TD_{T,S}$ decreases to 2.0 *Gy-eq* to the red bone marrow.

The primary exposure for RDDs are groundshine, inhalation, and deposition on the skin, hair, and clothes. The relative importance of the pathways depends on the material and the device geometry. Removal of outer clothing should reduce your external contamination by up to 90%. Washing exposed skin and hair will remove most of the rest. Inhalation or inadvertent ingestion of radioactive contamination within the immediate environment of the incident may lead to possible radiological consequences. The possibility of direct exposure from fragment of the source remaining in the immediate vicinity of the exposure is an important pathway. In the rare occasion of radioactive source-material shrapnel being embedded in an individual from the explosion, the dose rate at point p due to radioactivity of the nuclide in the tissue at a distance R from point p is computed as:

$$\dot{D} = C\Gamma\frac{4\pi}{\mu}(1 - e^{-\mu R}) \qquad (3.43)$$

where $\dot{D}$ is the dose rate in rem/hr, C is the concentration of the nuclide $Ci\ m^{-3}$, Γ is the specific gamma constant in $R\ m^{2}Ci^{-1}h^{-1}$, μ is the linear absorption coefficient in cm^{-1} and R is the distance in cm between the source volume and the tissue.

Internal contamination from radionuclide (*^{60}Co, ^{137}Cs, ^{192}Ir*) intake increases lifetime cancer risk and can potentially cause ARS if enough radioactive material is ingested or inhaled. Individuals contaminated during the Goiania incident suffered a range of acute injuries, including H-ARS, GI-ARS as well as a host of prodromal symptoms. Contaminated individuals in Goiania had ingested an estimated activity between *10^7 and 10^9 Bq* of *^{137}Cs* and received whole body doses between 3 and 8 Gy. The six-year-old girl who died a month after the exposure, had an intake of *^{137}Cs* of *1 GBq (27 mCi)*, the greatest recorded, and had an estimated internal dose of about 4 Gy at the time of death. Though highly unlikely, but in an accidental intake of 10 times greater than the specific ALI (inhalation and oral) of the radionuclides (*^{60}Co, ^{137}Cs, ^{192}Ir*), models of radionuclide metabolism and dosimetry is used to calculate the internal deposition and retention of these radionuclides and the resulting internal radiation dose.

^{60}Co

As *^{60}Co* source from Gamma Knife®, cobalt exists in metal pellet form and is considered to exhibit retention characteristics of class W compounds. ICRP 30 considers cobalt to be relatively poorly absorbed by the GI tract and therefore assigns an absorption coefficient *(f_1)* of 0.05 to both class W and Y compounds. Of the *^{60}Co* entering the blood stream, about half is excreted directly, with the remaining half distributed in the body. Of the amount distributed in the body, 10% is assumed to go to the liver and remaining 90% is distributed throughout the rest of the body. According to ICRP 30, the material deposited in body organs (other than lung) is removed from the organs at several rats. In the absence of retention data on a case-specific basis, the ICRP recommends that the following retention rates be applied to the material in the rest of the body:

$$R(t) = 0.5e^{-0.693t/0.5} + 0.3e^{-0.693t/6} + 0.1e^{-0.693t/60} + 0.1e^{-0.693t/800} \qquad (3.44)$$

Therefore, of cobalt entering the transfer compartment a fraction 0.5 is assumed to go directly to excretion, 0.05 to the liver and 0.45 to all other organs and tissues of the body amongst which it is assumed to be uniformly distributed. Of cobalt translocated from the transfer compartment to any tissue of the body, fractions 0.6, 0.2 and 0.2 are assumed to be retained with biological half-lives of 6, 60 and 800 days respectively. Cobalt is assumed to be retained in the transfer compartment with a half-life of 0.5 days (ICRP, 2016).

^{137}Cs

Evidence indicate that *CsCl* and other commonly occurring compounds of cesium are rapidly almost completely absorbed from the GI tract. In this research f_l is taken to be unity for all compounds of the element (ICRP, 2017). Animal experiments have shown that *CsCl* is rapidly and completely absorbed from the respiratory tract following inhalation. Specific parameter values for *CsCl* would be the same as default Type F cesium parameter values, and therefore cesium chloride is assigned to Type F. Cesium acts as a potassium analogue and is partitioned primarily into muscle tissue, though it can be found in soft tissues throughout the body. Retention of cesium and potassium are related, though cesium is generally retained longer than potassium. The retention of cesium is adequately represented by a two-exponential expression

$$R(t) = ae^{-0.693t/T_1} + (1-a)e^{-0.693t/T_2} \qquad (3.45)$$

Values of a have been reported in the range 0.06 to 0.15, values of T_1 from 1 to 2 days, and values of T_2 from 50 to 150 days. In this study, it is assumed that, of cesium entering the transfer compartment, a fraction, 0.1, is translocated to one tissue compartment and retained there with a half-life of 2 days, whereas the remainder is transferred to a second tissue compartment and retained there with a half-life of 110 days. It is also assumed that cesium translocated to these compartments is uniformly distributed throughout the body.

^{192}Ir

Evidence found on the behavior of inhaled iridium in human subjects following accidental intake of elemental iridium showed majority to be deposited in the upper respiratory tract. Only approximately 0.2% of the initial deposit was retained in the lungs after 2 days, clearing with a half-time of approximately 23 days. These results suggested that the rapid dissolution rate is high compared with the particle transport rate from the upper respiratory tract. In ICRP 30, an absorption value of 0.01 is recommended for all chemical forms. On that assumption, this study assumes f_l of approximately 0.01, indicating assignment to Type S. No human data are available on the absorption of iridium from the GI tract. The whole-body retention of iridium is well described by a function of the form:

$$R(t) = 0.95e^{-0.693t/2} + 0.05e^{-0.693t/14} \qquad (3.46)$$

Biokinetic data presented in ICRP publication 137 (ICRP, 2017)indicates that whole-body retention in not predictable on the basis of body size and does not vary greatly from one species to another. Three phases of excretion of absorbed or intravenously injected iridium are indicated: a rapid phase of loss, primarily in urine, with a half time of a few hour; and intermediate phase of loss with a half-time on the order of 1-2 weeks; and a show phase of loss with a half-time of several months. Concentrations of iridium in the kidneys and liver are much higher than those in most other tissues.

3.10 Stochastic effects of radiation

An RDD attack is likely to result in dispersion of radioactive substances. The potential radiation exposure can vary considerably in magnitude, depending upon factors such as the total amount of radioactive material, the energy with which they are dispersed into the environment, the nature of the surrounding environment, and the mechanisms of radionuclide dispersion and transfer. People directly involved in a radiological attack will include members of the public in the affected areas and also rescuers responding to the event. The overall risk of the individual person represents the summation of effects of external and internal exposures.

Pathways of external exposure including dose from the fragment wound and dose from inadvertent ingestion or inhalation of greater than 10 times the ALI of radionuclide is considered in the deterministic effect of the attack. Cancer and hereditary disease are stochastic effects believed to evolve from single mutated cells that have survived radiation exposure. Epidemiological studies of large groups of exposed and non-exposed people are generally required to reveal whether there is a radiation associated excess of stochastic effects. These epidemiological studies have allowed the ICRP to make estimates of radiation cancer risk. A comprehensive review of the epidemiological data has led the BEIR VII and the ICRP committee to conclude that the risk would continue in a linear fashion at lower doses without a threshold and that the smallest dose has the potential to cause a small increase in risk to humans. These assumptions of the LNT model remains a subject of controversy, where the risks from low doses of radiation are extrapolated by some investigators from the apparently linear relationship between cancer incidence and radiation exposure observed at markedly higher doses (Weber & Zanzonico, 2017). Despite the challenges associated with understanding the health effects of low doses of low-LET radiation, the BEIR-VII committee concludes that current scientific evidence is consistent with the hypothesis that there is a linear dose-response relationship between exposure to ionizing radiation and the development of radiation-induced solid cancers in humans. The committee further judges it unlikely that a threshold exists for the induction of cancers but notes that occurrence of radiation-induced cancers at low doses will be small (BIER, 1990; BEIR, 2006).

In the period of time from the first few hours to a few days after the RDD attack; it is presumed that the ultimate consequences of the event will be influenced by particular characteristics of the affected environment. Internal exposure would arise mainly as a result of ingestion of water or foodstuffs contaminated directly, or agricultural products such as milk derived from contaminated areas. Inhalation is a less likely route but should be considered if significant resuspension were to occur from radioactive material deposited on the ground. If there were a prolonged release, inhalation from the plume would also take place. In an RDD incident, any significant inhalation dose would come from plume passage within a few hundred meters of release. Based on the experiments for an outdoor explosion of an RDD, the plume passes the immediate area within ~10-15 minutes and is gone by the time most of the early first responders arrive (Harper et al., 2007).

Depending on the amount of radiation exposure, whether it is from outside the body (external) or from uptake of radioactive materials (inhalation, ingestion, or uptake through wounds or skin), various health effects can occur. Different types of radiation have different effectiveness to induce damage. Besides, different organs and tissues have different sensitivities to radiation exposure. Therefore, the absorbed dose has to be weighted to take account of these differences. The respective weighting factors are termed 'radiation weighting factors', w_R, and 'tissue weighting factors', w_T; their values are recommended by ICRP (ICRP, 1991). The quantities resulting from the absorbed dose weighting for the effectiveness of the different radiation types and the radiation sensitivity of different organs and tissues are termed 'equivalent dose' and 'effective dose', respectively. Figure3.13 provides a visual relation among the relevant quantities.

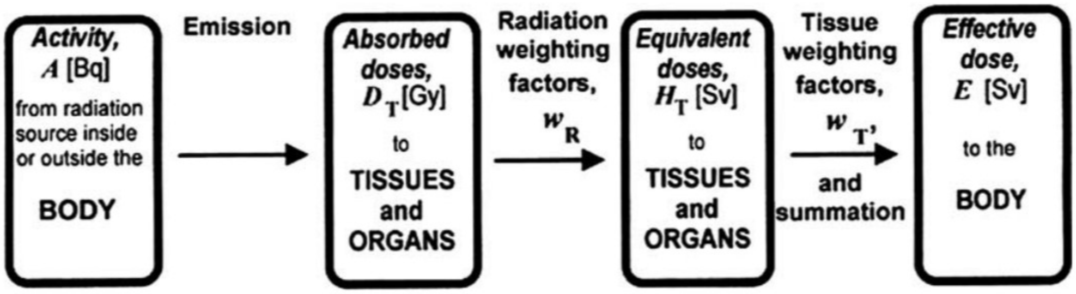


Figure 3. 13 Visual representation of activity, absorbed dose, equivalent dose, and effective dose.

The effective dose,E, results from weighting the equivalent dose by the tissue weighting factors, w_T, and summing up all over all tissues.

$$E_T = \sum w_T \sum_R w_R D_{T,R} \tag{3.47}$$

w_R is the radiation weighting factor for radiation R and $D_{T,R}$ is the average absorbed dose in the organ or tissue T. The unit of effective dose is *J/Kg* or *Sv.* The U.S. NRC defines the total effective dose equivalent (TEDE) as the sum of the effective dose equivalent ($H_E \; or \; E_T$) (for external exposures) and the committed effective dose equivalent ($H_{T,50}$) (for internal exposures). TEDE is the most complete expression of the combined dose from all applicable exposure pathways. In order to estimate TEDE in an affected urban area, simulations are performed using HOTSPOT Version 3.0.3, Health Physics software designed for short-term release durations and useful in predicting the consequences of radionuclide dispersal (Biancotto et al., 2020).

3.10.1 The HOTSPOT code and Risk coefficients

HOTSPOT *Health Physics Code* was developed and has been maintained by the U.S. DOE (Homann & Aluzzi, 2013). The code is freely available and was created to equip emergency response personnel and planners with a fast, field –portable set of software tools for evaluating incidents involving radioactive material. The code conservatively assesses the dose and the concentration of radionuclides on a spatial basis resulting from the atmospheric release of radioactive materials. The HOTSPOT code includes different atmospheric dispersion models to estimate the short-range (less than 10 km), downwind radiological impact following the release of radioactive material resulting from a short-term release, explosive release, fuel fire, or an area contamination event.

In the present assessment the *general explosion* module is used to study the atmospheric dispersion of radionuclides following an explosion involving radioactive material. HOTSPOT uses an empirically-based expression to describe the time-dependent height of the cloud top (*H*) as a function of the quantity of the explosive (*w*) and the time since detonation (*t*) for unstable and stable/ neutral atmospheres (as explained in the HOTSPOT user's Guide, *H* is in meter, *w* in pounds and *t* in seconds). In the code, the expression for the time after detonation (*t_m)* at which the maximum cloud rise is attained is:

$$t_m = 21.6w^{0.33} \tag{3.48}$$

The expressions for the stabilized cloud top (*H*) as a function of high explosive for unstable (stability class A, B and C) and stable/neutral (stability class D, E, F, and G) atmospheres are:

$$H_{A,B,C}(w) = 27.04w^{0.48} \tag{3.49}$$

$$H_{D,E,F,G}(w) = 23.3w^{0.44} \tag{3.50}$$

When the software is launched, the user is allowed to select either SI or U.S. units.

The HOTSPOT code uses Gaussian plume dispersion model where the *x* axis is the downwind axis, extending horizontally with the ground in the average wind direction. The *y* axis is the crosswind axis, perpendicular to the downwind axis, also extending horizontally. The *z* axis extends vertically from the ground. A plume travels along, or parallel to, the downwind axis, and reflects off the ground surface when the plume touches down (Figure3.14). *C(x,y,z,H)* is the time integrated atmospheric concentration $Ci - s\ m^{-3}$, with *H* being the effective release height (*m).*

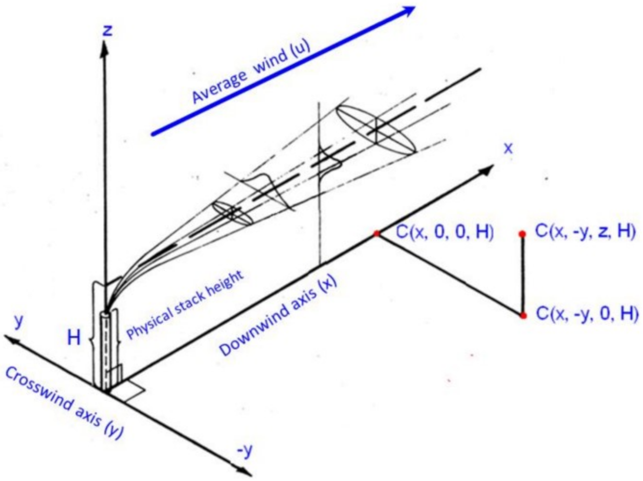


Figure 3.14 The HOTSPOT Health Physics Code Plume Coordinate System

The code assumes the target individual to remain at the same downwind location *(x,y,z)* throughout the passage of the plume and default release duration of the radioactive material is 10 minutes.

HOTSPOT gives the user the option to select two terrain types-Standard and City. The City terrain factor accounts for the increased plume dispersion from crowded structures and the heat retention characteristics of urban surfaces, such as asphalt and concrete. The City terrain factor will estimate lower concentrations than the standard factor, due to the increased dispersion from large urban structures and materials. HOTSPOT limits the maximum downwind distance to 200 *km* and minimum distance to 0.01 *km*. The present study uses the default source term geometry (of *0.01 km* and *100 km* plume downwind distance) to model the 'general explosion' module.

The standard deviation of the Gaussian concentration distribution in crosswind direction (σ_y) are representative of observing plume characteristics over a time period of 10 min. This averaging time in the HOTSPOT code is referred to as the sampling time. Concentrations downwind from a source decrease with increasing sampling time primarily because of a larger σ_y (increased meander of wind direction). The sample time for the explosive-release program, which is what this study uses for RDD, is fixed at 10 min and cannot be altered.

According to the HOTSPOT code, if the user is unable to visually estimate or calculate the effective release height, using the actual physical height of the stack as the effective release height (*H)* value is the recommended approach. In the present PFRI study, H is the roof of the healthcare building, set at 20 m - is considered to be the detonation location in the model. Radioactive material deposited on the ground can continue to expose individuals through ground shine and resuspension. The resuspension factor is defined as the ratio of the radionuclide air concentration above ground ($Ci\ m^{-3}$) and the radionuclide ground contamination ($Ci\ m^{-2}$). A typical output summary produces an outline of results for the radionuclide entered, along with the estimations of the projected committed effective dose equivalent values.

The present analysis considers three reference scenarios covering the detonation of three radionuclides (*^{60}Co, ^{137}Cs, ^{192}Ir)*. The TEDE is evaluated for different source activities. The material at risk for ^{60}Co is equal to $2.22 \times 10^{14} Bq\ (6000\ Ci)$, ^{137}Cs is equal to $1.07 \times 10^{14} Bq\ (2900\ Ci)$, and ^{192}Ir is equal to $5.55 \times 10^{11}\ Bq\ (15\ Ci)$. The rest of the HOTSPOT parameters such as: explosive weight, atmospheric conditions (wind speed and stability class), radionuclide solubility and respirable fraction in the plume are kept constant. Several assumptions are common in all simulations: the mass of the radionuclide is totally dispersed directly into the atmosphere and – in the evaluation of the TEDE-ground shine and re-suspension are also included; dose conversion coefficients in HOTSPOT are derived from the U.S. Federal Guidance Report (FGR) 11, with ICRP 30 being the intended lung model of choice. HOTSPOT's default settings of 4-day exposure time and breathing rate of $3.33 \times 10^{-4} m^3 s^{-1}$ are used. Results are presented based on the three TEDE contours. The dose perimeters (contours) shown below in Table 3.8 are adopted from the IAEA countermeasure zones recommended for all nuclear or radiological related incidents (IAEA, 2011).

Table 3.8 Dose contours recommended by the IAEA for urgent protective measures.

Generic intervention level (Effective dose) – IAEA (Sv)	Perimeter	Countermeasures
0.01	Outer	Sheltering
0.05	Middle	Evacuation in first week
1	Inner	Evacuation/relocation

Radiation dose levels (TEDE) within the contour are higher than the contour line value, and radiation dose levels outside the contour are lower than the contour value. As mentioned, the guidance is intended for all nuclear or radiological accidents or incidents. A RDD is, however, significantly different than the detonation of a nuclear device or an accident of the size of Chernobyl. Other countermeasures, including improvised respiratory protection, quick external decontamination and sequestering of individuals for further medical treatment (e.g., Prussian Blue, chelating agents etc.) should also be considered.

Estimation of the potential risk from low levels of ionizing radiation requires application of dose-to-risk conversion factors to an estimate of the dose. The U.S. EPA, in coordination with other Federal agencies involved in radiation protection, has issued Federal Radiation Guidance Report 13, *Cancer Risk Coefficients for Environmental Exposure to Radionuclides* (ICRP, 1994; U.S EPA, 1999), documenting a compilation of risk factors or doses from external gamma radiation and internal intakes of radionuclides. The PFRI model estimates the mortality and morbidity cancer risks for inhalation, ingestion and exposure pathways by multiplying the TEDE values by the cancer risk coefficients.

3.10.2 Risk coefficients -FGR 13

As per the Federal Guidance Report No. 13 (US EPA, 1999), for a given radionuclide and exposure mode, both a “mortality risk coefficient” and a “morbidity risk coefficient” are provided. A mortality risk coefficient is an estimate of the risk to an average member of the U.S. population, per unit activity inhaled or ingested for internal exposure or per unit time-integrated activity concentration in air or soil for external exposures, of dying from cancer as a result of intake of the radionuclide or external exposure to its emitted radiations. A morbidity risk coefficient is a comparable estimate of the average total risk of experiencing a radiogenic cancer, whether or not the cancer is fatal (US EPA, 1999).

The risk coefficients in the Federal report are expressed as the risk of cancer mortality and morbidity for inhalation, ingestion, and exposure per unit activity intake (Bq^{-1}). The risk coefficients for inhalation of radionuclides in particulate form are based on an assumed activity median aerodynamic diameter (AMAD) of 1 μm. The form of inhaled material is classified in terms of the rate of absorption from the lungs to blood, using the classification scheme of ICRP *Publication 66* (ICRP, 1994). Type F, Type M, and Type S represent, respectively, fast, medium, and slow rates of absorption of material inhaled in particulate form. Separate risk coefficients are calculated for ingestion of radionuclides in tap water and ingestion of radionuclides in food. Risk coefficients for external exposures are given for three scenarios, including submersion in contaminated air, exposure from contamination on the ground surface, and external exposure from soil contaminated to an infinite depth. The risk coefficients are derived using a hypothetical (stationary) population defined by U.S. cancer and total mortality statistics for a fixed time period (1989-1991). Based on the current U.S. population, risk coefficients might be refined by applying a scaling factor of 1.1 (mortality) and 1.14 (morbidity) to reflect differences in risk associated with the age distribution for hypothetical 2020 population vs. the stationary population used to derive the risk coefficients published in FGR 13 (US EPA, 1999).

In the FGR report, a risk coefficient, *r,* is specific to the radionuclide, the environmental medium, and the mode of exposure through that medium. The risk coefficients, when multiplied by activity intake (for internal exposures) or activity concentration (integrated over time for external exposures), provide estimates of the average probability of death or the development of a radiogenic cancer for the U.S. population (US EPA, 1999). For a given exposure scenario, the computation of lifetime cancer risk, *R*, associated with intake of, or external exposure to, a given radionuclide involves multiplication of the applicable risk coefficient *r* by the *per capita* activity intake *I* or external exposure *X*.

$$R = r \times I \tag{3.51}$$

$$R = r \times X \tag{3.52}$$

In Eq (3.51) and Eq(3.52), R is the average probability of radiogenic cancer incidence or death for a population, r is the cancer risk coefficient, and I (*Bq)*is the activity inhaled or ingested *per capita* and X is the time-integrated activity concentration of the radionuclide in air ($m^3Bq^{-1}s^{-1}$), on the ground surface ($m^2Bq^{-1}s^{-1}$), or within the soil ($kg\ Bq^{-1}s^{-1}$).

The risk coefficients can be used to approximate (1) cancer probabilities associated with a chronic lifelong exposure to a constant concentration of a radionuclide in the environmental medium, and (2) the average probability for members of a population acutely exposed to the radionuclide. Thus , from Eq(3.51), the number of individuals that would be expected to develop cancer, for example, from a lifelong exposure to a radionuclide at constant concentration in food, is $NR = N(r \times I)$. The inhaled ($Bq\ m^{-3}$), ingested ($Bq\ L^{-1}\ or\ Bq\ kcal^{-1}$), and the ground surface deposited ($m^2Bq^{-1}s^{-1}$) radionuclide concentration values are calculated from the HOTSPOT effective dose equivalent outputs. The assessment uses age and gender specific usage rates for tap water, food intake, and the average breathing rate of a reference man listed in the *FGR 13* report (U.S EPA, 1999).

3.11 Relative cancer risk and probability of causation

The term relative risk (RR) is used in several ways in epidemiologic studies. In general RR is the ratio of the risk of disease or death among the exposed population to the risk of disease or death among the unexposed. Excess relative risk (ERR) is the relative risk minus 1.0. Absolute risk is the simple rate of disease among a population. Absolute risk has the units of the rates being compared. Excess absolute risk (EAR) is the difference between two absolute risks. In modeling the relation between radiation exposure and disease, either the ERR or the EAR may be used. The present risk index study, models RR as a linear function of dose (BEIR, 2006; BEIR, 1990)

$$RR = 1 + (\alpha_1 D) if\ e \leq 10, \tag{3.53}$$

$$RR = 1 + (\alpha_1 D)\exp\big(\beta_1(e - 10)\big)\ if\ e > 10 \tag{3.54}$$

where *e* is age at exposure, *t* is time since exposure, and $\alpha_1 = 1.221\ Sv^{-1}$, $\beta_1 = -0.0464$, and D is the dose in *Gy.* The linear RR model has been used extensively in radiation epidemiology, including the A-bomb survivors. The model has served as the basis of cancer risk estimation by

BEIR committees and by the UNSCAR committee (NRC, 1999; UNSCEAR, 2000). The linear model has been chosen because it is supported by radiobiological models and because it fits the data from most historical studies.

Leukemia was the first cancer to be linked with radiation exposure in A-bomb survivors and has the highest relative risk of any cancer. Western populations develop a cancer at some time in their lives, and approximately three-quarters of these cancers prove fatal (Wakeford et al., 1998). Therefore, a substantial number of cases of malignant disease would be expected to occur in large populations irradiated at low levels, but relatively few of these cancers would be attributable to this enhanced exposure to radiation. It is difficult to distinguish radiation -induced cancer from a cancer arising from some other cause, and so this small number of extra cases cannot be identified individually. The concept of probability of causation has been developed in an attempt to identify those cases most likely to have been caused by exposure to radiation.

Probability of causation

The excess relative risk (ERR) is the proportional increase in the rate of the disease among those exposed, and therefore $ERR = RR - 1$. As an example, a relative risk (RR) of 2 ($ERR = 1$) implies that, under the assumption of a direct casual relationship, the exposure has doubled the risk of the disease-as many cases have been caused by the exposure as by background factors. The attributable fraction (AF) in the exposed group is the proportion of all cases of the disease that would not have occurred in the absence of the exposure, given that the exposure is a cause of the disease, so that at some time *t* after exposure,

$$AF = \frac{RR-1}{RR} = \frac{ERR}{RR}, \qquad (3.55)$$

and therefore when $RR = 2, AF = \frac{1}{2}$

The probability of causation (PC) or, more exactly, the assigned share (AS) is an extension of the concept of attributable fraction which assigns a conditional probability to an individual case of a disease having been caused by a particular prior exposure, using the experience of exposed populations to determine an appropriate relative risk,

$$PC(=AS) = \frac{RR-1}{RR} = \frac{ERR}{RR}, \qquad (3.56)$$

so that if the individual circumstances of exposure are such that, if applied to a suitable population, they would produce a $RR = 2$, then $PC = 50\%$ for each case of the disease so exposed. The fundamental assumption underlying the PC calculation is that the experience of an exposed population can be properly applied to an individual from that, or another, population.

Radiation risk has been intensely studied, although, to date, the knowledge is far from sufficient to a fully description of the variation of risk with time and age. For solid cancers, even if radiation increases the risk, the doses experienced are far from those needed to increase the risk significantly above the spontaneous range. The *PC* calculation concerning solid cancer is an option for high dose rates, as the solid tumor model is an excess absolute risk model. The leukemia model is an excess absolute risk model and would require the derivation of an appropriate background leukemia risk in order to determine the relative risk and hence a *PC*. Time dependent excess relative risk models have been derived separately for leukemia, respiratory cancer, female breast cancer and other cancers. These models adopt a dose response which is linear-quadratic for leukemia and linear for solid tumors. For example, the leukemia risk model is:

$$ERR = \alpha(d + \theta d^2)exp\beta, \qquad (3.57)$$

where α and θ re constants; β depends on two categories of age at exposure and, *d* is the equivalent dose to the red bone marrow in *Sv*. Using the BEIR V leukemia model, $\alpha = 0.243$, $\theta = 1.115$ and $\beta = 4.885$. For leukemia, high relative risks may take place even at low doses.

The relative risks and the probability of causation as a function of age for the dose values derived from TEDE are calculated as part of the PFRI model. Through the adaptation of BEIR V, RR and PC calculations, general form of the dependence of risk on dose and risk modifying factors are obtained.

3.12 Decontamination

RDDs are unlikely to result in large immediate health effects beyond those caused by explosive blast, although there may be some long-term effects to more exposed individuals. However, depending on the radionuclide involved, the economic consequences could be considerable. If the radionuclide is difficult to remove from surfaces, as some are the contaminated area could be off limits for months or even years. This would result in businesses within those areas being effectively shuttered and residents being relocated semi-permanently or permanently, while costly decontamination effort are undertaken. Internationally, there have been a few events that have caused widespread contamination. At Chernobyl and Fukushima, cleanup of the areas is still ongoing and has been a considerable struggle, albeit those events are larger in area and more contaminated than would be expected from an RDD incident. In Goiania, where a relatively small amount of radioactivity was spread by human action, 85 houses were contaminated, and 45 public places and 50 vehicles required decontamination. Seven of the houses were demolished because decontamination was not feasible (Bland & Potter, 2018).

The Department of Homeland Security in 2006 published their Protective Action Guides for Radiological Dispersal Device and Improvised Nuclear Device Incidents (U.S. DHS, 2006) which stated:

"Because of the broad range of potential impacts that may occur from RDDs and INDs ranging, for example, from light contamination of a street or building, to widespread destruction of a major metropolitan area, a pre-established numeric guideline was not recommended as best serving the needs of decision makers in the late phase. Rather, a site-specific process is recommended for determining the societal objectives for expected land uses and the options and approaches available to address RDD or IND contamination."

While this philosophy is understandable, a seemingly small decrease in the radiological limit standard for decontamination limits can result in a vastly more expensive and time-consuming decontamination. If this philosophy is retained, it is important to understand the ramifications of cleanup criteria for use in decision-making, but it may be preferable to prepare a technically- based general process and recommendations that could be somewhat tailored to the specific event. At this time, the International Commission on Radiological Protection (ICRP) recommends a residual radiation dose to residents over the long term of 1 $mSv\ yr^{-1}$, the National Council on Radiation Protection and Measurements (NCRP) recommends $0.25\ mSv\ yr^{-1}$, while EPA permits only $0.15\ mSv\ yr^{-1}$. Since there is no single US standard for post cleanup radiation levels, it is difficult to estimate the costs that would be directly associated with decontamination. The PFRI model in the present study uses a decontamination limit of 1 $mSv\ yr^{-1}$ to predict the length of closures. Few studies have analyzed scenarios, ranging from short (15 days) to long (1 year) time frames (Rosoff & von Winterfeldt, 2007). This model applies Eq (3.58) to calculate the time required for the dose rate to return to an acceptable level for all three radionuclides (^{60}Co, ^{137}Cs, ^{192}Ir).

$$\dot{D}(t) = \dot{D}(1)t^{-1.2} \qquad (3.58)$$

where,

$\dot{D}(1)$ is the dose rate at time of the explosion, and

$\dot{D}(t)$ is the desirable background dose rate ($0.02\ mSv\ hr^{-1}$) and

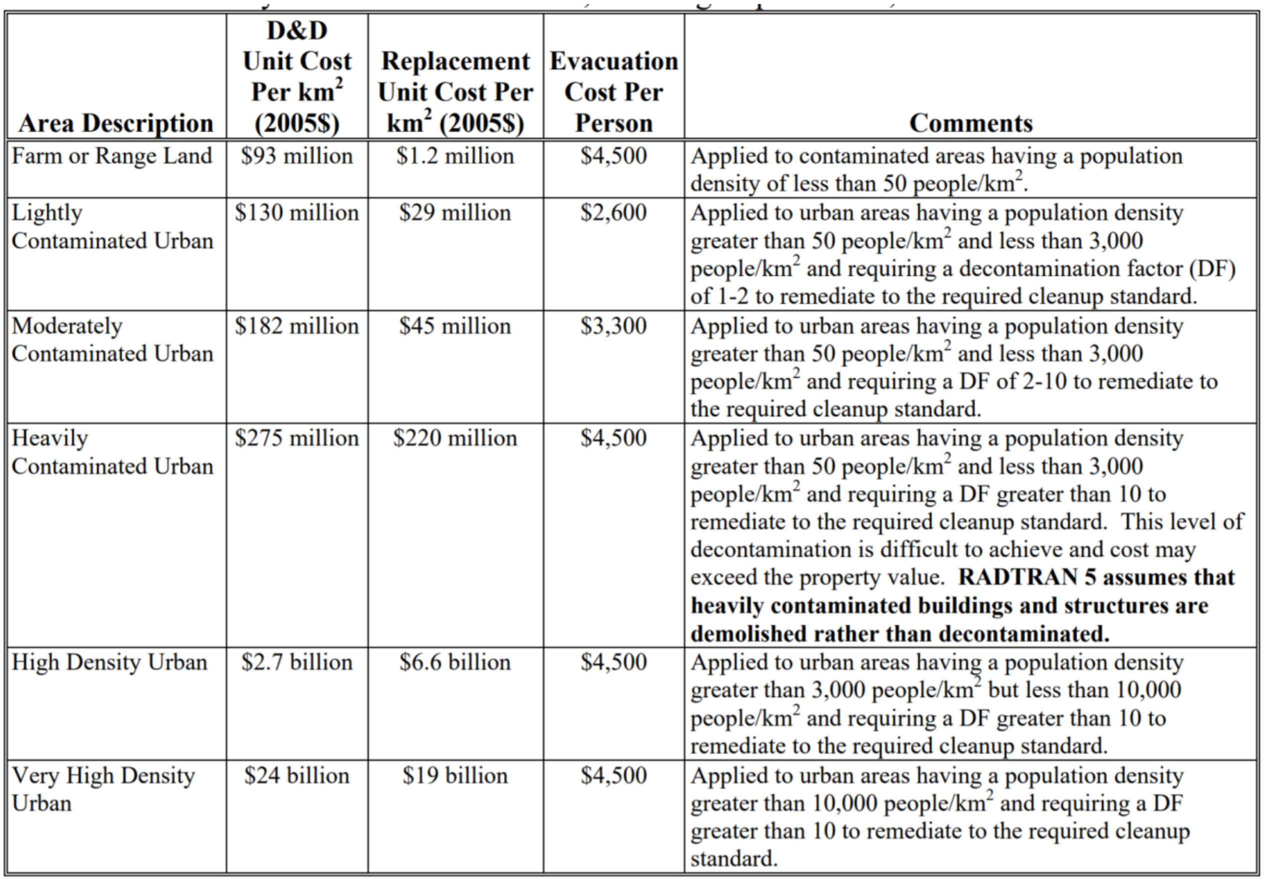
t is the time required for decontamination.

The cost of cleanup and restoration of buildings and land is dependent on the surface area requiring decontamination or the demolition and replacement of contaminated structures. The approach taken in this study is based on Reichmuth et al (2005) methodology of developing a unit cost factor ($\$\ km^{-2}$) for the cleanup of areas having different levels of population density; population density being used as a surrogate for economic activity.

Regardless of how small the radioactive device, all areas that may have received some radioactive material will have to be evacuated and closed off for monitoring and decontamination. The streets in the affected area will require decontamination, as will the exteriors of buildings. Depending upon the location of air intakes and open windows, interiors may also require treatment. Decontamination and focused cleanup techniques can range from simple actions such as the scrubbing and flushing of surfaces with uncontaminated water to the removal and disposal of soil and contaminated debris. Chemical removal of contamination from buildings would prove useful as well. It is possible that a sacrificial layer of a “sticky” substance, something like a transparent paint, could be applied to the building before an RDD incident and stripped off afterward. Nevertheless, under present regulations and applicable laws, any building that cannot be decontaminated so that the dose rate from residual radioactive debris from any radiation accident or incident is below the limits set by competent regulatory authorities, may not be occupied. Such a structure would have to abandoned in place and fenced off, or razed and removed, with all materials going to low-level radioactive waste disposal site. The replacement cost is also estimated using Reichmuth's figure of \$6.6 billion per square kilometer.

The cost of cleanup will be highly dependent on the aerial extent f cleanup, which, in turn, is highly dependent on the level of cleanup required. The cost of cleanup of any given area will be dependent on the relative level of economic development or financial investment that has been made in the area of concern. Reichmuth (2005) in her paper derived the unit cost to cleanup and replace and/or rebuild destroyed property using RADTRAN 5 (Sandia.gov/risk/radtran) companion economic model and the FRBYN 9/11 study (Bram et al., 2002). RADTRAN 5's companion economic model includes estimated unit costs ($\$ \, km^{-2}$) for: emergency actions (e.g., applying fixatives) following the event; access control (e.g., guards) to prevent unauthorized access to the contaminated areas; radiological characterization; decontamination/demolition operations; and disposal of radiologically contaminated waste. These elements were summed together to obtain the total cost of cleanup and site restoration. RADTRAN 5 varies these costs depending on whether the area is an urban area that is lightly contaminated, moderately contaminated, or heavily contaminated or whether the area is farm or range land. The unit costs from the economic model, assuming offsite disposal of radioactive waste, are summarized in Table 3.9.

Table 3. 9 Summary of unit costs for D&D, building replacement, and evacuation valuation (Reichmuth et al., 2005)



Area Description	D&D Unit Cost Per km^2 (2005$)	Replacement Unit Cost Per km^2 (2005$)	Evacuation Cost Per Person	Comments
Farm or Range Land	$93 million	$1.2 million	$4,500	Applied to contaminated areas having a population density of less than 50 people/km^2.
Lightly Contaminated Urban	$130 million	$29 million	$2,600	Applied to urban areas having a population density greater than 50 people/km^2 and less than 3,000 people/km^2 and requiring a decontamination factor (DF) of 1-2 to remediate to the required cleanup standard.
Moderately Contaminated Urban	$182 million	$45 million	$3,300	Applied to urban areas having a population density greater than 50 people/km^2 and less than 3,000 people/km^2 and requiring a DF of 2-10 to remediate to the required cleanup standard.
Heavily Contaminated Urban	$275 million	$220 million	$4,500	Applied to urban areas having a population density greater than 50 people/km^2 and less than 3,000 people/km^2 and requiring a DF greater than 10 to remediate to the required cleanup standard. This level of decontamination is difficult to achieve and cost may exceed the property value. **RADTRAN 5 assumes that heavily contaminated buildings and structures are demolished rather than decontaminated.**
High Density Urban	$2.7 billion	$6.6 billion	$4,500	Applied to urban areas having a population density greater than 3,000 people/km^2 but less than 10,000 people/km^2 and requiring a DF greater than 10 to remediate to the required cleanup standard.
Very High Density Urban	$24 billion	$19 billion	$4,500	Applied to urban areas having a population density greater than 10,000 people/km^2 and requiring a DF greater than 10 to remediate to the required cleanup standard.

In order to calculate the area that would need to be deconned and the replaced (km^2), the PFRI model uses Table 3.8 (TEDE) dose contour values to demarcate an orderly progression from low exposure to high exposure, especially near the blast area. It is likely that there will be multiple "hot" spots, which may result in higher radiation fields within areas that generally have lower radiation levels. The opposite may also occur since the deposition of the radioactive material is likely to be heterogenous. The gaussian plume simulated by the HOTSPOT code identifies an inner ellipse, middle ellipse, and outer ellipse covering an area exposed to 1 *Sv (100 rem), 0.05 Sv (5 rem),* and 0.01 *Sv (1 rem)* respectively. The area corresponding to the inner ellipse is recognized as an area that would have significant level of ground deposition and would require rigorous decontamination. The area that would require replacement of buildings is considered to be within a zone of 0.5 *km*.

Guidance on intervention levels for the protection of the public in the event of a nuclear or radiological incident or accident has been published by the ICRP and the IAEA, and these reports are compatible. Evacuation s the most disruptive of protective measures in a radiological accident, and decisions on whether to evacuate must be taken in the light of the specific circumstances prevailing. It is mentioned in the two reports that evacuation would not normally be contemplated at dose levels below $50\ mSv\ yr^{-1}$, and that it would almost certainly be implemented at dose levels above $500\ mSv\ yr^{-1}$. The PFRI model chooses the inner ellipse with a 1 *Sv* dose as the projected evacuation zone. This period of mandatory evacuation resulting from contamination or uninhabitable residential zones is considered equivalent to the decontamination time frame, which could be several days, many weeks or even months. The cost to evacuate and relocate the population living within the contaminated area uses the unit cost factor presented in Table 3.9. The cost is assumed to depend on the level of contamination; at higher contamination levels, the population is denied access for longer periods of time.

3.13 Cost benefit analysis (CBA) and value of statistical life (VSL)

Public policies and private sector investment proposals are often evaluated using Cost-Benefit Analysis (CBA) or Cost-Effectiveness Analysis (CEA), and these methodologies are also appropriate for evaluating public or private sector planning to manage terrorism risk (Boardman, 2011). Hausken (2018) uses the CBA methodology to model terrorists' choice of attack plans; costs to the defender resulting from a successful attack are evaluated by the terrorists' multi-objective utility function to assign benefits to the terrorist, and the costs to the terrorists include the logistics expenses of a successful attack and the costs of consequences of a failed attack such as terrorist casualties or loss of the terrorists' prestige.

Eckstein (1958) defines the benefits, B_t, and costs, C_t, resulting from the outcome of an event evaluated by CBA: benefits are the money value of the goods or positive externalities resulting from the outcome, and costs are the money value of the goods (typically production inputs) used up by the outcome or the negative externalities resulting from the outcome. The benefits or costs are measurable by consumers' willingness to pay for goods, which is usually expressed by market prices, and this willingness to pay may be estimated by other methods for goods that lack market prices (Eckstein, 1958). The CBA decision criterion would seek to maximize the Net Present Value (NPV) to select a single project or would seek to maximize the benefit-cost ratio, $\frac{B_t}{C_t}$, for selecting a group of projects subject to a budget constraint. In CBA, NPV is given by Eq (3.59)

$$NPV = \sum_t \frac{B_t - C_t}{(1+r)^t} \tag{3.59}$$

where r is some discount rate used for project selection, and t is time (Boardman, 2006). In many decision contexts where CBA is applied, e.g., approval of infrastructure investments with large environmental externalities, maximizing NPV has the effect of maximizing a social welfare utility function representing the aggregate utility of all community stakeholders for a decision (Boardman, 2006). Best practices under CBA for estimating the NPV of the costs of loss of life and economic consequences attributable to an RDD attack are used in the PFRI.

CEA bases decisions on a cost-effectiveness ratio where the numerator is some non-monetary measure of the outcome of a decision, e.g., reduction in the incidence of disease, and the denominator is the money value of production inputs necessary to realize the outcome of the decision (Edejer, 2003). Multiple cost-effectiveness ratios corresponding to various performance metrics of a system can be used to develop appropriate CEA decision criteria for particular applications of CEA.

The Value of Statistical Life (VSL) is an estimate of society's marginal willingness to pay to reduce the risk of loss of life. Loss of life cost estimates resulting from multiplying the estimated fatalities of an RDD attack by an appropriate VSL are compatible with CBA. Under CEA, the leading concept for measuring loss of life is Quality of Life Years (QOLY), a non-monetary metric that reflects the effects of disease or other factors on reducing quality of life. QOLY is not used in this current study.

Aldy & Viscusi, (2003) use the hedonic wage method to obtain VSL, where the marginal willingness to pay to avoid a fatality is the amount of compensation a wage earner would sacrifice to maintain constant utility while accepting an arbitrarily small decrease in their probability of workplace fatality:

$$Z(w,p) = (1-p)u_l(w) + pu_d(w) \tag{3.60}$$

where,

Z is the expected utility of the wage earner in the face of a risk of fatality with a known probability distribution.

p is the probability of death.

w is the market wage.

u_l is the wage earner's utility function when they are alive, and

u_d is the wage earner's utility when they die due to a workplace fatality.

Assuming the utility functions are twice differentiable, $u_l > u_d, u_l' > u_d' \geq 0, u_l'' \leq 0, u_d'' \leq 0$, for a decrease in p to p', the willingness to pay (WTP) to lower the risk of workplace fatality is obtained by solving the Eq (3.61)

$$Z((w - WTP), p') \ = \ Z(w, p) \qquad (3.61)$$

Thus, the marginal rate of substitution between the wage and risk of death, VSL, is obtained from the derivative $\frac{dw}{dp}$, given in Eq (3.62)

$$VSL = \ \frac{dw}{dp} = \frac{u_l(w) - u_d(w)}{(1-p)u_l'(w) + pu_d'(w)} \qquad (3.62)$$

Willingness to pay is not the only estimator available for the cost of loss of life consequences. The human capital approach uses economic measures of loss of life consequences such as lost lifetime expected income or foregone contribution to GDP (OECD, 2010). The Value of Statistical Life Years (VSLY) may be computed by using a methodology consistent with the human capital approach or by using willingness to pay per life year saved.

VSL estimated by the willingness to pay approach is the most prevalent in the literature on statistical methods for the valuation of loss of life consequences (OECD, 2010), and a comparison of VSL with VSLY estimated by the human capital approach shows that VSL is the most appropriate method for modeling the loss of life consequences of an RDD attack in the PFRI. VSL is the amount society would be willing to pay to prevent a single death (without the identity of the person who would die being known), so VSL gives the economic value of a human life regardless of its duration or quality. By contrast, VSLY gives the economic value of continuing a human life for an additional year, and VSLY is convenient for calculating the NPV of a group of human lives with a known age distribution and life expectancy.

According to Sunstein (2003), VSLY is more accurate than VSL for estimating the cost of loss of life consequences because VSLY eliminates the potential overstatement of loss of life costs resulting from VSL's failure to take into account the age distribution of the lives lost, and therefore VSLY should supplant VSL as the dominant paradigm for estimating loss of life consequences. Bram et al. (2002) use the VSLY approach to estimate the cost of the loss of life consequences of the September 11, 2001 attacks on New York City, computing the NPV of foregone lifetime expected earnings for the group of about 3,000 deceased victims. Yet in (Aldy & Viscusi, 2008), adjusting for the availability of consumer credit to smooth the level of consumption across a lifetime and the existence of age and cohort effects on lifetime expected income shows that VSL and VSLY both follow an inverted U-shaped curve, meaning that middle age workers had the highest VSLs and young or old workers had roughly equal VSLs. Sunstein (2003) argues that the statistical value of life for the young should exceed that of the old in certain contexts, but he concedes that this view is disputed on ethical grounds.

Despite VSLY's advantages and validity as an estimator of the cost of loss of life consequences, VSL is the better methodology for estimating the cost of loss of life consequences in RDD scenarios for four reasons. First, VSL is the most widely used and accepted methodology in the social sciences and public policy making for estimating the cost of loss of life consequences (OECD, 2010). Second, VSL is simpler to implement because it requires less information than VSLY. Third, VSL should not be expected to be less accurate than VSLY due to a failure to adjust the VSL to a known age distribution. RDD attacks effect a large enough random sample of the population near the blast site that the age distribution of the victims is reasonably approximated by the total population age distribution that is assumed in the willingness to pay studies used to estimate the VSL. Fourth, the problem of potentially overstating the economic value of lives lost that may exist for VSL in some applications is unlikely to be relevant to an RDD attack due to research showing that willingness to pay to avoid deaths from terrorism is about twice the level of willingness to pay to avoid deaths from normal causes that are assumed in studies that provide VSL values (Viscusi, 2009).

Hammitt and Triech (2007) provide three explanations for the existence of a premium on VSL for deaths caused by terrorism: 1) the identifiable-victim effect can increase society's willingness to pay to prevent death when a victim group has homogenous identifying characteristics; 2) politically charged victim groups such as terrorism victims are likely to have a higher than average VSL; and 3) predictions of future terrorist attacks invoke a "rule of rescue" or duty to prevent foreseeable deaths adding a terrorism premium to the normal level of VSL. VSL is likely to somewhat understate the true cost of the loss of life consequences of an RDD attack because VSL does not reflect society's additional willingness to pay to avoid deaths from terrorism. However, it is likely that VSLY would understate loss of life consequences by a greater amount than VSL, particularly if the victims of the RDD attack happen to have a relatively old age distribution.

3.14 Income and Wealth effects

An RDD attack would potentially shut down a large metropolitan area and shock entire regional economies, and some terrorists may prefer inflicting economic damage. Giesceke, et al. (2012) use a regional Computable General Equilibrium (CGE) model to forecast the economic consequences of an RDD attack on downtown Los Angeles, California. CGE models evolved from the Leontief input-output model, a system of linear equations that computes the total output of an economy as the sum of the inputs supplied by the interdependent sectors of the economy to each other and the outputs supplied by each sector to consumers (Mitra-Kahn, 2008). Regional CGE models can forecast the changes in economic activity for a region experiencing economic shocks such as an RDD attack. Giesecke, et al. (2012) forecast direct and indirect economic effects of the RDD attack over both the short-run and long-run timeframes by summing the economic consequences from injuries, deaths, capital damage, business interruption, decreased investment (due to an increase in the required rate of return), an increase in the cost of labor (due to perceived radiological health risks to workers) and a decrease in demand for the region's products (due to radiological contamination stigma).

The PFRI regional economic consequence model is streamlined in comparison to the regional CGE model of Giesecke et al (2012). Rather than adopt a complex input-output and behavioral model of dependencies between sectors of the economy and consumer demand, the PFRI models the geographic distribution of the direct physical effects of an RDD attack on the regional economy.

The following direct economic consequences of an RDD attack are considered in the PFRI over a short-run timeframe: loss of human capital, decontamination cost, evacuation cost, business interruption cost, lost personal income, and impaired real estate value. The CBA methodology is used in the cost accounting for these economic consequences, and the PFRI's economic loss severity value (C_{EL}) is a function of them.

Loss of human capital is the sum of the costs of loss of life consequences, injuries, and permanent disabilities. The cost of the loss of life consequence is computed by multiplying the VSL by the estimated number of fatalities from the RDD attack.

The PFRI includes a blast model and a radiological dispersal plume model, and these models are predictive of the total numbers of deaths and injuries and some of the resulting pathologies. C_{LL} models some broad types of injuries: injuries from fragmentation effects, injuries from blast overpressure, and a few possible cancers, but this model does not give a highly detailed breakdown of injury typology and severity, e.g., the proportion of fragmentation injuries resulting in life-threatening internal organ damage. The PFRI blast and plume models in theC_{LL} function are predictive of the exact quantities of deaths and injuries that would result from a real instance of an attack scenario, but the complexity of estimating the economic costs of the attack casualties requires a distribution of injury type, injury severity, permanent disabilities, and average medical costs for each class of casualties. Statistics on casualty type, severity, and medical cost of the April 19, 1995 Oklahoma City bombing are available. These statistics are suitable for developing structural engineering models for the purpose of designing public buildings that would suffer fewer casualties in the event of a terrorist bombing, so they were used in the PFRI to estimate the injury pattern and healthcare cost for bombing victims (Shariat et al., 1998).

The structural plans of facilities greatly impact the pattern of casualties that would result from an RDD attack. Facilities vary in their vulnerability to progressive structural collapses triggered by bomb blasts that can significantly increase the number and severity of casualties (U.S. DoD, 2009). The potential fragmentation effects of particular building materials and the occupancy load are among other structural design variables that significantly impact the pattern of casualties from a bomb blast. The new PFRI methodology does not currently incorporate a structural model of buildings, but this could be a future direction of research. Facilities using the PFRI would be able to substitute alternate blast models into C_{LL} and C_{EL} that consider private structural information about the facility in their internal security self-assessments. Modeling the economic costs of human casualties from RDD scenarios on the 1995 Oklahoma City bombing, as done in the current version of the PFRI, is an option for facilities using the PFRI methodology.

The cost to human capital from long-term disability is computed using a lifetime expected income model for workers in Marion County, with adjustments made for the age distribution and workforce participation of the local population.

Assumptions about the decontamination response to an RDD attack largely determine the parameters for modeling the local economic impacts. The direct economic consequences are geographically bounded by the perimeter of the area whose economy is directly impacted by physical effects of the attack, and the they are temporally bounded by the time required to complete the decontamination process. The PFRI's economic model is restricted to measurable economic variables and first order economic consequences of an RDD attack that would certainly occur.

There are several advantages to PFRI's economic model as compared to some of the more ambitious economic models of RDD terrorism that account for second order effects and the full complexity of regional interdependencies within a global economy. The PFRI's economic model gives a lower bound on the potential economic losses that is known with a high degree of confidence, and the information required to implement the PFRI economic model is readily available to its potential users at the level of healthcare facility administration. C_{EL} is an input to the terrorists' utility function in the PFRI, so it may be unrealistic to include state of the art CGE models as an input to the terrorists' decision process. Terrorists are intelligent and rational adversaries, so it is plausible that the same C_{EL} model found to be useful for the healthcare security administrators would be useful for the terrorists. And sophisticated macroeconomic forecasting is just as impracticable for the terrorists as it is for the healthcare facility staff. Moreover, complex macroeconomic models of RDD terrorism are of interest to the advancement of basic science, but they may fail as applied tools. Macroeconomic forecasting is notoriously unreliable, and scholars in the field warn practitioners against overreliance on the currently available macroeconomic theories.

The decontamination cost and replacement cost are modeled by multiplying the surface area that would be decontaminated or subject to building replacement activities by per square kilometer cost rates for each of these economic consequences found by Reichmuth, et al. (2005). Reliable estimates of decontamination and replacement cost rates were incorporated in Sandia Labs' RADTRAN-5 model, and these cost rates vary with the population density of the zone being decontaminated.

Evacuation cost is estimated by multiplying the total population to be evacuated by the evacuation cost per evacuee per day and the number of days of evacuation (which is equal to the decontamination period). The total population to be evacuated is determined by multiplying the per square kilometer population density by the area of the evacuation zone. The evacuee cost per evacuee per day is estimated by the sum of per evacuee roundtrip transportation cost, per evacuee per day shelter cost, and per evacuee per day cost of living. As with the estimation of business interruption cost (explained below), the limiting factors on total evacuation cost are the size of the evacuation zone and the decontamination time.

Business interruption cost is estimated by computing the amount of business revenue lost for firms in the contaminated zone during the entire decontamination period. The amount of business revenue lost is found by multiplying the average business revenue per day of the firms in the evacuation zone by the decontamination time. Although business interruption insurance would potentially provide economic relief to the affected businesses, the CBA methodology considers the depletion of insurance capital resulting from the RDD attack a cost to society (Boardman, 2011). CBA assesses the impacts of events from a whole-of-society standpoint. Insurance spreads the financial risk of RDD attack among a larger pool of policy holders than the particular insured persons or entities affected by the attack, but insurance does not in any way reduce the net cost to society of the attack. Costs to society in the form of increased insurance premiums, lower insurance company dividend payouts, and a cascade of other adverse economic consequences occur to offset the benefits of insurance claims to the insured.

Lost household income is estimated by using the lifetime expected income model for the population of Marion County to compute the amount of lost household income under the assumption that all workers in the contaminated zone would remain unemployed for the entire decontamination period. Although unemployment insurance would provide economic relief to the unemployed workers, the

CBA methodology considers the cost of depleting the unemployment insurance fund above normal levels for the business cycle as an additional cost to society of the RDD attack.

The impairment to real estate is computed by multiplying the total value of real estate in the contaminated zone by a 15% RDD real estate impairment rate found by Giesecke et al. (2011) in a review of the literature on the prior distribution of impairments to real estate from radiological or other comparable contamination incidents. Although terrorism clauses in property insurance policies could provide some relief to property owners, the CBA methodology considers the depletion of property insurance capital due to an RDD attack as a cost to society.

3.15 Loss of life and Economic loss consequence severity variable

The severity of the life loss consequence (C_{LL}) variable is calculated as a function of the casualties from the blast, fatalities from acute radiation exposure, and cancer risk caused by airborne dispersal of radioactive material (Eq. (3.63)).

$$C_{LL} = [\left(\frac{D_{BE}+D_{cancer}+D_{ARS}}{Population\ density}\right) + \left(\frac{I_{BE}+I_{cancer}+I_{ARS}}{Population\ density}\right)] \qquad (3.63)$$

where

C_{LL} is the life loss consequence severity variable

D_{BE} are the fatalities from the blast effects

D_{cancer} are the fatalities in future from relative cancer risk

D_{ARS} are the fatalities from acute radiation syndrome (ARS)

I_{BE} is the morbidity from the blast effects.

I_{cancer} is the morbidity from radiation induced cancer; and

I_{ARS} is the morbidity from deterministic effects

The Economic Loss consequence severity value (C_{EL}) is comprised of human capital loss, decontamination cost, evacuation cost, business interruption cost, lost household income and impaired real estate value.

Values of each variable in the economic loss model are computed for before and after the RDD attack. Coefficients denoted by B_i and A_i for before and after the RDD incident, respectively, are obtained by dividing each economic variable entry (E_{ij}) by its corresponding column total (E_j).

$$A_e or\ B_e = \frac{E_{es}}{\sum E_s} \tag{3.64}$$

where, e is the index of economic variables and s is the index of the states of the economy (i.e., before and after).

A linear regression of B_e on A_e is used to obtain the regression coefficient Y. The regression coefficient reflects the change in the economic variables before and after the RDD attack. The economic consequence loss, C_{EL}, is calculated using Eq. (3.65).

$$C_{EL} = 1/\sqrt{(I - D_E)^2 Y} \tag{3.65}$$

where

D_E is the difference between the two vector components A_e and B_e ; and

Y is the linear regression coefficient.

The economic consequence loss value (C_{EL}) represents the severity of the monetary loss directly or indirectly resulting from an executed RDD threat event.

The net consequence loss (C_{net}) is calculated by taking the average of $C_{EL}\ and\ C_{LL}$ (Eq. (3.66)).

$$C_{net} = \frac{(C_{EL} + C_{LL})}{2} \tag{3.66}$$

3.16 The PFRI

The PFRI is mathematically represented as the product of the maximum expected utility among the threat groups, the sum of geographic vulnerability and cultural vulnerability, and net consequences, as shown in Eq. (3.67). The exponential form of the equation allows the PFRI to be read on a scale from one to ten.

$$PFRI = e^{[\max\left(EU[X_{ij}]\times\left(V+(1-\min(Z_{gen},Z_{tech},Z_{sub}))\right)\right)\times C_{net}]} \tag{3.67}$$

The maximum expected utility is used to highlight the threat group that provides the highest risk to the asset. The minimum value of the nuclear security culture survey is used because the overall score masks the weaknesses that contribute most to vulnerability. The PFRI quantifies facility radiological risk, using a scale of 1-10 with a score of 1 meaning “very low risk” and a score of 10 meaning “very high risk”.

CHAPTER 4. NUMERICAL APPLICATION AND ILLUSTRATION OF THE MODEL

4.1 Hypothetical facility design

The hypothetical facility presented in this study applies and illustrates the risk analysis framework. The hypothetical facility is representative of a real medical facility and is used to avoid security concerns about publishing sensitive data. The facility, henceforth called St. Benedict Healthcare, is located in Marion county in the state of Indiana, USA.

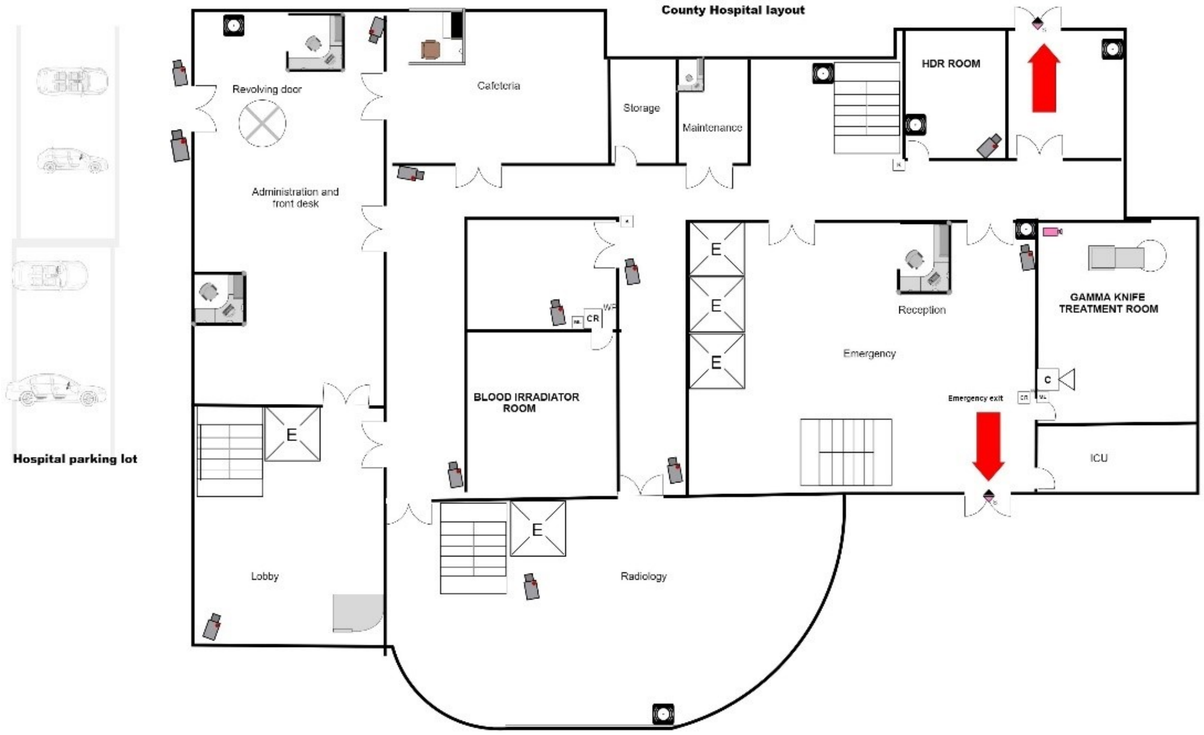


Figure 4.1 Facility layout of St. Benedict Healthcare.

St. Benedict Healthcare, shown in Fig. 4.1 has one main entrance and consists of three assets: Gamma Knife ® (^{60}Co), Blood irradiator *(^{137}Cs)* and the HDR brachytherapy device (^{192}Ir). The Gamma Knife ® instrument typically contains 201 ^{60}Co sources of approximately 1.1 *TBq* (30 *Ci*) each. The ^{137}Cs blood irradiator typically contains *CsCl* encapsulated sources with 44.4-

111 *TBq* (1200 *Ci* to 3000 *Ci*). The HDR brachytherapy treatment shielded lower cylinder contains 0.55 *TBq* (15 *Ci*) of ^{192}Ir seeds.

The physical protection system of St. Benedict Healthcare properly incorporates the elements of access authorization (e.g., trustworthiness and reliability determination), access control (e.g., electronic card readers, iris scanners), detection (e.g., infrared motion sensors), delay (e.g., reinforced concrete walls, reception areas) and response (e.g., guards, campus police) for protection of assets against theft of radioactive material or other malevolent human attacks.

St. Benedict Healthcare being a medical facility has no visible legal boundary, such as a fence, to warn trespassers (like NPP). The two passive, covert, line of sight sensors installed at the entrance perimeter of the facility, along with closed circuit television (CCTV) cameras and visual check security personnel, are jointly used for detection, surveillance and alarm assessment. The initial detection element is followed by two more CCTV cameras and internet protocol (IP) based video surveillance systems near the administration area and the lobby entrance. The presence of guards and doors offers a flexible and a continuous delay barrier. The administration front desk, lobby and the cafeteria introduce short impediments along the adversary path.

St. Benedict's administration access authorization program ensures that individuals who have unescorted access to category 1 or category 2 quantities of radioactive material are trustworthy and reliable and do not constitute an unreasonable risk to the public heath and safety or security of the radioactive material. As per *10 CFR 37.25(a)* St. Benedict Healthcare performs background investigation on the individual to obtain information necessary to determine if they should have unescorted access to risk-significant radioactive material or sensitive information. Such individuals could include the G2 threat group, who may require access but would not warrant unescorted access because of the infrequent need for access or the specific nature of the position.

The main door of all three asset rooms uses a personnel entry control system to authorize entry and to verify the authorization of personnel seeking entry to a controlled area. Consistent with *10 CFR 37.23*, a coded credential key card accompanied by a biometric scanner identity verifier restricts unauthorized access and offers a high level of security protection to the blood irradiator and the Gamma Knife® rooms. The HDR device being a category 2 material uses a personal identification number in combination with a key card to gain authorized access. In addition to this St. Benedict

Healthcare also makes use of intrusion detection sensors to maintain continuous monitoring and detection of unauthorized entry into the vital areas. An electromechanical sensor consisting of two components, a switch unit, and a magnetic unit, is mounted on the movable door as part of an effective intrusion detection system. An alarm is triggered when the door is opened, and the circuit is interrupted. A similar tamper mechanical contact switch recessed into the Gamma Knife® and the blood irradiator source cavity protects the source integrity by signaling an alarm upon detected meddling from an intruder. Along with the tamper alarms and surveillance cameras, a radiation monitoring system (RMS) is also integrated in the security structure to continually monitor the operational parameters in the room and measure the presence of unauthorized release of radioactive material in the surrounding environment. A video motion detection (VMD), another passive sensor, is used in the Gamma Knife and the blood irradiator room to provide continuous surveillance. Humans do not have the capability to continuously focus on a scene for extended lengths of time. VMD provides that continuous observation and alerts the monitoring station or individual to allow him or her to make the final decision on the presence of an intruder. St. Benedict Healthcare uses a twisted steel high-security chain with tamper-proof mounting bolts to secure the HDR device from theft. A duress alarm, which is an alarm that is manually activated by an individual, is carefully located close to the chained HDR device to alert the authorities of an unauthorized intrusion.

Responding to an assessed alarm is the final function of the physical protection program. The regulation at *10 CFR 37.49(d)* requires the licensee to request, without delay, an armed response from the local law enforcement agency to any unauthorized access involving an actual or attempted theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material. The response could be on-site guards or the local police. The St. Benedict Healthcare police dispatch center located 0.8 *km (*0.5 *mile*) from the hospital monitors and controls access to the buildings, monitors the surveillance cameras and responds to other security problems as needed.

4.2 Threat input

Threat input incorporates the utility of the adversary, utility of the material and the success probabilities of the attack scenarios

4.2.1 The material utility $U[mat]$

Given the attractiveness and the physical form of the three radioactive materials present in St. Benedict Healthcare facility, (^{60}Co ^{137}Cs ^{192}Ir), $U[mat]$ is evaluated using Eq (3.3) (3.4) and (3.5), presented in Table 4.1.

Table 4.1 Material utility of the assets present in St. Benedict Healthcare facility

Asset (Radionuclides)	Activity (A) (TBq)	Danger value (D) (TBq)	Mass (kg)	Physical form	$U[attractiveness]$	$U[form]$	$U[mat]$
^{60}Co	222.00	0.03	100.00	Metallic	1.00	0.95	0.95
^{137}Cs	107.00	0.10	50.00	Powdered salt	1.00	0.99	0.99
^{192}Ir	0.55	0.08	9.07	Metallic	0.89	0.95	0.85

Because of its dispersibility, penetrating radiation, source activity and the danger value, ^{137}Cs is found to have the highest material utility, $U[mat]$. ^{137}Cs in the form of $CsCl$ is soluble in water at room temperature, and if it is intentionally or accidentally removed from the container, it can readily be dispersed. The specific activity[5] of ^{137}Cs in the form of the salt is about 20 $Ci\ g^{-1}$, which is the maximum value relative to its alternate forms (e.g., glass or pollucite). ^{60}Co specific activity is 3.5 times higher than ^{137}Cs. One curie of ^{60}Co also emits nearly four times as much energy as one curie of ^{137}Cs, meaning ^{60}Co can give a higher dose to tissues than the same amount of ^{137}Cs would. The $U[mat]$ of ^{137}Cs appears to be higher than ^{60}Co to a terrorist adversary, as the selection of radioactive material depends on a combination of factors, including the source activity, sufficiently long half-life, relative attractiveness of the source, physical and chemical form of the source (i.e., dispersibility), ease of access, and the perceived consequences of the source.

4.2.2 The adversary utility $U[adv]$

With a defined set of radioactive material bundle $\{$ ^{137}Cs, ^{60}Co, $^{192}Ir\}$and their respective $U[mat]$, the next preferred course of action in the PFRI model is to identify the groups of perpetrators and

[5] The specific activity is the ratio of activity contained within a unit mass of the source.

evaluate their respective objectives. St. Benedict Healthcare analysis uses a value focused decision framework (Eq (3.6) and Eq (3.8)) to model the terrorist adversary portfolio. The adversary utility, $U[adv]$, assess how the values and beliefs of threat groups might influence the selection of an attack strategy. In profiling the terrorist adversary, some generalizations can be made on the basis on the examination of the literature on the psychology and sociology of terrorism published over the past several decades. However, one finding is that, unfortunately for profiling purposes, there does not appear to be a single terrorist personality. The personalities of terrorist adversaries may be as diverse as the personalities of people in any lawful profession. The basic profiles of the groups of perpetrators considered in this study for St. Benedict Healthcare are:

Religious fundamentalist (G1-Outsider)

Religious fundamentalist (*RF*) could be from any threat group (Table 2.2), but in this study *RF* is an outsider whose ideological motivations are linked to religious and political systems. According to the theory discussed in section 3.2.1, *RF* is on the *ideology brain*, which provides a set of beliefs that guide and justify a series of behavioral mandates and must be neither questionable nor questioned. *RF* is a young recruit of a terrorist organization who has no special skills or knowledge of radioactive material but exhibits absolute obedience to the leader of the movement. *RF* is even ready to be a martyr and engage in suicide attacks for the welfare of the terrorist group. The fundamental objective of *RF* is to cause widespread panic and disruption, creating economic warfare and propaganda through WMD terrorism.

National domestic extremist (G2-Semi-insider)

National domestic extremist (*NE*) could also belong to any threat group, but in this study, *NE* is a semi-insider who works as a third-party contractor personnel for St. Benedict Healthcare. *NE* could be an off-site maintenance personnel assigned to work on the security cameras or service the radiation devices, or it could be a mailman assigned to deliver radioactive packages to the facility. *NE* is someone like "Timothy McVeigh", who deeply distrusts the government and strongly believes in violent revolution in the U.S. leading to the overthrow of the federal government, a nuclear war, and, ultimately a race war - to attain a utopian government. *NE* displays the hallmarks of rational behavior that engages in reflective rather than impulsive decision making. *NE* strives to achieve an act of violence of tremendous strategic and symbolic importance. *NE* being a semi-insider possesses resources and capabilities to penetrate the security system. *NE's* privilege of escorted or unescorted access to the facility assists in conceptualizing and planning of the attack. *NE* is a rational actor who is motivated to overthrow the "unfair" government by inflicting some economic damage and loss of life through symbolic terrorism.

Disgruntled insider (G3-Insider)

Disgruntled insider (*DI*) could either be in G2 or in G3 threat group, and they are unhappy due to a belief that he/she was mistreated in the workplace. In this study, *DI* belongs to the threat group of insiders. *DI* seeks revenge or notoriety and is not hesitant to use their intimate knowledge of the applications, systems and authorized access privileges to harm the facility. *DI* is motivated by self-aggrandizement who wants to keep public attention low but also strives for vengeance at the same time. The fundamental objective of *DI* is to intentionally destroy and damage the facility for the sake of revenge.

Each of the fundamental objectives mentioned above for the terrorist adversaries *RF, NE and DI* are measured using attributes (X_k). The three attributes represented by X_{LL}, X_{EL}, X_{SY} are indexed by k. The initial estimate of attributes is based off the understanding of outcomes following the attacks of 9/11. Peirce's semiotic three-part (representamen-object-interpretant) triangle is used as an expressive measurement of constructing the terrorist adversary profiles by assigning swing weights to the terrorist adversaries' objectives. Table 4.2. displays the swing weights (w_{ij}), quantified on a scale of 0 to 1 and developed from Eq (3.7) and Eq (3.8), using generalized beta probability distribution functions. Swing weights rank the threat group attribute preference based on analyst's uncertainty about terrorists' value tradeoffs.

Table 4. 2 Swing weights developed for the terrorist adversary attribute ranking

Qualitative scale	EL	SY	LL
High	1.000	0.938	0.750
Med	0.938	0.750	0.438
Low	0.750	0.438	0.278

Given the motivations, a swing weight of high economic damage ($w_{EL,RF} = 1$) , high symbolism ($w_{SY,RF} = 0.938$) and moderate loss of life ($w_{LL,RF} = 0.438$) can be placed on the fundamental objective of terrorist adversary RF. Similarly, a swing weight of medium economic damage ($w_{EL,NE} = 0.938$), medium loss of life ($w_{LL,NE} = 0.438$) and high symbolism ($w_{SY,NE} = 0.938$) can be placed on the fundamental objective of terrorist adversary NE. The terrorist adversary DI, with a little interest in making a symbolic impact is placed with a low swing weight for symbolism ($w_{SY,DI} = 0.438$), a moderate swing weight for economic loss ($w_{EL,DI} = 0.938$), and a low swing weight for loss of life ($w_{LL,DI} = 0.278$).

The adversary utility for the three terrorist adversaries (*RF, DI, NE*) is calculated using Eq. (3.6) and Eq (3.8). Table 4.3 displays the $U[adv]$ for the three modeled terrorist adversaries.

Table 4.3 Terrorist adversary preference ranking and the total adversary utility

Modeled threat group	$U[X_{ED}]$	$U[X_{LL}]$	$U[X_{SY}]$	$U[adv]$
Religious fundamentalist (RF)	0.536	0.051	0.759	1.35
National domestic extremist (NE)	0.502	0.051	0.699	1.25
Disgruntled insider (DI)	0.502	0.033	0.326	0.86

The mathematical model shows that the *RF* adversary utility with a value of 1.35 presents the highest motivation of the three to carry out an RDD attack, followed by threat actors *NE* and *DI*. The numbers obtained for the multi-attribute adversary utility function for the three threat actors align well with their respective fundamental objectives. *DI* with the lowest multi-attribute utility implies a motive of self-aggrandizement than a societal loss. Appendix A lists adversary utility values for all possible combinations of terrorist adversary profiles relative to the weights on the three preference attributes.

The overall utility of each asset $U[tot]$ to the threat group equaled the product of the material input $U_i[mat]$ and adversary's utility as a function of the attributes, $U_j[adv]$ as presented in Table 4.4.

Table 4. 4 The total utility function of the three threat groups and the three assets

		$U[tot]$	
Modeled threat group	^{137}Cs	^{60}Co	^{192}Ir
Religious fundamentalist (*RF*)	2.34	1.28	1.15
National domestic extremist (*NE*)	2.25	1.19	1.07
Disgruntled insider (*DI*)	1.86	0.82	0.73

4.2.3 Probabilistic threat scenarios

A total of nine threat scenarios, three per asset are developed for St. Benedict Healthcare. Threat scenarios include the terrorist adversary attack strategy, physical protection system (PPS) elements, initiating events, probabilistic statistic methods and other aspects of pathway analysis. Probability of interruption P_I is computed using the pathway analysis model *EASI*, where the basis for evaluating the probability of ceasing the attack is based on detection, delay, response, and communication characteristics of PPS. The pathway analysis is supplemented by the components of PRA to calculate the overall success probability of theft or sabotage.

^{137}Cs Scenario I:

Scenario I identifies religious fundamentalist (RF) as the threat group of interest with the desire to sabotage the blood irradiator. The principal plotter in RF's terrorist organization has devoted a few months to familiarize itself with St. Benedict's security system, where it understands that the blood irradiator is located on the top floor of St. Benedict Healthcare and requires credential and biometric authorization to gain access. RF carefully minimizes detection through stealth and deceit and bypasses the security elements along the path. On arriving at the front door to the blood irradiator, RF changes its tactics and minimizes delay by taking an employee hostage to gain access to the vital area and plant an attack. Table 4.5 lists the sequence of actions the adversary is trying to perform to get to the source. The probability of detection P_D for each sensor encountered by an adversary is computed using Eq (3.9). The response force time was estimated to be 300 sec for St. Benedict Healthcare and was kept constant for all assets. The probability of response force arrival prior to the end of the adversary's action sequence was calculated using Eq (3.16). Since scenario I is a radiological sabotage, only the entry path is evaluated.

Table 4. 5 Pathway analysis of ^{137}Cs scenario I with G1 threat actor.

Blood irradiator Scenario I	Probability of guard communication	Response Force time in seconds	
		Mean	SD
	0.95	300	90

			Delay (seconds)	
Tasks	Task Description	P(Detection)	Mean	Standard Deviation
1	Enter Building (has weapon)	0.70	30	9
2	Walk 50 ft	0.00	10	3
3	Get in the Elevator (requires badge)	0.80	30	9
4	Walk 200 ft	0.00	10	3
5	Pass the hallway and the doors	0.85	30	9
6	Get to BI departmental door (1st barrier). Depending on the alarm system at door the detection prob changes	0.78	60	18
7	Walk to the asset room	0.00	20	6
8	Takes an hostage to get through the asset room and places his bomb on the device. Sabotage and detonate the entire device (Suicide bomber). The detection will change if the room has a duress code which will secretively send a message to monitoring center	0.82	90	27

Probability of interruption	**0.25**
Success probability of sabotage	**0.87**

A Monte Carlo simulation is run on the P_I outcome to obtain probability distribution of different outcomes occurring, thus accounting for the uncertainties in the variable. Referring from Table 3.2, the initiating event for ^{137}Cs source in this case is considered to be that the first door to the blood irradiator is accidently left propped open by an employee. As mentioned in chapter 3, it is assumed that at St. Benedict Healthcare 60 blood bags get irradiated every day, with 2 bags per irradiation cycle. An individual accesses the main door to the blood irradiator room 30 times in an entire working day (8 hours). If St. Benedict has 5 technicians with authorized privileges to access the room, then in total the main door to the blood irradiator room is accessed 150 times in an entire working day of 8 hours. In this 8-hour working day, let *B* be the *event* that the first door to the blood irradiator room is left propped open. Given that St. Benedict does not have a man trap device to detect the interlocking of the first door, the frequency that the first door is accidently left propped open is $\lambda = 3\ times\ d^{-1}$. The probability that the main door to the gamma knife, $P(B)$, is never left open $(X = 0)$ is calculated using Poisson distribution. The overall success probability of sabotage by the terrorist adversary *RF*, given the door to the blood irradiator was accidently left propped open is given by $\left(P_S = 1 - P(A)P(B)\right)$. The success probability of sabotage in scenario I is $P_S = 0.87$.

<u>*^{137}Cs Scenario II:*</u>

Scenario II describes a *^{137}Cs* source theft plot. The national domestic extremist (NE*)* is identified as the threat group acting maliciously in scenario II. NE, as noted, is a security camera maintenance contractor who is familiar with the security arrangements of St. Benedict Healthcare and has an authorized access to some areas.

Let A be the event that *^{137}Cs* source gets stolen by NE. Let B be the event that the security cameras in the room go through regular maintenance. NE plans to steal the source by minimizing suspicion, and therefore choses to attack after hours when the device is not in use and foot traffic is low. The probability that the *^{137}Cs* source is stolen by NE, given that no maintenance or repair was scheduled is given by $P(A)|P'(B)$. The probability that NE would get intercepted by the response force while stealing the source is given by P_I. NE, with their semi-insider privileges, has authorized access to get past the hallway, lobby door, and the elevator to get to the floor where the blood irradiator is located. NE based on their semi-insider privileges has been through the trustworthiness and reliability investigation (*10 CFR 37.23)* program at St. Benedict Healthcare.

NE is granted unescorted access to the facility and several other protection layers leading to the blood irradiator room, making P_D low. St. Benedict however restricts NE's access to items such as security system codes, biometric scanner, and keycards to the blood irradiator room. In the event of a scheduled maintenance or repair NE is escorted by a radiation safety officer or some other authorized personnel to access the blood irradiator room. Since the initiating event in this scenario, is referred to as the "device not in use", NE avoiding the escorted access considers waiting for that opportune time. Using deception and false maintenance work orders, NE convinces an authorized facility employee to use their credentials to gain access to the blood irradiator room after hours, when the device is no longer in use. Table 4.6 shows the sequence of tasks that NE takes to accomplish the theft. Since P_D is a product of sensing, transmission, and assessment of an alarm Eq (3.9) the detection remains low until the first sensing occurs at CDP.

Table 4. 6 Pathway analysis of ^{137}Cs scenario II with G2 threat actor.

Blood irradiator Scenario II	Probability of guard communication	Response Force time in seconds	
		Mean	SD
	0.95	300	90

			Delay (seconds)	
Tasks	Task Description	P(Detection)	Mean	Standard Deviation
1	Enter Building	0.002	20	6
2	Walk 50 ft	0.000	10	3
3	Get in the Elevator (requires badge)	0.027	20	6
4	Walk 200 ft	0.000	10	3
5	Pass the hallway and the doors	0.074	10	3
6	G2 is enters the BI departmental door (1st barrier).	0.068	60	18
7	Walk to the asset room	0.000	60	18
8	G2 is enters the asset room, foot traffic is low (after hours). G2 opens the device using its tools. The device has tamper switches which triggers alarms. Suspicion is built. No scheduled maintenance. Alarm sets off. Response alerted.	0.619	800	240
9	Escape	0.713	320	96

Probability of Interruption	**0.77**
Success probability of theft	**0.73**

`

The critical detection point (CDP) occurs at Task 8 (Table 4.6) where the adversary's remaining task time is greater than the response force time. At CDP, the intrusion from NE is detected as an alarm is triggered by the device tamper switch. The alarm is acknowledged by the dispatch center off-site, and the response force is alerted. The P_I for this scenario is calculated as 0.11 (Eq (3.16)). The probability of interruption is lower in this case than the first scenario as the first sensing (T_0) leading to an assessment occurs relatively later in the adversary sequence path. Instead of running multiple EASI analyses with different probability of detection and adversary task time, a Monte-Carlo simulation with a P_I mean and 2σ standard deviation was run to model the probability of different outcomes. The probability of interruption, P_I, is replaced by the expected value, P_{mI}, which is the mean of the estimated normally distributed probability distribution of a random sample. Thus, the probability that no theft occurs ($P'(A)$) is calculated by binomial distribution with $n = 1$ trials and $P_{mI} = 0.24$, probability of failure. The probability that no maintenance on the camera is scheduled ($P'(B)$) is calculated as a Poisson distribution, with mean $\mu = U/251$, where U is randomly generated number of days that the maintenance and repair of the security cameras are estimated to occur. The overall success probability of theft of *^{137}Cs* source in scenario II is calculated to be $1 - P'(A)P'(B) = 0.73$.

^{137}Cs Scenario III:

Scenario III assumes collusion of G2 and G3 threat group. It can be thought of as an extension to scenario II, where NE instead of relying on false work orders to get access to the blood irradiator room is assisted by an insider, DI. The pathway analysis is only performed on NE, which is similar to the adversary action sequence presented in Table 4.6. The task 8 detection probability obviously goes down with DI helping NE to bypass the tamper switch alarm recessed in the device. Insider personnel, DI (except for radiation safety officer), may not possess all the insider privileges including access to tamper sensors in the radiation monitoring system (RMS) or access to camera footage from the RMS station. In this scenario it is assumed that DI is knowledgeable about radioactive materials, dose rates and the concept of ALARA (As Low As Reasonable Achievable). Both DI and NE possess the capability to overwrite the camera footage and make efficient use of the available tools to open the blood irradiator and steal the source.

Table 4. 7 Pathway analysis of ^{137}Cs scenario III with G2 and G3 threat actors working in collusion.

Blood irradiator Scenario III	Probability of guard communication	Response Force time in seconds	
		Mean	SD
	0.95	300	90

			Delay (seconds)	
Tasks	Tasks	P(Detection)	Mean	Standard Deviation
1	G2 enters building	0.002	20	6
2	Walk 50 ft	0.000	10	3
3	Gets in the Elevator - Escorted by G3 (requires badge)	0.027	20	6
4	Walk 200 ft	0.000	10	3
5	Pass the hallway and the doors escorted by G3	0.074	10	3
6	G3 lets G2 to BI departmental door (1st barrier) so he works on the scheduled camera and door intrusion alarm system (detection will increase if a security officer stops to evaluate).	0.068	60	18
7	G3 lets G2 in the asset room	0.000	60	18
8	G2 disables or over-writes the camera system to reflect normal work routine. G3 helps G2 to get all the authorized access. They both use the tools to get the source from the device	0.144	600	180
9	Escape	0.437	200	60

Probability of interruption	**0.32**
Success probability of theft	**0.96**

With NE and DI working together, the adversary task time is reduced. The expected value of the probability of interruption, P_{mI}, obtained from the vector of 1000 random sample from Monte-Carlo simulation was estimated. Given that NE and DI plan to steal the source when the device is not in use, they get $n = 52$ trials based on 5 hours of device unavailability in a 24-hour working day. The binomial distribution is used to obtain the probability of observing $(X = 0)$ or $(X = 1)$ successes in n trials, with probability of success on a single trial denoted by $P_{mI} = 0.33$. The binomial distribution assumes that P_{mI} is fixed for all trials. The success probability of theft of ^{137}Cs source, given collusion of NE and DI, is computed to be 0.96.

<u>^{192}Ir Scenario I:</u>

RF is the threat group of interest in scenario I. The basic profile of RF is described by $U[adv]$ in section 4.2.1. RF considers the theft of *^{192}Ir* when the device is vulnerable. The HDR brachytherapy device is most vulnerable when it is not in use or when it undergoes source exchange (Table 3.2). The success probability of theft of *^{192}Ir* source is based on the prior distribution of the number of missing *^{192}Ir* source from the HDR device as derived from the NTI data. The CNS global incidents and trafficking database, reporting period 2013-2018, lists a total of 13 loss/theft/delivery failure incidents of the HDR source, with approximately 3 loss incidents per year. Based on an article from (Tim Williams, MD, Baco Raton regional hospital), the number of HDR units found in the US is approximately 800. Considering there were approximately 3 missing source incident a year, $event\ A$ is defined as the total number of reported loss of the HDR source in a year. Therefore, $P(A)$ is the prior probability of $event\ A$. $Event\ B$ is the evidence of the number of hours the device is not in use, in addition, to the number of hours the device undergoes source exchange in a year. As stated in section 3.5.2, the HDR device at St Benedict Healthcare treats 10 patients in a week, so 2 patients in a day. Each patient takes an hour approximately to get treated. The HDR device at St. Benedict is busy 20 $hours\ week^{-1}$. Considering a 40 $hour$ work week, the HDR device remains unused 20 $hours\ week^{-1}$. Considering the HDR device goes through a quarterly source exchange, the device in total will be vulnerable for 268 hours in a 3-month time frame, or a total of 1072 hours in a year. With the mean parameter $\mu = 89$ the probability that the source is vulnerable for $x = 250$ working days in a year is given by Poisson distribution $(P(B) = 0.004)$.

Table 4. 8 Pathway analysis of *^{192}Ir* scenario I with G1 threat actor.

HDR brachytherapy Scenario I

Probability of guard communication	Response Force time in seconds	
	Mean	SD
0.95	300	90

			Delay (seconds)	
Task	Task Description	P(Detection)	Mean	Standard Deviation
1	Enter Building	0.86	30	9
2	Walk 30 ft	0.00	10	3
3	Pass the cafeteria and lobby	0.00	30	9
4	Walk 200 ft	0.02	10	3
5	Pass the hallway and the doors	0.18	30	9
6	HDR door already open or hold a G3 actor hostage to let the intruder access	0.89	60	18
7	Walk to the device/asset	0.06	20	6
8	Cuts/Break the attached chain with a weapon/grinder tool and flee the HDR device (on wheels)	0.96	300	60
9	Escapes	0.960	100	30

Probability of interruption	**0.85**
Success probability of theft	**0.13**

The terrorist adversary RF would attack the source when it is vulnerable. The sequence of actions taken by RF is given in Table 4.8. The probability of detection is high for RF, as they enter the building and walk towards the HDR room. RF is an opportunistic terrorist who is not afraid to use force to gain access to the vital area. The adversary task time to cut a bolted steel chain attached to the HDR device is assumed to be 300 seconds, given that RF possess the electric grinder tools to cut it. The hardened chain provides path delay, providing the response force enough time margin to allow for a high probability of interruption. The probability of interruption was calculated to be $P_I = 0.85$. The overall success probability of the terrorist adversary RF stealing the source, given that the device was vulnerable, $P(A|B)$, was calculated using Bayes theorem (Eq (3.24)) to be 0.13.

^{192}Ir Scenario II:

This scenario is modeled as an intentional or unintentional mail delivery failure of *^{192}Ir* source. The G2 actor NE is assumed to be a mailman who is responsible for radioactive material package deliveries to healthcare facilities, such as St Benedict Healthcare. The success probability of theft in this case is calculated using Bayes theorem, based on the prior probability of the material loss, as mentioned in scenario I and the number of mail mis-deliveries. $Event\ A$ is defined based on the historical data of the number of radioactive material delivery failure or mis-routings according to the CNS global incident and trafficking report in North America (Harper et al., 2007). $Event\ B$ is the number of mis-deliveries from the mail carrier (FedEx). Considering there were 800 HDR units in North America, each HDR device goes through the source exchange 4 times a year and the source gets delivered twice per exchange. This makes a total of 6400 deliveries per year across the United States. According to the 2013-2017 NTI data, there has been 4 delivery failures of HDR sources. The probability of $event\ A$, $P(A)$, based on 1 radioactive package delivery failure each year, is calculated to be 0.00015. Similarly, based on the statistical data from FedEx, approximately 13 million packages get delivered worldwide every day, with ~7.5 million packages being delivered in the United States each day. The probability that some mails get misdelivered by a mail man is calculated to be $P(B) = 0.011$. The calculation uses a random number generator to estimate mis-deliveries from a uniform distribution between 75000 and 90000. Thus, given that the threat actor NE (mail man) is responsible to intentionally or unintentionally misroute packages, the probability that the misrouted package or the misdelivered package is a radioactive material package is given by $P(A|B) = 0.0012$.

^{192}Ir Scenario III:

The terrorist adversary DI in this scenario plans to steal the brachytherapy source based on the initiating event of source exchange. The $event\ A$ and the prior probability $P(A)$ of the lost or the missing source which is based on the historical NTI data remains the same in this scenario as well. The $event\ B$ is the number of hours or days that at least one HDR source (old source or the new source) remains vulnerable to theft due to source exchange. According to some research sources, the decayed ^{192}Ir HDR brachytherapy source at the time of source exchange is unloaded from the device and is transported in pig container. The source after being surveyed gets stored in a vault, until the arrival of the new source. After the source exchange the new source is stored in a safe lead metal bucket until it is shipped back to the manufacturer. Based on the assumption that 14 days out of the 3 months in a year at least one source is on site, a mean parameter μ of 56 days is taken to be the average number of days that the decayed or the new source is vulnerable to theft in a year. Assuming that the terrorist adversary DI, who is also an insider, is aware of the source exchange schedules and is authorized to have access to the vault room and the source metal bucket, DI makes a strategic plan to steal the source. The adversary path and the sequence of actions that DI takes to get to the source and steal it is presented in Table 4.9

Table 4. 9 Scenario III ^{192}*Ir* source theft by the threat actor DI (G3 threat group)

HDR brachytherapy Scenario III	Probability of guard communication	Response Force time in seconds	
		Mean	SD
	0.95	300	90

Task	Task Description	P(Detection)	Delay (seconds)	
			Mean	Standard Deviation
1	Enter Building	0.05	2	1
2	Walk towards the hot lab	0.08	10	3
3	G3 actor is aware that the source is in the hot lab/treatment room and so he/she accesses the room using the key	0.22	30	9
4	Walk to the asset	0.02	3	1
5	G3 actor disguises the source bucket to appear normal and walks out with it	0.34	100	30
6	Escapes	0.22	60	18

Probability of interruption	**0.06**
Success probability of theft/diversion	**0.85**

The probability of interruption is low because it is assumed that the total adversary task time is much less than the response force time of 300 sec. Since DI is an insider, the authorized access privileges help them to breach the security system. The failure of detection and deception of DI committing task 5 at St. Benedict Healthcare helps the terrorist adversary to complete the task without any delay or interruption. The lack of an intrusion detection sensor or an alarm system for a stored source in a vault or in a metal bucket posed few insurmountable obstacles to achieve their source theft/diversion goal. The P_I is calculated to be 0.06. The overall success probability of theft/diversion was, however, based on the pathway model of an insider and the probability of the ^{192}Ir brachytherapy source being vulnerable. The $P(A|B)$=0.85 is computed to include the cumulative detection probabilities along the adversary path, P_I , and the probability of missing/stolen source, $P(B)$, based on the historical data obtained from the NTI database $P(A)$.

The descriptions of the scenarios and their respective success probabilities of theft/diversion suggest that the terrorist attacking as an insider would be more likely to succeed than an infiltrator. Scenario III shows that a current employee (who became disgruntled) with long-term access and detailed knowledge of inner workings and schedules may know more about the source vulnerability than an infiltrator new to the organization, making the targeting process much simpler and covert.

^{60}Co Scenario I:

Scenario I describe and calculates the success probability of theft or diversion of *^{60}Co* by an outside perpetrator, RF. RF as noted from Table 4.3 possess strong motivation to cause harm, but lacks the capability, the technical knowledge, and the resources to access the Gamma Knife®. Referring to Table 3.2, the initiating event for a theft or diversion of *^{60}Co* source is dependent on the quarterly maintenance and repair of the Gamma Knife®. The quarterly maintenance of the Gamma Knife device is a requirement at St Benedict Healthcare. This scenario uses a Poisson random generator to generate random number of days that the Gamma Knife would need maintenance and repair based on a mean frequency of 8 days in a year. Keeping in mind the security operations of St Benedict Healthcare, a pathway model of probability of interruption is calculated for the terrorist adversary RF. Table 4.10 displays the sequence of tasks performed by RF to get to the source. It is also assumed that RF uses force against the facility employees to minimize delay and puts little regards towards probability of detection. The probability of detection is high at every delay element of the adversary path based on St. Benedict's adequate protection system.

Table 4. 10 Scenario I ^{60}Co source theft/diversion by the threat actor RF (G1 threat group)

Gamma Knife Scenario I	Probability of guard communication	Response Force time in seconds	
		Mean	SD
	0.95	300	90

			Delay (seconds)	
Task	Task Description	P(Detection)	Mean	Standard Deviation
1	Enter Building	0.26	2	1
2	Walk 80 ft	0.00	10	3
3	Enter Lobby door	0.51	10	3
4	Walk 150 ft	0.00	60	18
5	Force door open/Gamma knife door already open	0.72	60	18
6	Walk to the device/asset	0.42	3	1
7	Threaten the maintenance crew to open the device and gather the source pellets	0.81	1500	450
8	Escape	0.14	900	270

Probability of interruption	**0.94**
Success probability of theft	**0.29**

The in-device delay kits and other set of protection induce increased delay times affecting the use and maintenance of the device. The critical detection point (CDP), where the adversary task time remaining to complete the goal exceeds the response time, is reached quickly along the adversary path in this scenario. The probability that the threat actor RF will be interrupted before completing the task is computed to be high. Because of the uncertainty in the parameters, a Monte-Carlo simulation is used to generate a vector of 1000 iterations with a mean probability of $P_I$and 2σ standard deviation. The mean of the simulated outcomes, P_{mI}, is used as a probability of failure on a single trial in binomial distribution. The overall success probability of theft or diversion is calculated to be $P_S = 0.29$.

^{60}Co Scenario II:

As part of scenario II, a similar pathway model is used to calculate the cumulative probability of interruption for the terrorist adversary NE. The assumption made in this scenario is that NE, who is the maintenance personnel appointed by the device manufacturer and vetted by St. Benedict Healthcare, goes rogue. NE may not possess motivations as high as the RF, but they primarily have the highest capability, in this case, to abuse system and maximize their chance of success to have access to critical areas. G2 threat community carries the second highest $U[adv]$ because of their capability and the most resources available to carry out the task successfully. The probability of detection for scenario II is approximated to be low, because of the escorted access and the availability of propriety tools to open the radiation unit housing and steal the source. Using the detection probabilities and the delay component values, the probability of interruption was calculated to be $P_I = 0.85$, as seen in Table 4.11.

Table 4.11 Scenario II ^{60}Co source theft/diversion by the threat actor NE (G2 threat group)

Gamma Knife Scenario II	Probability of guard communication	Response Force time in seconds	
		Mean	SD
	0.95	300	90

			Delay (seconds)	
Task	Task Description	P(Detection)	Mean	Standard Deviation
1	Enter Building	0.03	2	1
2	Walk 80 ft	0.00	10	3
3	Enter Lobby door	0.03	10	3
4	Walk 150 ft	0.00	60	18
5	Open door (Escorted access)	0.07	10	3
6	Walk to the asset	0.17	3	1
7	Open the housing of the unit unload the source pellets in a lead bucket and walk out	0.82	240	72
8	Escape	0.83	300	90

Probability of interruption	**0.85**
Success probability of theft	**0.64**

The probability of interruption for scenario II is observed to be only slightly lower than scenario I. The detection probability is likely to increase if the RMS monitoring station notices a breach or abnormal behavior from NE. The escorted access by an RSO or the presence of any other insider personnel, would either deter a semi-insider to be malicious, or trigger a suspicion followed by detection. The frequency of repair and maintenance ($\lambda = 8\ days\ year^{-1}$) was kept constant as scenario I. The overall success probability of NE stealing the ^{60}Co source is computed to be 0.64.

^{60}Co Scenario III:

Scenario III proves to be the most vulnerable of the path as the threat actors NE and DI work in collusion to steal the ^{60}Co source on the day of maintenance or repair of the Gamma Knife device. The pathway analysis is only performed for NE, who would be scheduled to do the maintenance on the Gamma Knife at St. Benedict facility. The insider DI is assumed to work at the facility which allows them to arrive and leave as per their convenience. On the day of maintenance, DI is assumed to be at work at the facility before the arrival of the maintenance personnel NE. DI is assumed to help disable the tamper alarms and block the camera to defeat all means of detection. The detection probability, however, would change based on the facility, if they have additional safeguards against insiders to delay the adversary until the response force arrives. The probability of interruption of this scenario is calculated as 0.29. Table 4.12 displays the detection probabilities, delay times of the ordered sequence of tasks along the path of the adversary.

Table 4. 12 Scenario III ^{60}Co source theft/diversion by the threat actor DI in collusion with NE

Gamma Knife Scenario III	Probability of guard communication	Response Force time in seconds	
		Mean	SD
	0.95	300	90

Task	Task Description	P(Detection)	Delay (seconds)	
			Mean	Standard Deviation
1	Enter Building	0.01	4	1
2	Walk 80 ft	0.00	20	6
3	Enter Lobby door	0.03	20	6
4	Walk 150 ft	0.00	120	36
5	Open door (Escorted access)	0.07	10	3
6	Walk to the asset	0.07	3	1
7	Pretend to perform maintenance. Open the device and gather source pellets in a lead bucket. Insider helps to disable alarms and block cameras	0.17	200	60
8	Escape	0.46	200	60

Probability of interruption	**0.29**
Success probability of theft	**0.90**

Assuming the same estimated parameters of initiating event rate and the number of trials, the overall success probability of the theft of gamma knife, is computed to be 0.90. Although several combinations of insider threats are possible, emphasis is only placed on addressing the most probable insider semi-insider threat.

The results of the three scenarios considered above display the terrorist adversary's ability to accomplish the task in each situation and helps quantitatively assess the best chance for success. All of the theft or diversion scenarios models the exit path as escape. The scenarios do not list the specific protection delay element along the adversary escape route, only the average delay time required based on the situation. The terrorist adversaries after a successful theft is assumed to escape to the roof of St. Benedict Healthcare where they plan to detonate the source material with a conventional explosive to effectively disperse the radioactivity.

4.2.4 Expected Utility (EU)

As described in the explanation of utility maximization given in section 3.1.2, it is realistic to model the terrorist adversaries' behavior as following the decision criterion of expected utility maximization, i.e., they will evaluate all attack scenarios known to them and choose the scenario that maximizes their expected utility. The expected utility of each attack scenario computes the product of the overall success of theft probability and the total utility for each scenario Eq (3.2). The "no attack" outcomes are not modeled because the research has focused on the worst-case outcomes. The possible utilities or dis-utilities of the failure outcomes for all scenarios are thought to be negligible and therefore are assumed to be zero. Based on the numerical illustration described in section 4.2.3, the success probabilities of theft of the attack scenarios as a function of the intents and capabilities of each group were computed, $P_s\left(M_iX_j\right)_t$. The total utility is calculated as a function of material utility and adversary utility Eq (4.2). Table 4.13. displays the total utility function with respect to the three threat groups and the three assets. A simplifying assumption is made that each terrorist group only plans one type of attack for each time period analyzed.

$$EU\left[M_iX_j\right] = P_s\left(M_iX_j\right)_t \times U_{tot}(M_iX_j) \tag{4.1}$$

$$U_{tot}\left(M_iX_j\right) = U_j[adv] \times U_i[mat] \tag{4.2}$$

where

M_i is the choice of radioactive material for an attack attempt;

X_j is the intent from group j to attack;

t is the index of threat scenario for material i and threat group j;

P_s is the success probability of theft as assessed by the facility; and

U_{tot} is the total utility function assessing the adversary intentions and material preferences.

Table 4.13 The total utility function of the three threat groups with respect to three assets

Threat groups	$U[tot]$for Co-60	$U[tot]$for Cs-137	$U[tot]$for Ir-192
Religious fundamentalist (RF)	1.28	1.34	1.14
National domestic extremist (NE)	1.18	1.23	1.06
Disgruntled insider (DI)	0.86	0.85	0.73

According to the theory explained in section 3.1.2, the total utility function characterizes the following asset bundles with respect to the threat groups: (*^{60}Co, G1*), (*^{60}Co, G2), (^{60}Co, G3),* (*^{137}Cs, G1*), (*^{137}Cs, G2), (^{137}Cs, G3),* (*^{192}Ir, G1*), (*^{192}Ir, G2), (^{192}Ir, G3)*. The numbers generated by the total utility function are used to order the bundles. As seen in Table 4.13. more preferred bundles get assigned larger numbers than less-preferred bundles. Ranking: (^{137}*Cs, RF)*≻ (*^{60}Co, RF)*≻ (*^{137}Cs, NE*) ≻ (*^{60}Co, NE)* ≻*(^{192}Ir, RF)* ≻*(^{192}Ir, NE)* ≻ (*^{60}Co, DI)* ≻*(^{137}Cs, DI)* ≻*(^{192}Ir, DI).*

Table 4.14-4.16. displays the results of the facility expected utility to the threat group j of an attack using radioactive material i.

Table 4.14 Scenario probabilities of ^{60}Co, total utility functions and the expected utility to the different threat groups.

Scenario probabilities		
$P_s(Co_{60}, X_{RF})_1$	$P_s(Co_{60}, X_{NE})_2$	$P_s(Co_{60}, X_{DI})_3$
0.29	0.64	0.90
Total utility value		
$U_{tot}(Co_{60}X_{RF})$	$U_{tot}(Co_{60}X_{NE})$	$U_{tot}(Co_{60}X_{DI})$
1.28	1.18	0.82
Expected Utility		
$EU[Co_{60}X_{RF}]$	$EU[Co_{60}X_{NE}]$	$EU[Co_{60}X_{DI}]$
0.37	0.76	0.74

Table 4.15 Scenario probabilities of ^{137}Cs, total utility functions and the expected utility to the different threat groups.

Scenario probabilities		
$P_s(Cs_{137}, X_{RF})_1$	$P_s(Cs_{137}, X_{NE})_2$	$P_s(Cs_{137}, X_{DI})_3$
0.87	0.73	0.96
Total utility value		
$U_{tot}(Cs_{137}X_{RF})$	$U_{tot}(Cs_{137}X_{NE})$	$U_{tot}(Cs_{137}X_{DI})$
1.34	1.23	0.85
Expected Utility		
$EU[Cs_{137}X_{RF}]$	$EU[Cs_{137}X_{NE}]$	$EU[Cs_{137}X_{DI}]$
1.16	0.90	0.82

Table 4.16 Scenario probabilities of ^{192}Ir, total utility functions and the expected utility to the different threat groups.

Scenario probabilities		
$P_s(Ir_{192}, X_{RF})_1$	$P_s(Ir_{192}, X_{NE})_2$	$P_s(Ir_{192}, X_{DI})_3$
0.13	0.0012	0.85
Total utility value		
$U_{tot}(Ir_{192}X_{RF})$	$U_{tot}(Ir_{192}X_{NE})$	$U_{tot}(Ir_{192}X_{DI})$
1.14	1.06	0.73
Expected Utility		
$EU[Ir_{192}X_{RF}]$	$EU[Ir_{192}X_{NE}]$	$EU[Ir_{192}X_{DI}]$
0.15	0.0013	0.62

A utility function has the property that the expected utility of any alternative indicates its desirability. Specifically, the utility function is constructed such that alternatives with higher expected utilities are preferred to alternatives with lower expected utilities. Table 4.14-4.16 shows that the expected utility of each choice (asset) is calculated using Eq (4.1).

Typically, terrorists are modeled as expected utility maximizers. There is some controversy about whether terrorists (or any other human decision makers) are adequately modeled by expected utility maximization in every situation. Some terrorists are neither rational nor intelligent, and such terrorists would not necessarily be utility maximizers. Modeling irrational and unintelligent terrorists would be difficult, and such an approach risks understating the true level of risk because these terrorists are incompetent and therefore unlikely to succeed. For the purpose of the PFRI, which is to realistically model the terrorist threat, it seems plausible to assume that the terrorist adversary is rational and intelligent. As seen from Table 4.15, the choice of the terrorist adversary, RF, choosing to attack and sabotage ^{137}Cs presents the maximum expected utility, which implies that ^{137}Cs source is the most threatened asset at St. Benedict Healthcare. The RDD game theoretical model presented in Chapter 6 shows that the idea of defending the facility against the worst that an adversary could do is not a bad thing.

4.3 Vulnerability input

St. Benedict Healthcare facility is located in Marion county of Indiana, USA. Vulnerability input, as we know from section 2.3 integrates the degree of impact from locational hazard indicators and the facility nuclear security culture. As mentioned previously, downplaying, or neglecting locational hazards or human behavior can lead to physical weaknesses or gaps in security that adversaries can exploit.

4.3.1 Marion county locational hazard input

A comprehensive list of external natural hazards was extracted from the National Oceanic and Atmospheric Administration (NOAA) National Climatic Data Center (NCDC) storm events database. NOAA's storm event database documents the occurrence of storms and other significant weather phenomena having enough intensity to cause public health or economic problems. Marion County storm event data for the years of 2000-2017 were used. Natural disaster events were broken down into three broad categories: geological, meteorological, and hydrological. The county crime rate was another external indicator considered in this study. Federal Bureau of Investigation (FBI) Uniform Crime Reporting (UCR) program data from 2000-2017 was used. The UCR data includes the rates of violent and property crime. Power outages can disrupt the safety and security of facilities by disrupting operations of critical equipment. Fifteen years of power outage data compiled by the Department of Energy (DOE) was used. This data accounted for outages in Marion County from the major electricity providers and operators.

Each Marion county locational hazard indicator value was measured in different scales and units. The minmax normalization method, given in Eq (3.28), was used to rescale the data from 0 to 1. Transforming indicators to an identical scale, allowed for direct comparison. The normalized data was presented in the form of a 17×5 matrix, where each row was an observation of the yth year (2000-2017) and eth (meteorological, hydrological, property, violent crime, and power outage) locational hazard. Table 4.17 displays the normalized locational hazard indicator data.

Table 4.17 Normalized locational hazard data for Marion county from 2000-2017

Year	Meteorological hazard	Hydrological hazard	Property Crime	Violent Crime	Power Outage
2000	0.125	0.071	0.983	0.735	0.056
2001	0.107	0.000	0.212	0.524	0.111
2002	0.161	0.214	0.689	0.633	0.000
2003	0.250	0.571	0.618	0.680	1.000
2004	0.000	0.500	0.673	0.626	0.389
2005	0.375	0.286	0.734	0.939	0.361
2006	1.000	0.000	0.793	0.912	0.389
2007	0.161	0.286	0.874	1.000	0.056
2008	0.571	0.857	0.859	0.918	0.167
2009	0.714	0.429	0.698	0.789	0.389
2010	0.161	0.500	0.000	0.000	0.333
2011	0.661	0.429	0.863	0.701	0.694
2012	0.893	0.286	1.000	0.748	0.639
2013	0.446	0.214	0.833	0.776	0.944
2014	0.732	0.500	0.833	0.810	0.333
2015	0.411	0.857	0.780	0.905	0.222
2016	0.714	1.000	0.661	0.884	0.306
2017	0.268	0.071	0.379	0.741	0.583

Factor analysis was performed on the multivariate data to estimate the weights of each variable. As per the discussion in section 3.6, the measured variables in the factor analysis model depend on a smaller number of unobserved (latent) factors. Because each factor might affect several variables in common, they are known as common factors. Each variable is assumed to depend on a linear combination of the common factors, and the coefficients are known as loadings. Each measured variable also includes a component due to independent random variability, known as specific variance, because it is specific to one variable. Factor analysis was performed on the covariance matrix (Σ) to estimate the matrix of factor loadings $lambda$ (L) , and the elements of the diagonal matrix (Ψ). The MATLAB function $factoran$, uses the maximum likelihood estimate (MLE) procedure to find factors that maximizes the likelihood of producing the correlation matrix.

Table 4. 18 Factor loadings and the specific variance with respect to each variable

Locational hazard indicators	Factor 1 (Lambda)	Sigma (specific variance)
Meteorological disasters	0.4369	0.8091
Hydrological disasters	0.0825	0.9932
Property crime	0.9975	0.0050
Violent crime	0.7575	0.4262
Power disruption	0.3713	0.8622

Extraction method: Maximum Likelihood Estimate

Rotation method: Varimax

Table 4.18 gives a list of the estimated loadings and the estimated specific variances. For Marion county locational hazard data, the function $factoran$ is called specifying a model fit with one common factors. From the estimated loadings, it is clear that the one common factor in this model puts least weight (loading) on hydrological disasters, most weight of the property crime, followed by the violent crime. Meteorological disaster and power disruption were given almost comparable weights. By default, $factoran$ computes rotated estimates of the loadings to try and make their interpretation simpler. The varimax rotation is performed to simplify the columns of the factor matrix and provide meaningful interpretations to the factors. One interpretation of this fit is that the data might be thought of in terms of their vulnerability (latent variable) on the facility, for which property crime, violent crime would be the best available measurements, followed by lower loadings on meteorological disasters and power outages. The factor loadings of power disruption and meteorological disasters being so close to each other would imply that most of the power disruptions are caused as a result of meteorological disasters, impacting the vulnerability of the facility. Since, St. Benedict Healthcare is located in Marion county, facility's vulnerability from hydrological disaster is lot lower relative to other natural disasters. This would explain the lower loading on the hydrological disaster.

From the estimated specific variances in Table 4.18, we see that a particular locational hazard indicator varies quite a lot beyond the variation due to the common factor. A specific variance of 1 would indicate that there is no common factor component in that variable, while a specific variance of 0 would indicate that the variable is entirely determined by common factors. There is least amount of specific variation on property crime and high specific variation on hydrological disaster, which is consistent with the interpretation given in the single common factor. Therefore, factor analysis was used to assign weights to the normalized data of locational hazard indicators. Table 4.19. shows the computed normalized locational hazard weighted indicator data. Equation (3.27) was applied to construct an overall vulnerability index. The vulnerability index of St. Benedict Healthcare is calculated as 0.006.

Table 4. 19. Normalized locational hazard weighted indicators for Marion county from 2000-2017

Year	Meteorological hazard	Hydrological hazard	Property Crime	Violent Crime	Power Outage
2000	0.055	0.006	0.980	0.557	0.006
2001	0.047	0.000	0.212	0.397	0.000
2002	0.070	0.018	0.687	0.479	0.000
2003	0.109	0.047	0.616	0.515	0.006
2004	0.000	0.041	0.672	0.474	0.006
2005	0.164	0.024	0.732	0.711	0.006
2006	0.437	0.000	0.791	0.690	0.034
2007	0.070	0.024	0.871	0.757	0.022
2008	0.250	0.071	0.857	0.696	0.111
2009	0.312	0.035	0.697	0.598	0.030
2010	0.070	0.041	0.000	0.000	0.019
2011	0.289	0.035	0.861	0.531	0.065
2012	0.390	0.024	0.997	0.567	0.371
2013	0.195	0.018	0.831	0.587	0.021
2014	0.320	0.041	0.831	0.613	0.010
2015	0.179	0.071	0.778	0.685	0.000
2016	0.312	0.083	0.660	0.670	0.000
2017	0.117	0.006	0.378	0.562	0.000

The vulnerability value of 0.006 implies that St. Benedict Healthcare is located in an inherently low vulnerability area. It is unlikely that the facility's vulnerability to theft or sabotage of radioactive material would increase because of its location. The locational impact of St. Benedict on PFRI would be close to negligible.

4.3.2 Nuclear security culture at St. Benedict Healthcare

As discussed in section 3.7, two types of surveys “technical “and “general” were developed and deployed to examine the nuclear security culture of a medical facility. The general survey contained questions across four broad categories: 1) awareness of policies, 2) enforcement of policies, 3) leadership behavior and involvement, 4) and individual belief and attitude. A technical survey was distributed to relevant professional personnel having authorized access to radioactive materials and devices in the facility. The technical survey evaluated characteristics related to: 1) deter and detect, 2) response, 3) accountability and security awareness, 4) transport, 5) and training. The survey responses were taken from an assessment performed on an actual medical facility. General survey and technical survey participation were 16.2% and 9.37%, respectively. Questions for each survey were formatted with a choice of seven numerical responses from “strongly agree” (1) to “strongly disagree” (7).

Results of the two survey types were presented in three score ranges: weak (score > 4), neutral (score = 4), and strong (score < 4). The response percentages within the three score ranges are presented in Table 4.20. Appendix A provides with a list of all the questions used for both general and technical survey.

Table 4. 20 Summary of the nuclear security culture assessment

	Weak	Neutral	Strong
General			
Belief and Attitude	0.01	0.01	0.23
Leadership/Management	0.03	0.04	0.18
Policy	0.02	0.04	0.19
Enforcement	0.03	0.04	0.18
Total	***0.09***	***0.13***	***0.78*** ($\boldsymbol{Z_{gen}}$)
Technical			
Detect and Deter	0.02	0.04	0.15
Response	0.02	0.06	0.12
Accountability and Security Awareness	0.03	0.03	0.15
Transport	0.04	0.03	0.08
Training	0.03	0.05	0.07
Total	***0.14***	***0.21***	***0.58*** ($\boldsymbol{Z_{tech}}$)

The three categories of “leadership and management”, “policy” and “enforcement” under the general survey type showed consensus in the degree of perception across a range of respondents. Results showed that participants felt strongly towards questionnaire referring to individual job performance and elicited personal opinions about nuclear and radioactive material security, resulting in a higher weighted mean response rating in the category of “belief and attitude”. The weighted mean score rating of the two categories of “training” and “transport” under the technical survey type exhibited opinion disparities relative to rest of the three categories, implying deficiency in training evaluations and transit procedures. The equally weighted categorical average (Table.

4.20) was totaled, respective to its survey type to emphasize the cumulative impact of the score range on the organization's radiological security culture. The strong score range, Z_{gen} and Z_{tech}, reflected the impact of the facility's security culture on facility vulnerability to attack from threat groups G1 and G3. The strong score range, Z_{sub}, calculated as 0.72, reflected the impact of security culture on the facility's vulnerability to attack from the G2 threat group.

A high score range of Z_{sub} would be crucial where the work community overlaps substantially with the social community. As seen from the G2-G3 theft/diversion collusion attack scenarios presented in section 4.2.2, weaknesses in terms of professional conduct and personal accountability, along with sharing of critical "insider knowledge" with the non-facility workers may lead to a great deal of damage to the facility and its employees. A strong score range of 0.78 for Z_{gen} implied that most of the respondents felt positively towards the general survey type questionnaires overall.

Belief and attitude category of the general survey type showed the highest consensus among the participants, indicating a strong foundation towards an effective nuclear security culture. Behaviors are the ultimate, tangible demonstration of an organization's values, beliefs, and attitudes. To improve staff behavior, senior management must clearly understand their own roles and responsibilities for security, know when and how to use their authority, and provide management oversight. The strength score of 0.18 received by "Leadership and management" category of the survey demonstrated respondent's perception of quality management system and the strong belief that security culture is important. The strong score range, Z_{tech}, of the technical survey type gave a lower value of 0.58 relative to Z_{gen} and Z_{sub}, highlighting the inadequate understanding of detection, response, training and transport of radioactive material operations within the facility. A strong sense of vulnerability to the insider threat, for instance, may be missing, given the scattered perception the staff and other radioactive material users had towards the "training" and "security awareness" categories of the survey. A collective response of the participants pertaining to the question of "identifying suspicious behaviors in and around the medical facility" was found to be inclined towards a negative opinion. Such a response indicates that the reporting of serious concerns, often referred to as *whistleblowing*, is not an established policy at this facility.

Encouraging employees to report concerns seems inherently challenging, but on the other hand, they are also the first line of defense when it comes to keeping their fellow workers, communities, and organization safe and secure. A low score of Z_{tech} shows weakness in the impact of the G3 threat group towards vulnerability of the facility. This is because insiders with access rights, intimate knowledge of the facility operations, and authority over staff have the ability to bypass dedicated security measures and compromise material control and accountancy, cybersecurity, technical security features and more. As seen in the attack scenarios of ^{60}Co and ^{137}Cs, insiders have the resources and the capability to plan a theft event in coordination with the outside terrorist groups, and with the highest probability to succeed. It is an individual's peers who are best placed to notice a colleague's unusual behavior, sudden changes in attitude, or performance anomalies; in other words, signs that may point to the possibility that the colleague could become a threat. To avoid masking the weaknesses that contribute most to the vulnerability of the facility, the minimum value of the nuclear security culture survey (Z_{tech}) was used in the risk index calculation.

4.4 Consequence input

To evaluate the consequences, this analysis assumes the theft of the radioactive material was successful. The RDD is assumed to be detonated at the facility it is stolen from. Except for the sabotage scenario, all the other theft scenarios incorporate the adversary task time to escape either to the roof or the parking lot of St. Benedict Healthcare to detonate the source material and effectively disperse the radioactivity. Medical centers in itself are attractive terrorist targets for terrorist attacks. Most medical centers are located in the center of major metropolitan cities and are near several transportation modes (e.g., road, ship, and rail), presenting terrorists with several reasons to detonate the high activity radioactive material in the facility and cause widespread contamination to all symbolic buildings in the nearby area. The activity in the nearby metropolis, downtown area, recreational parks, and transportation system makes the terrorist attack on the hospital facility of significant consequence both to the local livelihood and as well as to the regional economy.

According to Kamen et al. (2019), some hospital entities are also highly attractive targets with respect to religiously motivated terrorists because of their strong religious affiliations. This analysis examines two detonation scenarios of the RDD bomb: 1) use of a 150 lbs. suitcase bomb (68 kg) detonated on top of the roof, and 2) use of a 2000 lbs. (907 kg) vehicle bomb detonated in a parking lot. The dangers of varying sources and quantities of radioactive material with respect to the amount of conventional explosive used is also explored. The RDD bomb when detonated, the radioactive material scatters into the environment, some forming a radioactive plume, and the remaining quantity falling in clumps or larger particulate matter near the location of the explosion. The RDD bomb can result into in both deaths and injuries from the initial blast of the conventional explosives as well as radiation sickness and cancer from exposure to the radioactive material. The consequences of the RDD is examined as a function of immediate fatalities from the blast and radiation, injuries from the blast, morbidity from stochastic effects, and the economic loss resulting from decontamination costs, evacuation costs, business losses, and property loss.

4.4.1 Blast effects

Two hypothetical case examples are considered here to study the effects of blast overpressure on the structure and targets. The propagation of blast waves caused by conventional weapons of 150 lbs. and 2000 lbs. TNT equivalent are examined using the theory discussed in section 3.8. Both of the improvised devices (IEDs) are assumed to be of a confined explosion type, where the explosive is encased, and the explosive energy is greater than the mechanical integrity of the casing material. The IEDs are also assumed to be in a conventional shaped charge form to be able to penetrate the reinforced concrete or the steel shielding surrounding the radioactive material. The portable suitcase used as a delivery mechanism for the 150 lbs. bomb is detonated remotely or by a suicide bomber on the rooftop of the healthcare. The suitcase is assumed to be made of a munition grade material filled with 150 lbs. of TNT and equipped with a radioactive material steel casing. A car loaded with 2000 lbs. explosives is used as a delivery mechanism by the terrorist adversaries in this second hypothetical scenario. It is set to explode remotely at St. Benedict Healthcare’s four storied parking lot.

On detonation of these bomb, the blast effects on the building structures and human targets were determined by analyzing the (1) overpressure that the building structural elements can withstand, (2) standoff distance that can be enforced, and (3) potential damage from a specific amount of explosives detonated at an enforceable standoff distance. The explosive scaling law (Eq. (3.29)) is used to relate the distances of the two TNT equivalent explosive amounts with the same peak overpressure. The blast data from 1 kg of TNT was used as a reference explosion. The scaled distances for the 150-pound suitcase bomb and 2000-pound car bomb is given in Table 4.21.

Table 4. 21 Scaled and standoff distances for equivalent charge weight TNT (kg)

	150-pound (68 kg)	2000-pound (907 kg)
Z (m kg^{-1} TNT equivalent)	R (m)	R (m)
1.5	6.12	14.51
2	8.16	19.35
4	16.32	38.71
6	24.48	58.06
10	40.81	96.76
12	48.97	116.12
20	81.61	193.53
30	122.42	290.29
50	204.03	483.82

Table 4.21 shows that with different weights of the same explosive, there will be an identical scaled distance where they will exhibit similar blast waves. The next step was to determine the overpressure a particular sized explosive device will generate when detonated at a specific distance from the building. The blast pressures experienced by a structure are in a most general sense related to the amount of explosive used and the distance of the building from the explosion. The peak incident pressure, charge weight, and the distance are mathematically related through an expression that varies as a function of the weight of the explosive and the cube of the distance, shown in Eq (3.30) and (3.31). Table 4.22 presents the computed peak overpressure results of the two types of bombs as a function of the standoff distances *(*R).

Table 4.22 Blast overpressure P_{so} as a function of the standoff distances (R)

W=68 kg TNT	W=907 kg TNT

R (m)	R (m)	P_{so}
6.12	14.51	43.66
8.16	19.35	22.67
16.32	38.71	5.90
24.48	58.06	3.06
40.81	96.76	1.43
48.97	116.12	1.10
81.61	193.53	0.49
122.42	290.29	0.22
204.03	483.82	0.02

It can be observed from Table 4.22 that the detonation of a 150-pound suitcase bomb would produce a peak overpressure of 5.9 psi at about 16 from the point of detonation and for a 2000-pound bomb, a similar overpressure of 5.8 psi is produced at a distance of 38.71 m from the point of detonation.

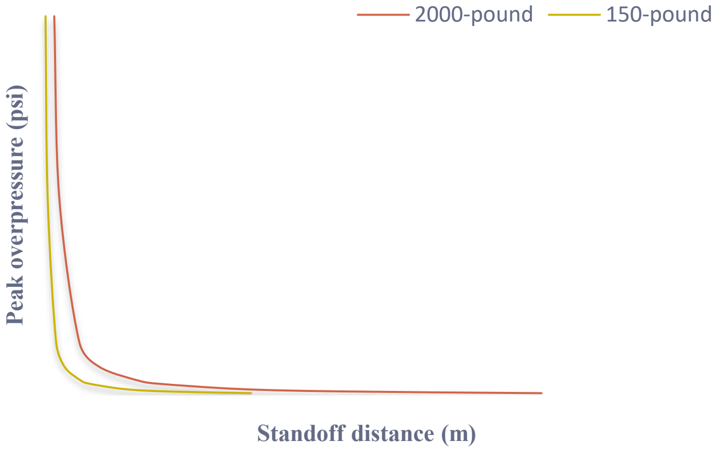


Figure 4.2 Plot showing the pressure decay with distance

The initial blast pressure increases to a value above ambient atmospheric pressure but decreases very quickly with increasing distance between the building and the bomb (Figure4.2). The basic idea behind explosive scaling law is that, for a target to experience the same overpressure with a smaller bomb, the target will need to be much closer to the bomb than with a more massive explosive. The damage levels of the blast load may be evaluated by explosive testing, engineering analysis or both. This research uses the reference curves and the damage approximation charts from Figure3.11 and 3.12 to describe the level of damage in terms minor moderate and major structural damage as a function of peak overpressure. A brief description of each damage level is:

- Minor: Nonstructural failure of building elements such as windows, doors, curtain walls, and false ceilings.
- Moderate: Structural damage is confined to a localized area and is usually repairable. Structural failure is limited to secondary structural members such as beams, slabs, and non-load bearing walls.
- Major: Loss of primary structural components such as columns or transfer girders. In this case, extensive fatalities are expected. Building is usually not repairable.

Figure3.11 is used as a useful tool to predict the expected overpressure on a building for a specific explosive weight and stand-off distance. The x-axis is the estimated explosive weight a terrorist might use, and y axis is the standoff distance from a building. By correlating the resultant effects of overpressure with other data, the degree of damage that the various components of a building might receive was estimated (Table 4.23). Table 3.5 is used as a guidance tool to compare different types of blast-induced trauma on the human target with the increasing blast pressure. According to data presented in NUREG/ CR-7201 (U.S. NRC, 2015) death can occur at a threshold pressure of 100 psi and certain death occurs for pressures of 200 psi. For a lung damage to occur, the air blast must strike the chest directly. The lung damage can occur for short duration (3 to 5 ms) pressures between 30 and 80 psi. The threshold for eardrum rupture to occur is 5 psi and for pressure lower than 5 psi a temporary hearing loss can occur.

Table 4.23 Damage approximations estimates of peak overpressure.

Peak over pressure (psi)	Damage to structures	Human target
43.66	Probable total destruction of most buildings	Possible lung damage
22.67	Probable total destruction of most buildings	Possible lung damage and eardrum rupture
5.90	Reinforced concrete buildings severely damaged	Eardrum rupture or temporary hearing loss
3.06	Collapse of wood-framed buildings	Temporary hearing loss
1.43	Failure of concrete block walls	Serious injuries are common
1.10	Panels of sheet metal buckled	People injured by debris
0.49	Minor damage to some buildings	Light injuries estimated
0.22	Typical window glass breakage	Light injuries estimated

Fragmentation effects

The blast and fragmentation radius of the weapon is always a factor in the area effect of an explosive weapon. Whether an explosive weapon is detonated in a fixed position (such as a car bomb) or whether it is dropped from the air or projected from the ground, the blast and fragmentation radius is always a determinant of the population directly affected and the damage likely to be produced.

Fragmentation typically affects a greater area than is reached by the blast effects. The fragments can still be deadly at greater distances, but they are generally more dispersed and so the likelihood of striking people decreases. As explained in section 3.8.1, the effects of fragmentation of a 150-pound bomb and the 2000-pound bomb are conceptualized in terms of the levels of risk presented to the population at specific distances.

As an example, the fragmentation effects of a high explosive munition can be seen in the common 122 mm artillery rocket type BM-21, model 9M22. The warhead of this munition contains 6.4 kg of TGAF-5[6] high explosive composition and generates a total of 3920 representative fragments,

[6] TGAF-5 is comprised of 40% TNT, 40% RDX, 17% Aluminum powder and 3% phelgmatiser.

with 1640 fragments weighting approximately 2.4 g, and 2280 fragments weighing 2.9 g. The standard Mk 82 bomb, in its simplest configuration contains approximately 89 kg of high explosive in a forged steel body weighting 142 kg (GICHD, 2017). The detonation of a Mk 82 bomb produces a peak overpressure of 117 kPa at 16m from the point of detonation. The design fragment from this weapon is less than 20 grams travelling 2400 $m\ s^{-1}$, which can penetrate up to 32 mm of steel armor plate. The number of fragments directly resulting from the RDD device is unknown; a scale model of the fragmentation effects of the RDD device is developed from the known specifications of the above-mentioned munition weapons. The 150-pound bomb was assumed to be 1/5th the size of BM-21, so the number of fragments were assumed to be likely in the range of ~500-700. The 2000-pound car bomb in this research is assumed to be about 4 times the mass of Mk 82 bomb, which is known to produce fewer than 3000 fragments. Car bomb, in this research, is assumed to produce fragmentation in the same range of Mk 82 bomb, assuming a cylinder of explosive with a conically shaped hollow cavity is placed in one end and a detonator is placed at the opposite end.

Given the initial number of fragments (N_0) for each bomb type, the expected number of fragments that would hit the target (N_{hits}) was calculated using Eq (3.32). The kinetic energy of the fragments from both bomb types were assumed to be 80 Joules. The level of damage sustained by the human target, with an impact energy of 70-80 J is assumed to be extensive, but the individual would still be able to function at reduced effectiveness $(P_{k|hit} = 0.2)$. Equation (3.33) was used to compute the distance from the point of explosion to the point at which the density of hazardous fragments has decreased to less than 1 hazardous fragment per $55.7\ m^2$, based on the net explosive weight of the bombs ($W = 150\ lb\ and\ W = 2000\ lb$). The lethal area, within which any person is likely to be killed and the casualty producing area within which casualties can be expected from the hazardous fragments is computed using Eq (3.35) and Eq (3.36). The total probability of kill given N fragmentation hits can be calculated using Eq (3.34). The expected number of casualties were estimated using Eq (3.37), assuming the population density km^{-2} surrounding the hypothetical facility of St Benedict is 3252. Table 4.24 lists the values of the blast fragmentation parameters for the 150-pound charge weight of the bomb and Table 4.25 lists the value of the blast fragmentation parameters for the 2000-pound charge weight of the bomb.

Table 4.24 Blast fragmentation parameters of a 150-pound suitcase bomb

$W\ (lb)$	$HFD\ (ft)$	$HFD\ (m)$	$HFD(mile)$
150	815.2371	248.5479	0.15408

Range(m)	N_{hits}	P_k	Casualty area (m^2)	Lethal area (m^2)	Fatalities from blast primary fragmentation	Casualties from blast primary fragmentation
3	6.192	0.749	21.163	15.849	0.052	0.069
6	1.548	0.292	33.019	9.645	0.031	0.107
8	0.871	0.177	35.490	6.268	0.020	0.115
10	0.557	0.117	36.720	4.294	0.014	0.119
20	0.139	0.031	38.449	1.177	0.004	0.125
25	0.089	0.020	38.664	0.762	0.002	0.126
30	0.062	0.014	38.782	0.532	0.002	0.126
50	0.022	0.005	38.953	0.193	0.001	0.127
80	0.009	0.002	39.012	0.076	0.000	0.127
90	0.007	0.002	39.020	0.060	0.000	0.127
100	0.006	0.001	39.026	0.049	0.000	0.127
200	0.001	0.000	39.044	0.012	0.000	0.127
250	0.001	0.000	39.046	0.008	0.000	0.127
Total expected fatalities and injuries					**0.127**	**1.549**

Table 4.25 Blast fragmentation parameters of a 2000-pound car bomb

$W\ (lb)$	$HFD\ (ft)$	$HFD\ (m)$	$HFD(mile)$
2000	1822.851	555.7473	0.344519

Range(m)	N_{hits}	P_k	Casualty area (m^2)	Lethal area (m^2)	Fatalities from blast primary fragmentation	Casualties from blast primary fragmentation
3	34.855	1.000	28.260	28.260	0.092	0.092
6	8.714	1.000	113.037	113.034	0.368	0.368
8	4.901	0.997	200.410	199.862	0.650	0.652
10	3.137	0.977	306.811	299.786	0.975	0.998
20	0.784	0.611	767.427	468.905	1.525	2.496
25	0.502	0.454	890.065	403.676	1.313	2.894
30	0.349	0.343	968.524	331.932	1.079	3.150
50	0.125	0.140	1100.680	154.331	0.502	3.579
80	0.049	0.057	1151.600	65.992	0.215	3.745
90	0.039	0.046	1158.690	52.786	0.172	3.768
100	0.031	0.037	1163.798	43.135	0.140	3.785
200	0.008	0.009	1180.332	11.092	0.036	3.838
250	0.005	0.006	1182.337	7.123	0.023	3.845
500	0.001	0.002	1185.018	1.789	0.006	3.854
555	0.001	0.001	1185.186	1.452	0.005	3.854
Total expected fatalities and injuries					**7.100**	**40.917**

In line with the theory given in section 3.8.1 and the results obtained from Tables 4.24 and 4.25, it is observed that the area affected by a blast can be viewed as several concentric circles that correspond to the nature of the likely injuries. The severity and complexity of injuries decrease with distance from the explosion but the number of injured increases. The probability that a given target is hit by at least one fragment reduces with distance. The further a target is from the point of explosion, the less likely it is to be impacted by the fragmentation produced. The hit probability is quite high at short distances from the point of detonation and the probability drops steeply as the distance increases.

Since this research considers 3252 as the approximate population density (persons per km^2), the total expected fatalities and injuries from the two explosive weight charges gives an indication of the number of people who might be put at risk from the fragmentation of the bomb. For the 150 lbs. bomb with a lethal radius of 4 m and a 74.9% probability of incapacitation at a radius of 3 m , the fragmentation of a suitcase bomb would approximately affect a total of 3 people within the hazard fragment distance of 248 m or 0.15 mile. For the 2000 lbs. bomb with a lethal radius of 19 m and a 97.7% probability of incapacitation at a radius of 9.8 m, the fragmentation of a car bomb would approximately affect a total of 47 people within the hazard fragment distance of 555 m or 0.34 mile.

The mortality and morbidity data published by Mallonee et al. (1996) on Oklahoma City bombing was scaled to account for the collapse and collateral damage resulting from the two types of bombs studied in this research. We assume St. Benedict Healthcare to have 400 people in the building at the time of the blast. According to the Oklahoma City bombing data records, among the people who were in the Murrah building, a total of 162 persons died as direct result of the blast and 319 persons sustained non-fatal injuries. The calculations of fatal and non-fatal injuries resulting from the 150 lb. and 2000 lb. explosives are based on blast and fragmentation effects of the weapon along with empirically obtained collapse and collateral damage level data of Oklahoma City bombing (Table 3.4). Table 4.26 provides the expected number of fatalities and injuries originating from the explosion source, primary fragments, and the collapse of main and nearby structures.

Table 4. 26 Expected number of fatalities and casualties from the blast

Effects	Fatalities		Injuries	
	$150\ lb$	$2000\ lb$	$150\ lb$	$2000\ lb$
Collapse + Blast	6	90	7	176
Fragmentation	1	7	2	40
Collateral damage	0	0	16	225
Total	**7**	**97**	**25**	**441**

Table 4.26 shows a conservative estimation of the total number of fatalities (D_{BE}) and total number of injuries (I_{BE}) from the two types of bombs, assuming a high-density urban area with a population density of 3252 people km^{-2} .

4.4.2 Mortality and morbidity from acute radiation exposure

Radiation is said to cause deterministic harm if an individual is exposed to radiation and becomes ill as a result. As an example, the dose rate from one curie of ^{137}Cs at one meter is 0.004 $Sv\ hr^{-1}$. Standing next to such a source for a year (8,760 hours) would result in 35 Sv exposure, an amount almost 12,000 times the normal background dose and certainly lethal. However, no victim of an RDD attack using explosively dispersed radioactive material will spend more than minutes or at most hours close to the source of radiation. The most likely ways for an RDD to sicken or kill victims with radiation are stealthy dispersal of radioactive material or shrapnel wounds from the radioactive pellet metal fragments. The risk of death from deterministic effects such as acute radiation syndrome (ARS) is evaluated for embedded high-activity shrapnel from ^{60}Co and ^{192}Ir metal pellets. In an accidental intake of radionuclides (^{60}Co, ^{137}Cs, ^{192}Ir), 10 times greater than their respective allowable limit of intake (ALI), radiation dose from the pathways of ingestion and inhalation is calculated.

We assume that a fragment of ^{60}Co having 0.01% or less of the initially detonated activity (222 TBq) hits and wounds an individual within a blast lethal radius of 3m-15m from the centroid. The probability of developing hematopoietic syndrome (H-ARS) from the calculated dose rate of the embedded fragment was computed by Eq (3.38). The hazard function given in Eq (3.42) was used to model the hazard lethality of H-ARS, where the shape parameter $V_{T,S}$ is 6, the dose rate effectiveness parameter $\theta_{T,S}^{1}$ is 0.1 $Gy\ h^{-1}$, the threshold dose $TD_{T,S}$ is 3 Gy and the dose rate that causes the syndrome in 50% of the population $\theta_{T,S}^{\infty}$ is 4.5 Gy. The relative biological effectiveness ($RBE_{T,R}$) for acute injury from gamma and beta was considered to be unity for all target organs.

The RBE-weighted absorbed dose in organ or tissue, AD_T, was calculated using Eq (3.43). To calculate the equivalent dose rate in $rem\ hr^{-1}$, the shrapnel was assumed to be a cylindrical source with radius of 0.1 m and height of 0.1 m. The volumetric concentration C ($GBq\ m^{-3}$) of uniformly distributed activity was calculated to be 0.116 $GBq\ m^{-3}$. Given the linear absorption coefficient of 3.11 cm^{-1}, the dose rate to an individual from the radioactive shrapnel embedded at a depth of 1 cm is calculated as 10.1 Gy, with a probability of 1 of developing the H-ARS syndrome. In an event of ^{192}Ir shrapnel wound with 1% or less of initially detonated activity (0.55 TBq), the dose from the fragment to an individual is calculated to be 0.72 Gy, with a very low risk or probability of developing the H-ARS syndrome.

Prediction of radiation doses from inhalation and ingestion of 10 times the ALI of ^{60}Co and ^{137}Cs were determined in the highly unlikely case of an acute exposure to the radionuclides from the RDD incident. Radiation dose via the inhalation pathway is determined by the radioactivity concentration in air, particle size, the nuclide present, and the type of radiation emitted. Lung and whole-body radiation dose increase as airborne radioactivity concentrations increases as particle size deceases until the particles are so small that they behave like a gas. A radionuclide with high dose conversion factor per unit activity inhaled is more toxic than one with a low dose conversion factor, and alpha emitting nuclides are more dangerous than others. From an internal dose perspective, alpha emitting radionuclides tend to have lower ALI values. This is demonstrated in the ALI limit for ^{241}Am, where the amount of inhaled radioactivity needed to produce a radiation dose of 0.05 *Sv* (5 rem) to the whole body is 2.96×10^{-8} GBq (0.0008 μCi), as compared to 0.0074 GBq (200 μCi) for ^{137}Cs and 0.0011 GBq (30 μCi) for ^{60}Co.

A large cloud of radioactive particles may be ingested as well as inhaled. People breathing through their mouths because of hard work or excitement can have particles settle in their mouths that are subsequently swallowed. Larger particles settling in the lungs or respiratory passages may be entrained in mucus, swept into the throat, and swallowed. Nervous individuals who bite their fingernails may swallow particles beneath (or on) the nails. Finally, radioactive particles may settle onto gardens or prepared foods (Karam, 2005). When the radioactive material is taken in by inhalation or ingestion or is presented to the skin, a fraction is absorbed and reaches the blood stream. The absorbed material is then distributed to various organs and tissues. The radioactivity is eventually removed from the fluids, organs, and tissues by radioactive decay and by biological processes. The absorption (uptake), distribution, and retention of a radionuclide is estimated from biokinetic models of the elements in humans. The retention rates of the radionuclides given in Eq (3.44) – (3.46) are used to calculate the whole-body burden through characteristics and physical dosimetric models of the transport and absorption of radionuclides in the human body.

Table 4. 27 Retention and dose of ^{137}Cs with time after inhaling 0.074 GBqof radioactive cesium, assuming no medical intervention.

$ALI\ (\mu Ci)$	200	$\Theta_{T,S}\ (Gy-eq]$	4.5
$Inhaled\ Activity\ (\mu Ci)$	2000	V	6
$Inhaled\ Activity\ (Bq)$	*7.40E+07*	$\Theta^{1}_{T,S}\ (Gy-eq]$	0.1
$SEE\ (MeV\ kg^{-1})$	0.006308	$Effective\ half\ life\ (t_{\frac{1}{2}})$	$70\ days$

Days	Retention (Bq)	Dose (AD_T) $(Gy-eq)$	Hazard function $(H_{T,S}(\tau))$	Risk $(P_{T,S})$
1	6.90E+07	5.98E-03	4.4E-17	0.0E+00
2	6.62E+07	1.14E-02	2.1E-15	2.1E-15
3	6.44E+07	1.66E-02	2.0E-14	2.0E-14
5	6.21E+07	2.64E-02	3.2E-13	3.2E-13
10	5.76E+07	4.78E-02	1.1E-11	1.1E-11
25	4.63E+07	8.94E-02	4.9E-10	4.9E-10
35	4.01E+07	**1.03E-01**	1.2E-09	1.2E-09
100	1.56E+07	8.62E-02	3.9E-10	3.9E-10
200	3.66E+06	2.77E-02	4.3E-13	4.3E-13
300	8.58E+05	7.13E-03	1.2E-16	0.0E+00
365	3.34E+05	2.85E-03	5.1E-19	0.0E+00
730	1.68E+03	1.47E-05	9.5E-33	0.0E+00
1095	8.41E+00	7.36E-08	1.5E-46	0.0E+00
1460	4.22E-02	3.69E-10	2.4E-60	0.0E+00
1825	2.12E-04	1.85E-12	3.9E-74	0.0E+00
2190	1.06E-06	9.30E-15	6.2E-88	0.0E+00

Table 4.27 calculates the daily dose rate received by a reference individual weighting 70 kg after inhaling 0.074 GBq (2000 μCi) of radioactive cesium. The estimated internal dose received by the

individual is calculated to be 0.10 Gy after about 35 days of initial intake of 0.074 GBq (2 mCi) of ${}^{137}Cs$. The factor SEE (specific effective energy) is the energy absorbed per unit tissue mass per transformation. The computation of the radiation-absorbed dose (AD_T) from a uniformly distributed gamma emitter within a tissue is given by Eq (4.3) (Cember & Johnson, 2011)

$$\dot{D}(\frac{Gy}{d}) = \frac{q(Bq)\times\frac{1tps}{Bq}\times E\frac{MeV}{t}\times 1.6\times\frac{10^{-13}J}{MeV}\times 8.64\times\frac{10^{4}s}{d}}{\frac{\frac{1J}{kg}}{Gy}} \qquad (4.3)$$

With the maximum estimated dose of 0.10 Gy from the inhalation of soluble ${}^{137}Cs$, assuming no administration of Prussian blue, the risk of developing H-ARS was found to be very low. Table 4.28 shows the estimated dose after ingestion of $10 \times ALI$ of ${}^{137}Cs$ (oral ALI). A value of 0.05 Gy was the maximum dose estimated, 35 days post intake.

Table 4.28 Retention and dose of ^{137}Cs with time after ingesting 0.037 GBq of radioactive cesium, assuming no medical intervention.

$ALI\ (\mu Ci)$	100	$\Theta_{T,S}\ (Gy - eq]$	4.5
$Ingested\ Activity\ (\mu Ci)$	1000	V	6
$Ingested\ Activity\ (Bq)$	*3.70E+07*	$\Theta^{1}_{T,S}\ (Gy - eq]$	0.1
$SEE\ (MeV\ kg^{-1})$	0.006308	$Effective\ half\ life\ (t_{\frac{1}{2}})$	$70\ days$

Days	Retention (Bq)	Dose (AD_T) $(Gy - eq)$	Hazard function $(H_{T,S}(\tau))$	Risk $(P_{T,S})$
1	3.45E+07	2.99E-03	6.82E-19	0
2	3.31E+07	5.71E-03	3.31E-17	0
3	3.22E+07	8.30E-03	3.12E-16	0
5	3.10E+07	1.32E-02	5.03E-15	5E-15
10	2.88E+07	2.39E-02	1.77E-13	1.77E-13
25	2.32E+07	4.47E-02	7.6E-12	7.6E-12
35	2.00E+07	**5.16E-02**	1.8E-11	1.8E-11
100	7.81E+06	4.31E-02	6.09E-12	6.09E-12
200	1.83E+06	1.38E-02	6.66E-15	6.66E-15
300	4.29E+05	3.57E-03	1.95E-18	0
365	1.67E+05	1.42E-03	7.92E-21	0
730	8.38E+02	7.33E-06	1.48E-34	0
1095	4.21E+00	3.68E-08	2.37E-48	0
1460	2.11E-02	1.85E-10	3.78E-62	0
1825	1.06E-04	9.27E-13	6.03E-76	0
2190	5.31E-07	4.65E-15	9.62E-90	0

From Table 4.27 and Table 4.28, it can be seen that after a single intake, the associated radiation dose rates, rapidly reach a maximum and then decrease because of radioactive decay and biological elimination. In the case of continuous, chronic exposure, organ and body burdens continue to build up until a maximum is reached at which the increase is balanced by the loss. The time to reach the maximum varies with the radionuclide and its chemical form. The maximum occurs earlier for radionuclides with short effective half-lives (as determined by radioactive decay and biological retention time). It occurs later for radionuclides with long effective half-lives. Table 4.29 shows the estimated dose received by the individual after an accidental intake of 0.074 GBq (2000 μCi) of ^{60}Co. The maximum (bolded in Table 4.29) for ^{60}Co intake occurs 25 days after ingestion.

Table 4. 29 Retention and dose of ^{60}Co with time after ingesting 0.074 GBq of radioactive cobalt, assuming no medical intervention.

$ALI\ (\mu Ci)$	200	$\Theta_{T,S}\ (Gy - eq]$	4.5
$Ingested\ Activity\ (\mu Ci)$	2000	V	6
$Ingested\ Activity\ (Bq)$	*7.40E+07*	$\Theta^{1}_{T,S}\ (Gy - eq]$	0.1
$SEE\ (MeV\ kg^{-1})$	0.0403	$Effective\ half\ life\ (t_{\frac{1}{2}})$	9.5 $days$

Days	Retention (Bq)	Dose (AD_T) $(Gy - eq)$	Hazard function $(H_{T,S}(\tau))$	Risk $(P_{T,S})$
1	3.70E+07	1.99E-02	1.09E-12	1.09E-12
2	3.12E+07	3.23E-02	4.84E-12	4.84E-12
3	2.76E+07	4.15E-02	2.13E-11	2.13E-11
5	2.27E+07	5.31E-02	8.8E-11	8.8E-11
10	1.70E+07	6.73E-02	2.78E-10	2.78E-10
25	1.27E+07	**8.15E-02**	2.52E-10	2.52E-10
35	1.14E+07	8.02E-02	2.94E-11	2.94E-11
100	7.34E+06	5.60E-02	5.27E-12	5.27E-12
200	5.51E+06	4.21E-02	1.52E-12	1.52E-12
300	4.48E+06	3.42E-02	6.95E-13	6.95E-13
365	3.93E+06	3.00E-02	8.8E-15	8.77E-15
730	1.90E+06	1.45E-02	1.12E-16	0
1095	9.16E+05	7.00E-03	1.41E-18	0
1460	4.42E+05	3.38E-03	1.79E-20	0
1825	2.14E+05	1.63E-03	2.27E-22	0
2190	1.03E+05	7.88E-04	2.88E-24	0

The whole-body retention model described by a function of the form given in Eq (3.46) for elemental ^{192}Ir was used to calculate the estimated dose rate in a human body after an intake of 0.11 GBq (3000 μCi) of radioactive iridium. The maximum of 0.012 Gy was achieved within 3 days of the initial intake. The exposure pathways for the three radionuclides are discussed in the decontamination section.

Acute exposure to high levels of radiation can lead to deterministic radiation effects, which are effects that will occur after a threshold dose is exceeded. The dose results estimated from 10 times the ALI intake of the dispersed radionuclides indicate that the threshold of 4 Gy of H-ARS was not exceeded. The dose from contaminated shrapnel from an explosively driven RDD was calculated to be lethal, given the fragment activity is $> 0.01\%$ of the initially detonated activity of ^{60}Co and ^{192}Ir. Barring the unexpected anomaly scenarios where a first responder or the members of public in the process of evacuation accidentally ingests or inhales high amounts of radioactivity $(1000 \times ALI)$ are likely to be contaminated with potentially serious or lethal whole-body dose.

Based on experiments for an outdoor explosion of an RDD, the plume is likely to pass from the immediate area within ~10 to 15 min, which would reduce the risk of acute inhalation of airborne activity to emergency responders and members of the general public in the area (Harper et al., 2007). Conversely, in a device that produces poor aerosolization, the material could result in dangerous localized hot spot and/or ballistic fragments that might create high external exposure rates.

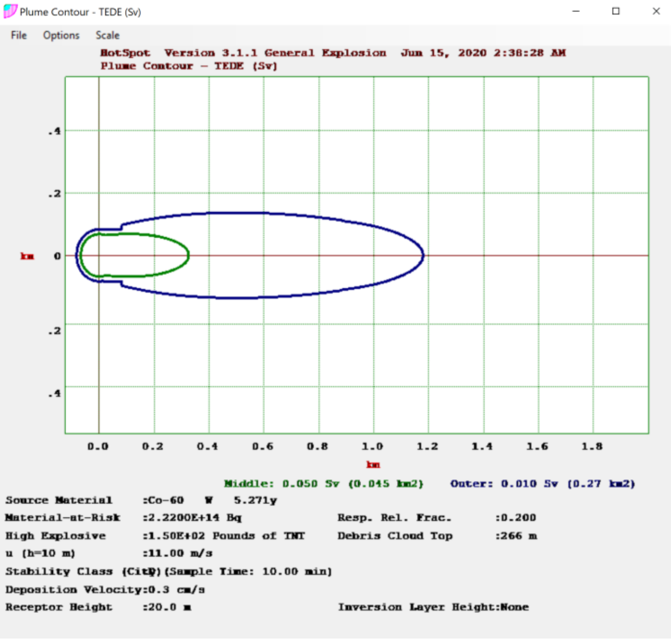
4.4.3 Mortality and morbidity from stochastic effects

Beyond the ARS and the early health effects, long-term health effects of an RDD incident include an increased risk of developing late radiation effects including cancer. The radiological consequences of an RDD bomb detonation in an urban area is assessed by evaluating the total effective dose equivalent (TEDE) received by the exposed population. The TEDE is estimated using the HOTSPOT code. HOTSPOT results can be considered conservative, as it calculates the dose to exposed individuals without any mitigation. In a real situation sheltering and decontamination procedures would reduce the dose received by exposed people significantly. The analysis uses the simplified HOTSPOT urban dispersion model. The weather at the time of the event is assumed to be dry with an average hourly wind speed in Marion county of 11 $m\ s^{-1}$ at 10 meters above ground in the prevailing direction (from south). The detonation height, as mentioned before is assumed to be 20 m. The respirable fraction was assumed to be 0.2 of the airborne fractions. The results are reported in terms of TEDE received by affected persons in the short time following the detonation. No specific exposure assumptions are considered; therefore, HOTSPOT's default settings of 4-day exposure and 10 min sample time are used. The solubility of the nuclide depends on the chemical form. Type “M” was considered for 60Co, type “F” was considered for ^{137}Cs and Type “S” for ^{192}Ir. Table 4.30 lists the parameters that influence the extent of the contamination and, in tun, the effective dose to affected persons.

Table 4. 30 Source term and the main parameters used to perform the HOTSPOT simulation.

	^{60}Co	^{137}Cs	^{192}Ir
Activity	$2.22 \times 10^{14}\ Bq$	$1.07 \times 10^{14} Bq$	$5.55 \times 10^{12}\ Bq$
High Explosive weight	68 kg (TNT)		
Wind speed	11 m/s		
Wind direction	180 (wind from south)		
Atmospheric stability class	D (city)		
Respirable Fraction	0.2		
Receptor height	20 m		
Sample time	10 min		
Inner contour dose	1 *Sv*		
Middle contour dose	0.05 *Sv*		
Outer contour dose	0.01 *Sv*		

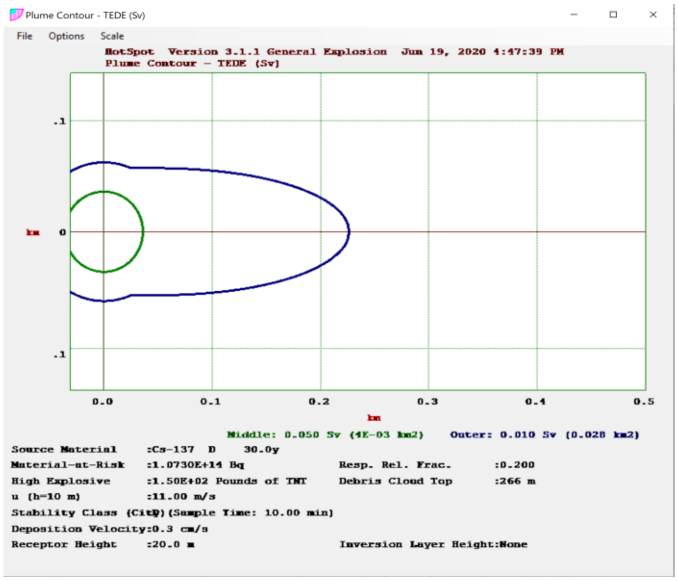
Thresholds are represented in terms of isodose lines, shown in Figure4.3, and Figure4.4. Figures (4.3) -(4.4) show TEDE plume contour plot, where the maximum distances of isodose curves from the zero point downwind are displayed. Area in color red indicates that the maximum TEDE is more than 1 *Sv* , area in color green means maximum TEDE exceeds 0.05 *Sv* and the area in color blue indicates that the maximum TEDE exceeds 0.01 *Sv*.



```
HotSpot  Version 3.1.1 General Explosion  Jun 15, 2020 2:38:28 AM
Plume Contour - TEDE (Sv)

                        Middle: 0.050 Sv (0.045 km2)   Outer: 0.010 Sv (0.27 km2)
Source Material     :Co-60   W   5.271y
Material-at-Risk    :2.2200E+14 Bq              Resp. Rel. Frac.      :0.200
High Explosive      :1.50E+02 Pounds of TNT     Debris Cloud Top      :266 m
u (h=10 m)          :11.00 m/s
Stability Class (CitD)(Sample Time: 10.00 min)
Deposition Velocity:0.3 cm/s
Receptor Height     :20.0 m                     Inversion Layer Height:None
```

Figure 4.3 Plume showing isodose values of TEDE as a function of the distance for ^{60}*Co* RDD blast scenario with 150 lb. explosive.

In the case of ^{60}*Co* RDD bomb explosion (Figure(4.3)), the 0.05 Sv value is exceeded within a distance of 0.33 km downwind (the area is equal to 0.05 km^2) and the maximum TEDE is 0.687 *Sv* at 10 m from the explosion. The inner dose contour value of 1 Sv was not exceeded. The outer dose contour value of 0.01 Sv is reached within a maximum downward distance of 1.2 km (with an area of 0.27 km^2). The dose values were calculated from minimum distance of 0.03 km to a maximum downwind distance of 80 km.



```
HotSpot  Version 3.1.1 General Explosion  Jun 19, 2020 4:47:39 PM
Plume Contour - TEDE (Sv)
```

```
                  Middle: 0.050 Sv (4E-03 km2)   Outer: 0.010 Sv (0.028 km2)
Source Material    :Cs-137  D    30.0y
Material-at-Risk   :1.0730E+14 Bq             Resp. Rel. Frac.     :0.200
High Explosive     :1.50E+02 Pounds of TNT    Debris Cloud Top     :266 m
u (h=10 m)         :11.00 m/s
Stability Class (CitD)(Sample Time: 10.00 min)
Deposition Velocity:0.3 cm/s
Receptor Height    :20.0 m                    Inversion Layer Height:None
```

Figure 4.4 Plume showing isodose values of TEDE as a function of the distance for ^{137}Cs RDD blast scenario with 150 lb. explosive.

In the case of ^{137}Cs RDD bomb explosion (Figure(4.4)), the 0.05 Sv value is exceeded within a distance of 0.05 km downwind (the area is equal to 0.0043 km^2) and the maximum TEDE is 0.084 *Sv* at 10 m from the explosion. The inner dose contour value of 1 Sv was not exceeded. The outer dose contour value of 0.01 Sv is reached within a maximum downward distance of 0.3 km (with an area of 0.028 km^2). In case of ^{192}Ir RDD bomb detonated using the sample explosive amount (150 lb.), none of the dose contour level values exceeded. The maximum TEDE at 10 m was recorded as 0.00058 Sv. Figure (4.5) shows the plume centerline TEDE (Sv), as a function of downwind distance.

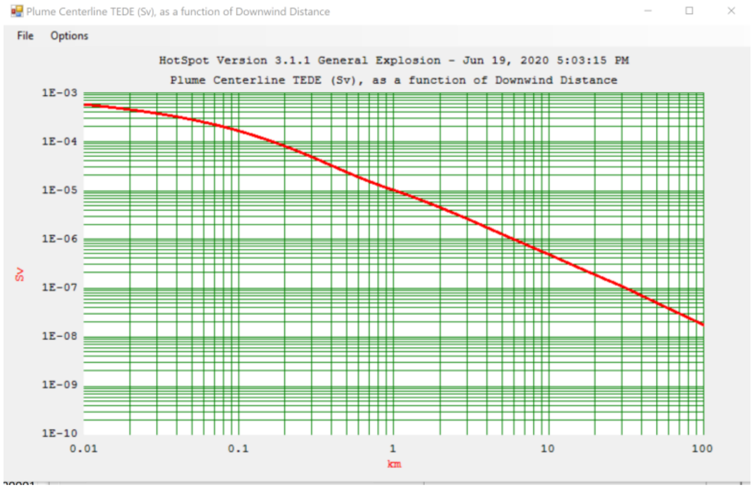


Figure 4.5 Plume centerline TEDE as a function of downwind distance for ^{192}Ir RDD blast scenario with 150 lb. explosive.

It was found that changing the explosive amount to 2000 lb. (907 kg), while keeping the other simulation parameters constant, the TEDE values were lower than the TEDE values obtained for a smaller explosive. This implies that the high explosive weight influences the spread of contamination. HOTSPOT simulations show that the increase in the explosive weight is associated with a reduction of the distance at which the considered limit of dose contour threshold values is reached. This result is not unexpected. In fact, the higher the explosive power, the higher the dispersion of the radionuclide and consequently lower the TEDE and ground deposition. However, it can be observed from Table (4.22) – (4.25), the safe distance and the hazard fragment distance increases from 204 m (68 kg TNT blast safe distance) and 248.5 m (68 g TNT HFD distance) to 483.8 m (907 kg TNT blast safe distance) and 555.7 m (907 kg TNT *HFD* distance). Table 4.31 shows the difference in effective dose values for the two types of high explosive amounts.

Table 4.31 The total effective dose equivalents for 150-pound and 2000-pound explosives at a distance of 30 m from the center of the explosion.

Activity-radionuclides	mSv (68 kg)	mSv (907 kg)
$2.22 \times 10^{14}\ Bq$ (^{60}Co)	440	110
$1.07 \times 10^{14} Bq$ (^{137}Cs)	50	14
$5.55 \times 10^{11}\ Bq$ (^{192}Ir)	0.38	0.072

In case such an event should take place, the general consensus is that the blast effects of the device would cause the largest number of causalities, by far larger than radiation alone.

As mentioned by Biancotto et al. (2020) another parameter that is likely to play a key role in the diffusion of radioactive material dispersed by an RDD is the wind speed. Changing the wind speed from $11\ m\ s^{-1}$ to $5\ m\ s^{-1}$ increases the TEDE by a factor of 4. The radioactive plume generated by the explosion is transported by the wind. The underlying assumption is that radioactivity travels longer distances, and its concentration decreases as the wind speed increases. As a net result, higher the wind speed, shorter the distance at which the TEDE limits are reached. Meteorological conditions may differ significantly between night and day and may even evolve quickly in a very short time. The present analysis assumes the stability class to be constant (stability class "D") during the entire transport. Increasing the instability, the radionuclide concentration is diluted, and the distance at which TEDE thresholds are reached decreases. Past research show that no matter what radionuclide is considered, there is approximately a fourfold increase in the dose when switching from stability class A to F (Biancotto et al., 2020; Yoo et al., 2011).

In the circumstances, where there is no continuous individual record of external exposure or radionuclide intake is available, an exposure pattern must be modeled. To estimate the mortality and the morbidity rates from the RDD incident, the present analysis develops inhalation, ingestion, and exposure pathway scenarios as a function of population density per square kilometers. The TEDE values, respirable time-integrated air concentration values and the ground surface deposition values from the HOTSPOT simulations are used to develop different exposure patterns for the three radionuclides. Given that a low value of the TEDE would be measured at the same distance compared to the case of an explosion by a less powerful device, the only stochastic effects discussed, hereafter, is from a 150-pound bomb and not from a 2000-pound bomb.

The intake from the inhaled radionuclides (^{60}Co, ^{137}Cs, ^{192}Ir) was estimated from the projection of radionuclide concentrations in air ($Bq\ sec\ m^{-3}$) . The average age and gender specific inhalation rate of $2.4 \times 10^{-4} m^3 s^{-1}$ was used in the calculation of risk. Risk coefficients (Bq^{-1}) for inhalation of radionuclides in air are expressed as risk of cancer mortality or morbidity per unit activity intake in the Federal Guidance Report (FGR) No. 13 (U.S. EPA, 1999). The cancer risk associated with the radionuclide intake is calculated as the product of the appropriate cancer risk coefficient and the corresponding radionuclide inhaled. This calculation presumes the risk to be directly proportional to the intake, i.e., it follows a linear, no-threshold (LNT) model (US EPA, 1999). Scaling factor of 1.10 and 1.14 are used for conversion of risk coefficients for the stationary population to more precise risk coefficients for a hypothetical short-term exposure to the current U.S. population. Table 4.32. lists the *FGR 13* risk coefficients (Bq^{-1}) for inhalation, ingestion, and exposure of radionuclides.

Table 4.32 Risk coefficients for inhalation, ingestion and exposure expressed as risk of cancer mortality and morbidity.

	Mortality				Morbidity			
	Inhalation (Bq^{-1})	Exposure (Plane) $m^2 Bq^{-1} s^{-1}$	Tap water ingestion (Bq^{-1})	Food intake ingestion (Bq^{-1})	Inhalation (Bq^{-1})	Exposure (Plane) $m^2 Bq^{-1} s^{-1}$	Tap water ingestion (Bq^{-1})	Food intake ingestion (Bq^{-1})
Co-60	2.32E-09	1.26E-16	2.75E-10	3.88E-10	2.72E-09	1.87E-16	4.25E-10	6.03E-10
Cs-137	2.19E-10	3.96E-20 (Ba-137m 3.12E-17)	5.66E-10	6.88E-10	3.21E-10	4.57E-20 (Ba-137m 4.60E-17)	8.22E-10	1.01E-09
Ir-192	4.24E-17	4.24E-17	1.12E-10	1.62E-10	6.24E-17	6.24E-17	1.99E-10	2.89E-10

Table 4.33 gives the mortality and morbidity risk associated with inhalation of ^{60}Co, ^{137}Cs, and ^{192}Ir as the cloud of the specific detonated radionuclide passes over the population.

Table 4. 33 Mortality and morbidity cancer risk associated with inhalation of ^{60}Co, ^{137}Cs, and ^{192}Ir during the first two days of the RDD explosion

Air concentration $(Bq \sec m^{-3})$	Air concentration $(Bq \sec m^{-3}$	Air concentration $(Bq \sec m^{-3})$	Mortality risk from inhaled nuclide	Morbidity risk from inhaled nuclide	Mortality risk from inhaled nuclide	Morbidity risk from inhaled nuclide	Mortality risk from inhaled nuclide	Morbidity risk from inhaled nuclide
Co	*Cs*	*Ir*	*Co*		*Cs*		*Ir*	
5.80E+08	2.80E+08	1.40E+06	3.11E-04	3.64E-04	9.36E-05	1.37E-04	1.24E-06	1.39E-06
3.00E+08	1.50E+08	7.50E+05	1.61E-04	1.88E-04	4.12E-05	6.03E-05	5.45E-07	6.13E-07
1.50E+08	7.40E+07	3.80E+05	8.04E-05	9.42E-05	2.06E-05	3.02E-05	2.77E-07	3.12E-07
9.40E+07	4.50E+07	2.30E+05	5.04E-05	5.90E-05	1.22E-05	1.78E-05	1.64E-07	1.84E-07
6.40E+07	3.10E+07	1.60E+05	3.43E-05	4.02E-05	8.23E-06	1.21E-05	1.09E-07	1.23E-07
4.80E+07	2.30E+07	1.20E+05	2.57E-05	3.01E-05	5.99E-06	8.78E-06	8.42E-08	9.47E-08
3.80E+07	1.80E+07	9.50E+04	2.04E-05	2.39E-05	4.86E-06	7.13E-06	6.44E-08	7.24E-08
3.10E+07	1.50E+07	7.90E+04	1.66E-05	1.95E-05	3.93E-06	5.76E-06	5.45E-08	6.13E-08
2.70E+07	1.30E+07	6.70E+04	1.45E-05	1.70E-05	3.37E-06	4.94E-06	4.56E-08	5.12E-08
2.30E+07	1.10E+07	5.90E+04	1.23E-05	1.44E-05	2.99E-06	4.39E-06	3.96E-08	4.46E-08
2.10E+07	1.00E+07	5.30E+04	1.12E-05	1.32E-05	2.62E-06	3.84E-06	3.57E-08	4.01E-08
9.80E+06	4.70E+06	2.50E+04	5.25E-06	6.15E-06	1.16E-06	1.70E-06	1.59E-08	1.78E-08
4.20E+06	2.00E+06	1.00E+04	2.25E-06	2.64E-06	4.68E-07	6.86E-07	6.44E-09	7.24E-09
2.50E+06	1.20E+06	6.40E+03	1.34E-06	1.57E-06	2.62E-07	3.84E-07	3.62E-09	4.07E-09
1.80E+06	8.70E+05	4.50E+03	9.64E-07	1.13E-06	1.81E-07	2.66E-07	2.48E-09	2.79E-09
1.40E+06	6.70E+05	3.50E+03	7.50E-07	8.79E-07	1.37E-07	2.00E-07	1.83E-09	2.06E-09
6.30E+05	3.10E+05	1.60E+03	3.37E-07	3.96E-07	5.43E-08	7.95E-08	7.43E-10	8.36E-10
3.00E+05	1.40E+05	7.50E+02	1.61E-07	1.88E-07	2.25E-08	3.29E-08	2.92E-10	3.29E-10
2.00E+05	9.40E+04	4.90E+02	1.07E-07	1.26E-07	1.25E-08	1.84E-08	1.68E-10	1.89E-10
1.40E+05	7.00E+04	3.60E+02	7.50E-08	8.79E-08	8.61E-09	1.26E-08	1.14E-10	1.28E-10

In doses calculated prospectively, intake of each radionuclide is estimated as a product of its concentration in food and tap-water and the quantity of it taken into the body through ingestion. The activity of the radionuclide ingested was assumed to be 1/10000th of the initial activity (A_0) in the environmental medium (Table 4.34). The assessment assumes usage rates of $1.11\ L\ d^{-1}$ of tap water and $2048\ kcal\ d^{-1}$ of food intake for the first 2 days following the explosion. Separate risk coefficients are calculated for ingestion of radionuclides in tap water and ingestion of radionuclides in food. Both sets of coefficients for the three radionuclides are given in Table 4.32. The assessment of intake of a radionuclide is derived from the HOTSOT total effective dose equivalent values. While the coefficients for ingestion are somewhat lower than inhalation, ingestion can be the most common means of entry into the body for ^{60}Co in this assessment. Table 4.34 displays the calculated mortality and morbidity cancer risk per unit activity intake during the first 2 days of ingestion following the RDD explosion.

Table 4. 34 Mortality and morbidity cancer risk associated with ingestion of ^{60}Co, ^{137}Cs, *and* ^{192}Ir during the first two days of the RDD explosion

Activity ingested (Bq)	Activity ingested (Bq)	Activity ingested (Bq)	Mortality risk from ingested food and tap water	Mortality risk from ingested food and tap water	Mortality risk from ingested food and tap water	Mortality risk from ingested food and tap water	Mortality risk from ingested food and tap water	Mortality risk from ingested food and tap water
Co	*Cs*	*Ir*	*Co*		*Cs*		*Ir*	
6.51E+07	1.67E+06	1.00E+05	1.79E-02	2.77E-02	1.15E-03	1.69E-03	1.63E-05	2.90E-05
2.96E+07	7.29E+05	4.49E+04	8.14E-03	1.26E-02	5.01E-04	7.36E-04	7.28E-06	1.30E-05
1.39E+07	3.64E+05	2.12E+04	3.83E-03	5.91E-03	2.51E-04	3.68E-04	3.43E-06	6.11E-06
8.29E+06	2.09E+05	1.27E+04	2.28E-03	3.52E-03	1.44E-04	2.12E-04	2.06E-06	3.67E-06
5.62E+06	1.43E+05	8.46E+03	1.55E-03	2.39E-03	9.82E-05	1.44E-04	1.37E-06	2.44E-06
4.14E+06	1.03E+05	6.35E+03	1.14E-03	1.76E-03	7.10E-05	1.04E-04	1.03E-06	1.83E-06
3.25E+06	8.20E+04	5.02E+03	8.95E-04	1.38E-03	5.64E-05	8.28E-05	8.14E-07	1.45E-06
2.66E+06	6.68E+04	3.97E+03	7.33E-04	1.13E-03	4.59E-05	6.74E-05	6.42E-07	1.15E-06
2.22E+06	5.77E+04	3.44E+03	6.10E-04	9.43E-04	3.97E-05	5.82E-05	5.57E-07	9.93E-07
1.92E+06	4.86E+04	2.91E+03	5.29E-04	8.18E-04	3.34E-05	4.91E-05	4.71E-07	8.40E-07
1.78E+06	4.55E+04	2.64E+03	4.88E-04	7.55E-04	3.13E-05	4.60E-05	4.28E-07	7.64E-07
7.69E+05	1.97E+04	1.19E+03	2.12E-04	3.27E-04	1.36E-05	1.99E-05	1.93E-07	3.44E-07
2.96E+05	7.59E+03	4.76E+02	8.14E-05	1.26E-04	5.22E-06	7.66E-06	7.71E-08	1.38E-07
1.78E+05	4.25E+03	2.62E+02	4.88E-05	7.55E-05	2.92E-06	4.29E-06	4.24E-08	7.56E-08
1.15E+05	2.94E+03	1.77E+02	3.17E-05	4.91E-05	2.03E-06	2.97E-06	2.87E-08	5.12E-08
8.58E+04	2.19E+03	1.32E+02	2.36E-05	3.65E-05	1.50E-06	2.21E-06	2.14E-08	3.82E-08
3.25E+04	8.20E+02	5.02E+01	8.95E-06	1.38E-05	5.64E-07	8.28E-07	8.14E-09	1.45E-08
1.21E+04	3.04E+02	1.85E+01	3.34E-06	5.16E-06	2.09E-07	3.07E-07	3.00E-09	5.35E-09
6.51E+03	1.70E+02	1.00E+01	1.79E-06	2.77E-06	1.17E-07	1.72E-07	1.63E-09	2.90E-09
4.29E+03	1.12E+02	6.61E+00	1.18E-06	1.82E-06	7.73E-08	1.13E-07	1.07E-09	1.91E-09

The possible outcome of radioactive contamination of food and water to a large number of people is highly unlikely in such a radiological attack, because of the large amounts of radioactive material that would be required to reach high levels of contamination in mass-produced or distributed samples. The mortality and morbidity cancer risk and the expected number of casualties from ingestion of radionuclide through food and tap water is conservatively estimated, assuming no evacuation or relocation for 2 days, and assuming no intervention in the consumption levels or establishment of intervention exemption levels for commodities including foodstuffs for 2 days following the RDD attack. Since, St. Benedict Healthcare is situated in an urban area the potential for dose via the radionuclide ingestion pathway is reduced as they use municipal water treatment and are not likely to obtain a large fraction of their food from home-grown vegetables or fruits. The article by Curado et al. (2019) cites the cancer incidence in a cohort directly exposed to ^{137}Cs in the Goiania accident in Brazil to be similar to that of the general population of the municipality of Goiania. After 30 years since the ^{137}Cs accident in Goiania only seven cancer cases were identified in a cohort of 102 contaminated patients. This result was found to not be statistically different from the general population of the municipality.

The *FGR 13* report (US EPA, 1999) also provides numerical factors for use in estimating the risk of cancer from low-level exposure to radionuclides. Risk coefficients for radionuclides expressed in terms of the probability of radiogenic cancer mortality or morbidity per unit time-integrated activity concentration in ground plane $(m^2Bq^{-1}s^{-1})$, for external exposure is given in Table (4.32). As in the internal exposure scenarios, it is assumed that the concentration of the radionuclide in the environmental medium remains constant and that all persons in the population are exposed to that environmental medium for 2 days. The external exposure risk coefficients are based on estimated dose rates for a reference adult male, standing outdoors with no shielding. No adjustments are made in this exposure scenario to account for potential differences with age and gender in the external doses received or for potential reduction in dose due to shielding by buildings during time spent indoors. From Table 4.32, the mortality and morbidity risk coefficients for external exposure to ^{137}Cs distributed on the ground surface are 3.96×10^{-20} and $4.57 \times 10^{-20} m^2Bq^{-1}s^{-1}$ respectively. For ^{137m}Ba the corresponding risk coefficients are 3.12×10^{-17} and $4.60 \times 10^{-17} m^2Bq^{-1}s^{-1}$ respectively. The exposure (time-integrated concentration) for each radionuclide during the assumed 2-day period was calculated using Eq (4.4)

$$Exposure = A_0 \int_0^T exp\left(\frac{-\ln(2)t}{\frac{T_1}{2}}\right) dt = \frac{A_0 T_{1/2}}{ln2}\left(1 - exp\left(\frac{-ln2T}{\frac{T_1}{2}}\right)\right) \qquad (4.4)$$

The growth of chain members in the environmental medium is not considered. For each radionuclide addressed, however, a separate risk coefficient is provided for each subsequent member of the chain that is of potential dosimetric significance. For instance, with *^{137}Cs*, a separate risk coefficient for exposure is provided for ^{137m}Ba to assess the risks from ingrowth of radionuclides in the environment. Cesium-137 forms ^{137m}Ba $(t_{1/2} = 2.552\,m)$ in 94.6% of its decays. Due to the short half-life of ^{137m}Ba, the concentration of *^{137}Cs* on the ground surface was multiplied by 0.94 to calculate the exposure from ^{137m}Ba.

Table 4. 35 Mortality and morbidity cancer risk from exposure to ground deposition from ^{60}Co, ^{137}Cs, and ^{192}Ir during the first two days of the RDD explosion

Ground surface deposition $(kBq\ m^{-2})$	Ground surface deposition $(kBq\ m^{-2})$	Ground surface deposition $(kBq\ m^{-2})$	Mortality risk from ground deposition	Morbidity risk from ground deposition	Mortality risk from ground deposition	Morbidity risk from ground deposition	Mortality risk from ground deposition	Morbidity risk from ground deposition
Co	Cs	Ir	Co		Cs + Ba-137m		Ir	
1.10E+06	5.20E+05	1.40E+06	2.39E-02	3.55E-02	3.55E-06	4.10E-06	1.96E-05	2.88E-05
4.70E+05	2.30E+05	7.50E+05	1.02E-02	1.52E-02	1.57E-06	1.81E-06	8.71E-06	1.28E-05
2.30E+05	1.10E+05	3.80E+05	5.00E-03	7.42E-03	7.52E-07	8.68E-07	4.06E-06	5.98E-06
1.30E+05	6.50E+04	2.30E+05	2.83E-03	4.19E-03	4.44E-07	5.13E-07	2.47E-06	3.63E-06
9.00E+04	4.40E+04	1.60E+05	1.96E-03	2.90E-03	3.01E-07	3.47E-07	1.67E-06	2.46E-06
6.60E+04	3.20E+04	1.20E+05	1.43E-03	2.13E-03	2.19E-07	2.52E-07	1.23E-06	1.82E-06
5.20E+04	2.50E+04	9.50E+04	1.13E-03	1.68E-03	1.71E-07	1.97E-07	9.44E-07	1.39E-06
4.30E+04	2.10E+04	7.90E+04	9.35E-04	1.39E-03	1.44E-07	1.66E-07	7.98E-07	1.18E-06
3.70E+04	1.80E+04	6.70E+04	8.04E-04	1.19E-03	1.23E-07	1.42E-07	6.68E-07	9.83E-07
3.20E+04	1.50E+04	5.90E+04	6.96E-04	1.03E-03	1.03E-07	1.18E-07	5.81E-07	8.55E-07
2.90E+04	1.40E+04	5.30E+04	6.30E-04	9.36E-04	9.57E-08	1.10E-07	5.23E-07	7.69E-07
1.30E+04	6.10E+03	2.50E+04	2.83E-04	4.19E-04	4.17E-08	4.81E-08	2.25E-07	3.31E-07
4.90E+03	2.40E+03	1.00E+04	1.07E-04	1.58E-04	1.64E-08	1.89E-08	8.71E-08	1.28E-07
2.80E+03	1.30E+03	6.40E+03	6.09E-05	9.03E-05	8.89E-09	1.03E-08	5.08E-08	7.48E-08
1.90E+03	9.10E+02	4.50E+03	4.13E-05	6.13E-05	6.22E-09	7.18E-09	3.41E-08	5.02E-08
1.40E+03	6.70E+02	3.50E+03	3.04E-05	4.52E-05	4.58E-09	5.28E-09	2.54E-08	3.74E-08
5.20E+02	2.50E+02	1.60E+03	1.13E-05	1.68E-05	1.71E-09	1.97E-09	9.44E-09	1.39E-08
1.90E+02	9.40E+01	7.50E+02	4.13E-06	6.13E-06	6.42E-10	7.41E-10	3.56E-09	5.23E-09
1.10E+02	5.10E+01	4.90E+02	2.39E-06	3.55E-06	3.49E-10	4.02E-10	1.89E-09	2.78E-09
6.80E+01	3.30E+01	3.60E+02	1.48E-06	2.19E-06	2.26E-10	2.60E-10	1.23E-09	1.82E-09

Tables 4.33 – 4.35 provides the estimates of the average probability of death or the development of a lifetime radiogenic cancer resulting from ingestion, inhalation and external exposures during the 2 days following the explosion. As explained in section 3.10.1, the lifetime cancer risk when multiplied with the population density of the area gives mortality and morbidity estimates from the RDD attack. The number of individuals that would be expected to develop cancer from first two days of continuous exposure to a radionuclide at constant concentration in food, tap water and ground is summarized in Table 4.36.

Table 4.36 Expected number of individuals to develop cancer from first two days of exposure to a radionuclide from the three different exposure pathways.

	Expected Mortality			Expected Morbidity		
	Inhalation	Ingestion	Exposure	Inhalation	Ingestion	Exposure
^{60}Co	0.38	17.26	22.25	0.44	26.68	33.03
^{137}Cs	0.09	1.05	0.00	0.14	1.54	0.00
^{192}Ir	0.00	0.02	0.00	0.00	0.04	0.00

4.4.4 Relative risk and probability of causation.

As discussed in section 3.10.2, the relative risk projection model assumes that following administration of a dose of radiation after some latent period the cancer rate rises in a manner proportional to the underlying cancer risk. Largely as a result of extra years of follow-up in the Japanese atomic bomb survivors, it became clear that the relative risk model fitted the solid cancer data much better than the absolute risk model. For this reason, most scientific committees tend to use the relative risk (RR) model rather than the absolute risk model for projecting solid cancer risks to the end of life. The present analysis uses Eq (3.53) and Eq (3.54) to express risk as the ratio of the rate of cancer among those exposed to the rate among a comparable group of individuals who are not exposed. Equation (3.55) is used to assess if the likelihood of the cause of cancer was from exposure to radiation.

The relative risk and the age-based probability of causation (PC) as a function of distance for the HOTPOT derived total effective dose equivalent values are given in Table 4.37 - 4.39 for radionuclides *^{60}Co, ^{137}Cs and ^{192}Ir,* respectively.

Table 4.37 Relative risk (RR) and probability of causation (PC) as a function of the effective dose equivalent (D) for ^{60}Co

D (Sv)	RR (<age 10)	RR (>age 10)	PC (<age 10)	PC (>age 10)
0.440	1.54	1.17	34.95%	14.70%
0.200	1.24	1.08	19.63%	7.27%
0.094	1.11	1.04	10.30%	3.55%
0.056	1.07	1.02	6.40%	2.15%
0.038	1.05	1.01	4.43%	1.47%
0.028	1.03	1.01	3.31%	1.09%
0.022	1.03	1.01	2.62%	0.85%
0.018	1.02	1.01	2.15%	0.70%
0.015	1.02	1.01	1.80%	0.58%
0.013	1.02	1.01	1.56%	0.51%
0.012	1.01	1.00	1.44%	0.47%
0.005	1.01	1.00	0.63%	0.20%
0.002	1.00	1.00	0.24%	0.08%

Table 4. 38 Relative risk (RR) and probability of causation (PC) as a function of the effective dose equivalent (D) for ^{137}Cs

D (Sv)	RR (<age 10)	RR (>age 10)	PC (<age 10)	PC (>age 10)
0.055	1.07	1.02	6.29%	2.11%
0.024	1.03	1.01	2.85%	0.93%
0.012	1.01	1.00	1.44%	0.47%
0.007	1.01	1.00	0.84%	0.27%
0.005	1.01	1.00	0.57%	0.18%
0.003	1.00	1.00	0.41%	0.13%
0.003	1.00	1.00	0.33%	0.11%
0.002	1.00	1.00	0.27%	0.09%
0.002	1.00	1.00	0.23%	0.07%
0.002	1.00	1.00	0.19%	0.06%
0.002	1.00	1.00	0.18%	0.06%
0.001	1.00	1.00	0.08%	0.03%
0.000	1.00	1.00	0.03%	0.01%

Table 4. 39 Relative risk (RR) and probability of causation (PC) as a function of the effective dose equivalent (D) for ^{192}Ir

D (mSv)	RR (<age 10)	RR (>age 10)	PC (<age 10)	PC (>age 10)
0.380	1.00	1.00	0.05%	0.01%
0.170	1.00	1.00	0.02%	0.01%
0.080	1.00	1.00	0.01%	0.00%
0.048	1.00	1.00	0.01%	0.00%
0.032	1.00	1.00	0.00%	0.00%
0.024	1.00	1.00	0.00%	0.00%
0.019	1.00	1.00	0.00%	0.00%
0.015	1.00	1.00	0.00%	0.00%
0.013	1.00	1.00	0.00%	0.00%
0.011	1.00	1.00	0.00%	0.00%
0.010	1.00	1.00	0.00%	0.00%
0.005	1.00	1.00	0.00%	0.00%
0.002	1.00	1.00	0.00%	0.00%

A median adult age of 34.5 years is used for RR and PC calculations. Although the TEDE values showed an exponential decline in dose from the event epicenter, the PC value showed that individuals within a range of 500 meter or less downwind from the event epicenter had a greater risk of developing a latent cancer. Latency period between exposure and cancer diagnosis is consistent with those accepted as a result of epidemiological studies of radiation exposed populations. It takes at least two years for leukemia and bone cancer and ten years for all other cancers to clinically manifest after exposure. According to the data presented in Table 4.37 – 4.39, it can be observed that higher the TEDE values, higher is the RR for young people (< 10 yrs.), followed by a higher probability of causation. This information can be helpful to prioritize the age groups that would require prompt evacuation from the area, in case of transport restriction or limitation. The results also show that the probability of causation decreases with the increase in age with all dose values. This suggests that older people have a lower probability of tumor development than the younger people. Cobalt-60 with its high energy gammas present the highest relative risk of developing cancer in adults and young people, followed by ^{137}Cs and ^{192}Ir.

4.4.5 Countermeasures

Selection of recommended values of generic intervention levels for urgent protective measures was guided by the IAEA numerical recommendations, presented in Table 3.8 (IAEA, 1994). According to the IAEA, these interventions are ‘generic’ in nature. That is, they are chosen to be reasonable for most situations. Protective actions and other decisions in the first few hours after notification of a radiological terrorism incident will probably have to be made with few field measurements or before data are available. There will be little or no knowledge of the initial quantity of radioactive material and the aerosolized fraction at the time the incident is discovered. The dose boundaries of *(1) Inner perimeter (1 Sv), (2) Middle perimeter (0.05 Sv), and (3) Outer perimeter (0.01 Sv)* are chosen to be the protective action levels in this assessment. It may be appropriate to deviate from these levels if the technical assumptions used here are not valid for a specific situation, or to consider social or political factors.

The suggested countermeasure is evacuation or relocation if the inner perimeter dose level is exceeded. Evacuation during the first week is the suggested countermeasure, given the effective dose equivalent exceeds 0.05 Sv. Both, the IAEA and the EPA recommend sheltering if the effective dose exceeds 0.01 Sv (IAEA, 2005b; U.S. EPA, 2016). In accordance with Harper et al. (2007), the guidelines used in this analysis can also be implemented for varying RDD device designs, such as, the intermediate size source 3700 TBq (100,000 Ci), and the very large source 7400 TBq (200,000 Ci). Table 4.40 gives the range of specific hazard boundaries from the point of release, specific to the radionuclide and the selected dose limit.

Table 4.40 Range of dose contours from the point of release, specific of the radionuclide and the selected dose limit.

	^{60}Co $2.22 \times 10^{14}\ Bq$	^{137}Cs $1.07 \times 10^{14} Bq$	^{192}Ir $5.55 \times 10^{11}\ Bq$
Inner (1 *Sv*)	Not exceeded	Not exceeded	Not exceeded
Middle (0.05 *Sv*)	0.33 km	0.036 km	Not exceeded
Outer (0.01 *Sv*)	1.2 km	0.23 km	Not exceeded

Table 4.40 gives the range of specific hazard boundaries from the point of release, specific to the radionuclide and the selected dose limit. the dose limit of 1 Sv is not exceeded in either of the three radionuclide RDD scenarios. The RDD scenario with ^{60}Co and ^{137}Cs detonation exceed the outer dose limit of 0.01 Sv out to 1.2 km and 0.23 km, respectively. In terms of TEDE (and ground deposition) the effect of ^{60}Co is higher than ^{137}Cs, making ^{60}Co the highest damaging candidate. But, considering the explosive dispersibility it would be difficult to pulverize a hard, tough metal like ^{60}Co compared to the soft, salt powder of *CsCl*.

As noted by Harper et al. (2007), in his outdoor experiment of assessing metal aerosolization, he finds that the metals with material properties (thermal and mechanical) conducive to aerosolization, gets aerosolized greater than 80% (conditional on the sophistication of the device). In the case in which material properties were not conducive to aerosolization, only 0.2% of the original mass was found to be aerosolized, and for metals like ^{60}Co, the majority of the material was found to be dispersed as large fragments. Given that the present analysis uses a 150 lb. bomb, it would be unlikely for it to have sufficient shattering power to pulverize all the radioactive material into a fine powder. In the HOTSPOT simulation run, the study considers the fraction of the aerosolized material that is respirable to be 0.2, assuming that only 20% of the original ^{60}Co pellets gets aerosolized. A reduction in aerosolized material leads to a net increase in the ground shine dose rate for ^{60}Co scenario, due to higher ground deposition. Given that no significant pulverization of the cobalt pellets would occur, they will be ejected as ballistic projectile, posing a significant health hazard if embedded into exposed people (as discussed in section 4.4.2). The ^{60}Co RDD scenario may not present a large area denial due to its inefficient aerosolization; it would still require evacuation, relocation, heavy decontamination and replacement countermeasures. For the purpose of calculation and planning, the current assessment expects at least $0.95\ km^2$ of contamination to the 0.01 Sv dose level from *^{60}Co*, followed by $0.098\ km^2$ for *^{137}Cs* scenario and $0.0031\ km^2$ for *^{192}Ir* RDD scenario.

Due to the physical form of $CsCl$, the effective and homogenous aerosolization of powdered salt may cause the hazard boundary to increase in size. RDD aerosolization experiments have shown that, even if a very large quantity of radioactive material is dispersed, the potential for early health effects is bounded within an area of 500 m in radius from the release point (Harper et al., 2007). It is known that the source used in such an incident had an activity < 370 TBq (10,000 Ci) of any radionuclide, the initial radiation hazard zone boundary can be established at 250 m (NCRP, 2011). Considering the hazard fragment distance (HFD) for a 150 lb. explosive was calculated to be 248 m, a hazard boundary of 250 m seemed reasonable for the radionuclides used in the present analysis. For the sake of simplicity and consistency, the dose (hazard) boundary displayed by *^{60}Co* was considered as an established distance for the countermeasure actions. In general, one could expect a factor of 2 or 3 variation in area with atmospheric conditions, the design of the device, the method of dispersal, and the chemical and physical form of the radionuclide. A radius of ~2 km was assumed as an adequate distance for evacuation purposes, business interruption calculations, property losses and loss of human capital for the three radionuclides studied in this analysis. The study assumes structures within 100 meters of the blast center would be contaminated at a level requiring replacement.

While there is no set international standard for cleanup, the ICRP has stated that the long-term goal should be to achieve levels of residual contamination approaching that which is considered "normal", i.e., $1\ mSv\ yr^{-1}$ (ICRP, 2009). The $1\ mSv\ yr^{-1}$ level is the approximate amount of radiation dose that the public receives from the normal terrestrial background. This international guideline for cleanup has been used at Fukushima and many other past radiological accidents.

The present assessment derives the rate of exposure from the ground deposition values, specific to the radionuclides, obtained from the HOTSPOT simulation. With the surface concentration $C_a\ (Ci\ m^{-2})$ of a gamma emitter whose source strength is Γ (rem per hour per Ci) at 1 m, then the dose equivalent rate at point p, at a distance h along the central axis is given by:

$$\dot{H} = \Gamma \frac{rem\,.m^2}{Ci\,.h} \times C_a \frac{Ci}{m^2} \times \pi \times ln \frac{r^2+h^2}{h^2} \frac{rem}{h} \tag{4.5}$$

The dose rates were calculated at distances 0.03 km to 2 km from a plane radiation source of radius 500 m. Equation (3.56) was used to compute the time required for the dose rate to return to an acceptable level of 1 $mSv\ yr^{-1}$ or 0.02 $mSv\ h^{-1}$ for the three radionuclides *(^{60}Co, ^{137}Cs, ^{192}Ir)*. A 135-day decontamination period was computed for *^{60}Co* RDD scenario. Although, a 26-day decontamination period was computed for *^{137}Cs* RDD scenario, considering the environmental impacts are determined by the fraction of the material that is aerosolized by the device, the *^{137}Cs* device may likely lead to a widespread dispersal. Mindful of *^{137}Cs* device's effective aerosolization, this analysis extends the decontamination period for *^{137}Cs* to a 68-day period (~ half of 135-day period). Since none of the dose values exceeded the dose limit boundaries, the decontamination period for ^{192}Ir was assumed to be a week (~ 7 days).

The National Council on Radiation Protection and Measurements (NCRP) report No. 165 (NCRP, 2011) recommends immediate sheltering followed by delayed, informed evacuation. People who are outdoors in the immediate area should get adequate shelter, and people indoors should remain indoors until the plume of airborne radioactive material has passed. Sheltering during the passage of the plume of airborne radioactive material will lower exposure but sheltering beyond the time could result in an additional exposure if radioactive air concentrations inside the buildings become higher than the outdoor concentrations. Although a wide range of variability is expected, estimates suggest that the concentrations inhaled inside the building could be ~5% of those in the outside environment.

Table 4.35 and 4.36 showed the mortality and morbidity risk of a continuous 2-day exposure to the deposited radionuclide (with no shielding) would result in about 22 latent cancer deaths, assuming an unmitigated exposure to *^{60}Co* within a range of 0.03 km to 2 km downwind from the center of the explosion. Evacuation should be delayed until after the plume passes. The optimal time for evacuation should be within few hours of the explosion, but considering there is a lag from the authorities in building protection factors, routes of exit from the hot zone, and other factors while evacuating; this study considers a maximum of 2-day period for a complete evacuation procedure. It is assumed that all residents and business within 2 km (1.24 miles) of St. Benedict Healthcare would evacuate within 2 days and would remain evacuated for 135 days, 68 days and 7 days for ^{60}Co, ^{137}Cs and ^{192}Ir RDD scenarios, respectively.

The amount of effort required to cleanup radioactive contamination will be a function of how much contamination exists relative to the allowed contamination, which in this case is assumed to be $1\,mSv\,yr^{-1}$. Decontamination factors (DF), in general, are employed to determine the effectiveness of a radiation dose reduction project. A decontamination factor is simply the radiation level prior to application of the process divided by the radiation level after the process is employed Eq (4.6).

$$DF = \frac{Radiation\ Level\ Prior\ to\ Decontamination}{Radiation\ Level\ After\ Decontamination} \tag{4.6}$$

A successful decontamination results in a decontamination factor greater than one. For example, if the radiation level prior to decontamination yields an annual dose of $20\ mSv\ yr^{-1}$ and the cleanup goal is to achieve the “normal” level of $1\ mSv\ yr^{-1}$, then the $DF = 20$. Past radiological accidents, particularly those involving ^{137}Cs, show that the actual DF’s achieved are much lower than the values obtained in lab testing or on conditions that do not reflect realistic conditions of a RDD scenario. Cesium-137 is particularly difficult to decontaminate because of its chemistry. It is known to chemically bond to many common building materials. Once on the surface it will also diffuse down into the material from that even surface removing technologies such as scabbling will not be completely effective. The data form Fukushima indicate that even the surface removing technologies when applied to residential areas were only able to achieve a DF of around 2-3 (Connell, 2017).

A DF of 2-5 is considered relatively light decontamination, a moderate DF is between 5 and 10, and a heavy decontamination (requiring demolition) would have a DF >10. Reichmuth et al., (2005) derives the decontamination costs of a given area from the relative level of economic development or financial investment that has been made in the area of concern. They develop unit cost factors $\$\ km^{-2}$ for cleanup of areas having different levels of population density; population density being used as a surrogate for economic activity, as described in section 3.11. St. Benedict Healthcare, situated in Marion county falls in the high-density urban zone with a population density of $3252\ people\ km^{-2}$, requiring a DF greater than 10 to remediate to the required cleanup standard as per Table (3.9).

4.4.6 Human Capital Economic Losses: Value of Statistical Life (VSL), Injuries and Disabilities

The Economic Loss consequence severity value (C_{EL}) is a function of loss of life consequences (human capital loss), decontamination cost, evacuation cost, business interruption cost, lost household income and impaired real estate value that is defined in Eq (3.64) and Eq (3.65). Each of these costs are estimated using economic statistics and reasonable assumptions about the St. Benedict RDD scenario. The principles of Cost Benefit Analysis (CBA) are followed to ensure that the costs are appropriately defined, e.g., the cost of lost household income is included in C_{EL} despite the fact that unemployment insurance would compensate the wage earners (Boardman, 2011). See section 3.12 for a more detailed discussion of the CBA methodology.

The theoretical reasons for using VSL for the valuation of loss of life consequences are given in section 3.12. There are many competing VSL estimates for the U.S. and other countries, and VSL researchers have not reached a consensus that any single VSL estimate should be used universally. The U.S. Department of Transportation and Viscusi & Masterman (2017) both recommend a Value of Statistical Life (VSL) of $9.6 million, and our review of the literature found that this VSL value is credible, widely supported by VSL researchers, and suitable for use in the PFRI. Under the VSL methodology, the economic value of deaths for the purpose of a risk informed security policy would be computed as the product of the total number of deaths from a scenario and the VSL. Multiplying the deaths estimated from blast effects, cancers, and ARS caused by the RDD attack by the VSL of $9.6 million yields a loss of life consequence value of $67.2 million.

The cost of injuries is computed as the sum of the costs in the following injury cost categories: first response, acute care for outpatient injuries, acute care for injuries requiring hospitalization, and long-term care. A cost model developed from studies of the actual costs of medical care in the response to the Oklahoma City bombing of April 19, 1995 is used to determine the average cost of medical care for each injury cost category (Shariat et al., 1998). The actual average costs for each injury cost category are known for the Oklahoma City bombing, and these average costs are adjusted to year 2020 dollars with the Consumer Price Index for All Urban Consumers: Medical Care in U.S. City Average published by the Bureau of Labor Statistics (U.S. Bureau of Labor Statistics, 2020). The average cost found for an injury cost category is multiplied by the estimated number of injuries falling under that category to obtain the total cost for the category. The total cost of injuries is the sum of the total costs for each injury cost category.

Shariat, Mallonee & Stidham (1998) found the proportion of Oklahoma City bombing injuries in each injury cost category and the average cost of treatment for each injury cost category. As a simplifying assumption for the hypothetical St. Benedict RDD scenario, the distribution of injuries by injury cost category resulting from the RDD attack on St. Benedict healthcare is assumed to be identical to the known distribution of injuries for the Oklahoma City bombing. The Oklahoma City bombing's injury pattern is typical of terrorist bombings, and data collected from studies of the injuries and damage to buildings is suitable to build structural engineering models of progressive building collapse (Mallonnee et al., 1996). For 25 injuries due to blast effects estimated for the St. Benedict RDD scenario, a total cost of injuries of $1.19 million was found.

A rate of permanent disability among the injured of 2%, which is approximately the rate observed for the Oklahoma City bombing, is assumed for the St. Benedict RDD scenario (Shariat et al., 1998). The estimated number of permanent disabilities was multiplied by the lifetime expected income forgone for a typical worker in Marion County. The lifetime expected income model for Marion County estimates the total future income lost for a permanently disabled victim adjusting for the age distribution and work force participation rate. For an estimated 0.58 permanent disabilities among the injured, a cost of permanent disabilities of $697,028 was found.

4.4.7 Economic loss - Decontamination Cost

The response to an RDD attack would incur costs from the evacuation of all residents within a 2 km radius of the blast centroid, the decontamination process, and the replacement of some contaminated structures. An evacuation zone with a 2 km radius is assumed for all St. Benedict RDD scenarios, and the duration of the evacuation would be identical to the decontamination time. The size of the decontamination zone would vary for each scenario and would typically be significantly less than the size of the evacuation zone. The zone immediately surrounding the blast centroid where structures would be replaced also varies in size with each scenario. The decontamination times also differ for each RDD scenario.

Evacuation cost is computed as the sum of transportation cost, housing cost, and other living expenses for the population to be evacuated from the contaminated zone. A roundtrip transportation cost of $200 per evacuee is assumed, which is roughly the per evacuee cost of charter bus transportation. The housing cost is assumed to be zero due to the availability of public buildings and red cross facilities to house the evacuees. The Indiana Federal per diem rate of $41.25 is assumed as the daily cost of other living expenses for the evacuees (U.S. GSA, 2019).

Decontamination cost is computed by multiplying the surface area of the contaminated zone as determined by the RDD blast and plume models by cost of $2.7 billion per square kilometer for high density urban zones found by Reichmuth et al. (2005). An appropriate replacement cost rate is $6.6 billion per square kilometer, and this replacement cost rate is multiplied by the area of the zone contaminated at a level requiring the replacement of all structures to obtain the total replacement cost.

4.4.8 Economic Losses to Businesses, Workers, and Real Estate

According to the Reference USA Database (2019), firms operating in the evacuation zone for the St. Benedict RDD scenario have a total annual gross revenue of $15.4 billion, so the cost of business interruption was estimated to be $42 million per day during the evacuation period.

A lifetime expected income model for the population of Marion County was used to estimate the total cost of lost income to persons who would become unemployed as a consequence of the RDD attack. The lifetime expected income model adjusts for age and the workforce participation rate to estimate the total income for any large group of people working in Marion County. The number of employees working at locations within the 2 km radius evacuation zone is about 158,025 (Reference USA, 2019). The evacuation zone contains many corporate offices and government agencies, and it is located near the Indiana state capitol. It was assumed that all workers whose job sites are within the evacuation zone would remain unemployed during the entire decontamination period. It is likely that a significant fraction of those assumed to remain unemployed would actually find new jobs during the decontamination period, and estimating the number of workers who would find new jobs is a topic for future research to enhance the PFRI model.

The impairment to real estate valuation is computed by multiplying the total value of real estate in the contaminated zone by a 15% RDD real estate impairment rate found by Giesecke et al. (2001). The Marion County Assessor’s office provided a data set with the assessed values of property for each parcel within a 2 km radius of the blast centroid. The impairment of real estate value was found to be $531 million for each RDD attack scenario. The decontamination times range from seven to 135 days, so a constant value for real estate impairment would be inconsistent with the assumption of rational behavior by economic agents. It was assumed that an irrational radiological stigma having little relation to the true scope of damage to physical assets and lasting one year or more following an RDD attack would cause most of the impairment to real estate value.

Giesecke et al. (2011) found from survey results that the majority of consumers would avoid doing business in the area affected by an RDD attack during the first year following the attack, with about 80% of consumers willing to resume normal activity in the affected area within 3 years of the attack. Normal levels of investment might not resume in the affected area for up to five years after the RDD attack, with the impact of radiological stigma on consumer behavior not fully attenuating until up to ten years later. Giesecke et al. (2011) found that the indirect or second order economic consequences of an RDD attack could be up to 14.9 times the direct economic consequences that are estimated in the PFRI economic model. For the ^{60}Co scenario given below in Table 4.49, the multiplier of 14.9 for indirect economic consequences would yield total economic consequences of $106.8 billion. However, Giesecke et al. (2011) note that economic relief measures and adaptive strategies by corporations could significantly reduce the indirect economic consequences multiplier. Thus, an indirect economic consequences multiplier of 14.9 would seem to reflect a worst-case outcome, not the most likely outcome. And an indirect economic consequences multiplier for an RDD attack in Marion County has not been assessed as of this writing.

The choice to focus on direct economic consequences in the PFRI economic model faces a trade-off between the advantages of offering a known lower bound on economic consequences in a model that is relatively accessible to healthcare professionals and other policymakers and the disadvantage of potentially significantly understating the total economic consequences of an RDD. Possibly, an accurate global macroeconomic forecast of RDD attack indirect economic effects is impossible, and such a forecast may not be necessary for the PFRI to be useful for risk management at the facility level, which is the primary intended use of the PFRI. Additional sophisticated macroeconomic modeling is a subject for future interdisciplinary research in the development of the PFRI.

Table 4.41 Economic loss consequence estimates of St. Benedict Healthcare RDD scenarios

Economic Loss Consequence				
Economic Consequence		**Amount of Loss**		
		^{60}Co	^{137}Cs	^{192}Ir
Decontamination Time		135 Days	68 Days	7 Days
Decontamination Area		0.951 Sq. Km.	0.098 Sq. Km.	0.00314 Sq. Km.
Loss of Human Capital				
	Loss of Life	$67,200,000.00	$67,200,000.00	$67,200,000.00
	Disabilities	$697,028.13	$697,028.13	$697,028.13
	Injuries	$1,185,490.06	$1,185,490.06	$1,185,490.06
Decontamination				
	Cost of Decontamination Services	$2,567,700,000.00	$264,600,000.00	$8,478,000.00
	Cost to Replace or Rebuild Contaminated Structures	$2,072,400.00	$2,072,400.00	$0.00
Evacuation		$235,730,393.20	$122,794,337.00	$19,971,957.47
Business Interruption				
	Direct Revenue Effects	$2,196,179,321.18	$1,106,223,658.08	$113,875,964.80
Lost Household Income				
	Direct Loss for Workers in Contaminated Zone	$1,565,270,196.29	$788,432,395.17	$81,162,158.33
Wealth Effects				
	Real Estate Impairment	$531,303,116.76	$531,303,116.76	$531,303,116.76
Total Economic Loss		**$7,167,337,945.62**	**$2,884,508,425.20**	**$823,873,715.56**

Table 4.41 shows that the economic consequences of the worst scenario, *^{60}Co,* are about 8.7 times the economic consequences of the best scenario, ^{192}*Ir*. The *^{60}Co* scenario involves a significant decontamination period, 135 days, and the decontamination of a densely populated urban zone of nearly one square kilometer. By contrast, the ^{192}*Ir* scenario entails a mere seven days of decontamination for a relatively small zone of only 3,140 square meters. At an economic consequence of $823 million, the ^{192}*Ir* scenario has significant economic consequences despite the small area affected and short decontamination time. Suppose an RDD attack results in a bomb detonation but is later found to require zero decontamination due to a failure in the execution of the attack. Despite the non-existent radiological impacts of a "dud" RDD device explosion, the symbolic, fear spreading effects of such an attack would be likely to elicit a radiological stigma with large economic effects if an evacuation lasting multiple days is triggered before a site assessment concludes that decontamination and evacuation is unnecessary.

4.4.9 The calculations for C_{LL} *and* C_{EL}

The calculations for the life loss consequence variable and the economic loss consequence variable were performed for the three radionuclide hypothetical detonations, independently.

The loss of life consequence variable

The variable C_{LL} is defined as the loss of life variable which includes the total fatalities (mortality) and total injuries (morbidity) associated with the executed threat. The blast model for a 150 lb. bomb provided the expected number of deaths and injuries resulting from the explosion source, primary fragments, and the collapse of the main and nearby buildings (Table 4.26). The total expected number of deaths (7) and the total expected number of injuries (25) from the explosion is assumed to be constant for the three radionuclides (*^{60}Co, ^{137}Cs, and ^{192}Ir*) RDD scenario. It is well known that the deterministic effects affect the functioning of tissues and organs with a severity that increases with dose. As discussed in section 4.4.2, a dose of 4.5 Gy (450 rad) was taken as a threshold of developing the hematopoietic syndrome. The results presented in sections 4.4.2 and 4.4.3, show that the effective dose values for either of the three radionuclide RDD scenarios do not exceed the dose threshold for deterministic effects. Possible exceptions, however, may include an inadvertent ingestion or inhalation of radioactive material or a lethal dose from a contaminated shrapnel from an explosively driven RDD. The probability of cancer incidence, or mortality per unit intake or unit exposure was calculated for the given population associated with the exposure.

In the postulated RDD scenarios, the results from Table (4.40) showed that the effective dose values did not exceed the 1 Sv inner ellipse boundary line. Assuming a continuous 2-day exposure (time-integrated concentration) to the detonated radionuclide, a 2-day ingestion of contaminated (total dietary) food and tap water intake, and a continuous inhalation of the contaminated air over a 2-day period, the estimated radiogenic cancer mortalities and morbidities of the population exposed were calculated for the three hypothetical radionuclide scenarios. Table 4.42 summarizes the total fatalities and casualties from the blast and radiation effects.

Table 4.42. Total expected mortality and morbidity from the hypothetical radionuclide RDD scenarios.

	Expected mortality	Expected morbidity
^{60}Co	48.32	85.15
^{137}Cs	9.57	26.67
^{192}Ir	8.02	25.04

The fatalities and morbidity values from Table 4.42 are used in Eq (3.57) to calculate the C_{LL} value. The population density for all three RDD detonation scenarios is assumed to be 3252 $people\ km^{-2}$. The C_{LL} for St. Benedict Healthcare, calculated for the three hypothetical RDD scenarios is given in Table (4.43).

Table 4.43 The life loss consequence severity variable for the three hypothetical RDD scenarios.

	^{60}Co	^{137}Cs	^{192}Ir
Mortality from blast effects (D_{BE})	7	7	7
Mortality from ARS (D_{ARS})	1.43	1	0
Mortality from cancer risk (D_{cancer})	39.89	1.14	0.017
Morbidity from blast effects(I_{BE})	25	25	25
Morbidity from ARS (I_{ARS})	0	0	0
Morbidity from cancer risk (I_{cancer})	60.15	1.67	0.045
Life loss consequence variable (C_{LL})	0.0012	0.00033	0.0003

According to the results presented, the hypothetical RDD detonation scenario with ^{60}Co gives the highest C_{LL}value relative to ^{137}Cs and ^{192}Ir. Given the high photon energies of ^{60}Co, high specific activity (relative to ^{137}Cs), and relatively high detonated activity amount 222 TBq (6000 Ci), a high C_{LL} of 0.0012 is not an unexpected result. Cobalt and Iridium are primarily a localized groundshine problem, and cesium could be either a groundshine or inhalation problem depending on the device design.

The economic loss consequence severity variable

As seen from section 4.4.6, an RDD incident would be expected to create significant economic consequences. In order to derive the economic loss consequence severity variable C_{LL}, an economic evaluation taxonomy is established that determines the net present value of the direct monetary loss across the six broad categories of economic sectors, including business interruption, loss of household income, property damage, decontamination, evacuation and loss of human capital. Each economic variable in Table 4.43 represents the state of economy for "before" (B_i) and "after" (A_i) the RDD incident. Reading across the rows of Table 4.43 illustrates a single economic sector's (variable) "before" and "after" attack values and reading down the columns of the Table 4.43-4.45 shows the dollar impact between the economic sectors.

Table 4.44 Economic impact estimates before and after the ^{60}Co RDD incident.

	^{60}Co RDD scenario			
Economy sectors (variables)	Before ($)	After ($)	B_i	A_i
Business interruption	5.94E+09	3.74E+09	0.75	0.49
Household income	1.09E+09	6.90E+08	0.14	0.09
Wealth effects (Property value)	5.31E+08	4.52E+08	0.07	0.06
Decontamination and replacement costs	3.85E+08	2.57E+09	0.05	0.33
Evacuation costs	4.71E+07	2.36E+08	0.01	0.03
Loss of human capital	6.91E+07	0.00E+00	0.01	0.00

Specific to the radionuclide detonated, several shutdown scenarios were analyzed ranging from 7 days for ^{192}Ir, 68 days for ^{137}Cs and 135 days for ^{60}Co. Estimates of the business interruption values are based on the gross revenue in the affected region "before" the RDD attack, followed by 10% reduction of assumed business activity "after" the RDD attack. In addition, the property area in the plume area upwind and downwind were estimated to drop by 25% during the first year following the attack. A default assumption of 135-day closure for businesses and the loss of household income, as a result was made for the three radionuclide RDD scenarios. The decontamination cost was found to be the higher for ^{60}Co than ^{137}Cs and ^{192}Ir. As mentioned previously, the cleanup of ^{137}Cs would be difficult, given the chemistry of cesium to bond to many common building materials. As demonstrated by the accident in Goiania, Brazil (IAEA, 1988), the dispersion of even relatively limited amount of ^{137}Cs in the form of a powdered salt can lead to significant contamination of the area. It can, therefore, be subjectively argued that ^{137}Cs RDD scenario may require heavy decontamination to remove or reduce the contaminated area to an acceptable level of radionuclide contamination, warranting longer clean up days and higher decontamination costs. Table 4.53 and 4.54 display the economic loss estimates for ^{137}Cs and ^{192}Ir RDD incident.

Table 4. 45 Economic impact estimates before and after the ^{137}Cs RDD incident.

	^{137}Cs RDD scenario			
Economy sectors (variables)	Before ($)	After ($)	B_i	A_i
Business interruption	3.32E+08	2.09E+08	0.18	0.06
Household income	5.51E+08	3.47E+08	0.31	0.09
Wealth effects (Property value)	5.31E+08	4.52E+08	0.30	0.12
Decontamination and replacement costs	3.85E+08	2.57E+09	0.21	0.69
Evacuation costs	2.46E+07	1.23E+08	0.01	0.03
Loss of human capital	6.91E+07	0.00E+00	0.04	0.00

Table 4. 46 Economic impact estimates before and after the ^{192}Ir RDD incident.

	^{192}Ir RDD scenario			
Economy sectors (variables)	Before ($)	After ($)	B_i	A_i
Business interruption	3.08E+08	1.94E+08	0.22	0.19
Household income	5.51E+08	3.47E+08	0.40	0.34
Wealth effects (Property value)	5.31E+08	4.52E+08	0.38	0.44
Decontamination and replacement costs	1.27E+06	8.48E+06	0.00	0.01
Evacuation costs	3.99E+06	2.00E+07	0.00	0.02
Loss of human capital	6.91E+07	0.00E+00	0.05	0.00

Under the 2007, Terrorism Risk Insurance Act (TRIA) (Thomas, 2016), terrorism insurance program requires that commercial property and casualty insurers offer terrorism coverage in the policies they are selling. According to the TRIA, for a terrorism loss to be covered by the program, the event giving rise to the loss must be certified as an act of terrorism by the Secretary of the Treasury in consultation with the Secretary of Homeland Security, and property and casualty insurance losses from the event must exceed $5 million. For an insurer to receive any benefits under the program, insurance industry losses from the terrorism event must exceed $200 million in 2020 dollars. Since all three radionuclide RDD scenario exceeds the $100 million dollar limit (Table 4.41) put forth by the TRIA program, the study assumes that St. Benedict Healthcare would be responsible for 20% of the cost and the facility would receive Federal assistance for the remaining 85% of the total costs. The dollar amount displayed for decontamination, replacement, and evacuation cost in the "before" column of the RDD attack reflects the 15% and 20% deductible amount, respectively, owed by the insurer (St. Benedict Healthcare) (Table 4.44, 4.45, 4.46).

Equation (3.65) is used to calculate the economic loss consequence severity value (C_{EL}) for the three radionuclide RDD incidents. The net consequence value (C_{net}) was also calculated for the three RDD scenarios (Eq (3.66)). Table 4.47 displays the C_{LL}, $C_{EL}$and C_{net} values for ^{60}Co, ^{137}Cs and ^{192}Ir RDD incident scenarios.

Table 4.47 Loss of life, Economic loss and net consequence loss estimates for ^{60}Co, ^{137}Cs and ^{192}Ir RDD incident scenarios.

	^{60}Co	^{137}Cs	^{192}Ir
C_{LL}	0.0012	0.00033	0.0003
C_{EL}	0.54	0.50	0.41
C_{net}	0.27	0.25	0.2

The C_{LL} values were found to be much lower than C_{EL}, presenting RDD incident as an economic weapon than a weapon of mass kill.

4.5 The PFRI for St. Benedict Healthcare

As discussed in sections 3.15, the potential facility risk index (PFRI) expresses the risk unique to the facility. It mathematically represents the triple input of threat, vulnerability, and consequences. A numeric score is allocated to each input. Assuming terrorist adversaries are utility maximizers, the maximum expected utility of 1.16, presented by the terrorist adversary RF, choosing to attack and sabotage ^{137}Cs is chosen as the threat component. The low locational vulnerability value of 0.006 implies St. Benedict Healthcare is relatively safe and less vulnerable to crime or other natural hazards. The minimum value of nuclear security culture, shown by Z_{tech}, was used to avoid masking the weakness that would contribute most to the vulnerability of the facility. The locational vulnerability value along with the nuclear security culture value form the vulnerability component of the PFRI model. The highest net consequence value (C_{net}), obtained assuming a hypothetical ^{60}Co RDD scenario event, shaped the consequence component of the PFRI model.

The PFRI index result for St. Benedict's calculated using Eq (3.67) is:

$$PFRI = e^{[1.16\times(0.006+(1-0.58))\times 0.27]} = 1.14$$

The resulting PFRI of 1.14 quantifies St. Benedict Healthcare facility as a "very low risk". The heatmap chart shown in Figure(4.6), graphically represents different levels of risk as a product of threat, vulnerability, and consequence. The chart identifies a numeric scale of 1 to 10 highlighting qualitative/verbal scale from "very low risk" to "very high risk". The green band in the heatmap represents "very low risk" to "low risk" (acceptable risk, no action needed). The yellow band represents "low moderate risk" to "high moderate risk", meaning if the risks fall into this zone then further analysis might be required to determine what action (if any) needs to be taken. The red band signifies "high risk" to "very high risk", requiring immediate action and response towards mitigating threat by enhancing security features, improving nuclear security culture or by minimizing consequences via adapting alternate technologies. The threat input scale can range from very low (0.1) to very high (1.5), the locational vulnerability input can range from very low (0.001) to very high (0.9), the cultural input could range from very good (0.9) to worse (0.1), and the consequence input can range from very low (0.1) to very high (1.5) to obtain a PFRI on the scale of "very low" (1) to "very high" (10).

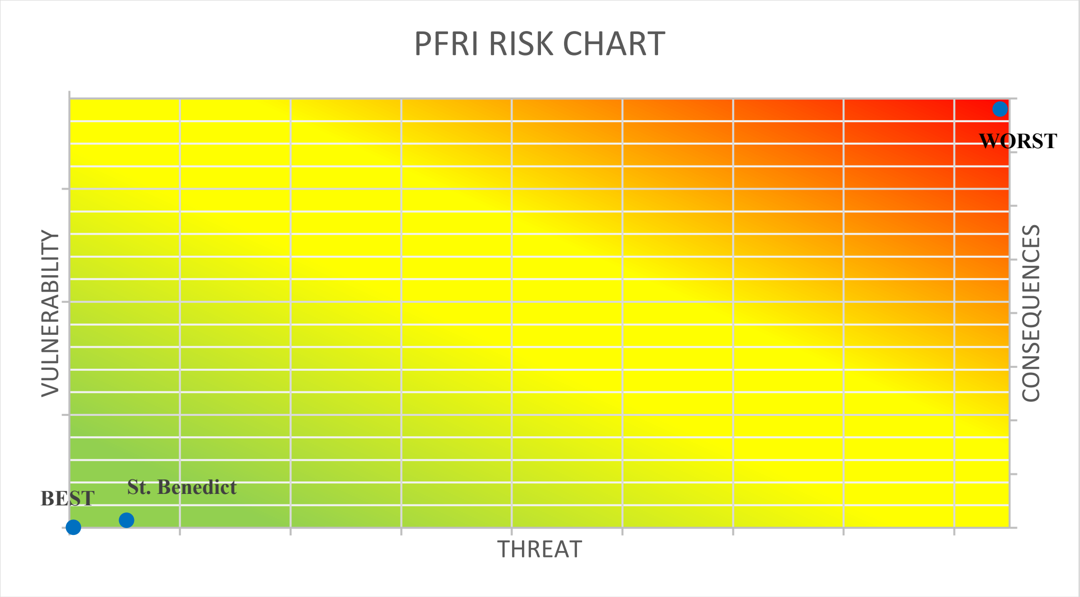


Figure 4.6 The St. Benedict Healthcare facility risk on the PFRI chart

The St. Benedict Healthcare score is shown in the PFRI risk chart given in Fig. 4.6. The threat component had the highest score due to the overall success probability of theft of the blood irradiator asset (^{137}Cs), the consequence component of the PFRI is relatively low for a high density urban region, due to low loss of life and a moderate economic consequence. The vulnerability component gives a low score due to minimal natural hazards and a moderate score for nuclear security culture. A sensitivity analysis of the PFRI may be performed to assess the reduction in risk with respect to the changes and improvements in the security system. According to a PFRI sensitivity analysis of St. Benedict Healthcare, improvements in nuclear security culture related to preventing insider threat yield the largest risk reduction. A cost-benefit analysis could determine whether nuclear security culture upgrades would reduce the PFRI score enough to justify the cost. Implementing improved security protocols and conducting workforce training are some recommendations towards reducing the PFRI score of a facility. The PFRI methodology is a useful starting point for any healthcare facility risk assessment, and it is a valuable input to facility decision makers considering potential investments in security upgrade

CHAPTER 5. RISK CODE TOOL

5.1 The PFRI (GUI) tool

This chapter presents the design of a graphical user interface (GUI) MATLAB program to calculate the potential facility risk index. The PFRI GUI tool is created to provide the facility licensee decision makers with a fast, facility-based risk assessment apparatus for evaluating RDD incident at a facility. The program and the risk metric can also be used for security analysis of the facility handling radioactive materials. The PFRI GUI tool involves evaluating the threat component, the vulnerability component, and the consequence component of the facility risk. The code utilizes the theory and methodology discussed in the previous chapters to estimate the risk of the facility accurately and efficiently to an RDD incident.

Matrices and arrays in general are the heart of MATLAB since all data in MATLAB are stored in arrays. Besides common matrix algebra operations, MATLAB offers array operations that allow one to quickly manipulate sets of data in a wide variety of ways. MATLAB offers programming features similar to those of other computer programming languages. MATLAB also offers an application development tool. This combination of array data structures, programming features, and GUI tools makes MATLAB an extremely powerful tool for solving problems in many fields. The PFRI user interface provides a point of contact or method of interaction between a licensee official and a computer program. It creates an interactive demonstration of the risk analysis method. The main advantage of creating the PFRI tool is to let the user have the ability to use a function over and over again, by using menus, buttons or text boxes as input methods.

5.2 Using the PFRI (GUI) tool

This section steps through an example of the St. Benedict facility risk model to highlight some of the features of the PFRI (GUI) tool.

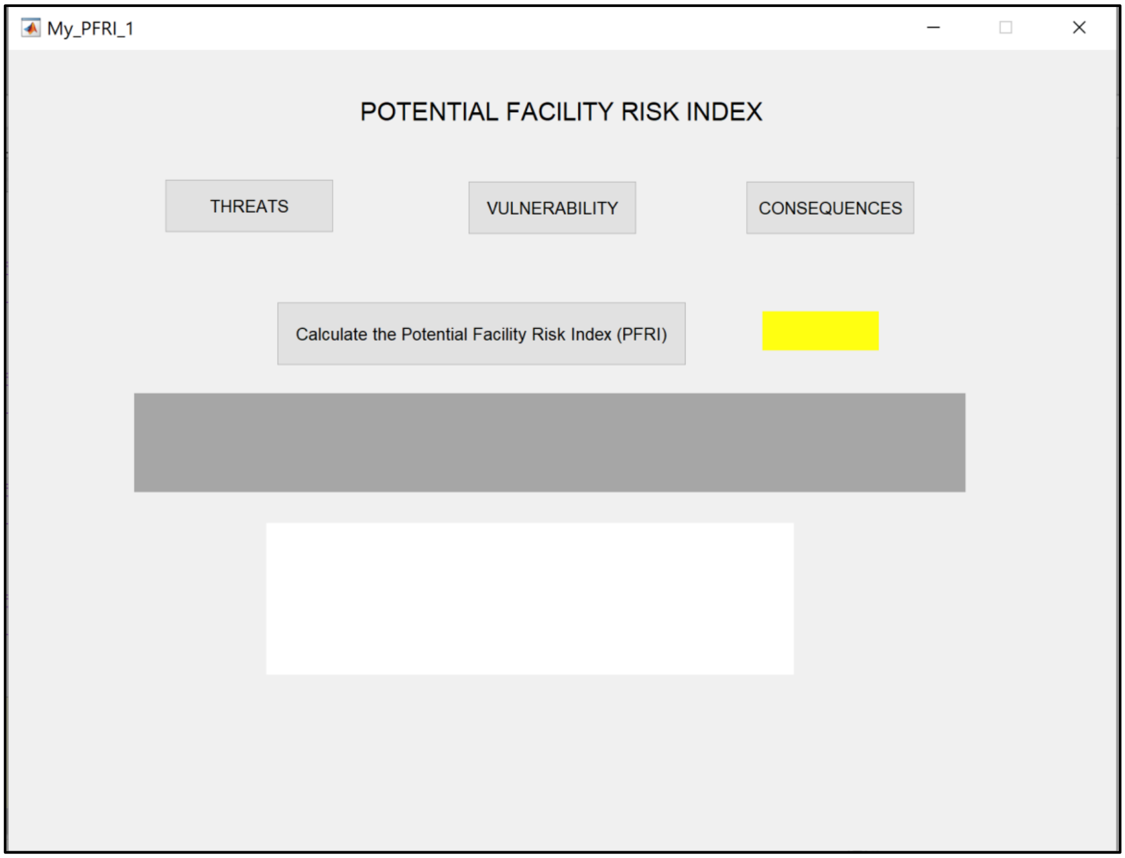

My_PFRI_1
POTENTIAL FACILITY RISK INDEX
THREATS
VULNERABILITY
CONSEQUENCES
Calculate the Potential Facility Risk Index (PFRI)

Figure 5.1 The main GUI of PFRI program tool

From the opening screen, select a component of the triple definition (threat(T), vulnerability (V), and consequences (C)). It is recommended to go sequentially from threat to vulnerability to consequence. An error exception is thrown if the button "Calculate the Potential Facility Risk Index (PFRI)" is clicked before the inputs of T, V and C have been defined and entered. When threat is chosen, a prompt will appear to select the type of devices at the facility and the threat group adversaries' attributes of life loss, economic damage and symbolism as shown below.

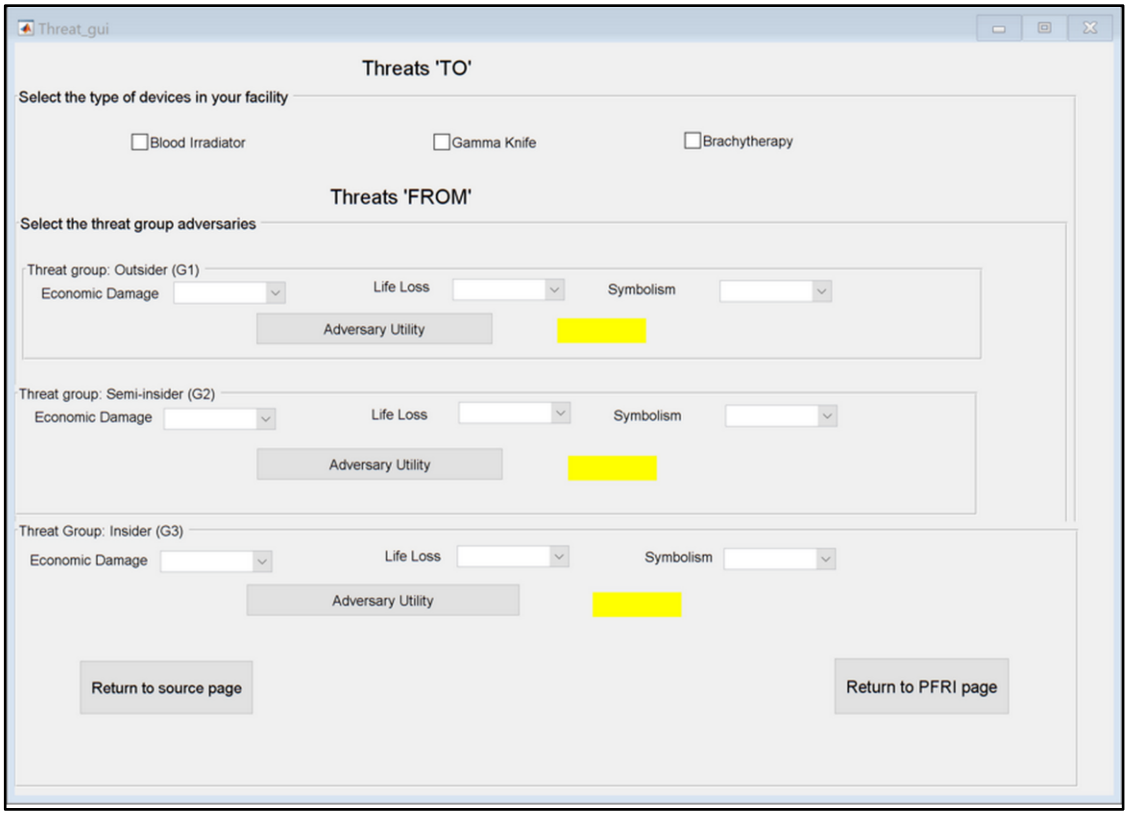
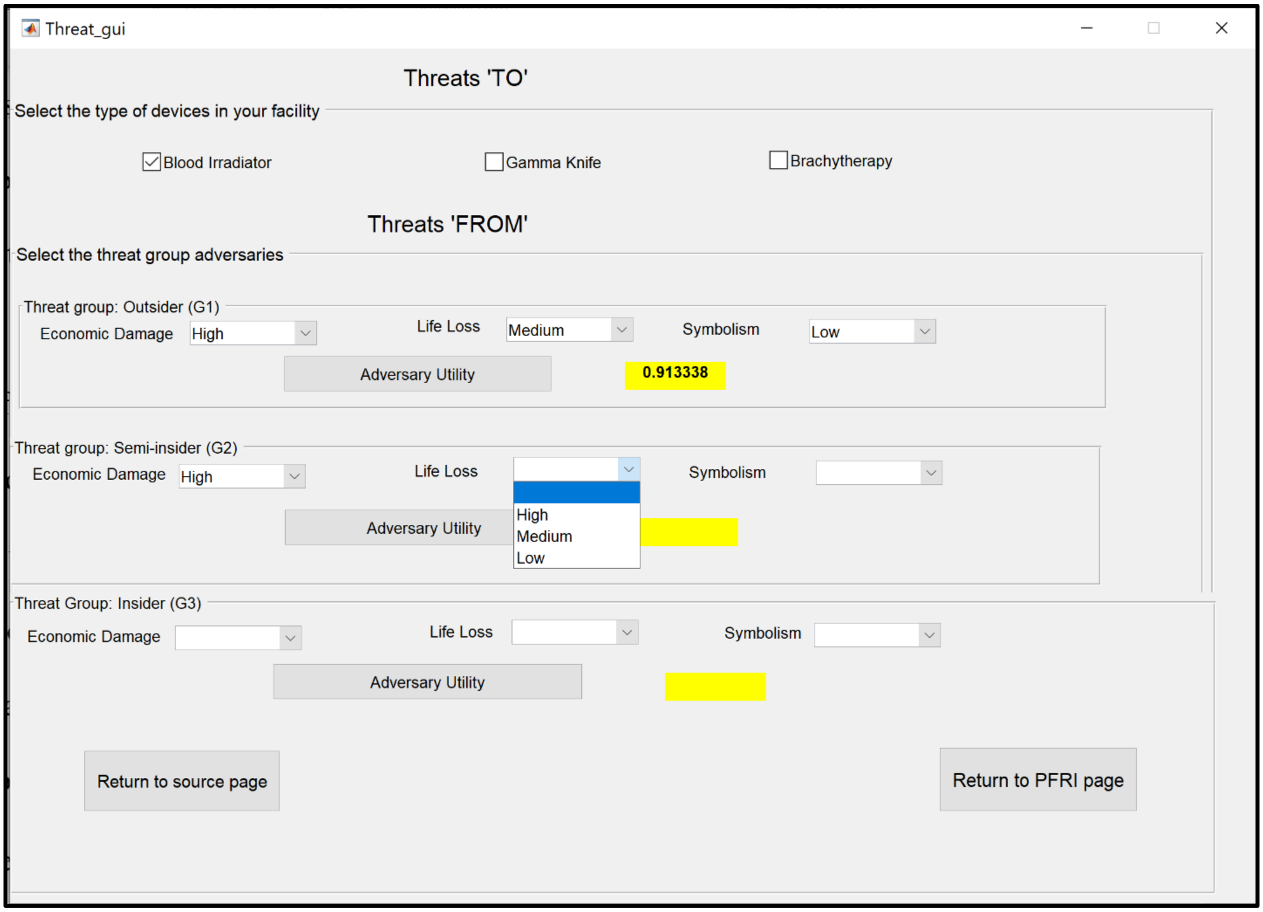


Figure 5.2 The “child” GUI (Threat) of the “parent” GUI (PFRI)

The user is able to navigate between the type of devices present at the facility. The user is able to choose more than one device. On selecting the checkbox of one of the three device options available, a prompt specific to the chosen device option is initiated. The “child” GUI of the selected checkbox device prompts the user to enter the details of the device and calculates the overall success probability of theft for the three scenarios defined in the previous chapters. Before we define the “child” GUI’s of “Blood irradiator”, “Gamma Knife”, and “Brachytherapy”, the program gives user several chances to select the threat group of adversaries belonging to Group 1 (G1), Group 2 (G2), and Group 3 (G3). The user can select the attributes for the groups before selecting the device or after defining the characteristics of the device. The program lets the user come back to the “Threat.gui” window to define the threat profiles of the threat groups. As learnt from the theory in the previous chapter, identification of threat is divided into “Threat TO” and “Threat FROM”, the user gets to choose the attributes of the three terrorist adversary profiles from each group (G1, G2, and G3). The choice of the attributes from “economic damage”, “life loss”, and “symbolism” is presented for all three threat groups (Figure5.3). The user according to their definition of the terrorist objectives may select the attributes that would satisfy their rational terrorist perspective.


Threat_gui

Threats 'TO'

Select the type of devices in your facility

☑ Blood Irradiator □ Gamma Knife □ Brachytherapy

Threats 'FROM'

Select the threat group adversaries

Threat group: Outsider (G1)

Economic Damage High
Life Loss Medium
Symbolism Low
Adversary Utility 0.913338

Threat group: Semi-insider (G2)

Economic Damage High
Life Loss
High
Medium
Low
Symbolism
Adversary Utility

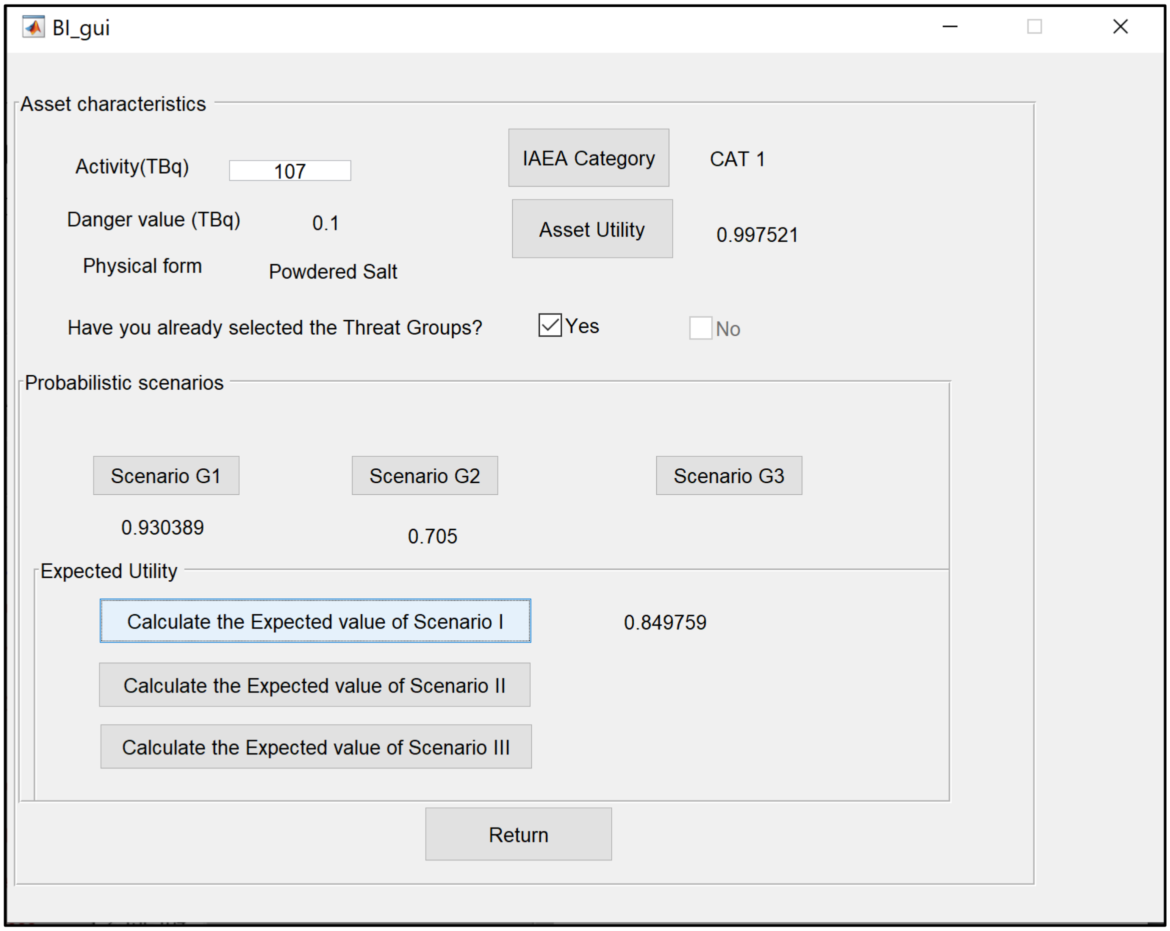
Threat Group: Insider (G3)

Economic Damage
Life Loss
Symbolism
Adversary Utility

Figure 5.3. The "Threat FROM" panel of the Threat.gui.

The user can choose the swing-weights of "high", "medium", and "low" from the drop down menu of the attributes. The button "Adversary utility", uses the formula and theory described in Chapter 3 and 4 to calculate the adversary utility based on the user selected criteria of the threat group adversaries. It is important to create the threat profile for each threat group. The two buttons of "Return to source page" and "Return to PFRI page" lets the user to return to the device "child" GUI and return to the main PFRI GUI window, respectively. The term source on the button refers to the device. On pushing the return button, the user can go back to the device GUI window to continue inputting data related to the device characteristics. The user can also push the return button to navigate back to the main PFRI window, to select another risk component.

The “BI.gui” window : After selecting the “blood irradiator” checkbox, a prompt window appears like below (Figure5.4.). The BI.gui window prompts the user to enter the activity of the radionuclide (*^{137}Cs)* present at the facility in “TBq”. On entering the activity, the program instantly displays the danger value in “TBq” and the subsequent physical form of the radionuclide. On clicking the button “IAEA category”, the program calculates based on the activity entered the category the radionuclide falls into. According to the IAEA, the radionuclide be Category 1 to Category 5, Category 1 being the most dangerous and Category 5, unlikely to be dangerous. The asset utility can be calculated instantly on clicking the button, “Asset Utility”. In the next step, the program lets the user select the threat group profiles if they have not done that already. The panel of “Probabilistic scenarios” calculates the overall probability of theft or sabotage using the “Estimated Adversary Sequence Interruption (EASI)” model introduced by and probabilistic risk assessment (PRA) model. The security features and the probability of detection of the security elements present in the facility is inherently taken as an input and does not let user change it. As a part of future direction, the program will be revised and updated to include the user inputs for every delay element on the adversary path and its corresponding probability of detection and the adversary task time. The push button of “Scenario G1” calculates the probability of theft as per the G1 threat actor capabilities and resources. The push button of “Scenario G2” calculates the probability of theft as per the G2 threat actor capabilities and resources. The push button of “Scenario G3” calculates the probability of theft as per the G3 threat actor capabilities and resources. The initiating events and the frequency of the device maintenance or the device unavailability rates are pre entered in the program. The push button “Calculate the Expected value of Scenario I” when clicked, gives the product of the theft success probability, adversary utility and the asset utility. The same is true for other expected utility scenario pushbuttons. Figure5.4 shows a preview of the “BI.gui” window with few values calculated and displayed in the program. The “Return” pushbutton when clicked, takes the user back to the “Threat.gui” window to have them select other devices present at the facility.



Activity(TBq) 107

Danger value (TBq) 0.1

Physical form Powdered Salt

CAT 1

0.997521

Have you already selected the Threat Groups? ☑ Yes □ No

Scenario G1: 0.930389

Scenario G2: 0.705

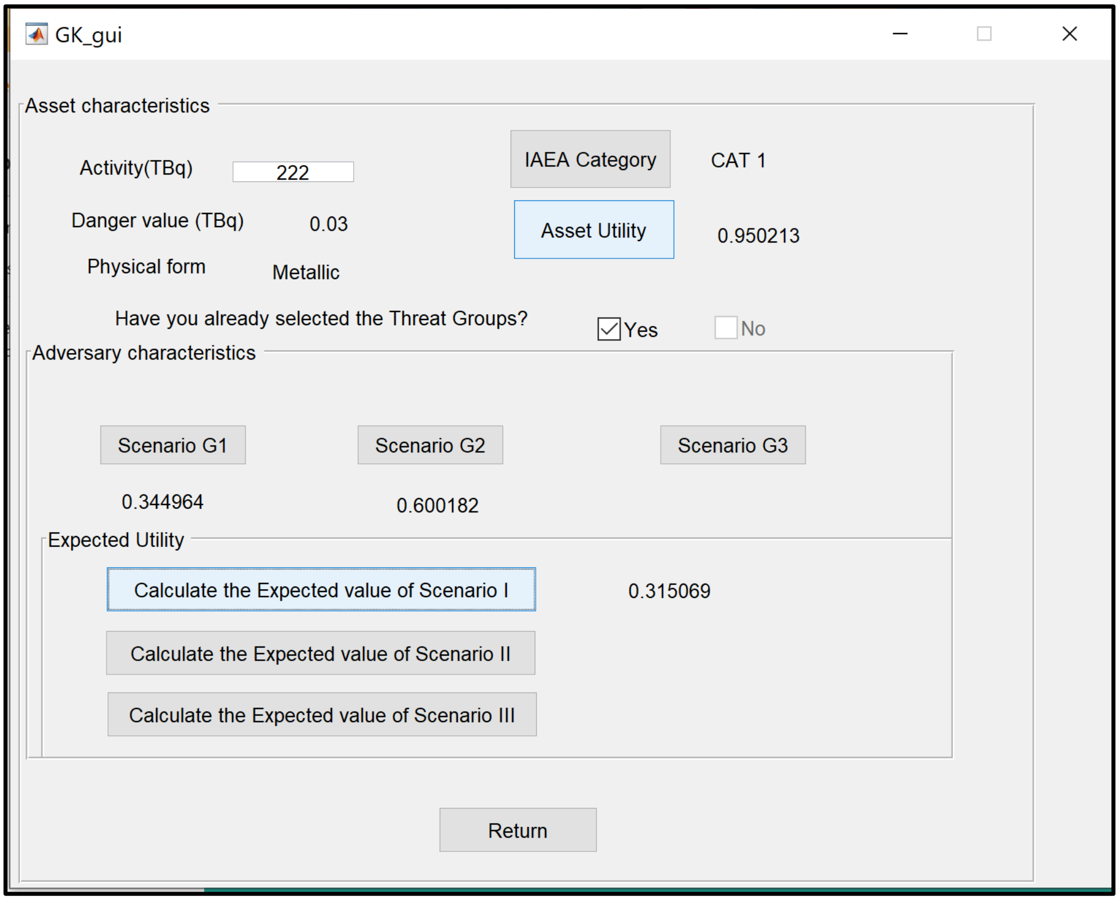
Calculate the Expected value of Scenario I: 0.849759

Figure 5.4. The “BI.gui” panel (child) GUI window of the (parent) GUI “Threat.gui”.

It is important to define the threat group profile before the user calculates the expected utility of each scenario. The program will throw an error exception if the threat groups are not defined and the adversary utility for each threat group is not calculated. The threat groups remain constant (or same) with respect to all asset and all the asset scenarios.

<u>The “GK.gui” window: </u>On selecting the “Gamma Knife” checkbox on the “Threat.gui” window, a prompt window appears as seen below (Figure5.5). The GK.gui window prompts the user to enter the activity of the radionuclide (^{60}Co) present at the facility in “TBq”. On entering the activity, the program instantly displays the danger value in “TBq” and the subsequent physical form of the radionuclide. On clicking the button “IAEA category”, the program calculates the Category of the radionuclide based on the activity entered by the user. The asset utility is computed on clicking the “Asset utility” push button. The calculation of asset utility is based on the physical form, activity,

and the danger value of the radionuclide. The overall theft probabilities for source theft scenarios were calculated based on the security elements of the Gamma Knife room, annual frequency rates of Gamma Knife maintenance and repairs, authorized access, capabilities and resources of the specific threat groups, response force time of the facility and the detection probabilities . The expected utility is computed for each scenario with respect to ^{60}Co source and the three threat group profiles. On clicking the push button for the expected utilities, the result is presented as the product of adversary utility asset utility and the theft success probabilities.


GK_gui
Asset characteristics
IAEA Category
Asset Utility
Adversary characteristics
Scenario G1
Scenario G2
Scenario G3
Expected Utility
Calculate the Expected value of Scenario I
Calculate the Expected value of Scenario II
Calculate the Expected value of Scenario III
Return

Activity(TBq) 222

Danger value (TBq) 0.03

Physical form Metallic

IAEA Category CAT 1

Asset Utility 0.950213

Have you already selected the Threat Groups? ☑ Yes □ No

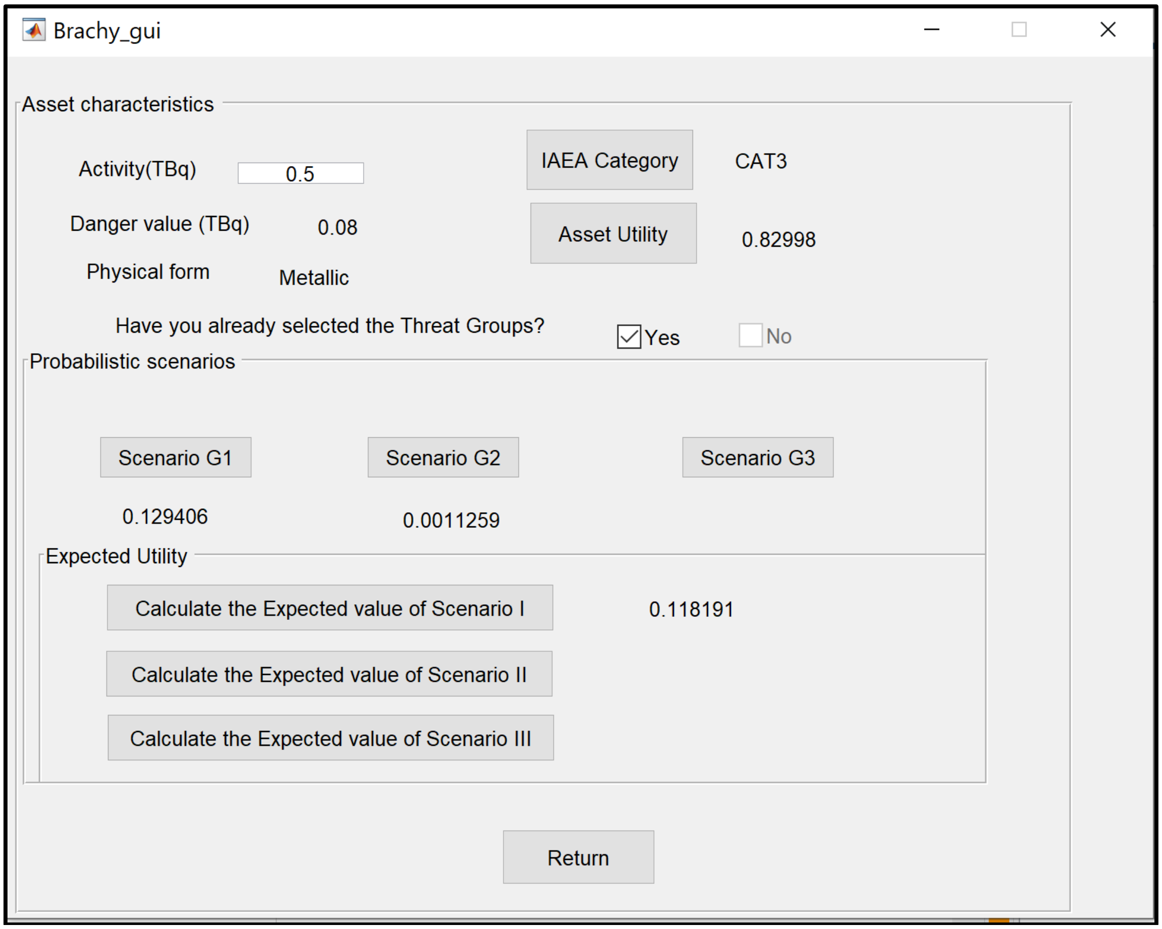
Scenario G1 0.344964

Scenario G2 0.600182

Calculate the Expected value of Scenario I 0.315069

Figure 5.5 The “GK.gui” panel (child) GUI window of the (parent) GUI “Threat.gui”.

The “Brachy.gui” window: On selecting the “Brachytherapy” checkbox on the “Threat.gui” window, a prompt window appears as seen below (Figure5.6). The Brachy.gui window prompts the user to enter the activity of the radionuclide (^{192}Ir) present at the facility in “TBq”. On entering the activity, the program instantly displays the danger value in “TBq” and the subsequent physical form of the radionuclide. Similar to the “BI.gui” and GK.gui”, the child GUI of “Brachy.gui” window displays the same pushbuttons and the format of the program. The “Asset Utility” pushbutton calculates the asset utility and the “IAEA Category” calculates the radionuclide Category as per the information provided by the user. The probabilistic scenario panel gives the overall theft probability of each scenario, upon clicking the specific scenario pushbuttons. The expected utility values differ from the other two device program windows. The “Return” pushbutton takes the user back to the parent GUI of “Threat.gui” main window to let them continue selecting the input parameters of the program.



Activity(TBq) 0.5
IAEA Category CAT3
Danger value (TBq) 0.08
Asset Utility 0.82998
Physical form Metallic

Have you already selected the Threat Groups? ☑ Yes □ No

Scenario G1 0.129406
Scenario G2 0.0011259

Calculate the Expected value of Scenario I 0.118191

Figure 5.6 The “Brachy.gui” panel (child) GUI window of the (parent) GUI “Threat.gui”.

Once the device characteristics for the facility are chosen, the user may return back to the main PFRI window to select another risk component. The asset utility, adversary utility, scenario probabilities and the expected utilities computations complete the threat component of the risk triple definition. Next is the vulnerability component. The user may click on the pushbutton

"Vulnerability" to calculate the locational hazard and facility nuclear security culture vulnerability value.

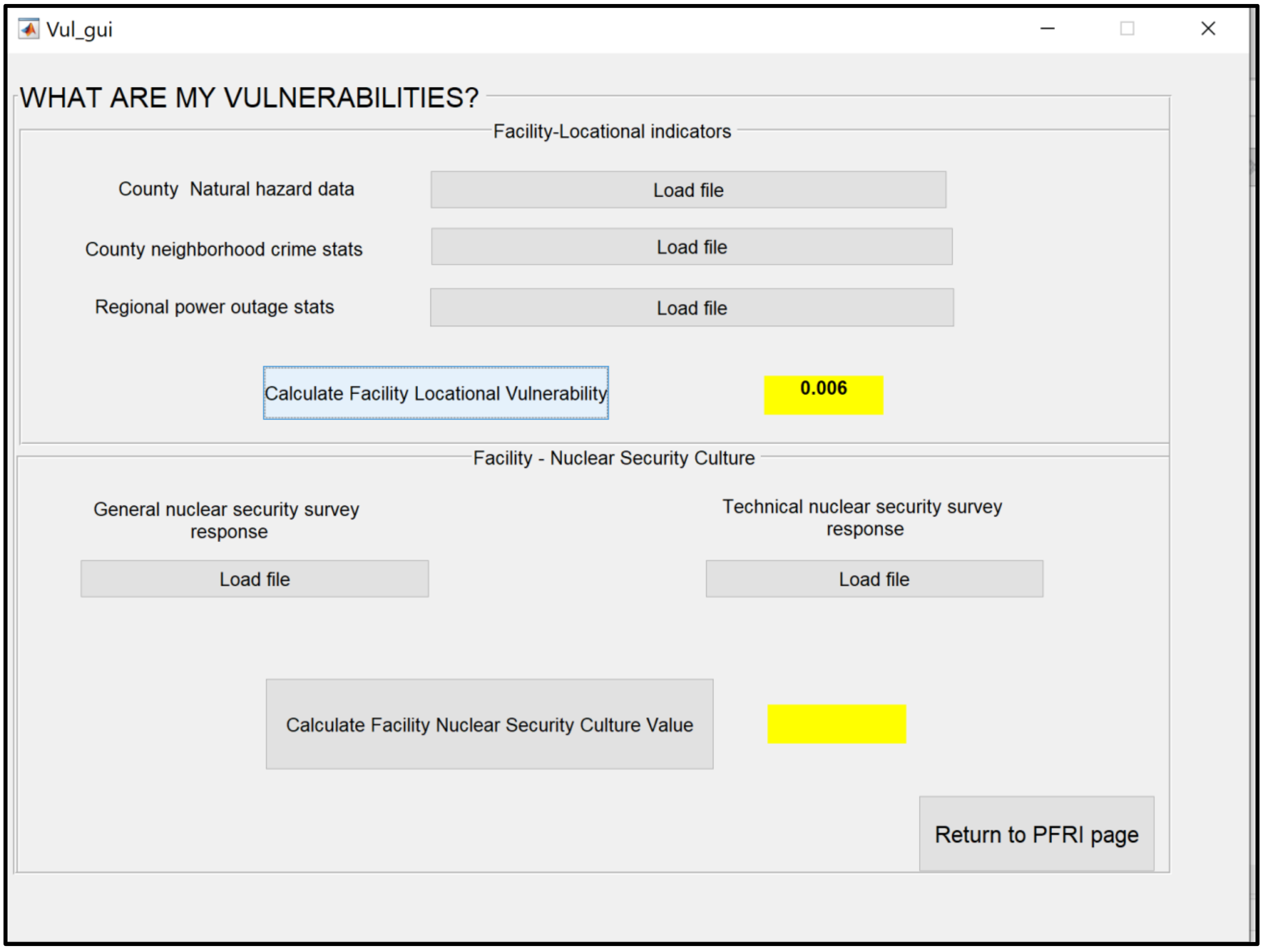
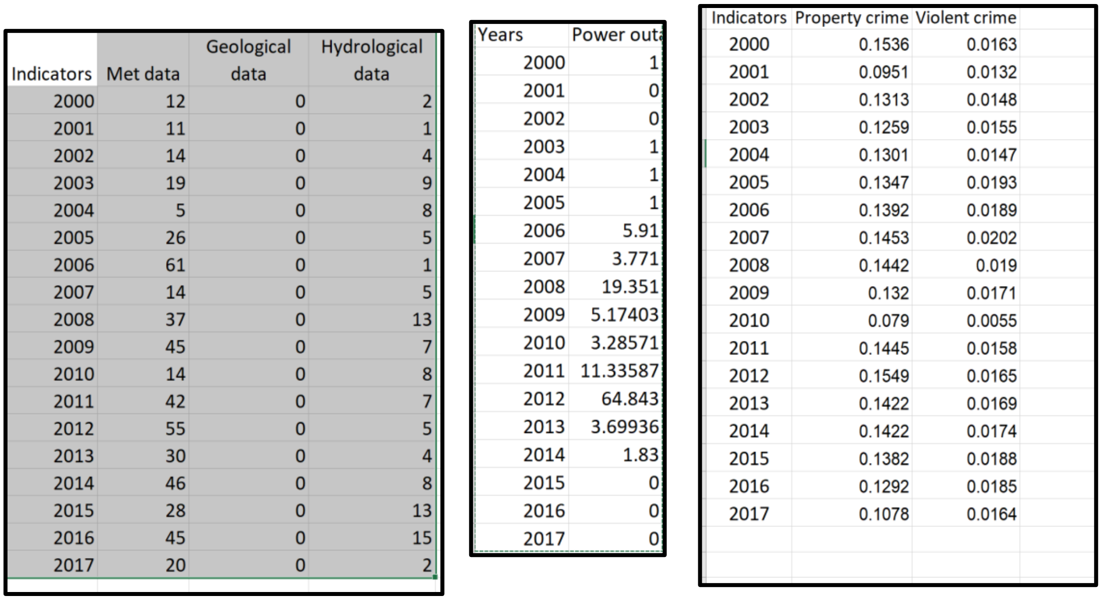

Vul_gui
WHAT ARE MY VULNERABILITIES?
Facility-Locational indicators
County Natural hazard data
Load file
County neighborhood crime stats
Load file
Regional power outage stats
Load file
Calculate Facility Locational Vulnerability
0.006
Facility - Nuclear Security Culture
General nuclear security survey response
Load file
Technical nuclear security survey response
Load file
Calculate Facility Nuclear Security Culture Value
Return to PFRI page

Figure 5.7 The "Vul.gui" panel (child) GUI window of the (parent) GUI "PFRI.gui".

The "Vul.gui" lets the user load the county natural hazard data, neighborhood crime data (violent and property), and regional power outage data. The uploaded data file should be in .xls format. The natural disaster data should be in the format shown below (Figure5.8). The natural disaster data obtained from the NOAA website is required to be consolidated in Meteorological data, geological data, and hydrological data. The county data in this case ranges from 2000-2017. The historical information can vary accordingly. The power outage and neighborhood crime data file should be saved and uploaded in .xls format as well. The crime stats should be in the % violent and property crime format as shown in Figure5.8. The power outage can be regional or county based.



Indicators	Met data	Geological data	Hydrological data
2000	12	0	2
2001	11	0	1
2002	14	0	4
2003	19	0	9
2004	5	0	8
2005	26	0	5
2006	61	0	1
2007	14	0	5
2008	37	0	13
2009	45	0	7
2010	14	0	8
2011	42	0	7
2012	55	0	5
2013	30	0	4
2014	46	0	8
2015	28	0	13
2016	45	0	15
2017	20	0	2

(a)

Years	Power outa
2000	1
2001	0
2002	0
2003	1
2004	1
2005	1
2006	5.91
2007	3.771
2008	19.351
2009	5.17403
2010	3.28571
2011	11.33587
2012	64.843
2013	3.69936
2014	1.83
2015	0
2016	0
2017	0

(b)

Indicators	Property crime	Violent crime
2000	0.1536	0.0163
2001	0.0951	0.0132
2002	0.1313	0.0148
2003	0.1259	0.0155
2004	0.1301	0.0147
2005	0.1347	0.0193
2006	0.1392	0.0189
2007	0.1453	0.0202
2008	0.1442	0.019
2009	0.132	0.0171
2010	0.079	0.0055
2011	0.1445	0.0158
2012	0.1549	0.0165
2013	0.1422	0.0169
2014	0.1422	0.0174
2015	0.1382	0.0188
2016	0.1292	0.0185
2017	0.1078	0.0164

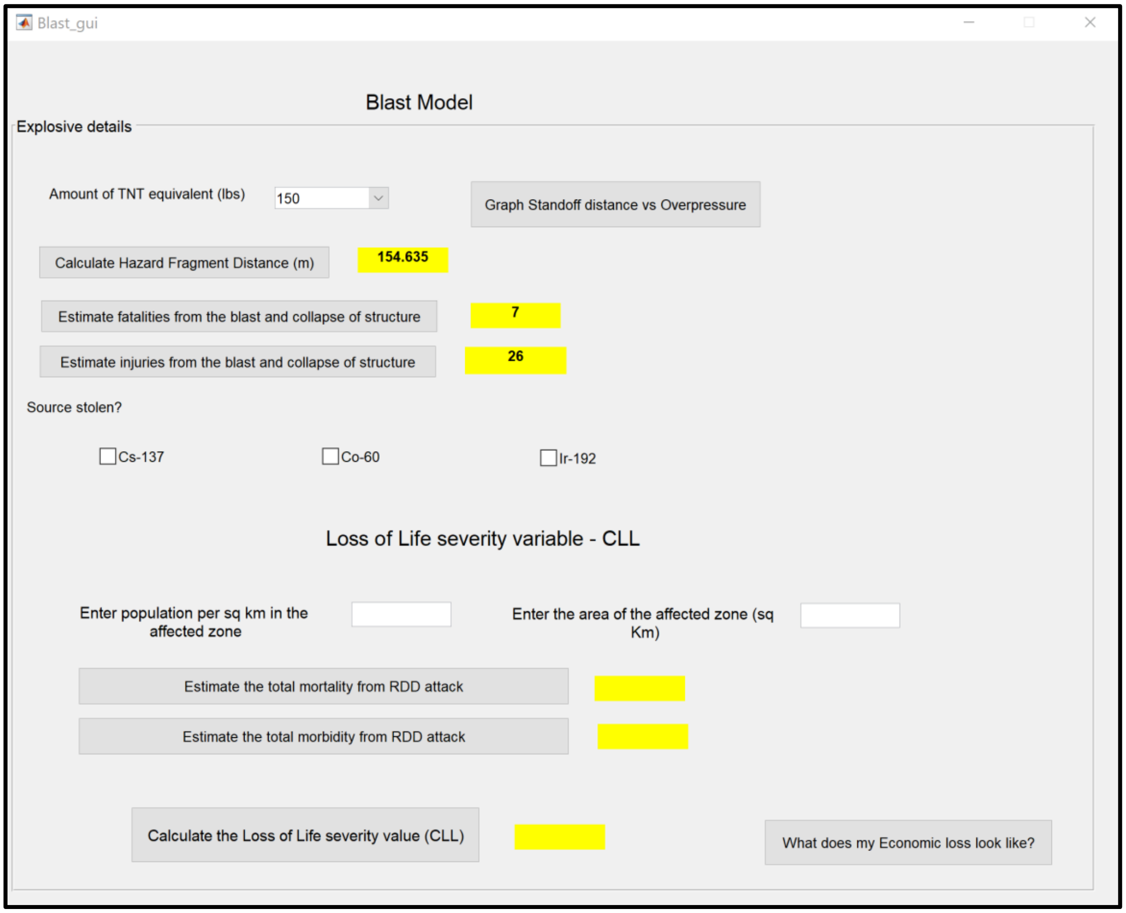
(c)

Figure 5. 8 Example data file format (a) Natural disasters in .xls format (b) Power outage data in .xls format (c) Property and violent crime data consolidated in one .xls file.

The .xls data files should be saved in the MATLAB files folder so it can easily be accessed by the program. It is recommended that the data for all the locational hazard parameters follow the exact format chronology for accurate results. Once the data files are uploaded, the user can click on the pushbutton " Calculate Facility Locational Vulnerability" to get a result between 0 and 1, 0 meaning facility location has very low impact on the risk and 1 meaning the facility location has a high impact on the risk. The program writes a new file in .xls format with new normalized and weighted data called as "LocationalVul", also stored in MATLAB file folder.

Similarly, the Vul.gui window also has the ability to calculate the vulnerability from the facility nuclear security culture. The licensee or the user will be required to do a nuclear security "general" and "technical" survey of the facility staff. The survey questionnaire is presented in Appendix A. The user is prompted to upload the general and technical security culture survey in .xls format. The analysis of the survey is simple that involves computing the percent response greater than 4 (weak), equal to 4 (neutral), and less than 4 (strength). The program computes the scores for both the survey results and for the subset survey as well. The output is the minimum of the three culture survey maximums (strength). The survey results would change according to the facility participants and their response scores. The output values of the locational vulnerability and nuclear security culture vulnerability is stored in the program and is imported to the PFRI gui in a form of arguments (variables) in a *callback* function. The pushbutton “Return to PFRI”, as the name suggests takes the user back to the main PFRI GUI window to select the last risk component. The MATLAB code is presented in Appendix B.

The last risk component of consequence calculates the fatalities and injuries from the blast, calculates the mortalities and morbidities from radiation deterministic and stochastic effects. When the user clicks the consequence pushbutton, a prompt window appears, which triggers the user to enter the explosive information and also the information of the source that is most probable to be stolen. Figure5.9 displays the child GUI (Blast.gui) of the parent (PFRI.gui). The upper half of the window is regarding the blast model and the lower half is the loss of life consequence algorithm.


Blast_gui
Blast Model
Explosive details
Graph Standoff distance vs Overpressure
Source stolen?
□Cs-137
□Co-60
□Ir-192
Loss of Life severity variable - CLL
Enter population per sq km in the affected zone
Enter the area of the affected zone (sq Km)
Estimate the total mortality from RDD attack
Estimate the total morbidity from RDD attack
Calculate the Loss of Life severity value (CLL)
What does my Economic loss look like?

Amount of TNT equivalent (lbs) 150

Calculate Hazard Fragment Distance (m) 154.635

Estimate fatalities from the blast and collapse of structure 7

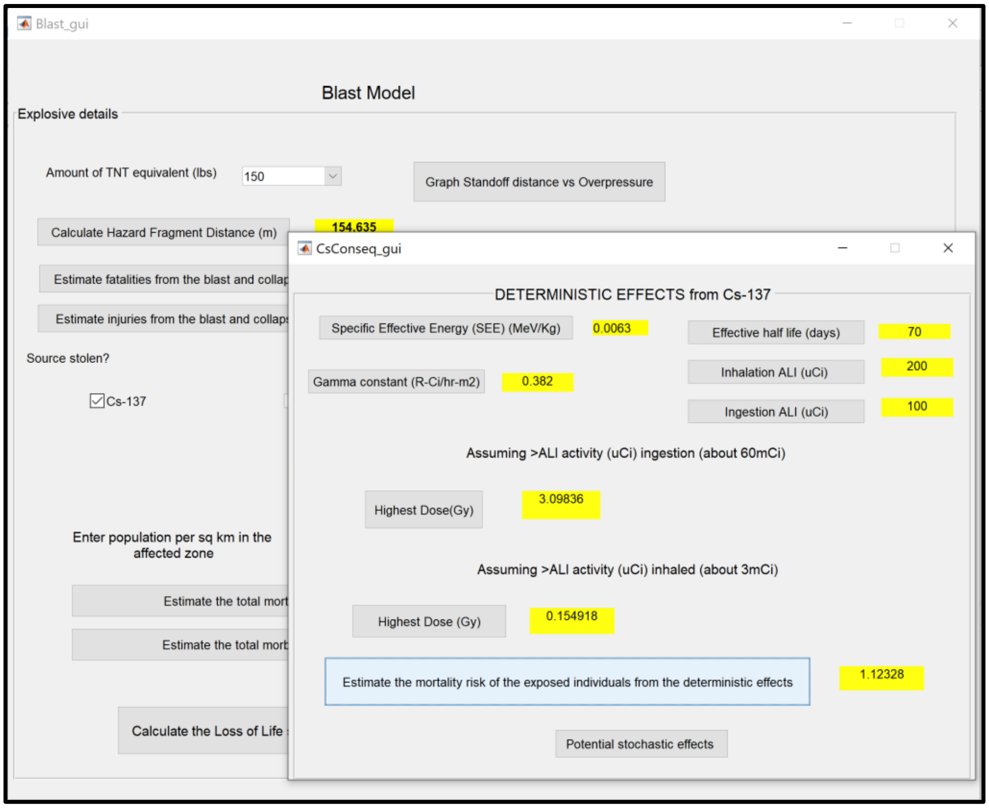
Estimate injuries from the blast and collapse of structure 26

Figure 5.9 The “Blast.gui” panel (child) GUI window of the (parent) GUI “PFRI.gui”.

“Blast.gui” is consequence sub-window. It represents the overall consequence including the blast model and the loss of life model from the stolen radionuclide. The user is asked to enter the amount of TNT equivalent information of the explosive used by the terrorist adversary. These values would be considered as an educated guess from the user of the facility based on the scenarios described in Chapter 4. The explosive amount options are populated in the drop-down menu. The current drop-down menu options only include 150 lb. and 2000 lb. The number of options can however be increased, and more choices can be added depending on the creativity of the licensee performing the risk assessment of the facility. Based on the amount of TNT chosen, the program calculates the hazard fragment distance and also graphs the standoff distance vs overpressure of the selected explosive amount. The computations of the estimation of fatalities and injuries from the blast and collapse of the structure is performed on the click of the pushbuttons.

The other half of the Blast.gui window prompts the user to select a radionuclide that would likely be stolen. When the user selects a checkbox, the other checkboxes gets disabled, letting the user to choose only one radionuclide among the three. It is recommended for the facility to, however, assess the consequences from all three radionuclides to understand the overall risk of theft and the subsequent consequences, if detonated at the facility. The user is also prompted to enter the population per square km in the affected zone and the area of the affected zone in square km. Using the information entered by the user, the program calculates the estimated fatalities and morbidities from the RDD incident. The calculation is followed by the computation of loss of life consequence severity variable C_{LL}.

Figure5.10 shows that when the user selects a radionuclide checkbox, a prompt window, specific to the selected radionuclide appears, where the user is able to determine the specific effective energy, the inhalation and ingestion ALI, gamma constant of the radionuclide. The program also calculates the highest dose received by an individual if they happen to ingest or inhale the activity greater than ALI of the radionuclide. To be consistent, the assumed activity inhaled and ingested is kept constant at 0.0011 TBq (30 mCi) and 0.0022 TBq (60 mCi), respectively, for all three radionuclides. The activity can be a user input in the future versions of the program. Figure5.10 displays the child GUI of CsConseq.gui of the parent Blast.gui. A similar deterministic effect sub-window is programmed for the radionuclides *^{60}Co* and *^{192}Ir.*


Blast_gui
Blast Model
Explosive details
Graph Standoff distance vs Overpressure
Estimate fatalities from the blast and collap
Estimate injuries from the blast and collaps
Source stolen?
Enter population per sq km in the affected zone
Estimate the total mort
Estimate the total morb
Calculate the Loss of Life
CsConseq_gui
DETERMINISTIC EFFECTS from Cs-137
Potential stochastic effects

Amount of TNT equivalent (lbs) 150

Calculate Hazard Fragment Distance (m) 154.635

☑Cs-137

Specific Effective Energy (SEE) (MeV/Kg) 0.0063

Effective half life (days) 70

Gamma constant (R-Ci/hr-m2) 0.382

Inhalation ALI (uCi) 200

Ingestion ALI (uCi) 100

Assuming >ALI activity (uCi) ingestion (about 60mCi)

Highest Dose(Gy) 3.09836

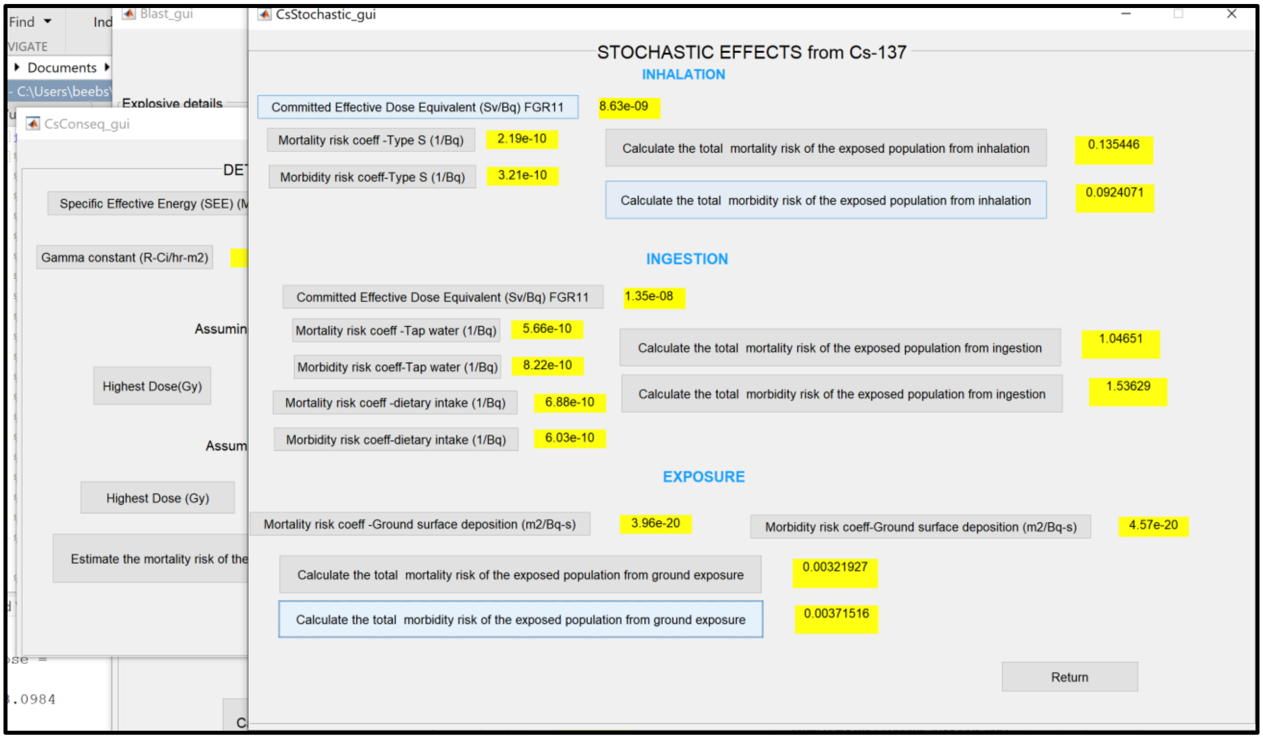
Assuming >ALI activity (uCi) inhaled (about 3mCi)

Highest Dose (Gy) 0.154918

Estimate the mortality risk of the exposed individuals from the deterministic effects 1.12328

Figure 5.10 The “CsConseq.gui” panel (child) GUI window of the (parent) GUI “Blast.gui”, on selecting ^{137}Cs radionuclide checkbox.

As seen from Figure5.10, the child GUI of *^{137}Cs* deterministic effect presents the user with a pushbutton “Potential stochastic effects” to let the user calculate the stochastic effects of the selected radionuclide. The window shown in Figure5.11 is linked to the child GUI of “CsConseq.gui”. Once the user has completed the computation of the deterministic effects of the radionuclide, the next step would be to incorporate the results from the stochastic effect of the radionuclide. The stochastic effects involve calculation of the total mortality and morbidity risk of the exposed population from inhalation and ingestion of food and tap water. It also calculates the risk from ground exposure. The sub-window shown in Figure5.11 indicates the effects from *^{137}Cs* as an example. A similar sub-window of the potential stochastic effects is programmed for the radionuclides *^{60}Co* and *^{192}Ir*.



STOCHASTIC EFFECTS from Cs-137

INHALATION

Committed Effective Dose Equivalent (Sv/Bq) FGR11: 8.63e-09
Mortality risk coeff -Type S (1/Bq): 2.19e-10
Morbidity risk coeff-Type S (1/Bq): 3.21e-10
Calculate the total mortality risk of the exposed population from inhalation: 0.135446
Calculate the total morbidity risk of the exposed population from inhalation: 0.0924071

INGESTION

Committed Effective Dose Equivalent (Sv/Bq) FGR11: 1.35e-08
Mortality risk coeff -Tap water (1/Bq): 5.66e-10
Morbidity risk coeff-Tap water (1/Bq): 8.22e-10
Mortality risk coeff -dietary intake (1/Bq): 6.88e-10
Morbidity risk coeff-dietary intake (1/Bq): 6.03e-10
Calculate the total mortality risk of the exposed population from ingestion: 1.04651
Calculate the total morbidity risk of the exposed population from ingestion: 1.53629

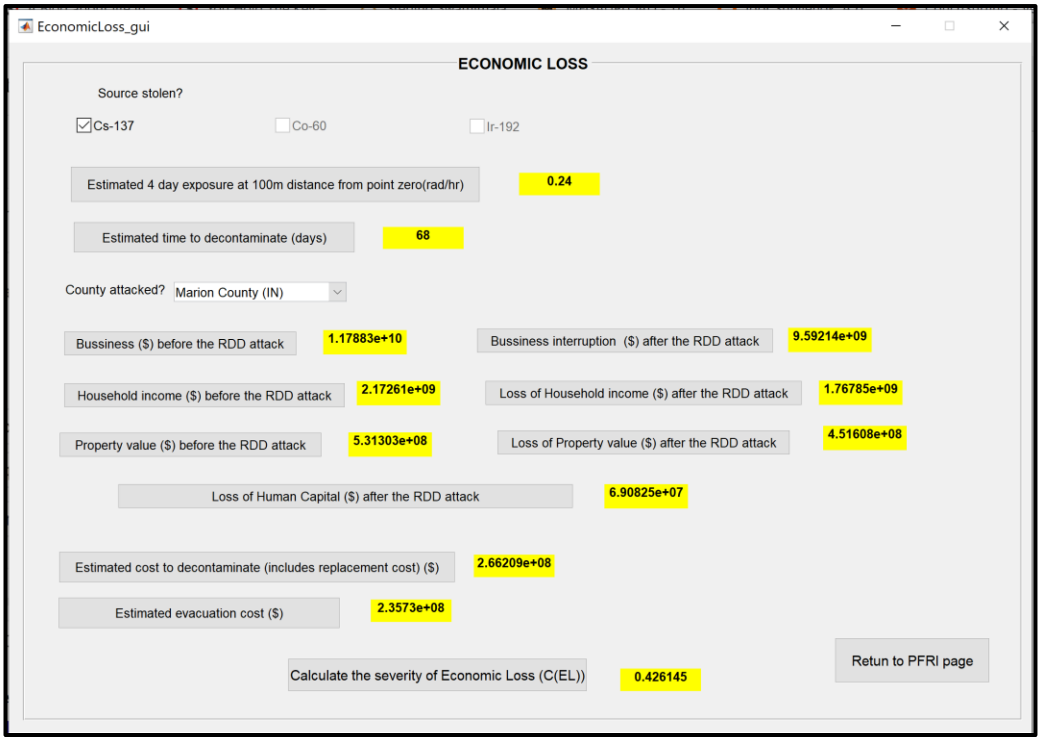
EXPOSURE

Mortality risk coeff -Ground surface deposition (m2/Bq-s): 3.96e-20
Morbidity risk coeff-Ground surface deposition (m2/Bq-s): 4.57e-20
Calculate the total mortality risk of the exposed population from ground exposure: 0.00321927
Calculate the total morbidity risk of the exposed population from ground exposure: 0.00371516

Figure 5. 11 The “CsStochastic.gui” panel (child) GUI window of the (parent) GUI “CsConseq.gui”, on selecting ^{137}Cs radionuclide checkbox.

The stochastic effect GUI is composed of pushbuttons. The window lists the parameter values that is used in the calculation of the estimated mortality and morbidity risk of the exposed population via the ingested, inhaled and exposure pathways. The values for CEDE, morbidity risk coefficients are displayed specific to the radionuclide. The values are displayed in the units given in the pushbuttons. Since they are coefficients captured from the FGR 11 and FGR13, they remain constant per radionuclide. The user may return anytime to the Blast.gui window by clinking on the Return pushbutton placed in the right corner of the stochastic effects window. The user is sent back to the Blast.gui window, where as mentioned before, the user is able to enter the population and the area of the affected zone to estimate the total mortality and morbidity due to the deterministic and stochastic effects from the RDD incident. The program computes the loss of life severity value, C_{LL}, for the selected radionuclide. It also presents the user with an option to quantify the economic loss that the facility would entail, given the RDD detonation occurs at the facility. On clicking the button “What does my Economic loss look like”, the user is forwarded to a new window GUI called “Economic loss”, shown in Figure5.12.

In the EconomicLoss.gui window, the user is once again asked to check the source stolen box. For accurate results, the user will be required to choose the same source that was chosen for the calculation of loss of life consequence variable, C_{LL}. The economic loss is different based on the radionuclide chosen because of the difference in the contamination zone and the time that would be required to decontaminate. In order to have the results of C_{EL} match the results of C_{LL}, the user should check the same radionuclide (as stolen) for correct assessment of the facility risk. Figure5.12 shows the results for ^{137}Cs as the assumed detonated radionuclide. The results would change as per the selected radionuclide. The user may also select the county the facility is located in. As of writing, the drop-down menu has Marion county as its only option, but it can be populated with the name and results of other counties based on the location of the healthcare facility.



EconomicLoss_gui

ECONOMIC LOSS

Source stolen?

☑Cs-137 □Co-60 □Ir-192

Estimated 4 day exposure at 100m distance from point zero(rad/hr) 0.24

Estimated time to decontaminate (days) 68

County attacked? Marion County (IN)

Bussiness ($) before the RDD attack 1.17883e+10

Bussiness interruption ($) after the RDD attack 9.59214e+09

Household income ($) before the RDD attack 2.17261e+09

Loss of Household income ($) after the RDD attack 1.76785e+09

Property value ($) before the RDD attack 5.31303e+08

Loss of Property value ($) after the RDD attack 4.51608e+08

Loss of Human Capital ($) after the RDD attack 6.90825e+07

Estimated cost to decontaminate (includes replacement cost) ($) 2.66209e+08

Estimated evacuation cost ($) 2.3573e+08

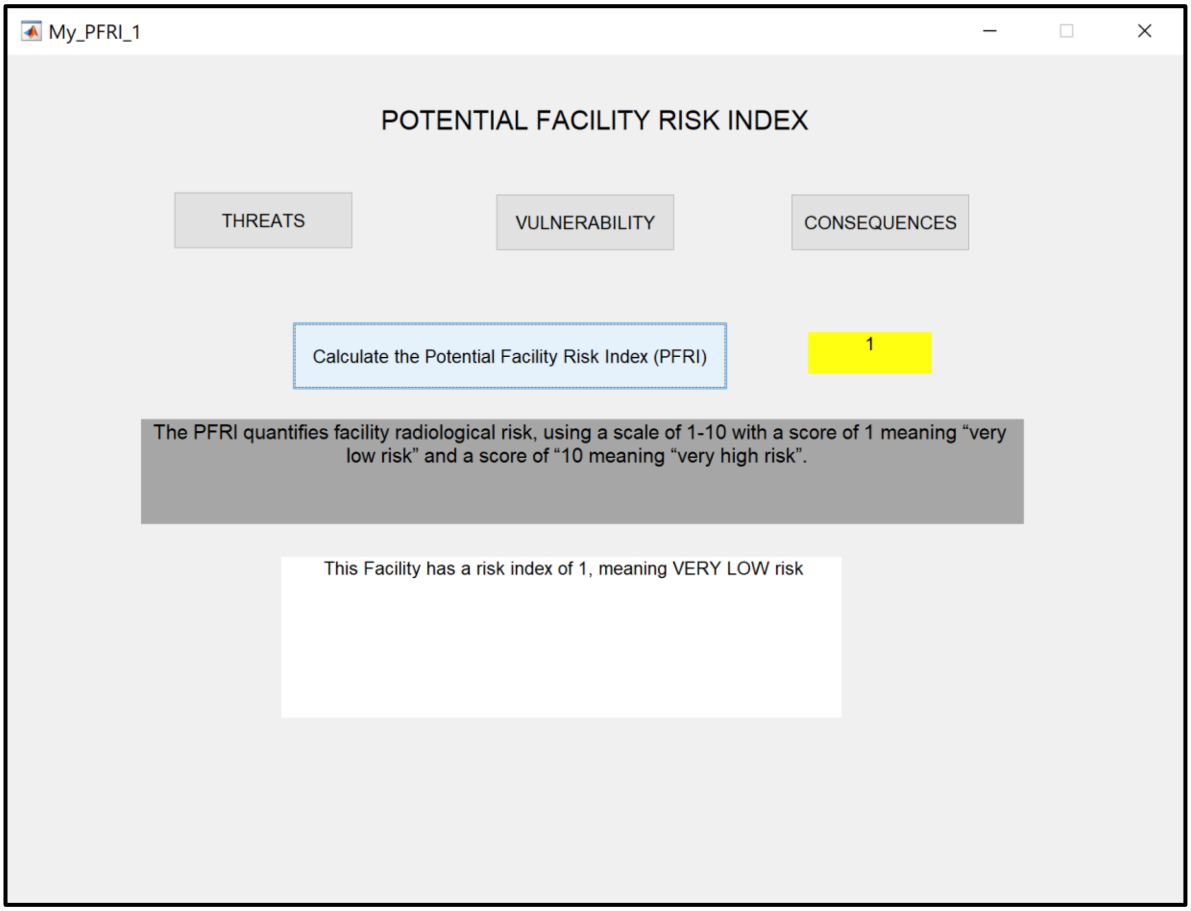
Calculate the severity of Economic Loss (C(EL)) 0.426145

Retun to PFRI page

Figure 5. 12 The "EconomicLoss.gui" panel (child) GUI window of the (parent) GUI "CsConseq.gui", on selecting ^{137}Cs radionuclide checkbox.

Depending on the radionuclide selected the program calculates and displays the estimated decontamination time and the 4-day exposure from the radionuclide ground deposition at 0.1 km distance from the blast. The program also gives an estimation of the business revenue before the RDD attack in ($) and business interruption or loss from the RDD attack ($). The household income and the property loss value before and after the RDD attack are also calculated in the program. The estimated cost to decontaminate and evacuate was projected as a part of the economic loss consequence program. Compounding the costs of before and after the attack, the pushbutton "Calculate the severity of Economic loss" when clicked gives the value for C_{EL}. The return button takes the user back to the main PFRI page.

The user when arrives back on the main PFRI page, at this stage, should mean that the components were computed separately in the process and the program is ready to calculate the final potential facility risk index PFRI. At this stage, the values of T, V and C are stored in the program and are used by the program tool to calculate the composite index of PFRI. The value as shown in Figure5.13 will be displayed as an integer between 1 and 10. The white box will provide the user with the description of what it means to get the particular PFRI value.


My_PFRI_1
POTENTIAL FACILITY RISK INDEX
THREATS
VULNERABILITY
CONSEQUENCES
Calculate the Potential Facility Risk Index (PFRI)

1

The PFRI quantifies facility radiological risk, using a scale of 1-10 with a score of 1 meaning "very low risk" and a score of "10 meaning "very high risk".

This Facility has a risk index of 1, meaning VERY LOW risk

Figure 5. 13 The PFRI of St. Benedict Healthcare calculated using the PFRI GUI tool

This concludes the PFRI GUI tool program calculations. The demonstration of the PFRI tool has appropriately shown that the vast amount of information required to calculated the potential facility risk index can easily be consolidated in one program, through the use of MATALB graphical user interface algorithms. The user friendly PFRI tool is easy to install and access by the healthcare staff. The efficiency of the tool was demonstrated by an exhaustive assessment of the facility risk, compounding the asset utilities, adversary profiles, theft scenarios, vulnerability of the facility and the incurred consequences from the RDD attack. The adequacy of the PFRI GUI tool will be achieved upon addition of other healthcare facility and county data. Because no benchmark data exists, this methodology cannot be validated in a traditional sense. Instead, this chapter demonstrates that the code acts as expected and that the hypothetical scenario of St. Benedict results explained in Chapter 4 is re-produced with the PFRI tool, validates that the code produces the correct result. As future direction for research, the code will continuously be updated to incorporate the most current data. The code will also be improved to include user input parameters in threat scenarios of the three radionuclides. The program can also be revised further to add more radionuclides based on the assessed radiological facility.

CHAPTER 6. GAME THEORY-RDD GAME

6.1 Introduction

Security resources must be deployed selectively and should be based on the current evaluation of the threat, and the vulnerability and potential consequences associated with the unauthorized removal or sabotage of radioactive materials (U.S. DHS, 2015). The potential facility risk index uses the principles of graded approach and justification towards building an integrated and cooperative defense system for source security. The research extends the classic risk assessment methodology by mapping the concepts of game theory to defend against an attacker whose choice of target is unknown.

There are several different ways of describing games mathematically. The representations presented here have the following formal elements in common:

- A list of players,
- A complete description of what the players can do (their possible actions),
- A description of what the player know when they act,
- A specification of how the players' actions lead to outcomes, and
- A specification of the players' preferences over outcomes.

At this level of abstraction, the mathematical representation of a game is similar to the description of games of leisure. For example, the rules of the board game chess specify elements 1 through 4 precisely: (1) there are two players; (2) the players alternate in moving pieces on the game board, subject to rules about what moves can be made in any given configuration of the board; (3) players observe each other's moves, so each knows the entire history of play as the game progresses; (4) a player who captures the other player's king wins the game, and otherwise a draw is declared. Although element 5 is not implied by the rules of chess, one generally can assume that players prefer winning over a draw and a draw over loosing.

Game theory is an abstract mathematical theory for analyzing interactions among multiple decision makers (players). Game-theoretic models are well suited to examine the possibility of achieving an optimum stable solution between the adversary and the defender. The decision makers may be nations, people, robots, or even corporations (Watson, 2001). The preferences of each player are specified by utility functions that quantify the amount of benefit resulting to each player from possible outcomes of the game; this benefit is referred to as the utility or payoff. A player's strategy in a game is a complete plan of action for whatever situation might arise. The strategy fully determines the player's behavior. Each player has two or more strategies or specific choices. Strategy profiles, which are the possible combinations of strategies that can be used by the players, give different payoffs to each player (Watson, 2011). In this context of radiological source security, players are the defense forces of the healthcare facility on one side and the terrorist or the attacker on the other side. The RDD game examines the strategic interaction between the two.

The work presented uses elements of non-cooperative game theory. Cooperative and non-cooperative theories are the two leading frameworks for analyzing games. Non-cooperative games are those in which the sets of possible actions of individual players give an outcome. Cooperative games are those in which the sets of possible joint actions of groups of players give an outcome. The players in a noncooperative game compete against each other, and each player is selfishly interested only in their own payoff. In some noncooperative games the players have perfect information about the game (such as chess), while in other cases, the players may have incomplete or asymmetrical information (such as many card games). Game theory captures the dynamic nature of security problems. Given a set of opponents and their respective goals, game theory yields the optimal way for each player to play the game, not how the game will actually be played. When applying game theory, it is vital to both define the goals of the adversary and defender as accurately as possible, but also assess the impacts of the adversary behaving in less than optimal ways

Equilibrium states are possible for one-shot games (games played only once), finitely repeated games, or infinitely repeated games. Nash equilibrium, named after Nobel laureate John Forbes Nash, is the most used solution concept in game theory. This notion captures a steady state play of a strategic game in which each player holds the correct expectation about the other player's behavior and acts rationally (Fudenberg & Tirole, 1991; Watson, 2001). If each player has chosen a strategy and neither player can increase their payoff by choosing an action different from his current one, then the current set of strategy choices and the corresponding payoffs constitute a Nash equilibrium.

In RDD game, a simultaneous one-shot non-cooperative game is applied to a healthcare facility (defender or player 1) housing radiation emitting devices and radioactive sources. The healthcare facility is defending its assets against a terrorist RDD attack (attacker or player 2).

6.2 Notation and mathematical formalism

For this study, we define the following sets and functions:

Players $i \in I = \{1,2\}$ where Player 1 is the healthcare facility, or the "defender" and Player 2 is the terrorist or the "attacker".

The study limits the asset (radioactive material) list to the highest value targets (i.e. high likelihood of success and high impact) available, rather than all the potential targets in the medical facility. Of the hundreds of radioactive materials available, three that are generally found in healthcare facilities are considered the most attractive candidates for use in RDD: ^{60}Co (radiosurgery devices), ^{137}Cs (blood irradiators) and ^{192}Ir (brachytherapy HDR device). The sources threatened with attack are the set $k \in K = \{Co, Cs, Ir\}$ with Co being the atomic symbol for Cobalt, Cs being the atomic symbol for Cesium, and Ir being the atomic symbol for Iridium.

Let S_i be the strategy space comprising each of the possible strategies $s_{ik} \in S_i$, where the k_{th} source is targeted by the i_{th} player. The strategy space of player 1 is $S_1 = \{defend\ Co, defend\ Cs, defend\ Ir\}$. The strategy space of player 2 is $S_2 = \{attack\ Co, attack\ Cs, attack\ Ir\}$. The pure strategy profile is a vector of the form $s = [s_{1k}, s_{2k}]$ that gives a particular combination of pure strategies that could be chosen by the players. The Cartesian product $S_1 \times S_2$ is the set of all possible pure strategy profiles in the game[7].

A mixed strategy θ_i is a randomization over pure strategies. Let Θ_i denote the space of player i's mixed strategy probabilities, $\theta_i(s_{ik})$, where θ_i is the probability assigned to the player i for defending or attacking the k_{th} source such that for each player i, $\theta_i(s_{ik}) \in [0,1]$ and $\sum_{ik} \theta_i(s_{ik}) = 1$.

[7] For example, if $S_1\{A, B\}$ and $S_2 = \{X, Y\}$, then $S = S_1 \times S_2 = \{(A, X), (A, Y), (B, X), (B, Y)\}$

$\boldsymbol{\rho_{in}} = [\theta_i(s_{i,Co}), \theta_i(s_{i,Cs}), \theta_i(s_{i,Ir})]$, $\boldsymbol{\rho_{in}} \in \Theta_i$, are the mixed strategy row vectors available to player i, where n is the index of possible mixed strategy vectors available to the i_{th} player. $\Theta_1 \times \Theta_2$ is the set of all possible mixed strategy profiles.

It is convenient to denote -i as the index of "all other players" than player i. For each player i, we define a von Neumann-Morgenstern utility (payoff) function u_i: $\mathrm{S}_1 \times \mathrm{S}_2 \rightarrow \mathbb{R}$ (a function whose domain is the set of pure strategy profiles and whose range is the set of real numbers) so that for each pure strategy $s_{ik} \in \mathrm{S}_i$ that the players could choose, $u_i(s_{ik,}s_{-ik})$ is the player i's payoff in the game (von Neumann & Morgenstern, 2007).

We extend the definition of a payoff function to mixed strategies by using the concept of *expected value*. We define the pure strategy payoff matrix $\boldsymbol{U_i}$ **:**

$$U_i = \begin{bmatrix} u_i(s_{iCo,}s_{-iCo}) & u_i(s_{iCo,}s_{-iCs}) & u_i(s_{iCo,}s_{-iIr}) \\ u_i(s_{iCs,}s_{-iCo}) & u_i(s_{iCs,}s_{-iCs}) & u_i(s_{iCs,}s_{-iIr}) \\ u_i(s_{iIr,}s_{-iCo}) & u_i(s_{iIr,}s_{-iCs}) & u_i(s_{iIr,}s_{-iIr}) \end{bmatrix} \tag{6.1}$$

When player i selects a mixed strategy vector $\boldsymbol{\rho_{in}}$, her *expected payoff,* $E[u_i]$, is the expectation of u_i with respect to the joint probability distribution resulting from the marginal probabilities in the mixed strategy profile ($\boldsymbol{\rho_{in}}, \boldsymbol{\rho_{-in}}$):

$$E[u_i] = \rho_{in}\, U_i(\rho_{-in})^T \tag{6.2}$$

where T denotes transposition.

6.2.1 Assumptions

Assumption 1 (Rationality & Intelligence):

Both players in this game are rational and intelligent. Rationality entails a player making all decisions with a view to maximizing their expected utility. Intelligence entails that a player knows the rules of the game and can accurately compute payoffs from all combinations of players' actions that can occur in the game.

Assumption 2 (Common Knowledge & Complete Information):

Each player in this game knows their own set of strategies and utility function and the set of strategies and utility function of the other player. It is common knowledge to both players that each player in the game knows the set of strategies and utility function of the other player. It is common knowledge that each player in the game is rational, intelligent, and aware of their own set of strategies and utility function. Common knowledge results in circularity of knowledge that can be stated as, "Player 1 knows that the game is being played, player 2 knows that player 1 knows that the game is being played, player 1 knows that player 2 knows that player 1 knows the game is being played, and so on..."

6.2.2 Definitions

Definition 1 (Mixed and Pure Strategies):

A strategy is a complete and contingent plan determined by a player in advance of starting the game (Watson, 2001). In the simultaneous one-shot game considered here, a pure strategy, $s_{ik} \in S_i$, results in only one of the i_{th} player's possible strategies being played with a probability of 1 and all other possible strategies being played with a probability of zero. Each mixed strategy, $\boldsymbol{\rho_{in}}$, is a vector of probabilities $\theta_i(s_{ik})$ of the i_{th} player playing each of their pure strategies, so every pure strategy is represented by a unique $\boldsymbol{\rho_{in}}$ and $S_i \subset \Theta_i$.

Definition 2 (Weak Dominance):

A pure strategy s_{ik} or mixed strategy $\boldsymbol{\rho_{in}}$ is weakly dominated if there exists a strategy (pure or mixed) $s'_{ik} \in S_i$ or $\rho'_{in} \in \Theta_i$ such that

$$u_i(s'_{ik}, s_{-ik}) \geq u_i(s_{ik}, s_{-ik})\, for\ all\ s_{-ik} \in S_{-i} \quad (6.3)$$

$$u_i(\rho'_{in}, \rho_{-in}) \geq u_i(\rho_{in}, \rho_{-in})\, for\ all\ \rho_{-in} \in \Theta_{-i} \quad (6.4)$$

Weak dominance results is a solution by the iterated elimination of dominated strategies wherein dominated strategy profiles are eliminated one at a time until only a single undominated strategy profile remains as the equilibrium solution .

Definition 3 (Pure Strategy Nash Equilibrium):

A pair of pure strategy profiles $(s_{ik}^{*}, s_{-ik}^{*})$, are a pure strategy Nash equilibrium if and only if:

$$u_i(s_{ik}^{*}, s_{-ik}^{*}) \geq u_i(s_{ik}, s_{-ik}^{*})\ for\ all\ s_{ik} \in S_i and\ s_{-ik} \in S_{-i} \tag{6.5}$$

A game may have several pure strategy Nash equilibria or none.

Definition 4 (Mixed Strategy Nash Equilibrium):

A pair of mixed strategies $(\rho_{in}^{*}, \rho_{-in}^{*})$, are a mixed strategy Nash equilibrium if and only if:

$$u_i(\rho_{in}^{*}, \rho_{-in}^{*}) \geq u_i(\rho_{in}, \rho_{-in}^{*}) for\ all\ \rho_{in} \in \Theta_i and\ \rho_{-in} \in \Theta_{-i} \tag{6.6}$$

Every finite simultaneous one-shot game has at least one mixed strategy Nash equilibrium

Definition 5 (Max-min Strategy):

Suppose that player i assumes that player -i will know whatever strategy is chosen by player i and respond by playing the strategy that minimizes the payoff to player i, that is, player -i follows the decision rule $\underbrace{min}_{s-ik} \mathrm{u}_1(\mathrm{s}_{\mathrm{ik}}, \mathrm{s}_{-\mathrm{ik}})$. Then player i's best response is to play the strategy resulting in the strategy profile that maximizes the objective function u_1, given the expected behavior of player -i. Thus, player i's max-min strategy, $s"_{ik}$ is chosen by the decision criterion:

$$\underbrace{max}_{s"ik} \underbrace{min}_{s-ik} u_1(s"_{ik}, \mathrm{s}_{-\mathrm{ik}}) \tag{6.7}$$

For the non-zero sum RDD game developed here, the definition of max-min strategy is restricted to pure strategy profiles. Every zero-sum game has a Nash equilibrium profile of max-min strategies for both players (possibly including mixed strategies), but this result is not obtained for non-zero-sum games. Following Wald (1949), decision theory literature has presented the max-min criterion as appropriate for decisions under uncertainty.

6.3 Game characteristics

The assumptions and definitions developed in the previous section apply to this game. The defender can choose to defend only one of three high risk radionuclides present at the healthcare facility: - Cobalt (^{60}Co), Cesium (^{137}Cs), or Iridium (^{192}Ir). The baseline level of defenses required as per *Title 10 of the Code of Federal Regulations (10 CFR) Part 37* (U.S NRC, 2013) has been implemented by the facility, and these defenses remain active and unchanged for the two radionuclides that are not hardened. The success probability of theft used in the model reflects the strength of the existing defenses prior to the start of the game. The attacker can attack only one of the three radionuclides. Each player is permitted to use pure or mixed strategies. The source in a defended state is invulnerable to attack.

The extended form of a game shows the decision nodes and payoffs for each player in the form of a game tree diagram (Fig. 6.1.). The branches of the diagram represent a possible strategy that could be chosen at the corresponding node, and branches terminating on an oval shape are unknown to the other player. This game assumes complete information, which is distinct from perfect information (Fudenberg & Tirole, 1991). Perfect information entails that any player can observe the actions of the other at all times throughout the game, meaning that in a simultaneous game of perfect information, the players would select their strategies simultaneously and with instantaneous knowledge of the decision made by the other player. The RDD game is simultaneous but has imperfect information, meaning that players select their strategies simultaneously but without being instantaneously informed of the outcome of the other player's decision.

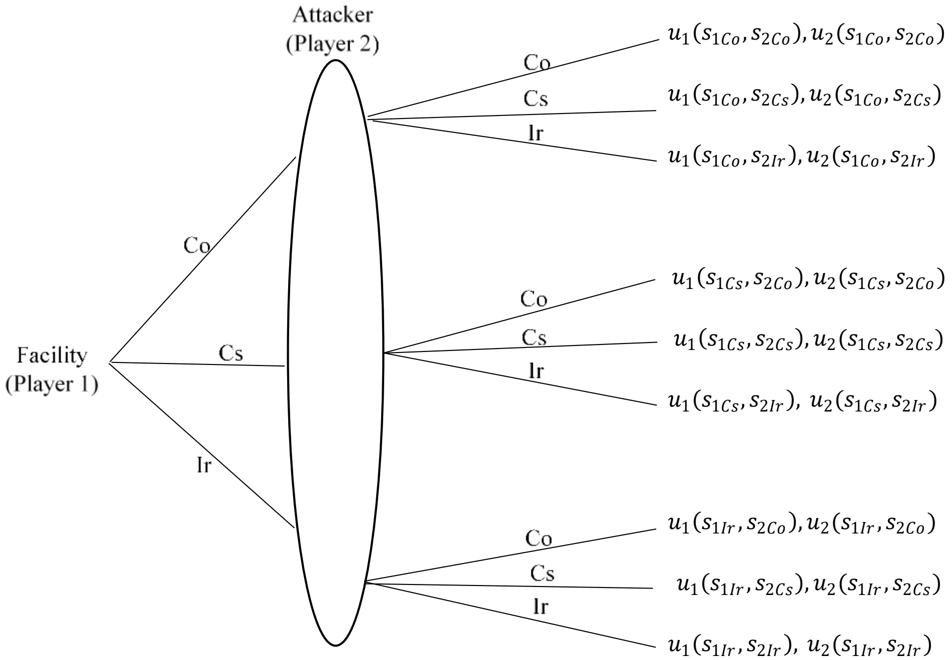

Attacker
(Player 2)
Facility
(Player 1)
Co
Cs
Ir
Co
Cs
Ir
Co
Cs
Ir
Co
Cs
Ir
$u_1(s_{1Co}, s_{2Co}), u_2(s_{1Co}, s_{2Co})$
$u_1(s_{1Co}, s_{2Cs}), u_2(s_{1Co}, s_{2Cs})$
$u_1(s_{1Co}, s_{2Ir}), u_2(s_{1Co}, s_{2Ir})$
$u_1(s_{1Cs}, s_{2Co}), u_2(s_{1Cs}, s_{2Co})$
$u_1(s_{1Cs}, s_{2Cs}), u_2(s_{1Cs}, s_{2Cs})$
$u_1(s_{1Cs}, s_{2Ir}), u_2(s_{1Cs}, s_{2Ir})$
$u_1(s_{1Ir}, s_{2Co}), u_2(s_{1Ir}, s_{2Co})$
$u_1(s_{1Ir}, s_{2Cs}), u_2(s_{1Ir}, s_{2Cs})$
$u_1(s_{1Ir}, s_{2Ir}), u_2(s_{1Ir}, s_{2Ir})$

Figure 6. 1 The RDD game tree with decision nodes and payoffs.

6.3.1 Utility Functions

The utility functions for the defender and the attacker are derived from the quantitative PFRI model. The attacker's and defender's expected utilities are functions of the attacker's success probability of theft. The attacker success probability distribution assigns a zero probability of success for any pure strategy profile $(s_{1k,}s_{2k})$ where $s_{1k} = s_{2k}$. The defender's utility function, u_1, gives the defender's disutility resulting from loss of life and economic loss consequences:

$$u_1(s_{1k,}s_{2k}) = EU[M_k X_2] = P_s(M_k X_2) \times (-C_{k,net}) \qquad (6.8)$$

where

M_k Attack the k_{th} radioactive material.

X_2 Intent (theft) from player 2 (attacker)

P_s Attacker's success probability of theft

$$C_{net} = \frac{(C_{EL}+C_{LL})}{2}, \tag{6.9}$$

where

As defined in Chapter 3:

$$C_{LL} = [\left(\frac{D_{BE}+D_{cancer}+D_{ARS}}{Population\ density}\right) + \left(\frac{I_{BE}+I_{cancer}+I_{ARS}}{Population\ density}\right)] \tag{6.10}$$

C_{LL} is the life loss consequence severity variable

D_{BE} are the fatalities from the blast effects

D_{cancer} are the fatalities in future from relative cancer risk

D_{ARS} are the fatalities from Acute Radiation Syndrome (ARS); and

I_{BE} blast effect mortality.

I_{cancer} is relative cancer risk mortality; and

I_{ARS} is the deterministic effect mortality

$$C_{EL} = 1/\sqrt{(I - D_E)^2 Y} \tag{6.11}$$

C_{EL} Economic Loss (EL) consequence severity variable

D_E is the difference between the two vector components A_i and B_i ; and

Y is the linear regression coefficient.

$$A_e or\ B_e = \frac{E_{et}}{\sum E_t} \tag{6.12}$$

where,

e is the index of economic variables and t is the index of the states of the economy (i.e., before and after the RDD attack).

In the PFRI model, the attacker's expected utility of each attack scenario was computed as a product of the overall success probability of theft (found using pathway analysis and probabilistic risk assessment methodologies) and the total attacker utility for a successful instance of each attack scenario. The attacker's disutility from a failed attack outcome is assumed to be -0.1 across all radionuclides and attack scenarios for the purpose of the RDD game. We define u_2, the attacker's utility function:

$$u_2(s_{1k,}s_{2k}) = \mathrm{EU}[\mathrm{M_k X_2}] = \mathrm{P_s}(\mathrm{M_k X_2}) \times \mathrm{U_{tot}}(\mathrm{M_k X_2}) - 0.1(1 - \mathrm{P_s}(\mathrm{M_k X_2})) \qquad (6.13)$$

where,

M_k attack the k_{th} radioactive material.

X_2 intent (theft) from player 2 (attacker)

P_s attacker's success probability of theft

U_{tot} total utility function assessing the attacker's intentions and radioactive material preferences.

Note that $u_2(s_{1k,}s_{2k})$ = -0.1 if and only if $s_{1k} = s_{2k}$

6.4 Model application to data

The normal form of a two-player game presents the payoffs from each strategy profile in the form of a matrix of ordered pairs giving the payoffs to each player from each pure strategy profile. The normal form of the RDD game is the matrix $\boldsymbol{U_{RDD}}$ of ordered pairs of elements from the payoff matrices $\boldsymbol{U_1}$ and $\boldsymbol{U_2}$:

$$\boldsymbol{U_{RDD}} = \begin{bmatrix} u_1(s_{1Co,}s_{2Co}), u_2(s_{1Co,}s_{2Co}) & u_1(s_{1Co,}s_{2Cs}), u_2(s_{1Co,}s_{2Cs}) & u_1(s_{1Co,}s_{2Ir}), u_2(s_{1Co,}s_{2Ir}) \\ u_1(s_{1Cs,}s_{2Co}), u_2(s_{1Cs,}s_{2Co}) & u_1(s_{1Cs,}s_{2Cs}), u_2(s_{1Cs,}s_{2Cs}) & u_1(s_{1Cs,}s_{2Ir}), u_2(s_{1Cs,}s_{2Ir}) \\ u_1(s_{1Ir,}s_{2Co}), u_2(s_{1Ir,}s_{2Co}) & u_1(s_{1Ir,}s_{2Cs}), u_2(s_{1Ir,}s_{2Cs}) & u_1(s_{1Ir,}s_{2Ir}), u_2(s_{1Ir,}s_{2Ir}) \end{bmatrix}$$

The payoffs of the normal form of the RDD game given below in Table 6.1, resulted from evaluating the utility functions u_1 and u_2 for consequence data and terrorist profiles developed for the St. Benedict scenario.

Table 6.1 The RDD game with pure strategy defender-attacker payoffs

RDD game – St. Benedict Healthcare				
	Attacker			
		Co	*Cs*	*Ir*
Defender	*Co*	0, -0.1	-0.15, 0.81	-0.084, 0.44
	Cs	-0.36, 0.89	0, -0.1	-0.084, 0.44
	Ir	-0.36, 0.89	-0.15, 0.81	0, -0.1

The "matching pennies" game is a classic example in game theory without any pure strategy Nash equilibria. The "matching pennies" game, as shown in Table 6.2, is played between two players – Even and Odd. Each player has a penny and must secretly turn the penny to heads or tails. The players then reveal their choices simultaneously. If the pennies match (both heads or both tails), then Even keeps both pennies, so wins one from Odd (+1 for Even, −1 for Odd). If the pennies do not match (one heads and one tails) Odd keeps both pennies, so receives one from Even (−1 for Even, +1 for Odd) (Fudenberg & Tirole, 1991). Like the "matching pennies" game, the RDD game lacks any pure strategy Nash equilibria. The RDD game has no dominated strategies, so there is no dominated strategy solution or solution resulting from the iterated elimination of dominated strategies (IEDS).

Table 6.2 A simple example game of “Matching Pennies”

Matching Pennies			
	Odd		
		Heads	Tails
Even	Heads	1, -1	-1, 1
	Tails	-1, 1	1, -1

Although there is not a canonical solution concept providing a pure strategy solution for the RDD game, applying a variation of the max-min solution concept results in a pure strategy solution that could be of interest to the defender. The max-min criterion states that it is rational for a conservative player to choose the strategy that maximizes their minimum possible payoff in the “worst-case” outcome resulting from the possible strategies of their opponent. The literature on max-min strategies describe them as “safety strategies” or “security strategies” because they enable the player to be certain that they have maximized the lower bound of possible outcomes of an otherwise highly uncertain game.

We consider the max-min strategy appropriate for a typical healthcare facility defender given the emphasis of the health physics profession on conservatism in risk assessment and preventing worst-case outcomes. It is not self-evident that the attacker would also use the max-min strategy. The more aggressive max-max strategy, in which the strategy allowing the maximum possible payoff is chosen, could be a better fit to terrorist psychology. If the defender commits to the max-min strategy, choosing to prevent a worst possible payoff of -0.36 by playing s_{1Co}, the attacker’s use of the max-max strategy resulting in the play of s_{2Co} would actually benefit the defender, giving the defender their best-case payoff of 0.

In the RDD game, the attacker is indifferent among their available pure strategies on the max-min criterion because their worst-case payoff is -0.1 for each pure strategy. Under the complete information assumption, the attacker would know that the defender is conservative. Thus, it would be rational for the attacker to infer that a conservative defender would play s_{1Co} to satisfy the max-min criterion if the game is limited to pure strategies. If the attacker infers that the defender would play a pure strategy of s_{1Co}, the attacker's best response would be to play s_{2Cs}, resulting in a pure strategy equilibrium solution of (s_{1Co}, s_{2Cs}) under a variation of the max-min equilibrium solution concept. Any unilateral deviation by the attacker from (s_{1Co}, s_{2Cs}) would result in a worse payoff for the attacker and a better payoff for the defender.

According to Nash (1951), every simultaneous one-shot game has at least one mixed strategy Nash equilibrium solution. For any strategy profile that is a Nash equilibrium, neither player could obtain a greater payoff by unilaterally deviating from the strategy profile. Hence player i would be indifferent between playing any of their pure strategies against the Nash equilibrium mixed strategy of their opponent, $\boldsymbol{\rho^*}_{\boldsymbol{-in}}$. It follows that for the RDD game there exists a Nash equilibrium mixed strategy profile $(\boldsymbol{\rho}^*_{\boldsymbol{1n}}, \boldsymbol{\rho}^*_{\boldsymbol{2n}})$ that can be obtained from the system of equations:

$$\rho^*_{1n}(U_2)^T(\hat{\imath})^T = \rho^*_{1n}(U_2)^T(\hat{\jmath})^T = \rho^*_{1n}(U_2)^T\left(\hat{k}\right)^T \tag{6.14}$$

$$\hat{\imath}U_1(\rho^*_{2n})^T = \hat{\jmath}U_1(\rho^*_{2n})^T = \hat{k}U_1(\rho^*_{2n})^T \tag{6.15}$$

where $\hat{\imath}, \hat{\jmath}, \widehat{k}$ are unit row vectors. The following system of equations is solved to determine the mixed strategy probabilities that are the components of the vectors $\boldsymbol{\rho}^*_{\boldsymbol{1n}}$ and $\boldsymbol{\rho}^*_{\boldsymbol{2n}}$**:**

$$\theta_1(s_{1Co})u_2(s_{1Co,}s_{2Co}) + \theta_1(s_{1Cs})u_2(s_{1Cs,}s_{2Co}) + (1 - \theta_1(s_{1Co}) - \theta_1(s_{1Cs}))u_2(s_{1Ir,}s_{2Co})$$

$$= \theta_1(s_{1Co})u_2(s_{1Co,}s_{2Cs}) + \theta_1(s_{1Cs})u_2(s_{1Cs,}s_{2Cs}) + (1 - \theta_1(s_{1Co}) - \theta_1(s_{1Cs}))u_2(s_{1Ir,}s_{2Cs})$$

$$= \theta_1(s_{1Co})u_2(s_{1Co,}s_{2Ir}) + \theta_1(s_{1Cs})u_2(s_{1Cs,}s_{2Ir}) + (1 - \theta_1(s_{1Co}) - \theta_1(s_{1Cs}))u_2(s_{1Ir,}s_{2Ir})$$

$$= \theta_2(s_{2Co})u_1(s_{1Co,}s_{2Co}) + \theta_2(s_{2Cs})u_1(s_{1Co,}s_{2Cs}) + (1 - \theta_2(s_{2Co}) - \theta_2(s_{2Cs}))u_1(s_{1Co,}s_{2Ir})$$

$$= \theta_2(s_{2Co})u_1(s_{1Cs,}s_{2Co}) + \theta_2(s_{2Cs})u_1(s_{1Cs,}s_{2Cs}) + (1 - \theta_2(s_{2Co}) - \theta_2(s_{2Cs}))u_1(s_{1Cs,}s_{2Ir})$$

$$= \theta_2(s_{2Co})u_1(s_{1Ir,}s_{2Co}) + \theta_2(s_{2Cs})u_1(s_{1Ir,}s_{2Cs}) + (1 - \theta_2(s_{2Co}) - \theta_2(s_{2Cs}))u_1(s_{1Ir,}s_{2Ir})$$

After obtaining the mixed strategy probabilities for a Nash equilibrium, the mixed strategy payoffs are computed as follows:

$$E[u_1] = \boldsymbol{\rho^*}_{\boldsymbol{1n}}\boldsymbol{U_1}(\boldsymbol{\rho}^*_{\boldsymbol{2n}})^{\boldsymbol{T}} \tag{6.16}$$

$$E[u_2] = \boldsymbol{\rho^*}_{\boldsymbol{1n}}\boldsymbol{U_2}(\boldsymbol{\rho}^*_{\boldsymbol{2n}})^{\boldsymbol{T}} \tag{6.17}$$

The results of the mixed Nash equilibrium solution are shown in Table 6.3.

Table 6. 3 The RDD game mixed strategy Nash equilibrium solution

RDD game mixed strategy Nash equilibrium solution			
	mixed strategy probabilities		mixed strategy payoffs
Defender	$\theta_1(s_{1Co})$	0.49	-0.09
	$\theta_1(s_{1Cs})$	0.45	
	$\theta_1(s_{1Ir})$	0.06	
Attacker	$\theta_2(s_{2Co})$	0.13	0.40
	$\theta_2(s_{2Cs})$	0.31	
	$\theta_2(s_{2Ir})$	0.56	

6.5 RDD game result

Game-theoretic models augment risk indexes such as the PFRI by providing decision makers with the capability to optimize their defenses against the predicted behavior of terrorist adversaries. Game theory could be used for decision making to bolster risk-informed radiological security. Our evaluation of the results of the RDD game for the St. Benedict Healthcare scenario results in an actionable security policy recommendation for the healthcare sector.

The RDD game uses recursive functions to model the adaptive response of terrorists to the defensive countermeasures of healthcare facilities, but the RDD game includes assumptions of rationality, common knowledge, and the availability of mixed strategies that may not be realistic in RDD scenarios (Bier et al., 2009). The mixed strategy Nash equilibrium solution of the RDD game has the payoff $u_1(\rho_{1n}^*, \rho_{2n}^*) = -0.09$, whereas the pure strategy solution under a variation of von Neumann's max-min solution concept has the payoff $u_1(s_{1Co}, s_{2Cs}) = -0.15$. The mixed Nash solution is preferable to the pure von Neumann max-min solution if two necessary conditions for its existence obtain: (1) mixed strategies are feasible for both players; and (2) both players correctly believe that their opponent is committed to the mixed strategy Nash equilibrium profile. Conditions (2) is not provided by the definition of common knowledge.

Condition (1) is unlikely to be satisfied for the terrorist attacker or the healthcare defender. There is some evidence that terrorists randomize their strategies, e.g., Timothy McVey claimed that he randomly turned to a phone book page to target the Alfred P. Murrah building in Oklahoma City (Wasson & Bluesteen, 2017). However, it is unlikely that many terrorists would be sufficiently familiar with game theory to compute Nash equilibrium mixed strategies (Pomper et al., 2014). Condition (1) appears unlikely for a real healthcare facility to satisfy due to the difficulty of randomizing defenses, which are typically static and continuously operating at full capacity. Mixed strategies have been implemented for the Department of Homeland Security to randomize patrols or surveillance of vital large-scale infrastructure, e.g., the assistant for randomizing monitoring over routes (ARMOR) deployed at the Los Angeles International Airport (Pita et al., 2009). Although the deployment at healthcare facilities of enhanced security patrols could be randomized, it would be difficult to persuade decision makers to invest in these costly security upgrades only for the purpose of deploying them randomly in support of a mixed strategy.

We have shown that condition (1) is unlikely to be satisfied in a realistic RDD game. If condition (1) is not satisfied, condition (2) cannot be satisfied because both players need to correctly believe that their opponent is committed to a mixed strategy, and such a belief cannot be correct if mixed strategies are infeasible. If the necessary conditions for a Nash equilibrium are unlikely to exist in a real instance of the RDD game, the Nash equilibrium solution is not robust for determining the optimal defense policy of the healthcare facility.

The max-min solution concept is highly robust under conditions of severe uncertainty because it gives the certain result that the lower bound on the uncertain payoffs is maximized. The necessary assumptions for the max-min equilibrium solution to exist in a real RDD game are rationality and common knowledge. Real world players do not possess the perfect rationality and common knowledge of an idealized game-theoretic model, but human behavior in real conflicts between terrorists and security forces is a reasonable approximation of these assumptions (Guikema, 2009). Thus, we find that the von Neumann max-min solution of (s_{1Co}, s_{2Cs}) is the most prescriptive result of the RDD game from the standpoint of healthcare sector security policy.

National and international organizations like the International Atomic Energy Agency (IAEA), the Nuclear Regulatory Commission (NRC), the National Nuclear Security Administration (NNSA) and the Health Physics Society (HPS) recommend replacing cesium chloride ($CsCl$) blood irradiators with alternate technologies (Pomper et al., 2014). The von Neumann max-min equilibrium solution of defending cobalt and attacking cesium confirms cesium's attractiveness to terrorists as an RDD weapon, providing an additional incentive to the current cooperative risk mitigation efforts to replace radioactive materials with alternate technologies. Implementing a policy of replacing the cesium source with an alternate technology in the St. Benedict Healthcare scenario affects the equilibrium solutions as shown in Table 6.4.

Table 6. 4 The RDD game reduced matrix upon source *(CsCl)* replacement

RDD game – reduced matrix upon source replacement			
	Attacker		
		Co	*Ir*
Defender	*Co*	0, -0.1	-0.084, 0.44
	Ir	-0.36, 0.89	0, -0.1

The max-min solution to the updated RDD game after the replacement of cesium blood irradiator with X-ray technology gives a strategy profile $\left(s_{1Co,}s_{2Ir}\right)$ with the payoffs $u_1\left(s_{1Co,}s_{2Ir}\right) = -0.084$ and $u_2\left(s_{1Co,}s_{2Ir}\right) = 0.44$. This solution is favorable to the defender because the defender's payoff is the second best possible (their best outcome would be u_1=0) and the attacker's payoff is the second worst possible (their worst outcome would be u_2 = -0.1). The defender's strategy has influenced the attacker to target iridium, which has significantly lower consequences for society than an RDD attack targeting cobalt or cesium.

A final consideration for applying the RDD game results to the healthcare sector is the need to comply with medical ethics and society's expectations for the healthcare sector. The RDD game gives the defender strategic options that can be interpreted as possible allocations of a defense upgrade available for only one of the three sources at a time. This simplified idealization captures the trade-offs inherent in budgeting scarce security resources. A realistic policy prescription following from the RDD game would be to replace the cesium source with an alternate technology and divide the available security resources equitably between the two remaining sources cobalt and iridium. A risk informed cost-benefit analysis drawing on input from the PFRI and the RDD game can ensure that each healthcare facility uses its security budget optimally to reduce the RDD threat.

CHAPTER 7. CONCLUSION AND FUTURE WORK

This research developed a risk-based methodology to evaluate facility-level radiological security. The methodology was applied to an RDD incident from three radionuclides of concern: ^{137}Cs, ^{60}Co, and ^{192}Ir. The results of the research have lead to the creation of a potential facility risk index (PFRI) for radiological security. The PFRI framework is based on the triplet definition of risk: threat, vulnerability, and consequences.

The first component of the PFRI, threat, uses both the IAEA radionuclide categorization system and the physical form of the radionuclide in the calculation of asset utility. The methodology employs multi-attribute utility functions and Pierce's semiotic three-part triangle to bias adversary decision making based on their motivations. Pathway analysis and elements of probabilistic risk assessment are used to develop pathways that an adversary can utilize to execute the theft of the radionuclide materials of concern. A game-theoretical model is used to bolster risk-informed decision making by replicating the strategic decision making of the adversary intent on executing the threat that maximizes their benefit.

The second component of the PFRI, vulnerability, includes locational hazards and nuclear security culture of the healthcare facility as weaknesses or gaps that, if neglected, would render the facility assets open to exploitation. Factor analysis was used as a statistical tool to assess the vulnerability.

The methodology used for the final component of PFRI, consequences, accounts for effects of blast and fragmentation from the explosive and deterministic and stochastic effects from radiation. This in line with the GAO's comments (U.S. GAO, 2019) and accounts for socioeconomic consequences from an RDD incident. To make the PFRI methodology available to the healthcare facility management, a GUI based PFRI tool was developed in MATLAB utilizing a Microsoft Excel database. The code results matched the St. Benedict RDD asset scenario results manually calculated in the initial phase of the process.

7.1 PFRI Implementation

The PFRI may be implemented by healthcare facility staff using a standard process to conduct self-assessments. To begin the process, a healthcare facility would obtain the PFRI GUI Tool. The explanation of the PFRI GUI Tool given in chapter 5 can be expanded to a user manual that may be consulted by facility staff. After gathering locational hazard vulnerability data, conducting the technical and general nuclear security culture surveys, generating terrorist adversary threat profiles, calculating the success probability of theft and sabotage scenarios, and gathering local economic data, the necessary information would be inputted to the PFRI GUI Tool to obtain a PFRI value for the facility. Calculating the success probability of theft and sabotage will vary depending on the layout of the facility. The adversary task sequence path and the adversary task time would depend on the performance of the facility's security features (detection delay and response), which may be tested in timed drills or other simulations to obtain an accurate self-assessment.

Upon completing a self-assessment, facility staff would evaluate their PFRI value on the heat map to determine whether an urgent security problem exists and where the greatest weaknesses lie. If the PFRI value is found to be in the red or yellow bands, immediate action to reduce the PFRI value to a level in the green band is highly recommended. If the PFRI value is found to be in the green band, an urgent security problem does not exist, but the PFRI remains a useful tool to sustain and improve the level of security. The three main factors determining the PFRI value that are controlled by the facility are security culture vulnerability, the physical protection system, and the adoption of alternate technologies. PFRI values in the upper left quadrant of the heat map (yellow band) are more sensitive to improvements in nuclear security culture, and PFRI values in the lower right quadrant (yellow band) are more sensitive to improvements in detection and delay components of the security system. PFRI values in the upper right quadrant of the heat map (red band) indicate the existence of an urgent security problem, and immediate upgrades to nuclear security culture and physical security systems or the adoption of alternate technologies would significantly reduce the PFRI value. Perhaps the greatest benefit of using the PFRI is for comparison with similar facilities. Although a direct comparison is likely not feasible, a facility could still use the information in the PFRI to better understand differences and similarities in their radiological security parameters.

For a healthcare facility with a PFRI value in the green band, immediate security improvements may not be necessary. However, a healthcare facility would typically have a budget for maintaining and upgrading its security systems over time. If funds are available to plan for incremental security investments over the long-term, a Cost Effectiveness Analysis (CEA) can be conducted to select the optimal allocation of the security budget funds among a menu of possible security investments. CEA compares Cost Effectiveness Ratios (CERs), selecting the combination of security investments that has the lowest CER while satisfying a budget constraint. For a study of the cost-effectiveness of potential security upgrades to lower the PFRI value, CER = $\frac{\Delta C}{\Delta E}$, where ΔC is the total cost of a combination of security upgrades and ΔE is the total reduction in PFRI value that would result from the upgrades.

Table 7.1 Illustration of CEA Methodology

Security Upgrade	Cost per Unit	PFRI Reduction per Unit	Per Unit CER
Security Culture Training Course	$100,000	0.2	$500,000
Security Camera	$700	0.001	$700,000
Alternate Technology	$590,000	0.6	$983,333

For the purpose of illustrating the CEA methodology, Table 7.1 gives fictional costs and associated PFRI reductions for security upgrades. Given a security budget of $590,000 and assuming that PFRI reductions scale linearly with additional units of each security upgrade, CEA would result in a budget allocation of $500,000 for five courses of security culture training and $89,600 for additional security cameras resulting in a CER of $523,050 and a total PFRI reduction of 1.128. To complete a CEA analysis of possible security upgrades, the healthcare facility staff would use the PFRI GUI Tool to determine the total reduction in PFRI for each combination of upgrades, and the combination with the lowest CER would be selected.

Public Policy and International Implications of PFRI

The PFRI is a novel risk index and is still under development. A discussion of the policy implications of the PFRI is not necessarily premature but may be viewed as an aspirational statement of the potential future uses of the PFRI that have motivated its development. One major policy implication of the PFRI research, discussed in chapter 6, is the suggestion that adopting alternative technologies significantly reduces the radiological terrorism risk.

Widespread adoption of the PFRI among a nation's healthcare facilities could provide nuclear regulatory agencies with a database of local PFRI data. Aggregating local facility level PFRI values can inform policy for a nation's overall RDD defense strategy. If a nation were to provide facilities with additional RDD security funding, a PFRI based worksheet could be used to apply for grants. The nation's nuclear agencies tasked with coordinating RDD defense could prioritize funding security upgrades to the facilities with the highest PFRI values. An equitable national RDD defense strategy should tend to equalize the PFRI values of all facilities. A policy that promotes large inequalities between the PFRI values of facilities may transfer the risk of RDD attack from facilities that are able to lower their PFRI values to those facilities whose PFRI values remain relatively high. Rational and intelligent terrorist adversaries could potentially adapt to the unequal defenses of facilities by targeting facilities that did not make any security upgrades during a time period when other facilities made significant upgrades. Possibly, suboptimal allocation of funds for RDD defense could result in defenses being upgraded at facilities with relatively low PFRI values that terrorist groups would not have considered attacking in any case.

Adoption of the PFRI by many IAEA member States would result in a wealth of data being made available to the radiological security community. Comparisons of PFRI values between particular groups of facilities in different countries would be useful. International comparisons of programs to lower PFRI values would enable nations to share lessons learned. The risk transfer problem encountered when security upgrade programs result in disparities in PFRI values within nations applies also for disparities between nations. IAEA member States should make a cooperative effort to reduce vulnerability to the RDD threat.

The PFRI's asset utility function incorporates the IAEA categorization of relative attractiveness of radioactive materials. Nations using other categorization systems would face a barrier to adoption of the PFRI unless they convert to the IAEA categorization. Widespread international adoption of the PFRI would bring nations into conformity with the IAEA categorization system, increasing the commensurability between national data sets. It may be challenging to persuade some nations' nuclear agencies to adopt the PFRI if the string of conformity with the IAEA categorization system is attached. Among other factors, bureaucratic inertia – the tendency of government workers to avoid unnecessary effort - would be a major obstacle to the international spread of the PFRI. Typically, the PFRI would be adopted in a particular nation through a top-down mechanism, with the nuclear agency encouraging and supporting its implementation at the facility level. In the event that a particular nation's bureaucracy would reject the PFRI, it is possible that support for the PFRI among health physics professionals and other elements of civil society could result in a bottom-up adoption of the PFRI in the nation.

7.2 PFRI Validation & Contribution to Scientific Knowledge

The PFRI is the result of interdisciplinary research drawing on physics, health physics, social science, terrorism studies, and economics. Assessing the level of validation obtained for the PFRI and its contribution to scientific knowledge requires an appropriate scientific standard that can span the variety of scientific methods used in each of the disciplines relevant to the PFRI. According to Creswell (2014), the appropriate research framework for a particular topic harmonizes the elements of epistemic views (postpositivist, constructivist, transformative, pragmatic), research approach (quantitative, qualitative, or mixed-methods), research design, and research methods.

A pragmatic epistemic view shapes the PFRI research because this view is appropriate for research motivated by the purpose of solving a specific problem (Creswell, 2014), and pragmatism also gives the flexibility needed to engage with the diverse and inconsistent epistemic views that may be encountered during interdisciplinary research. The pragmatic epistemic view is pluralistic, allowing the mixing of disparate epistemic views when necessary to tackle a problem (Creswell, 2014), so we have retained the postpositivist view emphasizing quantitative empirical research where it would be appropriate. Table 7.2 shows the validation and novel contribution to scientific knowledge achieved for each subcomponent of the PFRI.

We adopt a definition widely used in the computer modeling community of a *validated model* being a model with an accurate enough representation of reality to be adequate for its intended purpose (Breisbart, 2019). When scientific statements other than models are discussed, *validation* refers to evaluating scientific statements according to the accepted standard of scientific knowledge for the particular discipline being discussed. Because we worked across several disciplines that disagree about the definition of validation, this pluralistic approach was appropriate.

Validation of the PFRI as a risk metric would show that the PFRI adequately reflects the level of risk to healthcare facilities of an RDD attack for the purpose of assessing and enhancing facility security. Three objectives (discussed in chapter 1) were set for the performance of the PFRI to ensure the adequacy of risk measurement: 1) identify threats to facilities, collecting information about the likely adversaries and attack scenarios; 2) measure facility vulnerability in terms of locational hazards and security culture; and 3) measure the loss of life and economic consequences of an RDD attack on the facility. Validation of the PFRI relates to objectives (1-3) at two levels. At the first level, the model of RDD risk as the product of the three components of threat, vulnerability, and consequences may be validated. At the second level, the subcomponents used to obtain threat, vulnerability, and consequences can each be separately validated.

Validating the overall PFRI model largely depends on the validation previously established for the triplet definition of risk. The PFRI model specification follows the triplet definition of risk, a definition that has been endorsed by the IAEA, NRC, and GAO. The triplet definition of risk is considered generalizable to measuring any type of risk with quantifiable threat, vulnerability, and consequences components (Kaplan & Garrick, 1981). The widespread and longstanding acceptance of the validation of the triplet definition of risk as a general risk metric applicable to market risk, business risk, social risk, economic risk, health & safety risk, and geopolitical risk gives strong assurance that the central mathematical formalism of the PFRI has been validated (Kaplan & Garrick, 1981). The triplet definition of risk is a widely used and validated approach to modeling terrorism risk (Garrick et al., 2004).

The occurrence of RDD attacks is necessary to empirically test the PFRI model, but such attacks are precisely the events that the model is intended to prevent. An interesting paradox of PFRI research is that if the research is successful and the PFRI truly is a highly effective tool for preventing RDD terrorism, it is possible that no RDD attack would ever occur as a direct result of the research's success. In this case (whose likelihood of occurring we do not assess), it would never be possible to empirically validate the PFRI model because the model's existence would prevent the data necessary for its empirical validation from becoming available. Sparse empirical data is a generic problem for terrorism research (Schuurman, 2018). The occurrence of the large number of RDD attacks necessary for maximum empirical validation of the PFRI model is undesirable from an ethical or policy standpoint because it would entail assive failure to prevent RDD terrorism.

The need for a risk-informed defense against RDD attacks is urgent. Under the pragmatic epistemic view that is appropriate for counter-terrorism research, the best available methods and data must be applied to solve the urgent problem of preventing RDD attacks. Although the PFRI is not intended to predict the exact time, location, and scenario specifics of an RDD attack as a sort of early warning system, the PFRI is a sufficiently accurate metric of healthcare facility RDD attack risk for the purpose of informing decisions by security staff and policy makers that can significantly lower the risk of RDD attack.

The second level of validation for the PFRI methodology involves the discussion of the separate validation of each PFRI subcomponent given below in Table 7.2.

The PFRI model is further validated to the extent that its subcomponents are each separately validated. Future incremental improvements to the quality of data and methods used to compute threat, vulnerability, and consequences in the PFRI can increase confidence in the index.

Table 7. 2 The PFRI model validation and Novel contribution to scientific knowledge.

Sub-Components	**Validation**	**Novel Contriution to Scientific Knowledge**
The PFRI Model	The triplet definition of risk has been endorsed by the IAEA, NRC, and GAO.	A novel application of the risk triplet applied to the problem of RDD terrorism. The PFRI heat map is a novel translation of a quantitative risk metric to a qualitative scale.
THREAT		
U[adversary]	Swing weights can be elicited from subject matter experts or the intelligence community.	Novel formulation of terrorist threat group utility functions for the RDD threat.
U[material]	The categorizaiton of radioactive materials is accepted by the IAEA.	Novel use of radioactive material form in a utiity function.
Pathway Analysis	Pathway analysis is a standard methodology for assessing the effectiveness of physical protection systems at nuclear facilities (Garcia, 2007)	Novel application of pathway analysis to healthcare facilties and RDD scenarios.
Probabilistic Risk Assessment	Validated by reactor safety studies and aviation industry studies (WASH-1400).	Novel application to healthcare facilitiy RDD scenarios in conjunction with pathway analysis.
VULNERABILITY		
Locational Hazard Index	Locaitonal hazard index methodology developed by Zurovec et al. (2017)	Novel application of the locational hazard index methodology to RDD scenarios.
Security Culture Survey	The IAEA Nuclear Security Culture Guidelines are generally accepted by the IAEA member States.	Novel security culture survey designed to assess healthcare implementation of radiological security culture.
CONSEQUENCES		
Human Casualties - Fragmentation	Two fragmentation concepts developed and used by the U.S. military, hazard fragmentation distance probability of kill and damage criteria for fragmentation warheads, are the basis of the PFRI's model of deaths and injuries from blast fragmentation effects (GICHD, 2017).	The incorporation of the hazard fragmentation distance probability of kill and damage criteria for fragmentaiton warheards is basic physics and therefore not particularly novel.
Human Casualties - Blast Scaling Law	The blast scaling law is universally accepted (U.S.NRC., 2015).	The use of the blast scaling law in this research is not particularly novel.
Stochastic Effects - HOTSPOT	HOTSPOT is a gaussian plume model software for radiological releases developed at Lawrence Livermore National Lab (US EPA, 1999). Per capita risk coefficients for the year 2020 U.S. population from the Federal Guidance Report No. 13 were used to calculate the mortality and morbidity risks (Homann & Aluzzi, 2013).	The TEDE values simulated from HOTSPOT were used with the per capita risk coefficients to estimate cancer fatalities and morbidities for the PFRI.
Economic Loss - CBA & VSL	The CBA methodology is widely accepted as validated for the purpose of planning for natural disasters and terrorism by numerous professional organizations, government agencies, and courts of law (Boardman, 2011). Loss of life consequences were valued using a VSL methodology that is widely accepted (Boardman, 2011; Viscusi & Masterman, 2017).	A unique template for the facility self-assessment of RDD attack consequences is offered in the PFRI GUI Tool.
Economic Loss - Decontamination Cost	The decontamination and replacement cost rates used by Sandia Labs' RADTRAN 5 model are suitable to estimate the total decontamination cost of an RDD event (Reichmuth, Short & Wood, 2005).	The application of the previously established decontamination and replacment cost rates is not novel.

7.3 Future Directions for Research

Future directions for research may be grouped by the PFRI components of threat, vulnerability and consequences. The threat component could be significantly improved through additional research. Subject matter experts in the intelligence community could be surveyed to obtain better validated swing weights for $U[adv]$ (Rosoff & John, 2011)). The probability of attack is generally difficult to estimate for all categories of terrorism research. The use of some geopolitical threat index or access to intelligence community warnings about emerging RDD threats are possible ways that a probability of attack could be added to the threat component of the PFRI.

The threat component of the PFRI may be augmented by additional future game-theoretic research. The RDD Game presented in chapter 6 is one of many possible game-theoretic models that would be appropriate for radiological terrorism. The RDD Game itself may be enhanced to allow the defender to allocate a variable share of its budget for defense upgrades to each of the three radionuclides (as opposed to the current model, where the defense upgrade is a fixed investment permitted for only one among the three radionuclides). A game-theoretic model of terrorist target selection for a scenario to simultaneously attack multiple targets each located in different cities is another example of the potential future research.

The vulnerability component is less complex than the others but provides several opportunities for future research. More locational hazard vulnerability index data and culture survey data could be collected for a large number of additional healthcare facilities. Industrial facilities and university reactors are facility types with potential vulnerability to the RDD threat that should also be studied. Appropriate security culture studies for industrial facilities and university reactors could be designed, and other adjustments of the PFRI methodology to encompass additional facility types could be researched. Other RDD scenarios involving the diversion of sources (considering escape routes) or attacks on multiple facilities could be studied under the PFRI methodology.

The consequences component offers broad scope for future research due to the variety of disciplines, models, and data types included in this component. Better software could be obtained to model blast effects. The consequences model could be extended to include the radionuclides and other parameters that would be appropriate for RED attack scenarios. The 1995 Oklahoma City bombing provides excellent data for modeling deaths, injuries, and economic losses from a terrorist bomb blast (Mallonee et al., 1996)), but useful data for other terrorist bombings could be collected, such as the 1983 Beirut, Lebanon bombing of a U.S. marine barracks or the 1996 Khobar Towers bombing in Al Khobar, Saudi Arabia. C_{EL} estimates only first order economic consequences, but C_{EL} could be extended to include second order effects estimated by a computable general equilibrium model or some other type of macroeconomic model.

Experimental methods involving time study drills or other testing of security equipment could provide reliable reference data estimating the probabilities of detection and interruption used in the pathway analysis. It should be noted that the PFRI facility self-assessment process enables facility security staff to input private information on the performance of their own security systems into the PFRI GUI Tool, resulting in a PFRI value that would be more accurate than what could be obtained by an outsider to the facility.

The PFRI GUI Tool can be continuously improved and updated over time. Possibly, facility PFRI self-assessment values can be reported in real time. PFRI GUI Tool users may possibly develop interesting modified versions of the software.

APPENDIX A. SURVEYS

A.1. Survey for a healthcare facility

General nuclear security awareness survey

Belief and Attitude

1. I clearly know the difference between safety and nuclear and radioactive material security?
2. Threats on nuclear and radioactive material are increasing domestically and globally?
3. Nuclear and radioactive material security is as important as safety?
4. I consider myself personally responsible for security in my role at the IU Medical Center?

Leadership/Management

1. Management at the IU Medical Center communicates to us to the importance of security in many ways?
2. Management frequently inspects my work to ensure that procedures are being followed as expected?
3. All work at the IU Medical Center is planned and managed to ensure that the nuclear security is not compromised?
4. Procedures or contingency plans are easily and immediately available when needed?
5. Management involves staff members in the risk assessment and decision-making processes and other activities that affect them?
6. Management at IU Medical Center demonstrate a sense of urgency to correct significant security weaknesses or vulnerabilities?

Policy

1. I am aware of the policy at the IU medical center on nuclear and radioactive material security?
2. Media based communication systems (email, newsletters, etc.) are used at the IU Medical Center to disseminate policies regarding security to management and staff?
3. IU Medical Center has in place written policies, rules or procedures for termination of employment as they pertain to security of radioactive sources?

4. Every employee at the IU Medical Center is held accountable for adherence to established policies and procedures?
5. Action is taken by IU Medical Center when nuclear and radioactive material security performance does not meet expectations?
6. Security policy is reviewed and updated regularly with participation from senior management?

Enforcement

1. I was instructed during radiation safety training on requirements for reporting security violations or issues?
2. Penalties are applied to motivate personnel to follow procedures?
3. Regular management meetings at the IU Medical Center cover significant security related items?
4. I feel comfortable reporting any security violations or suspicions without fear of subsequently suffering disciplinary actions?
5. I find nuclear and radioactive material security related guides, training and procedures helpful and easy to understand?
6. I am informed of events related to threats and their potential bearing on nuclear security and nuclear security policy?
7. Management encourages me to seek, when necessary, clarification regarding my role and responsibility for safeguarding radioactive sources?

Technical nuclear security awareness survey

Detect

- IU Medical Center possesses measures for the detection of an attempt or an actual removal and/or sabotage of radioactive material?
- The IU Medical Center has the means to detect loss of radioactive sources/equipment through verification (Standard Operating Procedures)?
- Continuous surveillance or monitoring (CCTV, Alarms) are in place at the IU Medical Center to detect intrusions or unauthorized access?

Deter

- There is at least two layers of barriers (e.g. wall, cages) present at the IU Medical Center which together provide delay sufficient to enable response personnel to interdict?

Response

- IU Medical Center possess capabilities for an immediate response with size, equipment and training to interdict?
- Contingency plans are in place to guide the response team to malicious acts or equipment failure within the facility?
- Contingency plans are tested and coordinated with off-site backup forces.
- Provisions are in place at the IU Medical Center to ensure that security can be adjusted in response to an increased threat?

Accountability and Security awareness

- I believe radioactive material present at the hospitals are soft targets for terrorist?
- I am aware of the type of radioactive material used in the hospital for therapy or imaging?
- Each radioactive source is periodically inventoried and accounted for and would not go unnoticed if it is missing or stolen?
- Personnel responsible for a radioactive source, maintains record for that source, which includes relevant information about its characteristics?
- Is the use of alternative technology such as, X-ray irradiators, LINAC and cyclotrons making medical devices more prone to cyber-attacks?
- Access to confidential information is restricted to those who need such access and have been subjected to a trustworthiness check? (insider threat)
- Identification and verification, for example, swipe card reader or key code access controls are implemented at the IU Medical Center to restrict unauthorized personnel access?
- Visitors or patient's family members are not authorized to enter a restricted area without an escort?
- The security requirements should be adapted depending on whether the radioactive material is sealed, unsealed or waste?
- At the IU Medical Center, the associated security levels are implemented based on the attractiveness of radioactive material?

Transport

- Movement of packages containing radioactive materials are most vulnerable to an unauthorized access? (PP is least effective)
- Transportation of radioactive material inside the IU Medical Center is a secure process?
- Does the transport security system include measures to deter, detect and delay unauthorized access to radiological material while in transit?
- Measures are taken to determine the trustworthiness of individuals involved in shipping and receiving packages of radioactive sources?

Training

- All security systems are tested periodically including systems that are not activated during normal operation?
- Is IU Medical Center’s radiological security culture, blended into an overall security regime of the hospital?
- Is hospital security, including the radiological security exercised 24/7 at the IU Medical Center?
- Staff members at the IU medical center are trained on the secure use, storage and disposal of radioactive material?
- Training is provided to guide personnel in identifying suspicious behaviors in and around the IU Medical Center?
- Rewards and promotion systems are in place to recognize staff members contribution toward improving security?

- I believe that the hospitals or medical centers are at a higher risk of sabotage, unauthorized access or theft from terrorist groups to conduct a malicious act (Radiological Dispersal Device (RDD) or ‘dirty bomb’)?

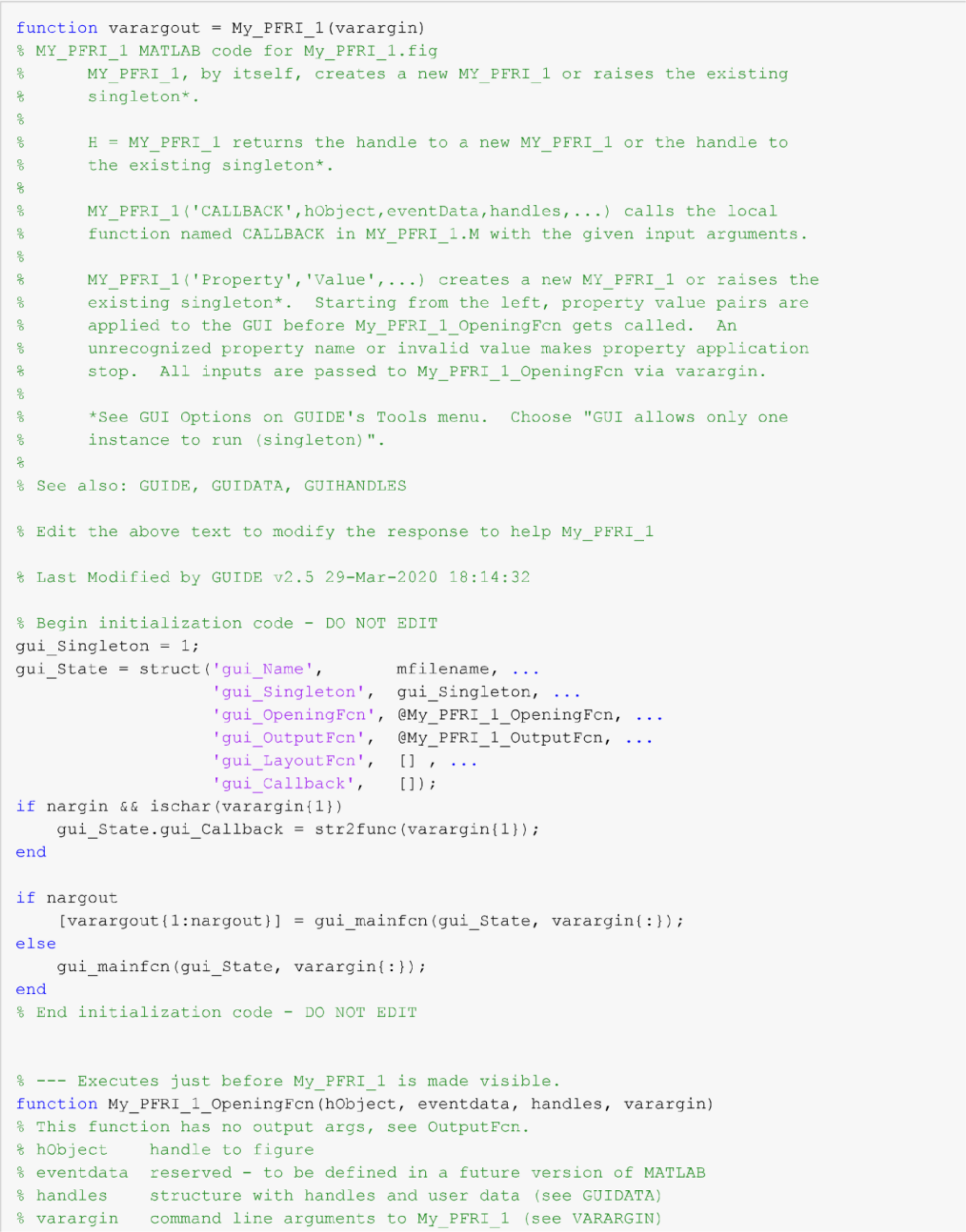
A.2. Possible combinations of threat adversary profiles

Loss of Life			**Economic Loss**			**Symbolic Loss**			
High	**Medium**	**Low**	**High**	**Medium**	**Low**	**High**	**Medium**	**Low**	**Adversary Utility**
		1			1			1	0.76
	1				1			1	0.78
1					1			1	0.82
		1		1				1	0.86
	1			1				1	0.88
		1	1					1	0.89
	1		1					1	0.91
1				1				1	0.92

1			1					1	0.95
		1			1		1		0.99
	1				1		1		1.01
1					1		1		1.05
		1		1			1		1.09
	1			1			1		1.11
		1	1				1		1.13
		1			1	1			1.13
	1		1				1		1.15
1				1			1		1.15
	1				1	1			1.15
1			1				1		1.18
1					1	1			1.19
		1		1		1			1.23
	1			1		1			1.25
		1	1			1			1.27
	1		1			1			1.28
1				1		1			1.29
1			1			1			1.32

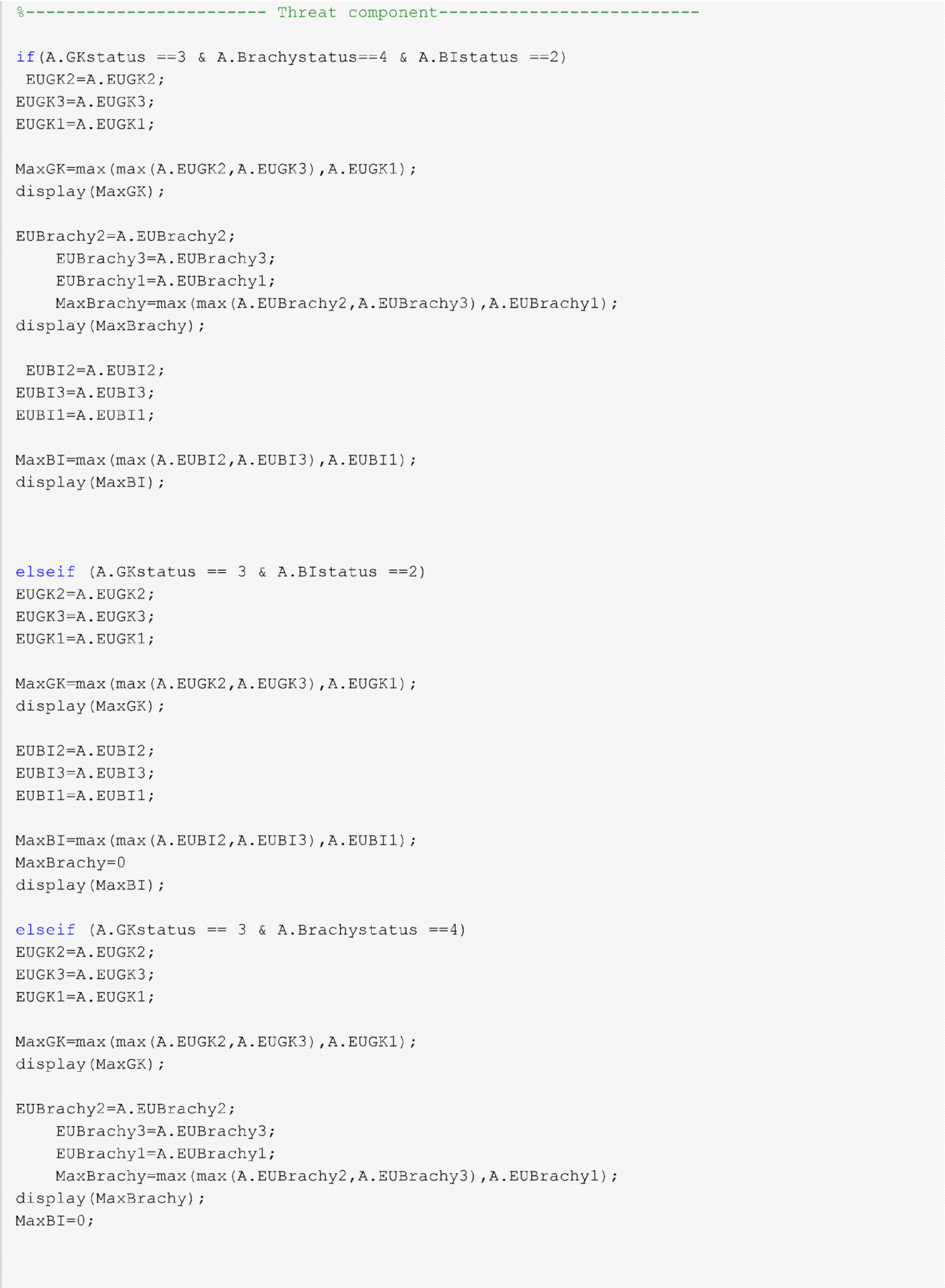
APPENDIX B. MATLAB CODE

B.1. The PFRI Tool



```
function varargout = My_PFRI_1(varargin)
% MY_PFRI_1 MATLAB code for My_PFRI_1.fig
%      MY_PFRI_1, by itself, creates a new MY_PFRI_1 or raises the existing
%      singleton*.
%
%      H = MY_PFRI_1 returns the handle to a new MY_PFRI_1 or the handle to
%      the existing singleton*.
%
%      MY_PFRI_1('CALLBACK',hObject,eventData,handles,...) calls the local
%      function named CALLBACK in MY_PFRI_1.M with the given input arguments.
%
%      MY_PFRI_1('Property','Value',...) creates a new MY_PFRI_1 or raises the
%      existing singleton*.  Starting from the left, property value pairs are
%      applied to the GUI before My_PFRI_1_OpeningFcn gets called.  An
%      unrecognized property name or invalid value makes property application
%      stop.  All inputs are passed to My_PFRI_1_OpeningFcn via varargin.
%
%      *See GUI Options on GUIDE's Tools menu.  Choose "GUI allows only one
%      instance to run (singleton)".
%
% See also: GUIDE, GUIDATA, GUIHANDLES

% Edit the above text to modify the response to help My_PFRI_1

% Last Modified by GUIDE v2.5 29-Mar-2020 18:14:32

% Begin initialization code - DO NOT EDIT
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @My_PFRI_1_OpeningFcn, ...
                   'gui_OutputFcn',  @My_PFRI_1_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end
% End initialization code - DO NOT EDIT


% --- Executes just before My_PFRI_1 is made visible.
function My_PFRI_1_OpeningFcn(hObject, eventdata, handles, varargin)
% This function has no output args, see OutputFcn.
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% varargin   command line arguments to My_PFRI_1 (see VARARGIN)
% Choose default command line output for My_PFRI_1
handles.output = hObject;

% Update handles structure
guidata(hObject, handles);

% UIWAIT makes My_PFRI_1 wait for user response (see UIRESUME)
% uiwait(handles.figure1);


% --- Outputs from this function are returned to the command line.
function varargout = My_PFRI_1_OutputFcn(hObject, eventdata, handles)
% varargout  cell array for returning output args (see VARARGOUT);
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Get default command line output from handles structure
varargout{1} = handles.output;

global checkboxStatus;



% --- Executes on button press in threat_push.
function threat_push_Callback(hObject, eventdata, handles,varargin)
% hObject    handle to threat_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
Threat_gui


% --- Executes on button press in vul_push.
function vul_push_Callback(~, eventdata, handles)
% hObject    handle to vul_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
Vul_gui;

% --- Executes on button press in conseq_push.
function conseq_push_Callback(hObject, eventdata, handles)
% hObject    handle to conseq_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
Blast_gui;


% --- Executes on button press in PFRI_push.
function PFRI_push_Callback(hObject, eventdata, handles)
```

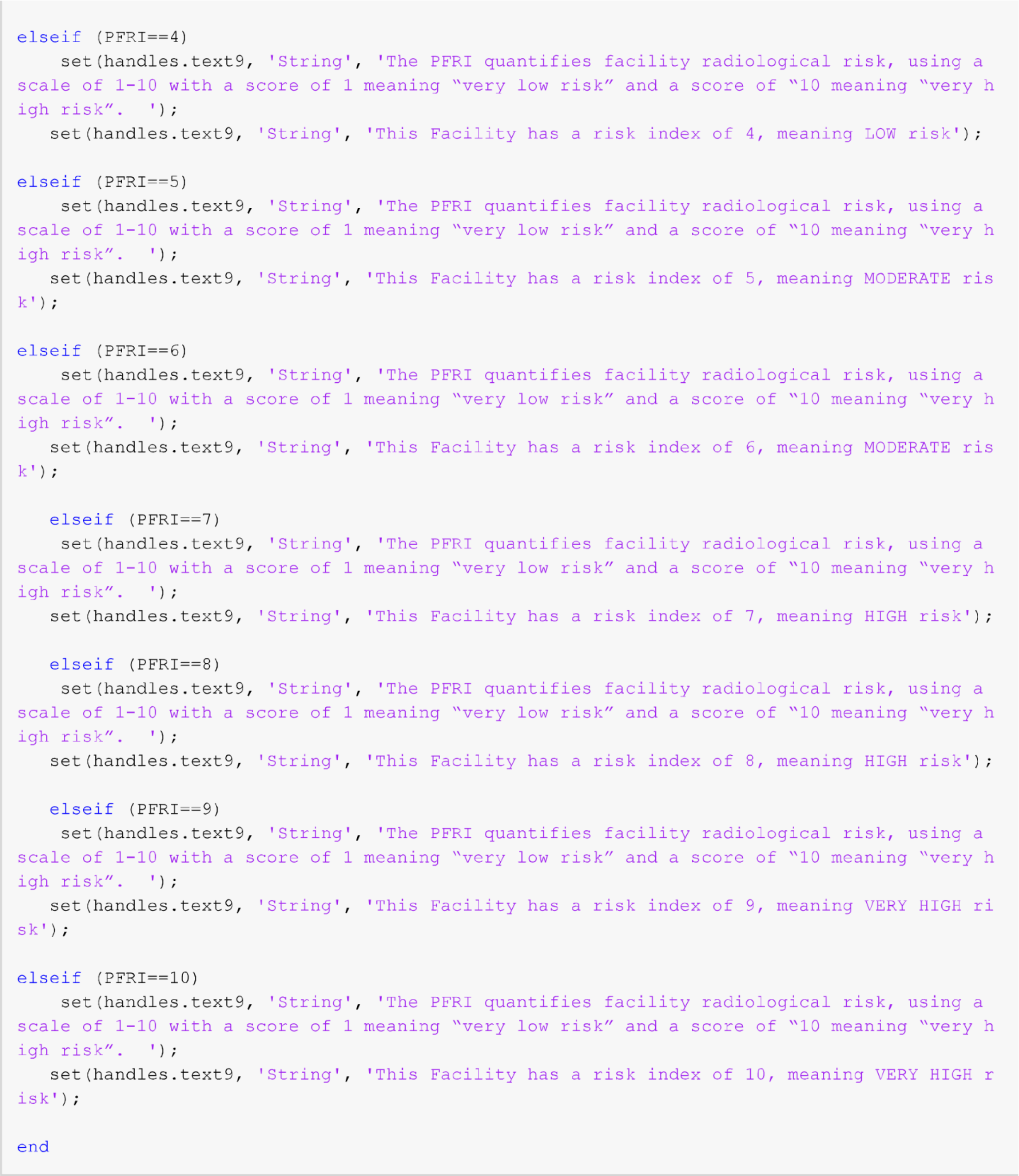
```
% hObject    handle to PFRI_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
```



```
%------------------------ Threat component--------------------------

if(A.GKstatus ==3 & A.Brachystatus==4 & A.BIstatus ==2)
 EUGK2=A.EUGK2;
EUGK3=A.EUGK3;
EUGK1=A.EUGK1;

MaxGK=max(max(A.EUGK2,A.EUGK3),A.EUGK1);
display(MaxGK);

EUBrachy2=A.EUBrachy2;
    EUBrachy3=A.EUBrachy3;
    EUBrachy1=A.EUBrachy1;
    MaxBrachy=max(max(A.EUBrachy2,A.EUBrachy3),A.EUBrachy1);
display(MaxBrachy);

 EUBI2=A.EUBI2;
EUBI3=A.EUBI3;
EUBI1=A.EUBI1;

MaxBI=max(max(A.EUBI2,A.EUBI3),A.EUBI1);
display(MaxBI);



elseif (A.GKstatus == 3 & A.BIstatus ==2)
EUGK2=A.EUGK2;
EUGK3=A.EUGK3;
EUGK1=A.EUGK1;

MaxGK=max(max(A.EUGK2,A.EUGK3),A.EUGK1);
display(MaxGK);

EUBI2=A.EUBI2;
EUBI3=A.EUBI3;
EUBI1=A.EUBI1;

MaxBI=max(max(A.EUBI2,A.EUBI3),A.EUBI1);
MaxBrachy=0
display(MaxBI);

elseif (A.GKstatus == 3 & A.Brachystatus ==4)
EUGK2=A.EUGK2;
EUGK3=A.EUGK3;
EUGK1=A.EUGK1;

MaxGK=max(max(A.EUGK2,A.EUGK3),A.EUGK1);
display(MaxGK);

EUBrachy2=A.EUBrachy2;
    EUBrachy3=A.EUBrachy3;
    EUBrachy1=A.EUBrachy1;
    MaxBrachy=max(max(A.EUBrachy2,A.EUBrachy3),A.EUBrachy1);
display(MaxBrachy);
MaxBI=0;
```

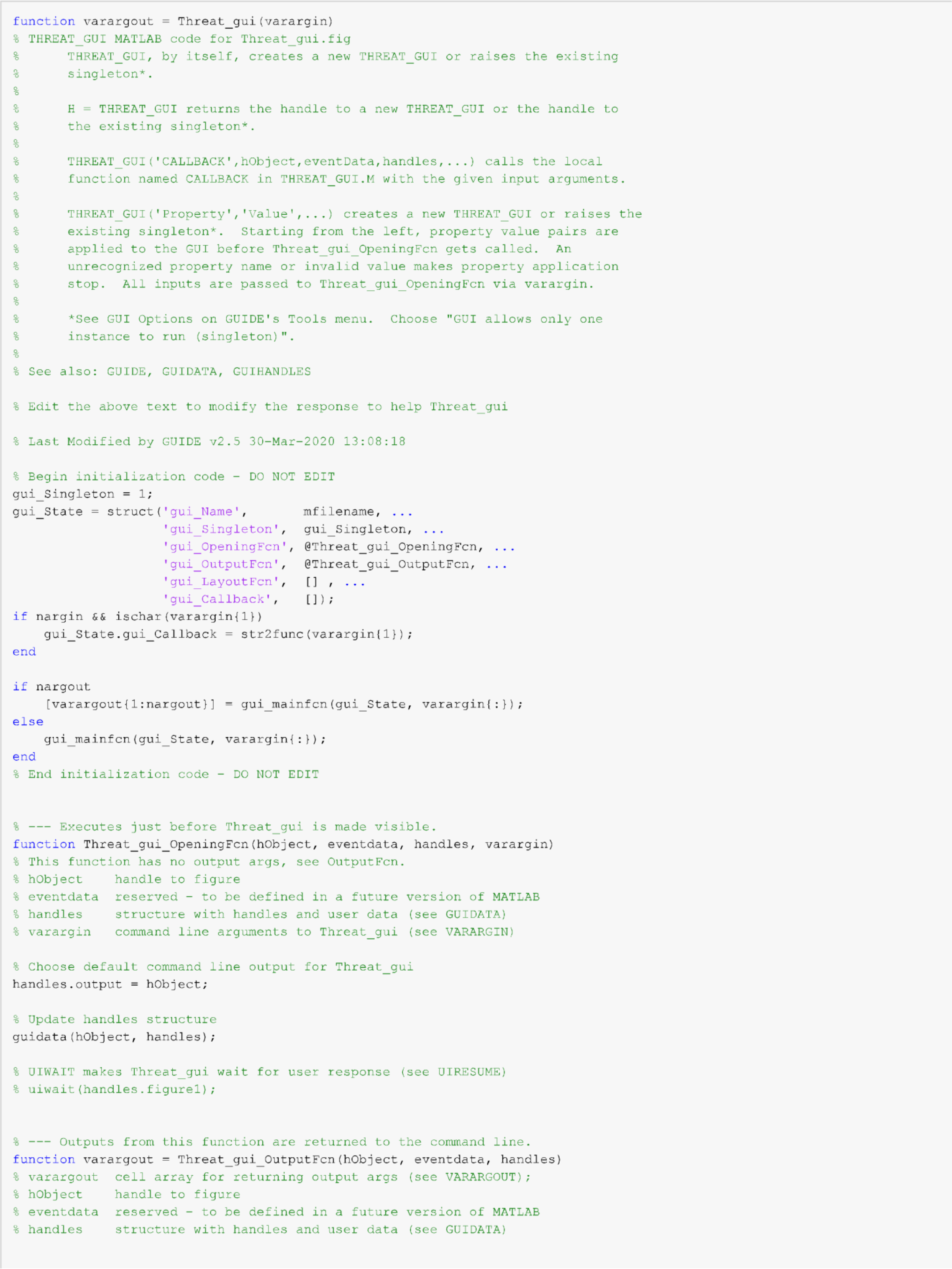
```
elseif (A.BIstatus == 2 & A.Brachystatus ==4)
EUBI2=A.EUBI2;
EUBI3=A.EUBI3;
EUBI1=A.EUBI1;

MaxBI=max(max(A.EUBI2,A.EUBI3),A.EUBI1);
display(MaxBI);

 EUBrachy2=A.EUBrachy2;
    EUBrachy3=A.EUBrachy3;
    EUBrachy1=A.EUBrachy1;
    MaxBrachy=max(max(A.EUBrachy2,A.EUBrachy3),A.EUBrachy1);
display(MaxBrachy);
MaxGK =0


elseif (A.GKstatus == 3 & A.BIstatus ==0 & A.Brachystatus==0)
EUGK2=A.EUGK2;
EUGK3=A.EUGK3;
EUGK1=A.EUGK1;

MaxGK=max(max(A.EUGK2,A.EUGK3),A.EUGK1);
MaxBI=0;
MaxBrachy=0;
display(MaxGK);



elseif (A.GKstatus == 0 & A.BIstatus ==2 & A.Brachystatus==0)


EUBI2=A.EUBI2;
EUBI3=A.EUBI3;
EUBI1=A.EUBI1;

MaxBI=max(max(A.EUBI2,A.EUBI3),A.EUBI1);
MaxBrachy=0;
MaxGK=0;
display(MaxBI);

elseif (A.GKstatus == 0 & A.BIstatus ==0 & A.Brachystatus==4)
    EUBrachy2=A.EUBrachy2;
    EUBrachy3=A.EUBrachy3;
    EUBrachy1=A.EUBrachy1;
    MaxBrachy=max(max(A.EUBrachy2,A.EUBrachy3),A.EUBrachy1);
display(MaxBrachy);
MaxBI=0;
MaxGK =0;

else
    msgbox('Something went wrong')

end


%--------------VULNERABILITY-------------
```

```
LocationalVul=A.Vulnerability;
CulturalVul=1-A.CultureVul;

%------------------CONSEQUENCES----------

Netconsequences=(A.CEL+A.CLL)/2;
display(Netconsequences)
%---------------------------------PFRI------------------

T=max(max(MaxGK,MaxBrachy),MaxBI);
%T=MaxBI;
display(T)
display(LocationalVul)
display(CulturalVul);
ProductPFRI=(T*(LocationalVul+CulturalVul)*Netconsequences);

PFRI=round(exp(ProductPFRI),0);
display(PFRI);
set(handles.PFRI_Static,'String',PFRI);



ThreatPFRI=xlsread('PFRI.xls','Sheet1', 'A1:A21');
GeogPFRI=xlsread('PFRI.xls','Sheet1', 'B1:B21');
CulPFRI=xlsread('PFRI.xls','Sheet1', 'C1:C21');
SumVPFRI=GeogPFRI(:)+CulPFRI(:);
ConseqPFRI=xlsread('PFRI.xls','Sheet1','D1:D21');
PFRItot=xlsread('PFRI.xls','Sheet3', 'A1:B11');
P=readtable('PFRI.xls', 'Sheet','Sheet4','Range', 'A1:E21', 'PreserveVariableNames', true)
;
H=xlsread('PFRI.xls', 'Sheet4', 'A1:E21');

x=H(:,1);
y1=H(:,2)
y2=H(:,4)

set(handles.text10, 'String', 'The PFRI quantifies facility radiological risk, using a sca
le of 1-10 with a score of 1 meaning "very low risk" and a score of "10 meaning "very high
 risk".  ');

if PFRI == 1

   set(handles.text9, 'String', '     This Facility has a risk index of 1, meaning VERY LO
W risk    ');
elseif (PFRI==2)
    set(handles.text9, 'String', 'The PFRI quantifies facility radiological risk, using a
scale of 1-10 with a score of 1 meaning "very low risk" and a score of "10 meaning "very h
igh risk".  ');
   set(handles.text9, 'String', 'This Facility has a risk index of 2, meaning VERY LOW ris
k');

elseif (PFRI==3)
    set(handles.text9, 'String', 'The PFRI quantifies facility radiological risk, using a
scale of 1-10 with a score of 1 meaning "very low risk" and a score of "10 meaning "very h
igh risk".  ');
   set(handles.text9, 'String', 'This Facility has a risk index of 3, meaning LOW risk');
```

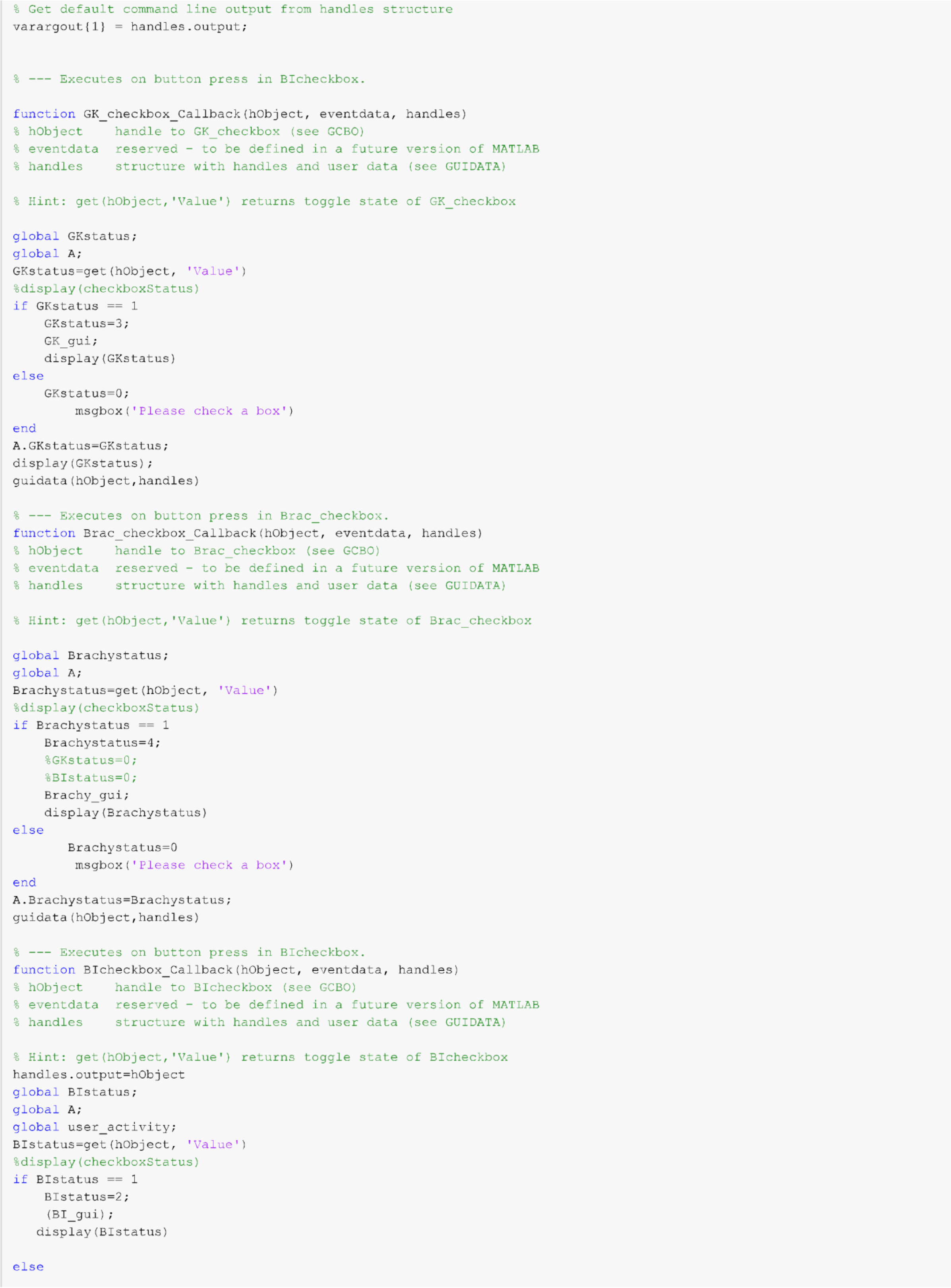


```
elseif (PFRI==4)
    set(handles.text9, 'String', 'The PFRI quantifies facility radiological risk, using a
scale of 1-10 with a score of 1 meaning “very low risk” and a score of “10 meaning “very h
igh risk”.  ');
   set(handles.text9, 'String', 'This Facility has a risk index of 4, meaning LOW risk');

elseif (PFRI==5)
    set(handles.text9, 'String', 'The PFRI quantifies facility radiological risk, using a
scale of 1-10 with a score of 1 meaning “very low risk” and a score of “10 meaning “very h
igh risk”.  ');
   set(handles.text9, 'String', 'This Facility has a risk index of 5, meaning MODERATE ris
k');

elseif (PFRI==6)
    set(handles.text9, 'String', 'The PFRI quantifies facility radiological risk, using a
scale of 1-10 with a score of 1 meaning “very low risk” and a score of “10 meaning “very h
igh risk”.  ');
   set(handles.text9, 'String', 'This Facility has a risk index of 6, meaning MODERATE ris
k');

   elseif (PFRI==7)
    set(handles.text9, 'String', 'The PFRI quantifies facility radiological risk, using a
scale of 1-10 with a score of 1 meaning “very low risk” and a score of “10 meaning “very h
igh risk”.  ');
   set(handles.text9, 'String', 'This Facility has a risk index of 7, meaning HIGH risk');

   elseif (PFRI==8)
    set(handles.text9, 'String', 'The PFRI quantifies facility radiological risk, using a
scale of 1-10 with a score of 1 meaning “very low risk” and a score of “10 meaning “very h
igh risk”.  ');
   set(handles.text9, 'String', 'This Facility has a risk index of 8, meaning HIGH risk');

   elseif (PFRI==9)
    set(handles.text9, 'String', 'The PFRI quantifies facility radiological risk, using a
scale of 1-10 with a score of 1 meaning “very low risk” and a score of “10 meaning “very h
igh risk”.  ');
   set(handles.text9, 'String', 'This Facility has a risk index of 9, meaning VERY HIGH ri
sk');

elseif (PFRI==10)
    set(handles.text9, 'String', 'The PFRI quantifies facility radiological risk, using a
scale of 1-10 with a score of 1 meaning “very low risk” and a score of “10 meaning “very h
igh risk”.  ');
   set(handles.text9, 'String', 'This Facility has a risk index of 10, meaning VERY HIGH r
isk');

end
```

THREAT GUI



```
function varargout = Threat_gui(varargin)
% THREAT_GUI MATLAB code for Threat_gui.fig
%      THREAT_GUI, by itself, creates a new THREAT_GUI or raises the existing
%      singleton*.
%
%      H = THREAT_GUI returns the handle to a new THREAT_GUI or the handle to
%      the existing singleton*.
%
%      THREAT_GUI('CALLBACK',hObject,eventData,handles,...) calls the local
%      function named CALLBACK in THREAT_GUI.M with the given input arguments.
%
%      THREAT_GUI('Property','Value',...) creates a new THREAT_GUI or raises the
%      existing singleton*.  Starting from the left, property value pairs are
%      applied to the GUI before Threat_gui_OpeningFcn gets called.  An
%      unrecognized property name or invalid value makes property application
%      stop.  All inputs are passed to Threat_gui_OpeningFcn via varargin.
%
%      *See GUI Options on GUIDE's Tools menu.  Choose "GUI allows only one
%      instance to run (singleton)".
%
% See also: GUIDE, GUIDATA, GUIHANDLES

% Edit the above text to modify the response to help Threat_gui

% Last Modified by GUIDE v2.5 30-Mar-2020 13:08:18

% Begin initialization code - DO NOT EDIT
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @Threat_gui_OpeningFcn, ...
                   'gui_OutputFcn',  @Threat_gui_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end
% End initialization code - DO NOT EDIT


% --- Executes just before Threat_gui is made visible.
function Threat_gui_OpeningFcn(hObject, eventdata, handles, varargin)
% This function has no output args, see OutputFcn.
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% varargin   command line arguments to Threat_gui (see VARARGIN)

% Choose default command line output for Threat_gui
handles.output = hObject;

% Update handles structure
guidata(hObject, handles);

% UIWAIT makes Threat_gui wait for user response (see UIRESUME)
% uiwait(handles.figure1);


% --- Outputs from this function are returned to the command line.
function varargout = Threat_gui_OutputFcn(hObject, eventdata, handles)
% varargout  cell array for returning output args (see VARARGOUT);
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
```



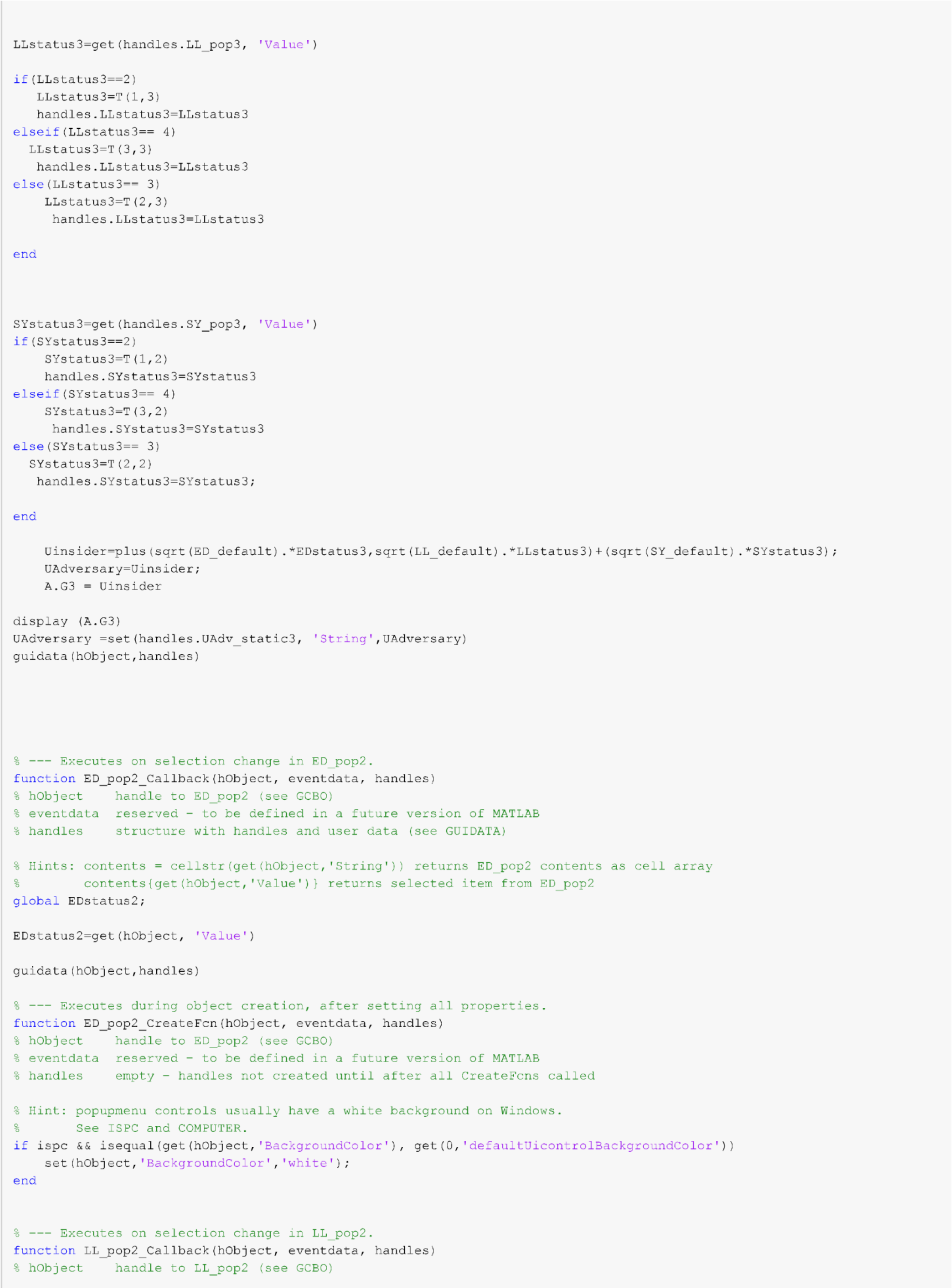
```
% Get default command line output from handles structure
varargout{1} = handles.output;


% --- Executes on button press in BIcheckbox.

function GK_checkbox_Callback(hObject, eventdata, handles)
% hObject    handle to GK_checkbox (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hint: get(hObject,'Value') returns toggle state of GK_checkbox

global GKstatus;
global A;
GKstatus=get(hObject, 'Value')
%display(checkboxStatus)
if GKstatus == 1
    GKstatus=3;
    GK_gui;
    display(GKstatus)
else
    GKstatus=0;
        msgbox('Please check a box')
end
A.GKstatus=GKstatus;
display(GKstatus);
guidata(hObject,handles)

% --- Executes on button press in Brac_checkbox.
function Brac_checkbox_Callback(hObject, eventdata, handles)
% hObject    handle to Brac_checkbox (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hint: get(hObject,'Value') returns toggle state of Brac_checkbox

global Brachystatus;
global A;
Brachystatus=get(hObject, 'Value')
%display(checkboxStatus)
if Brachystatus == 1
    Brachystatus=4;
    %GKstatus=0;
    %BIstatus=0;
    Brachy_gui;
    display(Brachystatus)
else
       Brachystatus=0
        msgbox('Please check a box')
end
A.Brachystatus=Brachystatus;
guidata(hObject,handles)

% --- Executes on button press in BIcheckbox.
function BIcheckbox_Callback(hObject, eventdata, handles)
% hObject    handle to BIcheckbox (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hint: get(hObject,'Value') returns toggle state of BIcheckbox
handles.output=hObject
global BIstatus;
global A;
global user_activity;
BIstatus=get(hObject, 'Value')
%display(checkboxStatus)
if BIstatus == 1
    BIstatus=2;
    (BI_gui);
   display(BIstatus)

else
```

```
    BIstatus=0
        msgbox('Please check a box')
end
A.BIstatus=BIstatus;
guidata(hObject,handles)






% --- Executes on selection change in ED_pop.
function ED_pop_Callback(hObject, eventdata, handles)
% hObject    handle to ED_pop (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: contents = cellstr(get(hObject,'String')) returns ED_pop contents as cell array
%        contents{get(hObject,'Value')} returns selected item from ED_pop


global EDstatus;

EDstatus=get(hObject, 'Value')

guidata(hObject,handles)
% --- Executes during object creation, after setting all properties.
function ED_pop_CreateFcn(hObject, eventdata, handles)
% hObject    handle to ED_pop (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: popupmenu controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end


% --- Executes on selection change in LL_pop.
function LL_pop_Callback(hObject, eventdata, handles)
% hObject    handle to LL_pop (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: contents = cellstr(get(hObject,'String')) returns LL_pop contents as cell array
%        contents{get(hObject,'Value')} returns selected item from LL_pop
global LLstatus
LLstatus=get(hObject, 'Value')


guidata(hObject,handles)

% --- Executes during object creation, after setting all properties.
function LL_pop_CreateFcn(hObject, eventdata, handles)
% hObject    handle to LL_pop (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: popupmenu controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end


% --- Executes on selection change in SY_pop.
function SY_pop_Callback(hObject, eventdata, handles)
% hObject    handle to SY_pop (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% Hints: contents = cellstr(get(hObject,'String')) returns SY_pop contents as cell array
%        contents{get(hObject,'Value')} returns selected item from SY_pop
global SYstatus
SYstatus=get(hObject, 'Value')

guidata(hObject,handles)

% --- Executes during object creation, after setting all properties.
function SY_pop_CreateFcn(hObject, eventdata, handles)
% hObject    handle to SY_pop (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: popupmenu controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end


% --- Executes on button press in Adv_push.
function Adv_push_Callback(hObject, eventdata, handles)
% hObject    handle to Adv_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global TGstatus;
filename='U_Adv_forCode.xls'
global EDstatus;
global LLstatus;
global SYstatus;
global Uoutsider
global Usemiinsider
global Uinsider
global T
global A
global ED_default
global SY_default
global LL_default

global UAdversary;
T=xlsread(filename)

ED_default=T(1,5)
LL_default=T(1,6)
SY_default=T(1,7)
%TGstatus=get(handles.TG_popgroup, 'Value')

global ED_high
global ED_med
global ED_low
global SY_high
global SY_med
global SY_low
global LL_high
global LL_med
global LL_low
global ED_default
global SY_default
global LL_default
global EDstatus;
T=xlsread(filename)
ED_high=T(1,1)
ED_med=T(2,1)
ED_low=T(3,1)
SY_high=T(1,2)
SY_med=T(2,2)
SY_low=T(3,2)
LL_high=T(1,3)
LL_med=T(2,3)
LL_low=T(3,3)
ED_default=T(1,5)
LL_default=T(1,6)
```

```
SY_default=T(1,7)

EDstatus=get(handles.ED_pop, 'Value')
switch EDstatus
    case 2
    EDstatus=T(1,1);
   % handles.EDstatus=EDstatus

    case 3
    EDstatus=T(2,1);
   %handles.EDstatus=EDstatus

    otherwise
    EDstatus=T(3,1);
    %handles.EDstatus=EDstatus
end

handles.EDstatus=EDstatus
guidata(hObject, handles)
display (EDstatus)


LLstatus=get(handles.LL_pop, 'Value')

if(LLstatus==2)
   LLstatus=T(1,3)
   handles.LLstatus=LLstatus
elseif(LLstatus== 4)
  LLstatus=T(3,3)
   handles.LLstatus=LLstatus
else(LLstatus== 3)
    LLstatus=T(2,3)
     handles.LLstatus=LLstatus

end



SYstatus=get(handles.SY_pop, 'Value')
if(SYstatus==2)
    SYstatus=T(1,2)
    handles.SYstatus=SYstatus
elseif(SYstatus== 4)
    SYstatus=T(3,2)
     handles.SYstatus=SYstatus
else(SYstatus== 3)
  SYstatus=T(2,2)
   handles.SYstatus=SYstatus;

end

    Uoutsider=plus(sqrt(ED_default).*EDstatus,sqrt(LL_default).*LLstatus)+(sqrt(SY_default).*SYstatus);
    UAdversary=Uoutsider
    A.G1=Uoutsider


display (A.G1)
UAdversary =set(handles.UAdv_static, 'String',UAdversary);
guidata(hObject,handles)


% --- Executes on selection change in TG_popgroup.



% --- Executes on selection change in ED_pop3.
function ED_pop3_Callback(hObject, eventdata, handles)
% hObject    handle to ED_pop3 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: contents = cellstr(get(hObject,'String')) returns ED_pop3 contents as cell array
%        contents{get(hObject,'Value')} returns selected item from ED_pop3
```

```
global EDstatus3;

EDstatus3=get(hObject, 'Value')

guidata(hObject,handles)

% --- Executes during object creation, after setting all properties.
function ED_pop3_CreateFcn(hObject, eventdata, handles)
% hObject    handle to ED_pop3 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: popupmenu controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end


% --- Executes on selection change in LL_pop3.
function LL_pop3_Callback(hObject, eventdata, handles)
% hObject    handle to LL_pop3 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: contents = cellstr(get(hObject,'String')) returns LL_pop3 contents as cell array
%        contents{get(hObject,'Value')} returns selected item from LL_pop3

global LLstatus3;

LLstatus3=get(hObject, 'Value')

guidata(hObject,handles)

% --- Executes during object creation, after setting all properties.
function LL_pop3_CreateFcn(hObject, eventdata, handles)
% hObject    handle to LL_pop3 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: popupmenu controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end


% --- Executes on selection change in SY_pop3.
function SY_pop3_Callback(hObject, eventdata, handles)
% hObject    handle to SY_pop3 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: contents = cellstr(get(hObject,'String')) returns SY_pop3 contents as cell array
%        contents{get(hObject,'Value')} returns selected item from SY_pop3

global SYstatus3
SYstatus3=get(hObject, 'Value')

guidata(hObject,handles)
% --- Executes during object creation, after setting all properties.
function SY_pop3_CreateFcn(hObject, eventdata, handles)
% hObject    handle to SY_pop3 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: popupmenu controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end
```

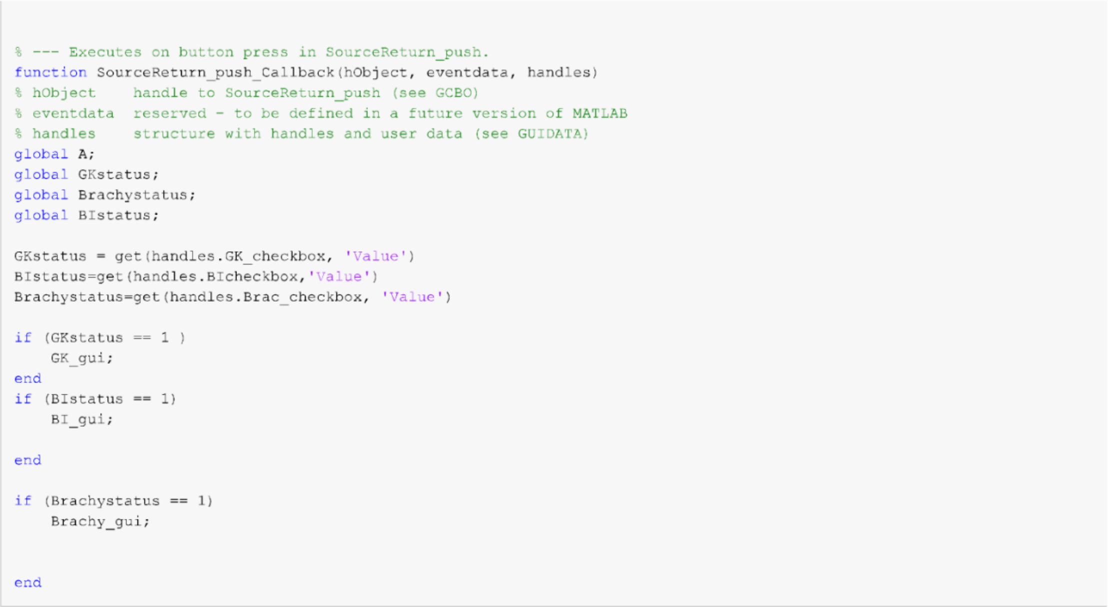
```
% --- Executes on button press in Adv_push3.
function Adv_push3_Callback(hObject, eventdata, handles)
% hObject    handle to Adv_push3 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global TGstatus;
filename='U_Adv_forCode.xls'
global EDstatus3;
global LLstatus3;
global SYstatus3;
global Uoutsider
global Usemiinsider
global Uinsider
global T
global ED_default
global SY_default
global LL_default

global UAdversary;
T=xlsread(filename)

ED_default=T(1,5)
LL_default=T(1,6)
SY_default=T(1,7)
%TGstatus=get(handles.TG_popgroup, 'Value')

global ED_high
global ED_med
global ED_low
global SY_high
global SY_med
global SY_low
global LL_high
global LL_med
global LL_low
global ED_default
global SY_default
global LL_default
global EDstatus3;
global A;
T=xlsread(filename)
ED_high=T(1,1)
ED_med=T(2,1)
ED_low=T(3,1)
SY_high=T(1,2)
SY_med=T(2,2)
SY_low=T(3,2)
LL_high=T(1,3)
LL_med=T(2,3)
LL_low=T(3,3)
ED_default=T(1,5)
LL_default=T(1,6)
SY_default=T(1,7)

EDstatus3=get(handles.ED_pop3, 'Value')
switch EDstatus3
    case 2
    EDstatus3=T(1,1);
   % handles.EDstatus=EDstatus

    case 3
    EDstatus3=T(2,1);
   %handles.EDstatus=EDstatus

    otherwise
    EDstatus3=T(3,1);
    %handles.EDstatus=EDstatus
end

handles.EDstatus3=EDstatus3
guidata(hObject, handles)
display (EDstatus3)
```



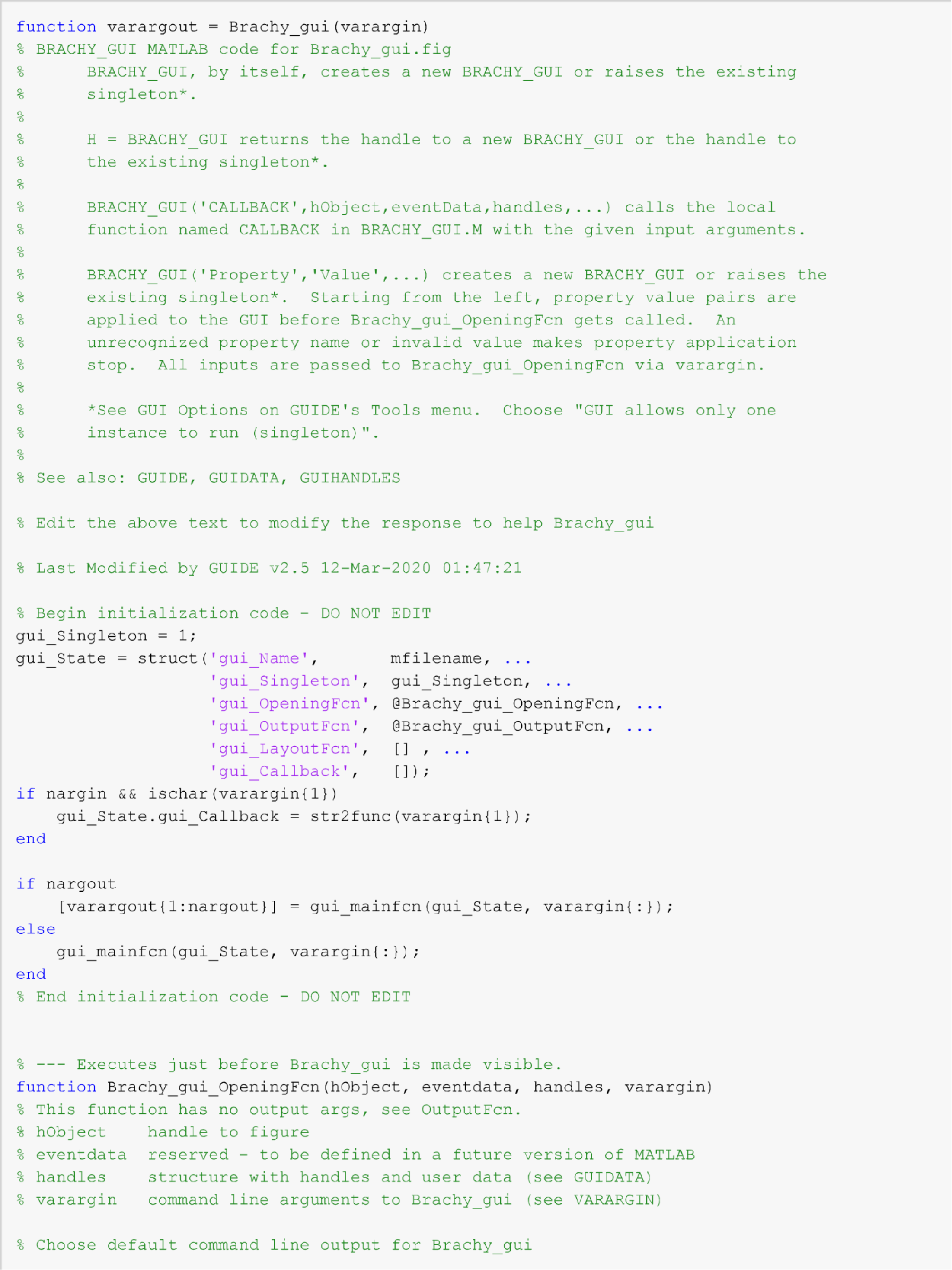
```
LLstatus3=get(handles.LL_pop3, 'Value')

if(LLstatus3==2)
   LLstatus3=T(1,3)
   handles.LLstatus3=LLstatus3
elseif(LLstatus3== 4)
  LLstatus3=T(3,3)
   handles.LLstatus3=LLstatus3
else(LLstatus3== 3)
    LLstatus3=T(2,3)
     handles.LLstatus3=LLstatus3

end



SYstatus3=get(handles.SY_pop3, 'Value')
if(SYstatus3==2)
    SYstatus3=T(1,2)
    handles.SYstatus3=SYstatus3
elseif(SYstatus3== 4)
    SYstatus3=T(3,2)
     handles.SYstatus3=SYstatus3
else(SYstatus3== 3)
  SYstatus3=T(2,2)
   handles.SYstatus3=SYstatus3;

end

    Uinsider=plus(sqrt(ED_default).*EDstatus3,sqrt(LL_default).*LLstatus3)+(sqrt(SY_default).*SYstatus3);
    UAdversary=Uinsider;
    A.G3 = Uinsider

display (A.G3)
UAdversary =set(handles.UAdv_static3, 'String',UAdversary)
guidata(hObject,handles)





% --- Executes on selection change in ED_pop2.
function ED_pop2_Callback(hObject, eventdata, handles)
% hObject    handle to ED_pop2 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: contents = cellstr(get(hObject,'String')) returns ED_pop2 contents as cell array
%        contents{get(hObject,'Value')} returns selected item from ED_pop2
global EDstatus2;

EDstatus2=get(hObject, 'Value')

guidata(hObject,handles)

% --- Executes during object creation, after setting all properties.
function ED_pop2_CreateFcn(hObject, eventdata, handles)
% hObject    handle to ED_pop2 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: popupmenu controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end


% --- Executes on selection change in LL_pop2.
function LL_pop2_Callback(hObject, eventdata, handles)
% hObject    handle to LL_pop2 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: contents = cellstr(get(hObject,'String')) returns LL_pop2 contents as cell array
%        contents{get(hObject,'Value')} returns selected item from LL_pop2
global LLstatus2;

LLstatus2=get(hObject, 'Value')

guidata(hObject,handles)

% --- Executes during object creation, after setting all properties.
function LL_pop2_CreateFcn(hObject, eventdata, handles)
% hObject    handle to LL_pop2 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: popupmenu controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end


% --- Executes on selection change in SY_pop2.
function SY_pop2_Callback(hObject, eventdata, handles)
% hObject    handle to SY_pop2 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: contents = cellstr(get(hObject,'String')) returns SY_pop2 contents as cell array
%        contents{get(hObject,'Value')} returns selected item from SY_pop2
global SYstatus2
SYstatus2=get(hObject, 'Value')

guidata(hObject,handles)


% --- Executes during object creation, after setting all properties.
function SY_pop2_CreateFcn(hObject, eventdata, handles)
% hObject    handle to SY_pop2 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: popupmenu controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end


% --- Executes on button press in Adv_push2.
function Adv_push2_Callback(hObject, eventdata, handles)
% hObject    handle to Adv_push2 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global TGstatus;
filename='U_Adv_forCode.xls'
global EDstatus2;
global LLstatus2;
global SYstatus2;
global Uoutsider
global Usemiinsider
global Uinsider
global T
global ED_default
global SY_default
global LL_default

global UAdversary2;
T=xlsread(filename)

ED_default=T(1,5)
```

```
LL_default=T(1,6)
SY_default=T(1,7)
%TGstatus=get(handles.TG_popgroup, 'Value')

global ED_high
global ED_med
global ED_low
global SY_high
global SY_med
global SY_low
global LL_high
global LL_med
global LL_low
global ED_default
global SY_default
global LL_default
global EDstatus;
global A;
T=xlsread(filename)
ED_high=T(1,1)
ED_med=T(2,1)
ED_low=T(3,1)
SY_high=T(1,2)
SY_med=T(2,2)
SY_low=T(3,2)
LL_high=T(1,3)
LL_med=T(2,3)
LL_low=T(3,3)
ED_default=T(1,5)
LL_default=T(1,6)
SY_default=T(1,7)

EDstatus2=get(handles.ED_pop2, 'Value')
switch EDstatus2
    case 2
    EDstatus2=T(1,1);
   % handles.EDstatus=EDstatus

    case 3
    EDstatus2=T(2,1);
   %handles.EDstatus=EDstatus

    otherwise
    EDstatus2=T(3,1);
    %handles.EDstatus=EDstatus
end

handles.EDstatus2=EDstatus2
guidata(hObject, handles)
display (EDstatus2)


LLstatus2=get(handles.LL_pop2, 'Value')

if(LLstatus2==2)
   LLstatus2=T(1,3)
   handles.LLstatus2=LLstatus2
elseif(LLstatus2== 4)
  LLstatus2=T(3,3)
   handles.LLstatus2=LLstatus2
else(LLstatus2== 3)
    LLstatus2=T(2,3)
     handles.LLstatus2=LLstatus2

end



SYstatus2=get(handles.SY_pop2, 'Value')
if(SYstatus2==2)
    SYstatus2=T(1,2)
    handles.SYstatus2=SYstatus2
elseif(SYstatus2== 4)
```

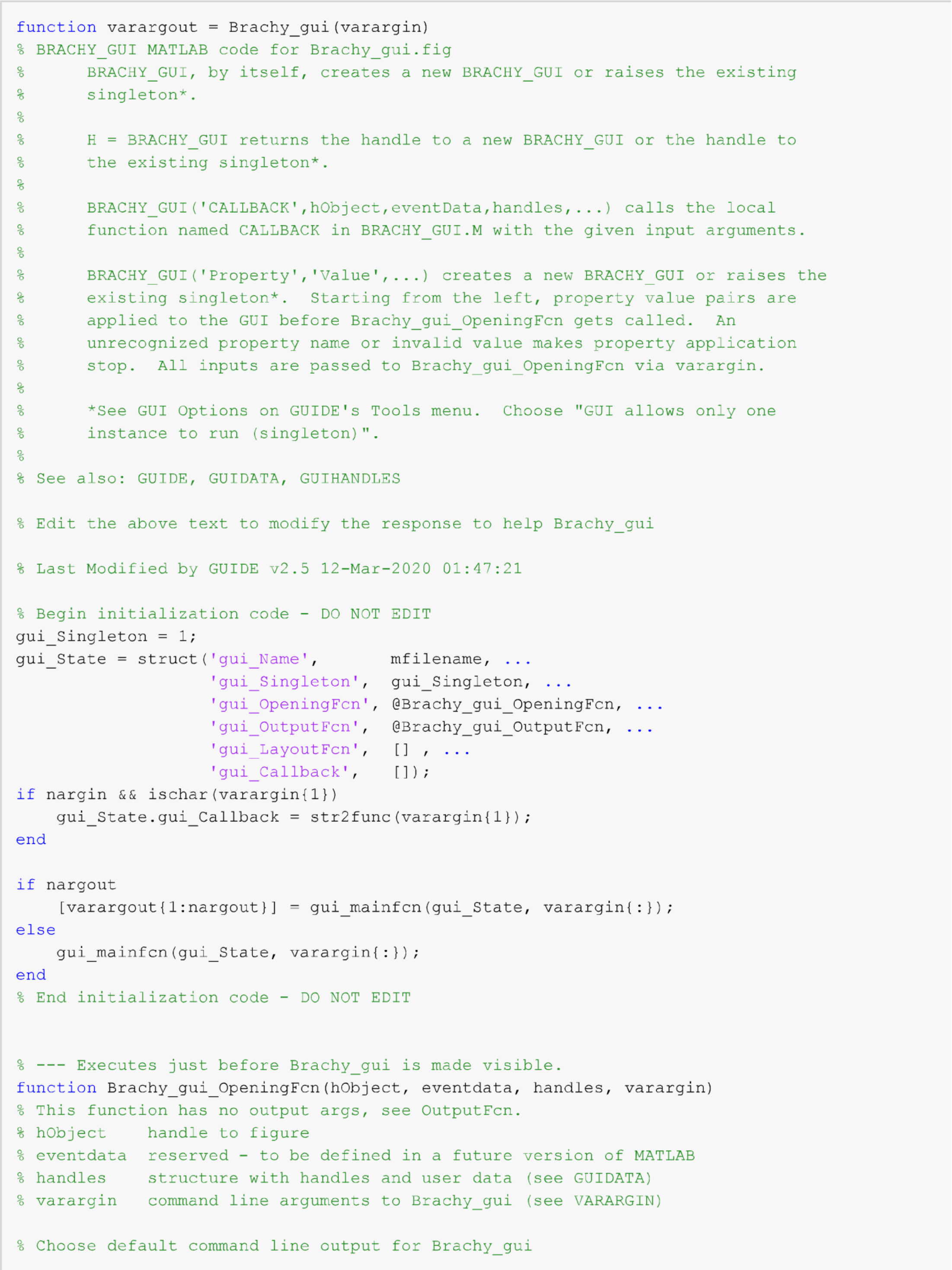
```
    SYstatus2=T(3,2)
     handles.SYstatus2=SYstatus2
else(SYstatus2== 3)
  SYstatus2=T(2,2)
   handles.SYstatus2=SYstatus2;

end

     Usemiinsider=plus(sqrt(ED_default).*EDstatus2,sqrt(LL_default).*LLstatus2)+(sqrt(SY_default).*SYstatus2);
     UAdversary=Usemiinsider;
     A.G2=Usemiinsider



display (A.G2)
UAdversary =set(handles.UAdv_static2, 'String',UAdversary)
guidata(hObject,handles)


% --- Executes on button press in Atmospherehazard_push.


% --- Executes on button press in Threat_PFRI_return_push.
function Threat_PFRI_return_push_Callback(hObject, eventdata, handles)
% hObject    handle to Threat_PFRI_return_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
global GKstatus;
global Brachystatus;
global BIstatus;

GKstatus = get(handles.GK_checkbox, 'Value')
BIstatus=get(handles.BIcheckbox,'Value')
Brachystatus=get(handles.Brac_checkbox, 'Value')

if(GKstatus == 1 & BIstatus == 1)
    A.GKstatus=3;
    A.BIstatus=2;
    A.Brachystatus=0;
elseif (GKstatus == 1 & Brachystatus ==1)
    A.GKstatus=3;
    A.BIstatus=0;
    A.Brachystatus=4;
elseif (BIstatus ==1 & Brachystatus==1)
    A.BIstatus=2;
    A.Brachystatus=4;
    A.GKstatus=0;
elseif (GKstatus==1 & Brachystatus ==1 & BIstatus ==1)
    A.BIstatus=2;
    A.Brachystatus=4;
    A.GKstatus=3;

elseif (GKstatus == 1 & BIstatus == 0 &Brachystatus==0)
    A.GKstatus=3;
    A.BIstatus=0;
    A.Brachystatus=0;
elseif (GKstatus == 0 & BIstatus == 1 &Brachystatus==0)
    A.BIstatus=2;
    A.GKstatus=0
    A.Brachystatus=0
elseif (GKstatus == 0 & BIstatus == 0 &Brachystatus==1)
    A.Brachystatus=4;
    A.GKstatus=0;
    A.BIstatus=0;
else
    msgbox('WTF')

end



My_PFRI_1;
```



```
% --- Executes on button press in SourceReturn_push.
function SourceReturn_push_Callback(hObject, eventdata, handles)
% hObject    handle to SourceReturn_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
global GKstatus;
global Brachystatus;
global BIstatus;

GKstatus = get(handles.GK_checkbox, 'Value')
BIstatus=get(handles.BIcheckbox,'Value')
Brachystatus=get(handles.Brac_checkbox, 'Value')

if (GKstatus == 1 )
    GK_gui;
end
if (BIstatus == 1)
    BI_gui;

end

if (Brachystatus == 1)
    Brachy_gui;


end
```



```
function varargout = Brachy_gui(varargin)
% BRACHY_GUI MATLAB code for Brachy_gui.fig
%      BRACHY_GUI, by itself, creates a new BRACHY_GUI or raises the existing
%      singleton*.
%
%      H = BRACHY_GUI returns the handle to a new BRACHY_GUI or the handle to
%      the existing singleton*.
%
%      BRACHY_GUI('CALLBACK',hObject,eventData,handles,...) calls the local
%      function named CALLBACK in BRACHY_GUI.M with the given input arguments.
%
%      BRACHY_GUI('Property','Value',...) creates a new BRACHY_GUI or raises the
%      existing singleton*.  Starting from the left, property value pairs are
%      applied to the GUI before Brachy_gui_OpeningFcn gets called.  An
%      unrecognized property name or invalid value makes property application
%      stop.  All inputs are passed to Brachy_gui_OpeningFcn via varargin.
%
%      *See GUI Options on GUIDE's Tools menu.  Choose "GUI allows only one
%      instance to run (singleton)".
%
% See also: GUIDE, GUIDATA, GUIHANDLES

% Edit the above text to modify the response to help Brachy_gui

% Last Modified by GUIDE v2.5 12-Mar-2020 01:47:21

% Begin initialization code - DO NOT EDIT
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @Brachy_gui_OpeningFcn, ...
                   'gui_OutputFcn',  @Brachy_gui_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end
% End initialization code - DO NOT EDIT


% --- Executes just before Brachy_gui is made visible.
function Brachy_gui_OpeningFcn(hObject, eventdata, handles, varargin)
% This function has no output args, see OutputFcn.
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% varargin   command line arguments to Brachy_gui (see VARARGIN)

% Choose default command line output for Brachy_gui
```

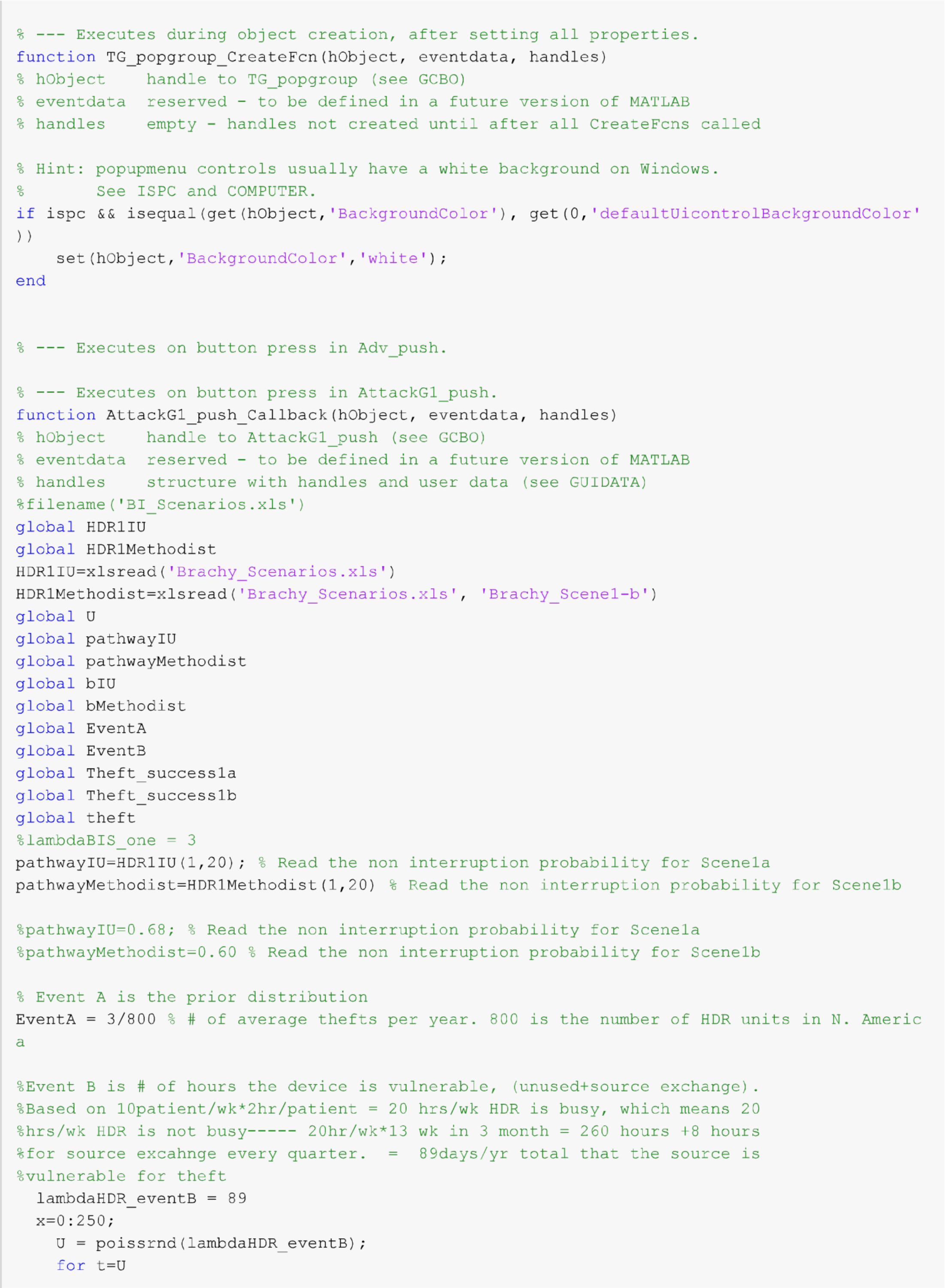


```
function varargout = Brachy_gui(varargin)
% BRACHY_GUI MATLAB code for Brachy_gui.fig
%      BRACHY_GUI, by itself, creates a new BRACHY_GUI or raises the existing
%      singleton*.
%
%      H = BRACHY_GUI returns the handle to a new BRACHY_GUI or the handle to
%      the existing singleton*.
%
%      BRACHY_GUI('CALLBACK',hObject,eventData,handles,...) calls the local
%      function named CALLBACK in BRACHY_GUI.M with the given input arguments.
%
%      BRACHY_GUI('Property','Value',...) creates a new BRACHY_GUI or raises the
%      existing singleton*.  Starting from the left, property value pairs are
%      applied to the GUI before Brachy_gui_OpeningFcn gets called.  An
%      unrecognized property name or invalid value makes property application
%      stop.  All inputs are passed to Brachy_gui_OpeningFcn via varargin.
%
%      *See GUI Options on GUIDE's Tools menu.  Choose "GUI allows only one
%      instance to run (singleton)".
%
% See also: GUIDE, GUIDATA, GUIHANDLES

% Edit the above text to modify the response to help Brachy_gui

% Last Modified by GUIDE v2.5 12-Mar-2020 01:47:21

% Begin initialization code - DO NOT EDIT
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @Brachy_gui_OpeningFcn, ...
                   'gui_OutputFcn',  @Brachy_gui_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end
% End initialization code - DO NOT EDIT


% --- Executes just before Brachy_gui is made visible.
function Brachy_gui_OpeningFcn(hObject, eventdata, handles, varargin)
% This function has no output args, see OutputFcn.
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% varargin   command line arguments to Brachy_gui (see VARARGIN)

% Choose default command line output for Brachy_gui
```

```
handles.output = hObject;

% Update handles structure
guidata(hObject, handles);
global user_activity;
% UIWAIT makes Brachy_gui wait for user response (see UIRESUME)
% uiwait(handles.figure1);


% --- Outputs from this function are returned to the command line.
function varargout = Brachy_gui_OutputFcn(hObject, eventdata, handles)
% varargout  cell array for returning output args (see VARARGOUT);
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Get default command line output from handles structure
varargout{1} = handles.output;



function Brachy_Activitytext_Callback(hObject, eventdata, handles)
% hObject    handle to Brachy_Activitytext (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: get(hObject,'String') returns contents of Brachy_Activitytext as text
%        str2double(get(hObject,'String')) returns contents of Brachy_Activitytext as a do
uble

handles.output=hObject
global user_activity;
global Dangervalue;
global Physicalform;
user_activity=str2double(get(hObject, 'String'));
if isempty(user_activity)
    errordlg('Please enter the activity of the source')
else
Dangervalue=str2double(set(handles.D_static, 'String','0.08'));
Physicalform=set(handles.form_static, 'String','Metallic');

end

guidata(hObject,handles)


% --- Executes during object creation, after setting all properties.
function Brachy_Activitytext_CreateFcn(hObject, eventdata, handles)
% hObject    handle to Brachy_Activitytext (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: edit controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'
))
    set(hObject,'BackgroundColor','white');
```

```
end


% --- If Enable == 'on', executes on mouse press in 5 pixel border.
% --- Otherwise, executes on mouse press in 5 pixel border or over Brachy_Activitytext.


% --- Executes on button press in Cat_pushbutton.
function Cat_pushbutton_Callback(hObject, eventdata, handles)
% hObject    handle to Cat_pushbutton (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
%THIS IS FOR IR-192
global ActivityDanger_ratio;
global user_activity;
global Dangervalue;
display (user_activity)
Dangervalue = str2double(get(handles.D_static, 'String'))
display (Dangervalue);
ActivityDanger_ratio=user_activity/Dangervalue;
display (ActivityDanger_ratio);
if(ActivityDanger_ratio >=1000)
    set(handles.Cat_static, 'String', 'CAT 1')
elseif(1<ActivityDanger_ratio<10)
    set(handles.Cat_static, 'String', 'CAT3')
else
    errordlg('Bad numbers, Enter the values between 0.037-0.55 TBq')
end
guidata(hObject,handles)


% --- Executes on button press in AssetBI_push.
function AssetBI_push_Callback(hObject, eventdata, handles)
% hObject    handle to AssetBI_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global Physicalform;
global formnumeric;
global U_form
global ActivityDanger_ratio;
global U_attractiveness;
global U_material;
Physicalform=(get(handles.form_static, 'String'));
if strcmp(Physicalform,'Powdered Salt')
    formnumeric=2
elseif strcmp(Physicalform, 'Metallic')
    formnumeric=1
else
    msgbox('Bad numbers, Sorry!')
end
U_form=1-exp(-formnumeric).^3
display (U_form);
U_attractiveness= 1-exp(-ActivityDanger_ratio/9.07).^3
display(U_attractiveness);
U_material=U_form.*U_attractiveness;
set(handles.Asset_static, 'String', U_material)
```

```
guidata(hObject,handles)


% --- Executes on selection change in TG_popgroup.
function TG_popgroup_Callback(hObject, eventdata, handles)
% hObject    handle to TG_popgroup (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: contents = cellstr(get(hObject,'String')) returns TG_popgroup contents as cell ar
ray
%        contents{get(hObject,'Value')} returns selected item from TG_popgroup
global TGstatus
global T;

global ED_high
global ED_med
global ED_low
global SY_high
global SY_med
global SY_low
global LL_high
global LL_med
global LL_low
global ED_default
global SY_default
global LL_default
filename='U_Adv_forCode.xls'
T=xlsread(filename)
ED_high=T(1,1)
ED_med=T(2,1)
ED_low=T(3,1)
SY_high=T(1,2)
SY_med=T(2,2)
SY_low=T(3,2)
LL_high=T(1,3)
LL_med=T(2,3)
LL_low=T(3,3)
ED_default=T(1,5)
LL_default=T(1,6)
SY_default=T(1,7)
TGstatus=get(hObject, 'Value')
%display(checkboxStatus)
if strcmp(TGstatus, 'Outsider(G1)')
    TGstatus=2;

  Fprintf(TGstatus)


elseif strcmp(TGstatus, 'Semiinsider(G2)')
    TGstatus=3;

elseif strcmp(TGstatus, 'Insider(G3)')
    TGstatus=4;

end
guidata(hObject,handles);
```



```
% --- Executes during object creation, after setting all properties.
function TG_popgroup_CreateFcn(hObject, eventdata, handles)
% hObject    handle to TG_popgroup (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: popupmenu controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'
))
    set(hObject,'BackgroundColor','white');
end


% --- Executes on button press in Adv_push.

% --- Executes on button press in AttackG1_push.
function AttackG1_push_Callback(hObject, eventdata, handles)
% hObject    handle to AttackG1_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
%filename('BI_Scenarios.xls')
global HDR1IU
global HDR1Methodist
HDR1IU=xlsread('Brachy_Scenarios.xls')
HDR1Methodist=xlsread('Brachy_Scenarios.xls', 'Brachy_Scene1-b')
global U
global pathwayIU
global pathwayMethodist
global bIU
global bMethodist
global EventA
global EventB
global Theft_success1a
global Theft_success1b
global theft
%lambdaBIS_one = 3
pathwayIU=HDR1IU(1,20); % Read the non interruption probability for Scene1a
pathwayMethodist=HDR1Methodist(1,20) % Read the non interruption probability for Scene1b

%pathwayIU=0.68; % Read the non interruption probability for Scene1a
%pathwayMethodist=0.60 % Read the non interruption probability for Scene1b

% Event A is the prior distribution
EventA = 3/800 % # of average thefts per year. 800 is the number of HDR units in N. Americ
a

%Event B is # of hours the device is vulnerable, (unused+source exchange).
%Based on 10patient/wk*2hr/patient = 20 hrs/wk HDR is busy, which means 20
%hrs/wk HDR is not busy----- 20hr/wk*13 wk in 3 month = 260 hours +8 hours
%for source excahnge every quarter.  =  89days/yr total that the source is
%vulnerable for theft
  lambdaHDR_eventB = 89
  x=0:250;
    U = poissrnd(lambdaHDR_eventB);
    for t=U
    y = poisspdf(x,t);
    end

    EventB = mean(y)

   % U = poissrnd(lambdaHDR_eventB);
    %  for t=U

          bIU=pathwayIU.*0.95

              nfailures=(pathwayIU.*randn(1000,1)+bIU)
              Theft_success1a = mean(nfailures)

               bMethodist=pathwayMethodist.*0.95

              nfailures=(pathwayIU.*randn(1000,1)+bMethodist)
              Theft_success1b = mean(nfailures)
   % y = binopdf(1,U,nf);
    %plot(nfailures,y,'+')

    %USing Bayes theorem
    global FinalIU_theft
    FinalIU_theft=Theft_success1a.*EventA/EventB
    global FinalMethodist_theft
    FinalMethodist_theft=Theft_success1b.*EventA/EventB

 global Totalprobability
 %Totalprobability = FinalIU_theft+FinalMethodist_theft/2
 Totalprobability = FinalMethodist_theft
     theft.GKS1=Totalprobability

  set(handles.sceneG1_static,'String', Totalprobability)


% --- Executes on button press in AttackG2_push.
function AttackG2_push_Callback(hObject, eventdata, handles)
% hObject    handle to AttackG2_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% --- Executes on button press in AttackG3_push.

%-----------------------------------------------------
% There are 800 HDR units in N. America. Each HDR goes through source
% exchang 4 times a year.
% 4*2=8 times source gets delivered (2 times source deliver each time)This
% is the number of times the source gets delivered for 1 HDR, but there are
% 800 HDR so total of 6400.
%According to NTI, there were 4 delivery failures in past 4 years, so 1
%every year. 1/6400 = 0.00015------P(A)
%Event B is the # of mail lost by mail carrier (Fedex/UPS)
%-----------------------------------------------------------
global EventA_Scene2
global EventB_Scene2

EventA_Scene2=1/6400 % If there were 1 delivery error each year in the past four years P(A
)
```

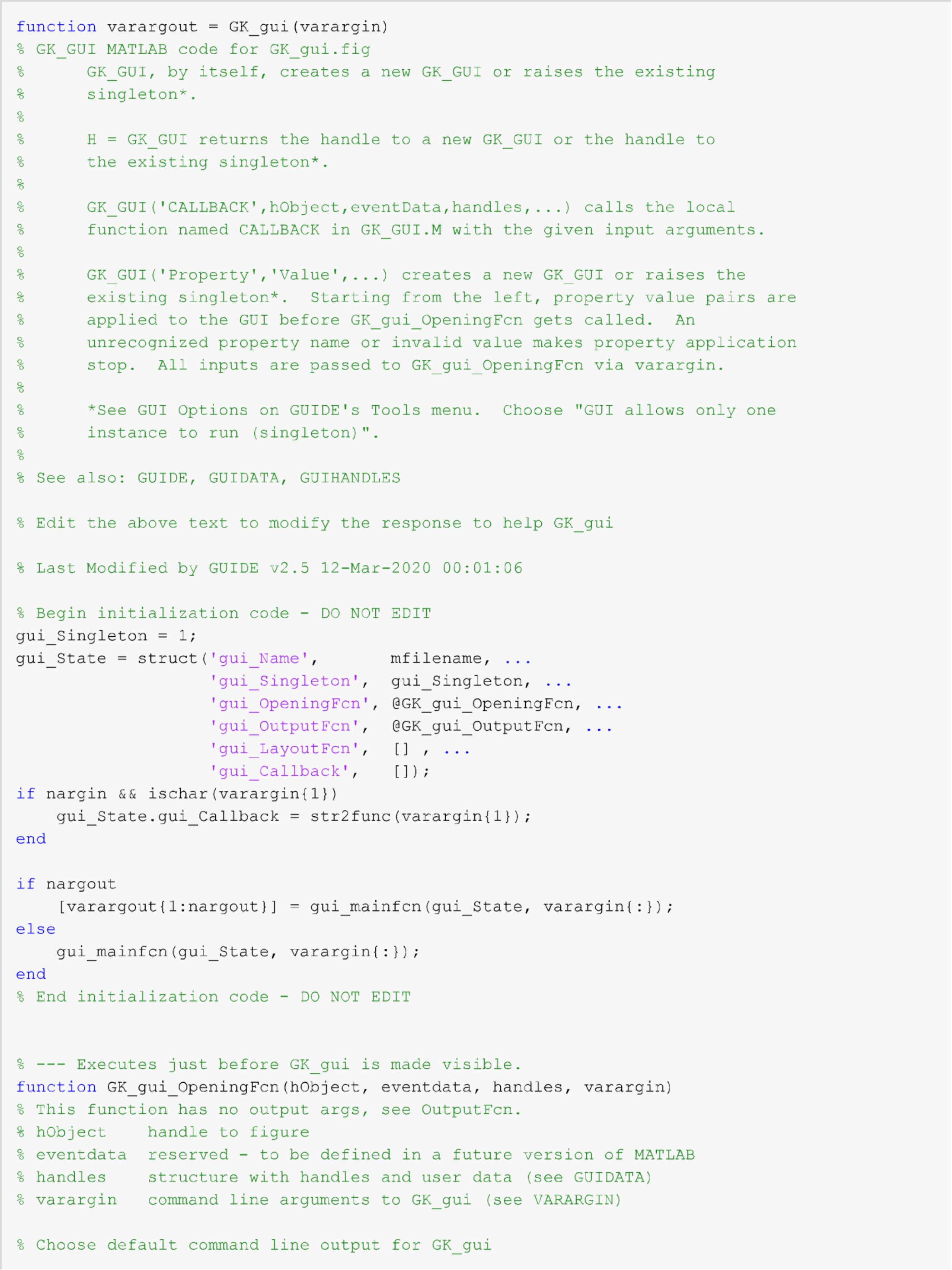
```
x=75000
R=randi([75000,90000],1,1)

EventB_Scene2=R/7500000 % Assuming ~7.5M pacakges get delivered each day with 1% being inaccurately delivered. P(B)



% Considering the misdelivery occured, what was the pobability that it was
% a rad package P(B|A)

global EventB_Ahappened
EventB_Ahappened = 6400/75000 %P(B|A)

global FinalTheftScene2   % P(A|B) Probability that the misdelivered package was a rad package( intentionally stolen),
%given B is true.
FinalTheftScene2=EventB_Ahappened.*EventA_Scene2/EventB_Scene2


set(handles.sceneG2_static,'String', FinalTheftScene2)



function AttackG3_push_Callback(hObject, eventdata, handles)
% hObject    handle to AttackG3_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global HDRScene3
HDRScene3=xlsread('Brachy_Scenarios.xls', 'Brachy_Scene3')
global U
global pathwayScene3
global b
global Theft_success
global EventA

pathwayScene3=HDRScene3(1,20) % P(B|A)
%pathwayScene3=0.72 % P(B|A)

EventA = 3/800 % # of average thefts per year. 800 is the number of HDR units in N. America %P(B)


lambdaHDRScene3_eventB = 56 % This is Mu in Poissons distribution
  x=0:250; % This is x in Poissons distribution
    U = poissrnd(lambdaHDRScene3_eventB);
    for t=U
    y = poisspdf(x,t);
    end
   global EventBScene3
    EventBScene3 = mean(y) % This is P(B)



          b=pathwayScene3.*0.95
```

```
              nfailures=(pathwayScene3.*randn(1000,1)+b)
              global Theft_success_Scene3
              Theft_success_Scene3 = mean(nfailures)

  global FinalTheftScene3
  display(EventA)
  display(EventBScene3)
  FinalTheftScene3=Theft_success_Scene3.*EventA/EventBScene3

  set(handles.sceneG3_static,'String', FinalTheftScene3)



  function EU_BISceneII_push_Callback(hObject, eventdata, handles)
% hObject    handle to EU_ BrachySceneII_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global EUbrachyScene2;
global BIProbScene
global UAdversary;
global Theftsuccess1;
global A
global theft

display(A.G2)
%display(theft.BIS1)

%AdvUtility1 = get(handles.Uadversary.UAdv1, 'String');
 BrachyProbScene2=str2double(get(handles.sceneG2_static,'String'));
 display(BrachyProbScene2)
EUbrachyScene2=(A.G2).*(BrachyProbScene2)
A.EUBrachy2=EUbrachyScene2;
set(handles.EU_BIS2_static,'String', EUbrachyScene2)
guidata(hObject,handles)

% --- Executes on button press in EU_BISceneII_push.
function EU_BIScene1_push_Callback(hObject, eventdata, handles)
% hObject    handle to EU_ BrachySceneII_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global EUbrachyScene1;
global BIProbScene
global UAdversary;
global Theftsuccess1;
global A
global theft

(A.G1)
%display(theft.BIS1)

%AdvUtility1 = get(handles.Uadversary.UAdv1, 'String');
 BrachyProbScene1=str2double(get(handles.sceneG1_static,'String'));
 display(BrachyProbScene1)
EUbrachyScene1=(A.G1).*(BrachyProbScene1)
A.EUBrachy1=EUbrachyScene1;
```

```
set(handles.EU_BIS1_static,'String', EUbrachyScene1)

guidata(hObject,handles)
% --- Executes on button press in EU_BI.
function EU_BI_Callback(hObject, eventdata, handles)
% hObject    handle to EU_BI (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global EUBrachyScene3;
global BrachyProbScene3
global UAdversary;
global Theftsuccess1;
global A
global theft

display(A.G3)
%display(theft.BIS1)

%AdvUtility1 = get(handles.Uadversary.UAdv1, 'String');
 BrachyProbScene3=str2double(get(handles.sceneG3_static,'String'));
 display(BrachyProbScene3)
EUBrachyScene3=(A.G3).*(BrachyProbScene3)
A.EUBrachy3=EUBrachyScene3;
set(handles.EU_BIS3_static,'String', EUBrachyScene3);
guidata(hObject,handles)

% --- Executes on button press in Yes_check.
function Yes_check_Callback(hObject, eventdata, handles)
% hObject    handle to Yes_check (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hint: get(hObject,'Value') returns toggle state of Yes_check
global value1
value1=get(handles.Yes_check, 'Value')
if(value1 == 1)
    set(handles.No_check, 'Enable', 'off')
else
    msgbox('Please check a box before you proceed')
end



% --- Executes on button press in No_check.
function No_check_Callback(hObject, eventdata, handles)
% hObject    handle to No_check (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hint: get(hObject,'Value') returns toggle state of No_check
global value1
global value2
value2=get(handles.No_check, 'Value')
if(value2 == 1)
  value1 = set(handles.Yes_check,'Enable', 'off')
(Threat_gui);
else
```

```
  msgbox('Please check a box before you proceed')
end


% --- Executes on button press in Return_push.
function Return_push_Callback(hObject, eventdata, handles)
% hObject    handle to Return_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
Threat_gui;
```

Published with MATLAB® R2019b

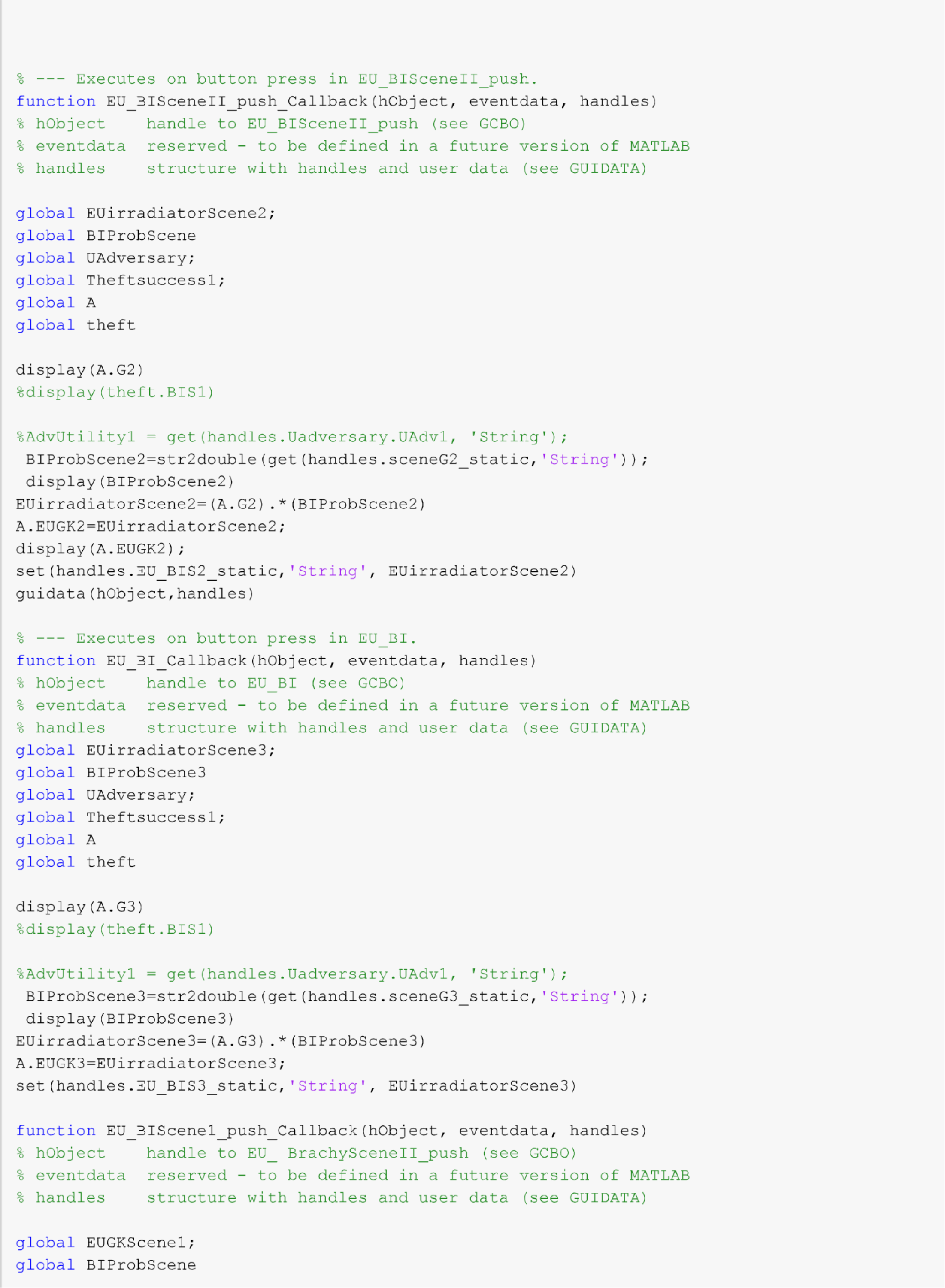


```
function varargout = GK_gui(varargin)
% GK_GUI MATLAB code for GK_gui.fig
%      GK_GUI, by itself, creates a new GK_GUI or raises the existing
%      singleton*.
%
%      H = GK_GUI returns the handle to a new GK_GUI or the handle to
%      the existing singleton*.
%
%      GK_GUI('CALLBACK',hObject,eventData,handles,...) calls the local
%      function named CALLBACK in GK_GUI.M with the given input arguments.
%
%      GK_GUI('Property','Value',...) creates a new GK_GUI or raises the
%      existing singleton*.  Starting from the left, property value pairs are
%      applied to the GUI before GK_gui_OpeningFcn gets called.  An
%      unrecognized property name or invalid value makes property application
%      stop.  All inputs are passed to GK_gui_OpeningFcn via varargin.
%
%      *See GUI Options on GUIDE's Tools menu.  Choose "GUI allows only one
%      instance to run (singleton)".
%
% See also: GUIDE, GUIDATA, GUIHANDLES

% Edit the above text to modify the response to help GK_gui

% Last Modified by GUIDE v2.5 12-Mar-2020 00:01:06

% Begin initialization code - DO NOT EDIT
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @GK_gui_OpeningFcn, ...
                   'gui_OutputFcn',  @GK_gui_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end
% End initialization code - DO NOT EDIT


% --- Executes just before GK_gui is made visible.
function GK_gui_OpeningFcn(hObject, eventdata, handles, varargin)
% This function has no output args, see OutputFcn.
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% varargin   command line arguments to GK_gui (see VARARGIN)

% Choose default command line output for GK_gui
```

```
handles.output = hObject;

% Update handles structure
guidata(hObject, handles);
global user_activity;
% UIWAIT makes GK_gui wait for user response (see UIRESUME)
% uiwait(handles.figure1);


% --- Outputs from this function are returned to the command line.
function varargout = GK_gui_OutputFcn(hObject, eventdata, handles)
% varargout  cell array for returning output args (see VARARGOUT);
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Get default command line output from handles structure
varargout{1} = handles.output;



function BI_Activitytext_Callback(hObject, eventdata, handles)
% hObject    handle to BI_Activitytext (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: get(hObject,'String') returns contents of BI_Activitytext as text
%        str2double(get(hObject,'String')) returns contents of BI_Activitytext as a double

handles.output=hObject
global user_activity;
global Dangervalue;
global Physicalform;
user_activity=str2double(get(hObject, 'String'));
if isempty(user_activity)
    errordlg('Please enter the activity of the source')
else
Dangervalue=str2double(set(handles.D_static, 'String','0.03'));
Physicalform=set(handles.form_static, 'String','Metallic');

end

guidata(hObject,handles)


% --- Executes during object creation, after setting all properties.
function BI_Activitytext_CreateFcn(hObject, eventdata, handles)
% hObject    handle to BI_Activitytext (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: edit controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'
))
    set(hObject,'BackgroundColor','white');
end
```

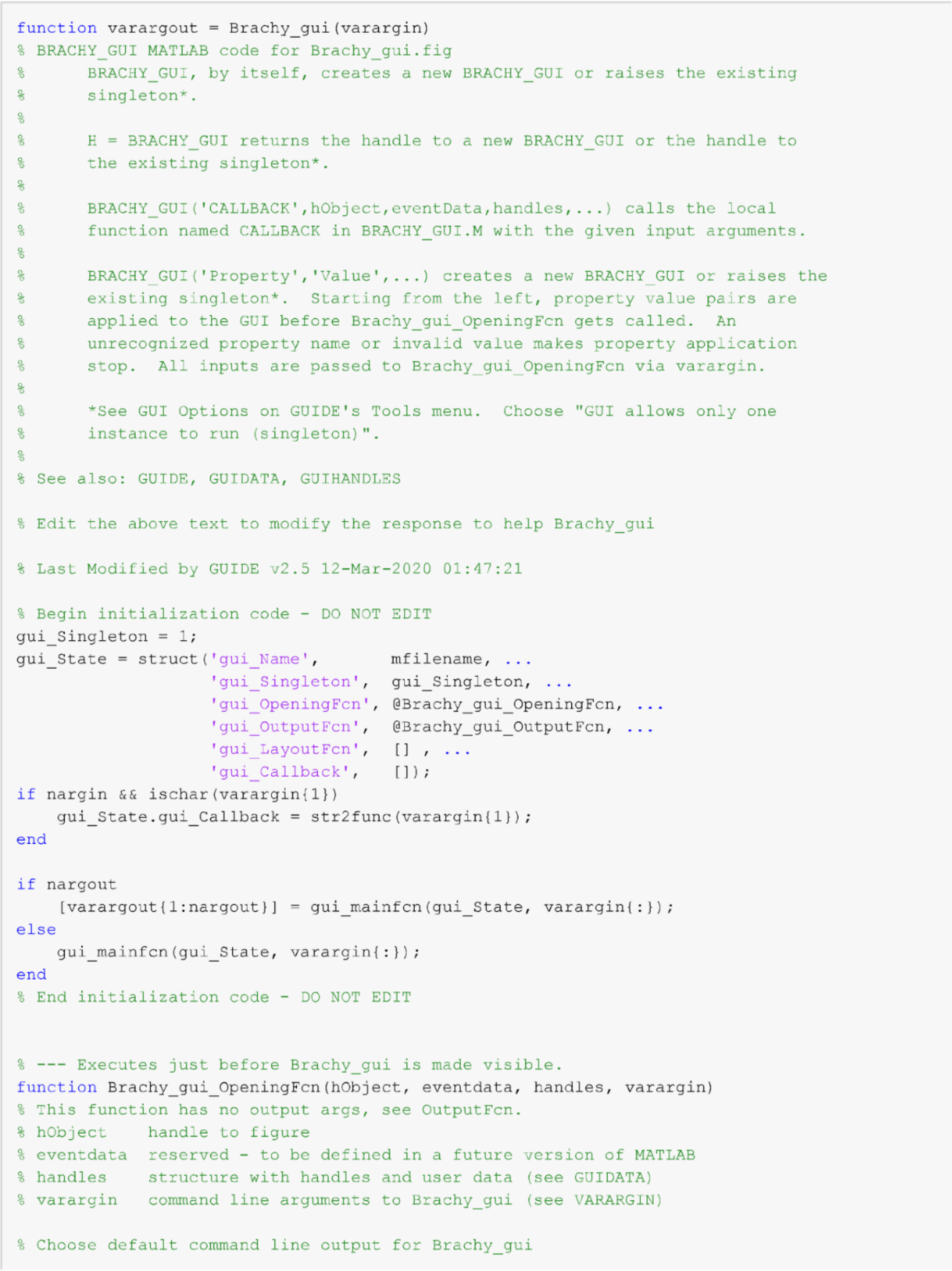
```
% --- If Enable == 'on', executes on mouse press in 5 pixel border.
% --- Otherwise, executes on mouse press in 5 pixel border or over BI_Activitytext.


% --- Executes on button press in Cat_pushbutton.
function Cat_pushbutton_Callback(hObject, eventdata, handles)
% hObject    handle to Cat_pushbutton (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global ActivityDanger_ratio;
global user_activity;
global Dangervalue;
display (user_activity)
Dangervalue = str2double(get(handles.D_static, 'String'))
display (Dangervalue);
ActivityDanger_ratio=user_activity/Dangervalue;
display (ActivityDanger_ratio);
if(ActivityDanger_ratio >=1000)
    set(handles.Cat_static, 'String', 'CAT 1')
elseif(1<ActivityDanger_ratio<10)
    set(handles.Cat_static, 'String', 'CAT 3')
else
    errordlg('Bad numbers')
end
guidata(hObject,handles)


% --- Executes on button press in AssetBI_push.
function AssetBI_push_Callback(hObject, eventdata, handles)
% hObject    handle to AssetBI_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global Physicalform;
global formnumeric;
global U_form
global ActivityDanger_ratio;
global U_attractiveness;
global U_material;
Physicalform=(get(handles.form_static, 'String'))
if strcmp(Physicalform,'Powdered Salt')
    formnumeric=2
elseif strcmp(Physicalform,'Metallic')
    formnumeric=1
else
    msgbox('Wrong form of the nuclide, Check your code')
end
U_form=1-exp(-formnumeric).^3
display (U_form);
U_attractiveness= 1-exp(-ActivityDanger_ratio/50).^3
display(U_attractiveness);
U_material=U_form.*U_attractiveness;
set(handles.Asset_static, 'String', U_material)

guidata(hObject,handles)
```

```
% --- Executes on selection change in TG_popgroup.
function TG_popgroup_Callback(hObject, eventdata, handles)
% hObject    handle to TG_popgroup (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: contents = cellstr(get(hObject,'String')) returns TG_popgroup contents as cell ar
ray
%        contents{get(hObject,'Value')} returns selected item from TG_popgroup
global TGstatus
global T;

global ED_high
global ED_med
global ED_low
global SY_high
global SY_med
global SY_low
global LL_high
global LL_med
global LL_low
global ED_default
global SY_default
global LL_default
filename='U_Adv_forCode.xls'
T=xlsread(filename)
ED_high=T(1,1)
ED_med=T(2,1)
ED_low=T(3,1)
SY_high=T(1,2)
SY_med=T(2,2)
SY_low=T(3,2)
LL_high=T(1,3)
LL_med=T(2,3)
LL_low=T(3,3)
ED_default=T(1,5)
LL_default=T(1,6)
SY_default=T(1,7)
TGstatus=get(hObject, 'Value')
%display(checkboxStatus)
if strcmp(TGstatus, 'Outsider(G1)')
    TGstatus=2;
elseif strcmp(TGstatus, 'Semiinsider(G2)')
    TGstatus=3;
elseif strcmp(TGstatus, 'Insider(G3)')
    TGstatus=4;
end
guidata(hObject,handles);

% --- Executes during object creation, after setting all properties.
function TG_popgroup_CreateFcn(hObject, eventdata, handles)
% hObject    handle to TG_popgroup (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: popupmenu controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'
))
    set(hObject,'BackgroundColor','white');
end


% --- Executes on button press in Adv_push.

% --- Executes on button press in AttackG1_push.
function AttackG1_push_Callback(hObject, eventdata, handles)
% hObject    handle to AttackG1_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
%filename('BI_Scenarios.xls')
global GK
GK=xlsread('GK_Scenarios.xls')
global U
global a
global b
global c
global lamdaGKS_one
global Theft_success1
global theft
%lambdaBIS_one = 3
a=GK(1,20)


  lambdaGKS_one = 8 % Maintenance and repair days

    U = poissrnd(lambdaGKS_one); %Generates random numbers considering mean of 8
      for t=U

          b=a.*0.95 %2 sigma std deviation

          % Vector is created with 1000 random values drawn from a uniform
          % distribution wth a mean of the failure probability of
          % interruption
              nfailures=(a.*randn(1000,1)+b)
              nf = mean(nfailures) % mean of the failure probabilities

    y = binopdf(1,U,nf); %U=8 which is # of trials, nf = failure prob
    %plot(nfailures,y,'+')


    Theft_success1 =mean(y);



     theft.GKS1=Theft_success1
  end
  set(handles.sceneG1_static,'String', Theft_success1)


% --- Executes on button press in AttackG2_push.
function AttackG2_push_Callback(hObject, eventdata, handles)
% hObject    handle to AttackG2_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global GKS2
GKS2=xlsread('GK_Scenarios.xls', 'GK_Scene2')
global U
global a
global b
global c
global lamdaGKS_two
global Theft_success
lambdaGKS_two = 8
a=GKS2(1,20)


     U = poissrnd(lambdaGKS_two);
      for t=U
          b=a.*0.95

              nfailures=(a.*randn(1000,1)+b)
              nf = mean(nfailures)

    y = binopdf(1,U,nf);
    %plot(nfailures,y,'+')

     Theft_success=1-mean(y)
  end
  set(handles.sceneG2_static,'String', Theft_success)

% --- Executes on button press in AttackG3_push.
function AttackG3_push_Callback(hObject, eventdata, handles)
% hObject    handle to AttackG3_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global GKS3
GKS3=xlsread('GK_Scenarios.xls', 'GK_Scene3')
global U
global a
global b
global c
global lamdaGKS_three
global Theft_success
lambdaGKS_three = 8
a=GKS3(1,19) %success prob

     U = poissrnd(lambdaGKS_three);
      for t=U
          b=a.*0.95

              nfailures=(a.*randn(1000,1)+b)
              nf = mean(nfailures)

    y = binopdf(0,U,nf);
    %plot(nfailures,y,'+')

     Theft_success=1-mean(y)
  end
  set(handles.sceneG3_static,'String', Theft_success)
```



```
% --- Executes on button press in EU_BISceneII_push.
function EU_BISceneII_push_Callback(hObject, eventdata, handles)
% hObject    handle to EU_BISceneII_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global EUirradiatorScene2;
global BIProbScene
global UAdversary;
global Theftsuccess1;
global A
global theft

display(A.G2)
%display(theft.BIS1)

%AdvUtility1 = get(handles.Uadversary.UAdv1, 'String');
 BIProbScene2=str2double(get(handles.sceneG2_static,'String'));
 display(BIProbScene2)
EUirradiatorScene2=(A.G2).*(BIProbScene2)
A.EUGK2=EUirradiatorScene2;
display(A.EUGK2);
set(handles.EU_BIS2_static,'String', EUirradiatorScene2)
guidata(hObject,handles)

% --- Executes on button press in EU_BI.
function EU_BI_Callback(hObject, eventdata, handles)
% hObject    handle to EU_BI (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global EUirradiatorScene3;
global BIProbScene3
global UAdversary;
global Theftsuccess1;
global A
global theft

display(A.G3)
%display(theft.BIS1)

%AdvUtility1 = get(handles.Uadversary.UAdv1, 'String');
 BIProbScene3=str2double(get(handles.sceneG3_static,'String'));
 display(BIProbScene3)
EUirradiatorScene3=(A.G3).*(BIProbScene3)
A.EUGK3=EUirradiatorScene3;
set(handles.EU_BIS3_static,'String', EUirradiatorScene3)

function EU_BIScene1_push_Callback(hObject, eventdata, handles)
% hObject    handle to EU_ BrachySceneII_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global EUGKScene1;
global BIProbScene
global UAdversary;
global Theftsuccess1;
global A
global theft

display(A.G1)
%display(theft.BIS1)

%AdvUtility1 = get(handles.Uadversary.UAdv1, 'String');
 GKProbScene1=str2double(get(handles.sceneG1_static,'String'));
 display(GKProbScene1)
EUGKScene1=(A.G1).*(GKProbScene1)
A.EUGK1=EUGKScene1;
set(handles.EU_BIS1_static,'String', EUGKScene1)


% --- Executes on button press in Yes_check.
function Yes_check_Callback(hObject, eventdata, handles)
% hObject    handle to Yes_check (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hint: get(hObject,'Value') returns toggle state of Yes_check
global value1
value1=get(handles.Yes_check, 'Value')
if(value1 == 1)
    set(handles.No_check, 'Enable', 'off')
else
    msgbox('Please check a box before you proceed')
end



% --- Executes on button press in No_check.
function No_check_Callback(hObject, eventdata, handles)
% hObject    handle to No_check (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hint: get(hObject,'Value') returns toggle state of No_check
global value1
global value2
value2=get(handles.No_check, 'Value')
if(value2 == 1)
  value1 = set(handles.Yes_check,'Enable', 'off')
(Threat_gui);
else
  msgbox('Please check a box before you proceed')
end


% --- Executes on button press in Return_push.
function Return_push_Callback(hObject, eventdata, handles)
% hObject    handle to Return_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
```

Brachy GUI



```
function varargout = Brachy_gui(varargin)
% BRACHY_GUI MATLAB code for Brachy_gui.fig
%      BRACHY_GUI, by itself, creates a new BRACHY_GUI or raises the existing
%      singleton*.
%
%      H = BRACHY_GUI returns the handle to a new BRACHY_GUI or the handle to
%      the existing singleton*.
%
%      BRACHY_GUI('CALLBACK',hObject,eventData,handles,...) calls the local
%      function named CALLBACK in BRACHY_GUI.M with the given input arguments.
%
%      BRACHY_GUI('Property','Value',...) creates a new BRACHY_GUI or raises the
%      existing singleton*.  Starting from the left, property value pairs are
%      applied to the GUI before Brachy_gui_OpeningFcn gets called.  An
%      unrecognized property name or invalid value makes property application
%      stop.  All inputs are passed to Brachy_gui_OpeningFcn via varargin.
%
%      *See GUI Options on GUIDE's Tools menu.  Choose "GUI allows only one
%      instance to run (singleton)".
%
% See also: GUIDE, GUIDATA, GUIHANDLES

% Edit the above text to modify the response to help Brachy_gui

% Last Modified by GUIDE v2.5 12-Mar-2020 01:47:21

% Begin initialization code - DO NOT EDIT
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @Brachy_gui_OpeningFcn, ...
                   'gui_OutputFcn',  @Brachy_gui_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end
% End initialization code - DO NOT EDIT


% --- Executes just before Brachy_gui is made visible.
function Brachy_gui_OpeningFcn(hObject, eventdata, handles, varargin)
% This function has no output args, see OutputFcn.
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% varargin   command line arguments to Brachy_gui (see VARARGIN)

% Choose default command line output for Brachy_gui
```

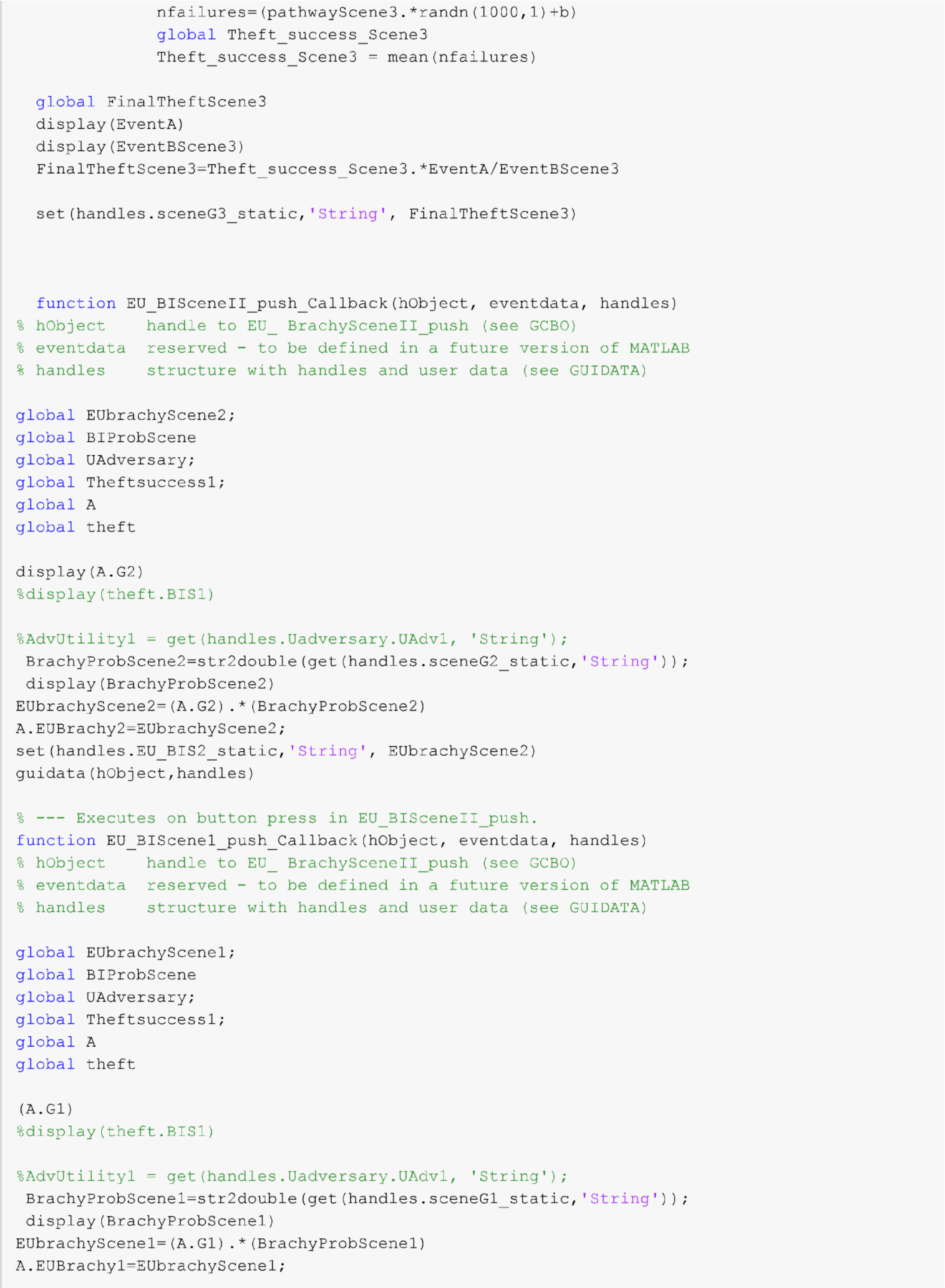
```
handles.output = hObject;

% Update handles structure
guidata(hObject, handles);
global user_activity;
% UIWAIT makes Brachy_gui wait for user response (see UIRESUME)
% uiwait(handles.figure1);


% --- Outputs from this function are returned to the command line.
function varargout = Brachy_gui_OutputFcn(hObject, eventdata, handles)
% varargout  cell array for returning output args (see VARARGOUT);
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Get default command line output from handles structure
varargout{1} = handles.output;



function Brachy_Activitytext_Callback(hObject, eventdata, handles)
% hObject    handle to Brachy_Activitytext (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: get(hObject,'String') returns contents of Brachy_Activitytext as text
%        str2double(get(hObject,'String')) returns contents of Brachy_Activitytext as a do
uble

handles.output=hObject
global user_activity;
global Dangervalue;
global Physicalform;
user_activity=str2double(get(hObject, 'String'));
if isempty(user_activity)
    errordlg('Please enter the activity of the source')
else
Dangervalue=str2double(set(handles.D_static, 'String','0.08'));
Physicalform=set(handles.form_static, 'String','Metallic');

end

guidata(hObject,handles)


% --- Executes during object creation, after setting all properties.
function Brachy_Activitytext_CreateFcn(hObject, eventdata, handles)
% hObject    handle to Brachy_Activitytext (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: edit controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'
))
    set(hObject,'BackgroundColor','white');
```

```
end


% --- If Enable == 'on', executes on mouse press in 5 pixel border.
% --- Otherwise, executes on mouse press in 5 pixel border or over Brachy_Activitytext.


% --- Executes on button press in Cat_pushbutton.
function Cat_pushbutton_Callback(hObject, eventdata, handles)
% hObject    handle to Cat_pushbutton (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
%THIS IS FOR IR-192
global ActivityDanger_ratio;
global user_activity;
global Dangervalue;
display (user_activity)
Dangervalue = str2double(get(handles.D_static, 'String'))
display (Dangervalue);
ActivityDanger_ratio=user_activity/Dangervalue;
display (ActivityDanger_ratio);
if(ActivityDanger_ratio >=1000)
    set(handles.Cat_static, 'String', 'CAT 1')
elseif(1<ActivityDanger_ratio<10)
    set(handles.Cat_static, 'String', 'CAT3')
else
    errordlg('Bad numbers, Enter the values between 0.037-0.55 TBq')
end
guidata(hObject,handles)


% --- Executes on button press in AssetBI_push.
function AssetBI_push_Callback(hObject, eventdata, handles)
% hObject    handle to AssetBI_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global Physicalform;
global formnumeric;
global U_form
global ActivityDanger_ratio;
global U_attractiveness;
global U_material;
Physicalform=(get(handles.form_static, 'String'));
if strcmp(Physicalform,'Powdered Salt')
    formnumeric=2
elseif strcmp(Physicalform, 'Metallic')
    formnumeric=1
else
    msgbox('Bad numbers, Sorry!')
end
U_form=1-exp(-formnumeric).^3
display (U_form);
U_attractiveness= 1-exp(-ActivityDanger_ratio/9.07).^3
display(U_attractiveness);
U_material=U_form.*U_attractiveness;
set(handles.Asset_static, 'String', U_material)
```

```
guidata(hObject,handles)


% --- Executes on selection change in TG_popgroup.
function TG_popgroup_Callback(hObject, eventdata, handles)
% hObject    handle to TG_popgroup (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: contents = cellstr(get(hObject,'String')) returns TG_popgroup contents as cell ar
ray
%        contents{get(hObject,'Value')} returns selected item from TG_popgroup
global TGstatus
global T;

global ED_high
global ED_med
global ED_low
global SY_high
global SY_med
global SY_low
global LL_high
global LL_med
global LL_low
global ED_default
global SY_default
global LL_default
filename='U_Adv_forCode.xls'
T=xlsread(filename)
ED_high=T(1,1)
ED_med=T(2,1)
ED_low=T(3,1)
SY_high=T(1,2)
SY_med=T(2,2)
SY_low=T(3,2)
LL_high=T(1,3)
LL_med=T(2,3)
LL_low=T(3,3)
ED_default=T(1,5)
LL_default=T(1,6)
SY_default=T(1,7)
TGstatus=get(hObject, 'Value')
%display(checkboxStatus)
if strcmp(TGstatus, 'Outsider(G1)')
    TGstatus=2;

  Fprintf(TGstatus)


elseif strcmp(TGstatus, 'Semiinsider(G2)')
    TGstatus=3;

elseif strcmp(TGstatus, 'Insider(G3)')
    TGstatus=4;

end
guidata(hObject,handles);
```

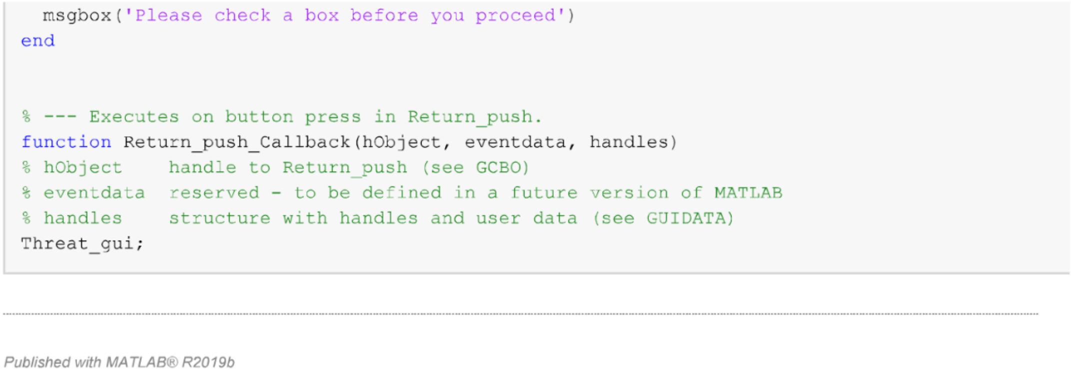
```
% --- Executes during object creation, after setting all properties.
function TG_popgroup_CreateFcn(hObject, eventdata, handles)
% hObject    handle to TG_popgroup (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: popupmenu controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'
))
    set(hObject,'BackgroundColor','white');
end


% --- Executes on button press in Adv_push.

% --- Executes on button press in AttackG1_push.
function AttackG1_push_Callback(hObject, eventdata, handles)
% hObject    handle to AttackG1_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
%filename('BI_Scenarios.xls')
global HDR1IU
global HDR1Methodist
HDR1IU=xlsread('Brachy_Scenarios.xls')
HDR1Methodist=xlsread('Brachy_Scenarios.xls', 'Brachy_Scene1-b')
global U
global pathwayIU
global pathwayMethodist
global bIU
global bMethodist
global EventA
global EventB
global Theft_success1a
global Theft_success1b
global theft
%lambdaBIS_one = 3
pathwayIU=HDR1IU(1,20); % Read the non interruption probability for Scene1a
pathwayMethodist=HDR1Methodist(1,20) % Read the non interruption probability for Scene1b

%pathwayIU=0.68; % Read the non interruption probability for Scene1a
%pathwayMethodist=0.60 % Read the non interruption probability for Scene1b

% Event A is the prior distribution
EventA = 3/800 % # of average thefts per year. 800 is the number of HDR units in N. Americ
a

%Event B is # of hours the device is vulnerable, (unused+source exchange).
%Based on 10patient/wk*2hr/patient = 20 hrs/wk HDR is busy, which means 20
%hrs/wk HDR is not busy----- 20hr/wk*13 wk in 3 month = 260 hours +8 hours
%for source excahnge every quarter.  =  89days/yr total that the source is
%vulnerable for theft
  lambdaHDR_eventB = 89
  x=0:250;
    U = poissrnd(lambdaHDR_eventB);
    for t=U
    y = poisspdf(x,t);
    end

    EventB = mean(y)

   % U = poissrnd(lambdaHDR_eventB);
    %  for t=U

          bIU=pathwayIU.*0.95

              nfailures=(pathwayIU.*randn(1000,1)+bIU)
              Theft_success1a = mean(nfailures)

               bMethodist=pathwayMethodist.*0.95

              nfailures=(pathwayIU.*randn(1000,1)+bMethodist)
              Theft_success1b = mean(nfailures)
   % y = binopdf(1,U,nf);
    %plot(nfailures,y,'+')

    %USing Bayes theorem
    global FinalIU_theft
    FinalIU_theft=Theft_success1a.*EventA/EventB
    global FinalMethodist_theft
    FinalMethodist_theft=Theft_success1b.*EventA/EventB

 global Totalprobability
 %Totalprobability = FinalIU_theft+FinalMethodist_theft/2
 Totalprobability = FinalMethodist_theft
     theft.GKS1=Totalprobability

  set(handles.sceneG1_static,'String', Totalprobability)


% --- Executes on button press in AttackG2_push.
function AttackG2_push_Callback(hObject, eventdata, handles)
% hObject    handle to AttackG2_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% --- Executes on button press in AttackG3_push.

%-----------------------------------------------------
% There are 800 HDR units in N. America. Each HDR goes through source
% exchang 4 times a year.
% 4*2=8 times source gets delivered (2 times source deliver each time)This
% is the number of times the source gets delivered for 1 HDR, but there are
% 800 HDR so total of 6400.
%According to NTI, there were 4 delivary failures in past 4 years, so 1
%every year. 1/6400 = 0.00015------P(A)
%Event B is the # of mail lost by mail carrier (Fedex/UPS)
%-----------------------------------------------------------
global EventA_Scene2
global EventB_Scene2

EventA_Scene2=1/6400 % If there were 1 delivary error each year in the past four years P(A
)
```

```
x=75000
R=randi([75000,90000],1,1)

EventB_Scene2=R/7500000 % Assuming ~7.5M pacakges get delivered each day with 1% being ina
ccurately delivered. P(B)



% Considering the misdelivery occured, what was the pobability that it was
% a rad package P(B|A)

global EventB_Ahappened
EventB_Ahappened = 6400/75000 %P(B|A)

global FinalTheftScene2   % P(A|B) Probability that the misdelivered package was a rad pac
kage( intentionally stolen),
%given B is true.
FinalTheftScene2=EventB_Ahappened.*EventA_Scene2/EventB_Scene2


set(handles.sceneG2_static,'String', FinalTheftScene2)



function AttackG3_push_Callback(hObject, eventdata, handles)
% hObject    handle to AttackG3_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global HDRScene3
HDRScene3=xlsread('Brachy_Scenarios.xls', 'Brachy_Scene3')
global U
global pathwayScene3
global b
global Theft_success
global EventA

pathwayScene3=HDRScene3(1,20) % P(B|A)
%pathwayScene3=0.72 % P(B|A)

EventA = 3/800 % # of average thefts per year. 800 is the number of HDR units in N. Americ
a %P(B)


lambdaHDRScene3_eventB = 56 % This is Mu in Poissons distribution
  x=0:250; % This is x in Poissons distribution
    U = poissrnd(lambdaHDRScene3_eventB);
    for t=U
    y = poisspdf(x,t);
    end
   global EventBScene3
    EventBScene3 = mean(y) % This is P(B)



          b=pathwayScene3.*0.95
```



```
              nfailures=(pathwayScene3.*randn(1000,1)+b)
              global Theft_success_Scene3
              Theft_success_Scene3 = mean(nfailures)

  global FinalTheftScene3
  display(EventA)
  display(EventBScene3)
  FinalTheftScene3=Theft_success_Scene3.*EventA/EventBScene3

  set(handles.sceneG3_static,'String', FinalTheftScene3)



  function EU_BISceneII_push_Callback(hObject, eventdata, handles)
% hObject    handle to EU_ BrachySceneII_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global EUbrachyScene2;
global BIProbScene
global UAdversary;
global Theftsuccess1;
global A
global theft

display(A.G2)
%display(theft.BIS1)

%AdvUtility1 = get(handles.Uadversary.UAdv1, 'String');
 BrachyProbScene2=str2double(get(handles.sceneG2_static,'String'));
 display(BrachyProbScene2)
EUbrachyScene2=(A.G2).*(BrachyProbScene2)
A.EUBrachy2=EUbrachyScene2;
set(handles.EU_BIS2_static,'String', EUbrachyScene2)
guidata(hObject,handles)

% --- Executes on button press in EU_BISceneII_push.
function EU_BIScene1_push_Callback(hObject, eventdata, handles)
% hObject    handle to EU_ BrachySceneII_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global EUbrachyScene1;
global BIProbScene
global UAdversary;
global Theftsuccess1;
global A
global theft

(A.G1)
%display(theft.BIS1)

%AdvUtility1 = get(handles.Uadversary.UAdv1, 'String');
 BrachyProbScene1=str2double(get(handles.sceneG1_static,'String'));
 display(BrachyProbScene1)
EUbrachyScene1=(A.G1).*(BrachyProbScene1)
A.EUBrachy1=EUbrachyScene1;
```

```
set(handles.EU_BIS1_static,'String', EUbrachyScene1)

guidata(hObject,handles)
% --- Executes on button press in EU_BI.
function EU_BI_Callback(hObject, eventdata, handles)
% hObject    handle to EU_BI (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global EUBrachyScene3;
global BrachyProbScene3
global UAdversary;
global Theftsuccess1;
global A
global theft

display(A.G3)
%display(theft.BIS1)

%AdvUtility1 = get(handles.Uadversary.UAdv1, 'String');
 BrachyProbScene3=str2double(get(handles.sceneG3_static,'String'));
 display(BrachyProbScene3)
EUBrachyScene3=(A.G3).*(BrachyProbScene3)
A.EUBrachy3=EUBrachyScene3;
set(handles.EU_BIS3_static,'String', EUBrachyScene3);
guidata(hObject,handles)

% --- Executes on button press in Yes_check.
function Yes_check_Callback(hObject, eventdata, handles)
% hObject    handle to Yes_check (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hint: get(hObject,'Value') returns toggle state of Yes_check
global value1
value1=get(handles.Yes_check, 'Value')
if(value1 == 1)
    set(handles.No_check, 'Enable', 'off')
else
    msgbox('Please check a box before you proceed')
end



% --- Executes on button press in No_check.
function No_check_Callback(hObject, eventdata, handles)
% hObject    handle to No_check (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hint: get(hObject,'Value') returns toggle state of No_check
global value1
global value2
value2=get(handles.No_check, 'Value')
if(value2 == 1)
  value1 = set(handles.Yes_check,'Enable', 'off')
(Threat_gui);
else
```

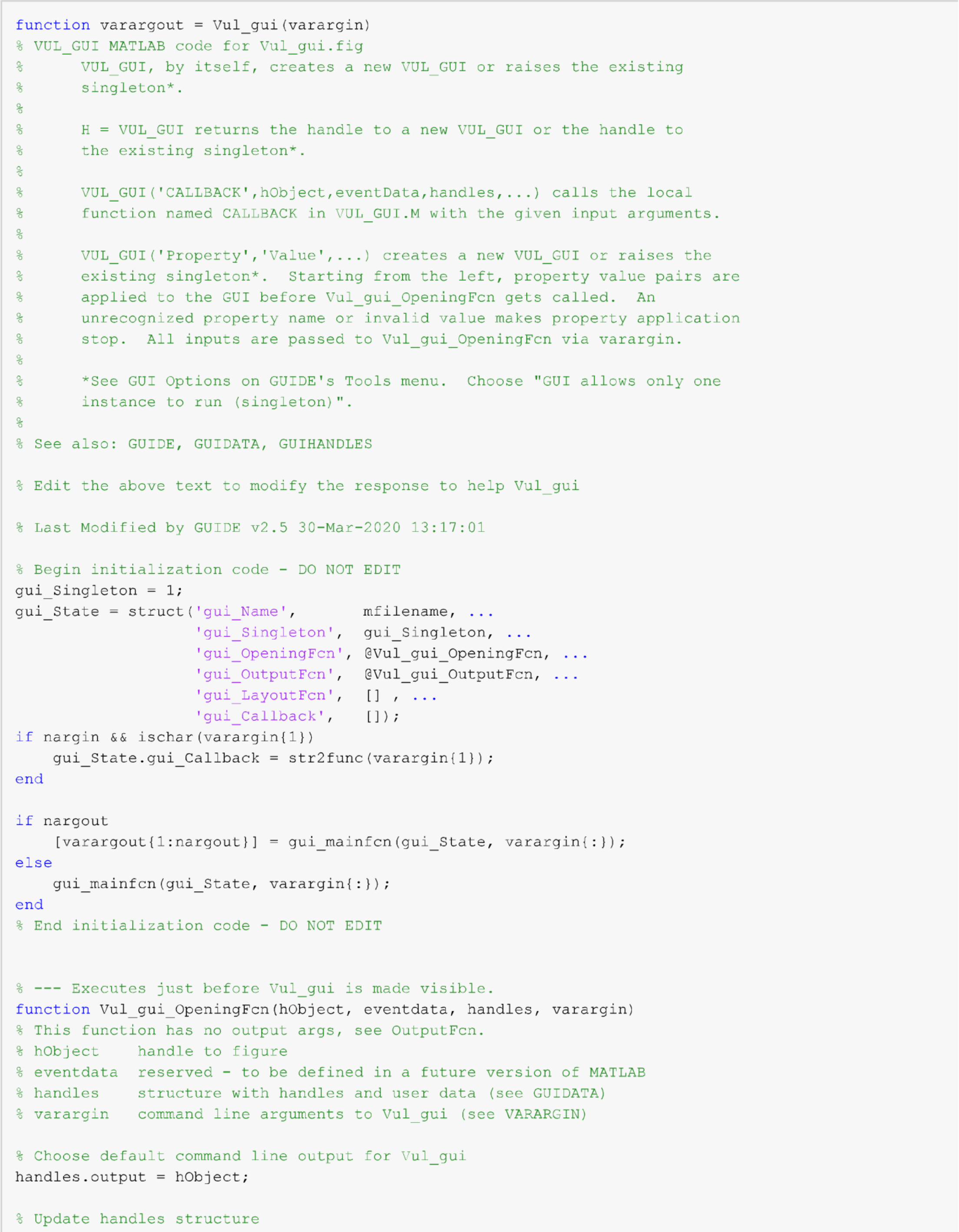


```
  msgbox('Please check a box before you proceed')
end


% --- Executes on button press in Return_push.
function Return_push_Callback(hObject, eventdata, handles)
% hObject    handle to Return_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
Threat_gui;
```

Published with MATLAB® R2019b

Vulnerability – Vul GUI

$e^{\pi i}+1=0$



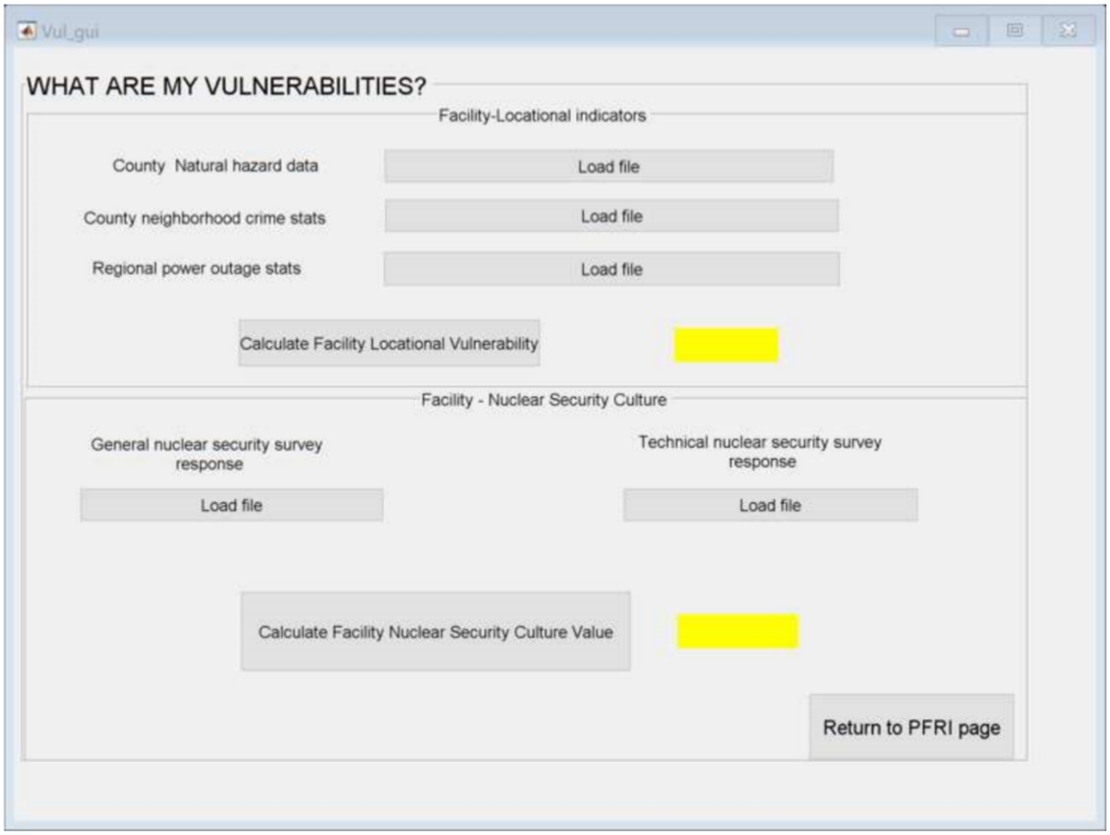
```
function varargout = Vul_gui(varargin)
% VUL_GUI MATLAB code for Vul_gui.fig
%      VUL_GUI, by itself, creates a new VUL_GUI or raises the existing
%      singleton*.
%
%      H = VUL_GUI returns the handle to a new VUL_GUI or the handle to
%      the existing singleton*.
%
%      VUL_GUI('CALLBACK',hObject,eventData,handles,...) calls the local
%      function named CALLBACK in VUL_GUI.M with the given input arguments.
%
%      VUL_GUI('Property','Value',...) creates a new VUL_GUI or raises the
%      existing singleton*.  Starting from the left, property value pairs are
%      applied to the GUI before Vul_gui_OpeningFcn gets called.  An
%      unrecognized property name or invalid value makes property application
%      stop.  All inputs are passed to Vul_gui_OpeningFcn via varargin.
%
%      *See GUI Options on GUIDE's Tools menu.  Choose "GUI allows only one
%      instance to run (singleton)".
%
% See also: GUIDE, GUIDATA, GUIHANDLES

% Edit the above text to modify the response to help Vul_gui

% Last Modified by GUIDE v2.5 30-Mar-2020 13:17:01

% Begin initialization code - DO NOT EDIT
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @Vul_gui_OpeningFcn, ...
                   'gui_OutputFcn',  @Vul_gui_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end
% End initialization code - DO NOT EDIT


% --- Executes just before Vul_gui is made visible.
function Vul_gui_OpeningFcn(hObject, eventdata, handles, varargin)
% This function has no output args, see OutputFcn.
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% varargin   command line arguments to Vul_gui (see VARARGIN)

% Choose default command line output for Vul_gui
handles.output = hObject;

% Update handles structure
```

```
guidata(hObject, handles);

% UIWAIT makes Vul_gui wait for user response (see UIRESUME)
% uiwait(handles.figure1);


% --- Outputs from this function are returned to the command line.
function varargout = Vul_gui_OutputFcn(hObject, eventdata, handles)
% varargout  cell array for returning output args (see VARARGOUT);
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Get default command line output from handles structure
varargout{1} = handles.output;


% --- Executes on button press in BIcheckbox.




% --- Executes on button press in Atmospherehazard_push.
function Atmospherehazard_push_Callback(hObject, eventdata, handles)
% hObject    handle to Atmospherehazard_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global NormalizedMet;
global NormalizedGeo;
global NormalizedHydro;
global A;
handles.NaturalDisasters=uigetfile('*.xls')
guidata(hObject,handles)
NaturalDisasters=handles.NaturalDisasters;
%Make sure the when you read your file, the chronology of the columns
%should be the same.
Yeardata=xlsread(NaturalDisasters,'A:A'); % This will read the first col, which is the A coloumn.
Met=xlsread(NaturalDisasters,'B:B')%This will read the second col, which is the B coloumn.
Geo=xlsread(NaturalDisasters,'C:C')%This will read the third col, which is the C coloumn.
Hydro=xlsread(NaturalDisasters,'D:D')%This will read the fourth col, which is the D coloumn.
% Below is the code for normalization of values.
for x=1:18
    NormalizedMet(x,1)=(Met(x,1)-min(Met))/(max(Met)-min(Met))
     NormalizedGeo(x,1)=(Geo(x,1)-min(Geo))/(max(Geo)-min(Geo))
      NormalizedHydro(x,1)=(Hydro(x,1)-min(Hydro))/(max(Hydro)-min(Hydro))
           x=x+1;
end
A.Met=NormalizedMet(:);
A.Geo=NormalizedGeo(:);
A.Hydro=NormalizedHydro(:);


% --- Executes on button press in Crime_push.
function Crime_push_Callback(hObject, eventdata, handles)
% hObject    handle to Crime_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global NormalizedPC;
global NormalizedVC;
global A;
```

```
handles.Crime=uigetfile('*.xls')
guidata(hObject,handles)
Crime=handles.Crime;
%Make sure the when you read your file, the chronology of the columns
%should be the same as the input
Propertycrime=xlsread(Crime,'B:B')%This will read the second col, which is the B coloumn.
Violentcrime=xlsread(Crime,'C:C')%This will read the third col, which is the C coloumn.
% Below is the code for normalization of values.
for x=1:18
    NormalizedPC(x,1)=(Propertycrime(x,1)-min(Propertycrime))/(max(Propertycrime)-min(Propertycrim
e))
     NormalizedVC(x,1)=(Violentcrime(x,1)-min(Violentcrime))/(max(Violentcrime)-min(Violentcrime))
           x=x+1;
end
A.PC=NormalizedPC(:);
A.VC=NormalizedVC(:);


% --- Executes on button press in Power_push.
function Power_push_Callback(hObject, eventdata, handles)
% hObject    handle to Power_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global NormalizedOutage;
global A;

handles.Poweroutage=uigetfile('*.xls')
guidata(hObject,handles)
Poweroutage=handles.Poweroutage;
%Make sure the when you read your file, the chronology of the columns
%should be the same as the input
Poweroutage=xlsread(Poweroutage,'B:B')%This will read the second col, which is the B coloumn.
% Below is the code for normalization of values.
for x=1:18
    NormalizedOutage(x,1)=(Poweroutage(x,1)-min(Poweroutage))/(max(Poweroutage)-min(Poweroutage))
           x=x+1;
end
A.Outage=NormalizedOutage(:); % NormalizedOutage data is assigned to A.Outage to be accessible as
call funcitons

% --- Executes on button press in PCA_push.
function PCA_push_Callback(hObject, eventdata, handles)
% hObject    handle to PCA_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global A;
global Vulnerability;
IngredientsCombined = [A.Met, A.Hydro, A.PC, A.VC, A.Outage];
display (IngredientsCombined)
%Do the PCA
%[coeff, score, latent,~,explained] = pca(IngredientsCombined)
coefs = pca(IngredientsCombined)
rotatedcoef = rotatefactors(coefs(:,1:3), 'Method', 'varimax')
%coefactor=factoran(IngredientsCombined)
% Calculate eigenvalues and eigenvectors of the covariance matrix
covarianceMatrix=cov(IngredientsCombined)
[V,D]=eig(covarianceMatrix) %V Eigenvectors and D is eigenvalues.
%[Lambda,Psi,T] = factoran(IngredientsCombined,1)
[Lambda,Psi,T] = factoran(IngredientsCombined,1)
Metwt=Lambda(1,1)
Hydrowt=Lambda(2,1)
```

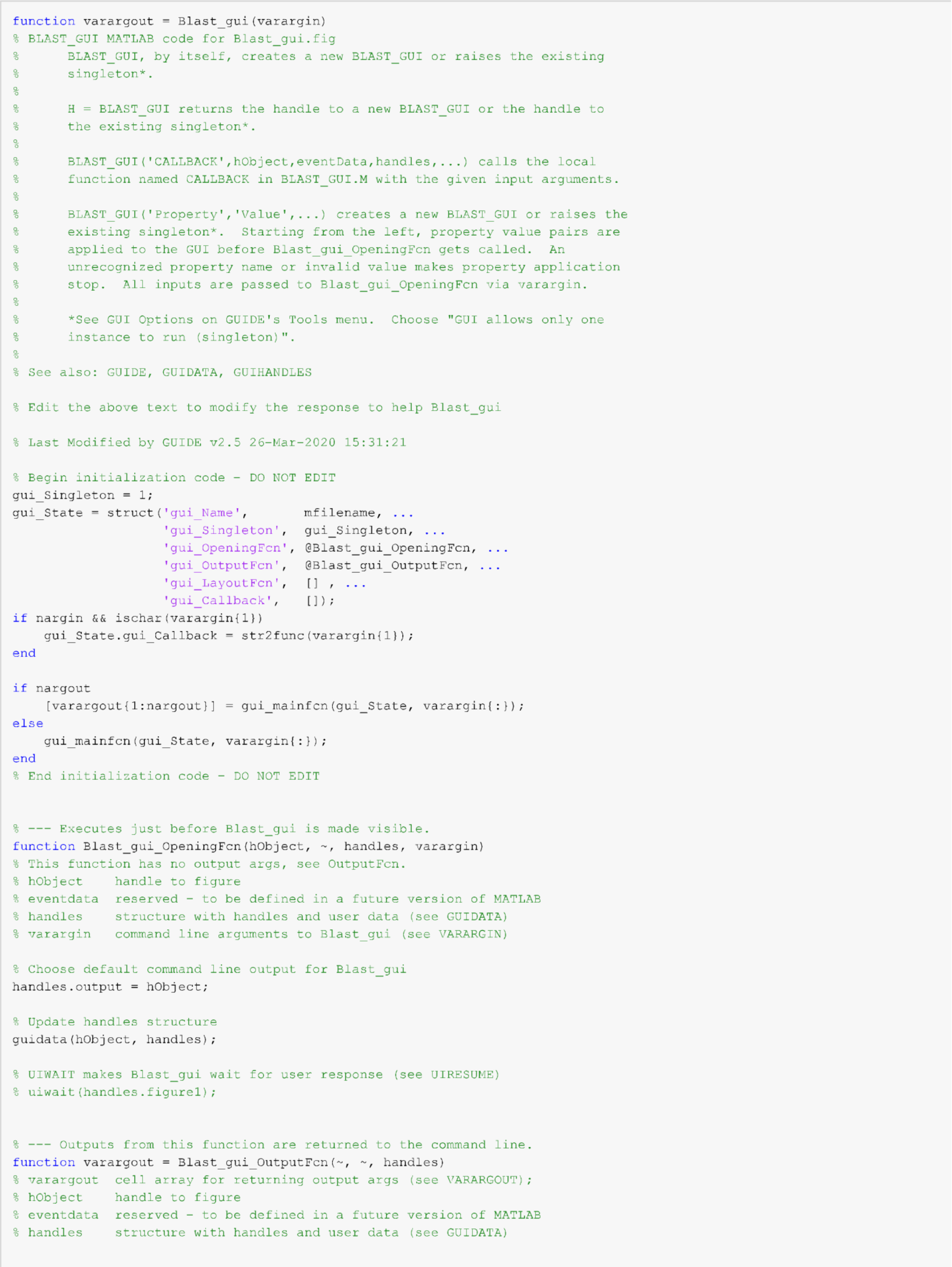
```
PCwt=Lambda(3,1)
VCwt=Lambda(4,1)
POwt=Lambda(5,1)


%Metwt=Lambda(1,2)
%Hydrowt=Lambda(2,1)
%PCwt=Lambda(3,1)
%VCwt=Lambda(4,1)
%POwt=Lambda(5,2)
Weights = [Metwt, Hydrowt, PCwt, VCwt, POwt]
Means=[mean(A.Met), mean(A.Hydro), mean(A.PC), mean(A.VC), mean(A.Outage)];
display(Means)

VariableDev=[std(A.Met), std(A.Hydro), std(A.PC), std(A.VC), std(A.Outage)];
display(VariableDev)

Metfinal=round((Metwt).*(A.Met-mean(A.Met))/std(A.Met),3);
Hydrofinal= round((Hydrowt).*(A.Hydro-mean(A.Hydro))/std(A.Hydro),3);
PCfinal=round((PCwt).*(A.PC-mean(A.PC))/std(A.PC),3);
VCfinal=round((VCwt).*(A.VC-mean(A.VC))/std(A.VC),3);
POfinal=round((POwt).*(A.Outage-mean(A.Outage))/std(A.Outage),3);

Scaled_final=[Metfinal,Hydrofinal,PCfinal,VCfinal,POfinal]
Scaled_final_col = [{'Meteorological hazard'},{'Hydrological hazard'}, {'Property Crime'}, {'Viole
nt Crime'},{'Power Outage'}]
Scaled_withweightsonly=[((Metwt).*(A.Met)), ((Hydrowt).*(A.Hydro)),((PCwt).*(A.PC)),((VCwt).*(A.VC
)), ((POwt).*(A.Outage))]


xlswrite('LocationalVul.xls',Scaled_final,'Sheet1','A2');
xlswrite('LocationalVul.xls',Scaled_final_col,'Sheet1', 'A1')

xlswrite('LocationalVul.xls',Scaled_final_col,'Sheet2', 'A1')
xlswrite('LocationalVul.xls',Weights,'Sheet2', 'A2')

xlswrite('LocationalVul.xls',Scaled_final_col,'Sheet3', 'A1')
xlswrite('LocationalVul.xls',Scaled_withweightsonly,'Sheet3', 'A2')


%writematrix(Joinvalues, 'LocationalVul.xls');

%set(handles.uitable1, 'Data', valuesascell{:});
%Scaled_withweights=[(Metwt).*(A.Met-mean(A.Met))/std(A.Met), ((Hydrowt).*(A.Hydro-mean(A.Hydro))/
std(A.Hydro)),(PCwt).*(A.PC-mean(A.PC))/std(A.PC),(VCwt).*(A.VC-mean(A.VC))/std(A.VC), (POwt).*(A.
Outage-mean(A.Outage))/std(A.Outage)]

Metcombined=Scaled_withweightsonly(:,1)
Hydrocombined=Scaled_withweightsonly(:,2)
PCcombined=Scaled_withweightsonly(:,3)
VCcombined=Scaled_withweightsonly(:,4)
POcombined=Scaled_withweightsonly(:,5)

sumMet=abs(sum(Metfinal))
sumHydro=abs(sum(Hydrofinal))
sumPC=abs(sum(PCfinal))
sumVC=abs(sum(VCfinal))
sumPO=abs(sum(POfinal))
Vulnerability = (sumMet+sumHydro+sumPC+sumVC+sumPO)
A.Vulnerability=Vulnerability;
set(handles.LocationVul_static, 'String',Vulnerability);
guidata(hObject,handles);
```

```
% --- Executes on button press in Gen_pushfile.
function Gen_pushfile_Callback(hObject, eventdata, handles)
% hObject    handle to Gen_pushfile (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global GensurveyCulture;
global Genscore;
global A;

handles.Gensurvey=uigetfile('*.xls')
guidata(hObject,handles)
Genculture=handles.Gensurvey;
%Make sure the when you read your file, the chronology of the columns
%should be the same as the input
GensurveyCulture=xlsread(Genculture,'A:AD')%This will read from col A to col AD. Entire sheet
Genscore=xlsread(Genculture,'Gen', 'AD2')% Reads the 1st row and 29th col. Matlab considers the 2n
d row in excel as its 1st.
% Strength score of Gen survey
A.Genculture=Genscore; % NormalizedOutage data is assigned to A.Outage to be accessible as call fu
ncitons


% --- Executes on button press in Tech_pushfile.
function Tech_pushfile_Callback(hObject, eventdata, handles)
% hObject    handle to Tech_pushfile (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global TechsurveyCulture;
global Techscore;
global Subscore;
global Subculture;
global A;

handles.Techsurvey=uigetfile('*.xls')
guidata(hObject,handles)
Techculture=handles.Techsurvey;
%Make sure the when you read your file, the chronology of the columns
%should be the same as the input
TechsurveyCulture=xlsread(Techculture,'A:AK')%This will read from col A to col AD. Entire sheet
Subculture=xlsread(Techculture,'Sheet2','A:V')

Techscore=xlsread(Techculture,'Sheet1','AK2')%This will read from col A to col AD. Entire sheet
Subscore=xlsread(Techculture,'Sheet2','C30')
%TechsurveyCulture(1,36)% Reads the 1st row and 29th col. Matlab considers the 2nd row in excel as
 its 1st. Strength score
%Subculture(30,2) % Strength score of Subculture
A.Techculture=Techscore; % NormalizedOutage data is assigned to A.Outage to be accessible as call
funcitons
A.Subculture=Subscore;

% --- Executes on button press in Culture_push.
function Culture_push_Callback(hObject, eventdata, handles)
% hObject    handle to Culture_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
global Genculture;

% This is an interesting discovery, turns out there is no syntax for
% min(array,array,array) so you have to use two mins and keep it to two
% dimensional.
global minculture_score
minculture_score=round(min(min(A.Genculture, A.Techculture), A.Subculture),3);
A.CultureVul=minculture_score;
set(handles.culture_static,'String',minculture_score);


% --- Executes on button press in PFRIreturn_push.
function PFRIreturn_push_Callback(hObject, eventdata, handles)
% hObject    handle to PFRIreturn_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

My_PFRI_1;
```


Vul_gui
WHAT ARE MY VULNERABILITIES?
Facility-Locational indicators
County Natural hazard data
Load file
County neighborhood crime stats
Load file
Regional power outage stats
Load file
Calculate Facility Locational Vulnerability
Facility - Nuclear Security Culture
General nuclear security survey response
Load file
Technical nuclear security survey response
Load file
Calculate Facility Nuclear Security Culture Value
Return to PFRI page

Published with MATLAB® R2019b

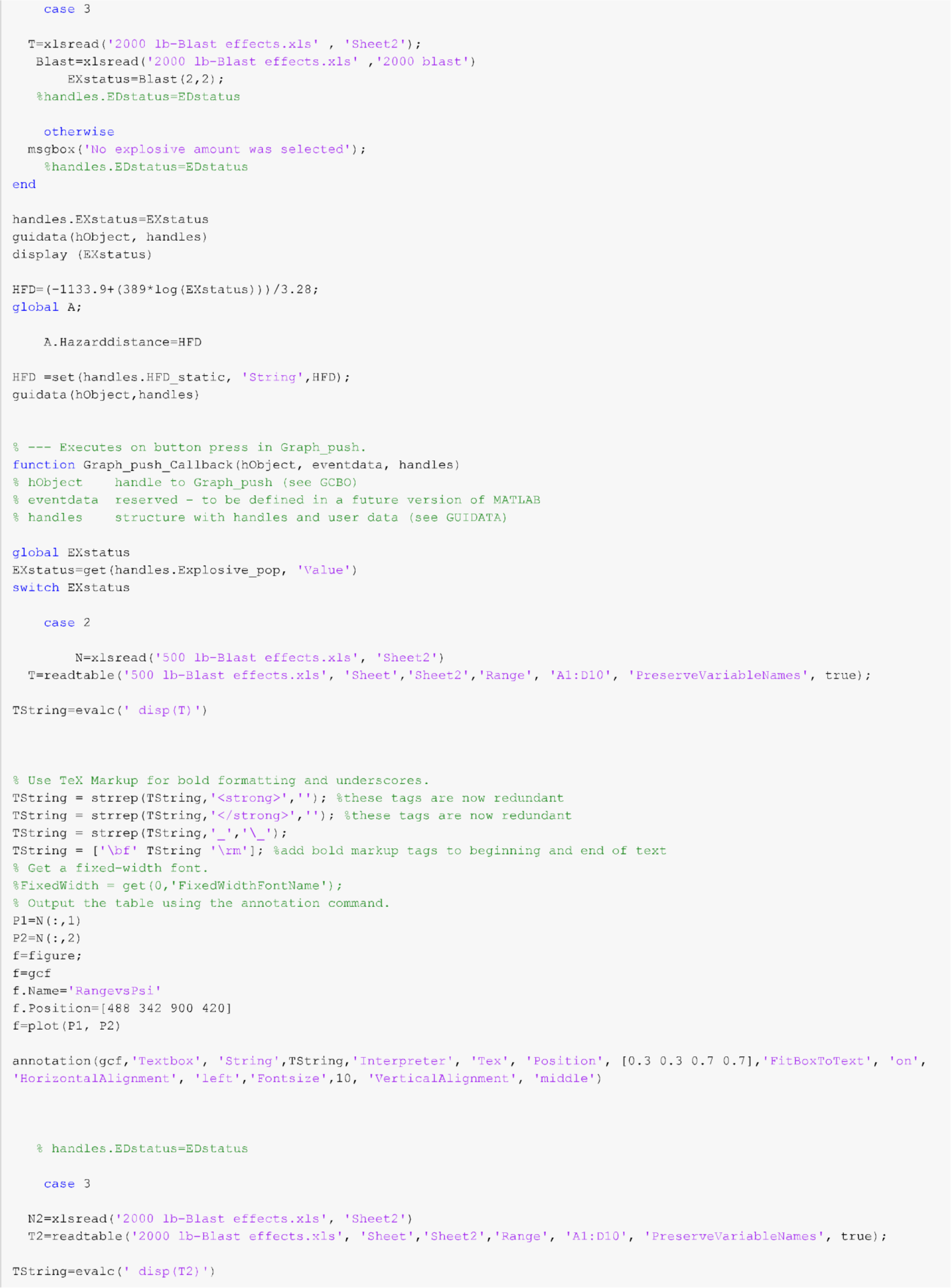
CONSEQUENCES – Blast.gui



```
function varargout = Blast_gui(varargin)
% BLAST_GUI MATLAB code for Blast_gui.fig
%      BLAST_GUI, by itself, creates a new BLAST_GUI or raises the existing
%      singleton*.
%
%      H = BLAST_GUI returns the handle to a new BLAST_GUI or the handle to
%      the existing singleton*.
%
%      BLAST_GUI('CALLBACK',hObject,eventData,handles,...) calls the local
%      function named CALLBACK in BLAST_GUI.M with the given input arguments.
%
%      BLAST_GUI('Property','Value',...) creates a new BLAST_GUI or raises the
%      existing singleton*.  Starting from the left, property value pairs are
%      applied to the GUI before Blast_gui_OpeningFcn gets called.  An
%      unrecognized property name or invalid value makes property application
%      stop.  All inputs are passed to Blast_gui_OpeningFcn via varargin.
%
%      *See GUI Options on GUIDE's Tools menu.  Choose "GUI allows only one
%      instance to run (singleton)".
%
% See also: GUIDE, GUIDATA, GUIHANDLES

% Edit the above text to modify the response to help Blast_gui

% Last Modified by GUIDE v2.5 26-Mar-2020 15:31:21

% Begin initialization code - DO NOT EDIT
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @Blast_gui_OpeningFcn, ...
                   'gui_OutputFcn',  @Blast_gui_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end
% End initialization code - DO NOT EDIT


% --- Executes just before Blast_gui is made visible.
function Blast_gui_OpeningFcn(hObject, ~, handles, varargin)
% This function has no output args, see OutputFcn.
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% varargin   command line arguments to Blast_gui (see VARARGIN)

% Choose default command line output for Blast_gui
handles.output = hObject;

% Update handles structure
guidata(hObject, handles);

% UIWAIT makes Blast_gui wait for user response (see UIRESUME)
% uiwait(handles.figure1);


% --- Outputs from this function are returned to the command line.
function varargout = Blast_gui_OutputFcn(~, ~, handles)
% varargout  cell array for returning output args (see VARARGOUT);
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% Get default command line output from handles structure
varargout{1} = handles.output;


% --- Executes on button press in BIcheckbox.





% --- Executes on selection change in Explosive_pop.
function Explosive_pop_Callback(hObject, ~, handles)
% hObject    handle to Explosive_pop (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: contents = cellstr(get(hObject,'String')) returns Explosive_pop contents as cell array
%        contents{get(hObject,'Value')} returns selected item from Explosive_pop


global EXstatus;

EXstatus=get(hObject, 'Value')

guidata(hObject,handles)
% --- Executes during object creation, after setting all properties.
function Explosive_pop_CreateFcn(hObject, ~, ~)
% hObject    handle to Explosive_pop (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: popupmenu controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end





% --- Executes on button press in Ir_check.
function Ir_check_Callback(hObject, eventdata, handles)
% hObject    handle to Ir_check (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hint: get(hObject,'Value') returns toggle state of Ir_check
global Irstatus;
Irstatus=get(hObject, 'Value');
%display(checkboxStatus)
if Irstatus == 1
    Irstatus=4;
    set(handles.Cs_check, 'Enable', 'off')
    set(handles.Co_check, 'Enable', 'off')
    IrConseq_gui;
    display(Irstatus)
else
        msgbox('Please check a box')
end
guidata(hObject,handles)

% --- Executes on button press in Co_check.
function Co_check_Callback(hObject, ~, handles)
% hObject    handle to Co_check (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hint: get(hObject,'Value') returns toggle state of Co_check
global Costatus;
Costatus=get(hObject, 'Value')
%display(checkboxStatus)
if Costatus == 1
```

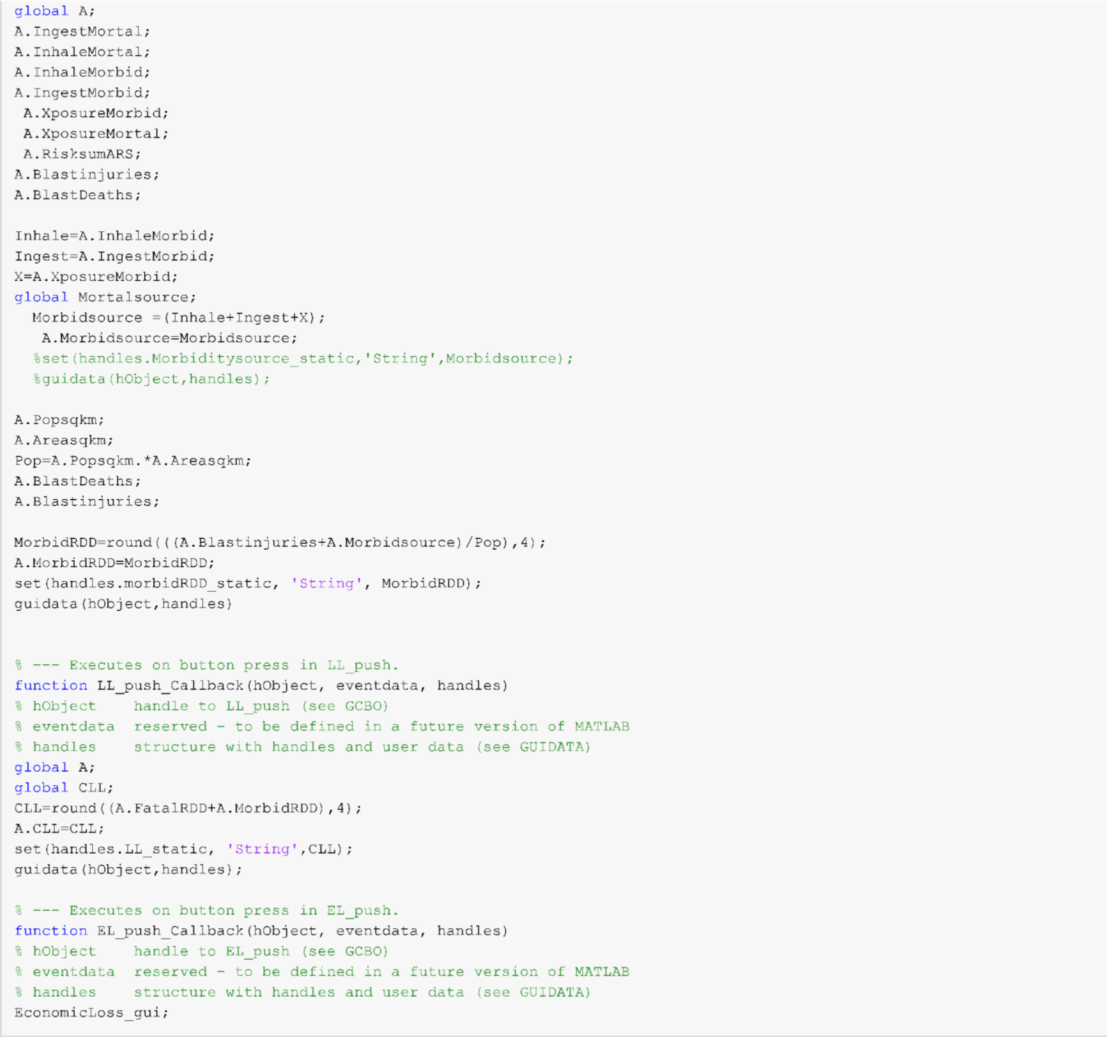
```
    Costatus=3;
    set(handles.Cs_check, 'Enable', 'off')
    set(handles.Ir_check, 'Enable', 'off')
    CoConseq_gui;
    display(Costatus)
else
        msgbox('Please check a box')
end


guidata(hObject,handles)

% --- Executes on button press in Cs_check.
function Cs_check_Callback(hObject, eventdata, handles)
% hObject    handle to Cs_check (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hint: get(hObject,'Value') returns toggle state of Cs_check
handles.output=hObject;
global Csstatus;
global user_activity;
Csstatus=get(hObject, 'Value')
%display(checkboxStatus)
if Csstatus == 1
    Csstatus=2;
    set(handles.Co_check, 'Enable', 'off')
    set(handles.Ir_check, 'Enable', 'off')
    CsConseq_gui;
   % (BI_gui);
   display(Csstatus)

else
        msgbox('Please check a box')
end
guidata(hObject,handles)


% --- Executes on button press in Injury_push.
function Injury_push_Callback(hObject, eventdata, handles)
% hObject    handle to Injury_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global EXstatus
EXstatus=get(handles.Explosive_pop, 'Value')
switch EXstatus
    case 2
  Fragment=xlsread('500 lb-Blast effects.xls', 'Frag');


    EXstatus=Fragment(1,26);

   % handles.EDstatus=EDstatus

    case 3

  Fragment=xlsread('2000 lb-Blast effects.xls'  , 'Frag');
          EXstatus=Fragment(1,26);
   %handles.EDstatus=EDstatus

    otherwise
  msgbox('No explosive amount was selected');
    %handles.EDstatus=EDstatus
end

handles.EXstatus=EXstatus
guidata(hObject, handles)


global Injury
global A;
```

```
    A.Blastinjuries=EXstatus

Injury =set(handles.injury_static, 'String',EXstatus);
guidata(hObject,handles)


%-------------------FATALITIES-----------------------------


% --- Executes on button press in Death_push.
function Death_push_Callback(hObject, eventdata, handles)
% hObject    handle to Death_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)


global EXstatus
EXstatus=get(handles.Explosive_pop, 'Value')
switch EXstatus
    case 2
  Fragment=xlsread('500 lb-Blast effects.xls', 'Frag');


    EXstatus=Fragment(1,19);

   % handles.EDstatus=EDstatus

    case 3

  Fragment=xlsread('2000 lb-Blast effects.xls'  , 'Frag');
          EXstatus=Fragment(1,19);
   %handles.EDstatus=EDstatus

    otherwise
  msgbox('No explosive amount was selected');
    %handles.EDstatus=EDstatus
end

handles.EXstatus=EXstatus
guidata(hObject, handles)


global Death
global A;

    A.BlastDeaths=EXstatus

Death =set(handles.death_static, 'String',EXstatus);
guidata(hObject,handles)




%----------------------------------Hazard FunctionDistance---------------------------
%Executes on button press in HFD_push.
function HFD_push_Callback(hObject, eventdata, handles)
% hObject    handle to HFD_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)


global EXstatus
EXstatus=get(handles.Explosive_pop, 'Value')
switch EXstatus
    case 2
  T=xlsread('500 lb-Blast effects.xls', 'Sheet2');
  Blast=xlsread('500 lb-Blast effects.xls','500 blast')

    EXstatus=Blast(2,2);

   % handles.EDstatus=EDstatus
```

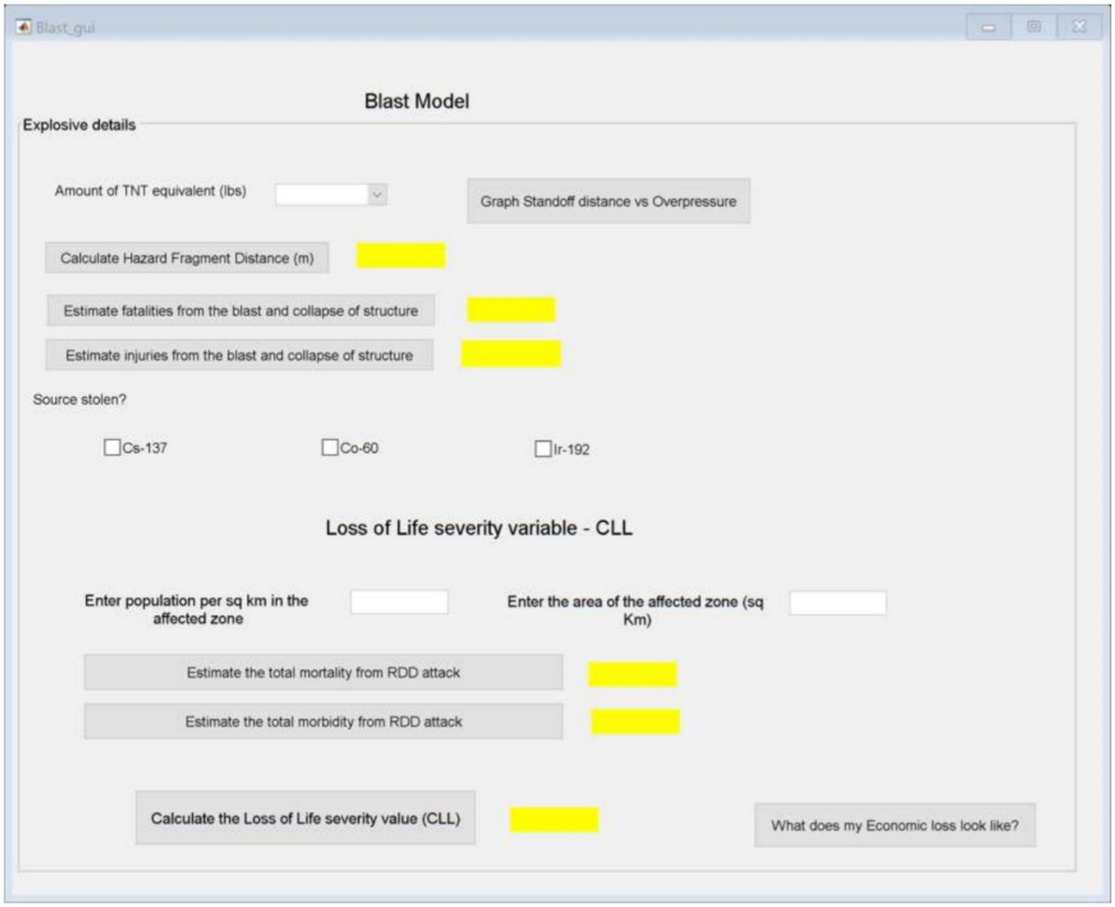


```
    case 3

  T=xlsread('2000 lb-Blast effects.xls' , 'Sheet2');
   Blast=xlsread('2000 lb-Blast effects.xls' ,'2000 blast')
       EXstatus=Blast(2,2);
   %handles.EDstatus=EDstatus

    otherwise
  msgbox('No explosive amount was selected');
    %handles.EDstatus=EDstatus
end

handles.EXstatus=EXstatus
guidata(hObject, handles)
display (EXstatus)

HFD=(-1133.9+(389*log(EXstatus)))/3.28;
global A;

    A.Hazarddistance=HFD

HFD =set(handles.HFD_static, 'String',HFD);
guidata(hObject,handles)


% --- Executes on button press in Graph_push.
function Graph_push_Callback(hObject, eventdata, handles)
% hObject    handle to Graph_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global EXstatus
EXstatus=get(handles.Explosive_pop, 'Value')
switch EXstatus

    case 2

        N=xlsread('500 lb-Blast effects.xls', 'Sheet2')
  T=readtable('500 lb-Blast effects.xls', 'Sheet','Sheet2','Range', 'A1:D10', 'PreserveVariableNames', true);

TString=evalc(' disp(T)')



% Use TeX Markup for bold formatting and underscores.
TString = strrep(TString,'<strong>',''); %these tags are now redundant
TString = strrep(TString,'</strong>',''); %these tags are now redundant
TString = strrep(TString,'_','\_');
TString = ['\bf' TString '\rm']; %add bold markup tags to beginning and end of text
% Get a fixed-width font.
%FixedWidth = get(0,'FixedWidthFontName');
% Output the table using the annotation command.
P1=N(:,1)
P2=N(:,2)
f=figure;
f=gcf
f.Name='RangevsPsi'
f.Position=[488 342 900 420]
f=plot(P1, P2)

annotation(gcf,'Textbox', 'String',TString,'Interpreter', 'Tex', 'Position', [0.3 0.3 0.7 0.7],'FitBoxToText', 'on',
'HorizontalAlignment', 'left','Fontsize',10, 'VerticalAlignment', 'middle')



   % handles.EDstatus=EDstatus

    case 3

  N2=xlsread('2000 lb-Blast effects.xls', 'Sheet2')
  T2=readtable('2000 lb-Blast effects.xls', 'Sheet','Sheet2','Range', 'A1:D10', 'PreserveVariableNames', true);

TString=evalc(' disp(T2)')
```

```
% Use TeX Markup for bold formatting and underscores.
TString = strrep(TString,'<strong>',''); %these tags are now redundant
TString = strrep(TString,'</strong>',''); %these tags are now redundant
TString = strrep(TString,'_','\_');
TString = ['\bf' TString '\rm']; %add bold markup tags to beginning and end of text
% Get a fixed-width font.
%FixedWidth = get(0,'FixedWidthFontName');
% Output the table using the annotation command.
P1=N2(:,1)
P2=N2(:,2)
f=figure;
f=gcf
f.Name='RangevsPsifor 2000 lb bomb'
f.Position=[488 342 900 420]
f=plot(P1, P2)

annotation(gcf,'Textbox', 'String',TString,'Interpreter', 'Tex', 'Position', [0.3 0.3 0.7 0.7],'FitBoxToText', 'on',
'HorizontalAlignment', 'left','Fontsize',10, 'VerticalAlignment', 'middle')

   %handles.EDstatus=EDstatus

    otherwise
  msgbox('No explosive amount was selected');
    %handles.EDstatus=EDstatus
end

handles.EXstatus=EXstatus
guidata(hObject, handles)
display (EXstatus)

guidata(hObject,handles)



function Popsqkm_edit_Callback(hObject, eventdata, handles)
% hObject    handle to Popsqkm_edit (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: get(hObject,'String') returns contents of Popsqkm_edit as text
%        str2double(get(hObject,'String')) returns contents of Popsqkm_edit as a double
handles.output=hObject
global Popsqkm;
global A;
Popsqkm=str2double(get(hObject, 'String'));
if isempty(Popsqkm)
    errordlg('Please enter a valid number')
else
A.Popsqkm=Popsqkm;

end
guidata(hObject,handles)

% --- Executes during object creation, after setting all properties.
function Popsqkm_edit_CreateFcn(hObject, eventdata, handles)
% hObject    handle to Popsqkm_edit (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: edit controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end



function Areasqkm_edit_Callback(hObject, eventdata, handles)
% hObject    handle to Areasqkm_edit (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: get(hObject,'String') returns contents of Areasqkm_edit as text
%        str2double(get(hObject,'String')) returns contents of Areasqkm_edit as a double

handles.output=hObject
global Areasqkm;
global A;
Areasqkm=str2double(get(hObject, 'String'));
if isempty(Areasqkm)
    errordlg('Please enter a valid number')
else
A.Areasqkm = Areasqkm;

end
guidata(hObject,handles);
% --- Executes during object creation, after setting all properties.
function Areasqkm_edit_CreateFcn(hObject, eventdata, handles)
% hObject    handle to Areasqkm_edit (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: edit controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end


% --- Executes on button press in fatalitiesRDD_push.
function fatalitiesRDD_push_Callback(hObject, eventdata, handles)
% hObject    handle to fatalitiesRDD_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global A;
A.IngestMortal;
A.InhaleMortal;
A.InhaleMorbid;
A.IngestMorbid;
 A.XposureMorbid;
 A.XposureMortal;
 A.RisksumARS;
A.Blastinjuries;
A.BlastDeaths;

Inhale=A.InhaleMortal
Ingest=A.IngestMortal
X=A.XposureMortal
global Mortalsource;
  Mortalsource =(Inhale+Ingest+X);
  display(Mortalsource)
  A.Mortalsource=Mortalsource;
  %set(handles.Fatalitiessource_static,'String',Mortalsource);

A.Popsqkm;
A.Areasqkm;
Pop=A.Popsqkm.*A.Areasqkm;
A.BlastDeaths;
A.Blastinjuries;

FatalRDD=round(((A.BlastDeaths+A.Mortalsource)/Pop),4);
A.FatalRDD=FatalRDD;
set(handles.fatalitiesRDD_static, 'String', FatalRDD);
guidata(hObject,handles);


% --- Executes on button press in MorbidRDD_push.
function MorbidRDD_push_Callback(hObject, eventdata, handles)
% hObject    handle to MorbidRDD_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
```

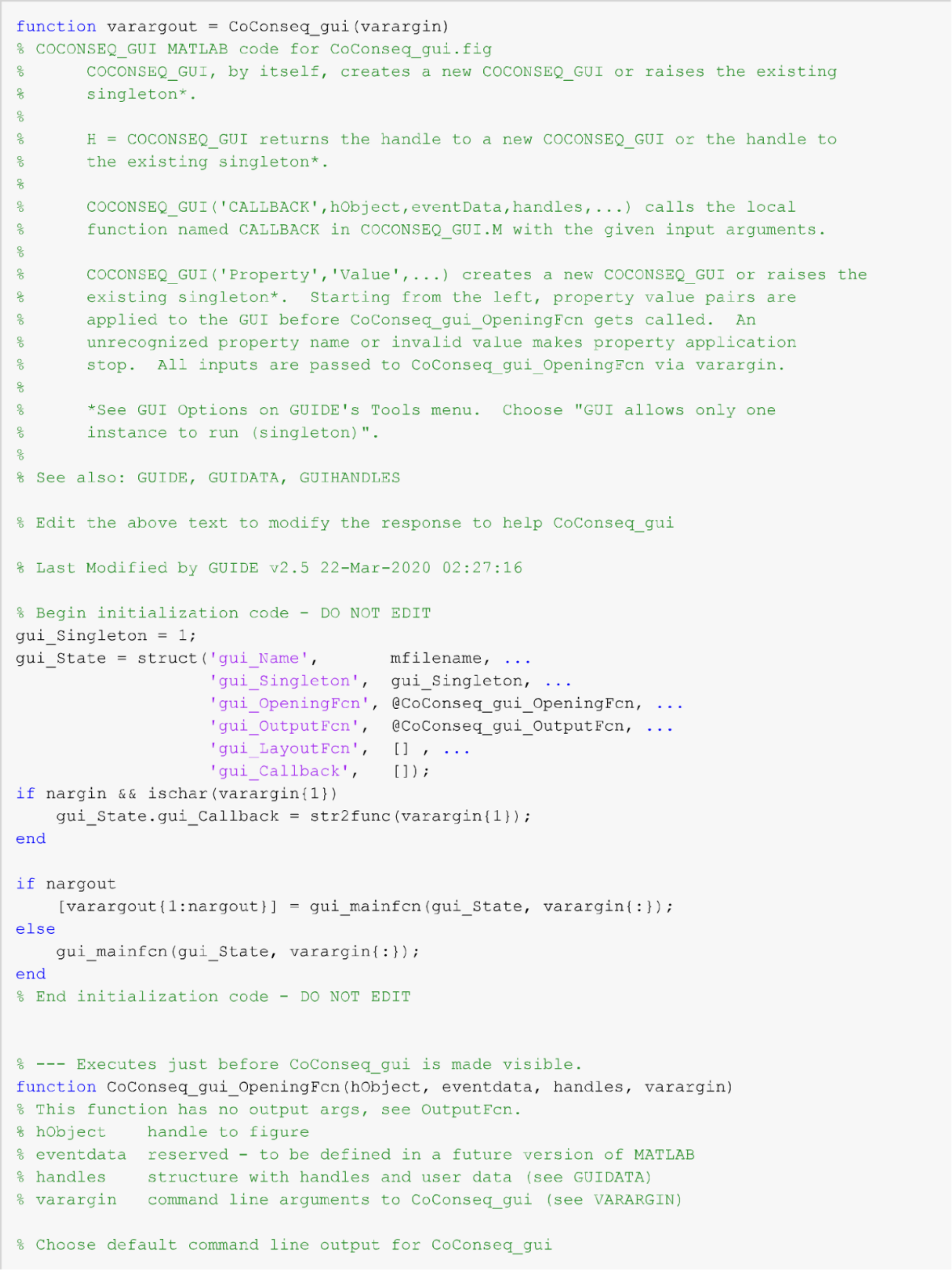


```
global A;
A.IngestMortal;
A.InhaleMortal;
A.InhaleMorbid;
A.IngestMorbid;
 A.XposureMorbid;
 A.XposureMortal;
 A.RisksumARS;
A.Blastinjuries;
A.BlastDeaths;

Inhale=A.InhaleMorbid;
Ingest=A.IngestMorbid;
X=A.XposureMorbid;
global Mortalsource;
  Morbidsource =(Inhale+Ingest+X);
   A.Morbidsource=Morbidsource;
  %set(handles.Morbiditysource_static,'String',Morbidsource);
  %guidata(hObject,handles);

A.Popsqkm;
A.Areasqkm;
Pop=A.Popsqkm.*A.Areasqkm;
A.BlastDeaths;
A.Blastinjuries;

MorbidRDD=round(((A.Blastinjuries+A.Morbidsource)/Pop),4);
A.MorbidRDD=MorbidRDD;
set(handles.morbidRDD_static, 'String', MorbidRDD);
guidata(hObject,handles)


% --- Executes on button press in LL_push.
function LL_push_Callback(hObject, eventdata, handles)
% hObject    handle to LL_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
global CLL;
CLL=round((A.FatalRDD+A.MorbidRDD),4);
A.CLL=CLL;
set(handles.LL_static, 'String',CLL);
guidata(hObject,handles);

% --- Executes on button press in EL_push.
function EL_push_Callback(hObject, eventdata, handles)
% hObject    handle to EL_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
EconomicLoss_gui;
```


Blast_gui
Blast Model
Explosive details
Amount of TNT equivalent (lbs)
Graph Standoff distance vs Overpressure
Calculate Hazard Fragment Distance (m)
Estimate fatalities from the blast and collapse of structure
Estimate injuries from the blast and collapse of structure
Source stolen?
□ Cs-137
□ Co-60
□ Ir-192
Loss of Life severity variable - CLL
Enter population per sq km in the affected zone
Enter the area of the affected zone (sq Km)
Estimate the total mortality from RDD attack
Estimate the total morbidity from RDD attack
Calculate the Loss of Life severity value (CLL)
What does my Economic loss look like?

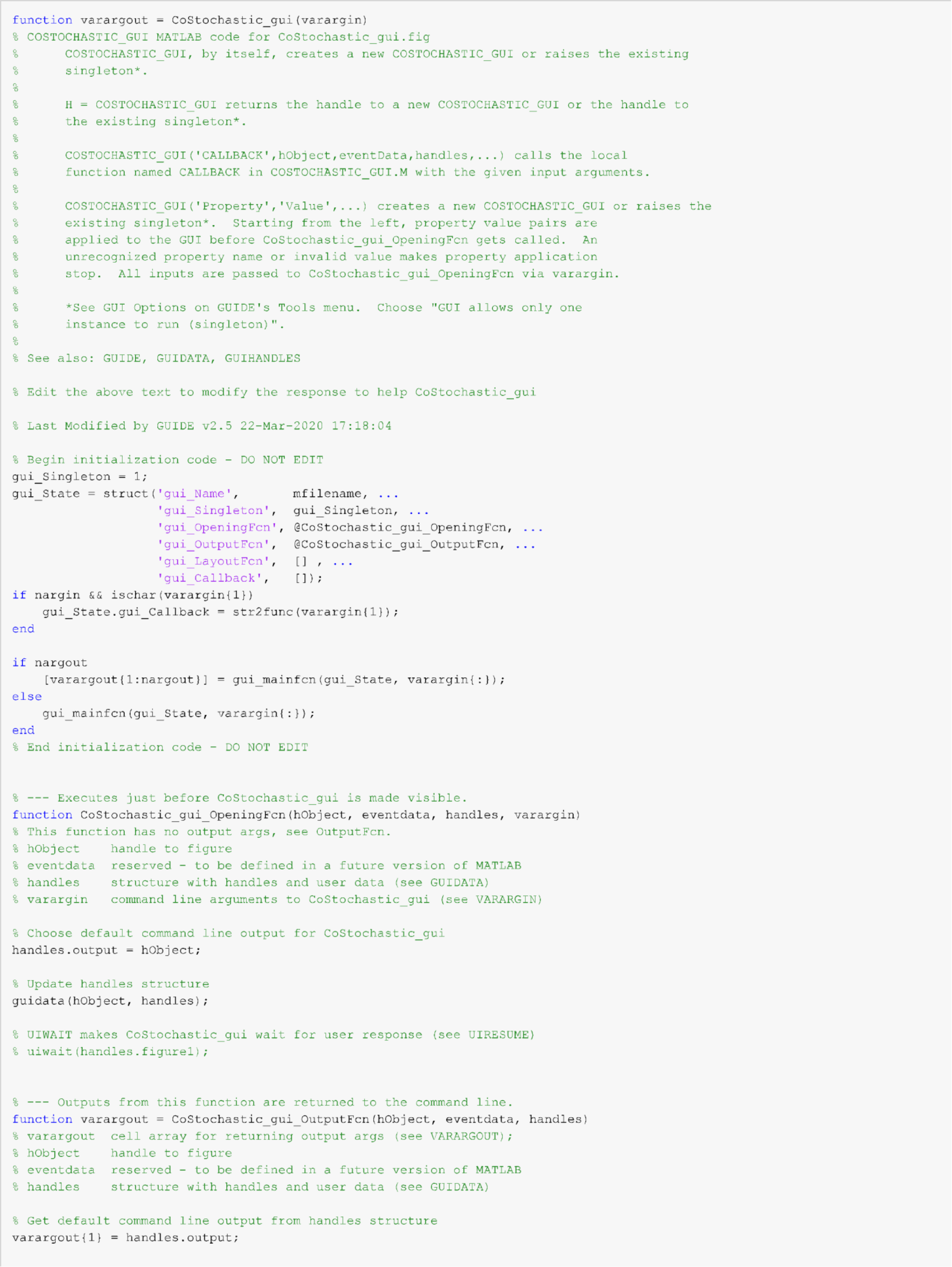
Published with MATLAB® R2019b

Consequences – DETERMISTIC EFFECTS



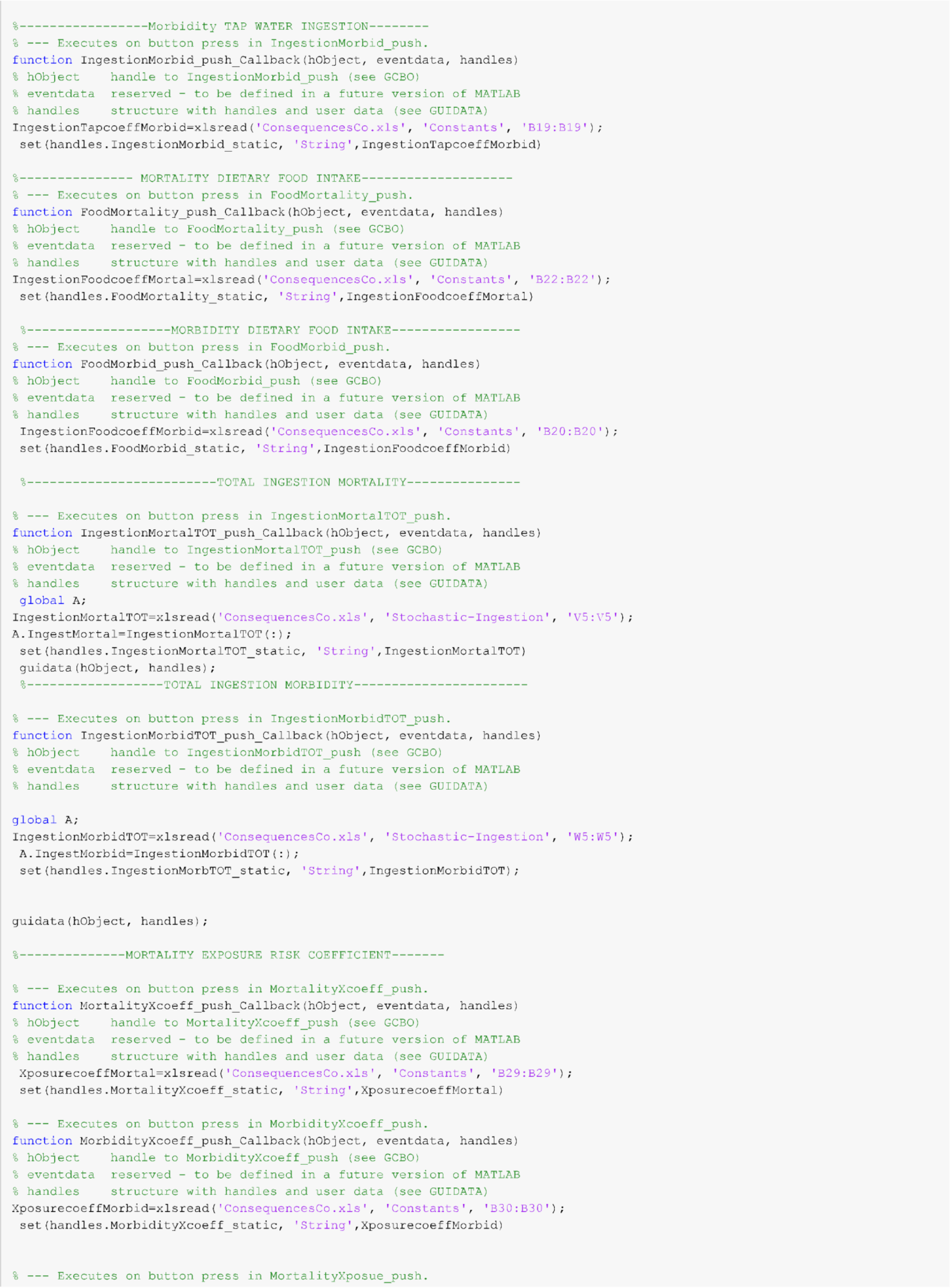
```
function varargout = CoConseq_gui(varargin)
% COCONSEQ_GUI MATLAB code for CoConseq_gui.fig
%      COCONSEQ_GUI, by itself, creates a new COCONSEQ_GUI or raises the existing
%      singleton*.
%
%      H = COCONSEQ_GUI returns the handle to a new COCONSEQ_GUI or the handle to
%      the existing singleton*.
%
%      COCONSEQ_GUI('CALLBACK',hObject,eventData,handles,...) calls the local
%      function named CALLBACK in COCONSEQ_GUI.M with the given input arguments.
%
%      COCONSEQ_GUI('Property','Value',...) creates a new COCONSEQ_GUI or raises the
%      existing singleton*.  Starting from the left, property value pairs are
%      applied to the GUI before CoConseq_gui_OpeningFcn gets called.  An
%      unrecognized property name or invalid value makes property application
%      stop.  All inputs are passed to CoConseq_gui_OpeningFcn via varargin.
%
%      *See GUI Options on GUIDE's Tools menu.  Choose "GUI allows only one
%      instance to run (singleton)".
%
% See also: GUIDE, GUIDATA, GUIHANDLES

% Edit the above text to modify the response to help CoConseq_gui

% Last Modified by GUIDE v2.5 22-Mar-2020 02:27:16

% Begin initialization code - DO NOT EDIT
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @CoConseq_gui_OpeningFcn, ...
                   'gui_OutputFcn',  @CoConseq_gui_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end
% End initialization code - DO NOT EDIT


% --- Executes just before CoConseq_gui is made visible.
function CoConseq_gui_OpeningFcn(hObject, eventdata, handles, varargin)
% This function has no output args, see OutputFcn.
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% varargin   command line arguments to CoConseq_gui (see VARARGIN)

% Choose default command line output for CoConseq_gui
```

```
handles.output = hObject;

% Update handles structure
guidata(hObject, handles);
global user_activity;
% UIWAIT makes CoConseq_gui wait for user response (see UIRESUME)
% uiwait(handles.figure1);


% --- Outputs from this function are returned to the command line.
function varargout = CoConseq_gui_OutputFcn(hObject, eventdata, handles)
% varargout  cell array for returning output args (see VARARGOUT);
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Get default command line output from handles structure
varargout{1} = handles.output;


% --- Executes on button press in stochastic_push.
function stochastic_push_Callback(hObject, eventdata, handles)
% hObject    handle to stochastic_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
CoStochastic_gui;


% --- Executes on button press in fragexposure_push.
function fragexposure_push_Callback(hObject, eventdata, handles)
% hObject    handle to fragexposure_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
ExposureFragment=xlsread('ConsequencesCo.xls', 'ARS-Fragment', 'G5:G5');
 set(handles.fragexposure_static, 'String',ExposureFragment)


% --- Executes on button press in deathArs_push.
function deathArs_push_Callback(hObject, eventdata, handles)
% hObject    handle to deathArs_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
riskfragment=xlsread('ConsequencesCo.xls', 'ARS-Fragment', 'I5:I5');
riskIngestARS=xlsread('ConsequencesCo.xls', 'ARS ingestion', 'Z2:Z2');
RisksumARS=riskfragment+riskIngestARS;
set(handles.deathars_static, 'String', RisksumARS);
  global A;
 A.RisksumARS=RisksumARS;
 guidata(hObject, handles);


% --- Executes on button press in SEE_push.
function SEE_push_Callback(hObject, eventdata, handles)
% hObject    handle to SEE_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
 EffectiveEnergy=xlsread('ConsequencesCo.xls', 'Constants', 'B2:B2');
 set(handles.SEE_static, 'String',EffectiveEnergy)

% --- Executes on button press in Effective_push.
function Effective_push_Callback(hObject, eventdata, handles)
% hObject    handle to Effective_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
Effectivelife=xlsread('ConsequencesCo.xls', 'Constants', 'B4:B4');
 set(handles.Effective_static, 'String',Effectivelife)

% --- Executes on button press in Gammaconstant_push.
function Gammaconstant_push_Callback(hObject, eventdata, handles)
% hObject    handle to Gammaconstant_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
Gammaconst=xlsread('ConsequencesCo.xls', 'Constants', 'B3:B3');
 set(handles.gamma_static, 'String',Gammaconst)

% --- Executes on button press in inhal_push.
function inhal_push_Callback(hObject, eventdata, handles)
% hObject    handle to inhal_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
InhalationALI=xlsread('ConsequencesCo.xls', 'Constants', 'B5:B5');
 set(handles.inhale_static, 'String',InhalationALI)

% --- Executes on button press in ingest_push.
function ingest_push_Callback(hObject, eventdata, handles)
% hObject    handle to ingest_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
IngestionALI=xlsread('ConsequencesCo.xls', 'Constants', 'B6:B6');
 set(handles.ingest_static, 'String',IngestionALI)


% --- Executes on button press in ARSIngest_pushc.
function ARSIngest_pushc_Callback(hObject, eventdata, handles)
% hObject    handle to ARSIngest_pushc (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
IngestionARS=xlsread('ConsequencesCo.xls', 'ARS ingestion', 'R1:R28');
Maxdose=max(IngestionARS(:))
 set(handles.ARSingestion_static, 'String',Maxdose)
```

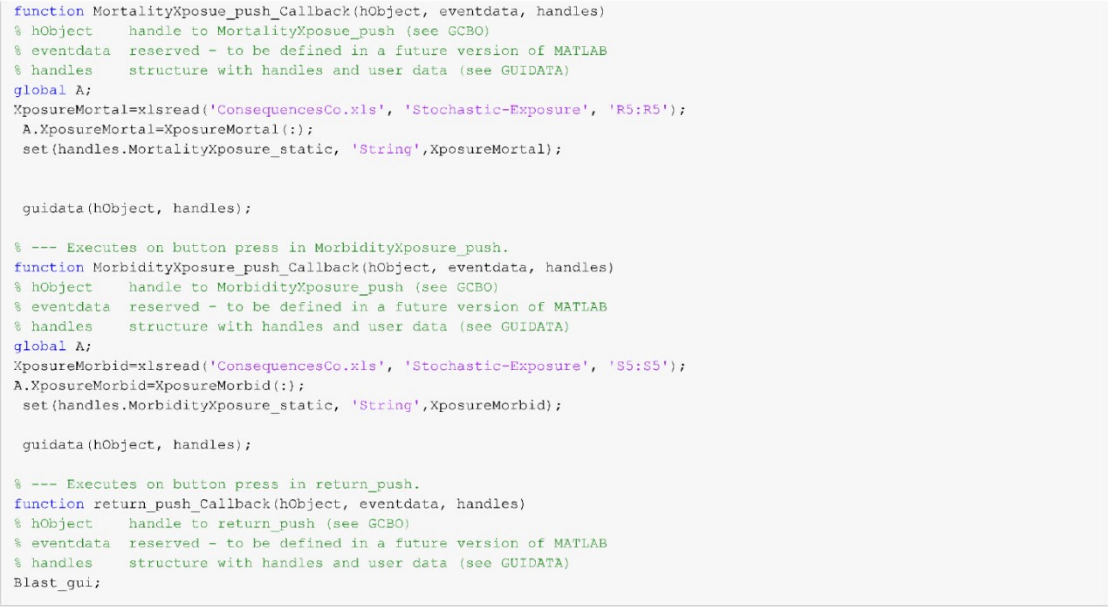


```
function varargout = CoStochastic_gui(varargin)
% COSTOCHASTIC_GUI MATLAB code for CoStochastic_gui.fig
%      COSTOCHASTIC_GUI, by itself, creates a new COSTOCHASTIC_GUI or raises the existing
%      singleton*.
%
%      H = COSTOCHASTIC_GUI returns the handle to a new COSTOCHASTIC_GUI or the handle to
%      the existing singleton*.
%
%      COSTOCHASTIC_GUI('CALLBACK',hObject,eventData,handles,...) calls the local
%      function named CALLBACK in COSTOCHASTIC_GUI.M with the given input arguments.
%
%      COSTOCHASTIC_GUI('Property','Value',...) creates a new COSTOCHASTIC_GUI or raises the
%      existing singleton*.  Starting from the left, property value pairs are
%      applied to the GUI before CoStochastic_gui_OpeningFcn gets called.  An
%      unrecognized property name or invalid value makes property application
%      stop.  All inputs are passed to CoStochastic_gui_OpeningFcn via varargin.
%
%      *See GUI Options on GUIDE's Tools menu.  Choose "GUI allows only one
%      instance to run (singleton)".
%
% See also: GUIDE, GUIDATA, GUIHANDLES

% Edit the above text to modify the response to help CoStochastic_gui

% Last Modified by GUIDE v2.5 22-Mar-2020 17:18:04

% Begin initialization code - DO NOT EDIT
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @CoStochastic_gui_OpeningFcn, ...
                   'gui_OutputFcn',  @CoStochastic_gui_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end
% End initialization code - DO NOT EDIT


% --- Executes just before CoStochastic_gui is made visible.
function CoStochastic_gui_OpeningFcn(hObject, eventdata, handles, varargin)
% This function has no output args, see OutputFcn.
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% varargin   command line arguments to CoStochastic_gui (see VARARGIN)

% Choose default command line output for CoStochastic_gui
handles.output = hObject;

% Update handles structure
guidata(hObject, handles);

% UIWAIT makes CoStochastic_gui wait for user response (see UIRESUME)
% uiwait(handles.figure1);


% --- Outputs from this function are returned to the command line.
function varargout = CoStochastic_gui_OutputFcn(hObject, eventdata, handles)
% varargout  cell array for returning output args (see VARARGOUT);
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Get default command line output from handles structure
varargout{1} = handles.output;
```

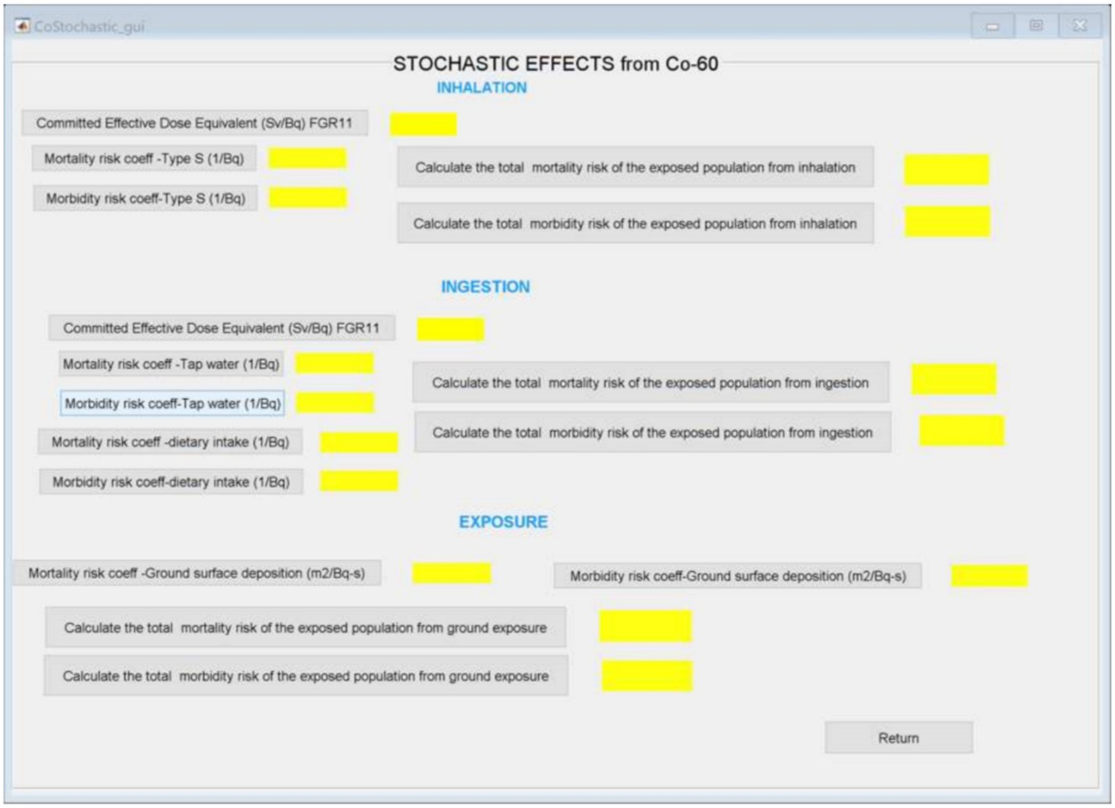
```
%-----------------------CEDE INHALATION-------------

% --- Executes on button press in CEDEInhalation_push.
function CEDEInhalation_push_Callback(hObject, eventdata, handles)
% hObject    handle to CEDEInhalation_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
 InhalationCEDE=xlsread('ConsequencesCo.xls', 'Constants', 'B15:B15');
 set(handles.CEDEinhalation_static, 'String',InhalationCEDE)

%---------------------------------MORTALITY COEFF INHALATION------
% --- Executes on button press in deathInhalation_push.
function deathInhalation_push_Callback(hObject, eventdata, handles)
% hObject    handle to deathInhalation_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
MortalInhalationcoeff=xlsread('ConsequencesCo.xls', 'Constants', 'B25:B25');
 set(handles.deathInhalation_static, 'String',MortalInhalationcoeff)

%------------------------------MORBIDITY COEFF INHALATION----------

% --- Executes on button press in Morbiditycoeffinhale_push.
function Morbiditycoeffinhale_push_Callback(hObject, eventdata, handles)
% hObject    handle to Morbiditycoeffinhale_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
MorbidInhalationcoeff=xlsread('ConsequencesCo.xls', 'Constants', 'B26:B26');
 set(handles.Morbidcoeffinhale_static, 'String',MorbidInhalationcoeff)


 %-----------------------MORBIDITY TOTAL INHALATION-------------

% --- Executes on button press in InhalationMorbidTOT_push.
function InhalationMorbidTOT_push_Callback(hObject, eventdata, handles)
% hObject    handle to InhalationMorbidTOT_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
InhalationMorbidTOT=xlsread('ConsequencesCo.xls', 'Stochastic-Inhalation', 'T5:T5');
%I= InhalationMorbidTOT(:)
A.InhaleMorbid=InhalationMorbidTOT(:);


 set(handles.InhalationMorbidTOT_static, 'String',InhalationMorbidTOT);
 guidata(hObject, handles);

  %-----------------------MORTALITY TOTAL INHALATION-------------

 % --- Executes on button press in InhalationMorbidTOT_push.
 function InhalationdeathTOT_push_Callback(hObject, eventdata, handles)
% hObject    handle to InhalationMorbidTOT_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
InhalationdeathTOT=xlsread('ConsequencesCo.xls', 'Stochastic-Inhalation', 'S5:S5');
A.InhaleMortal=InhalationdeathTOT(:);

 set(handles.InhalationdeathTOT_static, 'String',InhalationdeathTOT)
 guidata(hObject, handles);
 %------------------------CEDE Ingestion-----------------
% --- Executes on button press in CEDEIngestion_push.
function CEDEIngestion_push_Callback(hObject, eventdata, handles)
% hObject    handle to CEDEIngestion_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
IngestionCEDE=xlsread('ConsequencesCo.xls', 'Constants', 'B16:B16');
 set(handles.CEDEIngestion_static, 'String',IngestionCEDE)

 %---------------------MORTALITY TAP WATER INGESTION----------
% --- Executes on button press in Ingestiondeath_push.
function Ingestiondeath_push_Callback(hObject, eventdata, handles)
% hObject    handle to Ingestiondeath_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
IngestionTapcoeff=xlsread('ConsequencesCo.xls', 'Constants', 'B21:B21');
 set(handles.Ingestiondeath_static, 'String',IngestionTapcoeff)
```

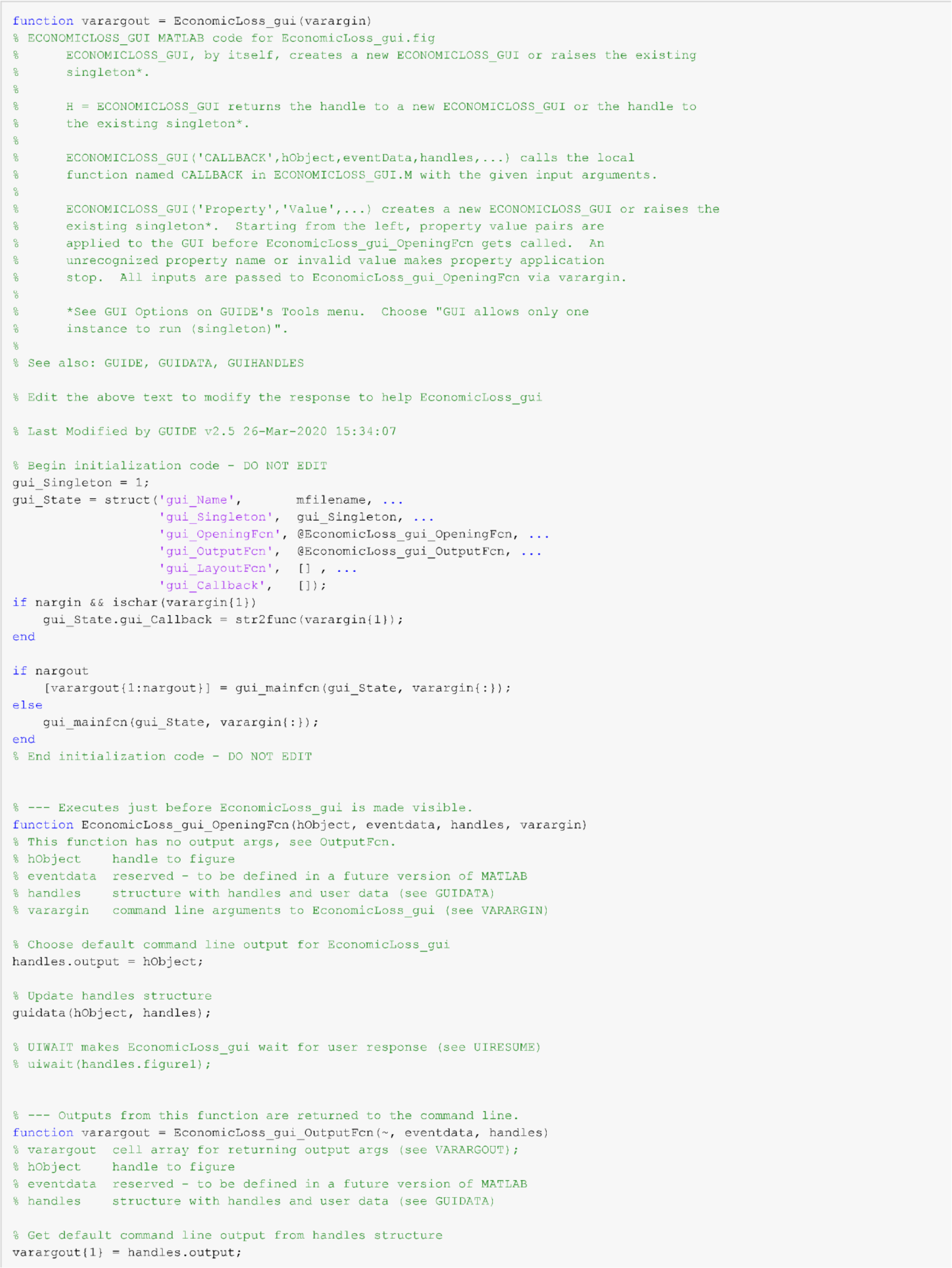


```
%-----------------Morbidity TAP WATER INGESTION--------
% --- Executes on button press in IngestionMorbid_push.
function IngestionMorbid_push_Callback(hObject, eventdata, handles)
% hObject    handle to IngestionMorbid_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
IngestionTapcoeffMorbid=xlsread('ConsequencesCo.xls', 'Constants', 'B19:B19');
 set(handles.IngestionMorbid_static, 'String',IngestionTapcoeffMorbid)

%--------------- MORTALITY DIETARY FOOD INTAKE--------------------
% --- Executes on button press in FoodMortality_push.
function FoodMortality_push_Callback(hObject, eventdata, handles)
% hObject    handle to FoodMortality_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
IngestionFoodcoeffMortal=xlsread('ConsequencesCo.xls', 'Constants', 'B22:B22');
 set(handles.FoodMortality_static, 'String',IngestionFoodcoeffMortal)

 %-------------------MORBIDITY DIETARY FOOD INTAKE-----------------
% --- Executes on button press in FoodMorbid_push.
function FoodMorbid_push_Callback(hObject, eventdata, handles)
% hObject    handle to FoodMorbid_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
 IngestionFoodcoeffMorbid=xlsread('ConsequencesCo.xls', 'Constants', 'B20:B20');
 set(handles.FoodMorbid_static, 'String',IngestionFoodcoeffMorbid)

 %-------------------------TOTAL INGESTION MORTALITY---------------

% --- Executes on button press in IngestionMortalTOT_push.
function IngestionMortalTOT_push_Callback(hObject, eventdata, handles)
% hObject    handle to IngestionMortalTOT_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
 global A;
IngestionMortalTOT=xlsread('ConsequencesCo.xls', 'Stochastic-Ingestion', 'V5:V5');
A.IngestMortal=IngestionMortalTOT(:);
 set(handles.IngestionMortalTOT_static, 'String',IngestionMortalTOT)
 guidata(hObject, handles);
 %------------------TOTAL INGESTION MORBIDITY-----------------------

% --- Executes on button press in IngestionMorbidTOT_push.
function IngestionMorbidTOT_push_Callback(hObject, eventdata, handles)
% hObject    handle to IngestionMorbidTOT_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global A;
IngestionMorbidTOT=xlsread('ConsequencesCo.xls', 'Stochastic-Ingestion', 'W5:W5');
 A.IngestMorbid=IngestionMorbidTOT(:);
 set(handles.IngestionMorbTOT_static, 'String',IngestionMorbidTOT);


guidata(hObject, handles);

%--------------MORTALITY EXPOSURE RISK COEFFICIENT-------

% --- Executes on button press in MortalityXcoeff_push.
function MortalityXcoeff_push_Callback(hObject, eventdata, handles)
% hObject    handle to MortalityXcoeff_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
 XposurecoeffMortal=xlsread('ConsequencesCo.xls', 'Constants', 'B29:B29');
 set(handles.MortalityXcoeff_static, 'String',XposurecoeffMortal)

% --- Executes on button press in MorbidityXcoeff_push.
function MorbidityXcoeff_push_Callback(hObject, eventdata, handles)
% hObject    handle to MorbidityXcoeff_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
XposurecoeffMorbid=xlsread('ConsequencesCo.xls', 'Constants', 'B30:B30');
 set(handles.MorbidityXcoeff_static, 'String',XposurecoeffMorbid)


% --- Executes on button press in MortalityXposue_push.
```

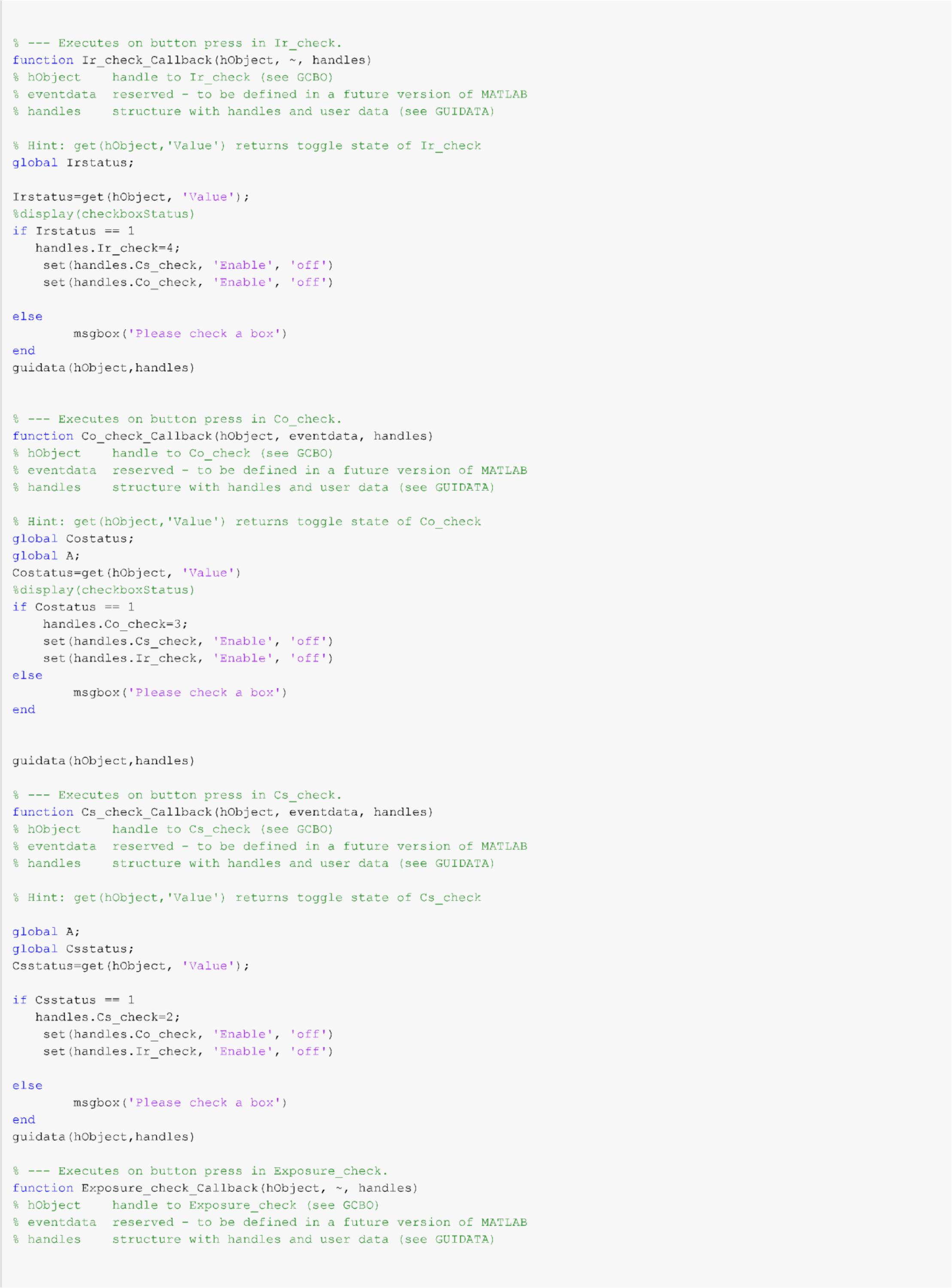


```
function MortalityXposue_push_Callback(hObject, eventdata, handles)
% hObject    handle to MortalityXposue_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
XposureMortal=xlsread('ConsequencesCo.xls', 'Stochastic-Exposure', 'R5:R5');
 A.XposureMortal=XposureMortal(:);
 set(handles.MortalityXposure_static, 'String',XposureMortal);


 guidata(hObject, handles);

% --- Executes on button press in MorbidityXposure_push.
function MorbidityXposure_push_Callback(hObject, eventdata, handles)
% hObject    handle to MorbidityXposure_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
XposureMorbid=xlsread('ConsequencesCo.xls', 'Stochastic-Exposure', 'S5:S5');
A.XposureMorbid=XposureMorbid(:);
 set(handles.MorbidityXposure_static, 'String',XposureMorbid);

 guidata(hObject, handles);

% --- Executes on button press in return_push.
function return_push_Callback(hObject, eventdata, handles)
% hObject    handle to return_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
Blast_gui;
```


CoStochastic_gui
STOCHASTIC EFFECTS from Co-60
INHALATION
Committed Effective Dose Equivalent (Sv/Bq) FGR11
Mortality risk coeff -Type S (1/Bq)
Morbidity risk coeff-Type S (1/Bq)
Calculate the total mortality risk of the exposed population from inhalation
Calculate the total morbidity risk of the exposed population from inhalation
INGESTION
Committed Effective Dose Equivalent (Sv/Bq) FGR11
Mortality risk coeff -Tap water (1/Bq)
Morbidity risk coeff-Tap water (1/Bq)
Mortality risk coeff -dietary intake (1/Bq)
Morbidity risk coeff-dietary intake (1/Bq)
Calculate the total mortality risk of the exposed population from ingestion
Calculate the total morbidity risk of the exposed population from ingestion
EXPOSURE
Mortality risk coeff -Ground surface deposition (m2/Bq-s)
Morbidity risk coeff-Ground surface deposition (m2/Bq-s)
Calculate the total mortality risk of the exposed population from ground exposure
Calculate the total morbidity risk of the exposed population from ground exposure
Return



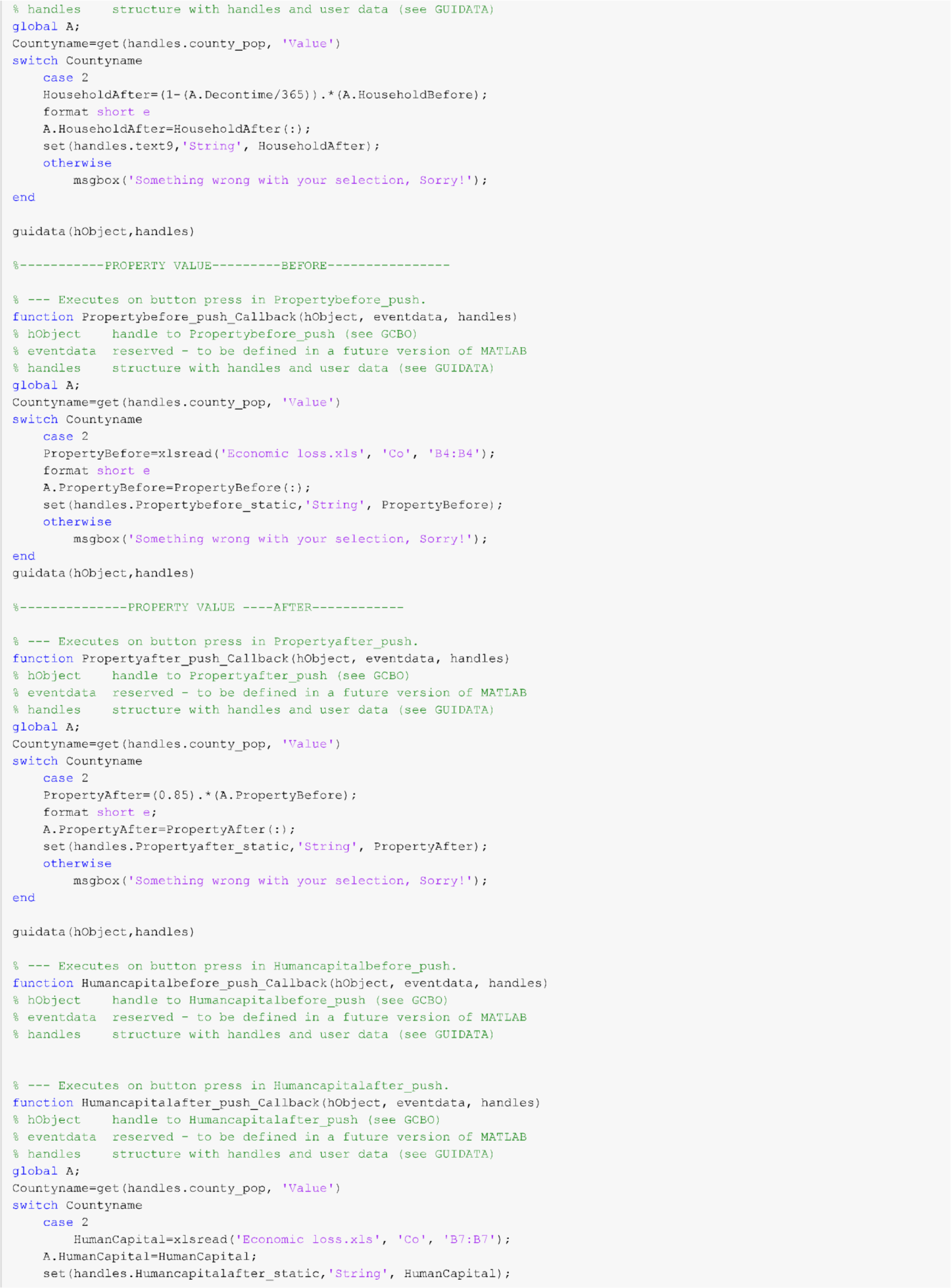
```
function varargout = EconomicLoss_gui(varargin)
% ECONOMICLOSS_GUI MATLAB code for EconomicLoss_gui.fig
%      ECONOMICLOSS_GUI, by itself, creates a new ECONOMICLOSS_GUI or raises the existing
%      singleton*.
%
%      H = ECONOMICLOSS_GUI returns the handle to a new ECONOMICLOSS_GUI or the handle to
%      the existing singleton*.
%
%      ECONOMICLOSS_GUI('CALLBACK',hObject,eventData,handles,...) calls the local
%      function named CALLBACK in ECONOMICLOSS_GUI.M with the given input arguments.
%
%      ECONOMICLOSS_GUI('Property','Value',...) creates a new ECONOMICLOSS_GUI or raises the
%      existing singleton*.  Starting from the left, property value pairs are
%      applied to the GUI before EconomicLoss_gui_OpeningFcn gets called.  An
%      unrecognized property name or invalid value makes property application
%      stop.  All inputs are passed to EconomicLoss_gui_OpeningFcn via varargin.
%
%      *See GUI Options on GUIDE's Tools menu.  Choose "GUI allows only one
%      instance to run (singleton)".
%
% See also: GUIDE, GUIDATA, GUIHANDLES

% Edit the above text to modify the response to help EconomicLoss_gui

% Last Modified by GUIDE v2.5 26-Mar-2020 15:34:07

% Begin initialization code - DO NOT EDIT
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @EconomicLoss_gui_OpeningFcn, ...
                   'gui_OutputFcn',  @EconomicLoss_gui_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end
% End initialization code - DO NOT EDIT


% --- Executes just before EconomicLoss_gui is made visible.
function EconomicLoss_gui_OpeningFcn(hObject, eventdata, handles, varargin)
% This function has no output args, see OutputFcn.
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% varargin   command line arguments to EconomicLoss_gui (see VARARGIN)

% Choose default command line output for EconomicLoss_gui
handles.output = hObject;

% Update handles structure
guidata(hObject, handles);

% UIWAIT makes EconomicLoss_gui wait for user response (see UIRESUME)
% uiwait(handles.figure1);


% --- Outputs from this function are returned to the command line.
function varargout = EconomicLoss_gui_OutputFcn(~, eventdata, handles)
% varargout  cell array for returning output args (see VARARGOUT);
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Get default command line output from handles structure
varargout{1} = handles.output;
```



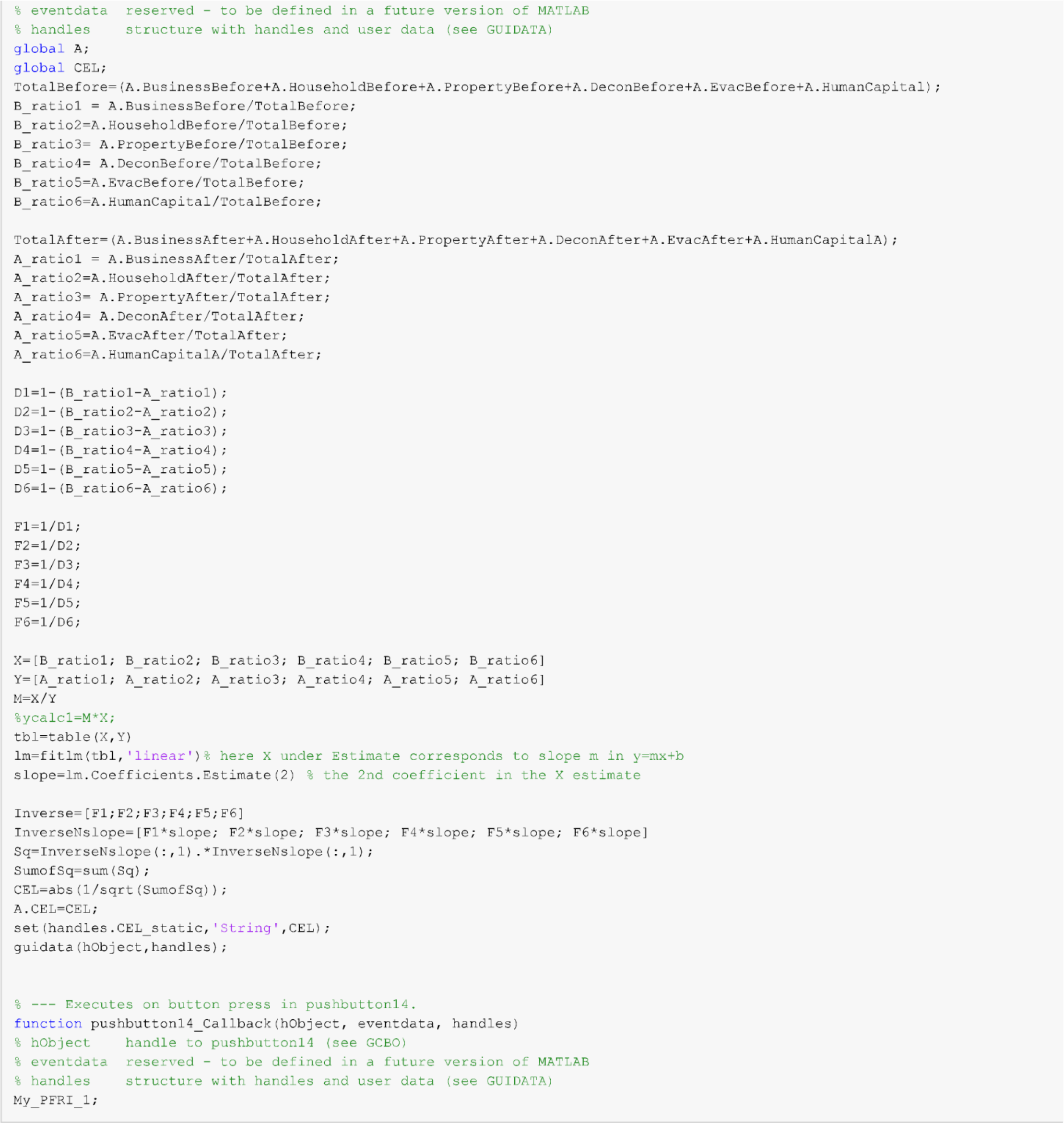
```
% --- Executes on button press in Ir_check.
function Ir_check_Callback(hObject, ~, handles)
% hObject    handle to Ir_check (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hint: get(hObject,'Value') returns toggle state of Ir_check
global Irstatus;

Irstatus=get(hObject, 'Value');
%display(checkboxStatus)
if Irstatus == 1
   handles.Ir_check=4;
    set(handles.Cs_check, 'Enable', 'off')
    set(handles.Co_check, 'Enable', 'off')

else
        msgbox('Please check a box')
end
guidata(hObject,handles)


% --- Executes on button press in Co_check.
function Co_check_Callback(hObject, eventdata, handles)
% hObject    handle to Co_check (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hint: get(hObject,'Value') returns toggle state of Co_check
global Costatus;
global A;
Costatus=get(hObject, 'Value')
%display(checkboxStatus)
if Costatus == 1
    handles.Co_check=3;
    set(handles.Cs_check, 'Enable', 'off')
    set(handles.Ir_check, 'Enable', 'off')
else
        msgbox('Please check a box')
end


guidata(hObject,handles)

% --- Executes on button press in Cs_check.
function Cs_check_Callback(hObject, eventdata, handles)
% hObject    handle to Cs_check (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hint: get(hObject,'Value') returns toggle state of Cs_check

global A;
global Csstatus;
Csstatus=get(hObject, 'Value');

if Csstatus == 1
   handles.Cs_check=2;
    set(handles.Co_check, 'Enable', 'off')
    set(handles.Ir_check, 'Enable', 'off')

else
        msgbox('Please check a box')
end
guidata(hObject,handles)

% --- Executes on button press in Exposure_check.
function Exposure_check_Callback(hObject, ~, handles)
% hObject    handle to Exposure_check (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
```

```
source_Cs=handles.Cs_check; %
source_Co=handles.Co_check; % this is working, it calls the value from the checkbox.
source_Ir=handles.Ir_check;

if(source_Cs == 2)
  ExposureDecon=xlsread('Economic loss.xls', 'Decon area dollar', 'J5:J5');
  ExposureDecon=round(ExposureDecon,2)
   set(handles.Exposure_static, 'String', ExposureDecon);

elseif (source_Co == 3)

 ExposureDecon=xlsread('Economic loss.xls', 'Decon area dollar', 'I5:I5');
 ExposureDecon=round(ExposureDecon,2)
   set(handles.Exposure_static, 'String', ExposureDecon);
elseif (source_Ir ==4)
        ExposureDecon=xlsread('Economic loss.xls', 'Decon area dollar', 'K5:K5');
        ExposureDecon=round(ExposureDecon,5)
   set(handles.Exposure_static, 'String', ExposureDecon);

else
  msgbox('Not an RDD, no source stolen!');
    %handles.EDstatus=EDstatus
end


guidata(hObject, handles)



%----------CALCULATE THE DECON TIME--------------


% --- Executes on button press in Decontime_check.
function Decontime_check_Callback(hObject, eventdata, handles)
% hObject    handle to Decontime_check (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
source_Cs=handles.Cs_check; %This calls the assigned value of cs_check which is 2
source_Co=handles.Co_check; % this is working, it calls the value from the checkbox.
source_Ir=handles.Ir_check;

if(source_Cs == 2)
  Decontime=xlsread('Economic loss.xls', 'Decon area dollar', 'N3:N3');
  Decontime=round(Decontime,0)
   set(handles.Decontime_static, 'String', Decontime);

elseif (source_Co == 3)

 Decontime=xlsread('Economic loss.xls', 'Decon area dollar', 'M3:M3');
 Decontime=round(Decontime,0)
   set(handles.Decontime_static, 'String', Decontime);
elseif (source_Ir ==4)
        Decontime=xlsread('Economic loss.xls', 'Decon area dollar', 'O3:O3');
   set(handles.Decontime_static, 'String', Decontime);

else
  msgbox('Not a RDD, no source stolen!');

end

A.Decontime=Decontime;

guidata(hObject, handles)

% --- Executes on selection change in county_pop.
function county_pop_Callback(hObject, eventdata, handles)
% hObject    handle to county_pop (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: contents = cellstr(get(hObject,'String')) returns county_pop contents as cell array
%        contents{get(hObject,'Value')} returns selected item from county_pop
global countyname;
countyname=get(hObject,'Value');
```

```
guidata(hObject,handles);

% --- Executes during object creation, after setting all properties.
function county_pop_CreateFcn(hObject, eventdata, handles)
% hObject    handle to county_pop (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: popupmenu controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end


% --- Executes on button press in Businessbefore_push.
function Businessbefore_push_Callback(hObject, eventdata, handles)
% hObject    handle to Businessbefore_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
Countyname=get(handles.county_pop, 'Value')
switch Countyname
    case 2
    BusinessBefore=xlsread('Economic loss.xls', 'Co', 'B2:B2');
    BusinessBefore=round(BusinessBefore/((A.Decontime)/365),3);
    format short e
    A.BusinessBefore=BusinessBefore(:);
    set(handles.BusinessBefore_static,'String', BusinessBefore);
    otherwise
        msgbox('Something wrong with your selection, Sorry!');
end

% --- Executes on button press in BusinessAfter_push.
function BusinessAfter_push_Callback(hObject, eventdata, handles)
% hObject    handle to BusinessAfter_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
Countyname=get(handles.county_pop, 'Value')
switch Countyname
    case 2

    BusinessAfter=(1-(A.Decontime/365)).*(A.BusinessBefore);
    format short e;
    A.BusinessAfter=BusinessAfter(:);
    set(handles.Businessafter_static,'String', BusinessAfter);
    otherwise
        msgbox('Something wrong with your selection, Sorry!');
end

guidata(hObject,handles)

% --- Executes on button press in Household_push.
function Household_push_Callback(hObject, eventdata, handles)
% hObject    handle to Household_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
Countyname=get(handles.county_pop, 'Value')
switch Countyname
    case 2
    HouseholdBefore=xlsread('Economic loss.xls', 'Co', 'B3:B3');
    HouseholdBefore=round(HouseholdBefore/((A.Decontime)/365),0);
    format short e
    A.HouseholdBefore=HouseholdBefore(:);
    set(handles.Household_static,'String', HouseholdBefore);
    otherwise
        msgbox('Something wrong with your selection, Sorry!');
end

% --- Executes on button press in pushbutton6.
function pushbutton6_Callback(hObject, eventdata, handles)
% hObject    handle to pushbutton6 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
```

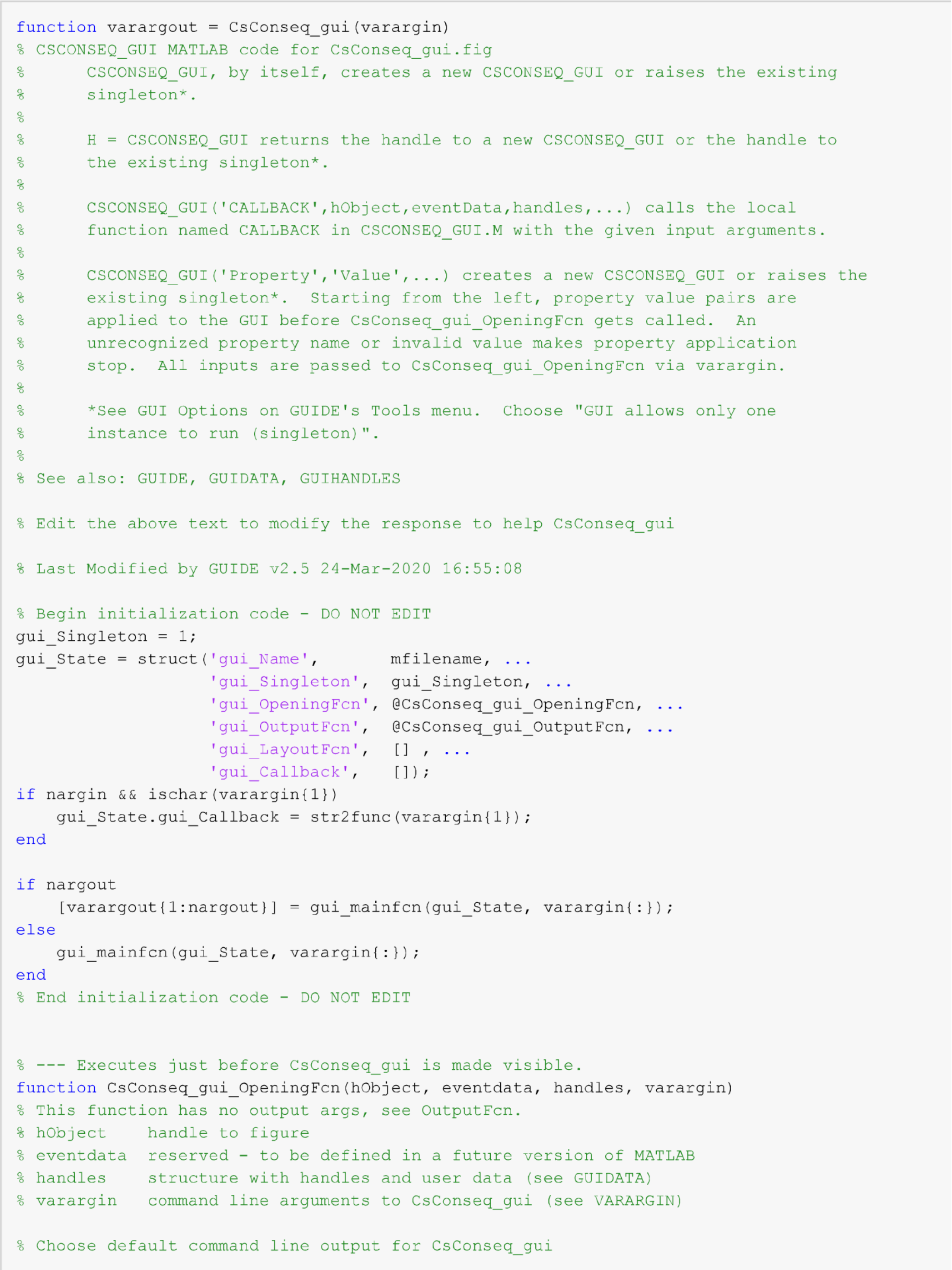


```
% handles    structure with handles and user data (see GUIDATA)
global A;
Countyname=get(handles.county_pop, 'Value')
switch Countyname
    case 2
    HouseholdAfter=(1-(A.Decontime/365)).*(A.HouseholdBefore);
    format short e
    A.HouseholdAfter=HouseholdAfter(:);
    set(handles.text9,'String', HouseholdAfter);
    otherwise
        msgbox('Something wrong with your selection, Sorry!');
end

guidata(hObject,handles)

%-----------PROPERTY VALUE---------BEFORE----------------

% --- Executes on button press in Propertybefore_push.
function Propertybefore_push_Callback(hObject, eventdata, handles)
% hObject    handle to Propertybefore_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
Countyname=get(handles.county_pop, 'Value')
switch Countyname
    case 2
    PropertyBefore=xlsread('Economic loss.xls', 'Co', 'B4:B4');
    format short e
    A.PropertyBefore=PropertyBefore(:);
    set(handles.Propertybefore_static,'String', PropertyBefore);
    otherwise
        msgbox('Something wrong with your selection, Sorry!');
end
guidata(hObject,handles)

%--------------PROPERTY VALUE ----AFTER------------

% --- Executes on button press in Propertyafter_push.
function Propertyafter_push_Callback(hObject, eventdata, handles)
% hObject    handle to Propertyafter_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
Countyname=get(handles.county_pop, 'Value')
switch Countyname
    case 2
    PropertyAfter=(0.85).*(A.PropertyBefore);
    format short e;
    A.PropertyAfter=PropertyAfter(:);
    set(handles.Propertyafter_static,'String', PropertyAfter);
    otherwise
        msgbox('Something wrong with your selection, Sorry!');
end

guidata(hObject,handles)

% --- Executes on button press in Humancapitalbefore_push.
function Humancapitalbefore_push_Callback(hObject, eventdata, handles)
% hObject    handle to Humancapitalbefore_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)


% --- Executes on button press in Humancapitalafter_push.
function Humancapitalafter_push_Callback(hObject, eventdata, handles)
% hObject    handle to Humancapitalafter_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
Countyname=get(handles.county_pop, 'Value')
switch Countyname
    case 2
        HumanCapital=xlsread('Economic loss.xls', 'Co', 'B7:B7');
    A.HumanCapital=HumanCapital;
    set(handles.Humancapitalafter_static,'String', HumanCapital);
    otherwise
        msgbox('Something wrong with your selection, Sorry!');
end
HumanCapitalA=0
A.HumanCapitalA=HumanCapitalA;
guidata(hObject,handles)

% --- Executes on button press in Deconcost_push.
function Deconcost_push_Callback(hObject, eventdata, handles)
% hObject    handle to Deconcost_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
source_Cs=handles.Cs_check; %This calls the assigned value of cs_check which is 2
source_Co=handles.Co_check; % this is working, it calls the value from the checkbox.
source_Ir=handles.Ir_check;

if(source_Cs == 2)
  Deconcost=xlsread('Economic loss.xls', 'Decon area dollar', 'U4:U4');
  Deconcost=round(Deconcost,0)
   set(handles.Deconcost_static, 'String', Deconcost);

elseif (source_Co == 3)

 Deconcost=xlsread('Economic loss.xls', 'Decon area dollar', 'T4:T4');
 Deconcost=round(Deconcost,0)
   set(handles.Deconcost_static, 'String', Deconcost);
elseif (source_Ir ==4)
        Deconcost=xlsread('Economic loss.xls', 'Decon area dollar', 'V4:V4');
   set(handles.Deconcost_static, 'String', Deconcost);

else
  msgbox('Not a RDD, no source stolen!');

end

DeconBefore=0.15*Deconcost;
A.DeconBefore=DeconBefore;

DeconAfter=Deconcost;
A.DeconAfter=Deconcost;



guidata(hObject, handles)


% --- Executes on button press in Evacuate_push.
function Evacuate_push_Callback(hObject, eventdata, handles)
% hObject    handle to Evacuate_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global A;
Countyname=get(handles.county_pop, 'Value')
switch Countyname
    case 2
    Evaccost=xlsread('Economic loss.xls', 'Co', 'B6:B6');

    A.Evaccost=Evaccost(:);
    set(handles.Evacuate_static,'String', Evaccost);
    otherwise
        msgbox('Something wrong with your selection, Sorry!');
end

EvacBefore=0.20*Evaccost;
EvacAfter=Evaccost;

A.EvacBefore=EvacBefore;
A.EvacAfter=Evaccost;
guidata(hObject,handles)

% --- Executes on button press in CEL_push.
function CEL_push_Callback(hObject, eventdata, handles)
% hObject    handle to CEL_push (see GCBO)
```



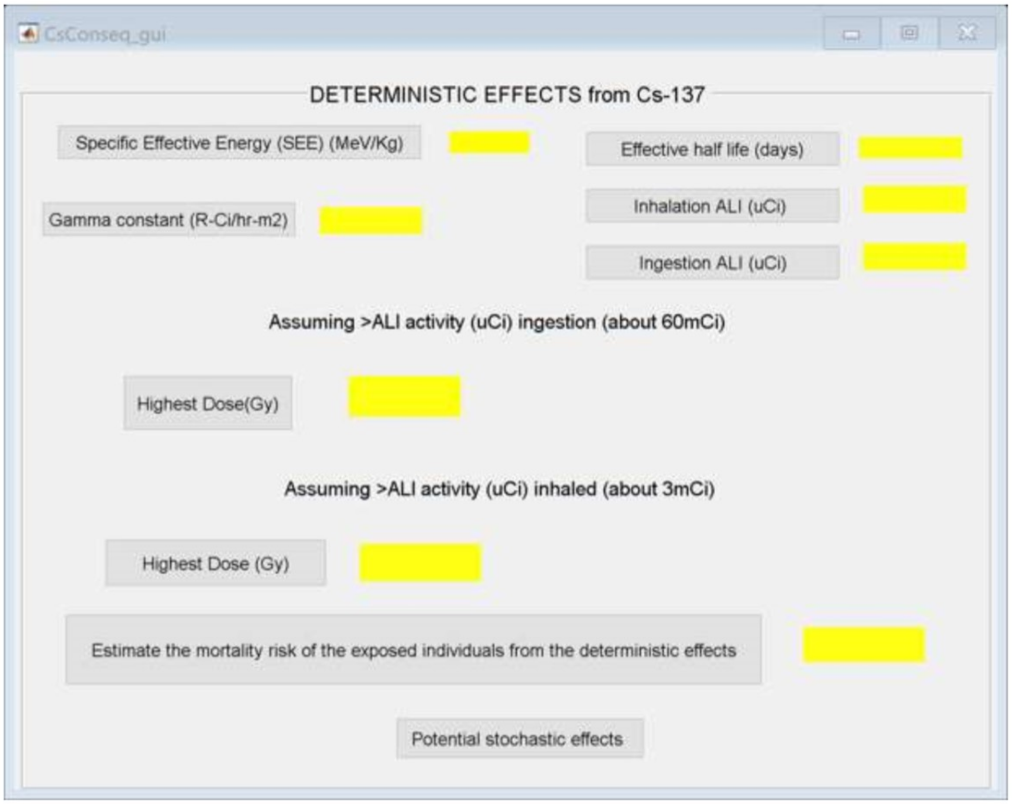
```
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
global CEL;
TotalBefore=(A.BusinessBefore+A.HouseholdBefore+A.PropertyBefore+A.DeconBefore+A.EvacBefore+A.HumanCapital);
B_ratio1 = A.BusinessBefore/TotalBefore;
B_ratio2=A.HouseholdBefore/TotalBefore;
B_ratio3= A.PropertyBefore/TotalBefore;
B_ratio4= A.DeconBefore/TotalBefore;
B_ratio5=A.EvacBefore/TotalBefore;
B_ratio6=A.HumanCapital/TotalBefore;

TotalAfter=(A.BusinessAfter+A.HouseholdAfter+A.PropertyAfter+A.DeconAfter+A.EvacAfter+A.HumanCapitalA);
A_ratio1 = A.BusinessAfter/TotalAfter;
A_ratio2=A.HouseholdAfter/TotalAfter;
A_ratio3= A.PropertyAfter/TotalAfter;
A_ratio4= A.DeconAfter/TotalAfter;
A_ratio5=A.EvacAfter/TotalAfter;
A_ratio6=A.HumanCapitalA/TotalAfter;

D1=1-(B_ratio1-A_ratio1);
D2=1-(B_ratio2-A_ratio2);
D3=1-(B_ratio3-A_ratio3);
D4=1-(B_ratio4-A_ratio4);
D5=1-(B_ratio5-A_ratio5);
D6=1-(B_ratio6-A_ratio6);

F1=1/D1;
F2=1/D2;
F3=1/D3;
F4=1/D4;
F5=1/D5;
F6=1/D6;

X=[B_ratio1; B_ratio2; B_ratio3; B_ratio4; B_ratio5; B_ratio6]
Y=[A_ratio1; A_ratio2; A_ratio3; A_ratio4; A_ratio5; A_ratio6]
M=X/Y
%ycalc1=M*X;
tbl=table(X,Y)
lm=fitlm(tbl,'linear')% here X under Estimate corresponds to slope m in y=mx+b
slope=lm.Coefficients.Estimate(2) % the 2nd coefficient in the X estimate

Inverse=[F1;F2;F3;F4;F5;F6]
InverseNslope=[F1*slope; F2*slope; F3*slope; F4*slope; F5*slope; F6*slope]
Sq=InverseNslope(:,1).*InverseNslope(:,1);
SumofSq=sum(Sq);
CEL=abs(1/sqrt(SumofSq));
A.CEL=CEL;
set(handles.CEL_static,'String',CEL);
guidata(hObject,handles);


% --- Executes on button press in pushbutton14.
function pushbutton14_Callback(hObject, eventdata, handles)
% hObject    handle to pushbutton14 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
My_PFRI_1;
```

Consequence - Cesium



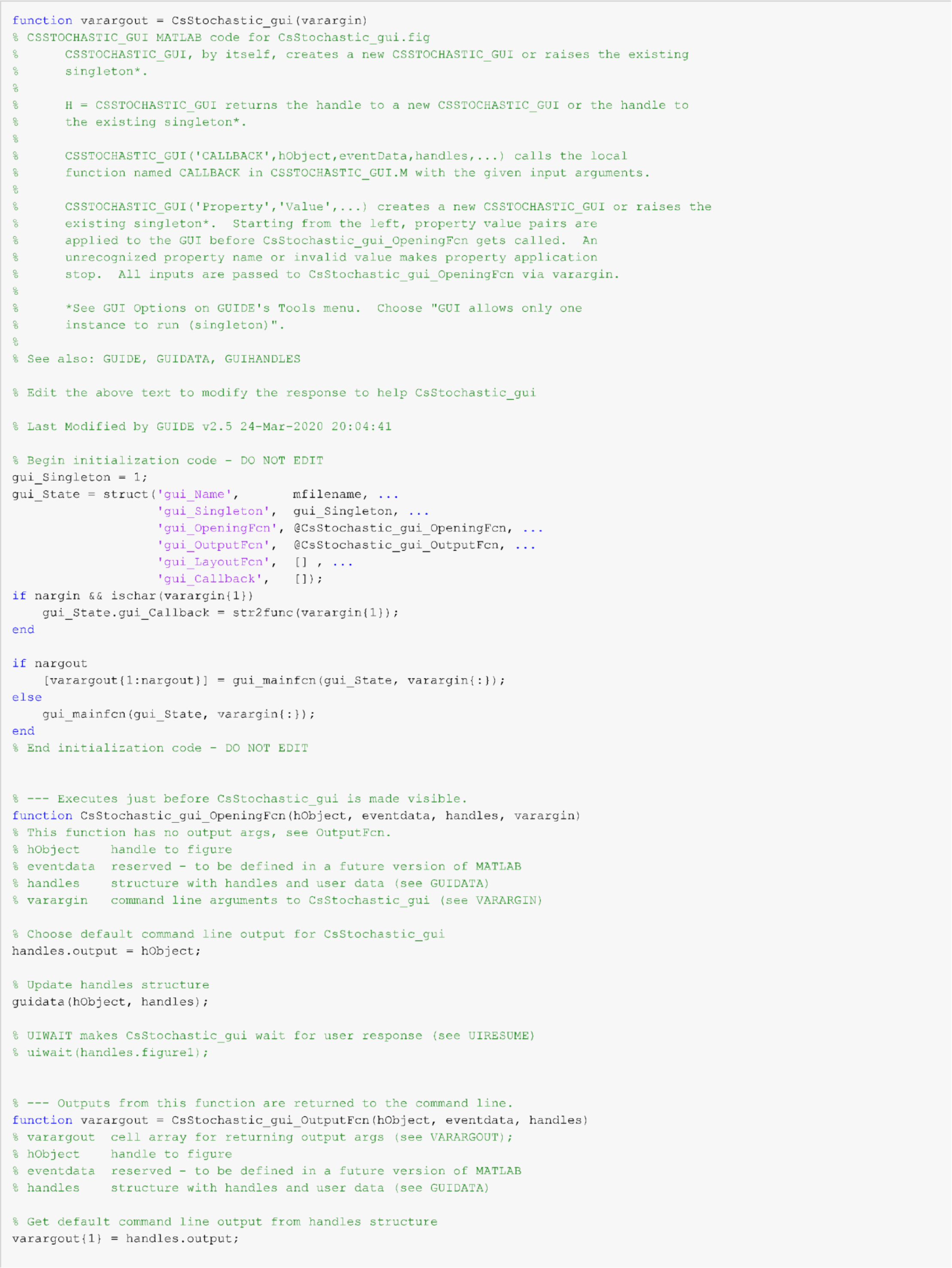
```
function varargout = CsConseq_gui(varargin)
% CSCONSEQ_GUI MATLAB code for CsConseq_gui.fig
%      CSCONSEQ_GUI, by itself, creates a new CSCONSEQ_GUI or raises the existing
%      singleton*.
%
%      H = CSCONSEQ_GUI returns the handle to a new CSCONSEQ_GUI or the handle to
%      the existing singleton*.
%
%      CSCONSEQ_GUI('CALLBACK',hObject,eventData,handles,...) calls the local
%      function named CALLBACK in CSCONSEQ_GUI.M with the given input arguments.
%
%      CSCONSEQ_GUI('Property','Value',...) creates a new CSCONSEQ_GUI or raises the
%      existing singleton*.  Starting from the left, property value pairs are
%      applied to the GUI before CsConseq_gui_OpeningFcn gets called.  An
%      unrecognized property name or invalid value makes property application
%      stop.  All inputs are passed to CsConseq_gui_OpeningFcn via varargin.
%
%      *See GUI Options on GUIDE's Tools menu.  Choose "GUI allows only one
%      instance to run (singleton)".
%
% See also: GUIDE, GUIDATA, GUIHANDLES

% Edit the above text to modify the response to help CsConseq_gui

% Last Modified by GUIDE v2.5 24-Mar-2020 16:55:08

% Begin initialization code - DO NOT EDIT
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @CsConseq_gui_OpeningFcn, ...
                   'gui_OutputFcn',  @CsConseq_gui_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end
% End initialization code - DO NOT EDIT


% --- Executes just before CsConseq_gui is made visible.
function CsConseq_gui_OpeningFcn(hObject, eventdata, handles, varargin)
% This function has no output args, see OutputFcn.
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% varargin   command line arguments to CsConseq_gui (see VARARGIN)

% Choose default command line output for CsConseq_gui
```

```
handles.output = hObject;

% Update handles structure
guidata(hObject, handles);
global user_activity;
% UIWAIT makes CsConseq_gui wait for user response (see UIRESUME)
% uiwait(handles.figure1);


% --- Outputs from this function are returned to the command line.
function varargout = CsConseq_gui_OutputFcn(hObject, eventdata, handles)
% varargout  cell array for returning output args (see VARARGOUT);
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Get default command line output from handles structure
varargout{1} = handles.output;


% --- Executes on button press in stochastic_push.
function stochastic_push_Callback(hObject, eventdata, handles)
% hObject    handle to stochastic_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
CsStochastic_gui;


% --- Executes on button press in fragexposure_push.
function fragexposure_push_Callback(hObject, eventdata, handles)
% hObject    handle to fragexposure_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
ARSInhalation=xlsread('ConsequencesCs.xls', 'ARS-Inhalation', 'S2:S25');
Maxdose=max(ARSInhalation(:))
 set(handles.fragexposure_static, 'String',Maxdose)


% --- Executes on button press in deathArs_push.
function deathArs_push_Callback(hObject, eventdata, handles)
% hObject    handle to deathArs_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
riskinhalation=xlsread('ConsequencesCs.xls', 'ARS-Inhalation', 'AA2:AA2');
riskIngestARS=xlsread('ConsequencesCs.xls', 'ARS ingestion', 'AA3:AA3');
format short e;
RisksumARS=(riskinhalation+riskIngestARS);
set(handles.deathars_static, 'String', RisksumARS);
  global A;
 A.RisksumARS=RisksumARS;
 guidata(hObject, handles);


% --- Executes on button press in SEE_push.
function SEE_push_Callback(hObject, eventdata, handles)
% hObject    handle to SEE_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
 EffectiveEnergy=xlsread('ConsequencesCs.xls', 'Constants', 'B2:B2');
 set(handles.SEE_static, 'String',EffectiveEnergy)

% --- Executes on button press in Effective_push.
function Effective_push_Callback(hObject, eventdata, handles)
% hObject    handle to Effective_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
Effectivelife=xlsread('ConsequencesCs.xls', 'Constants', 'B4:B4');
 set(handles.Effective_static, 'String',Effectivelife)

% --- Executes on button press in Gammaconstant_push.
function Gammaconstant_push_Callback(hObject, eventdata, handles)
% hObject    handle to Gammaconstant_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
Gammaconst=xlsread('ConsequencesCs.xls', 'Constants', 'B3:B3');
 set(handles.gamma_static, 'String',Gammaconst)

% --- Executes on button press in inhal_push.
function inhal_push_Callback(hObject, eventdata, handles)
% hObject    handle to inhal_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
InhalationALI=xlsread('ConsequencesCs.xls', 'Constants', 'B5:B5');
 set(handles.inhale_static, 'String',InhalationALI)

% --- Executes on button press in ingest_push.
function ingest_push_Callback(hObject, eventdata, handles)
% hObject    handle to ingest_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
IngestionALI=xlsread('ConsequencesCs.xls', 'Constants', 'B6:B6');
 set(handles.ingest_static, 'String',IngestionALI)


% --- Executes on button press in ARSIngest_pushc.
function ARSIngest_pushc_Callback(hObject, eventdata, handles)
% hObject    handle to ARSIngest_pushc (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
IngestionARS=xlsread('ConsequencesCs.xls', 'ARS ingestion', 'S3:S28');
Maxdose=max(IngestionARS(:))
 set(handles.ARSingestion_static, 'String',Maxdose)
```

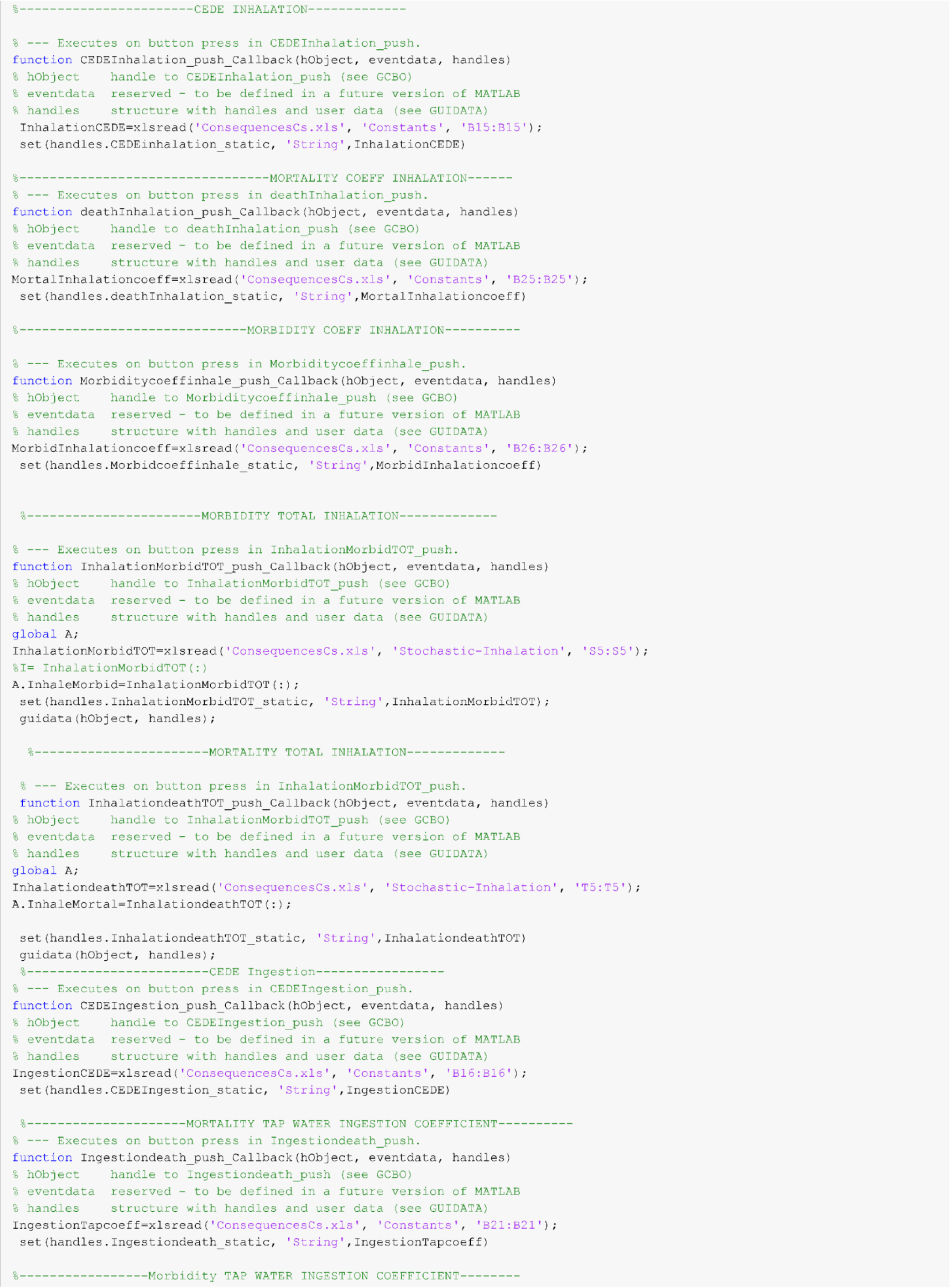

CsConseq_gui
DETERMINISTIC EFFECTS from Cs-137
Specific Effective Energy (SEE) (MeV/Kg)
Effective half life (days)
Gamma constant (R-Ci/hr-m2)
Inhalation ALI (uCi)
Ingestion ALI (uCi)
Assuming >ALI activity (uCi) ingestion (about 60mCi)
Highest Dose(Gy)
Assuming >ALI activity (uCi) inhaled (about 3mCi)
Highest Dose (Gy)
Estimate the mortality risk of the exposed individuals from the deterministic effects
Potential stochastic effects

Published with MATLAB® R2019b

Stochastic effects - Cesium

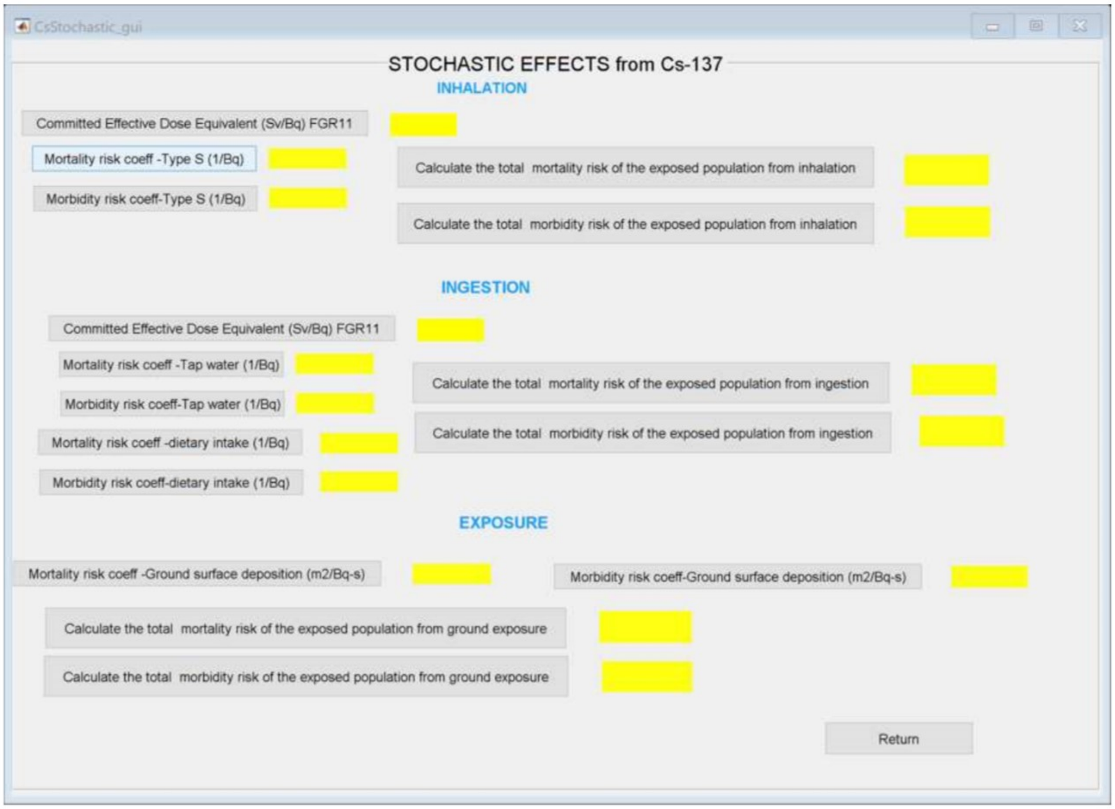


```
function varargout = CsStochastic_gui(varargin)
% CSSTOCHASTIC_GUI MATLAB code for CsStochastic_gui.fig
%      CSSTOCHASTIC_GUI, by itself, creates a new CSSTOCHASTIC_GUI or raises the existing
%      singleton*.
%
%      H = CSSTOCHASTIC_GUI returns the handle to a new CSSTOCHASTIC_GUI or the handle to
%      the existing singleton*.
%
%      CSSTOCHASTIC_GUI('CALLBACK',hObject,eventData,handles,...) calls the local
%      function named CALLBACK in CSSTOCHASTIC_GUI.M with the given input arguments.
%
%      CSSTOCHASTIC_GUI('Property','Value',...) creates a new CSSTOCHASTIC_GUI or raises the
%      existing singleton*.  Starting from the left, property value pairs are
%      applied to the GUI before CsStochastic_gui_OpeningFcn gets called.  An
%      unrecognized property name or invalid value makes property application
%      stop.  All inputs are passed to CsStochastic_gui_OpeningFcn via varargin.
%
%      *See GUI Options on GUIDE's Tools menu.  Choose "GUI allows only one
%      instance to run (singleton)".
%
% See also: GUIDE, GUIDATA, GUIHANDLES

% Edit the above text to modify the response to help CsStochastic_gui

% Last Modified by GUIDE v2.5 24-Mar-2020 20:04:41

% Begin initialization code - DO NOT EDIT
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @CsStochastic_gui_OpeningFcn, ...
                   'gui_OutputFcn',  @CsStochastic_gui_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end
% End initialization code - DO NOT EDIT


% --- Executes just before CsStochastic_gui is made visible.
function CsStochastic_gui_OpeningFcn(hObject, eventdata, handles, varargin)
% This function has no output args, see OutputFcn.
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% varargin   command line arguments to CsStochastic_gui (see VARARGIN)

% Choose default command line output for CsStochastic_gui
handles.output = hObject;

% Update handles structure
guidata(hObject, handles);

% UIWAIT makes CsStochastic_gui wait for user response (see UIRESUME)
% uiwait(handles.figure1);


% --- Outputs from this function are returned to the command line.
function varargout = CsStochastic_gui_OutputFcn(hObject, eventdata, handles)
% varargout  cell array for returning output args (see VARARGOUT);
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Get default command line output from handles structure
varargout{1} = handles.output;
```



```
%-----------------------CEDE INHALATION-------------

% --- Executes on button press in CEDEInhalation_push.
function CEDEInhalation_push_Callback(hObject, eventdata, handles)
% hObject    handle to CEDEInhalation_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
 InhalationCEDE=xlsread('ConsequencesCs.xls', 'Constants', 'B15:B15');
 set(handles.CEDEinhalation_static, 'String',InhalationCEDE)

%---------------------------------MORTALITY COEFF INHALATION------
% --- Executes on button press in deathInhalation_push.
function deathInhalation_push_Callback(hObject, eventdata, handles)
% hObject    handle to deathInhalation_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
MortalInhalationcoeff=xlsread('ConsequencesCs.xls', 'Constants', 'B25:B25');
 set(handles.deathInhalation_static, 'String',MortalInhalationcoeff)

%------------------------------MORBIDITY COEFF INHALATION----------

% --- Executes on button press in Morbiditycoeffinhale_push.
function Morbiditycoeffinhale_push_Callback(hObject, eventdata, handles)
% hObject    handle to Morbiditycoeffinhale_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
MorbidInhalationcoeff=xlsread('ConsequencesCs.xls', 'Constants', 'B26:B26');
 set(handles.Morbidcoeffinhale_static, 'String',MorbidInhalationcoeff)


 %-----------------------MORBIDITY TOTAL INHALATION-------------

% --- Executes on button press in InhalationMorbidTOT_push.
function InhalationMorbidTOT_push_Callback(hObject, eventdata, handles)
% hObject    handle to InhalationMorbidTOT_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
InhalationMorbidTOT=xlsread('ConsequencesCs.xls', 'Stochastic-Inhalation', 'S5:S5');
%T= InhalationMorbidTOT(:)
A.InhaleMorbid=InhalationMorbidTOT(:);
 set(handles.InhalationMorbidTOT_static, 'String',InhalationMorbidTOT);
 guidata(hObject, handles);

  %-----------------------MORTALITY TOTAL INHALATION-------------

 % --- Executes on button press in InhalationMorbidTOT_push.
 function InhalationdeathTOT_push_Callback(hObject, eventdata, handles)
% hObject    handle to InhalationMorbidTOT_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
InhalationdeathTOT=xlsread('ConsequencesCs.xls', 'Stochastic-Inhalation', 'T5:T5');
A.InhaleMortal=InhalationdeathTOT(:);

 set(handles.InhalationdeathTOT_static, 'String',InhalationdeathTOT)
 guidata(hObject, handles);
 %------------------------CEDE Ingestion-----------------
% --- Executes on button press in CEDEIngestion_push.
function CEDEIngestion_push_Callback(hObject, eventdata, handles)
% hObject    handle to CEDEIngestion_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
IngestionCEDE=xlsread('ConsequencesCs.xls', 'Constants', 'B16:B16');
 set(handles.CEDEIngestion_static, 'String',IngestionCEDE)

 %---------------------MORTALITY TAP WATER INGESTION COEFFICIENT----------
% --- Executes on button press in Ingestiondeath_push.
function Ingestiondeath_push_Callback(hObject, eventdata, handles)
% hObject    handle to Ingestiondeath_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
IngestionTapcoeff=xlsread('ConsequencesCs.xls', 'Constants', 'B21:B21');
 set(handles.Ingestiondeath_static, 'String',IngestionTapcoeff)

%-----------------Morbidity TAP WATER INGESTION COEFFICIENT--------
```

```
% --- Executes on button press in IngestionMorbid_push.
function IngestionMorbid_push_Callback(hObject, eventdata, handles)
% hObject    handle to IngestionMorbid_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
IngestionTapcoeffMorbid=xlsread('ConsequencesCs.xls', 'Constants', 'B19:B19');
 set(handles.IngestionMorbid_static, 'String',IngestionTapcoeffMorbid)

%-------------- MORTALITY DIETARY FOOD INTAKE coefficient--------------------
% --- Executes on button press in FoodMortality_push.
function FoodMortality_push_Callback(hObject, eventdata, handles)
% hObject    handle to FoodMortality_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
IngestionFoodcoeffMortal=xlsread('ConsequencesCS.xls', 'Constants', 'B22:B22');
 set(handles.FoodMortality_static, 'String',IngestionFoodcoeffMortal)

 %------------------MORBIDITY DIETARY FOOD INTAKE COEFFICIENT-----------------
% --- Executes on button press in FoodMorbid_push.
function FoodMorbid_push_Callback(hObject, eventdata, handles)
% hObject    handle to FoodMorbid_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
 IngestionFoodcoeffMorbid=xlsread('ConsequencesCo.xls', 'Constants', 'B20:B20');
 set(handles.FoodMorbid_static, 'String',IngestionFoodcoeffMorbid)

 %------------------------TOTAL INGESTION MORTALITY---------------

% --- Executes on button press in IngestionMortalTOT_push.
function IngestionMortalTOT_push_Callback(hObject, eventdata, handles)
% hObject    handle to IngestionMortalTOT_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
 global A;
IngestionMortalTOT=xlsread('ConsequencesCs.xls', 'Stochastic-Ingestion', 'U5:U5');
A.IngestMortal=IngestionMortalTOT(:);
 set(handles.IngestionMortalTOT_static, 'String',IngestionMortalTOT)
 guidata(hObject, handles);
 %-----------------TOTAL INGESTION MORBIDITY-----------------------

% --- Executes on button press in IngestionMorbidTOT_push.
function IngestionMorbidTOT_push_Callback(hObject, eventdata, handles)
% hObject    handle to IngestionMorbidTOT_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global A;
IngestionMorbidTOT=xlsread('ConsequencesCs.xls', 'Stochastic-Ingestion', 'V5:V5');
 A.IngestMorbid=IngestionMorbidTOT(:);
 set(handles.IngestionMorbTOT_static, 'String',IngestionMorbidTOT);


guidata(hObject, handles);

%-------------MORTALITY EXPOSURE RISK COEFFICIENT-------

% --- Executes on button press in MortalityXcoeff_push.
function MortalityXcoeff_push_Callback(hObject, eventdata, handles)
% hObject    handle to MortalityXcoeff_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
 XposurecoeffMortal=xlsread('ConsequencesCs.xls', 'Constants', 'B29:B29');
 set(handles.MortalityXcoeff_static, 'String',XposurecoeffMortal)

% --- Executes on button press in MorbidityXcoeff_push.
function MorbidityXcoeff_push_Callback(hObject, eventdata, handles)
% hObject    handle to MorbidityXcoeff_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
XposurecoeffMorbid=xlsread('ConsequencesCs.xls', 'Constants', 'B30:B30');
 set(handles.MorbidityXcoeff_static, 'String',XposurecoeffMorbid)


% --- Executes on button press in MortalityXposue_push.
function MortalityXposue_push_Callback(hObject, eventdata, handles)
% hObject    handle to MortalityXposue_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
XposureMortal=xlsread('ConsequencesCs.xls', 'Stochastic-Exposure', 'Q5:Q5');
 A.XposureMortal=XposureMortal(:);
 set(handles.MortalityXposure_static, 'String',XposureMortal);


 guidata(hObject, handles);

% --- Executes on button press in MorbidityXposure_push.
function MorbidityXposure_push_Callback(hObject, eventdata, handles)
% hObject    handle to MorbidityXposure_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global A;
XposureMorbid=xlsread('ConsequencesCs.xls', 'Stochastic-Exposure', 'R5:R5');
A.XposureMorbid=XposureMorbid(:);
 set(handles.MorbidityXposure_static, 'String',XposureMorbid);

 guidata(hObject, handles);

% --- Executes on button press in return_push.
function return_push_Callback(hObject, eventdata, handles)
% hObject    handle to return_push (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
Blast_gui;
```


CsStochastic_gui
STOCHASTIC EFFECTS from Cs-137
INHALATION
Committed Effective Dose Equivalent (Sv/Bq) FGR11
Mortality risk coeff -Type S (1/Bq)
Morbidity risk coeff-Type S (1/Bq)
Calculate the total mortality risk of the exposed population from inhalation
Calculate the total morbidity risk of the exposed population from inhalation
INGESTION
Committed Effective Dose Equivalent (Sv/Bq) FGR11
Mortality risk coeff -Tap water (1/Bq)
Morbidity risk coeff-Tap water (1/Bq)
Mortality risk coeff -dietary intake (1/Bq)
Morbidity risk coeff-dietary intake (1/Bq)
Calculate the total mortality risk of the exposed population from ingestion
Calculate the total morbidity risk of the exposed population from ingestion
EXPOSURE
Mortality risk coeff -Ground surface deposition (m2/Bq-s)
Morbidity risk coeff-Ground surface deposition (m2/Bq-s)
Calculate the total mortality risk of the exposed population from ground exposure
Calculate the total morbidity risk of the exposed population from ground exposure
Return

Published with MATLAB® R2019b

REFERENCES

Adams, T. G., & Casagrande, R. (2019). Modeling the Optimum Prussian Blue Treatment for Acute Radiation Syndrome Following 137 Cs Ingestion. *Health Physics*, *116*(1), 88–95. https://doi.org/10.1097/HP.0000000000000966

Aldy, J. E., & Viscusi, W. K. (2008). Adjusting the value of a statistical life for age and cohort effects. *Review of Economics and Statistics*. https://doi.org/10.1162/rest.90.3.573

Beccari, B. (2016). A comparative analysis of disaster risk, vulnerability and resilience composite indicators. *PLoS Currents*.

https://doi.org/10.1371/currents.dis.453df025e34b682e9737f95070f9b970

Beisbart, C. (2019). *Computer Simulation Validation: Fundamental Concepts, Methodological Frameworks, and Philosophical Perspectives*. Library of Congress Control Number: 2018966848. Springer Nature Switzerland AG.

Biancotto, S., Malizia, A., Pinto, M., Contessa, G. M., Coniglio, A., & D'Arienzo, M. (2020). Analysis of a dirty bomb attack in a large metropolitan area: Simulate the dispersion of radioactive materials. *Journal of Instrumentation*, *15*(2). https://doi.org/10.1088/1748-0221/15/02/P02019

Bier, V. M., Cox, L. A., & Azaiez M, N. (2009). *Why both game theory and reliability theory are important in defending infrastructure against intelligent attacks - Game theoretic risk analysis of security threats* . Springer US.

Bland, J., & Potter, C. G. (2018). *Radiological Exposure Devices (RED) Technical Basis for Threat Profile Sandia National Laboratories*.

Boardman, A. E. (2011). Cost-benefit analysis: concepts and practice. In *The Pearson series in economics*. Pearson Education, Inc. New Jersey.

Bram, J., Orr, J., & Rapaport, C. (2002). Measuring the Effects of the September 11 Attack on New York City. *Federal Reserve Bank of New York Economic Policy Review*, *8*(2), 5–20. http://www.ny.frb.org/research/epr/%5Cnhttp://search.ebscohost.com/login.aspx?direct=true&db=ecn&AN=0637233&site=ehost-live

Brode, H. L. (1955). Numerical solutions of spherical blast waves. *Journal of Applied Physics*. https://doi.org/10.1063/1.1722085

Bruneau, E. (2016). Understanding the Terrorist Mind. *Cerebrum : The Dana Forum on Brain Science*, November, 1–14.

Cember, H., & Johnson, E. T. (2011). *Introduction to Health Physics. Fourth Edition*. https://doi.org/10.1063/1.2916417

Cho, J., Han, S. H., Kim, D. S., & Lim, H. G. (2018). Multi-unit Level 2 probabilistic safety assessment: Approaches and their application to a six-unit nuclear power plant site. *Nuclear Engineering and Technology*, *50*(8), 1234–1245. https://doi.org/10.1016/j.net.2018.04.005

Connell, L. W. (2017). Dirty Bomb Risk and Impact. *U.S. Department of Energy, Sandia National Laboratories*. https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/2017/179121r.pdf (Accessed: 20 April 2020).

Crane, A. T. (1990). Physical vulnerability of electric systems to natural disaster and sabotage. *Terrorism*, *13*(3), 189–190. https://doi.org/10.1080/10576109008435829

Crenshaw, M. (2000). The psychology of terrorism: An agenda for the 21st century. *Political Psychology*. https://doi.org/10.1111/0162-895X.00195

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches-Fourth Edition*. Sage, Los Angeles. ISBN 978-1-4522-2609-5

Curado, M. P., Oliveira, M. M. de, Valverde, N. D., & Cruz, A. D. da. (2019). Cancer incidence in the cohort exposed to Cesium-137 accident in Goiânia (Brazil) in 1987. *Journal of Health & Biological Sciences*, *7*(3), 228. https://doi.org/10.12662/2317-3076jhbs.v7i3.2429.p228-232.2019

Denney, S. H. (1970). *A review of literature on the theory of hit and kill probabilities*. [A Thesis, United States Naval Postgraduate School].

Eckstein, O (1958). Water-resource development; the economics of project evaluation. Cambridge, Harvard University Press. Retrieved from https://hdl.handle.net/2027//ien.35556021298609.

Elliott, Grant. "US Nuclear Weapon Safety and Control". MIT Program in Science, Technology and Society (2005)

Etzioni, A. (2010). Bounded rationality. *Socio-Economic Review*, *8*(2), 377–383. https://doi.org/10.1093/ser/mwq002

Ezell, B. C., Bennett, S. P., von Winterfeldt, D., Sokolowski, J., & Collins, A. J. (2010). Probabilistic risk analysis and terrorism risk. *Risk Analysis*, *30*(4), 575–589. https://doi.org/10.1111/j.1539-6924.2010.01401.x

Federal Emergency Management Agency. (2003a)*, Primer for Design Safe Schools Projects in Case of Terrorist Attacks* (FEMA 428).

Federal Emergency Management Agency. (2003b). *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks* (FEMA 427).

Federal Emergency Management Agency. (2018). *Threat Identification and Rating*. FEMA (452)

Federation of American Scientist. Naval Weapons Engineering. (July 25, 1997). *Damage Criteria for Warheads.* Retrieved from https://fas.org/man/dod-101/navy/docs/es310/dam_crit/dam_crit.htm. Accessed on July 7th, 2020.

Ferguson, C. D., Potter, W. C., Sands, A., Spector, L. S., & Wehling, F. L. (2005). *The Four Faces of Nuclear Terrorism*. https://doi.org/10.4324/9780203956922

Fudenberg, D., & Tirole, J. (1991). *Game theory.* The MIT Press. Cambridge, Massachusetts.

Garcia, M. L. (2007). *Design and Evaluation of Physical Protection Systems: Second Edition*. https://doi.org/10.1016/C2009-0-25612-1

Garrick, B. J., Hall, J. E., Kilger, M., McDonald, J. C., O'Toole, T., Probst, P. S., Parker, E. R., Rosenthal, R., Trivelpiece, A. W., van Arsdale, L. A., & Zebroski, E. L. (2004). Confronting the risks of terrorism: Making the right decisions. In *Reliability Engineering and System Safety* (Vol. 86, Issue 2). Elsevier Ltd. https://doi.org/10.1016/j.ress.2004.04.003

Gbetibouo, G. A. (2009). Understanding farmers' perceptions and adaptations to climate change and variability: The case of the Limpopo basin, South Africa. *IFPRI Discussion Paper 00849*. https://doi.org/10.1068/a312017

Giesecke, J. A., Burns, W. J., Barrett, A., Bayrak, E., Rose, A., Slovic, P., & Suher, M. (2012). Assessment of the Regional Economic Impacts of Catastrophic Events: CGE Analysis of Resource Loss and Behavioral Effects of an RDD Attack Scenario. *Risk Analysis*, *32*(4), 583–600. https://doi.org/10.1111/j.1539-6924.2010.01567.x

Guikema, S. D. (2009). Game theory models of intelligent actors in reliability analysis: An overview of the state of the art. In International Series in Operations Research and Management Science. https://doi.org/10.1007/978-0-387-87767-9_2

Hal Varian. (2010). *Intermediate Microeconomics* 8th Edition. W.W. Norton & Company, 2010. https://doi.org/10.1007/s13398-014-0173-7.2

Hammitt, J. K., & Treich, N. (2007). Statistical vs. identified lives in benefit-cost analysis. *Journal of Risk and Uncertainty*. https://doi.org/10.1007/s11166-007-9015-8

Harper, F. T., Musolino, S. v., & Wente, W. B. (2007). Realistic radiological dispersal device hazard boundaries and ramifications for early consequence management decisions. *Health Physics*, *93*(1), 1–16. https://doi.org/10.1097/01.HP.0000264935.29396.6f

Hausken, K. (2018). A cost–benefit analysis of terrorist attacks. *Defence and Peace Economics*. https://doi.org/10.1080/10242694.2016.1158440

Homann, S., Aluzzi, F. (2013).HotSpot Health Physics Codes. National Atmospheric Release Advisory Center,Version 3.0, User's Guide. Livermore, CA.

Hubbard, D. W. (2010). *How to Measure Anything, Second Edition*. Wiley. https://doi.org/10.1002/9781118983836

Hudson, R. A., Majeska, M., & Metz, H. C. (1985). The Sociology and Psychology of Terrorism: Who Becomes a terrorist and Why? *Federal Research Division, Library of Congress*, *4*(2), 62–66.

Institute for Digital Research & Education, Statistical Consulting, A Practical introduction to Factor Analysis: Exploratory Factor analysis, UCLA, Available at https://stats.idre.ucla.edu/spss/seminars/introduction-to-factor-analysis/a-practical-introduction-to-factor-analysis/, Accessed on May 19, 2020.

Kaiser, H. F. (1960). The application of electronic computers to factor analysis. *Educ. Psychol. Meas,* 20, 141-151.

Kamen, J., Hsu, W. Y., Boswell, B., & Hill, C. (2019). Successful Migration from Radioactive Irradiators to X-ray Irradiators in One of the Largest Medical Centers in the US. *Health Physics*, *117*(5), 558–570. https://doi.org/10.1097/HP.0000000000001095

Kassim, S., Hasan, H., Mohd Ismon, A., & Muhammad Asri, F. (2013). Parameter estimation in factor analysis: Maximum likelihood versus principal component. *AIP Conference Proceedings*, *1522*(April), 1293–1299. https://doi.org/10.1063/1.4801279

Keeney, R. L. (1977). The Art of Assessing Multi-attribute Utility Functions. *Organizational Behavior and Human Performance*. https://doi.org/10.1016/0030-5073(77)90065-4

Keeney, R. L., & von Winterfeldt, D. (2011). A Value Model for Evaluating Homeland Security Decisions. *Risk Analysis*, *31*(9), 1470–1487. https://doi.org/10.1111/j.1539-6924.2011.01597.x

Khripunov, I. (2006). *Nuclear Security Culture: From Concept to Practice*. 1–16.

Korda, M., & Kristensen, H. M. (2019). U.S. Ballistic missile defenses. *Bulletin of the Atomic Scientists*, *75*(6), 295–306. https://doi.org/10.1080/00963402.2019.1680055

Kutkov, V. (2011). Severe deterministic effect of external exposure and intake of radioactive material: Basis for emergency response criteria. *Journal of Radiological Protection 31(2):237-53*. DOI: 10.1088/0952-4746/31/2/003.

Kwanga, G. M., Shabu, T., & Adaaku, E. M. (2017). Natural Disasters and Crime Incidence: A Case of 2012 Flooding in Benue State, Nigeria. *International Journal of Geology, Agriculture and Environmental Sciences*, *October*, 43–48. www.woarjournals.org/IJGAES

Kyne, D., & Harris, J. T. (2015). A longitudinal study of human exposure to potential nuclear power plant risk. *International Journal of Disaster Risk Science*, *6*(4), 399–414. https://doi.org/10.1007/s13753-015-0075-0

Levine, E. S. (2012). Estimating Conditional Probabilities of Terrorist Attacks: Modeling Adversaries with Uncertain Value Tradeoffs. *Risk Analysis*, *32*(2), 294–303. https://doi.org/10.1111/j.1539-6924.2011.01655.x

Mærli, M. B. (2010). *The threat of nuclear terrorism*. *Nuclear Proliferation and International Order: Challenges to the Non-Proliferation Treaty*. https://doi.org/10.4324/9780203844823

Mallonee, S., Shariat, S., Stennies, G., Waxweiler, R., Hogan, D., & Jordan, F. (1996). Physical injuries and fatalities resulting from the Oklahoma City bombing. *Journal of the American Medical Association*. https://doi.org/10.1001/jama.276.5.382

Marchand, K. A., & Alfawakhiri, F. (2004). *Blast and Progressive Collapse. Facts for Steel Buildings.* American Institute of Steel Construction, Inc. https://www.aisc.org/globalassets/aisc/publications/facts-for-steel-buildings-2-blast-and-progressive-collapse.pdf

Matusitz, J. A. (2015). *Symbolism in terrorism.* Rowman and Littlefield.

Mazonka, O. (2012). *Cumulative Probability of Blast Fragmentation Effect*. 1–27. https://arxiv.org/ftp/arxiv/papers/1304/1304.2285.pdf

McGill, W. L., Ayyub, B. M., & Kaminskiy, M. (2007). Risk analysis for critical asset protection. In *Risk Analysis*. https://doi.org/10.1111/j.1539-6924.2007.00955.x

Medalia, J. (2012). *Dirty Bombs: Technical Background, Attack, Prevention and Response*, *Issues for Congress*. Congressional Research Service. 1–85.

Meyer et al. (2018). *CNS Global Incidents and Trafficking Database*. James Martin Center for Nonproliferation Studies. Nuclear Threat Initiative.

Mitra-Kahn, B. H. B. H. (2008). Debunking the Myths of Computable General Equilibrium Models. *SCEPA Working Papers*.

Morris, E., Hoe, A., Potter, J., (1987). *The Psychology of Terrorism*. https://doi.org/10.1007/978-1-349-18983-0_5

Mowatt-Larssen, R. (2010). Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality? *Belfer Center for Science and International Affairs*, *January*, 1–32. http://belfercenter.ksg.harvard.edu/files/al-qaeda-wmd-threat.pdf

Myers, C. T (2012). *Quantitative Methodology for Assessing State-Level Nuclear Security Measures.* [Doctoral dissertation, A&M University].

Myers, K. A (1963). *Lethal Area Description.* Technical Note No. 1510. Ballistic Research Laboratories. Weapon Systems Laboratory.

Nash, J.(1951). Non-Cooperative Games. *The Annals of Mathematics.* https://doi.org/10.2307/1969529

National Public Radio, How Natural Disasters make major cities vulnerable to national security threats, Available on https://www.npr.org/2017/09/10/549989643/how-natural-disasters-make-major-cities-vulnerable-to-national-security-threats, Accessed on May 3, 2020.

National Research Council. (2006). Health risks from Exposure to Low Levels of Ionizing Radiation: BEIR VII Phase 2. In *BEIR VII*. Washington DC: The National Academies Press. https://doi.org/10.17226/11340

National Research Council. (1990*). Health Effects of Exposure to Low Levels of Ionizing Radiation (BEIR V)*. https://doi.org/10.2307/3577873

National Commission on Radiation Protection. (2011*). Responding to a Radiological or Nuclear Terrorism Incident: A Guide for Decision Makers.* NCRP Report No. 166. https://doi.org/10.1088/0952-4746/31/3/b01

Ngo, T., Mendis, P., Gupta, A., & Ramsay, J. (2007). Blast loading and blast effects on structures - An overview. *Electronic Journal of Structural Engineering*, *7* (December), 76–91.

Pita, J., Jain, M., Ordóñez, F., Portway, C., Tambe, M., & Western, C. (2009). Los Angeles Airport Security. AI Magazine, 43–57.

Pomper, M. A., & Tarini, G. (2017). Nuclear terrorism - Threat or not? *AIP Conference Proceedings*, *1898*(November). https://doi.org/10.1063/1.5009230

Pomper, M., Murauskaite, E., & Coppen, T. (2014). *Promoting Alternatives to High-Risk Radiological Sources: The Case of Cesium Chloride in Blood Irradiation* (Issue March). https://www.nonproliferation.org/wp-content/uploads/2014/03/140312_alternative_high_risk_radiological_sources_cesium_chloride_blood.pdf

Rane et al. (2018). Nuclear and Radiological Source Security Culture Assessment of Radiation Users at a University. *Health Phys 115 4 (2018)637-645*.

Reichmuth et al. (2005). *Economic Consequences of a RAD/NUC attack: Cleanup standards significantly affect cost.* R&D Partnerships in Homeland Security. Boston, Ma . https://fas.org/man/eprint/econcon.pdf

Reference USA-a division of info group (2019). *U. S. Businesses* [Data file]. Retrieved from http://resource.referenceusa.com/available-databases/.

Rosoff, H., & von Winterfeldt, D. (2007). A risk and economic analysis of dirty bomb attacks on the ports of Los Angeles and Long Beach. *Risk Analysis*, *27*(3), 533–546. https://doi.org/10.1111/j.1539-6924.2007.00908.x

Rosoff, H & John, R. (2011). Decision Analysis by Proxy for Rational Terrorists. *AAAI Proceedings.* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.159.4749&rep=rep1&type=pdf

Ruby, C. L. (2002). The Definition of Terrorism. *Analyses of Social Issues and Public Policy*. https://doi.org/10.1111/j.1530-2415.2002.00021.x

Schuurman, B. (2018). Research on Terrorism, 2007-2016: A Review of Data, Methods, and Authorship. Terrorism and Political Violence. DOI: 10.1080/095446553.2018.1439023. https://doi.org/10.1080/09546553.2018.1439023

Scott. (1980). Proposed estimates of the probability of inducing pulmonary injury sufficient to cause death from radiation pneumonitis and pulmonary fibrosis after briefly inhaling a mixture of insoluble j8-emitting particles*. *Health Physics*. https://doi.org/10.1097/00004032-198004000-00011

Scott, & Hahn. (1980). A model that leads to the weibull distribution function to characterize early radiation response probabilities. *Health Physics*, *38*(4), 635–642. https://doi.org/10.1097/00004032-198009000-00010

Selten, R. (2001). What Is Bounded Rationality? *Journal of Institutional and Theoretical Economics.* Vol 146, No (4) 649-658.

Shariat, S., Mallonee, S., Chief, M. P. H., & Stidham, S. S. (1998). *Oklahoma City Bombing Injuries*. *1299*(405). www.health.state.ok.us/program/injury

Simon, H. (1957). *Administrative behavior*. Free press, New York.

Sunstein, C. R. (2003). Lives, Life-Years, and Willingness to Pay. *Columbia Law Review*, *104:205*.

Tambe, M., & Jain, M. (2011). Introduction and overview of security games. Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned, 9781107096, 1–24. https://doi.org/10.1017/CBO9780511973031.001

Thomas, J. E. (2016). Benefits of the U.S. Program for Terrorism Insurance from a Comparative Perspective. *SSRN Electronic Journal*, 79–91. https://doi.org/10.2139/ssrn.2779695

The Geneva International Centre for Humanitarian Demining (2017). *Explosive weapon effects overview*. https://www.gichd.org/fileadmin/GICHD-resources/rec-documents/Explosive_weapon_effects_web.pdf

The Guardian (2007) Scientists call for defensive action over radiological attacks, Available at https://www.theguardian.com/science/2007/aug/10/uknews.terrorism, Accessed on 17, April 2020.

The International Atomic Energy Agency. (2005a). *Categorization of Radioactive Sources.* Safety Standards Series No. RS-G-1.9. *IAEA, Safety Guide*, 70. http://www-pub.iaea.org/MTCD/publications/PDF/Pub1227_web.pdf

The International Atomic Energy Agency. (2005b). Development of an extended framework for emergency response criteria. *IAEA-TECDOC-1432*, *January*.

The International Atomic Energy Agency. (2007). *Terminology Used in Nuclear Safety and Radiation Protection*. https://www.iaea.org/publications/7648/iaea-safety-glossary

The International Atomic Energy Agency. (2008). *Nuclear Security Culture: Implementing Guide*. *IAEA Nuclear Security Series*, *7*. https://www.iaea.org/publications/7977/nuclear-security-culture

The International Atomic Energy Agency. (2010). *The Interface Between Safety and Security at Nuclear Power Plants.* International Nuclear Safety Group (INSAG). https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1472_web.pdf.

The International Atomic Energy Agency. (2015). Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control. *Nuclear Security Series*, *24-G* (24). https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1678_web.pdf

The International Atomic Energy Agency (1994*). Intervention criteria in a nuclear or radiation emergency*. Safety Series No. 109. https://www.iaea.org/publications/5159/intervention-criteria-in-a-nuclear-or-radiation-emergency

The International Atomic Energy Agency. (2001). *Code of Conduct on Security and Safety of Radioactive Sources.* https://www.iaea.org/publications/6181/code-of-conduct-on-the-safety-and-security-of-radioactive-sources

The International Commission on Radiation Protection. (1991). *Recommendations of the International Commission on Radiological Protection*. *ICRP Publication 60*. Ann. ICRP 21 (1-3) https://doi.org/10.1016/0720-048x(92)90214-t

The International Commission on Radiation Protection. (2016). *Occupational Intakes of Radionuclides: Part 2, ICRP Publication 134.* Ann. ICRP 45(3/4). https://www.icrp.org/publication.asp?id=ICRP%20Publication%20134.

The International Commission Radiation Protection. (2017). *Occupational Intakes of Radionuclides: Part 3, ICRP Publication 137.* Ann , ICRP *46* (3–4), 1–486. https://doi.org/10.1177/0146645317734963

The International Commission on Radiological Protection. (2009). *Application of the Commission's recommendations to the protection of people living in long-term contaminated areas after a nuclear accident or a radiation emergency*. *ICRP Publication 111.* Ann. ICRP 39(3). https://doi.org/10.1016/j.icrp.2009.09.008

The Organization of Economic Co-operation and Development. (2010). *The Value Of Statistical Life: a Meta-Analysis*. Environment Policy Committee.

The United States Bureau of Labor Statistics (2020). Consumer Price Index for All Urban Consumers: Medical Care in U.S. City Average [CPIMEDSL]. Retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/CPIMEDSL.

The United Nations Scientific Committee on the Effects of Atomic Radiation. (2000*). Sources and Effects of Ionizing Radiation*, Report to the General Assembly, with Scientific Annexes. UNSCEAR 2000 Report. https://doi.org/10.1097/00004032-199907000-00007

The United States Department of the Army. (2011). *Ammunition and Explosives Safety Standards.*

The United States Department of Transportation (2016). Revised Departmental Guidance on Valuation of a Statistical Life in Economic Analysis. Retrieved from https://www.transportation.gov/office-policy/transportation-policy/revised-departmental-guidance-on-valuation-of-a-statistical-life-in-economic-analysis

The United States Department of Homeland Security. (2006). Department of Preparedness Directorate; Protective Action Guides for Radiological Dispersal Device (RDD) and Improvised Nuclear Device (IND) incidents; Notice. *Federal Register*, *71*, 1–24.

The United States Department of Defense. (2009). *Unified Facilities Criteria (UFC): Design of Buildings to Resist Progressive Collapse*, Unified Facilities Criteria (UFC) 4-023-03

The United States Department of Homeland Security. (2015). Presidential Policy Directive 21 Implementation: An interagency security committee white paper. Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper.

The United States Department of Transportation. (2011). Calculation of Safety Clear Zones for Experimental Permits under 14 CFR 437.53(a). *Federal Aviation Administration. Guide No. 437.53-1.* https://www.faa.gov/space/licensing_process/regulations/media/Guide-Cal-of-Safety-Clear-Zones.pdf

The United States Environmental Protection Agency. (1999). Cancer Risk Coefficients for Environmental Exposure to Radionuclides. *EPA 402-R-99-001 FGR*, *13*, 395–415. https://doi.org/10.1201/9780429055362-9

The United States Environmental Protection Agency. (2016). Final Revision to the PAG Manual: Protective Action Guides and Planning Guidance for Radiological Incidents. *Federal Register*, *January*. file:///Files/FE/FE1AA2C8-2B30-4977-889F-9102F3D28B8F.pdf

The United States Government Accountability Office. (2019). Combating nuclear terrorism: NRC needs to take additional actions to ensure the security of high-risk radioactive material. *Key Government Reports. Volume 20: Homeland Security - April 2019*, *April*, 89–142.

The United States. General Services Administration (GSA) (2019). Federal Indiana per diem rates. Retrieved from https://www.gsa.gov/travel/plan-book/per-diem-rates/per-diem-rates lookup/?action=perdiems_report&state=IN&fiscal_year=2020&zip=&city=.

The United States Nuclear Regulatory Commission (1975*). Reactor safety study. An assessment of accident risks in U. S. commercial nuclear power plants. Executive Summary*. WASH-1400, NUREG-75/014. https://doi.org/10.2172/7134131

The United States Nuclear Regulatory Commission (1991). *Standards for Protection Against Radiation.* 10 Code of Federal Regulations Part 20.

The United States Nuclear Regulatory Commission (1993). Health Effects Models for Nuclear Power-Plant Accident Consequence Analysis NUREG/CR-4212, Vol. 56, Issue 4. pbadupws.nrc.gov/docs/ML0500/ML050030192

The United States Nuclear Regulatory Commission. (2015). *Characterizing Explosive Effects on Underground Structures.* NUREG/CR-7201.

https://www.nrc.gov/docs/ML1524/ML15245A640.pdf

The United States Nuclear Regulatory Commission. (1999). *Health Effects of Exposure to Radon*. NUREG CR-4214, Rev 2. https://doi.org/10.17226/5499

The United States Nuclear Regulatory Commission. (2003). *Handbook of Parameter Estimation for Probabilistic Risk Assessment.* NUREG CR-6823.

The United States Nuclear Regulatory Commission, Office of Public Affairs - Backgrounder on Computer Modeling of Severe Accidents, Available at https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/bg-soarca.html, Updated February 25, 2020, Accessed March 18, 2020.

The World Health Organization (2003). *WHO Guide to Cost-Effectiveness Analysis*. https://doi.org/10.2165/00019053-199508050-00001

The White House. "Remarks by President Barack Obama". Office of the Press Secretary. (2009)

Um, V. (2009). Discussing Concepts of Terrorist Rationality: Implications for Counter Terrorism Policy. *Economics of Security Working Paper, No. 22.* German Institute of Economic Research Berlin. https://www.econstor.eu/bitstream/10419/119347/1/diw_econsec0022.pdf

Varian. (1992). *Microeconomic Analysis. Third edition*. W.W. Norton & Company, Inc.

Viscusi, W. K. (2009). Valuing risks of death from terrorism and natural disasters. *Journal of Risk and Uncertainty*. https://doi.org/10.1007/s11166-009-9068-y

Viscusi, W. K., & Aldy, J. E. (2003). The Value of a Statistical Life: A Critical Review of Market Estimates Throughout the World. *Journal of Risk and Uncertainty*, Springer, vol. 27(1), pages 5-76,

Viscusi, W. K., & Masterman, C. J. (2017). Income Elasticities and Global Values of a Statistical Life. *Journal of Benefit-Cost Analysis*. https://doi.org/10.1017/bca.2017.12

Von Neumann, J., & Morgenstern, O. (2007). *Theory of Games and Economic Behavior*. https://doi.org/10.2307/2019327

Wald, A. (1949). Statistical Decision Functions. The Annals of Mathematical Statistics. https://doi.org/10.1214/aoms/1177730030

Wakeford, R., Antell, B. A., & Leigh, W. J. (1998). A review of probability of causation and its use in a compensation scheme for nuclear: Industry workers in the United Kingdom. *Health Physics*, *74*(1), 1–9. https://doi.org/10.1097/00004032-199801000-00001

Wasson, J., & Bluesteen, C. (2017). Cognitive defense: Influencing the target choices of less sophisticated threat actors. *Homeland Security Affairs*.

Watson, J. (2001). *Strategy: An Introduction to Game Theory*. W.W Norton & Company, New York.

Whitehead, D. W., Potter, C. S., & O'Connor, S. L. (2007). Nuclear Power Plant Security Assessment Technical Manual. *Sandia National Lab SAND2007-5591*.

Willis, H. H. (2007). Guiding resource allocations based on terrorism risk. *Risk Analysis*, *27*(3), 597–606. https://doi.org/10.1111/j.1539-6924.2007.00909.x

Willis, H., Morral, A., Kelly, T., & Medby, J. (2018). *Estimating Terrorism Risk*. https://doi.org/10.7249/mg388

World nuclear Association, Safety of Nuclear Power Reactors, Available at https://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/safety-of-nuclear-power-reactors.aspx, Updated June 2019, Accessed March 18, 2020.

Yang, J. E. (2012). Development of an integrated risk assessment framework for internal/external events and all power modes. *Nuclear Engineering and Technology*, *44*(5), 459–470. https://doi.org/10.5516/NET.03.2012.706

Yoo, H., Lee, J., & Kwak, S. (2011). Analysis of Radiological Terrorism on Metropolitan Area. *Energy and Environment Research*, *1*(1), 24–31. https://doi.org/10.5539/eer.v1n1p24

Zimmerman, P. D., & Loeb, C. (2004). Dirty Bombs : The Threat Revisited. *Defense Horizons*, *38*, 1–12.

Žurovec, O., Čadro, S., & Sitaula, B. K. (2017). Quantitative assessment of vulnerability to climate change in rural municipalities of Bosnia and Herzegovina