The Design of a Physical Protection System for the 444TBq $^{60}$Co Irradiation Source at the Centre for Applied Radiation Science and Technology, Mafikeng, South Africa

C. C. Arwui

24860328

Thesis submitted in fulfilment of the requirements for the award of Doctoral of Philosophy Degree in Physics at the Mafikeng Campus of the North-West University

Supervisor: Prof. V.M. Tshivhase

April 2017
DECLARATION

I declare that, except for reference to other researchers work cited, this thesis is my own research and that it has neither in part nor in whole been presented elsewhere for a degree.

Cyrus Cyril Arwui

Date
DEDICATION
This work is dedicated to my wife and children, Mary Rita Arwui, Ruth Arwui and Cyril Mawuenam Arwui Junior, my parents, Francis Korsi Arwui and Elizabeth Geze, my siblings, Bridget Arwui, Cynthia Arwui and Michael Mawunya Arwui.
ACKNOWLEDGEMENT

My first and foremost thanks go to the Almighty God for seeing me through this research successfully. I would like to express my deep and sincere appreciation to all who helped in diverse ways to support my work. In particular, I would like to mention the following; Professor Victor Makondelele Tshivhase, Director (Centre for Applied Radiation Science and Technology of the North-West University), Dr. Rudolph M. Nchodu, iThemba Laboratories for Accelerator Based Sciences, Professor Abdul Shakoor, Directorate of Physical Protection (Pakistan Nuclear Regulator), Dr. Roger Johnston, Founder, CEO, and Chief Vulnerability Wrangler at Right Brain Sekurity, Professor Manny Mathuthu, Deputy Radiation Protection Officer (Centre for Applied Radiation Science and Technology of the North-West University), for their kind support and professional guidance. The encouragement, support and advice from Tebogo Gilbert Kupi, Radiation Protection Officer (Centre for Applied Radiation Science and Technology of the North-West University) are very much appreciated. My sincere gratitude goes to my colleagues Nhlakanipho Wisdom Mdziniso and Kamunda Caspah for their contributions.
TABLE OF CONTENTS

DECLARATION I

DEDICATION II

ACKNOWLEDGEMENT III

TABLE OF CONTENTS IV

LIST OF TABLES VIII

LIST OF FIGURES IX

LIST OF ABBREVIATIONS XIII

ABSTRACT XIII

CHAPTER 1 INTRODUCTION AND BACKGROUND 1
  1.1 Introduction 1
  1.2 Nuclear Security Regime 1
  1.3 Legally Binding International Instruments 9
    1.3.2 Binding Instruments under the Auspices of the United Nations 11
    1.3.3 UN Security Council Resolutions 12
  1.4 Legally Non-Binding International Instruments 12
    1.4.1 Non-Binding Instruments under the auspices of the IAEA 12
    1.4.2 Non-Binding Instruments under the auspices of the United Nations 14
  1.5 Legislative and Regulatory Framework of South Africa concerning Nuclear Security 14
  1.6 Nuclear Security at Public Events 17
  1.7 Physical Protection Regime 19
  1.8 Problem Statement 30
  1.9 Research Aim and Objectives 31
    1.9.1 Aim 31
    1.9.2 Objectives 31

CHAPTER 2 LITERATURE STUDY 33
2.1 Types of Radiation
  - 2.1.1 Alpha particles (α)  
  - 2.1.2 Beta particles (β)  
  - 2.1.3 Gamma rays (γ)  
  - 2.1.4 X-rays  
  - 2.1.5 Neutrons  

2.2 Radiation and Matter  

2.3 Biological Consequences of Exposure to Ionizing Radiation  

2.4 Health Effects
  - 2.4.1 Stochastic Health Effects  
  - 2.4.2 Non-Stochastic or Deterministic Effects  

2.5 Levels of Exposure
  - 2.5.1 Nuclear Radiation Dose Units  

2.6 Cobalt 60  

2.7 Work Done in the Research Field
  - 2.7.1 Categorization of Radioactive Sources  
  - 2.7.2 Design Basis Threat  
  - 2.7.3 Physical Protection Systems  
  - 2.7.4 Security Evaluation Tools  
  - 2.7.5 Security Simulations  
  - 2.7.7 Intrusion Detection Systems  
  - 2.7.8 Vulnerability Assessments  
  - 2.7.9 Cyber Security  
  - 2.7.10 Security Breaches  
  - 2.7.11 Training with Physical Protection System Facilities  
  - 2.7.12 Security Risk Management  

CHAPTER 3 MATERIALS AND METHODS OF INVESTIGATION  

3.1 Materials  

3.1.1 Assessment of Assets  
  - 3.1.2 Source Operation and Specifications  
  - 3.1.3 Pneumatic System  
  - 3.1.4 Engineered Safety Features  

3.2 Methods of Investigation  
  - 3.2.1 Evaluation of Existing Physical Protection Systems  
  - 3.2.2 Assessment of Risk to the Facility  
  - 3.2.3 Assessment of Risk due to the $^{60}$Co irradiation source  
  - 3.2.4 Threat Assessment
3.2.4.1 Types and Tactics of Adversaries 71
3.2.4.2 Capabilities of Adversaries 72
3.2.4.3 Potential Actions and Motivations of Adversaries 74
3.2.5 Design Basis Threat 74
3.2.6 Design of the New PPS 76
3.2.6.1 Detection Stage 77
3.2.6.2 Delay Stage 78
3.2.6.3 Response Stage 80
3.2.7 Functions of the Devices used in the Design 87
3.2.7.1 Balanced Magnetic Switches 87
3.2.7.2 Passive Infrared Sensors 87
3.2.7.3 Closed Circuit Television Cameras 88
3.2.7.4 Duress or Panic Button 89
3.2.7.5 Gamma Radiation Detector 89
3.2.7.6 Arm and Disarm Keypad 89
3.2.7.7 Card Reader with PIN 89
3.2.7.8 Tamper-Indicating Device 90
3.2.7.9 Exit Button 90
3.2.7.10 Acoustic Glass Break Sensors 90
3.2.8 Administrative Procedures with Regards to Safety and Security of the Center 91
3.2.8.1 Center Access 91
3.2.8.2 Key and Access Control System 91
3.2.8.3 Office Security 92
3.2.8.4 Communication 92
3.2.8.5 Information 93
3.2.8.6 Safety 93
3.2.8.7 First Aid 93
3.2.8.8 Fire 94
3.2.8.9 Accidents and Incidents at Work Place 94
   a. Incident and Accident reporting procedure 95
   b. Incident and Accident reporting Investigations 95
3.2.9 Evaluation of the New PPS 95
3.2.9.1 Use of Location Variable in EASI 97
3.2.9.2 Examples Explaining the Use of B, M and E in EASI 97
3.2.10 Adversary Sequence Diagrams 98

CHAPTER 4 DATA ANALYSIS AND RESULTS 101
4.1 Risk to the Center 101
4.2 Risk due the $^{60}$Co Irradiation Source 101
4.3 Response Force Time and Task Times with corresponding Mean and Standard Deviation Values 103
4.4 Evaluation Results of EASI Code 108
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.5 Evaluation Results from the EASIM Code</td>
<td>135</td>
</tr>
<tr>
<td>CHAPTER 5 DISCUSSIONS</td>
<td>167</td>
</tr>
<tr>
<td>5.1 Discussions of Results</td>
<td>167</td>
</tr>
<tr>
<td>CHAPTER 6 CONCLUSIONS AND RECOMMENDATIONS</td>
<td>174</td>
</tr>
<tr>
<td>6.1 Conclusions</td>
<td>174</td>
</tr>
<tr>
<td>6.2 Recommendations</td>
<td>175</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>177</td>
</tr>
<tr>
<td>APPENDICES</td>
<td>188</td>
</tr>
</tbody>
</table>
**LIST OF TABLES**

Table 3.1: The list of assets located in the three buildings of the Center .................................. 62
Table 3.2: Selected crimes committed in Mafikeng and Mmabatho in 2013 ............................ 69
Table 3.3: Selected crimes committed in Mafikeng and Mmabatho in 2014 ............................. 70
Table 3.4: Selected crimes committed in Mafikeng and Mmabatho in 2015 ............................. 71
Table 3.5: Symbols and description in proposed PPS ................................................................. 86

Table 4.1: Calibration radioactive source materials with their activities and other reference values .......................................................................................................................................... 103
Table 4.2: Practical action times.................................................................................................. 104
Table 4.3: Range of action times required to perform a task...................................................... 105
Table 4.4: Mean and standard deviation values of response force time (RFT)......................... 106
Table 4.5: Mean and standard deviation values of adversary delay time (Tdelay) ...................... 107
Table 4.6: Adversary paths and their $P_t$, $P_N$ and $P_E$ values for the proposed PPS design for building F2C using EASI (sabotage scenario) ................................................................. 155
Table 4.7: Adversary paths and their $P_t$, $P_N$ and $P_E$ values of the proposed PPS design for building F2C using EASI (theft scenario) ................................................................. 156
Table 4.8: Adversary paths and their $P_t$, $P_N$ and $P_E$ values of the implementation by GTRI for building F2C using EASI (sabotage scenario) ................................................................. 157
Table 4.9: Adversary paths and their $P_t$, $P_N$ and $P_E$ values of the implementation by GTRI for building F2C using EASI (theft scenario) ................................................................. 158
Table 4.10: Adversary paths and their $P_t$, $P_N$ and $P_E$ values of the proposed PPS design for building F2A using EASI (theft scenario) ................................................................. 159
Table 4.11: Adversary paths and their $P_t$, $P_N$ and $P_E$ values of the proposed PPS design for building F2E using EASI (theft scenario) ................................................................. 159
Table 4.12: Multiple adversary pathways and their $P_t$, $P_N$ and $P_E$ values of the proposed PPS design for building F2C using EASIM (sabotage scenario) ..................................................... 160
Table 4.13: Multiple adversary pathways and their $P_t$, $P_N$ and $P_E$ values of the proposed PPS design for building F2C using EASIM (theft scenario) ..................................................... 160
Table 4.14: Multiple adversary pathways and their $P_t$, $P_N$ and $P_E$ values of the implementation by GTRI for building F2C using EASIM (sabotage scenario) ..................................................... 161
Table 4.15: Multiple adversary pathways and their $P_t$, $P_N$ and $P_E$ values of the implementation by GTRI for building F2C using EASIM (theft scenario) ..................................................... 161
Table 4.16: Multiple adversary pathways and their $P_t$, $P_N$ and $P_E$ values of the proposed PPS design for building F2A using EASIM (theft scenario) ..................................................... 162
Table 4.17: Multiple adversary pathways and their $P_t$, $P_N$ and $P_E$ values of the proposed PPS design for building F2E using EASIM (theft scenario) ..................................................... 162
LIST OF FIGURES

Figure 2.1: A summarized picture showing the penetrating power of alpha particles, beta particles and gamma rays [15] ..................................................................................................... 35
Figure 2.2: Ionization process that removes an electron from the atom leaving it positively charged [15] .................................................................................................................................. 37
Figure 2.3: Average radiation exposure from all sources ................................................................................................................................. 41
Figure 2.4: Decay scheme of Cobalt – 60. ........................................................................................................................................... 42
Figure 3.1: Google map showing the layout of the North-West University (NWU) .......................................................... 59
Figure 3.2: Floor plan of building F2C at CARST ................................................................................................................................. 60
Figure 3.3: Floor plan of building F2E at CARST ................................................................................................................................. 60
Figure 3.4: Floor plan of building F2A at CARST ................................................................................................................................. 61
Figure 3.5: Flow diagram for the steps in the methodology ...................................................................................................................... 61
Figure 3.6: Eldorado 78 60Co package at storage facility awaiting preparation for transport . .................................................................................. 64
Figure 3.7: Eldorado 78 60Co package description ........................................................................................................................................... 64
Figure 3.8: An example of hand-held and power tools that can be used to attack security and facilities ....................................................................................................................................... 73
Figure 3.9: Proposed PPS design for F2C irradiation facility ......................................................................................................................... 82
Figure 3.10: Proposed PPS design for building F2E ........................................................................................................................................ 83
Figure 3.11: Proposed PPS design for building F2A ........................................................................................................................................ 84
Figure 3.12: Proposed design of the inner burglar gate for all buildings ........................................................................................................... 85
Figure 3.13: ASD showing different adversary paths for the CARST buildings ............................................................................................. 99
Figure 3.14: ASD showing different adversary paths for Building F2C ................................................................................................. 100
Figure 3.15: ASD showing the functional protection elements for building F2C ................................................................................................. 100
Figure 4.1: Theft evaluation result for building F2C and path 1C ........................................................................................................... 108
Figure 4.2: Theft evaluation result for building F2A and path 1A ........................................................................................................... 108
Figure 4.3: Theft evaluation result for building F2E and path 1E ........................................................................................................... 108
Figure 4.4: Sabotage evaluation result for path 1C ................................................................................................................................. 109
Figure 4.5: Sabotage evaluation result for path 2C ................................................................................................................................. 109
Figure 4.6: Sabotage evaluation result for path 3C ................................................................................................................................. 109
Figure 4.7: Sabotage evaluation result for path 4C ................................................................................................................................. 110
Figure 4.8: Sabotage evaluation result for path 5C ................................................................................................................................. 110
Figure 4.9: Sabotage evaluation result for path 6C ................................................................................................................................. 110
Figure 4.10: Sabotage evaluation result for path 7C ................................................................................................................................. 111
Figure 4.11: Sabotage evaluation result for path 8C ................................................................................................................................. 111
Figure 4.12: Sabotage evaluation result for path 9C ................................................................................................................................. 111
Figure 4.13: Sabotage evaluation result for path 10C ................................................................................................................................. 112
Figure 4.14: Sabotage evaluation result for path 11C ................................................................................................................................. 112
Figure 4.15: Sabotage evaluation result for path 13C ................................................................................................................................. 113
Figure 4.16: Sabotage evaluation result for path 14C ................................................................................................................................. 113
Figure 4.17: Theft evaluation result for path 1C ................................................................................................................................. 113
Figure 4.18: Theft evaluation result for path 2C ................................................................................................................................. 114
Figure 4.19: Theft evaluation result for path 3C ................................................................................................................................. 114
Figure 4.20: Theft evaluation result for path 4C ................................................................................................................................. 115
Figure 4.21: Theft evaluation result for path 5C ................................................................................................................................. 115
Figure 4. 22: Theft evaluation result for path 6C ................................................................. 115
Figure 4. 23: Theft evaluation result for path 7C ................................................................. 115
Figure 4. 24: Theft evaluation result for path 8C ................................................................. 116
Figure 4. 25: Theft evaluation result for path 9C ................................................................. 116
Figure 4. 26: Theft evaluation result for path 10C .............................................................. 116
Figure 4. 27: Theft evaluation result for path 11C .............................................................. 117
Figure 4. 28: Theft evaluation result for path 12C .............................................................. 117
Figure 4. 29: Theft evaluation result for path 13C .............................................................. 117
Figure 4. 30: Theft evaluation result for path 14C .............................................................. 118
Figure 4. 31: Sabotage evaluation result of GTRI for path 1C .......................................... 118
Figure 4. 32: Sabotage evaluation result of GTRI for path 2C .......................................... 118
Figure 4. 33: Sabotage evaluation result of GTRI for path 3C .......................................... 119
Figure 4. 34: Sabotage evaluation result of GTRI for path 4C .......................................... 119
Figure 4. 35: Sabotage evaluation result of GTRI for path 5C .......................................... 119
Figure 4. 36: Sabotage evaluation result of GTRI for path 6C .......................................... 120
Figure 4. 37: Sabotage evaluation result of GTRI for path 7C .......................................... 120
Figure 4. 38: Sabotage evaluation result of GTRI for path 8C .......................................... 120
Figure 4. 39: Sabotage evaluation result of GTRI for path 9C .......................................... 121
Figure 4. 40: Sabotage evaluation result of GTRI for path 10C ........................................ 121
Figure 4. 41: Sabotage evaluation result of GTRI for path 11C .......................................... 121
Figure 4. 42: Sabotage evaluation result of GTRI for path 13C ........................................ 122
Figure 4. 43: Sabotage evaluation result of GTRI for path 14C ........................................ 122
Figure 4. 44: Theft evaluation result of GTRI for path 1C .................................................. 122
Figure 4. 45: Theft evaluation result of GTRI for path 2C .................................................. 123
Figure 4. 46: Theft evaluation result of GTRI for path 3C .................................................. 123
Figure 4. 47: Theft evaluation result of GTRI for path 4C .................................................. 123
Figure 4. 48: Theft evaluation result of GTRI for path 5C .................................................. 124
Figure 4. 49: Theft evaluation result of GTRI for path 6C .................................................. 124
Figure 4. 50: Theft evaluation result of GTRI for path 7C .................................................. 124
Figure 4. 51: Theft evaluation result of GTRI for path 8C .................................................. 125
Figure 4. 52: Theft evaluation result of GTRI for path 9C .................................................. 125
Figure 4. 53: Theft evaluation result of GTRI for path 10C ............................................... 125
Figure 4. 54: Theft evaluation result of GTRI for path 11C ............................................... 126
Figure 4. 55: Theft evaluation result of GTRI for path 12C ............................................... 126
Figure 4. 56: Theft evaluation result of GTRI for path 13C ............................................... 126
Figure 4. 57: Theft evaluation result of GTRI for path 14C ............................................... 127
Figure 4. 58: Theft evaluation result for path 1A .............................................................. 127
Figure 4. 59: Theft evaluation result for path 2A .............................................................. 128
Figure 4. 60: Theft evaluation result for path 3A .............................................................. 128
Figure 4. 61: Theft evaluation result for path 4A .............................................................. 128
Figure 4. 62: Theft evaluation result for path 5A .............................................................. 129
Figure 4. 63: Theft evaluation result for path 6A .............................................................. 129
Figure 4. 64: Theft evaluation result for path 7A .............................................................. 129
Figure 4. 65: Theft evaluation result for path 8A .............................................................. 130
Figure 4. 66: Theft evaluation result for path 9A .............................................................. 130
Figure 4. 67: Theft evaluation result for path 10A ............................................................ 130
Figure 4. 68: Theft evaluation result for path 1E. ................................................................. 131
Figure 4. 69: Theft evaluation result for path 2E. ................................................................. 131
Figure 4. 70: Theft evaluation result for path 3E. ................................................................. 131
Figure 4. 71: Theft evaluation result for path 4E. ................................................................. 132
Figure 4. 72: Theft evaluation result for path 5E. ................................................................. 132
Figure 4. 73: Theft evaluation result for path 6E. ................................................................. 132
Figure 4. 74: Theft evaluation result for path 7E. ................................................................. 133
Figure 4. 75: Theft evaluation result for path 8E. ................................................................. 133
Figure 4. 76: Theft evaluation result for path 9E. ................................................................. 133
Figure 4. 77: Theft evaluation result for path 10E. ............................................................... 134
Figure 4. 78: Theft evaluation result for building F2C and pathways 1-2-3C. ....................... 135
Figure 4. 79: Theft evaluation result for building F2A and pathways 1-2-6A ....................... 136
Figure 4. 80: Theft evaluation result for building F2E and pathways 1-2-3E ....................... 136
Figure 4. 81: Sabotage evaluation result for pathways 1-2-3C. ............................................ 137
Figure 4. 82: Sabotage evaluation result for pathways 1-4-14C. ......................................... 137
Figure 4. 83: Sabotage evaluation result for pathways 3-8-13C. ......................................... 138
Figure 4. 84: Sabotage evaluation result for pathways 4-5-6C. ......................................... 138
Figure 4. 85: Sabotage evaluation result for pathways 7-8-5C. ......................................... 139
Figure 4. 86: Sabotage evaluation result for pathways 10-11-13C. ..................................... 139
Figure 4. 87: Theft evaluation result for pathways 1-2-3C. ................................................ 140
Figure 4. 88: Theft evaluation result for pathways 1-4-14C. .............................................. 140
Figure 4. 89: Theft evaluation result for pathways 4-5-6C. ............................................... 141
Figure 4. 90: Theft evaluation result for pathways 7-8-5C. ............................................... 141
Figure 4. 91: Theft evaluation result for pathways 9-10-12C. .......................................... 142
Figure 4. 92: Theft evaluation result for pathways 11-8-13C. .......................................... 142
Figure 4. 93: Sabotage evaluation result of GTRI for pathways 1-2-3C. ............................ 143
Figure 4. 94: Sabotage evaluation result of GTRI for pathways 1-4-14C. ......................... 143
Figure 4. 95: Sabotage evaluation result of GTRI for pathways 3-8-13C. ......................... 144
Figure 4. 96: Sabotage evaluation result of GTRI for pathways 4-5-6C. ............................ 144
Figure 4. 97: Sabotage evaluation result of GTRI for pathways 7-8-5C. ........................... 145
Figure 4. 98: Sabotage evaluation result of GTRI for pathways 10-11-13C. ...................... 145
Figure 4. 99: Theft evaluation result of GTRI for pathways 1-2-3C. ................................ 146
Figure 4. 100: Theft evaluation result of GTRI for pathways 1-4-14C. ............................. 146
Figure 4. 101: Theft evaluation result of GTRI for pathways 4-5-6C. ................................ 147
Figure 4. 102: Theft evaluation result of GTRI for pathways 7-8-5C. ................................ 147
Figure 4. 103: Theft evaluation result of GTRI for pathways 9-10-12C. ......................... 148
Figure 4. 104: Theft evaluation result of GTRI for pathways 11-8-13C. ........................... 148
Figure 4. 105: Theft evaluation result for pathways 1-2-6A. ........................................... 149
Figure 4. 106: Theft evaluation result for pathways 2-5-1A. ........................................... 149
Figure 4. 107: Theft evaluation result for pathways 3-6-8A. ........................................... 150
Figure 4. 108: Theft evaluation result for pathways 3-7-9A. ........................................... 150
Figure 4. 109: Theft evaluation result for pathways 4-5-9A. ........................................... 151
Figure 4. 110: Theft evaluation result for pathways 4-9-10A. ......................................... 151
Figure 4. 111: Theft evaluation result for pathways 1-2-3E. ............................................ 152
Figure 4. 112: Theft evaluation result for pathways 2-5-10E. ......................................... 152
Figure 4. 113: Theft evaluation result for pathways 3-7-9E. ............................................ 153
Figure 4.114: Theft evaluation result for pathways 4-5-6E...................................................... 153
Figure 4.115: Theft evaluation result for pathways 4-6-10E...................................................... 154
Figure 4.116: Theft evaluation result for pathways 7-8-9E...................................................... 154
Figure 4.117: Adversary paths and their $P_E$ values for a lower RFT using EASI – sabotage scenario for building F2C study and implementation by GTRI. .................................................. 163
Figure 4.118: Adversary paths and their $P_E$ values for a lower RFT using EASI – theft scenario for building F2C study and implementation by GTRI............................................................... 163
Figure 4.119: Adversary paths and their $P_E$ values for a lower RFT using EASI – theft scenario for building F2A. ........................................................................................................................ 164
Figure 4.120: Adversary paths and their $P_E$ values for a lower RFT using EASI – theft scenario for building F2E ................................................................................................................. 164
Figure 4.121: Adversary pathways and their $P_E$ values for a lower RFT using EASIM – sabotage scenario for building F2C study and implementation by GTRI. ................................................. 165
Figure 4.122: Adversary pathways and their $P_E$ values for a lower RFT using EASIM – theft scenario for building F2C study and implementation by GTRI............................................................... 165
Figure 4.123: Adversary pathways and their $P_E$ values for a lower RFT using EASIM – theft scenario for building F2A .................................................................................................................. 166
Figure 4.124: Adversary pathways and their $P_E$ values for a lower RFT using EASIM – theft scenario for building F2E ................................................................................................................. 166

Figure 5: 1: EASI $P_E$ values of the existed PPS, the proposed PPS and the GTRI ..................... 169
Figure 5: 2: EASI $P_E$ values for the existed PPS and the proposed PPS for buildings F2A and 170
Figure 5: 3: EASIM $P_E$ values of the existed PPS, the proposed PPS and the GTRI.............. 171
Figure 5: 4: EASIM $P_E$ values for the existed PPS and the proposed PPS for buildings F2A ... 172
LIST OF ABBREVIATIONS

ASSESS  Analytical System and Software for the Evaluation of Safeguards and Security
CPPNM  Convention on the Physical Protection of Nuclear Materials and Nuclear Facilities
TECDOC  Technical Document
IPPAS  International Physical Protection Advisory Service
CARST  Centre for Applied Radiation Science and Technology
IAEA  International Atomic Energy Agency
SAVI  System Analysis of Vulnerability to Intrusion
EASI  Estimate of Adversary Sequence Interruption
SAPE  System Analysis of Physical Protection Effectiveness
PPS  Physical Protection System
DBT  Design Basis Threat
NRC  Nuclear Regulatory Commission
IDS  Intrusion Detection System
VDI  Vulnerability Disclosure Index
EPR  Emergency Preparedness and Response
PIR  Passive Infra-Red
RFT  Response Force Time
MOU  Memorandum of Understanding
ASD  Adversary Sequence Diagram
PC  Probability of Communication
PD  Probability of Detection
NM  Nuclear Material
RDD  Radiological Dispersal Device
RED  Radiological Exposure Device
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IND</td>
<td>Improvised Nuclear Device</td>
</tr>
<tr>
<td>POE</td>
<td>Points of Entry</td>
</tr>
<tr>
<td>RPM</td>
<td>Radiation Portal Monitor</td>
</tr>
<tr>
<td>PRD</td>
<td>Personal Radiation Detector</td>
</tr>
<tr>
<td>PRS</td>
<td>Portable Radiation Scanner</td>
</tr>
<tr>
<td>NPT</td>
<td>Non-Proliferation Treaty</td>
</tr>
<tr>
<td>RID</td>
<td>Radionuclide Identification Device</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logical Controller</td>
</tr>
<tr>
<td>ITDB</td>
<td>Incident Trafficking Database</td>
</tr>
</tbody>
</table>
ABSTRACT
The accelerated technological change experienced by the world at the outset of the twenty-first century including technologies used in the nuclear field can pose serious risks to public health, property and the environment if not controlled and handled appropriately. Nuclear and other radioactive materials are being used in a growing variety of settings to advance development in most Countries. In total there are approximately 17,500 registered radioactive sources in South Africa and these sources need to be protected against adversaries coupled with several cases of infiltration of the Pelindaba nuclear research facility outside Pretoria means there should be a robust nuclear security regime put in place. This study designed a physical protection system (PPS) for the $^{60}$Co irradiation source which will be used at the Centre for Applied Radiation Science and Technology (CARST) of the North-West University (Mafikeng Campus). The PPS effectiveness was analyzed and evaluated quantitatively by the use of the Estimate of Adversary Sequence Interruption (EASI) code and the Estimation of Adversary Sequence Interruption for Multiple Pathways (EASIM) code. These evaluations were done to calculate the Probability of effectiveness ($P_E$) from the Probability of Interruption ($P_I$) and the Probability of Neutralization ($P_N$) of a potential adversary attack scenario along a specific path for the EASI code and along multiple pathways simultaneously for the EASIM code. The $P_E$ values show the extent to which the security system is effective.

Results obtained from this study indicated low values of $P_E$ for the existing protection system and high values of $P_E$ for the proposed physical protection system design. This increase in the $P_E$ value indicates a potentially higher overall level of security for the proposed PPS of the center consisting of three buildings namely F2C, F2A and F2E. The effectiveness of the proposed PPS for the proposed paths increased from zero (0) to a minimum of 0.50 and a maximum of 0.80 for sabotage scenario of F2C and a minimum of 0.50 and a maximum of 0.85 for theft scenario of F2C, F2A and F2E. The EASIM code’s results increased from zero (0) to a minimum of 0.55 and a maximum of 0.69 for sabotage scenario of F2C and a minimum of 0.54 to a maximum of 0.80 for theft scenario of F2C, F2A and F2E, thus indicating an increased level of overall effectiveness for the proposed PPS.
CHAPTER 1 Introduction and background

This chapter gives a concise explanation of the research work carried out. It includes the background, problem statement, aims, objectives, scope and relevance of the research work.

1.1 Introduction

Nuclear security is defined by the International Atomic Energy Agency (IAEA) as the measures put in place for the prevention, detection of and response to theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive material or their associated facilities and activities [1]. IAEA has grouped nuclear security risks into four potential categories which include the theft of a nuclear weapon, construction of nuclear explosive devices through unauthorized acquisition of nuclear materials, use of radioactive sources including dirty bombs maliciously and radiological hazards caused by the attack on, or the sabotage of a facility or a transport vehicle [2]. Out of these four nuclear security risks, only the last two are relevant to this research work.

In the day-to-day management of nuclear technologies and nuclear applications where nuclear material or other radioactive material are used or transported, nuclear security becomes a fundamental element. The provision of security for nuclear material and other radioactive material and their associated facilities and activities is the sole responsibility of every individual State. Each State has the task of ensuring the security of such material in use, storage, or in transport. The State also needs to combat illicit trafficking and the inadvertent movement of such material, and also to be prepared to respond to a nuclear security event. To be able to provide adequate security there is the need to establish, maintain and sustain an effective nuclear security regime appropriate to the relevant State [3].

1.2 Nuclear Security Regime

In the first stage, the nuclear security regime of a state should consist of legislative and regulatory framework, administrative systems and measures that govern the security of nuclear material or other radioactive material and their associated facilities and associated activities. The second stage should be made up of the institutions and organizations which will be responsible
for ensuring the implementation of the legislative and regulatory framework together with the administrative systems of nuclear security within the State. Thirdly, the regime should include nuclear security systems and measures for the prevention of, detection of and response to nuclear security events [3]. A nuclear security regime should have the objectives to protect against unauthorized removal of radioactive material used in associated facilities and in activities, and to protect against sabotage of other radioactive material. It should ensure the implementation of measures to locate and recover radioactive material which is lost, missing or stolen and to re-establish regulatory control rapidly and comprehensively to prevent harmful consequences of a nuclear security event [4]. These objectives can only be realized through security measures that deter, detect, delay and respond to an act that is potentially malicious, while allowing the use of radioactive material and associated facilities and activities in a safe and secure manner. The security measures in place should be based on a risk-informed graded approach so that security is provided for radioactive material corresponding to the level of potential radiological consequences it may produce arising from their use in a malicious act [4]. A graded approach is used to provide higher levels of protection against events that could result in higher consequences or that have lower consequences but high probabilities of occurring. In the case of unauthorized removal, the State should consider categorizing of nuclear material in order to ensure the appropriate relationship between the nuclear material of concern and the physical protection measures implemented. Threshold(s) of unacceptable radiological consequences should be established by the State in order to determine appropriate levels of physical protection. Existing nuclear safety and radiation protection should be taken into account in the event of selecting protection measures against sabotage [5]. These measures should use the concept of defence in depth in their operations.

The three physical protection functions of detection, delay, and response should each use defense in depth, and apply a graded approach to provide the appropriate levels of protection. Defense-in-depth should take into account the capability of the physical protection system and the system for nuclear material accountancy and control to protect against insiders and external threats, as well as insiders cooperating with external actors [5]. The State’s requirements for physical protection should reflect a concept of several layers and methods of protection (structural, technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve his objectives [4]. Other elements and activities of a nuclear
security regime are intelligence gathering, assessment of the threat to radioactive material and associated locations and facilities, vulnerability assessments, security evaluations and testing, the use of various technical hardware systems, response capabilities and the mitigation of unauthorized activities. These elements cannot be addressed in isolation by any single government or industrial organization or subsection of such an organization [6].

The nuclear security regime should cover nuclear material and other radioactive material, whether it is under or out of regulatory control, as well as associated facilities and associated activities throughout their lifetimes. It should reflect the risk of harm to persons, property, the organization, the government, society and the environment. For a national nuclear security regime to be effective it should be built on the implementation of relevant international legal instruments, information protection, physical protection, material accounting and control, detection of and response to trafficking in such material as well as a national response plan with complete contingency measures [3]. In maintaining and sustaining the nuclear security regime, personal dedication, accountability and understanding by all individuals engaged in any activity which has a bearing on the security of nuclear activities is needed. These attributes of individuals working in the nuclear sector can be best described as effective nuclear security culture which depends on proper planning, training, personnel selection, awareness, operation and maintenance, as well as on people who plan, operate and maintain nuclear security systems. Well-designed systems are vulnerable to degradation if the procedures necessary to operate and maintain them are poor, or if the operators fail to follow procedures, or if the personnel who are supposed to follow the procedures are not motivated or educated to do so. Thus, the entire nuclear security regime stands or falls because of the people involved and their leaders, and it is the human factor, including management leadership and insider threat mitigation, that must be addressed in any effort to enhance the existing nuclear security culture which will, in turn, enhance the nuclear security regime [6].

The legislative arm of government needs to establish competent authorities such as regulatory bodies (mentioned earlier), authorities related to border control, law enforcement and any authority deemed fit by the State with specific and well-demarcated responsibilities by law. These authorities must be given adequate legal power and sufficient financial, human and
technical resources to be able to fulfill their assigned nuclear security responsibilities through proper coordination and communication. The regulatory body established by law to regulate the activities of the institutions and companies using nuclear material, other radioactive materials and their associated facilities and associated activities should be independent of any interference in their nuclear security decision making. Independence here means functionally and financially independent from the entities or institutions they regulate and from any other bodies that deal with the promotion or utilization of nuclear material or other radioactive material so as not to influence the regulatory body’s judgement [3]. The regulatory body should have the mandate to implement the legislative and regulatory framework of nuclear security and authorize activities only when they comply with its nuclear security regulations.

Computer security should be incorporated in general terms into the legal or legislative and regulatory framework for nuclear security. Adequate implementations of the legislative and regulatory frameworks can potentially have a major impact on the safety and security of nuclear facilities. In connection with the computer security, the State’s legal system should at least provide the legislative and regulatory framework that covers protection of sensitive information and addresses any activity that might precipitate breaches of nuclear security. Computer security with its specific issues like cyber security may need special legislative provisions to take into account the unique crimes and modes of operation associated with computer systems which undergo technological changes always in their operations.

Current legislation of States should be carefully considered as to whether they are adequate to cover malicious acts that may be perpetrated with the aid of computers [7]. The regulatory body should demand from operators or managers of facilities that they develop, implement, test, periodically review, and revise as necessary a security plan and comply strictly with its provisions. There should be detailed description of the overall nuclear security system in place in the plan to protect the radioactive material and associated facilities including measures to address an increased threat level, response to nuclear security events and protect sensitive information. The regulatory body can use the information in the security plan of operators and facilities, along with on-site inspections in its determination of issuing authorization [4]. Verification of continued compliance should be done by the regulatory body with nuclear security regulations.
and relevant authorization conditions through periodic inspections, ideally including unannounced inspections and ensuring that corrective actions are taken. Where needed, requirements for operators, shippers and/or carriers to have appropriate and effective security measures to detect nuclear security events and to report any such event promptly with the aim of providing a timely response should be established by the regulatory body. Operators or managers of facilities should be required to implement a security system that meets applicable nuclear security regime objectives. The system should be designed to adequately perform the security functions of detection, delay, and response in order to provide countermeasures to malicious acts [4].

Law enforcement and border control authorities should establish law enforcement systems, procedures and measures relevant to nuclear security. These should be for the export, import, and border control of nuclear material and other radioactive material. Security procedures for transport should also be consistent with international transport regulations. If there are violations of the State’s laws or regulations, punishments which are proportionate to the gravity of the harm that will be caused or would have been caused by these acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities should be instituted [3].

Designated border control authorities acting on behalf of the State should take appropriate steps which include coordination between States where imports and exports are done prior to the transfer, to reduce the likelihood of malicious acts in connection with the importer or exporter of quantities of radioactive material above thresholds that are defined by the IAEA [4]. The nuclear security regime should ensure that nuclear security threats and credibility of the threat, both internal and external to the State, are identified and assessed, regardless of whether the targets of nuclear security threats are within or outside the State’s jurisdiction. The nuclear security regime should also incorporate measures for protecting people at major public events held in the State such as a sporting contest or high level political meeting which might present unique security challenges. Nuclear and other radioactive material used with criminal or terrorist intent, during or targeting such events, poses serious threats [8].
For sustainability of the regime all competent authorities, authorized persons and all organizations with nuclear security responsibilities should be involved in developing, implementing and maintaining appropriate and effective integrated management systems which include quality management systems, as well as internal and external critical security assessments, and demonstration of good leadership in nuclear security matters at the highest levels.

There should also be development, fostering and maintenance of a robust nuclear security culture with sufficient allocation of financial, human and technical resources to organizations to carry out their nuclear security responsibilities on a continuous basis with the use of a structured risk management informed approach [3]. The structured risk management approach identified should be used to reduce the risks of malicious or inadvertent acts to an acceptable level and needs to be followed to the letter. The State should consider reducing the security risk associated with radioactive material, particularly radioactive sources, by encouraging the use of alternative radionuclides, alternate chemical forms, or non-radioactive technology. The State should also encourage designing radioactive devices used in facilities that are more tamper resistant [4]. Risk management is very relevant at all stages of the life cycle of any facility’s systems such as design, development, operations and maintenance [7]. Maintenance, training, and evaluation should be routinely conducted by competent personnel to ensure the effectiveness of the nuclear security systems and have in place processes for using best practices and lessons learned from their experience from the nuclear security field.

The authorities should establish and apply measures to minimize the possibility of insiders (workers within facilities) becoming nuclear security threats either deliberately or inadvertently and routinely perform quality assurance, vulnerability assessments, and other assessment activities to identify and address the issues and factors that may affect the capacity to provide adequate nuclear security including cyber security at all times [3]. In the event that nuclear material and other radioactive material are out of regulatory control, the state should have a comprehensive and complete set of specific legislative provisions to provide relevant administrative and enforcement powers in order for the various competent authorities to be able to undertake their activities in an effective manner. Again sufficient and sustained
resources should be provided to the various competent authorities to enable them to carry out their assigned functions which include preventing a criminal act or an unauthorized act with nuclear security implications involving nuclear and other radioactive material out of regulatory control. These administrative and enforcement powers should also enable them to detect through an instrument alarm and/or an information alert system of the presence or indications of a criminal act or an unauthorized act with nuclear security implications involving nuclear or other radioactive material that are out of regulatory control in particular. In order to achieve these aims, a national detection strategy needs to be developed to establish detection systems and perform initial assessments of the instrument alarms and/or information alerts promptly to ascertain the occurrence of a nuclear security event [9]. To respond to a nuclear security event, competent authorities identified by the State’s legislative arm of government to deal with nuclear security issues should be informed early after any suspicion that there is a criminal act or unauthorized act with respect to nuclear security consequences. This will enable the authorities to respond quickly to assess and validate the potential consequences of the said event and to locate, identify, categorize and characterize nuclear and other radioactive material involved and secure such material in the application of other response measures appropriate to the nuclear security event, such as neutralization of the device. The authorities will be required to recover, detain and/or seize such material and again place under regulatory control. Evidence should be collected, preserved, stored, transported and analyzed including the application of nuclear forensics measures, related to a criminal act, or an unauthorized act, with nuclear security implications that involves such material and finally apprehend and subsequently prosecute or extradite alleged offenders [9].

States should consider using nuclear forensics to assist designated authorities in order to determine the origin and history of seized material; this may contribute to deterring criminal or unauthorized acts involving nuclear or other radioactive material. Nuclear forensics is also an important element of the response measures [9].

Another nuclear security risk relates to the issue of illicit trafficking of nuclear material and other radioactive material which are transported by public postal system through both national and international mail. States need to put in place a radiation monitoring system in vital locations
where mail is been transported to detect any illicit trafficking. In the process of implementing a public mail radiation monitoring system, there should be good understanding and preparation of the legal, practical and economic factors. Issues to be considered include the establishment of a legal basis for the public mail monitoring, defining the responsible authority, contracting a project management team and defining and implementing the mail monitoring projects [10]. Studies conducted on the field have demonstrated that effective radiation monitoring cannot be guaranteed without proper training of the responsible supervisors and staff, even with the highest quality of equipment installed [11]. Adequate training on radiation protection basics should be given to the emergency response team, the responsible managers, postal supervisors, and workers for their own safety and that of the public. This training should include appropriate theoretical lectures and practical exercises. The planning of the training and its periodic revision should be described in the response plan of the postal organization. It is also advisable to include this training in other existing emergency training structures [10]. This training should include exactly what to do in the event that a nuclear material or other radioactive materials and their associated devices are found in national or international mail. The following steps should be discussed by the training for radiation protection purposes: Objects suspected should not be touched; there should be an evacuation of the immediate area and prevention of access to the object; the maximum practical distance should be kept between the people and the object; regulatory authorities should be notified, as well as emergency services and other competent authorities [12].

The security environment poses extraordinary challenges nationally and internationally for the prevention of the spread of nuclear weapons and materials. There are suspicions that a number of armed non-state actors are actively seeking to acquire nuclear weapons or the material and the technology required to produce them. In addition, the rate of expansion of nuclear technology, as well as the development of civilian nuclear energy capacity, will in future pose an increased challenge to non-proliferation efforts [13]. Even though these challenges exist, many African countries have improved substantially over the past 15 years, in nuclear security, largely due to the development of national strategies and increased international cooperation in the field. According to Bunn [14] as of April 2010, 17 countries have eliminated all of the weapons-usable nuclear material on their soil.
Despite recent advances, global nuclear security is still inadequate and a major nuclear security incident would have far-reaching consequences and therefore effective nuclear security must be a global concern. While the overall responsibility for nuclear security within a State rests entirely with that State, the need for regional and international cooperation has become increasingly necessary with the growing recognition that, countering the threats to nuclear security within one State will depend on the adequacy and effectiveness of nuclear security measures taken by other States, particularly when nuclear material and other radioactive material are transported between countries [1]. A single incident or series of apparently isolated incidents within a State may provide valuable information to assess security threats beyond the boundaries of that State. Such information will help authorities in other States to identify and apprehend traffickers elsewhere. In the event of nuclear and other radioactive material being offered for illegal sale, information from such transactions will go a long way to enable both national and international bodies to assess whether activities of such material poses a significant security threat, and can help identify potential buyers, their capabilities and their motives [15]. Since illicit trafficking and theft of nuclear material can lead to nuclear proliferation and the possible construction of improvised nuclear devices (IND) or radiological dispersal and exposure devices (REDs), measures to detect and respond to such acts are essential components of a comprehensive nuclear security program. There have been continued reports of illicit trafficking in nuclear and other radioactive material which underline the need for States to have nuclear security measures in place [15]. In order to prevent potential threats which include nuclear threats to national security from armed non-state actors and organized criminal groups, States have and must develop strategies in line with their international obligations. However, unlike the international nuclear safety framework, the international structure governing nuclear security is not as extensive, advanced or entrenched [16].

1.3 Legally Binding International Instruments
The IAEA and its partners have developed international legal instruments to guide states in terms of coordination and cooperation. With regard to the international legal framework, there is the need to emphasize three aspects. First, it is very important that states give the broadest and most active support to the relevant international instruments. Secondly, the provisions of these instruments should be incorporated and reflected in the national laws and regulations of all
states. Thirdly, there should be harmonization of national laws and regulations that could contribute to the detection of criminal or unauthorized acts by reducing delay and confusion in the handling of incidents of a cross-boundary event, and by enhancing the coordination of needed response actions [15].

1.3.1 Binding Instruments under the Auspices of the IAEA

The convention on the physical protection of nuclear materials (CPPNM) initially applied to nuclear material used for peaceful purposes while undergoing international transport. This convention did not apply to nuclear materials used for military purposes or the ones used for peaceful purposes which were not in international transport [1, 17].

The IAEA in July 2005 adopted an amendment to the convention on the physical protection of nuclear materials (CPPNM) at a conference organized in Vienna [1, 18], which strengthened the CPPNM significantly. The areas covered by the amendment include extension of the convention’s scope to cover nuclear material in domestic use, storage and transport. The others are the protection of nuclear material and facilities from sabotage, creating new offences for smuggling and certain group activities, clarification of national responsibilities for physical protection and the protection of confidential and sensitive information. The remaining areas are incorporating the objectives and fundamental principles of physical protection, agreeing on relevant definitions and the expansion of the scope of punishable acts.

The convention on early notification of a nuclear accident is highly relevant to the detection of and response to criminal or unauthorized acts involving nuclear and other radioactive material. This is because such a nuclear accident by virtue of its circumstances may involve the potential or actual release of radioactive material which could possibly have an impact across more than two national boundaries. The convention constitutes part of the international framework for responding to radiological emergencies that could result from criminal or unauthorized acts [1, 19].
1.3.2 Binding Instruments under the Auspices of the United Nations

In December 1996, an ad hoc committee was established by the UN General Assembly in its resolution 51/210 of 17, with a specific mandate of expanding a number of legal instruments for the prevention, suppression and elimination of terrorism and to establish an international convention for the suppression of bombings by terrorists. Subsequently the committee was mandated to establish an international convention for the suppression of acts of nuclear terrorism to supplement existing international instruments which are related [20]. State parties under this convention have the obligation to criminalize a range of potential activities involving nuclear or other radioactive material. They are to characterize such criminal or unauthorized acts involving radioactive material with the intent to cause death, serious bodily injury or property damage as unlawful and punishable offences. The offences include intentional possessions, use, threat, attempt or participation in acts of terror involving nuclear material and other radioactive material. In many respects, the offences established under this convention should be parallel to those established in the CPPNM.

The non-proliferation treaty on nuclear weapons (NPT) is one of the several international legal instruments which seek to prevent the transfer of nuclear explosive devices, nuclear weapons, fissionable materials from a nuclear weapon state to a non-nuclear-weapon state. Non-nuclear weapon states are not also supposed to request these weapons or fissionable materials from a nuclear weapon state. The NPT has been signed by all member states of the United Nations with the exception of India, Israel and Pakistan. The IAEA has a role as a watchdog for the safeguards under the NPT [20]. The NPT has three pillars namely, to prevent the spread of nuclear weapons and weapon technology, to further the goal of nuclear disarmament, and to promote cooperation in the peaceful uses of nuclear energy [16]. The involvement of African countries in international nuclear disarmament and non-proliferation negotiations is perceived as being marginal. However, non-proliferation and disarmament issues should be of great concern to African countries because they cannot afford to be complacent about it. To be able to reduce the insecurity on the continent of Africa, there should be active participation in international negotiations by African States to drive home their concerns in the process of disarmament and the scarce resources which might be used for mitigation in the event of a nuclear accident will be available for human and social development. Even though African States are perceived generally
not to prioritize participation in international legal regimes governing nuclear weapons and material, understanding of Africa’s numerous challenges facing the individual States should be taken into consideration. The discussion of nuclear material security in Africa should acknowledge the different sources of insecurity on the continent which include the unavailability or scarcity of food, unequal land distribution and the abuse of power exhibited by some African leaders through perceived corrupt practices. Ensuring the security of nuclear materials in Africa is therefore but one element of the continent’s overall security architecture [16].

1.3.3 UN Security Council Resolutions
Immediately after the terrorist attack on September 11, 2001, the UN Security Council adopted UNSCR 1373 to unequivocally condemn the attacks and also put in place wide-ranging, comprehensive steps and strategies to combat international terrorism [1].

Three years later, the UN adopted UNSCR 1540 after a debate on weapons of mass destruction to foster its continuous efforts to elaborate a comprehensive counter-terrorism regime. In this resolution, the UN decided that all States shall refrain from supporting, by any means, non-state actors that attempt to acquire, use or transfer nuclear, chemical or biological weapons and their delivery systems [1].

The two resolutions, UNSCR 1373 (2001) and UNSCR 1540 (2004) were both adopted under Chapter VII of the UN Charter and are therefore binding on all States. The IAEA in approving the Nuclear Security Plan for 2006–2009, also approved these resolutions as integral parts of the IAEA’s legal framework for nuclear security and its nuclear security programme of activities [1].

1.4 Legally Non-Binding International Instruments

The IAEA and the UN have adopted other conventions together with the member States in order to boost nuclear security. These conventions are not legally binding on the member states but States are advised to incorporate these conventions in their nuclear security regimes.

1.4.1 Non-Binding Instruments under the auspices of the IAEA
Following the Recommendations for the Physical Protection of Nuclear Material and several revisions, Nuclear Security Recommendations on Physical Protection of Nuclear Material and
Nuclear Facilities (INFCIRC/225/Revision 5) now reflects the recommendations of the national experts to assist States in implementing a comprehensive physical protection regime for nuclear facilities and nuclear materials. It includes any obligations they may have under international agreements, such as the 2005 Amendment to the CPPNM. Although the recommendations contained in INFCIRC/225/Revision 5 are not binding, they acquire binding nature when included as an obligation in national laws or international agreements, including IAEA Project and Supply Agreements and the Revised Supplementary Agreements for the Provision of Technical Assistance by the IAEA [5].

Another non-binding instrument is the Code of Conduct on the Safety and Security of Radioactive Sources and the Supplementary Guidance on the Import and Export of Radioactive Sources. It was prepared by technical and legal experts in 1999 and endorsed by the General Conference. The General Conference invited Member States to take note of the Code and to consider, as appropriate, means of ensuring its wide application. In accordance with the Revised Action Plan in 2001, the IAEA Secretariat convened a meeting of technical and legal experts to review the effectiveness of the Code at which the Code’s provisions were strengthened in the light of the events of 11 September 2001.

A Conference on Security of Radioactive Sources was held in Vienna in March 2003 and recommended that States make a concerted effort to follow the principles contained in the Code. The G-8 annual summit held in Evian, France, in June 2003 also issued a statement on ‘non-proliferation of weapons of mass destruction, securing radioactive sources’ in which it encouraged all countries to strengthen controls on radioactive sources and observe the Code of Conduct [1].

Various States raised concerns regarding the import and export of radioactive sources, as a matter that needed to be further explored and some guidance developed. Accordingly the IAEA Secretariat convened a meeting of technical and legal experts to develop such guidance. In July 2004, the experts reached consensus on the text of the Guidance on the Import and Export of Radioactive Sources. The Board approved the Guidance on 14 September 2004. The General
Conference endorsed both the Code and the Guidance in September 2003 and September 2004, respectively [1].

1.4.2 Non-Binding Instruments under the auspices of the United Nations
The United Nations Global Counter-Terrorism Strategy (A/RES/60/288) came out of the 2005 World Summit where the Heads of State and Government mandated the General Assembly to develop a counter-terrorism strategy to promote comprehensive and coordinated responses to one of humanity’s major threats. In April 2006, the Secretary-General issued recommendations for a global counterterrorism strategy, which led to the unanimous adoption by the General Assembly, on 8 September 2006, of the United Nations Global Counter-Terrorism Strategy. The Strategy was launched at a high level meeting of the General Assembly on 19 September 2006 and marks the first time that the 192 Member States of the United Nations agreed on a common strategic approach to fight terrorism. The Strategy contains a plan of action to address the conditions conducive to the spread of terrorism; to prevent and combat terrorism; to take measures to build state capacity to fight terrorism; to strengthen the role of the United Nations in combating terrorism; and to ensure the respect of human rights while countering terrorism [1].

1.5 Legislative and Regulatory Framework of South Africa concerning Nuclear Security
The Hazardous Substance Act (15) of 1973 [21] gives the legal backing to the Department of Health of South Africa to regulate hazardous substances. The Act was to provide for the control of substances that may cause injury or ill-health or death to human beings due to their toxic, corrosive, irritant, strongly sensitizing or flammable nature or the generation of pressure in certain circumstances. It was also for the control of certain electronic products and to provide the division of such products into groups in relation to the degree of danger and to provide for the prohibition and control of the importation, manufacture, sale, use, operation, application, modification, and disposal or dumping of such products. The provisions of the Act relating to Group IV hazardous substances came into operation in 1993. Group IV hazardous substance means radioactive material which is outside a nuclear installation as defined in the Nuclear Energy Act, 1993, and is not a material which forms part of or is used or intended to be used in the nuclear fuel cycle [21]. In the Act, these Group IV hazardous substances have an activity concentration of more than 100 becquerels per gram and a total activity of more than 4000
becquerels, or have an activity concentration of 100 becquerels or less per gram or a total activity of 4000 becquerels or less and which the Minister has by notice in the Gazette declared to be a Group IV hazardous substance. These substances should be used or intended to be used for medical, scientific, agricultural, commercial or industrial purposes, and can include any radioactive waste arising from such uses. Subject to the provisions of the Act, the Director-General of the Department of Health may on application in the prescribed manner and on payment of the prescribed fee (if any) and subject to the prescribed conditions and such further conditions as the Director-General may in each case determine, issue to any person or company a licence to enable that person or company to safely and securely handle Group IV hazardous substances that is outside a nuclear installation [21]. The license can be suspended or cancelled if the holder in applying for the that licence furnished the Director-General with untrue or misleading information; if the holder failed to comply with the conditions of the licence; if the holder failed to comply with the provisions of the Act; if the holder has been convicted of an offense whose nature in the opinion of the Director-General renders the person unsuitable to handle Group IV hazardous substances; or if the holder does not use the licence for the purpose it was applied for.

The National Nuclear Regulator (NNR) Act (47) of 1999 [22] established the NNR as the National Competent Authority with legal backing to regulate and oversee the the location, design, construction, operation, decontamination, decommissioning and closure of any nuclear installation. The act also enables the NNR to regulate vessels propelled by nuclear power or having radioactive material on board that is capable of causing nuclear damage, as well as any action which is capable of causing nuclear damage. This Act does not apply to the exposure to cosmic radiation or to potassium-40 in the body, or any other radioactive material or actions not amenable to regulatory control. The Act also does not apply to any action where the radioactivity concentrations of individual radioactive nuclides, or the total radioactivity content, are below the exclusion levels provided for in the safety standards. It also does not apply to the Group IV hazardous substances as defined in section 1 of the Hazardous Substances Act, 1973 (Act No. 15 of 1973), nor to exposure to ionizing radiation emitted from equipment, declared to be a Group III hazardous substance in terms of section 2(1)(b) of the Hazardous Substances Act, 1973 [22].
The NNR’s Regulatory Framework consists of legally binding requirements by International Safety Conventions, laws passed by Parliament that govern the regulation of South Africa’s nuclear industry, regulations, authorizations, conditions of authorizations, requirements and guidance documents that the NNR uses to regulate the industry. Requirements are developed in conjunction with the applicable authorized action and effectively cover all the relevant requirements of the holder. The NNR enforces these requirements on all applicants and authorization holders. Certain requirements in the legislation are prescriptive to the extent that no further elaboration is necessary. Other requirements are broad in nature. The NNR establishes additional requirements based on international best practices. These requirements are registered either directly in the authorizations or in a Requirements Documents [23].

The objectives of the National Nuclear Regulator are to provide for the protection of persons, property and the environment against nuclear damage through the establishment of standards and regulatory practices; to exercise regulatory control related to safety over the location, design, construction, operation, manufacture of component parts, decontamination, decommissioning and closure of nuclear installations; to regulate vessels propelled by nuclear power or having radioactive material on board which is capable of causing nuclear damage through the granting of nuclear authorisations; to provide assurance of compliance with the conditions of nuclear authorizations through the implementation of a system of compliance inspections; to fulfil national obligations in respect of international legal instruments concerning nuclear safety and to ensure that provisions for nuclear emergency planning are in place [22].

The NNR has put in place regulatory requirements for the assurance of nuclear security or physical protection system at nuclear installations or associated actions in the Republic of South Africa. These regulatory requirements were developed in accordance to the National Nuclear Regulator Act (No.47 of 1999), the South African Nuclear Energy Policy (2008), Minimum Information Security Standards (MISS) and IAEA Nuclear Security Series No.7. The IAEA Nuclear Security Series No.7 is the IAEA implementing guide on Nuclear Security Culture which provides characteristics, attitudes and behavior of individuals, organizations and institutions in supporting the establishment of effective nuclear security [23].
The NNR compliance assurance programmes for nuclear security or physical protection system are done in a manner that maintains the proper relationship and co-existence of nuclear safety, security and safeguards. The PPS that are established in nuclear installations should be characterized by active and passive designed measures to safeguard personnel; means to prevent the unauthorized access to equipment, a facility or installation, audit materials, information, documents or electronic data and methods for safeguarding all these items against industrial espionage, sabotage, damage and/or theft.

By regulation, authorized operators must ensure that security measures provided for handled or processed radioactive material (or nuclear material) and for controlled information are in accordance with binding international instruments such as The Treaty on Non-proliferation of Nuclear Weapons (NPT). IAEA physical protection objectives (GOV/2001/41), The Convention on the Physical Protection of Nuclear Material (CPPNM) and its Amendment, The International Convention for the Suppression of Acts of Nuclear Terrorism, Safeguards agreements and additional protocols, United Nations Security Council Resolutions 1540 (2004) and 1673 (2006) and also the United Nations Security Council Resolution 1373 (2001) [23] must also be political commitments whereupon the IAEA conducts regular verification and technology controls at Member State’s nuclear installations.

1.6 Nuclear Security at Public Events
In general, the State is responsible for the security of nuclear material or other radioactive material, associated facilities and practices. While the State strives to protect people, environment, facilities through providing security measures, adversaries are always looking for security vulnerabilities. Therefore, the State should assess and audit these measures periodically to identify weaknesses and areas of possible improvement. States should particularly make it a point to provide nuclear security at more locations than just nuclear facilities. One place States should place a high priority on effective security is public events. Adversaries will always want to take advantage of any situation they deem vulnerable to engage in malicious or authorized acts, and to cause harm to people [8]. Such attacks can lead to severe health, social, psychological, economic, political and environmental consequences as a result of the dispersal of nuclear and other radioactive material in public places, such as with the help of radiological
dispersal devices (RDDs). Dangerous radioactive material can also be placed in public places in the form of radiological exposure devices (REDs) with the deliberate intention of irradiating persons near a fixed point source. A nuclear yield can also be generated by, for example, an improvised nuclear device (IND). Another possible attack can be a deliberate act of contaminating food or water supplies with radioactive material [8]. At major public events, the nuclear security, needs to be an integral part of the overall security plan for the event, and should be linked to the nuclear security regime of the State.

Generally, nuclear and other radioactive material can be detected by instruments without intrusive search using various kinds of specialized but commercially available radiation detection instruments. Criminal or terrorist acts involving nuclear and other radioactive material at major public events can potentially be prevented by the deployment of radiation detection instruments on the event grounds purposely for detecting and interdicting the material before the criminal or terrorist act is carried out [8]. Detection instruments for nuclear and other radioactive material are described in detail in references [15, 24].

Trained personnel are needed to use these instruments for maximum effectiveness. Radiation detection instruments that can be used at major public events can be divided into four categories: radiation portal monitors (RPMs), personal radiation detectors (PRDs), hand-held instruments and portable radiation scanners (PRSs). RPMs by their design are suitable to be used at controlled convergence security screening points for detecting the presence of nuclear and other radioactive material, either in the possession of passengers/pedestrians or transported by vehicles. PRDs are usually small, light-weight instruments worn by personnel on a belt or uniform. When in the presence of elevated radiation levels, a PRD alerts the user in real time. PRDs can also be used under specific situations by trained personnel when more sensitive instruments are unavailable for checking individuals or small packages, and only when the distance between the detector and the source is relatively small [8]. Handheld instruments are portable devices used for detecting, locating and/or identifying nuclear and other radioactive material. Handheld instruments can be divided into three subcategories. There are gamma search devices, neutron search devices and radionuclide identification devices (RIDs). Gamma search devices are designed to detect and locate sources of gamma rays. Neutron search devices detect
and locate sources of neutrons, particularly nuclear material or commercial neutron sources. Neutron search devices can be combined with gamma search detectors. Radionuclide identification devices (RIDs) are multipurpose instruments used for search and identification of nuclear and other radioactive material. They may also be useful assessing an alarm sounded by an RPM or PRD [8]. The final category of radiation detection instruments is the PRS or advanced mobile radiation detection instruments; these consist of automated gamma spectrometers and radionuclide identification software. They frequently allow mapping with a global positioning system (GPS) and possess communication capabilities. Often they are used for pre-event radiological surveys and background mapping. They can also be used for real-time detection at or near strategic locations. There are two types of mobile measurement systems which include measurements done to survey small areas using backpacks, and measurements done to survey large areas using aircraft, vehicles or watercraft. Mobile measurement monitors cannot detect alpha or beta radiation, and therefore additional types of monitors are required for that purpose [8].

As mentioned previously, the nuclear security systems and measures needed to implement a national strategy for the detection of nuclear and other radioactive material out of regulatory control should integrate the nuclear security detection architecture. These systems and measures should work hand-in-hand under a concept of operations. They should be supported by law enforcement, intelligence agencies, systems of regulatory compliance as well as human resources (e.g., enforcement officials, experts, local and national response teams, and other authorities) to ensure their effectiveness [25].

1.7 Physical Protection Regime
A State should have a physical protection regime which is an essential part of the overall nuclear security regime. The objectives of a physical protection regime should be to protect against unauthorized removal of nuclear material or any radioactive material, locate and recover missing nuclear material or radioactive material and ensure the effective implementation of rapid and comprehensive measures to locate and, (where appropriate), recover missing or stolen nuclear material or radioactive material. Other objectives include protecting nuclear material and nuclear facilities against sabotage, mitigating or minimizing the consequences of sabotage. The physical
protection regime can achieve these objectives through the prevention of malicious acts using
deterrence and protection of sensitive information, by managing any attempted malicious act and
mitigating the consequences of a malicious act [5]. The State’s physical protection regime should
counter sabotage for all nuclear material in use, in storage, in transport and for all nuclear
facilities. The regime should be reviewed and updated regularly to reflect changes in the threat,
new understanding of security vulnerabilities and advances in physical protection strategies,
approaches, systems, and technology. It should also take into account the introduction of new
types of nuclear material and nuclear facilities. A risk management system is needed as well to
ensure that the State’s physical protection regime is capable of keeping the risk of unauthorized
removal and sabotage at acceptable levels. This requires the assessment of threats and
vulnerabilities, understanding the corresponding potential consequences of threats and
vulnerabilities, and developing a legislative, regulatory and programmatic framework which will
ensure that appropriate effective physical protection measures are put in place [5].

One important part of the nuclear security measures is to design a robust physical protection
system or physical security system to protect and secure a nuclear facility, materials or
radioactive sources. A PPS integrates strategies, people, procedures, and equipment for the
protection of assets or facilities against theft, sabotage or other malevolent attacks or inadvertent
compromises of security [26]. Security professionals are the right people to be contracted by
facilities to design security systems to deter adversaries from committing a malicious act or to
minimize the consequences through detection, delay and response in the likelihood of an
adversary succeeding in completing such a malicious act. Such an act would consist of a number
of actions by one or more adversaries (threat) to obtain access to a source (target) either in order
to commit an act of sabotage or another malicious act, or in order to remove the source without
authorization [27].

In designing a physical protection system for a facility, the designer (security professional)
should incorporate computer security in the overall security plan for the protection system
because computer security plays an increasingly vital role in ensuring that system objectives are
met. Such computer security planning will help protect computer systems, networks and other
digital systems that are critical for the safe and secure operation of the facility and for preventing
theft, sabotage and other malicious acts. Computer security has the objectives of protecting the confidentiality, integrity and availability attributes of electronic data or computer systems and processes. By the identifying and protecting of these attributes in data or systems, the security objectives can be met [7]. Computers and computer systems used in this thesis refer to the computation, communication, instrumentation and control devices that make up functional elements of the nuclear facility. This does not relate to only desktop computers, mainframe systems, servers, network devices, but also to lower level components such as embedded systems and programmable logic controllers (PLCs). In essence, this design of PPS incorporating computer security should be concerned with all digital or electronic components that may be susceptible to compromise. The concept of computer security should cover the security of all computers as defined above and all interconnected systems and networks formed by the sum of the elements. Computer security is a subset of information security as defined in ISO/IEC 27000 [28] with which it shares many of the goals, methodology and terminology [7].

The design of an effective PPS needs to follow a methodical approach in which the designer should weigh the objectives of the PPS against the available resources and then evaluate the proposed design to determine how well it meets the objectives. Outside evaluations should also be sought. Without careful assessments, the PPS might waste valuable resources on unnecessary protection or will fail to provide adequate protection at critical points of the facility [29]. The system itself typically has a number of elements namely, deterrence, detection, delay and response [26].

One kind of physical deterrence (overt deterrence) occurs when a motivated adversary wishes to perform a malicious act and is discouraged from doing so by some physically visible or publicly known measures put in place at the facility. Deterrent measures have the ability to convince an adversary to see the malicious act as too difficult, the success of the act too uncertain, and consequence of the act to the adversary too unpleasant to justify the undertaking and thereby makes the facility an unattractive target, so the adversary may abandon the attack. A well designed overt physical deterrence measure specifically communicates to the adversary, about the presence of measures performing the other security functions. If this communication has the intended effect, deterrence is the result [27]. The presence of security guards in parking lots,
adequate lighting in the night at the facility, posting of signs and the use of barriers such as bars on windows and doors are examples of overt deterrents. In the event that an adversary goes against all odds and chooses to attack anyway, deterrence cannot be very helpful in discouraging the adversary and is thus of little use. It will be a great mistake to assume that because an adversary has not challenged a system, the effectiveness of the system has been proven [29]. The deterrence function of a PPS is difficult to measure and reliance on a successful deterrence is risky and therefore it is considered a secondary function. As more research is done on the measurability and long-term value of deterrents, these values may be incorporated into protection system design. For the present, however, there is no statistically valid information to support the effectiveness of deterrents but there are studies that suggest that deterrence is not as effective for real-world implementation as is hoped in theory [30].

Detection, in contrast to deterrence is the discovery of an attempted or actual intrusion which could have the intention of unauthorized removal or sabotage of a radioactive source. There are several means to achieve detection including visual observation, video surveillance, electronic sensors, intrusion detectors, accountancy records, tags and tamper-indicating devices, process monitoring systems, and other means. The adversary’s awareness or suspicion of the existence of detection measures can also serve as a deterrent [27].

An adversary’s attempt to gain unauthorized access or to remove or sabotage a radioactive source can be impeded by delay measures through barriers or other physical means. A measure of delay is the factor of time after detection that the good guys (designers of a PPS) forces on the adversary [27]. The concept of multiple layers and methods of protection (structural, technical, personnel and organizational) that have to be overcome or circumvented by adversaries in order to achieve their objectives should be reflected in the protection requirements. Traditionally, the primary means of preventing and mitigating the consequences of security breaches is through defense in depth. Defense in depth in computer security is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail or be defeated before computer systems can be compromised. Subsequent levels or barriers would be available if one level of protection or barrier were to fail or be defeated. When defense in depth is properly implemented, it increases the odds that no single technical, human or
organizational failure can lead to the compromise of computer or physical systems. The independent effectiveness of the different levels of defense is a necessary element of defense in depth though most times layers are meant to work together [7].

In designing physical security, the physical barriers used in the delay stage often need doors or gates in them for authorized staff to go in and out. This requires the use of guards and/or some kind of entry control system that could be anything from metal keys to biometric scanners. Adversary awareness of delay barriers can also serve as deterrents [26].

A security management system should be in place in the security planning to implement security management measures which address access control, trustworthiness, information protection, preparation of a security plan, training and qualification, accounting, inventory and event reporting issues. Stringent security management measures should use a graded approach. Operators or license holders should provide a means of physically controlling access that allows only individuals with authorized access to enter areas where radioactive material is present. Only authorized individuals who demonstrate need for access into critical areas for the performance of their jobs and are trustworthy should be granted to unescorted access but there should be measures to check abuse. Other individuals should be allowed access to these areas only if they are escorted or observed by an individual authorized for unescorted access or if compensatory measures for the security of radioactive material have been implemented [4].

In terms of trustworthiness, the competent authority should verify individuals with authorized access to radioactive material and/or security sensitive information to ensure that the trustworthiness and reliability of these individuals are in accordance with the State’s national practices. The objectives of trustworthiness measures could range from confirmation of identity to a comprehensive background check by the legitimate national authority using a graded approach. These will include verification of references to determine the integrity and reliability of each person. Interviewing neighbors, relatives and co-workers of and employee or potential employee might also be considered. Threats posed by insiders can be partially mitigated by the determination of trustworthiness and reliability of individual workers; access should be limited for security-sensitive information to only the people who need that information in order to
perform their jobs. Key elements of information protection include identification of the information that must be protected, designating which individuals will have authorized access to such information, and protecting such information from disclosure to individuals who do not have this access [4]. Facility operators must ensure that all personnel with security responsibilities are appropriately trained and qualified before they commence their responsibilities; this should be checked again periodically. Operators should do careful inventory and accounting of radioactive sources, particularly in the case of mobile sources consistent with a graded approach. A list of radioactive material under the responsibility of operators should be established and maintained. At prescribed intervals established by the regulatory body, operators should conduct a full inventory and verify that the radioactive materials are present at its authorized location. Inventory verification can be used as part of detection measures. An absence or discrepancy regarding the presence or amount of radioactive material, should be promptly investigated. Operators should promptly report to the regulatory body and other relevant competent authorities (e.g., law enforcement agencies) any evidence of the loss of control of radioactive material [4].

Security Response consists of the actions undertaken following detection in order to prevent an adversary from succeeding, or mitigating potentially severe consequences. These actions are typically performed by security or law enforcement personnel and other State agencies which make up the response team. Their duties include interrupting and subduing an adversary while the attempted unauthorized removal or sabotage is in progress, preventing the adversary from using the radioactive source to cause harmful consequences, recovering the radioactive source, or otherwise reducing the severity of the consequences. The prospect of successful response can also serve as a deterrent to other adversaries [27]. Managers of nuclear facilities or license holders and authorities concerned with the Response process should draw up contingency emergency plans to respond to unauthorized removal of nuclear material, or attempted sabotage of nuclear facilities or nuclear material. These plans should be carefully prepared and appropriately implemented [5].

Among all critical facilities, nuclear facilities and nuclear weapon sites require the highest level of PPS. Consequently, the IAEA adopted a convention [31] and published documents outlining
requirements for physical protection at nuclear facilities [32]. Current evaluation of the threat, vulnerability assessments, the relative attractiveness of a radioactive source, the nature of the source and potential consequences associated with its unauthorized removal or sabotage should be considered when selecting security requirements and should be based on a graded approach. A graded approach ensures that the highest consequence sources receive the greatest degree of security [27]. In implementing a graded approach, security systems may consider the tasks that range from preventing a malicious act to reducing its likelihood [4].

The design of an effective PPS should include the determination of PPS objectives, the initial design or characterization of the PPS, the continuing evaluation of the design and in many cases the redesigning or refinement of the design. In developing the objectives, the designer of the PPS must begin by gathering information about facility operations and conditions, such as a comprehensive description of the facility, operational states and the physical protection requirements [29]. The designer then needs to identify the threat. The term ‘threat’ used here describes an individual or individuals with the motivation, intention and capability to commit a malicious act to cause harm to people, damage to property or harm to the environment [33]. Identifying the threat involves understanding potential adversaries and their attributes, such as class, capabilities, motivations, technical sophistication, and tactics. The next step is for the designer to identify targets or assets to be protected. Targets may be in different forms like physical items, electronic data, technical knowledge, buildings, people or anything that could impact business operations or security. By doing this, the designer now knows the objectives of the PPS, which is what to protect against whom [29]. A formal threat assessment and an established Design Basis Threat are typically used for the design and evaluation of nuclear security systems. The DBT describes the attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed [32]. After the threat assessment and the DBT which is derived from the threat assessment, the next step is to design the new system or characterize and modify the existing system. In designing a new system, people, procedures and equipment must be integrated to meet the system objectives. If there is an existing system already, it must be characterized to establish a baseline of performance [29]. After designing the PPS or characterizing it, an analysis and evaluation must be done to ensure it meets the PPS
objectives. Evaluation must allow for features working together to assure protection rather than regarding each feature separately but this is always not the case and it must not assume the features will work together reliably. An evaluation benefits from modeling techniques and vulnerability assessments due to the complexity of protection systems [29].

Another critical issue a designer of a PPS must face is the insider threat from within the organization or facility. ‘Insider’ in this sense describes an individual with authorized access to a nuclear facility, a transport operation or sensitive information. Insider threat can also include dangerous actions by individuals that are inadvertent due to human error, carelessness, poor training, or inadequate motivation. Threats from insiders in particular, present a unique problem for a physical protection system. Insiders normally take advantage of their access rights, complemented by their authority and knowledge of a facility to bypass dedicated physical protection elements or other provisions such as measures for safety, material control and accountancy as well as operating measures and procedures. As personnel who have access to positions of trust, insiders are capable of carrying out ‘defeat’ methods not so readily available to outsiders when confronted with protection elements and access controls. Insiders have more opportunities to select the most vulnerable target and the best time to execute the malicious act, and they may work in collaboration with outsiders willingly or through coercion [33]. Their likelihood of success of an insider attack can be maximized over an extended period of time. These include tampering with safety or security equipment to prepare for an attempt or act of sabotage, or falsifying accounting records to repeatedly steal small amounts of nuclear material. An insider may be in any position at the facility, from the highest-level employee to the lowest. There are different motivations insiders have and these may be passive or active, non-violent or violent. ‘Motivation’ describes the forces that compel an adversary to perform or attempt to perform a malicious act. These may include ideological, personal, financial and psychological factors and other forces such as coercion. An individual could be forced to become an insider by coercion or by coercing his/her family members [33]. Insiders could act independently or in collusion with others and could become malicious on a single impulse, or act in a premeditated and well prepared manner depending upon their motivation. Insiders can vary as to whether they are passive or active. Passive insiders are not violent and usually provide information that could help adversaries to perform or attempt to perform a malicious act. Active insiders on the other
hand are willing to provide information, perform actions themselves and may choose to be violent or non-violent. Active insiders are willing to open doors or locks, tamper with seals, or provide hands-on help and aid in neutralizing response force personnel. Non-violent active insiders will typically not want to give up their identity and therefore will not risk engaging response forces but they may limit their activities to tampering with accounting and control, and safety and security systems. Violent active insiders may use force regardless of whether it enhances their chances of success or not, and they may also act rationally or irrationally [33].

The absence of a healthy security culture, good security awareness, effective trustworthiness programmes, performance appraisals and industrial relation policies are some of the employment issues that may be conducive for insiders to perform malicious acts.

There should be a comprehensive approach to counter insider threats. A nuclear facility can rarely prevent insider threat totally, but the risk can be reduced. While it is rare, there should ideally be several layers of defense that insiders would have to overcome or circumvent in order to achieve their objectives. Such layers might include both administrative aspects (procedures, instructions, administrative sanctions, access control rules, confidentiality rules) and technical aspects (multiple protection layers fitted with detection and delay). It is usually much more difficult to implement preventive and protective measures to counter insider threat than implementing measures to counter the outsider threat due to the access, knowledge, authority and attributes of insiders. Although most PPS are designed against the outsider threat, any elements that could provide protection against the insider threat should be considered. These elements include detection, delay, response and mitigation capacities [33]. To be able to deter and detect the protracted theft of nuclear material by an insider, the physical protection system should be assisted by effective nuclear material accountancy and control measures [5].

Radioactive materials are used throughout the world for a wide variety of beneficial purposes. This means that there is a great demand for effective security measures to prevent the acquisition of such material by malicious actors. Security should be provided for radioactive material to ensure that there is a balance between managing radioactive materials securely while still enabling it to be used safely by authorized persons without unduly limiting its use for societal
benefits [4]. Radioactive sources provide great benefit to humanity, through their use in agriculture, industry, medicine, research and the vast majority are used in well-regulated environments. There is a small fraction of radioactive sources over which control has been lost, which has sometimes resulted in accidents with serious consequences. There is a growing concern that terrorist or criminal groups could gain access to high-level radioactive sources and use them maliciously. Consequently, there has been a global trend towards increased control, accounting and security of radioactive sources to prevent their malicious use and any potential associated consequences [27]. In the event that adversaries are able to go, defeat or bypass security measures the security vulnerabilities that were exploited should be identified and the initial system must be redesigned to correct the problems and reevaluated for effectiveness [29].

There can be many factors leading to loss of control of radioactive sources. These include ineffective regulations and regulatory oversight, the lack of management commitment or worker training, poor source design and poor physical protection of sources during storage or transport, poor or non-existent mitigation or the insider threat, poor or non-existent vulnerability assessments, insufficient funding, and a weak security culture. The challenge is to address this wide range of risks with effective actions [34]. A high-degree of confidence in the effectiveness of the physical protection of nuclear and other radioactive material and associated facilities and transport requires a close correlation between protective measures and the threats.

In case of an emergency, the most important aspects of managing a radiological emergency is the ability to promptly and adequately determine the threat and take appropriate actions to protect members of the public and emergency workers. Experience shows that the public’s perception of the risk posed by the threat may be more important than the actual risk. Consequently, an important part of a security program is providing the public, ideally in advance of an attack or incident, with timely, informative, understandable and consistent information on the true risk [34]. In order to be able to manage nuclear security events well, the State should have a comprehensive national response plan for nuclear security events combined with the national radiological emergency plan [35]. This Plan should be the basis for establishing communication systems needed for prompt and effective response; it should also serve as a guide for the competent authorities to ensure that all necessary preparedness and response tasks are given the appropriate resources and support. The plan should describe the process for various competent
authorities to fulfill their roles and responsibilities in response to nuclear security events, including the notification and activation of all relevant competent authorities, notification of relevant international organizations and potentially affected States and coordinating various organizations and command and control units. The plan should also include measures to locate, identify and categorize nuclear and other radioactive material and to detain and/or seize, recover and control material or render harmless any threat or associated device. It should provide measures to collect, secure and analyze evidence, as well as isolate, classify, package and document any nuclear or other radioactive material, to assist in relevant investigations [9].

There should be international cooperation amongst States in the event of nuclear security incidents. There should be an exchange of accurate and verified information on nuclear security events amongst States in accordance with international obligations and national legislation, taking into account the designation of roles and responsibilities. There is a need for accurate information flow between States, either directly or through the IAEA, the United Nations, or other relevant international organizations, as appropriate [9]. Any nuclear material or other radioactive material over which control has been lost with potential trans-boundary implications, the State concerned should provide information about the incident or in accordance with its international obligations and national legislation.

States should make it a point to participate in and report relevant nuclear security events to applicable regional and international information databases for example the IAEA’s Incident and Trafficking Database (ITDB). Information exchange amongst States on lessons learned after relevant nuclear security events are vital in the fight against nuclear terrorism [9]. The common aim of nuclear security and nuclear safety are to protect persons, property, confidential information, society and the environment. Security measures and safety measures have to be designed and implemented in an integrated manner to develop synergy between these two areas and also in a way that guarantees that security measures do not compromise safety and safety measures do not compromise security [3]. Even though nuclear safety and nuclear security consider the risk of inadvertent 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 different attitudes and behaviors, such as efforts to deter malicious acts and
confidentiality of information as compared with safety culture. Safety culture is the assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, protection and safety issues receive the attention warranted by their significance [36, 37].

1.8 Problem Statement
There has been accelerated technological change experienced by the world at the outset of the twenty-first century. Technologies using nuclear and other radioactive material are no exception to this trend, and such materials are being used in a growing variety of settings to advance development in various countries. If these nuclear safety and security issues are not controlled and handled appropriately, such material can pose serious risks to public health, property and the environment [15]. The likelihood that terrorist or other criminal organizations could obtain the necessary material, components and expertise to construct a nuclear explosive device or RDD is high due to the advances in information technology and the availability of widespread radioactive material [15].

There is growing concern in the international community that possible malicious acts involving nuclear material or other radioactive material are more likely due to the increased demand for nuclear energy and the renewed interest in expanding or developing nuclear power programmes and nuclear applications. Moreover, it is becoming clearer that this nuclear revival will not only be limited to countries with extensive experience in nuclear programmes, but will also affect countries with currently limited nuclear activities and those that plan to substantially expand their nuclear activities in the future. Therefore the need for an increase in well qualified experts and specialists in nuclear security is very essential [25].

Radioactive materials used in irradiating facilities such as the $^{60}$Co at the Centre for Applied Radiation Science and Technology of the North-West University can pose a major security and safety challenge due to high exposure rates from these sources if they are lost, stolen, sabotaged, or tampered with. It is therefore required by regulatory authorities and the operators to take into account all factors and security systems needed to adequately secure these facilities [38]. Terrorists need only to identify and exploit the weakest link in the chain of nuclear security to
acquire enough fissile material to make and detonate a bomb or make a dispersal of a radioactive material in a major city. According to the IAEA’s Incidents and Trafficking Database (ITDB), from January 1993 to December 2011, a total of 2164 confirmed incidents were reported by both participating States and some non-participating States. Out of the 2164 confirmed incidents, 399 involved unauthorized possession and related criminal activities, 588 incidents involved the theft or loss of nuclear or other radioactive material and a total of 1124 cases involved other unauthorized activities, including the unauthorized disposal of radioactive materials or discovery of uncontrolled sources. Due to insufficient information, the remaining 53 cases could not be categorized [39]. Globally, between 1972 and 2007, 17 major terror attacks or acts of sabotage were carried out against nuclear power stations [40].

Existing and potential sources of Nuclear and Radioactive materials are a reality in Africa and according to the IAEA, the countries of Algeria, Egypt, Ghana, Libya, Morocco, Nigeria and South Africa all have operational research nuclear reactors. The Democratic Republic of Congo’s (DRC) research reactors are no longer in operation. South Africa also has a nuclear power reactor and is about to build six more. In total, there are approximately 17,500 registered radioactive sources in South Africa and these sources need to be secured.

This research seeks to design a robust PPS for CARST to secure the $^{60}$Co irradiation source in order to avoid or minimize the infiltrations experienced at the Pelindaba nuclear research facility outside Pretoria [41]. This will be done by comparing different PPS designs and evaluating the proposed PPS with different security models and computer codes.

1.9 Research Aim and Objectives

1.9.1 Aim
The main aim of this research is to provide adequate physical protection security by evaluating a proposed design of a PPS using different security models and appropriate computer codes for the 444 TBq $^{60}$Co irradiation facility in the F2C building and the entire Centre for Applied Radiation Science and Technology, North West University (Mafikeng Campus).

1.9.2 Objectives
The objectives of this research are to:
Evaluate the current status of the physical protection system for both the $^{60}$Co radioactive source used in F2C irradiating facility and the entire Center.

Assess the threat the Center is exposed to and propose a Design Basis Threat.

Propose a new PPS design for the Center based on the DBT. The process will utilize a performance-based system to design the PPS.

Analyze and evaluate the PPS effectiveness for the protection of the radioactive source and the entire Center using the Estimate of Adversary Sequence Interruption and the Analytic System and Software for Evaluating Safeguards and Security models. This analysis will be to ascertain how effective the design will be against malevolent action by potential adversaries.

Validate the design implementation by the Global Threat Reduction Initiative (GTRI) with the EASI and ASSESS models for effectiveness.
CHAPTER 2 Literature Study

This chapter discusses radiation types, radiation interaction with matter, health effects and level of exposures and also presents a detailed overview of work done in the thesis area in published literature.

2.1 Types of Radiation

Most radioactive materials emit different types of radiation. Some examples of the types of radiation are alpha (α) particles, beta (β) particles and gamma (γ) rays. X-rays however, are a type of low-energy gamma radiation that is produced in a different way. This process involves the firing of electron beams at a metal target (usually tungsten) to produce the X-rays. The electrons in the metal target absorb energy from the electron beam and then release the energy in the form of X-rays as they undergo relaxation to the ground state. The X-rays disappear once the beam is switched off and therefore X-ray machines are not considered to be radioactive. Because of this, X-ray machines in general are of no concern from the viewpoint of illicit trafficking or other unauthorized transfer of radioactive material though the X-ray tubes should be safeguarded by the regulatory authority in the case of decommissioning. During atomic fission and nuclear fusion, unstable nucleus emit another form of radiation called neutrons (n). The properties and characteristics of the above mentioned radiations are summarized below [15].

2.1.1 Alpha particles (α)

Alpha particles are nuclei of the helium atom. They contain two protons and two neutrons and are relatively heavy, high-energy particle and also positively charged from the two protons because of the absence of electrons. They can be blocked completely by paper or skin and have a range in air as short as 1–2 cm [42]. Alpha particles also have a velocity in air of approximately one-twentieth the speed of light, depending upon the individual particle's energy. Atoms that emit alpha particles tend to be very large atoms with high atomic numbers, though there are some exceptions. Naturally occurring alpha emitters have atomic numbers of at least 82, e.g., lead (Pb). Alpha particles (radiation) outside of the body is not hazardous but can be hazardous if the alpha-emitting material is inhaled or ingested so that it enters the body. This is due to the large Linear Energy Transfer (LET) that can result to nearby tissues. Alpha radiation is known to
cause lung cancer in humans when alpha-emitting materials are inhaled into the lungs. The
greatest exposures to alpha radiation for average humans is from the inhalation of radon and its
decay products which also emit potent alpha radiation [42].

2.1.2 Beta particles (β)
An unstable nuclei of an atom usually ejects fast-moving electrons called Beta particles. These
particles are much smaller than alpha particles and are negatively charged. Depending on their
energies, they can penetrate further into matter with a range several metres of air and few
millimetres or centimetres of solid material. Beta radiation can be blocked by both plastic a few
centimeters thick and glass a few millimetres thick [15]. The individual speed of beta particles
depends on how much energy they possess and this varies over a wide range. Beta particle
energy causes harm to living cells when transferred because it can break chemical bonds and
form ions. Beta radiation can cause both acute and chronic health effects. Acute exposures are
not really common unless there is contact with a strong beta source from an abandoned industrial
instrument; chronic effects are much more common. Chronic effects result from fairly low-level
exposures over a long period of time. They can develop slowly from 5 years to 30 years. The
main chronic health effect from beta radiation is cancer. When taken internally, beta emitters can
be hazardous because they can cause tissue damage and increase the risk of cancer, which
increases with increasing dose. Large exposures to high energy beta particles can cause skin
burns [42].

2.1.3 Gamma rays (γ)
Gamma radiation is a type of electromagnetic or photon radiation which is similar to light or
radio waves except that it has much higher energy and is massless with no electrical charge.
Gamma radiation is often emitted from an unstable nucleus that is emitting a beta particle.
Ionization takes place in atoms when Gamma radiation passes through matter, primarily due to
the interactions it has with electrons. Gamma photons travel at the speed of light and can cover
hundreds to thousands of meters in air before spending their energy. Due to the high energy,
gamma radiation is very penetrating through many kinds of materials including human tissue.
Only materials such as concrete, steel or lead with a substantial thickness can be used to
effectively slow or to provide good shielding. Gamma radiation is hazardous from outside the
body due to the ability to deliver significant doses to internal organs even without inhaling or ingesting the material. Gamma radiation, however, has less LET than alphas and betas [15].

2.1.4 X-rays
X-rays, like gamma rays, are electromagnetic in nature and pose the same kind of hazard, but are different in their origins. While gamma rays are emitted from the nucleus of an atom, X-rays originate in the electron fields surrounding the nucleus or are machine-produced. The latter involves a rapid slowing down of an electron beam. Like gamma rays, X-rays are penetrating and in the absence of shielding by dense material like concrete or lead, they can deliver significant hazardous doses to internal organs. [42].

![Figure 2.1: A summarized picture showing the penetrating power of alpha particles, beta particles and gamma rays [15].](image)

2.1.5 Neutrons
Neutron radiation involves neutral particles being released from an atom. Neutrons have no charge and about the same mass as a proton. Neutrons are a type of (indirectly) ionizing radiation
that come about due to ion-producing collisions with matter and absorption/decay processes. Neutrons are emitted by unstable nuclei especially during nuclear fission and nuclear fusion. With the exception of a component of cosmic rays in the upper atmosphere that interacts with air to produce neutrons, they are mostly produced artificially. However, neutrons are emitted by plutonium in detectable quantities and can be used in nuclear weapons [15]. Neutron sources are found in moisture and density gauges used commercially. Neutron radiation is used by researchers to investigate the sub-atomic structure of matter. Neutrons have been used in the security arena as part of a technology that can detect the existence of explosives and other dangerous items. The medical community relies on neutron radiation for production of medical isotopes and certain direct therapies. Because they are electrically neutral, neutrons can be very penetrating and therefore require heavy shielding to reduce exposures. It is rare to have significant neutron radiation in the human environment but this can occur, for example, if there is an improperly handled neutron source or an unexpected criticality accident. These occurrences are unlikely to happen in populated areas because these materials are handled in secure locations [42].

2.2 Radiation and Matter

Radiation comes in two forms namely ionization radiation and non-ionization radiation. When ionization radiation passes through matter, there is energy deposited in that material matter by the radiation. Due to the electrical charge of both alpha and beta particles they deposit energy through electrical interactions with electrons in the matter they interact with. Gamma rays lose energy in different ways through their interactions but in each way liberation of electrons from atoms happens. Neutrons also lose energy in different ways but the most important way is through collisions with nuclei that contain protons. These protons are set in motion and being charged, they again deposit energy through electrical interactions. Thus the ionization by neutrons is indirect. In all ionization radiation, the radiation produces electrical interactions in the material. In situations where an electron in an atom receives enough energy from these interactions, it may escape from the atom, leaving behind a positively charged atom (ion). This process in which a neutral atom (or molecule) becomes charged is called ionization. Non-ionizing radiation does not cause ionization in matter. Examples of non-ionizing radiations include radio frequency waves, microwaves, infrared radiation, and visible light [15].
2.3 Biological Consequences of Exposure to Ionizing Radiation

The cell is the basic unit of biological tissue and an important molecule in the cell is deoxyribonucleic acid (DNA). DNA is located mainly in the nucleus of the cell. One should not confuse the nucleus of the cell with the nucleus of an atom. It is during the interaction of ionizing radiation directly or indirectly with the DNA of the cell that causes biological damage. In direct interaction, radiation interacts with the atoms of the DNA molecule or some other cellular component critical to the survival of the cell. Such interactions may affect the ability of the cell to reproduce and survive. If a lot of atoms are affected during this process such that the chromosomes do not replicate properly or there is significant alteration in the information carried by the DNA molecule, then the cell may be destroyed by “direct” interference with its life-sustaining system [43]. In indirect interaction, the radiation might not be able to interfere directly with the DNA of the atoms since these are just a small part of the cell. This is because each cell is mostly water. Therefore, the probability of the radiation interacting with water that makes up most of the cell’s volume is high. When radiation interacts with water it may break bonds that hold the water molecule together and produce fragments such as hydrogen (H) and hydroxyls
(OH). These fragments may recombine or may interact with other fragments or ions to form compounds such as water which would not be harmful to the cell, but can also combine to form toxic substances such as hydrogen peroxide (H$_2$O$_2$) which can contribute to the destruction of the cell. If the DNA is damaged during this interaction by radiation exposure, it can sometimes be repaired by the human body. However, if the damage is not repaired or not repaired correctly, the cell may die or mutate [43].

2.4 Health Effects

In order for radiation effects to be noted, there needs to be sufficiently high doses. The dosage determines the number of cells that die. This means that a very high dose to the whole body can cause a person to die within days or weeks. A 5 Gray (Gy) dose or more received instantaneously, for example, will probably be lethal to the skin and can cause erythema (skin burns). This type of skin burn may be more severe than a conventional skin burn because the damage will go deeper due to the penetration of the radiation and affect deeper cells of the body. Cell mutation can presumably happen at any level of radiation exposure, even though the probability (risk) of the mutation leading to health consequences depends on the magnitude of the dose received. For example, if the dose is lower than the threshold dose which will show observable health effects and it is delivered over a longer period of time, there is still the possibility of cancer appearing later in life. It is also possible that children of the irradiated person may suffer health consequences, although such health consequences have never actually been observed in human populations at a statistically significant level. The main concern with low doses of radiation is causing cancer and because of this, information on the effects of exposure to ionizing radiation is collected and assessed periodically by the United Nations Scientific Committee on the Effects of Atomic Radiation (UNSCEAR) [11].

2.4.1 Stochastic Health Effects

Stochastic effects are associated with long-term, low-level (chronic) exposure to radiation. The word stochastic refers to having a random probability distribution or pattern that may be analyzed statistically but may not be predicted precisely. Increased levels of exposure will make these health effects more likely to occur, but do not influence the type or severity of the effect. Cancer is considered the primary health effect from radiation exposure by most people; it is the
uncontrolled growth of cells in the body. Natural processes control the rate at which cells grow and replace themselves and also control the body's processes for repairing or replacing damaged tissues. Damage occurring at the cellular or molecular level can be disruptive to the control processes, thereby permitting the uncontrolled growth of cells which may result in cancer. This is why ionizing radiation's ability to break chemical bonds in atoms and molecules makes it such a potent carcinogen. Changes to the DNA are called mutations. Sometimes the body fails to repair these mutations or even creates mutations during repair. The mutations can be teratogenic or genetic. Teratogenic mutations are caused by exposure of the fetus in the uterus and affect only the individual who was exposed. Genetic mutations are passed on to offspring [42].

2.4.2 Non-Stochastic or Deterministic Effects
Non-stochastic or deterministic effects appear in cases where the body is exposed to high levels of radiation which are greater than a threshold value of dose after which observable effects will be seen. The severity of the damage caused by such high doses increases with increasing exposure. Short-term and high-level exposures are referred to as acute exposure. Most radiation health effects that are not cancerous are caused by acute exposures, which in turn lead to non-stochastic or deterministic effects. Unlike cancer, health effects from acute exposure to radiation usually appear quickly and include burns and radiation sickness. Radiation sickness is also called radiation poisoning. This “poisoning” can cause premature aging or even death. If the dose is fatal, death usually occurs within one or two months. The symptoms of radiation sickness includes nausea, weakness, hair loss, skin burns and diminished organ function. Medical patients receiving radiation treatments often experience acute effects, because they are receiving relatively high doses of radiation during treatment [42].

2.5 Levels of Exposure
Radioactive materials occur naturally throughout the environment and therefore ionizing radiation becomes a fact of life. The naturally occurring radioactive materials (NORMs) are a continuous source of radiation exposure because they are present in all soils, rocks and building material. They are also present in the diet we eat and therefore every human being contains trace amounts of radiation. Some examples include carbon-14, potassium-40, uranium, thorium and the daughter products of these materials such as radium-226 and polonium-210 (both of these are
daughters of uranium-238). Another source of radiation exposure is from cosmic rays which reach the Earth from outer space. Radon-222 which is a gas and a radioactive daughter product of uranium-238 is the highest source of exposure dose of radiation from natural sources. This is because, being a gas, it escapes into the air that humans breathe and leads to a dose primarily to the lungs. Apart from the natural sources of radiation exposure, humans have found ways of producing radiation and radioactive materials artificially after the discovery of X-rays and radioactivity. These artificial radiation or radioactive materials are now used in medical diagnosis and for therapeutic, research, and commercial purposes. In addition to these, radioactive material of artificial origin has been introduced into the environment as a consequence of the fallout from the atmospheric testing of nuclear weapons and discharges of radioactive waste from the nuclear industry [15].

UNSCEAR assesses the biological effects of radiation exposure and also collects and collates information routinely on the doses that persons received from radiation from both natural and artificial sources. The results of the review published by UNSCEAR in 2000 reflects in the pie chart in figure 2.3 [11]. The annual effective dose estimated over the population of the world was about 2.8 mSv according to the report. Out of this value, a little over 85% of the total is from natural sources with about half coming from radon-222. Medical exposure of patients accounted for 14% of the total. The greatest variations in dose arise from radon in the home which is capable of giving an annual doses of 10 mSv or more. In most countries, annual radiation doses to occupational workers are limited by law to 50 mSv or less, though only a small fraction of the workforce exceeds 20 mSv. Members of the public are unlikely to receive more than a fraction of 1 mSv in a year from exposure to artificial sources due to controlled measures put in place to prevent these exposures. Patients during diagnostic procedures may receive around 10 mSv/year [11].

2.5.1 Nuclear Radiation Dose Units
For a unit mass of matter like human tissue, the amount of energy that ionizing radiation deposits is called the “absorbed dose” and is measured in a unit called the gray (Gy). Because different types of ionizing radiation interact differently with biological materials, equal amounts of energy deposited do not necessarily have the same biological effects. An example, a 1 Gy absorbed dose
to tissue from alpha radiation will be more harmful than the same absorbed dose from beta radiation. This is because an alpha particle loses its energy much more densely along its path. Due to this disparity, the quantity equivalent dose has been defined in order to put all the different types of ionizing radiation on an equal basis and is measured in a unit called Sievert (Sv) [11]. This can be obtained by multiplying the absorbed dose by a radiation weighting factor. Effective dose is also expressed in Sieverts and is obtained by multiplying the equivalent dose by a tissue or organ weighting factor that reflects the relative risk to that tissue or organ and then summing all of these weighted equivalent doses over all of the tissues or organs exposed. The weighting factor was introduced to solve the complication of risks caused by exposure to ionizing radiation in order to put everything on the same basis since the risks differ according to the tissue or organ exposed. In this way, the effective dose provides a measure of the radiation risk to people, irrespective of whether they have been exposed externally or by radioactive material deposited inside the body [11].

![Image](image-url)  
Figure 2.3: Average radiation exposure from all sources [11].

### 2.6 Cobalt 60
Cobalt (Co) is a metal and not radioactive as found in nature. Naturally non-radioactive cobalt occurs in various minerals and has been used for thousands of years to impart blue color to ceramic and glass, as first demonstrated by Swedish scientist George Brandt in 1735. Before then, many people thought that the cause of the blue color was from bismuth which occurs in nature alongside cobalt. Unstable cobalt is radioactive and man-made, and was discovered by
Glenn T. Seaborg and John Livingood at the University of California - Berkeley in the late 1930's. Cobalt-60 is the commonest radioactive isotope of cobalt [42] and is produced when structural materials like steel are exposed to neutron radiation as a by-product of nuclear reactor operations. Equation one (1) illustrates how radioactive cobalt-60 is derived from cobalt-59.

\[
^{59}\text{Co} (n, \gamma) ^{60}\text{Co}
\]

(1)

The γ-ray arises from the difference in binding energies of \(^{59}\text{Co}\) and \(^{60}\text{Co}\). This decays by a beta (β) emission to excited \(^{60}\text{Ni}^*\) which then assumes its stable state of \(^{60}\text{Ni}\) by emitting two γ-rays with energies 1.17 MeV and 1.33 MeV. The small energy difference in these gamma rays leads to the modelling of the source as monoenergetic with an average energy of 1.25MeV and with a half-life of 5.27 years. The two stage decay of the source can be represented as follows:

\[
^{60}\text{Co} \rightarrow ^{60}\text{Ni}^* + ^0\beta
\]

(2)

\[
^{60}\text{Ni}^* \rightarrow ^{60}\text{Ni} + \gamma (1.25 \text{ MeV})
\]

(3)

Figure 2.4: Decay scheme of cobalt – 60.

All cobalt isotopes including cobalt-60 are hard, brittle, gray metal with a bluish tint. They are solid under normal conditions and are similar to the properties of iron and nickel generally. Cobalt, like iron, can be magnetized. Cobalt-60 can be used in leveling and thickness gauges in industrial applications and large sources of cobalt-60 are used for sterilization of certain foods.
due to the powerful gamma radiation that kill bacteria and other pathogens without damaging the product, neither do they leave the product radioactive. Industrial radiography also makes use of cobalt-60 in a process similar to x-ray to detect structural flaws in metal parts. In medicine cobalt-60 is used in radiotherapy at hospitals [42]. Radionuclides such as cobalt-60 used in industry or medical treatment are usually encased in shielded metal containers or housings and they are referred to as radiation “sources”. Operators are kept from being exposed to the strong radiation due to the shielding. Nevertheless, medical or industrial radiation sources are lost or stolen occasionally, and these sources are referred to as “orphan sources”. Orphan sources represent a significant risk to the health of the public and the environment.

All ionizing radiation including that from cobalt-60 is known to be a risk factor for cancer. Due to the strong gamma rays emitted, external exposure to cobalt-60 is also considered a significant threat to life. The level of health risk depends on the quantity involved and on exposure conditions such as length of time of exposure, distance from the source (for external exposure) and whether the source was ingested or inhaled [42].

2.7 Work Done in the Research Field

2.7.1 Categorization of Radioactive Sources
The IAEA in 2003 amended the IAEA-TECDOC-1191 which provided a useful system for categorizing radioactive sources, according to radiological and other risks. The objective of the new IAEA-TECDOC-1344 [44] was to provide a simple, logical, consistent system for ranking radioactive sources based on their potential to cause harm to human health, and also group the practices in which these sources are used discretely into categories. The purpose of the categorization of radioactive sources was to provide an acceptable basis for risk-informed decision making internationally. It is expected that the new categorization system will be used as an input to many activities relating to the safety and security of radioactive sources. The categorization of the radioactive sources used especially in industry, medicine, agriculture, research and education are provided in the new IAEA-TECDOC-1344. Radioactive sources, such as radioisotope thermoelectric generators (RTGs), that may be under military control also fall under the principles of this new categorization [44].
2.7.2 Design Basis Threat

Hagemann [45] presented a study on the Design Basis Threat in which he stated that developing a European physical protection concept was one of the security fundamentals that a State's physical protection system should be based on. The author further maintains that the most commonly used methodology for the design and evaluation of physical protection of nuclear material and facilities is the DBT methodology. This methodology uses identification of a threat, which is developed from the State’s evaluation of existing threats. The author continued to state that open borders inside the European Union enable those individuals, who could create a potential threat to nuclear material or nuclear facilities, to move from one Member State to another without restrictions or the realistic opportunity for relevant authorities to be informed timely about such possible movements. The similarity in the results may put in question the idea of defining national Design Basis Threat in each State to identify threats to the individual States [45]. The author explained that the similarities in the threat evaluation and the DBT will then contribute to more similarity in the design basis for physical protection concepts. The DBT is an important basis, but there are more factors, which determine the design and the evaluation of a physical protection concept. These factors are related to the State's physical protection system, which consists of elements like the State’s response capabilities to malevolent acts against nuclear material or facilities, the culture and the legal and regulatory framework of physical protection. The development of a European physical protection concept would clearly be part of the efforts and policy in order to harmonize rules, regulations and standards within the European Union although each State should identify its own threats on local conditions. The author’s study did not touch on the political aspects and potential problems related to harmonization in the EU and did not speculate upon the possibilities, however the DBT methodology was investigated. The relevant elements to be the subject for harmonization were to be identified and their functions evaluated [45].

2.7.3 Physical Protection Systems

Nawal and Nassef [46] presented a study on the main objective of a physical protection System, in which they said its main purpose is to prevent radiological sabotage of nuclear facility and theft of nuclear materials. Their paper describes a procedure for effective physical protection of nuclear facilities, as well as physical protection of nuclear Materials (NMs) in use, storage, and
transport. Their procedure involves categorizing the nuclear facility targets and how to protect them. The authors then propose a preliminary plan for a site visit for the purposes of evaluating the PPS, and ensuring that it is in Compliance with the IAEA standards, which is part of The International Physical Protection Advisory Service (IPPAS) guidelines [47], and also meets the necessary conditions set out in Egyptian Regulations (licensing) of the facility. The implementation of this plan could strengthen physical protection of Egyptian nuclear facilities [46].

In 2012, similar work was done by Martin Hromada and Ludek Lukas in which they discussed the conceptual approach of Critical Infrastructure Protection measures and evaluation. They saw this as a basic element of maintaining vital societal functions from social and economic perspective. The authors emphasized the need for optimal and relevant protection and security measures selection for establishing a framework for evaluation of Critical Infrastructure Protection and interconnection to risk assessment in the Czech Republic [48].

Bakr and Hamed [34] presented a study on the experience in many parts of the world which continues to show that movements of radioactive material outside of the regulatory control and legal framework may occur. The aim of their article was to discuss a proposed physical protection system for improving the protection of radioactive sources used for medical purposes in a radiotherapy facility in Egypt.

Nawal M. Said and M. H. Nassef in 2014, emphasized the main objective of a physical protection system as the ability to prevent radiological sabotage of the nuclear facility and theft of nuclear materials. Their paper described a procedure for effective physical protection of nuclear facilities as well as physical protection of nuclear materials (NMs) in use, storage and in transport. Their procedure involved categorizing the nuclear facility targets and how to protect them. They then proposed a preliminary plan for a site visit for the purposes of evaluating the PPS to ensure that it is in compliance with the International Atomic Energy Agency standards, and the International Physical Protection Advisory Service (IPPAS) guidelines. They also pointed out that this met the necessary conditions set out in Egyptian regulations (licensing) of
the facility. They recommended that this plan be implemented in order to strengthen physical protection of Egyptian nuclear facilities [46].

### 2.7.4 Security Evaluation Tools

In 2013, Haitao, et al. studied protection effectiveness as an important metric to judge whether a security system was good or not. In their paper, a security system deployed in a guard field involving guards and security systems was regarded abstractly as a security network. A quantitative method for evaluating protection effectiveness based on entropy theory was introduced. They proposed a protection intensity model, which can be used to calculate the protection intensity of a stationary or moving object provided by a security system or a security network. Using the protection intensity model, an algorithm for finding the minimal protection intensity paths of a field deployed multiple security system is proposed. The minimal protection intensity paths could be considered as the measure of effectiveness of the security networks. Finally, they presented the simulation of the methods and models [49].

Lovecek, et al. [50] described the structure of complex security system dedicated to protection of critical infrastructure elements, such as strategic state objects, from intentional actions of people that aim to steal and damage or destroy their objects of interest. Their study defined basic factors of security system that should be taken into account in case of its qualitative evaluation – technical effectiveness or reliability, human factors, economic efficiency and optimality. The main significance of the paper was the analysis and comparison of tools for quantitative evaluation of security systems of critical infrastructure elements such as SATANO, EASI, ASD, SAVI, ASSESS, JCATS, SAPE, SPRUT, Vega-2 and Analizator SFZ.

Norichika Terao and Mitsutoshi Suzuki [51] describe how EASI, a computer code, can be used to evaluate the probability of an adversary’s interruption ($P_I$) in a specific scenario. The purpose of their study was to devise a quantification method for $P_I$ by considering the influence of uncertainty and variability. They attempted to devise a new calculation method for three components of $P_I$ which are the probability of detection $P(D_i)$, the probability of successful communication to the response force $P(C_i)$ and the probability of the response force arriving prior to the end of the adversary’s completion of the attack $P(R/A_i)$. In addition they designed a
hypothetical nuclear facility and an adversary attack scenario on which they then assess the $P_1$ value using their new method. They also set the performance Parameters of the facility as temporary hypothetical values without a real performance test. Finally they attempted to express the uncertainty and variability of each element of the facility using the Monte Carlo method [51].

Echeta, et al. in 2014 presented a study that attempted to quantitatively analyse the effectiveness of a physical protection system designed for an oil refinery using the estimate of adversary sequence interruption model. The output from the model is the Probability of Interruption of a potential attack scenario along a specific path. The effectiveness of a security system depends on the value of the probability of interruption. Results obtained show that the values of the probability of interruption of the adversaries for the most likely adversary paths were very low. Therefore they proposed an upgrade in the protection elements and realised that the values of the new probability of interruption increased from 0 to a range of 0.66 to 0.89. They concluded that the overall security has been strengthened with the upgrade in protection elements [52].

2.7.5 Security Simulations
Sabina, et al. [53] explored the use of discrete-event simulation for the design and control of protection systems for fixed-site facilities housing items of significant value. They began by discussing several modeling and simulation activities currently performed in designing and analyzing these protection systems, and then discussed capabilities that design/analysis tools should have. The remainder of the paper then discussed in detail how some of these new capabilities have been implemented in software to achieve a prototype design and analysis tool. The simulation software technology provided a communications mechanism between a running simulation and one or more external programs. In the prototype security analysis tool, these capabilities are used to facilitate human-in-the-loop interaction and to support a real-time connection to a virtual reality (VR) model of the facility being analyzed. This simulation tool can be used for both training (in real-time mode) and facility analysis and design (in fast mode).

Bari, et al. in 2006 published a research article that provided an overview of the methodology approach developed by the Generation IV International Forum Expert Group on Proliferation Resistance and Physical Protection for evaluation of Proliferation Resistance and Physical
Protection robustness of Generation IV nuclear energy systems options. The methodology considered a set of alternative systems and evaluated their resistance or robustness to a collection of potential threats. For the challenges considered, the response of the system to these challenges is assessed and expressed in terms of outcomes. The challenges to the system are given by the threats posed by potential proliferant States and sub-national adversaries on the nuclear systems. The characteristics of the Generation IV systems, both technical and institutional, were used to evaluate their response to the threats and determine their resistance against the proliferation threats and robustness against sabotage and theft threats. The system response encompasses three main elements that include System Element Identification, in which the nuclear energy system is decomposed into smaller elements (subsystems) at a level amenable to further analysis [54]. The second element is Target Identification and Categorization, in which a systematic process is used to identify and select representative targets for different categories of pathways within each system element that actors (proliferant States or adversaries) might choose to use or attack. Pathway identification and refinement was the third element. Pathways are defined as potential sequences of events and actions followed by the proliferant State or adversary to achieve its objectives (proliferation, theft or sabotage). For each target, individual pathway segments are developed through a systematic process, analyzed at a high level and screened where possible. Segments are connected into full pathways and analyzed in detail. The outcomes of the system response are expressed in terms of PR & PP measures. Measures are high-level characteristics of a pathway that include information important to the evaluation methodology users and to the decisions of a proliferant State or adversary. The authors first evaluated for segments and then aggregated for complete pathways. Results were aggregated as appropriate to permit pathway comparisons and system assessment. The article highlighted the current achievements in the development of the Proliferation Resistance and Physical Protection Evaluation Methodology. They also briefly stated the way forward together with some conclusions [54].

Inkom, et al. [55] describe the design of a Radio Frequency Identification (RFID) personnel access control/anti-intruder system that uses an active Quad Tag (RWD-QT) Reader/Writer module in direct conjunction with a Microchip PIC18F4550 microcontroller which provides control, non-volatile memory, data processing and external communication functions. The designed system obtains signals from an RFID module, motion detectors and vibration sensors to
effectively control a dot-matrix LED display. It also controls the alarm sounders, an electric strike door and in the process provide a low-cost power-efficient and a reliable means of supplementing traditional methods of providing physical protection for research reactor buildings. Relevant IAEA documents such as INFCIRC/225/Rev.4 and TECDOC 967 (Rev.1) were duly consulted for the necessary guidance in this research and development effort by the authors.

2.7.6 Defense-in-Depth
Coole, et al. [56] presented a paper on how a common language in the sense of joint, with consistency of meaning is a critical step in the evolution of a profession. They further stated that whilst the debate as to whether or not security should be considered a profession is ongoing there is no doubt that the wider community of professionals operating in the security domain is working towards achieving recognition of security as a profession. The concepts of defense-in-depth, protection-in-depth and security-in-depth have been used synonymously by different groups across the domain. They further emphasized that these concepts represent the very foundation of effective security architecture which are hierarchical in nature and have specific meaning. Their paper through comparative analysis clearly defines the difference between defense-in-depth, protection-in-depth and security-in-depth and establishes the hierarchy such that common understanding can be achieved.

2.7.7 Intrusion Detection Systems
In 2011, the United States’ Nuclear Regulatory Commission (NRC) published a report which provides information relative to designing, installing, testing, maintaining, and monitoring intrusion detection systems (IDSs) and subsystems used for the protection of facilities licensed by the NRC. The report contains information on the application, use, function, installation, maintenance, and testing parameters for internal and external IDSs and subsystems, including information on communication media, assessment procedures, and monitoring. The information is intended to assist licensees in designing, installing, employing, and maintaining IDSs at their facilities [57].
Dean, et al. [58] developed a model for malicious intrusions in infrastructure facilities using a network representation of the system structure together with Markov models of intruder progress and strategy. The structure provides an explicit mechanism to estimate the probability of successful breaches of physical security and to evaluate potential improvements. It is thought that intruders often plan their attacks using simulation to analyze varying levels of imperfect information. An example is an intruder attempting to place an explosive device on an airplane at an airport gate, illustrating the structure and potential application of the model.

Francesco Flammini in 2010 found that it is prudent to establish a good trade-off between the probability of detection (POD), the false alarm rate (FAR) and the reliability of detectors. He said existing solutions try to achieve this aim either by using the most advanced technologies or by combining basic sensors in logical OR/AND relations. However, these approaches are either not cost-effective or they do not allow for the necessary flexibility to obtain the right balance. In the paper, he proposed a majority voting scheme for multiple technology detectors which he evaluated using stochastic modeling techniques. He believes this solution has major advantages and permits good overall dependability while allowing the use of low-cost detectors. This approach also enables a precise-fine tuning of POD and FAR parameters. To the best of his knowledge, no similar system has been studied in depth in the research literature. He provided a set of results which clearly show the advantages of his proposed approach [59].

Zidan W. I. [60] described how Cluster Sensors are vital components of physical protection systems and because of that are, used extensively to detect intrusion. He insisted that it was essential to ensure that a particular sensor met the design criteria of the physical protection system. In his paper, performance evaluation and operational procedures of Glass Breakage (GB) and Open Door (OD) sensors were presented and discussed. Several intrusion tests were carried out inside the detection areas of the sensors in order to evaluate their performance during a particular intrusion process. Experimental results were then presented in the paper and the probabilities of detection for both GB and OD sensors were estimated.
2.7.8 Vulnerability Assessments

In 2009, Sung, et al. presented a vulnerability assessment which, according to them, is essential for the efficient operation of a PPS. Previous assessment codes have used a simple model called an adversary sequence diagram. In their study, the use of a two-dimensional (2D) map of a facility as a model for a PPS was suggested as an alternative approach. The analysis of a 2D model, however, consumes a lot of computer time. Accordingly, a generalized heuristic algorithm has been applied to address this issue. The proposed assessment method was implemented in a computer code called System Analysis of Physical Protection Effectiveness (SAPE). This code was evaluated for feasibility by applying it to various facilities. To help upgrade a PPS, a sensitivity analysis of all protection elements along a chosen path is proposed. SAPE helps to accurately and intuitively assess PPS [61].

Roger Johnston [62] presented how security vulnerabilities should be handled by saying, when security vulnerabilities are discovered; it is often unclear how much public disclosure of the vulnerabilities is prudent. This is especially true for both physical security and cyber security. “We never want to help the ‘bad guys’ more than the ‘good guys’, but if the good guys are not made aware of the problems, they are unlikely to fix them”, was a quote in his analysis. The paper presented a unique semi-quantitative tool, called the “Vulnerability Disclosure Index” (VDI), to help determine how much disclosure of vulnerabilities is warranted and in what forum. The author stipulated that the VDI certainly does not represent the final, definitive answer to this complex issue. It does, however, provide a starting point for thinking about some of the factors that must go into making such a decision. Moreover, anyone using the VDI tool can at least claim to have shown some degree of responsibility in contemplating disclosure issues.

The Stanford Study Group in 2004 presented a paper that came out of a week-long study in August 2002 to assist ongoing efforts inside and outside the government to remedy some vulnerabilities of the international shipping. The objective of the study was to identify the most important research initiatives and the major policy issues that need to be addressed in order to improve security of imported goods by involving shipping containers. This would help particularly against the importation of nuclear materials and weapons since these containers will be scanned for radiation levels. This process also helps in maintaining an open trading system.
For the international shipping system to be effective, it should be able to detect nuclear weapons or special nuclear material before they reach U.S. ports and must be international in scope and reach. The group suggested that it must be acceptable economically both in terms of total cost and with respect to how these costs are allocated [63]. This was to be done through degrading gracefully when subjected to attack, producing actionable intelligence in a timely manner, treating false alarms realistically, adapting to a variety of local physical and political conditions, auditing, securing and granting access to the needed foreign and domestic security agencies and having clear lines of oversight responsibility. The group finally stated that the system should be flexible enough to allow for regular updates as users and operators gain experience and system performance is reviewed. The study employed a sample technical approach that was feasible technically and operationally and involves components already in the early deployment stage. The approach involves container certification, monitoring at ports of embarkation and debarkation continuously during shipment and storage and continuous data fusion. Their specific recommendations regarding system characteristics included rigorous testing during deployment and in the field, international coordination of standards and protocols, careful analysis of the system for compatibility with pertinent governmental policies and business and labor agreements and finally early provision for forward-looking research and development [63].

2.7.9 Cyber Security

Atul, et al. in 2013 presented a study on how Cyber security is used to protect information and information systems (networks, computers, data bases, data centers and applications) with appropriate procedural and technological security measures. The authors make it clear that firewalls, antivirus software, and other technological solutions for safeguarding personal data and computer networks are essential but are not sufficient to ensure security. They maintain that, as their nation rapidly builds its Cyber-Infrastructure, it is equally important that citizens are educated on how to work properly with such an infrastructure. To the authors, Cyber-Ethics, Cyber-Safety and Cyber-Security are issues that need to be integrated into the educational process beginning at an early age. Security counter measures help ensure the confidentiality, availability, and integrity of information systems by preventing or mitigating asset losses from Cyber security attacks. Recently, cyber security has emerged as an established discipline for computer systems and infrastructures with a focus on protection of valuable information stored
in those systems from adversaries who want to obtain, corrupt, damage, destroy or prohibit access to it [64]. In their work, the authors consider a wide-range of metaphors including those relating to military and other types of conflict, biological, health care, markets, three-dimensional space, and physical asset protection. These, in turn, lead to consideration of a variety of possible approaches for improving cyber security in the future. These approaches were labelled, “Heterogeneity”, “Motivating Secure Behavior” and “Cyber Wellness”. Cyber Security plays an important role in the development of information technology as well as Internet services, but attention is often primarily drawn to cyber security when there is a cyber-crime. They reiterate that the first thought on national cyber security therefore should be to determine how good the infrastructure for handling cyber-crimes is. The paper focuses on emerging trends in cyber security while adopting new technologies such as mobile computing, cloud computing, e-commerce and social networking. The paper also describes the problems caused by a lack of coordination between security agencies and the institutions involved in critical IT infrastructure [64].

Ralston, et al. [65] describes how the growing dependence of critical infrastructures and industrial automation on interconnected physical and cyber based control systems has resulted in a growing and previously unforeseen cyber security threat to Supervisory Control and Data Acquisition (SCADA) and Digital Combat Simulator (DCS) systems. Industrial organizations such as NERC and AGA as well as government organizations in the United States like NIST and SANDIA are responding to the cyber security threat faced by control systems and critical infrastructure through the development of guidelines, best practices, test beds, security tools and new technology. The authors refer to published research papers such as Byres and Lowe in 2005, Miller in 2005 and Greer in 2006, which all described the threats and vulnerabilities faced by SCADA and DCS systems and the challenges presented in attempting to secure these systems. Other research articles such as Byres and Franz in 2006, Strickles, et al. in 2003 were also cited for describing the application of existing security technologies and security practices [65]. The authors claim that the articulation of risk is an important component of a comprehensive, realistic, and long-term commitment to securing SCADA and DCS systems. They explain how Risk Assessment methods such as HHM, IIM and RFRM have been successfully applied to SCADA systems and have highlighted the need for quantifiable metrics. Quantifiable risk
analysis falls under the general category of probability risk analysis (PRA) which includes methods like FTA, ETA and FEMA. The authors stated that what is needed for SCADA and DCS cyber security risk analysis is to quantitatively determine the probability of an attack, the impact of the attack and the reduction in risk associated with a particular countermeasure. They further comment on two recent methods, one which was based on compromise graphs and the other on augmented vulnerability trees that have specifically targeted SCADA security [65].

Kristl A. G and Gregory D. W. in 2005 presented research on the increasing reliance on cyber technology to operate and control physical security system components. They claim there is a need for methods to assess and model the interactions between the cyber system and the physical security system to understand the effects of cyber technology on overall security system effectiveness. Their paper evaluates two methodologies for their applicability to the combined cyber and physical security problem. The comparison metrics include probabilities of detection, probability of interruption and probability of neutralization (P_N) which contribute to calculating the probability of system effectiveness (P_E) and the probability that the system can thwart an adversary attack [66]. P_E is well understood in practical applications of physical security but when the cyber security component is added, system behavior becomes more complex and difficult to model. The paper also examines two approaches which Bounding Analysis Approach (BAA) and Expected Value Approach (EVA) to determine their applicability to the combined physical and cyber security issue. These methods were assessed for a variety of security system characteristics to determine whether reasonable security decisions could be made based on their results. The assessments provided insight on an adversary’s behavior depending on what part of the physical security system is cyber-controlled. Analysis showed that the BAA is more suited to facility analyses than the EVA because it has the ability to identify and model an adversary’s most desirable attack path [66].

McDonald, et al. [67] describe a new hybrid modeling and simulation architecture that has been developed at Sandia for understanding and developing protections against and mitigations for cyber threats upon control systems. The authors first outlined the challenges to PCS security that can be addressed using these technologies. The paper then described Virtual Control System Environments (VCSE) that uses this approach and briefly discussed security research that Sandia
has performed using VCSE. The paper concludes with recommendations to the control systems security community for applying this valuable technology.

In 2015, Akinjide A. Akinola presented a study on how nuclear power plants have increased their vulnerability to cyber-attacks due to the widespread introduction of digital network systems to their operating systems. The author presented an attack tree approach that evaluates and analyse cyber-attacks quantitatively in a nuclear power plant network. He used information on a hypothetical nuclear power plant network to build attack trees that show different attack paths that external adversaries can use to compromise the network. In order to characterize the ease or difficulty of compromising each attack tree, he assigned numerical values to the leaf nodes. He then calculated the Return on Attack (ROA) for each intermediate node and the root node. This calculation was done by randomly varying the vulnerability values of the leaf nodes within the designated range. On observing high ROA values with the two Attack trees, he introduced and implemented countermeasures and modified the constructed network systems. He then recalculated the ROA and found out that the ROA values for the nodes were observed to decrease after implementing the countermeasures on the networks [68].

2.7.10 Security Breaches
John T. Jackson Jr. in 2011 presented a study on how the vulnerabilities of Balanced Magnetic Switches (BMS) render them defeatable by trivial means. He provided a detailed description of the most common BMS and the procedures accounting for its defeat that includes a method of how to design defeat tools and apparatus for analysis of any common BMS based upon glass reed technology [69].

Alexei Toropov [70] presented a study on the various techniques for defeating locks based on the act of exploiting vibration. He make reference to "bumping" as one of the techniques for manipulating cylinder locks that has become widespread in recent years. His problem was the fact that a large variety of mechanical locks can be opened quickly in a non-destructive manner by using simple attack tools. He studied the physical phenomena responsible for the vibration techniques of lock opening. He also considered the period of time during which the pins of a cylinder lock remain separated as a function of natural frequency, damping properties and lock
design parameters. On the basis of his analysis, he suggested some changes to lock design and assembly that can enhance the security of the lock and resist bumping attacks.

McNell, et al. in 2014 performed a series of lock breaching tests with five sets of standard shackle locks and 4 sets of puck style locks to test for vulnerability to a variety of tools like dremel rotary tool, an oxyacetylene torch, a drill press, a low temperature impact and compressive cutting jaws. In the dremel rotary tool test, they realized that the lock shackles were exposed to a dremel abrasive cutting wheel for a fixed time and the depth of penetration was measured. In the oxyacetylene test, the lock shackle was moved under an oxyacetylene flame at a constant velocity and the depth of cut was measured. In the drill press test, the lock was confined in a vice and two drill attempts were made using two different diameter drill bits and the percentage of lock failures was recorded. In the low temperature impact test, a pendulum was dropped while the lock temperature was lowered using difluoroethane (canned air) and the percentage of lock failures was recorded. Finally, in the compressive cutting test, the lock shackle was pressed by carbide tipped cutting jaws and the maximum Force at failure was measured. Results were compared to a previous study and were in general agreement, except the low temperature impact test [71].

2.7.11 Training with Physical Protection System Facilities

In 2015, Waller, et al. presented a research study on how difficult it is to train personnel about physical protection systems at nuclear facilities because these security systems are always in a continuous operation. This sometimes makes it practically impossible to access these systems for training problematic scenarios. The authors said an interactive model of a nuclear facility to demonstrate physical protection systems can provide instructive and cost-effective training to a wide range of personnel. They therefore modelled, designed and fabricated a hypothetical Lagassi Nuclear Research Institute (LNRI), which is been used by the International Atomic Energy Agency for nuclear security training. The PPS were divided into major categories consisting of lighting, fences, cameras, motion detection, annunciations and intrusion simulation. To allow for an interactive element, they used a Raspberry Pi microcomputer as an interface between various sensors introduced into the physical model, the alarms and the user [72]. The Interface code was written in the Python Programming language to allow sensors to
communicate with the computer. The model was tested for a specific fence-defeat training scenario and found to be a useful tool that allows a user both to visualize the protected area and interact with alarm panels. In addition, the measured delays through the alarm sequences were interfaced through the Raspberry Pi to a spreadsheet that estimates probability of interruption such that the user may determine whether an adversary has been interrupted prior to achieving his goal. This feature demonstrated to the user the benefit of timely alarm communications. The interactive physical model is a cost effective alternative to hands-on systems training [72].

2.7.12 Security Risk Management

Gebhard Geiger and Anselm Schaefer [73] published a paper talking about how violations of physical protection combined with threats of misuse of nuclear material that include terrorist attacks pose increasing challenges to global security. In view of this, they exploited recent advances in theoretical, applied risk and decision analysis to attain methodological and procedural improvements in security risk management with a special focus on quantitative risk assessment and the demarcation of acceptable risk. More precisely, they employed a recently developed model of optimal risky choice to compare and assess the cumulative probability distribution functions attached to safety and security risks. They said other related problems such as the standardization of risk acceptance criteria frequently used in physical protection could also be approached on this basis. With regard to nuclear and radiological threats, their paper suggests possible applications of the improved methods to the safety and security management of nuclear material, cost efficiency of risk management practices and the harmonization of international safety and security standards of physical protection. [73].

In 2015, Raphaël Duguay presented a paper on a high-level overview of the threats that high-risk radioactive sources represent and also their potential use as radiological weapons. His objective was to provide a discussion on existing threat assessment methodologies and security practices to protect high-risk radioactive sources including physical protection systems and security management. He explored the particular challenges associated with protecting high-risk radioactive sources against potential insider threats and some of the gaps related to transportation of such sources. Following the theory of Situational Crime Prevention, he proposed different
security approaches for mitigating the risk, explored different options and offered recommendations [74].
CHAPTER 3 Materials and Methods of Investigation

This chapter describes the materials used in the research work and also the methods of investigation such as evaluation of existing protection system, developing a Design Basis Threat and the procedure followed in the assessment, designing and evaluation of a PPS.

3.1 Materials

The purpose of installing a PPS is to protect a facility from unauthorized entry of adversaries and insiders who plans to engage in malevolent actions. The most important objectives are to prevent sabotage of critical equipment, deter theft of assets or information from within the facility, and protect people. A PPS must do its functions by either deterrence or a combination of detection, delay, and response [29]. To address the threats from malevolent acts involving radioactive sources, the designer of the PPS should bear in mind that radiological sources of certain magnitudes and types are more attractive to adversaries with malevolent intent than others [34]. This study assessed the current physical protection systems of the Centre for Applied Radiation Science and Technology and the assets therein (especially the $^{60}$Co source to be used for irradiation) and proposed a secure PPS. The PPS was designed for all three buildings in the Center, namely F2A, F2C and F2E, but more emphasis was placed on F2C because it houses most of the Center’s assets including the $^{60}$Co source used for irradiation. The layout of the University and floor plans of CARST buildings are shown in figures 3.1 to 3.4.

![Google map showing the layout of the North-West University (NWU).](image)

Figure 3.1: Google map showing the layout of the North-West University (NWU).
Figure 3. 2: Floor plan of building F2C at CARST

Figure 3. 3: Floor plan of building F2E at CARST
Figure 3. 4: Floor plan of building F2A at CARST

Figure 3. 5: Flow diagram for the steps in the methodology
3.1.1 Assessment of Assets

The first step involved identifying the main assets of the Center.

Table 3. 1: The list of assets located in the three buildings of the Center.

<table>
<thead>
<tr>
<th>Building F2A</th>
<th>Building F2C</th>
<th>Building F2E</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 MiniBeta Liquid Scintillator with a 370kBq $^{226}$Ra source</td>
<td>2 High Purity Germanium Detectors</td>
<td>1 Liquid Scintillator (for Alpha and Beta Spectroscopy with a 555kBq $^{152}$Eu source</td>
</tr>
<tr>
<td>Stationary Items of the Center</td>
<td>4 Sodium Iodide Detectors</td>
<td>1 Eco-Gamma Monitor</td>
</tr>
<tr>
<td>12 Computers</td>
<td>2 Alpha Spectrometers</td>
<td>2 Alpha Guard Pro Monitors</td>
</tr>
<tr>
<td>1 High Purity Germanium Detector</td>
<td>15 Computers</td>
<td>2 Computers</td>
</tr>
<tr>
<td></td>
<td>2.5 TBq $^{60}$Co Source</td>
<td></td>
</tr>
</tbody>
</table>

**Calibration Radioactive Source materials**

<table>
<thead>
<tr>
<th>Nuclide</th>
<th>Activity</th>
<th>Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>$^{137}$Ba</td>
<td>40.7kBq</td>
<td>solid</td>
</tr>
<tr>
<td>$^{137}$Cs</td>
<td>40.2kBq</td>
<td>solid</td>
</tr>
<tr>
<td>$^{60}$Co</td>
<td>39.7kBq</td>
<td>solid</td>
</tr>
<tr>
<td>$^{60}$Co</td>
<td>452kBq</td>
<td>solid</td>
</tr>
<tr>
<td>$^{22}$Na</td>
<td>37.2kBq</td>
<td>solid</td>
</tr>
<tr>
<td>$^{24}$Am</td>
<td>34.7kBq</td>
<td>solid</td>
</tr>
<tr>
<td>$^{152}$Eu</td>
<td>44.8kBq</td>
<td>solid</td>
</tr>
<tr>
<td>$^{226}$Ra</td>
<td>31.9kBq</td>
<td>solid</td>
</tr>
</tbody>
</table>

The initial activity in 1987 of the $^{60}$Co source which is the main asset in Building F2C was 93 TBq or 2500 Curie. Based on these figures, calculations were done to get the current activity as of June 2015. The maximum activity that the Eldorado 78 can accommodate is a total activity of 444 TBq or 12000 Curie. The higher activity of the source makes it more prudent to have a secured PPS in place because when the source is upgraded, it becomes more harmful if it gets out of regulatory control [75]. Current radiation measurements with the source in the safe position are 1 µSv per hour on the side of the shield (closest to the source). The dose rate at the collimators is 23 µSv per hour but this is probably because the collimators are made of the Depleted Uranium.
If the source is upgraded to 12000 Curie (444 TBq), the estimated dose rate at 1 meter from the same survey point, increases to 50 µSv per hour. This is acceptable for a low-occupancy irradiation vault but not accepted when the source gets out of regulatory control [75].

3.1.2 Source Operation and Specifications
The Eldorado 78 machine makes use of an existing treatment head with an existing radioactive source. The beam direction is vertical [beam up] but can be changed to face any direction of choice. Specimens are placed on a Perspex window mounted into the top cover the size of which matches the field aperture of the beam collimator of approximately 200 x 200mm. The collimator is always at full aperture field size. The design of the system allows the source to be replaced at any time as long as it is supplied in a standard Theratronics round source drawer. The Console provides power to the machine via a 15 Amp circuit breaker which in turn is supplied from a standard 230 V wall socket. The source position is indicated via 20mm LED lights, fully exposed when red and fully retracted when green [75].

3.1.3 Pneumatic System
The compressor provides air pressure that is maintained at between 40 and 60 psi. The air cylinder pressure is maintained at 28 psi by a pressure control valve / pressure gauge combination. The speed of the source drawer movement is controlled by adjustable air flow adjustors to maintain a fixed transfer time. A pressure switch safety interlock activates if the pressure falls below the minimum air tank pressure, the solenoid valves are de-activated and the source returns to the fully retracted position [75].

3.1.4 Engineered Safety Features
The system is designed to automatically retract the source in the event of;

- Timer reading zero;
- Set time being cancelled;
- Power failing;
- Main tank air pressure falling below pre-set safety level;
- The door to the room is opening;
- The emergency button on the console being depressed.
Figure 3. 6: Eldorado 78 $^{60}$Co package at storage facility awaiting preparation for transport [75].

Figure 3. 7: Eldorado 78 $^{60}$Co package description [75].
3.2 Methods of Investigation

3.2.1 Evaluation of Existing Physical Protection Systems

The second step evaluated the protection systems available at the center, if any. Currently, the Center has modest deterrents in place such as metal fence around the three buildings and burglar bar gates on all entrance doors of the buildings (F2A, F2C and F2E) except one door at F2C. The burglar bar gates for F2E are all located before the entrance doors whilst for F2A and F2C, one of their burglar bar gates is located behind the entrance door and the others are located before the entrance doors. Building F2C has three entrance doors and building F2A has two entrance doors while building F2E has four entrance doors. The windows of all the three buildings are also lined with burglar bars at their openings. These bars are aligned across the windows in F2E but are only aligned at the edges leaving the centers open for both F2C and F2A. The room housing the $^{60}$Co source has no windows but has two doors, one opening to the outside opposite the Animal health department and the other opening into a Nuclear Physics laboratory with high purity germanium detectors, sodium iodide detectors and alpha spectrometers. These doors are made of wood. There are no monitoring cameras in the rooms or on access doors. The access to the source room is locked manually. The functions of the existing protection system in the Center are dependent mainly on the initial response of the security guards who only come in the evenings.

In the event of any intrusion the guards call the University security for help. The security office is located a kilometer away from the Center. Thus, upgrading the PPS is clearly necessary to cover the main functions of detection, delay, and response for ensuring the security and safety of the radioactive source and other critical assets.

3.2.2 Assessment of Risk to the Facility

The third step involved assessing the risk to the facility (Center). Risk is associated with virtually every activity one can imagine, but for the purposes of this research, we are going to limit the meaning to the uncertainty of financial loss, the variations between actual and expected results or the probability that a loss has occurred or will occur [76]. Risk should not be confused with perils, which are the causes of risk, for example fire, flood and earthquake. Nor should risk be confused with a hazard (or vulnerability), which is a contributing factor of a peril, example a loaded gun, a bottle of caustic acid, a bunch of oily rags or a warehouse used for storing highly flammable products. The possible end result of risk is actual loss or a decrease in value.
Generally, risk is speculative. Risk Assessment is a rational and orderly approach to problem identification and probability determination. It is a method for estimating the expected loss from the occurrence of an adverse event. Risk Assessment will never be a precise methodology because it is about estimation and probabilities [76]. The Centre for Applied Radiation Science and Technology is dedicated to teaching, research, and guiding students and young scientists in the field of Applied Radiation Sciences. The Center conducts research into Naturally Occurring Radioactive Materials (NORMs) and man-made radioactive materials in mining sites throughout South Africa. It has at its disposal critical equipment used in its training and research work. In any security event concerning the assets of the facility, the Center stands the chance of economic loss since these assets are worth millions of Rands (South Africa’s currency).

Most facilities conduct routine Risk Assessment for their security system in order to determine whether their security measures are adequate to protect the relevant asset. These routine assessments help to identify areas that need improvement if the existing systems are not adequate or if there are changes in threats or assets needing protection. These Risk Assessments might well produce different results for different facilities, but generally they all include consideration of likelihood of a negative event, in this case a security incident and its consequences. Security risk can be measured quantitatively through the use of the equation:

\[ R = P_A \times (1 - P_E) \times C \]  

(4)

where:

- \( R \) is the risk to the facility in the event of an adversary getting access to or stealing critical assets;
- \( P_A \) is the probability of an adversary attack during a period of time;
- \( P_E \) is the effectiveness of the PPS against the identified threat;
- \((1 - P_E)\) is the vulnerability of the PPS against the identified threat;
- \( C \) is the consequence value [77].

The probability of an adversary attack during a period of time (\(P_A\)) can be very difficult to determine, but the probability ranges from 0 (no chance at all of an attack) to 1.0 (certainty of an attack). Critical assets that are valuable and whose consequence of loss will be high if a security event occurs often certainly require protection even if \(P_A\) is low. To be conservative, we set the \(P_A\) at 1.0, i.e., we assume that there will be an attack.
The effectiveness of the PPS to identified threat is related to the probability of interruption by the respondents and the probability of neutralization of the adversary, and is given by the equation:

\[ P_E = P_I \times P_N. \]  

(5)

### 3.2.3 Assessment of Risk due to the $^{60}$Co irradiation source

The risk to the $^{60}$Co source was assessed. In an event where there is unauthorized removal of the source from the Center out of regulatory control, unwarranted irradiation of the public and environment may occur. In the event of a sabotage attack where the adversary just needs to be close to the asset and enough time to cause damage, there may be irradiation of the public and environment. For example, given that the doors of the source room are currently made of wood and are not fire-resistant, a fire in the room set by adversaries could result in a serious radiation incident. If adversaries try to remove the source from its protecting shield after successfully taking the source from the Center, this could also lead to the irradiation and contamination of themselves, the public and the environment. If there is an attempt to acquire scrap metals for sale by removing the source head of the irradiating unit, irradiation and contamination may also occur [78]. Similar sources to the Center’s $^{60}$Co source can be found worldwide and number in the millions. Consequently, security measures should be directed at those sources that pose the greatest risks. With this in mind, the IAEA developed a new categorization system for radioactive sources in October of 2003 [44] to ensure that the sources are maintained under a control commensurate with the radiological risks. This categorization system is based on the potential for radioactive sources to cause deterministic effects, i.e., health effects which do not appear until threshold values are exceeded and for which the severity of effect increases with the dose beyond the threshold. An amount of radioactive material is considered “dangerous” if it could cause permanent injury or be immediately life threatening if not managed safely and securely [78]. The risk to the public for an uncontrolled dangerous source is calculated through the following equations:

For all materials, the risk factor is calculated by the aggregate of A/D equation

\[ \text{Aggregate } \frac{A}{D_1} = \sum_i \frac{A_i}{D_{i,j}} \]  

(6)

where:

Aggregate A/D is the risk factor, (its value ranges from 0.01 to 1000 or above);
Ai is the activity in (TBq) of each radionuclide over which control could be lost during an emergency/event; and
D1,i is the constant for isotopes [44].

For dispersible materials, the risk factor (RF) is calculated by the equation:

\[
\text{Aggregate} \frac{A}{D_2} = \sum_i \frac{A_i}{D_{2,i}}
\]  (7)

where:
Ai is the activity in (TBq) of each radionuclide i that is in a dispersible form over which control could be lost during an emergency/event; and
D_{2,i} is the constant for isotopes [44].

3.2.4 Threat Assessment

A DBT was developed at the fourth step which was based on the threat assessment of the facility’s assets and radioactive sources. The purpose of doing a Design Basis Threat, which is a way to identify threats was to use it as a tool to provide a common basis for planning for physical protection by the operator and approval of its physical protection plan by the competent authority for nuclear security. The use of a DBT threat assessment methodology is recommended by the IAEA as the best method to design the security measures for specific sources [79]. An analysis was done for the possible consequences of unauthorized acquisition of the radioactive sources from the Center, and based on the vulnerability assessment for specific sources, determination of the risk was made. The level of this risk determined the security measures required to protect the sources. The higher the risk, the more capability will be required from the security systems to protect the sources [80]. The facility for which the threat was assessed is CARST located on the campus of the North-West University (Mafikeng Campus). The Center is located between an undergraduate residence of the University named Lots City and the Animal health department of the University. The University is located at Mmabutho, a town in the North West Province of South Africa. Mmabutho is closer to the Mafikeng town which is the capital town of the North West Province. The Center has four (4) permanent workers of which two live in Mmabutho and the other two live in Mafikeng. Crimes rates in and around Mafikeng and Mmabutho are high and, as a result, a threat to the facility. In 2013, Mafikeng recorded a total of 4107 crimes while
Mmabatho recorded a total of 4349 [81]. In 2014 Mafikeng again recorded 4172 crimes while Mmabatho recorded a total of 3908 crimes [82]. In 2015 Mafikeng recorded 4139 crimes while Mmabatho recorded a total of 4395 crimes [83]. The next three tables below show some selected crimes out of the total crimes that are a threat to the facility.

Tables 3.2 to 3.4 represent selected crimes committed in Mafikeng and Mmabatho in the North-West Province of South Africa in 2013, 2014, and 2015. The province has 78 towns and cities. Out of this number the top ten in terms of number of crimes are projected. The crimes, number, and the position out of the top ten worst cities and towns of the 78 are presented in the tables.

Table 3.2: Selected crimes committed in Mafikeng and Mmabatho in 2013 [81].

<table>
<thead>
<tr>
<th>Crime</th>
<th>Mafikeng (No. of cases)</th>
<th>Position out of top 10 worst cities</th>
<th>Mmabatho (No. of cases)</th>
<th>Position out of top 10 worst cities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlawful possession of fire arms and ammunition</td>
<td>9</td>
<td>-</td>
<td>4</td>
<td>-</td>
</tr>
<tr>
<td>Common robbery</td>
<td>164</td>
<td>2\textsuperscript{nd}</td>
<td>110</td>
<td>5\textsuperscript{th}</td>
</tr>
<tr>
<td>Robbery with aggravating circumstances</td>
<td>205</td>
<td>6\textsuperscript{th}</td>
<td>308</td>
<td>3\textsuperscript{rd}</td>
</tr>
<tr>
<td>Malicious injury to properties</td>
<td>260</td>
<td>5\textsuperscript{th}</td>
<td>333</td>
<td>3\textsuperscript{rd}</td>
</tr>
<tr>
<td>Burglary at non-residential premises</td>
<td>313</td>
<td>3\textsuperscript{rd}</td>
<td>135</td>
<td>10\textsuperscript{th}</td>
</tr>
<tr>
<td>Drug related crimes</td>
<td>112</td>
<td>-</td>
<td>302</td>
<td>7\textsuperscript{th}</td>
</tr>
<tr>
<td>Robbery at non-residential premises</td>
<td>32</td>
<td>-</td>
<td>83</td>
<td>1\textsuperscript{st}</td>
</tr>
<tr>
<td>Kidnapping</td>
<td>19</td>
<td>1\textsuperscript{st}</td>
<td>9</td>
<td>8\textsuperscript{th}</td>
</tr>
<tr>
<td>Burglary at residential premises</td>
<td>385</td>
<td>-</td>
<td>844</td>
<td>4\textsuperscript{th}</td>
</tr>
<tr>
<td>Robbery at residential premises</td>
<td>24</td>
<td>-</td>
<td>77</td>
<td>3\textsuperscript{rd}</td>
</tr>
<tr>
<td>Crimen injuria (stalking)</td>
<td>80</td>
<td>4\textsuperscript{th}</td>
<td>54</td>
<td>6\textsuperscript{th}</td>
</tr>
<tr>
<td>Carjacking</td>
<td>9</td>
<td>9\textsuperscript{th}</td>
<td>13</td>
<td>5\textsuperscript{th}</td>
</tr>
</tbody>
</table>
Table 3.3: Selected crimes committed in Mafikeng and Mmabatho in 2014 [82].

<table>
<thead>
<tr>
<th>Crime</th>
<th>Mafikeng (No. of cases)</th>
<th>Position out of top 10 worst cities</th>
<th>Mmabatho (No. of cases)</th>
<th>Position out of top 10 worst cities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlawful possession of fire arms and ammunition</td>
<td>8</td>
<td>-</td>
<td>21</td>
<td>6th</td>
</tr>
<tr>
<td>Common robbery</td>
<td>133</td>
<td>2nd</td>
<td>96</td>
<td>6th</td>
</tr>
<tr>
<td>Robbery with aggravating circumstances</td>
<td>234</td>
<td>8th</td>
<td>330</td>
<td>2nd</td>
</tr>
<tr>
<td>Malicious injury to properties</td>
<td>169</td>
<td>-</td>
<td>220</td>
<td>6th</td>
</tr>
<tr>
<td>Burglary at non-residential premises</td>
<td>213</td>
<td>5th</td>
<td>131</td>
<td>9th</td>
</tr>
<tr>
<td>Drug related crimes</td>
<td>223</td>
<td>-</td>
<td>385</td>
<td>8th</td>
</tr>
<tr>
<td>Robbery at non-residential premises</td>
<td>48</td>
<td>5th</td>
<td>76</td>
<td>3rd</td>
</tr>
<tr>
<td>Kidnapping</td>
<td>13</td>
<td>7th</td>
<td>14</td>
<td>5th</td>
</tr>
<tr>
<td>Burglary at residential premises</td>
<td>415</td>
<td>-</td>
<td>651</td>
<td>4th</td>
</tr>
<tr>
<td>Robbery at residential premises</td>
<td>35</td>
<td>9th</td>
<td>82</td>
<td>2nd</td>
</tr>
<tr>
<td>Crimen injuria (stalking)</td>
<td>46</td>
<td>8th</td>
<td>41</td>
<td>-</td>
</tr>
<tr>
<td>Carjacking</td>
<td>10</td>
<td>7th</td>
<td>15</td>
<td>3rd</td>
</tr>
</tbody>
</table>
Table 3.4: Selected crimes committed in Mafikeng and Mmabatho in 2015 [83].

<table>
<thead>
<tr>
<th>Crime</th>
<th>Mafikeng (No. of cases)</th>
<th>Position out of top 10 worst cities</th>
<th>Mmabatho (No. of cases)</th>
<th>Position out of top 10 worst cities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlawful possession of fire arms and ammunition</td>
<td>15</td>
<td>-</td>
<td>16</td>
<td>10th</td>
</tr>
<tr>
<td>Common robbery</td>
<td>114</td>
<td>2nd</td>
<td>108</td>
<td>4th</td>
</tr>
<tr>
<td>Robbery with aggravating circumstances</td>
<td>236</td>
<td>7th</td>
<td>352</td>
<td>2nd</td>
</tr>
<tr>
<td>Malicious injury to properties</td>
<td>156</td>
<td>-</td>
<td>188</td>
<td>8th</td>
</tr>
<tr>
<td>Burglary at non-residential premises</td>
<td>268</td>
<td>4th</td>
<td>172</td>
<td>7th</td>
</tr>
<tr>
<td>Drug related crimes</td>
<td>278</td>
<td>-</td>
<td>433</td>
<td>7th</td>
</tr>
<tr>
<td>Robbery at non-residential premises</td>
<td>50</td>
<td>5th</td>
<td>70</td>
<td>2nd</td>
</tr>
<tr>
<td>Kidnapping</td>
<td>9</td>
<td>8th</td>
<td>8</td>
<td>-</td>
</tr>
<tr>
<td>Burglary at residential premises</td>
<td>410</td>
<td>-</td>
<td>920</td>
<td>2nd</td>
</tr>
<tr>
<td>Robbery at residential premises</td>
<td>34</td>
<td>-</td>
<td>108</td>
<td>1st</td>
</tr>
<tr>
<td>Crimen injuria (stalking)</td>
<td>45</td>
<td>7th</td>
<td>25</td>
<td>-</td>
</tr>
<tr>
<td>Carjacking</td>
<td>5</td>
<td>-</td>
<td>7</td>
<td>-</td>
</tr>
</tbody>
</table>

### 3.2.4.1 Types and Tactics of Adversaries

In any attack against a facility, there are three general kinds of potential adversaries involved. These include outside adversaries (“Outsiders”), inside adversaries (“Insiders” who work at the facility or provide services), and Outsiders working in collusion with Insiders [29]. Outsiders can be a group of criminals, terrorists or extremists. There are two types of insider adversaries, passive and active. These have been explained in detail in the introduction of this research work. There are three types of tactics, adversaries employ during an attack which they think increases their chances of achieving their aim or objectives. These tactics include force, deceit, and stealth. Considering the high crime rates and serious crimes in the neighborhood or the Center (Mafikeng
and Mmabatho), force is certainly a probable tactic. The crimes in the area include unlawful possession of fire arms and ammunition, robbery with aggravating circumstances, robbery at both residential and non-residential premises and malicious injury to properties. The tactics of Deceit can be used during crimes such as common robbery, kidnapping and some crimes under crimen injuria including stalking. Stealth will be employed to enter premises under false pretense to commit crimes such as burglary at both residential and non-residential premises. In addition, all three infiltrations at Pelindaba (where the apartheid government conducted nuclear weapons research and production) should inform the designer of a PPS which kind of threats are deserving of greatest attention. In the 2005 infiltration, protection measures were breached to be able to enter the facility and steal a portable computer. This breach could be by outsiders or outsiders working in collusion with insiders. These adversaries might have defeated the security system by using false authorizations and identification (deceit) or by having an insider to defeat the detection systems to allow outsiders to enter facility covertly (Stealth). These tactics can be employed by either of the groups of adversaries mentioned above. In 2007, the adversaries used the tactics of force to enter the Pelindaba facility; they were armed and managed to deactivate security layers and enter through different directions in groups. There was an element of Stealth tactics also since these armed men were able to penetrate the control room for a period of 45 minutes and escaped without being detected by the detection layers of the physical protection system. These attacks may have been masterminded by a certain group of people such as criminal outsiders, disgruntled insider employees (former or present at the facility), competitors of the facility and any of the three combinations [29]. The third violation of protective measures at the Pelindaba facility in 2012 was described as an act of “common” criminality [41]. The tactics employed in this case might have been stealth by an insider or deceit by an outsider working in collusion with an insider.

3.2.4.2 Capabilities of Adversaries

With the above mentioned crimes, adversaries’ capabilities can be deduced. Adversaries can possess arms and ammunitions unlawfully and use them in robbery with aggravating circumstances, robbery at both residential and non-residential premises and malicious injury to property. Other tools apart from weapons (arms and ammunition) can be used in various crimes. As an example, pliers, hacksaw blades and crow bars can be used in crimes like burglary at both
residential and non-residential premises. Knives can be used in crimes such as common robbery and kidnapping. In addition to the weapons or hand tools adversaries bring along in an attack, they use any other tools or equipment that they find inside the attacked premises that will facilitate their attack. Another factor that describes adversary capability is the means of transportation (for example cars, trucks, helicopter etc.). With carjacking crimes in both Mmabatho and Mafikeng, adversaries have been known to steal cars or trucks to use in another crime, then dispose of them afterwards.

Figure 3.8: An example of hand-held and power tools that can be used to attack security and facilities [29].

The aftermath of the Sarin attacks on the Tokyo subway, the attacks on 9/11 in the USA, anthrax attacks in New York and Florida and the Madrid and London train bombings have compelled security analysts (especially nuclear security professionals) to include weapons of mass destruction (WMD) as an emerging adversary capabilities. WMD include chemical, biological, radiological or explosive materials which are capable of causing mass casualties, public fear and lasting contamination [29]. It should be noted that this emerging capability may not be used against all facilities but because they are emerging we need to plan for them in our security designs, especially with the insurgency of Boko Haram and Al-Shabaab militants in Eastern and Western Africa.
The above information guided my design for the PPS. This research work took into consideration all tactics, capabilities, types of attack and groups of people who might attack so as to put in place a PPS effective at protecting the Center against these attacks.

3.2.4.3 Potential Actions and Motivations of Adversaries

When there is an attack on a facility, adversaries have in mind specific goals for the attack. Usually their actions depend on their goals. These goals can include theft, sabotage, terrorism, retaliation, and political protest. Considering the threat to the facility and the crimes committed around the facility, the above mentioned actions can be linked to the different crimes. Theft, extortion and kidnapping will be of particular concern. Motivations of adversaries could be ideological, economical (financial benefits) or personal. The center could be attacked by a set of people who are ideologically opposed to nuclear technology. It appears however, that economical gain is by far the most likely motivation for adversaries. Extremists and terrorists may be rewarded financially by their leaders. A company might pay criminals to destroy the facilities and equipment of its competitor. Often, adversaries are paid to cause harm, or they do it to benefit themselves. Many of the crimes committed in Mafikeng or Mmabatho are for financial gain. A current or former disgruntled employee of a facility could have the motivation to either work alone or with outsiders to execute an attack on the facility. Thus the importance of measures to mitigate employee disgruntlement.

3.2.5 Design Basis Threat

According to the IAEA Code of Conduct, facilities using Radioactive Sources in Categories 1 to 3 should have systems and measures designed and based on a threat assessment.

In the immediate towns surrounding the Centre for Applied Radiation Science and Technology, there is a significant amount of criminal activity during the day and at night. The existence of the university and its facilities is well known in these communities, as is the existence of the irradiator. There has, however, been little apparent interest or inquiry to date other than from students and researchers. On the average, there have been 10 carjackings, 12 instances of unlawful possession of fire arms and ammunition, 121 common robberies, 278 robberies with aggravating circumstances, 221 malicious damage to properties and 405 burglaries at non-
residential and residential premises crimes per year in the two towns. Other crimes include, on the average, 289 drug-related crimes, 60 robberies at non-residential and residential premises, 12 kidnappings and 49 stalking crimes per year in the two towns.

There have been two organized protests in 2008 and 2015, in which some student “activists” and others protested and vandalized grocery and computer accessory shops on the Mafikeng Campus of the North-West University. The two protests received considerable media attention. The student activists were able to drive the university security guards out of the campus. The police were only summoned when the University was closed down and student needed to vacate the campus.

A recent intelligence report shows that a group of terrorists can potentially use radioactive material/sources to create panic in the two towns to divert the attention of security agencies in other to assist their other criminal activities [83].

A designer of physical security systems for nuclear facilities using Category 1-3 radioactive sources must take into account the determination, violent nature and potential tactics of both Insider and Outsider adversaries. Countermeasures should be developed for a minimum of at least 2 – 3 adversary personnel. The following should also be taken into consideration:

- Most adversaries are well trained and will possess skills in handling radioactive material and are likely to have at least hand tools for use in breaching barriers to entry.
- Knowledgeable individual(s) who work in the facilities may give inside assistance in an attempt to participate in a passive role (e.g., facilitate entrance and exit, disable alarms and communications) and also participate in violent and non-violent attacks. This internal threat can arise from any employee in any position of the facility.
- Insiders may help Outsiders with (A) Access to and detailed knowledge of nuclear power plants or other nuclear facilities and/or (B) Items that could facilitate theft of nuclear materials (e.g., small tools, false documents, facility keys and pass codes, substitute nuclear material).
- The Adversary’s weapons may include pistols since there are already a number of crimes in the area involving the unlawful possession of fire arms and ammunition.
• Adversaries may make available an adequate vehicle for transporting radioactive source from the site, perhaps obtained from carjacking or from rentals.

3.2.6 Design of the New PPS
The fifth step involves the design of the PPS. In designing the PPS, this study took into consideration a performance-based design. For example, intrusion sensor performance will depend on the probability of detection (P_D), nuisance alarm rate (NAR), the ability of adversaries to defeat the sensors, and the sensor’s vulnerabilities. Sensor effectiveness depends on P_D and the confidence level (C_L) for the sensor. The P_D and C_L values can be determined for specific sensors when several tests have been carried out on them by manufacturers and users. Ideally, P_D and C_L would be 1.0 or 100% but in reality, values will be less [77]. Values of P_D and C_L are often conditionally based on the assumptions that were made about the sensor’s operating conditions during testing, but these values may differ when they find themselves in actual use. Selection of the sensor types depends on the DBT or threats faced by the facility, whether the threats are merely vandalizing properties by teenagers, or more sophisticated attacks by adversaries with sufficient knowledge and skill. The detection criteria that will be used in this design is for the sensor system to detect adversaries of a minimum weight of 45 kg crossing the detection zone, or in the presence of the detection zone. This must be the case whether the adversary is running, walking, crawling, rolling or jumping. This weight threshold of 45 kg is chosen because the crimes occurring in the region around the facility are often carried out by persons between the ages of 18 and 55, mostly men. The average weight of an 18 year man is around 55 kg [81].

Detection will not be complete without analyzing the alarms generated during detection. An alarm does not automatically mean an attack is underway. Some alarms could be false or nuisance alarms depending on the environment and sensor locations. In assessing the response needed to a given alarm, it is necessary to determine the cause of the alarm and whether or not that particular alarm warrants a response. False or nuisance alarms can occur due to weather conditions such as wind, rain or lightening. They can also be produced through vibration of equipment in the facility or a passing heavy-duty vehicle. In this work, the nuisance alarm rate or false alarm rate (FAR) was determined for a specific period (two months) after the implementation of the proposed design.
Now every sensor can be defeated by either bypassing the finite detection zone of the sensor to avoid detection, by tampering with the alarm (including at the factory), or by otherwise spoofing or jamming the sensor. The steps that were taken in designing the PPS was to attempt to minimize the feasibility of these defeats, and mitigate by selecting a sensor system resistant to defeat [77].

On the basis of the worst envisioned threat, a PPS was designed and proposed. It incorporated the following three key functions: detection, delay and response. The PPS has the capability to verify the various roles of the proposed system: in-depth protection, balanced protection, and timely detection/response. The PPS operates in two protection zones, the controlled zone and the supervised zone. Administrative procedures were developed to integrate with interior intrusion sensors, access controls and material and equipment monitoring. These administrative procedures can be effective against insider threats. The door that opens opposite the Animal Health Department outside the building was used as the emergency door in case a worker in the irradiation room encounters an emergency.

3.2.6.1 Detection Stage
The controlled zone of the Building F2C in the proposed design makes use of various detection devices including Fixed CCTV Cameras (day/night), Balanced Magnetic Switches (BMS), Fixed Duress Buttons, and Dual Technology PIR/Doppler Microwave motion detector, Radiation Detector, Proximity Card Reader requiring the use of personal identification number (PIN), Glass Break Sensors and an Arm/Disarm Keypad. Supervised zone for Building F2C in the proposed design also makes use of detection devices including Fixed Closed-Circuit Television (CCTV) Cameras (day/night), Balanced Magnetic Switches and Dual Technology PIR/Doppler Microwave motion detector. The other buildings F2A and F2E also make use of some of the devices mentioned above.

The CCTV cameras that will be installed have built-in infrared illuminators. Images from these cameras are used for assessment when an alarm was received. The cameras were used to make judgement of the area, resulting in a loss of signal alarm. BMSs are installed on the secure side of each door. BMS alarms sound when doors are held open for more than 30 seconds, but sound immediately when a door is forced open. The BMS has a tamper alarm and the alarms indicate
where the door is specifically located. Duress buttons are installed in secure rooms such as the source room and the control room. The duress buttons are accessible to operations personnel at all times. Duress alarms indicate their specific location. Dual Technology PIR/Doppler Microwave motion detector are installed at identified locations. Alarms from the PIR/Doppler Microwave motion detector sound when intrusion occurs and indicate the specific location. These sensors also have tamper alarms which are activated through the access control PIN pad (Arm/Disarm Keypad) when any individual tries to override them. A gamma radiation detector is installed in the source room that issues an alarm when the gamma count rate exceeds a prescribed threshold above background. This threshold is set in order to prevent nuisance alarms. A gamma detector alarm means the radiological source has been taken from the device shielding. Burglar bars are installed on the two windows in the controlled zone. These devices are all connected to video monitors, a high audible alarm and a light alarm. For the detection functions to be effective, it is necessary for the devices to be able to sense adversary action [31].

3.2.6.2 Delay Stage

The delay stage makes use of Electric Strike Locks, Tamper Devices, High Security Padlocks, Exit Buttons, Security-Harden Doors and inner Burglar Bar Gates for both the controlled and supervised zones of Building F2C. Building F2A and F2E also make use of some of the above mentioned technology. For the delay stage to be effective, two elements, i.e., physical barriers and protective force, were employed to enhance delay of an adversary. Physical Barriers come in the form of several structural installations in the PPS designs of buildings F2C, F2A and F2E to make it difficult for adversary to overcome them in other to succeed.

For Building F2C, door one (D1) and door two (D2) shown in figure 3.2 were replaced with high security-hardened doors and were locked with electric strike locks. These hardened doors were solid-core wood and their hinge pins were welded in place to prohibit removal. An inner burglar bar gate was proposed to be installed behind D1 into the room. This burglar bar gate was of a specific design shown in figure 3.12; it was intended to increase the difficulty of being defeated and this design was transferred to the already existing burglar bar gate behind door four (D4). I proposed that window burglar bars be installed on all glass windows. An inner burglar bar gate A, with a similar design was to be installed between door five (D5) and door six (D6) to provide.
an additional delay. All gates have two separate locks, i.e., high security padlocks and a lock that uses a mechanical key. The locks on door three (D3), D4 and D5 are all replaced with electric strike locks. Doors D1, D2 and D5 have Proximity Card Readers with a PIN required in addition to a Proximity Card to gain access. Doors D8, D9 and D10 are locked with a lock that uses a mechanical key.

For Building F2A, an inner burglar bar gate was proposed for use behind door D7, and an outer burglar bar gate before D1. These are to be locked with a security padlock and a lock that uses a mechanical key. All windows will have burglar bars on them. Doors D1 and D7 are to be locked with electric strike locks. Doors D2 and D6 have Proximity Card Readers with a PIN requirement in order to control access.

For Building F2E, inner burglar bar gates were proposed for behind all entrance doors to the building to provide more delay. These doors are doors D1, D9, D11 and D12. The bar gates are all to be locked using high security padlocks and a lock that uses a mechanical key. All inner burglar bar gates are of the same design for all buildings. All the above mentioned doors in addition to door D4 are to be locked with electric strike locks. Doors D4 and D6 have Proximity Card Readers with a PIN requirement to control access.

A key control system was put in place to control unauthorized access for all doors. A Protective force incorporating trained security guards patrols the Center. They check that doors are closed and locked at night and man the security control room where video monitoring of the devices used in the detection stage takes place. Help is intended to come from the security control room when video indicates there may be ongoing intrusion, which might sound an alarm or observed by the trained guards patrolling the Center and report to the security control room using their communication devices. To reduce unnecessary responses, analysis of the intrusion detection is done first before action is undertaken. The measure of the delay effectiveness is the time required by the adversary, after detection, to bypass or defeat each delay element or barrier [79].
3.2.6.3 Response Stage

The response stage consists of the actions undertaken as a result of what has occurred at the detection and delay stages. The response force team takes over to prevent adversary success. Response, as it is used here, consists of interruption, which is defined as a sufficient number of response force personnel arriving at the appropriate location to stop the adversary’s progress. It includes accurate communications between the protection force members about information concerning adversary actions and the deployment of the response force team. The Response can make use of three main strategies: containment, denial and occasionally assault. Containment is used against adversary whose primary intent is theft. The response team uses this strategy to prevent the adversary from leaving the site with the stolen assets. A denial strategy is used against adversaries whose goal is to sabotage or undertake a violent attack. The response team uses it to prevent the adversary from completing the sabotage task to the equipment or assets or person(s) they are targeting or carrying out a violent attack. In some cases, the response team may need to use some degree of force to overcome the adversary [29]. For the purposes of this research, all three strategies were planned for. Response can also be divided into two major categories: immediate on-site response (timely response) and after-the-fact recovery response. In this research, because the protection system is for the $^{60}$Co irradiation source and valuable research equipment, timely response needs to be the focus. The potential use of minimal force by law enforcement officers in the response team adds an added advantage because these officers are backed by the legal authority to arrest or detain suspects, and are authorized to use appropriate force in their line of duty. There are different levels of force in the force continuum, starting with the mere presence of a guard as a deterrent or delay, through the use of less-than-lethal force, and when justified, the use of deadly force. It should be noted that, in a PPS the number of guards should be decreased and the resources used to add more technology to supplement the duties of guards at the detection stage. This is because reducing the number of guards is cheaper, it reduces the insider threat by having fewer of guards, it reduces injury and deaths to guards, and finally it makes guards more efficient. This lowers cost but improves PPS effectiveness [29].

For this stage to be effective, the time between notification of an intrusion or attack and the interruption of the adversary action should be done quickly enough so that the response force
time (RFT) is less than the adversary action time. Since communication is a vital part of the response function and can be compromised, devices used for communication must be carefully chosen. Voice and other systems that allow guards and response force team members to communicate with each other are part of the communication network. This network requires reliability and resistance to physical damage, eavesdropping, deception and jamming. The radio systems used by most guards used by security companies during response are conventional narrow-band frequency modulated (FM) and clear-voice radio systems, but these possess serious disadvantages. Anyone with a conventional receiver can tune to the proper frequency and easily monitor the transmissions as long as that person is in close range [77]. Communication systems that can provide the resistances needed are currently available but with higher cost; they are called “spread-spectrum” systems. This research factored in the cost effective aspect of the PPS in protecting the Center assets and acquired two of the spread-spectrum systems to supplement the FM systems and also allows for other alternative means when jamming becomes a problem for the radios. These alternatives are landline and cellular telephones, intercoms, hand signals, lights, whistles and pagers. Many of these were used during normal operations of the facility and so when jamming occurs, they can be relied upon to continue effective communication in the response stage [29].

To have an effective Response, the University contracted guards from a security company. A Memorandum of Understanding (MOU) between the company and the police authority was drafted. Effective, routine training of security guards was planned through a joint training exercise with the police, and application for the authorization of the usage of security devices to permit fast response were made. All these procedures were documented and duties allocated to each individual or group to prevent conflict during Response [34].

Figures 3.9 to 3.12 show the proposed PPS design for each building and a proposed design of a burglar bar gate to increase delay along the adversary paths.
Figure 3.9: Proposed PPS design for F2C irradiation facility.
Figure 3. 10: Proposed PPS design for building F2E.
Figure 3.11: Proposed PPS design for building F2A.
Figure 3.12: Proposed design of the inner burglar gate for all buildings.

Table 3.5 shows the symbols of devices and their numbers used in the PPS designs of the three buildings.
Table 3.5: Symbols and description in proposed PPS

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="symbol" alt="Electric Strike Lock" /></td>
<td>13</td>
<td>Electric Strike Lock</td>
</tr>
<tr>
<td><img src="symbol" alt="Fixed CCTV Camera" /></td>
<td>12</td>
<td>Fixed CCTV Camera (day /night)</td>
</tr>
<tr>
<td><img src="symbol" alt="Tamper Device" /></td>
<td>1</td>
<td>Tamper Device</td>
</tr>
<tr>
<td><img src="symbol" alt="High Security Lock" /></td>
<td>37</td>
<td>High Security Lock</td>
</tr>
<tr>
<td><img src="symbol" alt="Door Lock" /></td>
<td>12</td>
<td>Door Lock</td>
</tr>
<tr>
<td><img src="symbol" alt="Proximity Card Reader with PIN" /></td>
<td>7</td>
<td>Proximity Card Reader with PIN</td>
</tr>
<tr>
<td><img src="symbol" alt="Glass Break Sensor" /></td>
<td>13</td>
<td>Glass Break Sensor</td>
</tr>
<tr>
<td><img src="symbol" alt="Balanced Magnetic Switch" /></td>
<td>13</td>
<td>Balanced Magnetic Switch</td>
</tr>
<tr>
<td><img src="symbol" alt="Exit Button" /></td>
<td>3</td>
<td>Exit Button</td>
</tr>
<tr>
<td><img src="symbol" alt="Arm / Disarm Keypad" /></td>
<td>2</td>
<td>Arm / Disarm Keypad</td>
</tr>
<tr>
<td><img src="symbol" alt="Fixed Duress Button" /></td>
<td>2</td>
<td>Fixed Duress Button</td>
</tr>
<tr>
<td><img src="symbol" alt="Security Harden Door" /></td>
<td>2</td>
<td>Security Harden Door</td>
</tr>
<tr>
<td><img src="symbol" alt="Light Alarm" /></td>
<td>1</td>
<td>Light Alarm</td>
</tr>
<tr>
<td><img src="symbol" alt="High Audible Alarm" /></td>
<td>1</td>
<td>High Audible Alarm</td>
</tr>
<tr>
<td><img src="symbol" alt="External CCTV Cameras" /></td>
<td>14</td>
<td>External CCTV Cameras</td>
</tr>
<tr>
<td><img src="symbol" alt="Passive Infra-Red Motion Sensor (Dual tech)" /></td>
<td>6</td>
<td>Passive Infra-Red Motion Sensor (Dual tech)</td>
</tr>
<tr>
<td><img src="symbol" alt="Radiation Detector" /></td>
<td>1</td>
<td>Radiation Detector</td>
</tr>
</tbody>
</table>
3.2.7 Functions of the Devices used in the Design

Devices used in the proposed design are described as follows based on characteristics, mode of operation, identified potential defeat methods and how these could be prevented to achieve an effective system that can secure the assets of the facility and also prevent loss and sabotage.

3.2.7.1 Balanced Magnetic Switches

Magnetic switches are made up of a magnetic unit and a switch unit. The magnetic unit contains a permanent magnet and is normally installed on the door or window which opens to allow entry into the protected area. The switch unit is installed on the fixed part of the door and adjacent to the magnetic unit, which travels with the rotating or sliding door when it is opened. These two units come together to complete a circuit when the door or window is closed. Disengaging the magnet from the switch triggers an alarm. This switch can be defeated by placing a stronger external magnet in or behind the switch housing to still keep it in the ‘closed’ or ‘on’ position without generating an alarm even if the window or door is opened [84]. This PPS design makes use of a magnetic switch with an additional bias magnet in the switch unit which can be adjusted to complicate this kind of defeat using an external magnet. This type of switch is called balance magnetic switch (BMS). A BMS provides a higher level of intrusion detection for doors and windows than ordinary magnetic switches. It makes attacks against the magnetic switch more difficult and time-consuming. If an intruder attempts to spoof a BMS using a magnet, the same strength of the magnet in the switch unit is required to achieve that aim, and therefore the intruder becomes disadvantaged because it will be difficult to guess the strength of magnet the manufacturer used. Lower or stronger magnets used in the defeat process will trigger an alarm because of the difference in net effect of the magnets [84]. The BMS sensor was chosen as a boundary-penetrating sensor because it detects penetration of the boundary of the Buildings F2C, F2A and F2E to an interior area of the laboratories, offices and store rooms.

3.2.7.2 Passive Infrared Sensors

Passive infrared sensors are visible sensors that are installed in the interior area of a room and do volumetric detection. This means that PIR can detect an intruder in the volume protected by it regardless of the point of entry of the intruder. A PIR can detect energy changes in a room or in its volume emanating from an intruder because a human body emits energy which can be equal
to the heat of a 50W light bulb [85]. This principle is feasible due to the characteristics of infrared radiation. These characteristics include all objects being able to emit infrared radiation and the intensity depends on the temperature of the object. The energy from infrared radiation is transmitted without any physical contact between the object transmitting it and the receiving sensor. A PIR sensor works by receiving infrared radiation from an intruder and converting that into electrical signal to generate an alarm. It is important to note that a PIR motion detector is a change detector; it is sensitive only to relatively sudden changes in the infrared intensity in a room, but is not sensitive to the absolute temperature or infrared intensity. Detection therefore depends on the difference in temperature between the intruder and the background temperature, and this difference is termed as minimum resolvable temperature (MRT). Combining a Doppler microwave sensor with a PIR into a “dual technology” motion detector greatly reduces the rate of false alarms from the PIR sensor alone but decreases intrusion sensitivity. Dual technology motion detectors were chosen in the design because they add some measure of difficulty in their defeat and also reduce the nuisance alarm rate.

3.2.7.3 Closed Circuit Television Cameras

A CCTV camera system typically consists of a video camera, camera lens, a monitor and sometimes additional TV monitors with cords for wired models. Other CCTV systems also employ some kind of video recorders in order to capture the video for later analysis. A video monitoring detector (VMD) processes the video signal from a CCTV camera. Lighting is often a requirement depending on the time of video camera. For continuous operation of these cameras the light should ideally be as uniform as possible to avoid excessive shadowing. Signals from the video camera can be transmitted from the video camera to the monitor through wired or wireless connections. A wired CCTV video camera sends the particular signals through wires to the television screen or the recording, whereas a wireless system transmits the signal electromagnetically without the need for wires. A VMD detects changes in the video images and therefore any significantly rapid change in the video scene can trigger an alarm [86].
3.2.7.4 Duress or Panic Button
A duress or panic button is an electronic device that is designed to assist personnel in emergency situations to be able to sound an alarm about a critical or hazardous situation. Duress or panic alarms are not always controlled by a duress or panic button, but in this design, the use of these buttons is ideal. When personnel or assets are in any form of danger, the button is pressed in order to alert security guards to respond [87].

3.2.7.5 Gamma Radiation Detector
A gamma radiation detector generates an alarm when the gamma count rate exceeds a prescribed threshold above background, indicating that a radioactive source has been removed from the device shielding. The threshold here will be set such that the alarm triggers when the source is removed from its shield in order to prevent nuisance alarms caused by random fluctuations in background counts. This is because when the source is in the “on” position during irradiation periods, the probability of high nuisance alarms is high [88].

3.2.7.6 Arm and Disarm Keypad
An arm and disarm keypad is to be installed in both the source room and control room to enable the activation of the room intrusion detection system. A type of keypad was selected to be able to automatically rearm the system after 20 seconds of entering the room in case of an unauthorized entry. With respect to staff inside the rooms, this automatic rearming of the system gives a sound indicating or reminding the personnel to deactivate the arming or leave the room prior to rearming the system [29].

3.2.7.7 Card Reader with PIN
A card reader with PIN capability operates in two ways. It reads personnel cards for access control on one hand, and also requires a unique PIN to be entered from personnel. It only grants access if both conditions are met. This process makes it more difficult for adversaries to gain entry, as they need to both possess a valid card and know the PIN or extract it from an authorized employee if they are to access the Card Reader in the conventional way. The PIN entering process gives the personnel who otherwise has been coerced in granting access the opportunity to enter a silent duress code which triggers an alarm as duress indicating the location in the facility, though doing so may put such personnel at personal risk [89].
3.2.7.8 Tamper-Indicating Device
A durable tether was proposed to be used to tie the $^{60}$Co source machine in position either into the wall of the room or fixed to the floor to prevent it from theft by adversaries. This approach is used because it makes it more difficult for an adversary to take out the tether from the source machine. It should be noted that this measure is used only against theft and not sabotage of the source machine. But the tether is also fixed in a way to create space for the operation and maintenance of the source machine. If the tether is cut or removed from the wall or floor, an alarm triggers at the alarm monitoring location [90].

3.2.7.9 Exit Button
Request to exit buttons was installed on the secure side of the three doors (two doors of the source room and the door of the control room) to enable exit from the rooms after getting access into them through the card reader and PIN [91]. These are important for safety reasons.

3.2.7.10 Acoustic Glass Break Sensors
A glass break sensor was proposed to be installed in each room that had glass windows. In the event of a glass breaking, an alarm is generated. Acoustic sensors are designed specifically to detect the sound of breaking glass at a selected sound frequency and intensity. These sensors are activated as soon as they detect the sound of shattering glass. They protect a wider area but cannot detect through walls and therefore the glass windows or doors should always be on the line of site of the sensor but not too far from the sensor. If windows are far apart it is advisable to attached glass breaking sensors to each of them. Glass-breaking sensors are designed to detect a break-in before an intruder has time to get inside the structure [92].

3.2.7.11 Light Alarm and High Audible Alarm (Siren)
All alarms from the intrusion detection system and the access control system (ACS) are connected to the alarm monitoring station (AMS), and also are capable of sounding an audible alarm at the center to alert the onsite guard of an intrusion. The intrusion detection system is connected to the light system which glows alerting intrusion and also to a siren which sounds alerting intrusion on the premises of the facility [29].
3.2.8 Administrative Procedures with Regards to Safety and Security of the Center

Administrative procedures are the rules and regulations governing the mode of operation of the Center and include certain requirements of employees to obtain good safety and security. They are guidelines to follow in the day-to-day activities of the Center to safely and securely achieve its vision and mission.

3.2.8.1 Center Access

The small gate of the fence to the buildings is open from Monday through Friday, 8:00 a.m. to 5:00 p.m. Any staff or student who want access to the buildings outside of these days and hours needs to book and record into the key log book for the keys (both the main gate and the laboratory to be used) from the guards on duty and return them after use. The vehicle entrance gate of the fence is always locked and opens upon the request by staff and students who wish to drive vehicles carrying either samples or materials for research purposes into the Center.

3.2.8.2 Key and Access Control System

All keys of the Center are under lock and key in the stationary room in a key locker. Staff and students who wish to work after hours must book for the keys of the laboratories to be used stating the purpose of booking the keys and the time to return them. All this information should be entered into a key log book in the office of the administrator of the Center, but when he/she is unavailable this should be done at the guard’s post. No student living outside the University Campus is allowed possession of keys. The Administrator periodically changes door access locks and padlocks of the gates for security reasons, and has the sole responsibility controlling key access. He/she also changes the PINs to be used on the proximity card reader as well as codes used to arm/disarm the intrusion detection system. The changing of door locks, PINs and codes is carried out with the permission of the Director of the Center and any staff connected to these PINs and codes should liaise with the administrator for their new PIN or code. For security reasons keys, PINs and codes should not be given out to a third party without the consent of the Administrator and this transfer must be documented.
3.2.8.3 Office Security

Access to the offices and laboratories is strictly controlled and restricted to students and staff. Visitors are permitted access to the offices of staff through the Administrator. All visitors are to report to the Administrator who then informs the staff to be visited to come and meet the visitor at the Administrator’s office before escorting them. Any visitor who is not a student of the North-West University and affiliated with the Center should be questioned by staff or students regarding the purpose of their presence at the Center. No money or valuable property should be left unattended, as CARST insurance coverage does not extend to personal property and does not accept liability for loss of employee’s belongings on the premises. In the event of a fire or emergency, staff and students should leave their workstations immediately and not stop to clear papers or collect personal belongings. Staff should note the location of fire exits and extinguishers before an emergency occurs. In non-emergency situations, staff members should ensure that all CARST materials and correspondence are properly secured and not accessible to unauthorized persons. Gates and doors are to remain locked outside office hours, and suitable security measures must be taken through the use of alarms and intrusion detection systems. To assist in maintaining office security, the last employee to leave the office should ensure that all entrances are locked. In the case of movement of equipment by any staff, Security personnel should seek confirmation or approval from the Director before allowing movement.

3.2.8.4 Communication

CARST seeks to provide all employees with current information on activities and developments affecting the Center. Staff members are strongly encouraged to ask questions, maintain an active interest in CARST activities, safety, and security, and be interactive and offer suggestions. To promote staff involvement in the Center’s work, periodic meetings must be arranged by the management. The use of photocopying, printing and telephone equipment for personal needs are to be recorded and reimbursed on a monthly basis. Limits should be accorded personal telephone calls and other communication to essential matters. When absent from the office, employees should provide information as to where they can be contacted if necessary. The Administrator handles incoming and outgoing mail and registers them in the Mail Register. However, any employee who picks up mail must record its particulars in the fax Register. In this era of cyber infiltration, any employee who receives a mail containing portable devices from an unknown
source should first identify these devices as legitimate before taking them to their offices since some of these devices can compromise security when near or attached to personal computers.

3.2.8.5 Information

The Center’s business should be kept confidential at all times. All letterheads, forms, and other stationery bearing the logo of CARST should be kept under lock and key. Back-up copies of computer data files should be regularly updated to ensure security of documentation in the case where data is destroyed through cyber infiltration, malware, human error, earthquake or fire. Backups of all important documents and records, including computerized information essential to the basic operation of the Center’s business should be kept and maintained outside the offices. These records include those pertaining to the training and research, grants management, publications, the accounts, personnel contracts, and any other record of a commitment by CARST. Computers belonging to the Center being loaned to other departments for use at meetings should be cleared of data. External visitors are not allowed to use office computers but can use student computers under supervision.

3.2.8.6 Safety

The intention of the Center is to provide a safe and healthy working environment for all employees and students. CARST is responsible for the health, safety and welfare of employees and students at work on site at the Center. To meet this obligation, the Head of Department will conduct periodic workplace inspections. These inspections are intended to check whether staff and students are performing their duties safely.

3.2.8.7 First Aid

First aid will preferably be administered by trained first aiders within CARST, but if the absence of a first aider, other employers or students with knowledge of first aid should assist. For its success, the Center will organize minimum first aid training for all employees and students. A list of the members of staff trained in first aid will be circulated to all employees on a periodic basis and at least once a year. This list will also be provided to new employees as well. The Safety Officer will be responsible for coordinating health and safety matters in CARST and charged with the duty of updating this information.
3.2.8.8 Fire

The list of trained staff as fire wardens will be circulated to all employees including new employees together with diagrams of the office layout indicating fire exits, locations of fire extinguishers and location at which all employees and visitors will assemble prior to evacuation of the building. The procedures to be followed in the event of fire are displayed visibly in the laboratories. The person responsible for coordinating health and safety matters in CARST is also responsible for updating this information. The Center will train employees and available students on the usage of fire extinguishers, it is also the responsibility of the Director of the Center to ensure that qualified fire wardens are available at the Center. Fire warden records form, will be maintained to note when fire wardens require refresher courses and further training but the regular training of using fire extinguishers will be held twice a year for everyone. Emergency exits are clearly identified and prominently displayed. Employees are required to familiarize themselves with the best escape route in the event of an emergency. The official assembly point for the buildings is the area allocated between buildings F2A and F2E. The administrator is responsible for notifying the emergency services in case of emergency. All employees must be accounted for before permitting them to return to the building or dispersing them. No employee is permitted to return to the building until emergency services or fire wardens give clearance. Emergency evacuation exercises should be organized and carried out on a regular basis by the safety officer and fire wardens. Fire alarms should be tested periodically by the safety officer. A minimum of three days’ notice should be given prior to such testing. Particular attention should be given and periodic inspection carried out to ensure that flammable materials (paper, liquids) are not being stored on or in close proximity to electrical equipment (transformers, UPS, voltage regulators, etc.). Any loose switches, faulty plugs or other defective apparatus must be reported immediately to the Safety Officer. Unauthorized personnel should not attempt to correct such faults. Any suspicion of burning or smoldering must be reported to the Safety Officer or fire warden immediately, who is responsible for such investigation.

3.2.8.9 Accidents and Incidents at Work Place

In situations where an employee becomes injured in the workplace during office hours, it is the responsibility of the Safety Officer or his assistants allocated such duties to make appropriate
arrangements for medical attention. There will always be someone responsible for this arrangement at the Center.

a. Incident and Accident reporting procedure

- All incidents involving injury must be reported to the Safety Officer.
- The Safety Officer is responsible for keeping full and accurate records and investigating the incident as soon as possible.
- Every employee who is injured at work and employees assisting the injured individual must report the accident as soon as reasonably practical. Accident log forms are available for recording all incidents and actions taken to prevent occurrence of similar incidents.

b. Incident and Accident reporting Investigations

An investigation is not a witch-hunt and not about pinning blame or finding scapegoats. It is all about finding out why the incident/accident occurred and how similar incidents can be prevented in the future. The following steps should be undertaken in an incident/accident investigations:

- Objectively and collectively identify all contributing factors and causes of the incident/accident.
- Collect information.
- Analyze data to identify contributory factors and their inter-relationship.
- Determine the root/real/underlying causes of events contributing to incidents/accidents.
- Design appropriate action plans to prevent further incidents and accidents.
- Create ownership amongst employees by making them part of the investigation process.
- Demonstrate that the Laboratory is concerned about safety, health, environment and quality.
- Comply with all legal requirements [93].

3.2.9 Evaluation of the New PPS

The sixth and last step involves using computer codes to evaluate the effectiveness of the proposed PPS design and implementation in the context of the PPS by the Global Threat Reduction Initiative. Computer software called EASI [29] and ASSESS were chosen to use for this purpose. ASSESS is an enhanced version of SAVI (System Analysis of Vulnerability to
Intrusion) with additional insider attack analysis and neutralization modules. ASSESS was not yet ready for distribution to some African countries, including South Africa, during the period of this study and therefore EASI was used alone for the evaluation. In view of this, I studied the algorithm of the EASI code and used it to create another code for multiple pathways since the EASI program only evaluates a specific pathway at a time. This new code was called EASIM (Estimation of Adversary Sequence Interruption for Multiple Paths).

The EASI model makes use of input parameters which represent the physical protection functions of detection, delay and response. The likelihood of good communication through an alarm signal is also required by the model. Detection and communication inputs are represented in the form of probabilities and fed into the model on the assumption that all functions are performed successfully [29]. Delay and response inputs are represented in the form of mean times and standard deviations for each element. Inputs fed into the model represent a specific adversary path. The EASI input for the detection function is the probability of detection for each sensor encountered by the adversary. Normally, this is dependent on the capabilities of the adversary. $P_D$ is the product of the probability that the detector senses abnormal or unauthorized activities by the adversary ($P_S$), the probability that an alarm indication is transmitted to an evaluation or assessment point ($P_T$) and the probability of accurate assessment of the alarm ($P_A$). Thus,

$$P_D = P_S \times P_T \times P_A.$$  \hspace{1cm} (8)

The communication of an alarm to the response force after detection is inputted into EASI as the probability of successful guard communication $P_C$. Typically, the likelihood of successful communication to the response force increases with time. $P_C$ for most systems designed by Sandia Laboratory is usually set to at least 0.95. It should be noted, however, that $P_C$ can be determined experimentally by measuring the RFT i.e., the time it takes to receive the communication, assess it and respond to it [29]. The adversary task time is the amount of time it takes to reach the target, which involves performing certain tasks or traveling distinct path segments that add to the delay time. Generally it is impossible to predict the exact time the adversary will need to perform these tasks or proceed across the appropriate distinct path segments. These sometimes depend on the capabilities and resources of the adversary and the
difficulties the delays provide. The adversary and the response force will not always perform a task within exactly the time predicted. For example, the adversary may take more or less time to get through a door, or the response force might have trouble starting a vehicle.

3.2.9.1 Use of Location Variable in EASI
There is a data column in the model labeled “locations” in which some letters corresponding to various situations are inputted. These locations are used to describe where in the model detection falls relative to delay for the specific protection element. If detection and delay both exist at an element, the detection may start before delay, at the end of delay or somewhere in-between. EASI uses detection relative to delay time to accurately model system effectiveness. In order to do this, the letter “B” is entered for detection before delay, “M” for detection during delay (middle) and “E” for detection after, or at the end of delay. If there is no detection associated with the delay, the parameters of the location will not matter. If “B” is allocated to the location, the delay time is calculated using the mean delay time for the task to undertake the standard deviation. When an “E” is allocated, EASI uses zero (0) as the delay time for that task. The use of “M” indicates that the delay happens somewhere in between the beginning and ending values, and therefore it is approximated as one-half the mean the standard deviation [29].

3.2.9.2 Examples Explaining the Use of B, M and E in EASI
A volumetric sensor in a room monitoring a door, can be used to illustrate the parameter B allocation. In an attack, as soon as the adversary starts penetrating the door, the sensor will detect the intrusion but the adversary must still finish penetrating the door to get to the asset. The volumetric sensor detects the intrusion in the volume occupied by the adversary before the door delays the adversary. The use of B in this instance is appropriate [29].

In the case of an M allocation, an adversary might want to use an explosive device to penetrate a wall. In doing that, the adversary first needs to set up the explosive device then retreat to a safe place for the explosion to occur before coming back. Here, the placement of the explosive would be detected first, but the adversary will have to return to the wall and get through the hole to continue the attack. At this point, the adversary will be detected during the delay of getting through the hole in the wall [29].
A door with a fixed BMS sensor can be an example assigned to an E location. In the process of opening or picking the door lock, the sensor will not register an alarm until the door is opened a small distance. The door mostly serves as the delay until it is opened a small amount, causing an alarm to be annunciated. Thus the detection comes at the end of the delay, which limits the effectiveness of the delay [29].

3.2.10 Adversary Sequence Diagrams

In any facility, there are different layers of protection that must be defeated or bypassed by adversaries, and in doing that they have multiple options. If an adversary wants to penetrate a building which is locked, the penetration can be done through doors, windows, walls or the roof or using insiders to leave the door unlocked. The number of paths into the facility the adversary could attack from, easily number into the hundreds of thousands because the adversary can choose any option on any layer. In order to use the EASI model on such facilities, the analyst needs a method to record these paths in a systematic way. This method is called an adversary sequence diagram (ASD). ASD represents graphically the protection system elements that are used to evaluate the effectiveness of the PPS at the facility. It illustrates the paths that adversaries could attempt to follow in order to accomplish attacks. For a specific PPS and a specific threat, the most vulnerable path, or the path with the lowest P_f can be determined using EASI. The effectiveness of the total PPS will be established through this path. There are three basic ways that enable an analyst to create an ASD for a specific site. These include modeling the facility by separating it into adjacent physical areas, defining protection layers and path elements between the adjacent areas, and recording detection and delay values for each element [29].

In analyzing a sabotage attack, the entry paths would be evaluated on the assumption that the protection elements will be traversed in only one direction. This is because the act of sabotage only requires proximity to the asset long enough to cause damage to it, and the adversary does not require to exit from the facility to be successful. Theft analysis requires both entry and exit of the protection elements. This is because the adversary will usually have to exit the facility with the stolen asset to be successful. It should be noted however, that though not usually nuclear thefts, involve the adversary leaving the stolen asset in the trash or mailing it from the shipping department, rather than leaving with it and risk getting caught outside the facility. The most
important goal of protection here is to interrupt the adversary before the target is removed from its location. This requires that only the entry path be considered. [29].

Figure 3.13: ASD showing different adversary paths for the CARST buildings
Figure 3.14: ASD showing different adversary paths for Building F2C

Figure 3.15: ASD showing the functional protection elements for building F2C.
CHAPTER 4 Data Analysis and Results

This chapter presents results of the research work which include the risk to the Center, risk due to the $^{60}$Co irradiation source and the evaluated effectiveness based on the probability of interruption and neutralization values for the various adversary paths chosen.

4.1 Risk to the Center

The risk to the Center can be calculated from equation four (4) but $P_E$ should be calculated first from equation five (5). Thus,

\[ P_E = P_I \times P_N \]
\[ P_E = 0 \times 0 \]
\[ P_E = 0. \]

Therefore the calculation of the risk with a consequence value of five million South African Rands (R 5,000,000). This is because if a security event should occur either through sabotage or theft the Center will lose economically because its research equipment is valued at approximately five million South African Rands.

\[ R = P_A \times (1 - P_E) \times C \]
\[ R = 1 \times (1 - 0) \times 5000000 \]
\[ R = 5,000,000 \text{ Rands}. \]

4.2 Risk due the $^{60}$Co Irradiation Source

The initial activity of this source in 1987 was 93 TBq or 2500 Curie. We can calculate the current activity of the source using the equation;

\[ A = A_0 e^{-\lambda t} \]  \hspace{1cm} (9)

where:
A is the current activity of the source;
$A_0$ is the initial activity of the source in 1987;
$\lambda$ is the decay constant of the source;
t is time during this decay.
The decay constant ($\lambda$) is calculated from the half-life ($T_{1/2}$) of the $^{60}$Co source (5.27 years) by the relation:

$$\lambda = \frac{\ln 2}{T_{1/2}}$$

(10)

$$\lambda = \frac{0.693}{5.27} = 0.1315 \text{ y}^{-1}$$

The time of decay from 1987 to June 2015 is 27.5 years and therefore the current activity of the source will be given by:

$$A = 93 e^{-0.1315 \times 27.5}$$

$$A = 2.50 \text{ TBq or 67.6 Ci}.$$  

The risk due to the 2.5 TBq (2500 GBq) $^{60}$Co source used at the irradiation facility at CARST can be calculated from equation six (6) using the D-value of $^{60}$Co (30 GBq). Thus,

$$RF = \frac{A}{D} = \frac{2500}{30} = 83.$$  

The facility’s intention is to upgrade the source activity from 2.50 TBq (2500 GBq) to the maximum activity the irradiator can accommodate which is 444 TBq (444000 GBq).

With the maximum activity, and using the D-value of $^{60}$Co (30 GBq), the ratio $A/D$ can be calculated as

$$RF = \frac{A_{\text{max}}}{D} = \frac{444000}{30} = 14800.$$  

Table 4.1 shows the calibration or test sources with their actual activities, exempt activities, $A/D$ values, and exempt/D values. This was compiled to ascertain the security levels to assign them. The sources $^{60}$Co (452 kBq), $^{137}$Cs (40.2 kBq), $^{241}$Am (34.7 kBq), $^{226}$Ra (31.9 kBq) and $^{226}$Ra (370 kBq) in table with D-values in [55] fell in the range $0.01 > A/D \geq \text{Exempt/D}$ thus belonging to category 5 sources. These category 5 sources require minimum security for their protection as specified in [95] for radioactive sources and due to the security systems put in place for the 2.5 TBq $^{60}$Co irradiation source all these other sources were adequately protected.
The rest of the sources $^{60}$Co (39.7 kBq), $^{133}$Ba (40.7 kBq), $^{152}$Eu (44.8 kBq), $^{152}$Eu (555 kBq) and $^{22}$Na (37.2 kBq) with activities less than their exemption activities are therefore exempted from regulation and were adequately secured with the security systems.

Table 4.1: Calibration radioactive source materials with their activities and other reference values

<table>
<thead>
<tr>
<th>Radionuclide</th>
<th>A/D Value</th>
<th>Exempt Activity/D [105]</th>
<th>Exempt Activity (Bq)</th>
<th>Actual Activity (Bq)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$^{60}$Co</td>
<td>$1.32 \times 10^{-6}$</td>
<td>$3.33 \times 10^{-6}$</td>
<td>$1.0 \times 10^{5}$</td>
<td>$3.97 \times 10^{4}$</td>
</tr>
<tr>
<td>$^{60}$Co</td>
<td>$1.51 \times 10^{-5}$</td>
<td>$3.33 \times 10^{-6}$</td>
<td>$1.0 \times 10^{5}$</td>
<td>$4.52 \times 10^{5}$</td>
</tr>
<tr>
<td>$^{133}$Ba</td>
<td>ND</td>
<td>ND</td>
<td>$1.0 \times 10^{6}$</td>
<td>$4.07 \times 10^{4}$</td>
</tr>
<tr>
<td>$^{152}$Eu</td>
<td>ND</td>
<td>ND</td>
<td>$1.0 \times 10^{6}$</td>
<td>$4.48 \times 10^{4}$</td>
</tr>
<tr>
<td>$^{152}$Eu</td>
<td>ND</td>
<td>ND</td>
<td>$1.0 \times 10^{6}$</td>
<td>$5.55 \times 10^{5}$</td>
</tr>
<tr>
<td>$^{22}$Na</td>
<td>ND</td>
<td>ND</td>
<td>$1.0 \times 10^{6}$</td>
<td>$3.72 \times 10^{4}$</td>
</tr>
<tr>
<td>$^{137}$Cs</td>
<td>$4.02 \times 10^{-7}$</td>
<td>$1.0 \times 10^{-7}$</td>
<td>$1.0 \times 10^{4}$</td>
<td>$4.02 \times 10^{4}$</td>
</tr>
<tr>
<td>$^{241}$Am</td>
<td>$5.78 \times 10^{-7}$</td>
<td>$1.66 \times 10^{-7}$</td>
<td>$1.0 \times 10^{4}$</td>
<td>$3.47 \times 10^{4}$</td>
</tr>
<tr>
<td>$^{226}$Ra</td>
<td>$7.98 \times 10^{-7}$</td>
<td>$2.50 \times 10^{-7}$</td>
<td>$1.0 \times 10^{4}$</td>
<td>$3.19 \times 10^{4}$</td>
</tr>
<tr>
<td>$^{226}$Ra</td>
<td>$1.39 \times 10^{-5}$</td>
<td>$2.50 \times 10^{-7}$</td>
<td>$1.0 \times 10^{4}$</td>
<td>$3.70 \times 10^{5}$</td>
</tr>
</tbody>
</table>

$ND= No\ dangerous\ Value$

4.3 Response Force Time and Task Times with corresponding Mean and Standard Deviation Values

Table 4.2 shows the practical action times of each adversary task along the pathways. These action times were practically performed on layers of the buildings which were considered not to have any effect on the structural integrity. These actions include picking a door lock, climbing the building, cutting the security padlocks, cutting the computer padlocks, cutting the hasp of a burglar gate and breaking ceiling. Other actions were by expert advice.
Table 4.2: Practical action times

<table>
<thead>
<tr>
<th>Activity</th>
<th>Action Times (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Picking a lock of ordinary door with hand tools</td>
<td>90</td>
</tr>
<tr>
<td>Picking a padlock with hand tools</td>
<td>30</td>
</tr>
<tr>
<td>Picking a lock of a steel clad door with hand tools</td>
<td>120</td>
</tr>
<tr>
<td>Cutting a security hasp of a steel clad door with a grinder</td>
<td>35</td>
</tr>
<tr>
<td>Breaking a security hasp of a steel clad door with a hammer</td>
<td>45</td>
</tr>
<tr>
<td>Cutting a lock of ordinary door with a grinder</td>
<td>20</td>
</tr>
<tr>
<td>Cutting the strand shackle of a padlock with a grinder</td>
<td>15</td>
</tr>
<tr>
<td>Cutting a padlock with a grinder</td>
<td>15</td>
</tr>
<tr>
<td>Cutting the strand shackle of a padlock with a hacksaw</td>
<td>60</td>
</tr>
<tr>
<td>Cutting a lock of a steel clad door using a grinder</td>
<td>40</td>
</tr>
<tr>
<td>Cutting a shackle of outer window burglar bar with a grinder</td>
<td>10</td>
</tr>
<tr>
<td>Cutting a shackle of outer window burglar bar with a hacksaw blade</td>
<td>60</td>
</tr>
<tr>
<td>Removing a screw from the window burglar bar from the wall with hand tools</td>
<td>20</td>
</tr>
<tr>
<td>Cutting a shackle of inner window burglar bar with a grinder</td>
<td>10</td>
</tr>
<tr>
<td>Cutting a shackle of inner window burglar bar with a hacksaw blade</td>
<td>45</td>
</tr>
<tr>
<td>Cutting a tether wire with a grinder</td>
<td>10</td>
</tr>
<tr>
<td>Cutting a tether wire with a hacksaw blade</td>
<td>50</td>
</tr>
<tr>
<td>Cutting a tether wire with a plier cutter</td>
<td>45</td>
</tr>
<tr>
<td>Cutting a computer padlock with a grinder</td>
<td>5</td>
</tr>
<tr>
<td>Cutting a computer padlock with a hacksaw blade</td>
<td>25</td>
</tr>
<tr>
<td>Cutting a computer padlock with a wire cutter</td>
<td>40</td>
</tr>
<tr>
<td>Removing $^{60}$Co source collimator with a grinder</td>
<td>60</td>
</tr>
<tr>
<td>Removing $^{60}$Co source collimator with a hacksaw blade or hand tools</td>
<td>150</td>
</tr>
<tr>
<td>Removing a computer or stationary item</td>
<td>20</td>
</tr>
<tr>
<td>Setting up an explosive to the source</td>
<td>20</td>
</tr>
</tbody>
</table>
Table 4.3 shows the range of action times from the lowest time to the highest time it took to practically perform a task along the paths.

Table 4.3: Range of action times required to perform a task.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Range of Action Times (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breakthrough D1, D2 or D5</td>
<td>110 – 210</td>
</tr>
<tr>
<td>Breakthrough D3, D4, D6, D7, D8, D9 or D10</td>
<td>20 – 90</td>
</tr>
<tr>
<td>Breakthrough Inner Burglar Bar Gate</td>
<td>60 – 210</td>
</tr>
<tr>
<td>Breakthrough Outer Burglar Bar Gate</td>
<td>50 – 150</td>
</tr>
<tr>
<td>Remove Outer Window Burglar Bars</td>
<td>60 – 180</td>
</tr>
<tr>
<td>Remove Inner Window Burglar Bars</td>
<td>30 – 135</td>
</tr>
<tr>
<td>Break Into Ceiling</td>
<td>55 – 125</td>
</tr>
<tr>
<td>Remove Roof</td>
<td>306 – 789</td>
</tr>
<tr>
<td>Break Through Wall</td>
<td>180 – 480</td>
</tr>
<tr>
<td>Remove Targets (Equipment)</td>
<td>210 – 390</td>
</tr>
<tr>
<td>Remove Target (Computers, Stationary, Chemicals)</td>
<td>25 – 60</td>
</tr>
<tr>
<td>Sabotage Target</td>
<td>80 – 170</td>
</tr>
</tbody>
</table>
Table 4.4 shows the mean and standard deviation (STD) values of the response force time (RFT). This includes the STD for normal distribution of the times and also the STD for group of five times distribution. This is due to the fact that the EASI code requires STD which is a third of the mean for all inputs for high confidence level. Details of this can be found in appendix B in table B1. The use of the mean and STD values in EASI allows consideration of the fact that guards will not always respond in exactly the same or equal intervals of time and also that adversaries may require less or more time to defeat a barrier along the path.

Table 4.4: Mean and standard deviation values of response force time (RFT)

<table>
<thead>
<tr>
<th>Mean of RFT (seconds)</th>
<th>STD of RFT for Normal Distribution (seconds)</th>
<th>STD of RFT for Group of Five Distribution (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>487.00</td>
<td>140.04</td>
<td>146.10</td>
</tr>
</tbody>
</table>

Table 4.5 shows the means and STD values of all action times of the adversary used in the study. It also includes the STD for normal distribution of the times and also the STD for group of five times distribution. Details of these can be found in appendix B from table B2 to table B24. These values were the input variables used to evaluate the effectiveness of the PPS.
Table 4.5: Mean and standard deviation values of adversary delay time (Tdelay)

<table>
<thead>
<tr>
<th>Adversary Action</th>
<th>Mean (seconds)</th>
<th>STD of Normal Distribution (seconds)</th>
<th>STD of Group of Five Distribution (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>11.10</td>
<td>3.20</td>
<td>3.33</td>
</tr>
<tr>
<td>Run to Building</td>
<td>15.00</td>
<td>4.19</td>
<td>4.50</td>
</tr>
<tr>
<td>Breakthrough D1, D2, D5 of F2C</td>
<td>148.50</td>
<td>40.21</td>
<td>44.55</td>
</tr>
<tr>
<td>Breakthrough D2,D6 (F2A) or D4,D6 (F2E)</td>
<td>148.50</td>
<td>40.21</td>
<td>44.55</td>
</tr>
<tr>
<td>Breakthrough D3,D4,D6,D7,D8,D9,D10 of F2C</td>
<td>56.50</td>
<td>16.83</td>
<td>16.95</td>
</tr>
<tr>
<td>Breakthrough D1, D3, D4, D5, D7 of F2A</td>
<td>56.50</td>
<td>16.83</td>
<td>16.95</td>
</tr>
<tr>
<td>Breakthrough D1-D3, D5, and D6-D13 of F2E</td>
<td>56.50</td>
<td>16.83</td>
<td>16.95</td>
</tr>
<tr>
<td>Breakthrough Outer Burglar Gate</td>
<td>94.00</td>
<td>27.02</td>
<td>28.20</td>
</tr>
<tr>
<td>Breakthrough Inner Burglar Gate</td>
<td>159.80</td>
<td>43.82</td>
<td>47.94</td>
</tr>
<tr>
<td>Breakthrough Inner Burglar Gate A</td>
<td>159.80</td>
<td>43.82</td>
<td>47.94</td>
</tr>
<tr>
<td>Run to Controlled Area</td>
<td>7.60</td>
<td>2.12</td>
<td>2.28</td>
</tr>
<tr>
<td>Enter Wash Room</td>
<td>6.00</td>
<td>1.68</td>
<td>1.80</td>
</tr>
<tr>
<td>Remove Roof</td>
<td>306.70</td>
<td>83.71</td>
<td>92.01</td>
</tr>
<tr>
<td>Break Through Wall</td>
<td>323.10</td>
<td>89.20</td>
<td>96.93</td>
</tr>
<tr>
<td>Climb Building</td>
<td>35.10</td>
<td>9.56</td>
<td>10.53</td>
</tr>
<tr>
<td>Break Window Glass</td>
<td>30.00</td>
<td>8.32</td>
<td>9.00</td>
</tr>
<tr>
<td>Remove Outer Window Burglar Bars</td>
<td>128.40</td>
<td>35.97</td>
<td>38.52</td>
</tr>
<tr>
<td>Remove Inner Window Burglar Bars</td>
<td>89.10</td>
<td>25.31</td>
<td>26.73</td>
</tr>
<tr>
<td>Break Into Ceiling</td>
<td>79.50</td>
<td>21.79</td>
<td>23.85</td>
</tr>
<tr>
<td>Jump into Room</td>
<td>18.30</td>
<td>5.10</td>
<td>5.49</td>
</tr>
<tr>
<td>Walk through Maze</td>
<td>10.30</td>
<td>2.90</td>
<td>3.09</td>
</tr>
<tr>
<td>Sabotage Target</td>
<td>118.00</td>
<td>32.43</td>
<td>35.40</td>
</tr>
<tr>
<td>Remove Target (Computers, Stationary, Chemicals)</td>
<td>40.00</td>
<td>10.97</td>
<td>12.00</td>
</tr>
<tr>
<td>Remove Target (Equipment)</td>
<td>281.30</td>
<td>76.02</td>
<td>84.39</td>
</tr>
<tr>
<td>Run to Underground Room</td>
<td>9.00</td>
<td>2.49</td>
<td>2.70</td>
</tr>
<tr>
<td>Walk through LAB</td>
<td>12.40</td>
<td>3.47</td>
<td>3.72</td>
</tr>
<tr>
<td>Walk to Offices</td>
<td>9.20</td>
<td>2.59</td>
<td>2.76</td>
</tr>
</tbody>
</table>
4.4 Evaluation Results of EASI Code

Figures 4.1 to 4.3 show the evaluation results of Adversary Paths for Buildings F2C, F2E and F2A for the existed PPS using the EASI Code before the implementation of the new Design by the GTRI – Sabotage/Theft.

Figure 4.1: Theft evaluation result for building F2C and path 1C.

Figure 4.2: Theft evaluation result for building F2A and path 1A.

Figure 4.3: Theft evaluation result for building F2E and path 1E.
Figures 4.4 to 4.16 show evaluation results of adversary paths for building F2C using the EASI code for the proposed design – sabotage scenario

<table>
<thead>
<tr>
<th>Task Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delay (in Seconds):</th>
<th>Mean</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
<td></td>
</tr>
<tr>
<td>2 Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
<td></td>
</tr>
<tr>
<td>3 Open Outer Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>94</td>
<td>28.2</td>
<td></td>
</tr>
<tr>
<td>4 Open Door 1</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td>44.55</td>
<td></td>
</tr>
<tr>
<td>5 Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td>47.94</td>
<td></td>
</tr>
<tr>
<td>6 Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
<td>3.09</td>
<td></td>
</tr>
<tr>
<td>7 Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>118</td>
<td>35.4</td>
<td></td>
</tr>
</tbody>
</table>

| Probability of Interruption:     | 0.51         |          |                     |      |                    |

Figure 4.4: Sabotage evaluation result for path 1C.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delay (in Seconds):</th>
<th>Mean</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
<td></td>
</tr>
<tr>
<td>2 Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
<td></td>
</tr>
<tr>
<td>3 Open Door 4</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
<td></td>
</tr>
<tr>
<td>4 Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td>47.94</td>
<td></td>
</tr>
<tr>
<td>5 Run to Controlled Area</td>
<td>0</td>
<td>E</td>
<td>7.6</td>
<td>2.28</td>
<td></td>
</tr>
<tr>
<td>6 Open Inner Burglar Gate A</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td>47.94</td>
<td></td>
</tr>
<tr>
<td>7 Open Door 2</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td>44.55</td>
<td></td>
</tr>
<tr>
<td>8 Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
<td>3.09</td>
<td></td>
</tr>
<tr>
<td>9 Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>118</td>
<td>35.4</td>
<td></td>
</tr>
</tbody>
</table>

| Probability of Interruption:     | 0.77         |          |                     |      |                    |

Figure 4.5: Sabotage evaluation result for path 2C.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delay (in Seconds):</th>
<th>Mean</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
<td></td>
</tr>
<tr>
<td>2 Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
<td></td>
</tr>
<tr>
<td>3 Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td>47.94</td>
<td></td>
</tr>
<tr>
<td>4 Run to Controlled Area</td>
<td>0.9</td>
<td>E</td>
<td>7.6</td>
<td>2.28</td>
<td></td>
</tr>
<tr>
<td>5 Open Inner Burglar Gate A</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td>47.94</td>
<td></td>
</tr>
<tr>
<td>6 Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
<td>3.09</td>
<td></td>
</tr>
<tr>
<td>7 Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>118</td>
<td>35.4</td>
<td></td>
</tr>
</tbody>
</table>

| Probability of Interruption:     | 0.77         |          |                     |      |                    |

Figure 4.6: Sabotage evaluation result for path 3C.
Figure 4. 7: Sabotage evaluation result for path 4C.

Figure 4. 8: Sabotage evaluation result for path 5C.

Figure 4. 9: Sabotage evaluation result for path 6C.
### Figure 4. 10: Sabotage evaluation result for path 7C.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
</tr>
<tr>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15.0</td>
</tr>
<tr>
<td>Open Door 3</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
</tr>
<tr>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
</tr>
<tr>
<td>Run to Controlled Area</td>
<td>0.9</td>
<td>E</td>
<td>7.6</td>
</tr>
<tr>
<td>Open Door 7</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
</tr>
<tr>
<td>Break Double Ceiling</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
</tr>
<tr>
<td>Jump into Room</td>
<td>0.9</td>
<td>E</td>
<td>18.3</td>
</tr>
<tr>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>118</td>
</tr>
</tbody>
</table>

**Probability of Interruption:** 0.64

### Figure 4. 11: Sabotage evaluation result for path 8C.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
</tr>
<tr>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15.0</td>
</tr>
<tr>
<td>Open Door 4</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
</tr>
<tr>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
</tr>
<tr>
<td>Run to Controlled Area</td>
<td>0.9</td>
<td>E</td>
<td>7.6</td>
</tr>
<tr>
<td>Enter Wash Room</td>
<td>0</td>
<td>E</td>
<td>6.0</td>
</tr>
<tr>
<td>Break Double Ceiling</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
</tr>
<tr>
<td>Jump into Room</td>
<td>0.9</td>
<td>E</td>
<td>18.3</td>
</tr>
<tr>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>118</td>
</tr>
</tbody>
</table>

**Probability of Interruption:** 0.53

### Figure 4. 12: Sabotage evaluation result for path 9C.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
</tr>
<tr>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15.0</td>
</tr>
<tr>
<td>Open Door 5</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
</tr>
<tr>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
</tr>
<tr>
<td>Open Inner Burglar Gate A</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
</tr>
<tr>
<td>Open Door 5</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
</tr>
<tr>
<td>Sabotage Control Room (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>118</td>
</tr>
</tbody>
</table>

**Probability of Interruption:** 0.76

---

111
It should be noted that, identified path 12C was only evaluated for theft scenario only. This is because, there is no asset of the center on that path that can be sabotaged.
Figure 4.15: Sabotage evaluation result for path 13C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds)</th>
<th>Probability of Interruption: 0.84</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Door 10</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
</tr>
<tr>
<td>4</td>
<td>Break Double Wall</td>
<td>0</td>
<td>E</td>
<td>646.2</td>
<td>193.86</td>
</tr>
<tr>
<td>5</td>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
<td>2.08</td>
</tr>
<tr>
<td>6</td>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>118</td>
<td>35.4</td>
</tr>
</tbody>
</table>

Figure 4.16: Sabotage evaluation result for path 14C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds)</th>
<th>Probability of Interruption: 0.62</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Climb Building</td>
<td>0.9</td>
<td>E</td>
<td>35.1</td>
<td>10.53</td>
</tr>
<tr>
<td>4</td>
<td>Remove Roof</td>
<td>0</td>
<td>E</td>
<td>306.7</td>
<td>92.01</td>
</tr>
<tr>
<td>5</td>
<td>Break Ceiling</td>
<td>0</td>
<td>E</td>
<td>79.5</td>
<td>23.85</td>
</tr>
<tr>
<td>6</td>
<td>Jump into Room</td>
<td>0.9</td>
<td>E</td>
<td>18.3</td>
<td>5.49</td>
</tr>
<tr>
<td>7</td>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
<td>3.09</td>
</tr>
<tr>
<td>8</td>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>118</td>
<td>35.4</td>
</tr>
</tbody>
</table>

Figures 4.17 to 4.30 show evaluation results of adversary paths for building F2C using the EASI code for the proposed design – theft scenario.

Figure 4.17: Theft evaluation result for path 1C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds)</th>
<th>Probability of Interruption: 0.76</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Outer Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>94</td>
<td>28.2</td>
</tr>
<tr>
<td>4</td>
<td>Open Door 1</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td>44.55</td>
</tr>
<tr>
<td>5</td>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td>47.94</td>
</tr>
<tr>
<td>6</td>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
<td>3.09</td>
</tr>
<tr>
<td>7</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td>84.39</td>
</tr>
</tbody>
</table>

113
### Figure 4.18: Theft evaluation result for path 2C.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds):</th>
<th>Probability of Interruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>0.89</td>
</tr>
<tr>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Open Door 4</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
<td></td>
</tr>
<tr>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td></td>
</tr>
<tr>
<td>Run to Controlled Area</td>
<td>0.9</td>
<td>E</td>
<td>7.6</td>
<td></td>
</tr>
<tr>
<td>Open Inner Burglar Gate A</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td></td>
</tr>
<tr>
<td>Open Door 2</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td></td>
</tr>
<tr>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
<td></td>
</tr>
<tr>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td></td>
</tr>
</tbody>
</table>

### Figure 4.19: Theft evaluation result for path 3C.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds):</th>
<th>Probability of Interruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>0.89</td>
</tr>
<tr>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Open Door 3</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
<td></td>
</tr>
<tr>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td></td>
</tr>
<tr>
<td>Run to Controlled Area</td>
<td>0.9</td>
<td>E</td>
<td>7.6</td>
<td></td>
</tr>
<tr>
<td>Open Inner Burglar Gate A</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td></td>
</tr>
<tr>
<td>Open Door 2</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td></td>
</tr>
<tr>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
<td></td>
</tr>
<tr>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td></td>
</tr>
</tbody>
</table>

### Figure 4.20: Theft evaluation result for path 4C.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds):</th>
<th>Probability of Interruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>0.93</td>
</tr>
<tr>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Remove Outer Window Burglar Bars</td>
<td>0</td>
<td>E</td>
<td>128.4</td>
<td></td>
</tr>
<tr>
<td>Break Window Glass</td>
<td>0.9</td>
<td>E</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>Remove Inner Window Burglar Bars</td>
<td>0</td>
<td>E</td>
<td>89.1</td>
<td></td>
</tr>
<tr>
<td>Jump into Room</td>
<td>0</td>
<td>E</td>
<td>18.3</td>
<td></td>
</tr>
<tr>
<td>Run to Controlled Area</td>
<td>0.9</td>
<td>E</td>
<td>7.6</td>
<td></td>
</tr>
<tr>
<td>Open Inner Burglar Gate A</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td></td>
</tr>
<tr>
<td>Open Door 2</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td></td>
</tr>
<tr>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
<td></td>
</tr>
<tr>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td></td>
</tr>
</tbody>
</table>
Figure 4. 21: Theft evaluation result for path 5C.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delay (Seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
</tr>
<tr>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
</tr>
<tr>
<td>Open Door 10</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
</tr>
<tr>
<td>Break Wall</td>
<td>0</td>
<td>E</td>
<td>323.1</td>
</tr>
<tr>
<td>Break Ceiling</td>
<td>0</td>
<td>E</td>
<td>79.5</td>
</tr>
<tr>
<td>Jump into Room</td>
<td>0</td>
<td>E</td>
<td>18.3</td>
</tr>
<tr>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
</tr>
<tr>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
</tr>
</tbody>
</table>

Probability of Interruption: 0.85

Figure 4. 22: Theft evaluation result for path 6C.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delay (Seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
</tr>
<tr>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
</tr>
<tr>
<td>Open Door 8</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
</tr>
<tr>
<td>Remove Roof</td>
<td>0</td>
<td>E</td>
<td>306.7</td>
</tr>
<tr>
<td>Break Ceiling</td>
<td>0</td>
<td>E</td>
<td>79.5</td>
</tr>
<tr>
<td>Jump into Room</td>
<td>0</td>
<td>E</td>
<td>18.3</td>
</tr>
<tr>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
</tr>
<tr>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
</tr>
</tbody>
</table>

Probability of Interruption: 0.84

Figure 4. 23: Theft evaluation result for path 7C.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delay (Seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
</tr>
<tr>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
</tr>
<tr>
<td>Open Door 3</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
</tr>
<tr>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
</tr>
<tr>
<td>Run to Controlled Area</td>
<td>0.9</td>
<td>E</td>
<td>7.6</td>
</tr>
<tr>
<td>Open Door 7</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
</tr>
<tr>
<td>Break Double Ceiling</td>
<td>0</td>
<td>E</td>
<td>159</td>
</tr>
<tr>
<td>Jump into Room</td>
<td>0</td>
<td>E</td>
<td>18.3</td>
</tr>
<tr>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
</tr>
</tbody>
</table>

Probability of Interruption: 0.84
### Figure 4. 24: Theft evaluation result for path 8C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds):</th>
<th>Probability of Interruption:</th>
<th>0.79</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Open Door 4</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td>47.94</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Run to Controlled Area</td>
<td>0.9</td>
<td>E</td>
<td>7.6</td>
<td>2.28</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Enter Wash Room</td>
<td>0</td>
<td>E</td>
<td>6</td>
<td>1.8</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Break Double Ceiling</td>
<td>0</td>
<td>E</td>
<td>159</td>
<td>47.7</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Jump into Room</td>
<td>0</td>
<td>E</td>
<td>18.3</td>
<td>5.49</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td>84.39</td>
<td></td>
</tr>
</tbody>
</table>

### Figure 4. 25: Theft evaluation result for path 9C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds):</th>
<th>Probability of Interruption:</th>
<th>0.89</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Open Door 4</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td>47.94</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Run to Controlled Area</td>
<td>0.9</td>
<td>E</td>
<td>7.6</td>
<td>2.28</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Open Inner Burglar Gate A</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td>47.94</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Open Door 5</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td>44.55</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td>84.39</td>
<td></td>
</tr>
</tbody>
</table>

### Figure 4. 26: Theft evaluation result for path 10C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds):</th>
<th>Probability of Interruption:</th>
<th>0.78</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Open Door 3</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td>47.94</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Enter Wash Room</td>
<td>0</td>
<td>E</td>
<td>6</td>
<td>1.8</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Break Double Ceiling</td>
<td>0</td>
<td>E</td>
<td>159</td>
<td>47.7</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Jump into Room</td>
<td>0</td>
<td>E</td>
<td>18.3</td>
<td>5.49</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td>84.39</td>
<td></td>
</tr>
</tbody>
</table>
### Figure 4.27: Theft evaluation result for path 11C.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds):</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1 3.33</td>
</tr>
<tr>
<td>2. Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15 4.5</td>
</tr>
<tr>
<td>3. Remove Outer Window Burglar Bars</td>
<td>0</td>
<td>E</td>
<td>128.4 38.52</td>
</tr>
<tr>
<td>4. Break Window Glass</td>
<td>0.9</td>
<td>E</td>
<td>39 9</td>
</tr>
<tr>
<td>5. Remove Inner Window Burglar Bars</td>
<td>0</td>
<td>E</td>
<td>89.1 26.73</td>
</tr>
<tr>
<td>6. Jump into Room</td>
<td>0</td>
<td>E</td>
<td>18.3 5.49</td>
</tr>
<tr>
<td>7. Open Door 5</td>
<td>0.9</td>
<td>E</td>
<td>148.5 44.55</td>
</tr>
<tr>
<td>8. Open Door 2</td>
<td>0.9</td>
<td>E</td>
<td>148.5 44.55</td>
</tr>
<tr>
<td>9. Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3 3.09</td>
</tr>
<tr>
<td>10. Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3 84.39</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Probability of Interruption:** 0.89

### Figure 4.28: Theft evaluation result for path 12C.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds):</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1 3.33</td>
</tr>
<tr>
<td>2. Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15 4.5</td>
</tr>
<tr>
<td>3. Remove Outer Window Burglar Bars</td>
<td>0</td>
<td>E</td>
<td>128.4 38.52</td>
</tr>
<tr>
<td>4. Break Window Glass</td>
<td>0.9</td>
<td>E</td>
<td>30 9</td>
</tr>
<tr>
<td>5. Remove Inner Window Burglar Bars</td>
<td>0</td>
<td>E</td>
<td>89.1 26.73</td>
</tr>
<tr>
<td>6. Jump into Room</td>
<td>0</td>
<td>E</td>
<td>18.3 5.49</td>
</tr>
<tr>
<td>7. Open Door 5</td>
<td>0.9</td>
<td>E</td>
<td>148.5 44.55</td>
</tr>
<tr>
<td>8. Open Door 2</td>
<td>0.9</td>
<td>E</td>
<td>148.5 44.55</td>
</tr>
<tr>
<td>9. Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3 3.09</td>
</tr>
<tr>
<td>10. Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3 84.39</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Probability of Interruption:** 0.55

### Figure 4.29: Theft evaluation result for path 13C.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds):</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1 3.33</td>
</tr>
<tr>
<td>2. Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15 4.5</td>
</tr>
<tr>
<td>3. Open Door 10</td>
<td>0.9</td>
<td>E</td>
<td>56.5 16.95</td>
</tr>
<tr>
<td>4. Break Double Wall</td>
<td>0</td>
<td>E</td>
<td>646.2 193.86</td>
</tr>
<tr>
<td>5. Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3 3.09</td>
</tr>
<tr>
<td>6. Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3 84.39</td>
</tr>
<tr>
<td>7.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Probability of Interruption:** 0.90
Figure 4. 30: Theft evaluation result for path 14C.

Figures 4.31 to 4.43 show validation results of the proposed design implementation of building F2C by the global threat reduction initiative using the EASI code - sabotage scenario.

Figure 4. 31: Sabotage evaluation result of GTRI for path 1C.

Figure 4. 32: Sabotage evaluation result of GTRI for path 2C.
### Figure 4.33: Sabotage evaluation result of GTRI for path 3C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Mean (in Seconds)</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Door 3</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
</tr>
<tr>
<td>4</td>
<td>Run to Controlled Area</td>
<td>0</td>
<td>E</td>
<td>7.6</td>
<td>2.28</td>
</tr>
<tr>
<td>5</td>
<td>Open Door 2</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td>44.55</td>
</tr>
<tr>
<td>6</td>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
<td>3.09</td>
</tr>
<tr>
<td>7</td>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>118</td>
<td>35.4</td>
</tr>
</tbody>
</table>

### Figure 4.34: Sabotage evaluation result of GTRI for path 4C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Mean (in Seconds)</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Remove Outer Window Burglar Bars</td>
<td>0</td>
<td>E</td>
<td>128.4</td>
<td>38.52</td>
</tr>
<tr>
<td>4</td>
<td>Break Window Glass</td>
<td>0</td>
<td>E</td>
<td>30</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>Remove Inner Window Burglar Bars</td>
<td>0</td>
<td>E</td>
<td>89.1</td>
<td>26.73</td>
</tr>
<tr>
<td>6</td>
<td>Jump into Room</td>
<td>0</td>
<td>E</td>
<td>18.3</td>
<td>5.49</td>
</tr>
<tr>
<td>7</td>
<td>Run to Controlled Area</td>
<td>0</td>
<td>E</td>
<td>7.6</td>
<td>2.28</td>
</tr>
<tr>
<td>8</td>
<td>Open Door 2</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td>44.55</td>
</tr>
<tr>
<td>9</td>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
<td>3.09</td>
</tr>
<tr>
<td>10</td>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>118</td>
<td>35.4</td>
</tr>
</tbody>
</table>

### Figure 4.35: Sabotage evaluation result of GTRI for path 5C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Mean (in Seconds)</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Door 10</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
</tr>
<tr>
<td>4</td>
<td>Break Wall</td>
<td>0</td>
<td>E</td>
<td>32.3</td>
<td>96.93</td>
</tr>
<tr>
<td>5</td>
<td>Break Ceiling</td>
<td>0</td>
<td>E</td>
<td>79.5</td>
<td>23.85</td>
</tr>
<tr>
<td>6</td>
<td>Jump into Room</td>
<td>0.9</td>
<td>E</td>
<td>18.3</td>
<td>5.49</td>
</tr>
<tr>
<td>7</td>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
<td>3.09</td>
</tr>
<tr>
<td>8</td>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>118</td>
<td>35.4</td>
</tr>
</tbody>
</table>
Figure 4.36: Sabotage evaluation result of GTRI for path 6C.

Figure 4.37: Sabotage evaluation result of GTRI for path 7C.

Figure 4.38: Sabotage evaluation result of GTRI for path 8C.
Figure 4.39: Sabotage evaluation result of GTRI for path 9C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Mean</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
<td></td>
</tr>
<tr>
<td>Run to Building</td>
<td>0</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
<td></td>
</tr>
<tr>
<td>Open Door 4</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
<td></td>
</tr>
<tr>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td>47.94</td>
<td></td>
</tr>
<tr>
<td>Run to Controlled Area</td>
<td>0</td>
<td>E</td>
<td>7.6</td>
<td>2.28</td>
<td></td>
</tr>
<tr>
<td>Open Door 5</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td>44.55</td>
<td></td>
</tr>
<tr>
<td>Sabotage Control Room (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>118</td>
<td>35.4</td>
<td></td>
</tr>
</tbody>
</table>

Probability of Interruption: 0.01

Figure 4.40: Sabotage evaluation result of GTRI for path 10C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Mean</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
<td></td>
</tr>
<tr>
<td>Run to Building</td>
<td>0</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
<td></td>
</tr>
<tr>
<td>Open Door 3</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
<td></td>
</tr>
<tr>
<td>Enter Wash Room</td>
<td>0</td>
<td>E</td>
<td>6</td>
<td>1.8</td>
<td></td>
</tr>
<tr>
<td>Break Double Ceiling</td>
<td>0</td>
<td>E</td>
<td>6</td>
<td>1.8</td>
<td></td>
</tr>
<tr>
<td>Jump into Room</td>
<td>0.9</td>
<td>E</td>
<td>18.3</td>
<td>5.49</td>
<td></td>
</tr>
<tr>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>118</td>
<td>35.4</td>
<td></td>
</tr>
</tbody>
</table>

Probability of Interruption: 0.01

Figure 4.41: Sabotage evaluation result of GTRI for path 11C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Mean</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
<td></td>
</tr>
<tr>
<td>Run to Building</td>
<td>0</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
<td></td>
</tr>
<tr>
<td>Remove Outer Window Burglar Bars</td>
<td>0</td>
<td>E</td>
<td>128.4</td>
<td>38.52</td>
<td></td>
</tr>
<tr>
<td>Break Window Glass</td>
<td>0.9</td>
<td>E</td>
<td>39</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Remove Inner Window Burglar Bars</td>
<td>0</td>
<td>E</td>
<td>89.1</td>
<td>26.73</td>
<td></td>
</tr>
<tr>
<td>Jump into Room</td>
<td>0</td>
<td>E</td>
<td>18.3</td>
<td>5.49</td>
<td></td>
</tr>
<tr>
<td>Open Door 5</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td>44.55</td>
<td></td>
</tr>
<tr>
<td>Open Door 2</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td>44.55</td>
<td></td>
</tr>
<tr>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
<td>3.09</td>
<td></td>
</tr>
<tr>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>118</td>
<td>35.4</td>
<td></td>
</tr>
</tbody>
</table>

Probability of Interruption: 0.52
Figure 4.42: Sabotage evaluation result of GTRI for path 13C.

Figures 4.44 to 4.57 show validation results of the proposed design implementation of Building F2C by the Global Threat Reduction Initiative using the EASI Code - Theft Scenario.

Figure 4.44: Theft evaluation result of GTRI for path 1C.
**Figure 4.45:** Theft evaluation result of GTRI for path 2C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds)</th>
<th>Probability of Interruption: 0.10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Door 4</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
</tr>
<tr>
<td>4</td>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td>47.04</td>
</tr>
<tr>
<td>5</td>
<td>Run to Controlled Area</td>
<td>0</td>
<td>E</td>
<td>7.6</td>
<td>2.28</td>
</tr>
<tr>
<td>6</td>
<td>Open Door 2</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td>44.55</td>
</tr>
<tr>
<td>7</td>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
<td>3.09</td>
</tr>
<tr>
<td>8</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td>84.39</td>
</tr>
</tbody>
</table>

**Figure 4.46:** Theft evaluation result of GTRI for path 3C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds)</th>
<th>Probability of Interruption: 0.10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Door 3</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
</tr>
<tr>
<td>4</td>
<td>Run to Controlled Area</td>
<td>0</td>
<td>E</td>
<td>7.6</td>
<td>2.28</td>
</tr>
<tr>
<td>5</td>
<td>Open Door 2</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td>44.55</td>
</tr>
<tr>
<td>6</td>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
<td>3.09</td>
</tr>
<tr>
<td>7</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td>84.39</td>
</tr>
</tbody>
</table>

**Figure 4.47:** Theft evaluation result of GTRI for path 4C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds)</th>
<th>Probability of Interruption: 0.10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Remove Outer Window Burglar Bars</td>
<td>0</td>
<td>E</td>
<td>128.4</td>
<td>38.52</td>
</tr>
<tr>
<td>4</td>
<td>Break Window Glass</td>
<td>0</td>
<td>E</td>
<td>39</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>Remove Inner Window Burglar Bars</td>
<td>0</td>
<td>E</td>
<td>89.1</td>
<td>26.73</td>
</tr>
<tr>
<td>6</td>
<td>Jump into Room</td>
<td>0</td>
<td>E</td>
<td>18.3</td>
<td>5.49</td>
</tr>
<tr>
<td>7</td>
<td>Run to Controlled Area</td>
<td>0</td>
<td>E</td>
<td>7.6</td>
<td>2.28</td>
</tr>
<tr>
<td>8</td>
<td>Open Door 2</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td>44.55</td>
</tr>
<tr>
<td>9</td>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
<td>3.09</td>
</tr>
<tr>
<td>10</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td>84.39</td>
</tr>
</tbody>
</table>
Figure 4.48: Theft evaluation result of GTRI for path 5C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Mean</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Door 10</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
</tr>
<tr>
<td>4</td>
<td>Break Wall</td>
<td>0</td>
<td>E</td>
<td>323.1</td>
<td>96.93</td>
</tr>
<tr>
<td>5</td>
<td>Break Ceiling</td>
<td>0</td>
<td>E</td>
<td>79.5</td>
<td>23.85</td>
</tr>
<tr>
<td>6</td>
<td>Jump into Room</td>
<td>0.9</td>
<td>E</td>
<td>18.3</td>
<td>5.49</td>
</tr>
<tr>
<td>7</td>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
<td>3.09</td>
</tr>
<tr>
<td>8</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td>84.39</td>
</tr>
</tbody>
</table>

Probability of Interruption: 0.10

Figure 4.49: Theft evaluation result of GTRI for path 6C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Mean</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Door 8</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
</tr>
<tr>
<td>4</td>
<td>Remove Roof</td>
<td>0</td>
<td>E</td>
<td>306.7</td>
<td>92.01</td>
</tr>
<tr>
<td>5</td>
<td>Walk through Ceiling</td>
<td>0</td>
<td>E</td>
<td>79.5</td>
<td>23.85</td>
</tr>
<tr>
<td>6</td>
<td>Jump into Room</td>
<td>0.9</td>
<td>E</td>
<td>18.3</td>
<td>5.49</td>
</tr>
<tr>
<td>7</td>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>10.3</td>
<td>3.09</td>
</tr>
<tr>
<td>8</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td>84.39</td>
</tr>
</tbody>
</table>

Probability of Interruption: 0.10

Figure 4.50: Theft evaluation result of GTRI for path 7C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Mean</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Door 3</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
</tr>
<tr>
<td>4</td>
<td>Run to Controlled Area</td>
<td>0</td>
<td>E</td>
<td>7.6</td>
<td>2.28</td>
</tr>
<tr>
<td>5</td>
<td>Open Door 7</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
</tr>
<tr>
<td>6</td>
<td>Break Double Ceiling</td>
<td>0</td>
<td>E</td>
<td>159</td>
<td>47.7</td>
</tr>
<tr>
<td>7</td>
<td>Jump into Room</td>
<td>0.9</td>
<td>E</td>
<td>18.3</td>
<td>5.49</td>
</tr>
<tr>
<td>8</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td>84.39</td>
</tr>
</tbody>
</table>

Probability of Interruption: 0.09
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Mean:</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Door 4</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
</tr>
<tr>
<td>4</td>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td>47.94</td>
</tr>
<tr>
<td>5</td>
<td>Run to Controlled Area</td>
<td>0</td>
<td>E</td>
<td>7.6</td>
<td>2.28</td>
</tr>
<tr>
<td>6</td>
<td>Enter Wash Room</td>
<td>0</td>
<td>E</td>
<td>6</td>
<td>1.8</td>
</tr>
<tr>
<td>7</td>
<td>Break Double Ceiling</td>
<td>0</td>
<td>E</td>
<td>159</td>
<td>47.7</td>
</tr>
<tr>
<td>8</td>
<td>Jump into Room</td>
<td>0.9</td>
<td>E</td>
<td>18.3</td>
<td>5.49</td>
</tr>
<tr>
<td>9</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td>84.39</td>
</tr>
</tbody>
</table>

Table: Probability of Interruption: 0.09

Figure 4. 51: Theft evaluation result of GTRI for path 8C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Mean:</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Door 4</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
</tr>
<tr>
<td>4</td>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td>47.94</td>
</tr>
<tr>
<td>5</td>
<td>Run to Controlled Area</td>
<td>0</td>
<td>E</td>
<td>7.6</td>
<td>2.28</td>
</tr>
<tr>
<td>6</td>
<td>Enter Wash Room</td>
<td>0</td>
<td>E</td>
<td>6</td>
<td>1.8</td>
</tr>
<tr>
<td>7</td>
<td>Break Double Ceiling</td>
<td>0</td>
<td>E</td>
<td>159</td>
<td>47.7</td>
</tr>
<tr>
<td>8</td>
<td>Jump into Room</td>
<td>0.9</td>
<td>E</td>
<td>18.3</td>
<td>5.49</td>
</tr>
<tr>
<td>9</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td>84.39</td>
</tr>
</tbody>
</table>

Table: Probability of Interruption: 0.09

Figure 4. 52: Theft evaluation result of GTRI for path 9C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Mean:</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Door 4</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
</tr>
<tr>
<td>4</td>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td>47.94</td>
</tr>
<tr>
<td>5</td>
<td>Run to Controlled Area</td>
<td>0</td>
<td>E</td>
<td>7.6</td>
<td>2.28</td>
</tr>
<tr>
<td>6</td>
<td>Enter Wash Room</td>
<td>0</td>
<td>E</td>
<td>6</td>
<td>1.8</td>
</tr>
<tr>
<td>7</td>
<td>Break Double Ceiling</td>
<td>0</td>
<td>E</td>
<td>159</td>
<td>47.7</td>
</tr>
<tr>
<td>8</td>
<td>Jump into Room</td>
<td>0.9</td>
<td>E</td>
<td>18.3</td>
<td>5.49</td>
</tr>
<tr>
<td>9</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td>84.39</td>
</tr>
</tbody>
</table>

Table: Probability of Interruption: 0.09

Figure 4. 53: Theft evaluation result of GTRI for path 10C.
**Figure 4. 54:** Theft evaluation result of GTRI for path 11C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Mean</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Remove Outer Window Burglar Bars</td>
<td>0</td>
<td>E</td>
<td>128.4</td>
<td>38.52</td>
</tr>
<tr>
<td>4</td>
<td>Break Window Glass</td>
<td>0.9</td>
<td>E</td>
<td>30</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>Remove Inner Window Burglar Bars</td>
<td>0</td>
<td>E</td>
<td>89.1</td>
<td>26.73</td>
</tr>
<tr>
<td>6</td>
<td>Jump into Room</td>
<td>0</td>
<td>E</td>
<td>18.3</td>
<td>5.49</td>
</tr>
<tr>
<td>7</td>
<td>Open Door 5</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td>44.55</td>
</tr>
<tr>
<td>8</td>
<td>Open Door 2</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td>44.55</td>
</tr>
<tr>
<td>9</td>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>16.3</td>
<td>3.09</td>
</tr>
<tr>
<td>10</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td>84.39</td>
</tr>
</tbody>
</table>

**Probability of Interruption:** 0.77

**Figure 4. 55:** Theft evaluation result of GTRI for path 12C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Mean</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Remove Outer Window Burglar Bars</td>
<td>0</td>
<td>E</td>
<td>128.4</td>
<td>38.52</td>
</tr>
<tr>
<td>4</td>
<td>Break Window Glass</td>
<td>0.9</td>
<td>E</td>
<td>30</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>Remove Inner Window Burglar Bars</td>
<td>0</td>
<td>E</td>
<td>89.1</td>
<td>26.73</td>
</tr>
<tr>
<td>6</td>
<td>Jump into Room</td>
<td>0</td>
<td>E</td>
<td>18.3</td>
<td>5.49</td>
</tr>
<tr>
<td>7</td>
<td>Open Door 5</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td>44.55</td>
</tr>
<tr>
<td>8</td>
<td>Open Door 2</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td>44.55</td>
</tr>
<tr>
<td>9</td>
<td>Walk through Maze</td>
<td>0</td>
<td>E</td>
<td>16.3</td>
<td>3.09</td>
</tr>
<tr>
<td>10</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td>84.39</td>
</tr>
</tbody>
</table>

**Probability of Interruption:** 0.09

**Figure 4. 56:** Theft evaluation result of GTRI for path 13C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Mean</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Door 10</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
</tr>
<tr>
<td>4</td>
<td>Break Double Wall</td>
<td>0</td>
<td>E</td>
<td>646.2</td>
<td>193.86</td>
</tr>
<tr>
<td>5</td>
<td>Walk through Maze</td>
<td>0.9</td>
<td>E</td>
<td>10.3</td>
<td>3.09</td>
</tr>
<tr>
<td>6</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>281.3</td>
<td>84.39</td>
</tr>
</tbody>
</table>

**Probability of Interruption:** 0.09
Figure 4. 57: Theft evaluation result of GTRI for path 14C.

Figures 4.58 to 4.67 show evaluation results of adversary paths for building F2A using the EASI code for the proposed design – theft scenario.

Figure 4. 58: Theft evaluation result for path 1A.
Figure 4. 59: Theft evaluation result for path 2A.

Figure 4. 60: Theft evaluation result for path 3A.

Figure 4. 61: Theft evaluation result for path 4A.
Figure 4. 62: Theft evaluation result for path 5A.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Probability of Guard Communication</th>
<th>Response</th>
<th>Force Time (in Seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
</tr>
<tr>
<td>2 Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
</tr>
<tr>
<td>3 Open Outer Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>94</td>
</tr>
<tr>
<td>4 Open Door 7</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
</tr>
<tr>
<td>5 Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
</tr>
<tr>
<td>6 Open Door 6</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
</tr>
<tr>
<td>7 Walk to Office G07</td>
<td>0</td>
<td>E</td>
<td>9.2</td>
</tr>
<tr>
<td>8 Open Door 5</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
</tr>
<tr>
<td>9 Remove Target (Computers)</td>
<td>0</td>
<td>E</td>
<td>40</td>
</tr>
</tbody>
</table>

Probability of interruption: 0.60

Figure 4. 63: Theft evaluation result for path 6A.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Probability of Guard Communication</th>
<th>Response</th>
<th>Force Time (in Seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
</tr>
<tr>
<td>2 Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
</tr>
<tr>
<td>3 Open Outer Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>94</td>
</tr>
<tr>
<td>4 Open Door 7</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
</tr>
<tr>
<td>5 Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
</tr>
<tr>
<td>6 Open Door 6</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
</tr>
<tr>
<td>7 Walk to Office G07</td>
<td>0</td>
<td>E</td>
<td>9.2</td>
</tr>
<tr>
<td>8 Open Door 2</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
</tr>
<tr>
<td>9 Remove Target (Stationary)</td>
<td>0</td>
<td>E</td>
<td>40</td>
</tr>
</tbody>
</table>

Probability of interruption: 0.75

Figure 4. 64: Theft evaluation result for path 7A.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Probability of Guard Communication</th>
<th>Response</th>
<th>Force Time (in Seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
</tr>
<tr>
<td>2 Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
</tr>
<tr>
<td>3 Open Outer Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>94</td>
</tr>
<tr>
<td>4 Open Door 7</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
</tr>
<tr>
<td>5 Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
</tr>
<tr>
<td>6 Open Door 8</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
</tr>
<tr>
<td>7 Remove Target (Equipment)</td>
<td>0</td>
<td>E</td>
<td>281.3</td>
</tr>
</tbody>
</table>

Probability of interruption: 0.73
Figure 4. 65: Theft evaluation result for path 8A.

Figure 4. 66: Theft evaluation result for path 9A.

Figure 4. 67: Theft evaluation result for path 10A.
Figures 4.68 to 4.77 show evaluation results of adversary paths for building F2E using the EASI code for the proposed design– theft scenario.

### Estimate of Adversary Sequence

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Probability of Guard Communication</th>
<th>Location</th>
<th>Delays (in Seconds):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability of Interruption</td>
<td>0.74</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Mean Delay</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Outer Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>94</td>
<td>28.2</td>
</tr>
<tr>
<td>4</td>
<td>Open Door 9</td>
<td>0.9</td>
<td>E</td>
<td>46.5</td>
<td>16.95</td>
</tr>
<tr>
<td>5</td>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td>54.9</td>
</tr>
<tr>
<td>6</td>
<td>Open Door 8</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
</tr>
<tr>
<td>7</td>
<td>Walk through LAB</td>
<td>0.9</td>
<td>E</td>
<td>12.4</td>
<td>3.72</td>
</tr>
<tr>
<td>8</td>
<td>Remove Target (Equipment)</td>
<td>0</td>
<td>E</td>
<td>281.3</td>
<td>84.39</td>
</tr>
</tbody>
</table>

Figure 4. 68: Theft evaluation result for path 1E.

### Estimate of Adversary Sequence

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Probability of Guard Communication</th>
<th>Location</th>
<th>Delays (in Seconds):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability of Interruption</td>
<td>0.62</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Mean Delay</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Outer Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>94</td>
<td>28.2</td>
</tr>
<tr>
<td>4</td>
<td>Open Door 1</td>
<td>0.9</td>
<td>E</td>
<td>46.5</td>
<td>16.95</td>
</tr>
<tr>
<td>5</td>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td>54.9</td>
</tr>
<tr>
<td>6</td>
<td>Open Door 4</td>
<td>0</td>
<td>E</td>
<td>148.5</td>
<td>44.58</td>
</tr>
<tr>
<td>7</td>
<td>Walk to Door 9</td>
<td>0</td>
<td>E</td>
<td>9.2</td>
<td>2.76</td>
</tr>
<tr>
<td>8</td>
<td>Walk to Office G11</td>
<td>0.9</td>
<td>E</td>
<td>159.8</td>
<td>47.94</td>
</tr>
<tr>
<td>9</td>
<td>Open Door 10</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
</tr>
<tr>
<td>10</td>
<td>Remove Target (Chemicals)</td>
<td>0</td>
<td>E</td>
<td>40</td>
<td>12</td>
</tr>
</tbody>
</table>

Figure 4. 69: Theft evaluation result for path 2E.

### Estimate of Adversary Sequence

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Probability of Guard Communication</th>
<th>Location</th>
<th>Delays (in Seconds):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability of Interruption</td>
<td>0.74</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Mean Delay</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>111</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Outer Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>94</td>
<td>28.2</td>
</tr>
<tr>
<td>4</td>
<td>Open Door 11</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
</tr>
<tr>
<td>5</td>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td>47.94</td>
</tr>
<tr>
<td>6</td>
<td>Walk to Office G11</td>
<td>0.9</td>
<td>E</td>
<td>9.2</td>
<td>2.76</td>
</tr>
<tr>
<td>7</td>
<td>Open Door 10</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>16.95</td>
</tr>
<tr>
<td>8</td>
<td>Remove Target (Equipment)</td>
<td>0</td>
<td>E</td>
<td>281.3</td>
<td>84.39</td>
</tr>
</tbody>
</table>

Figure 4. 70: Theft evaluation result for path 3E.
### Figure 4. 71: Theft evaluation result for path 4E.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds)</th>
<th>Probability of Interruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>0.66</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Open Outer Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>94</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Open Door 11</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Walk through LAB</td>
<td>0.9</td>
<td>E</td>
<td>12.4</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Remove Target (Equipment)</td>
<td>0</td>
<td>E</td>
<td>281</td>
<td></td>
</tr>
</tbody>
</table>

### Figure 4. 72: Theft evaluation result for path 5E.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds)</th>
<th>Probability of Interruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>0.79</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Open Outer Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>94</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Open Door 9</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Open Door 8</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Walk through LAB</td>
<td>0</td>
<td>E</td>
<td>12.4</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Open Door 7</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Open Door 6</td>
<td>0.9</td>
<td>E</td>
<td>148.5</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Open Door 3</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Remove Target (Computers)</td>
<td>0</td>
<td>E</td>
<td>40</td>
<td></td>
</tr>
</tbody>
</table>

### Figure 4. 73: Theft evaluation result for path 6E.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds)</th>
<th>Probability of Interruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>0.74</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Open Outer Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>94</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Open Door 12</td>
<td>0.9</td>
<td>E</td>
<td>56.5</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>E</td>
<td>159.8</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Open Door 13</td>
<td>0</td>
<td>E</td>
<td>56.6</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Walk through LAB</td>
<td>0</td>
<td>E</td>
<td>12.4</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Remove Target (Equipment)</td>
<td>0</td>
<td>E</td>
<td>281.3</td>
<td></td>
</tr>
</tbody>
</table>

132
Figure 4. 74: Theft evaluation result for path 7E.

Figure 4. 75: Theft evaluation result for path 8E.

Figure 4. 76: Theft evaluation result for path 9E.
Figure 4. 77: Theft evaluation result for path 10E.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>P(Detection)</th>
<th>Location</th>
<th>Delays (in Seconds)</th>
<th>Probability of Interruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>0</td>
<td>E</td>
<td>11.1</td>
<td>0.82</td>
</tr>
<tr>
<td>Run to Building</td>
<td>0.9</td>
<td>E</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Climb Building</td>
<td>0.9</td>
<td>E</td>
<td>35.1</td>
<td></td>
</tr>
<tr>
<td>Remove Roof</td>
<td>0</td>
<td>E</td>
<td>306.7</td>
<td></td>
</tr>
<tr>
<td>Break Ceiling</td>
<td>0</td>
<td>E</td>
<td>79.5</td>
<td></td>
</tr>
<tr>
<td>Jumps into Room</td>
<td>0</td>
<td>E</td>
<td>18.3</td>
<td></td>
</tr>
<tr>
<td>Walk through LAB</td>
<td>0</td>
<td>E</td>
<td>12.4</td>
<td></td>
</tr>
<tr>
<td>Remove Target (Equipment)</td>
<td>0</td>
<td>E</td>
<td>281.3</td>
<td></td>
</tr>
</tbody>
</table>
4.5 Evaluation Results from the EASIM Code

The EASI and ASSESS codes were proposed for this research but ASSESS was not yet ready for distribution to African countries, including South Africa, during the evaluation stage of this study and therefore EASI was used for the evaluation. In view of this, I studied the algorithm of the EASI code and created another code from it to be used for multiple pathways since the EASI code only evaluates a specific pathway at a time. This new code was called EASIM (Estimation of Adversary Sequence Interruption for Multiple Paths). This was used for multiple paths simultaneously.

Figures 4.78 to 4.80 show evaluation results of multiple adversary pathways for buildings F2C, F2A and F2E using EASIM code for the existed PPS before the implementation of the new design by the GTRI – sabotage/theft scenario.

![Table of Pathways and Delays](image)

Figure 4. 78: Theft evaluation result for building F2C and pathways 1-2-3C.
**Figure 4. 79: Theft evaluation result for building F2A and pathways 1-2-6A**

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD-1</th>
<th>PD-2</th>
<th>PD-3</th>
<th>Location-1</th>
<th>Location-2</th>
<th>Location-3</th>
<th>Mean-1</th>
<th>Mean-2</th>
<th>Mean-3</th>
<th>STD-3</th>
<th>STD-2</th>
<th>STD-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>11.1</td>
<td>11.1</td>
<td>11.1</td>
<td>3.33</td>
<td>3.33</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>4.3</td>
<td>4.3</td>
<td>4.3</td>
</tr>
<tr>
<td>3</td>
<td>Open Outer Burglar Gate</td>
<td>Open Outer Burglar Gate</td>
<td>Open Outer Burglar Gate</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>84</td>
<td>84</td>
<td>84</td>
<td>28.2</td>
<td>28.2</td>
<td>28.2</td>
</tr>
<tr>
<td>4</td>
<td>Open Door 1</td>
<td>Break Window Glass</td>
<td>Open Door 1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>56.3</td>
<td>56.3</td>
<td>56.3</td>
<td>16.95</td>
<td>16.95</td>
<td>16.95</td>
</tr>
<tr>
<td>5</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>159.8</td>
<td>159.8</td>
<td>159.8</td>
<td>47.84</td>
<td>47.84</td>
<td>47.84</td>
</tr>
<tr>
<td>6</td>
<td>Walk through LAB</td>
<td>Jump into Room</td>
<td>Open Door 6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>12.4</td>
<td>18.3</td>
<td>148.5</td>
<td>44.25</td>
<td>2.49</td>
<td>3.72</td>
</tr>
<tr>
<td>7</td>
<td>Walk to Office G1</td>
<td>Walk through LAB</td>
<td>Walk to Office G1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>9.2</td>
<td>12.4</td>
<td>9.2</td>
<td>2.78</td>
<td>2.78</td>
<td>2.78</td>
</tr>
<tr>
<td>8</td>
<td>Open Door 2</td>
<td>Remove Target (Equipment)</td>
<td>Open Door 2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>148.3</td>
<td>216.5</td>
<td>148.3</td>
<td>44.35</td>
<td>44.35</td>
<td>44.35</td>
</tr>
<tr>
<td>9</td>
<td>Remove Target (Stationary)</td>
<td>Remove Target (Stationary)</td>
<td>E</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>40</td>
<td>40</td>
<td>40</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 4. 80: Theft evaluation result for building F2E and pathways 1-2-3E**

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD-1</th>
<th>PD-2</th>
<th>PD-3</th>
<th>Location-1</th>
<th>Location-2</th>
<th>Location-3</th>
<th>Mean-1</th>
<th>Mean-2</th>
<th>Mean-3</th>
<th>STD-3</th>
<th>STD-2</th>
<th>STD-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>11.1</td>
<td>11.1</td>
<td>11.1</td>
<td>3.33</td>
<td>3.33</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>4.3</td>
<td>4.3</td>
<td>4.3</td>
</tr>
<tr>
<td>3</td>
<td>Open Outer Burglar Gate</td>
<td>Open Outer Burglar Gate</td>
<td>Open Outer Burglar Gate</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>84</td>
<td>84</td>
<td>84</td>
<td>28.2</td>
<td>28.2</td>
<td>28.2</td>
</tr>
<tr>
<td>4</td>
<td>Open Door 1</td>
<td>Open Door 11</td>
<td>Open Door 11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>56.5</td>
<td>56.5</td>
<td>56.5</td>
<td>18.95</td>
<td>18.95</td>
<td>18.95</td>
</tr>
<tr>
<td>5</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>159.8</td>
<td>159.8</td>
<td>159.8</td>
<td>47.84</td>
<td>47.84</td>
<td>47.84</td>
</tr>
<tr>
<td>6</td>
<td>Walk through LAB</td>
<td>Open Door 4</td>
<td>Open Door 4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>12.4</td>
<td>148.5</td>
<td>148.5</td>
<td>44.25</td>
<td>44.25</td>
<td>44.25</td>
</tr>
<tr>
<td>7</td>
<td>Walk to Office G1</td>
<td>Remove Target (Equipment)</td>
<td>Remove Target (Equipment)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>201.3</td>
<td>201.3</td>
<td>201.3</td>
<td>84.39</td>
<td>84.39</td>
<td>84.39</td>
</tr>
<tr>
<td>8</td>
<td>Open Door 10</td>
<td>E</td>
<td>E</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>56.5</td>
<td>56.5</td>
<td>18.95</td>
<td>18.95</td>
<td>18.95</td>
<td>18.95</td>
</tr>
<tr>
<td>9</td>
<td>Remove Target (Chemicals)</td>
<td>E</td>
<td>E</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>40</td>
<td>40</td>
<td>40</td>
<td>12</td>
<td>12</td>
<td>12</td>
</tr>
</tbody>
</table>

**Estimation of Adversary Sequence**

**Interruption for Multiple Pathways**

**Probability of Guard Communication**

<table>
<thead>
<tr>
<th>Probability of Guard Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.09</td>
</tr>
</tbody>
</table>

**Response Force Time (in seconds)**

<table>
<thead>
<tr>
<th>Mean</th>
<th>STD</th>
</tr>
</thead>
<tbody>
<tr>
<td>487</td>
<td>141.1</td>
</tr>
</tbody>
</table>

**Probability of Interruption**

<table>
<thead>
<tr>
<th>Probability of Interruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.09</td>
</tr>
</tbody>
</table>
Figures 4.81 to 4.86 show evaluation results of multiple adversary pathways for building F2C using the EASIM code for the proposed design—sabotage scenario.

<table>
<thead>
<tr>
<th>Task</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD-1</th>
<th>PD-2</th>
<th>PD-3</th>
<th>Location 1</th>
<th>Location 2</th>
<th>Location 3</th>
<th>Mean 1</th>
<th>Mean 2</th>
<th>Mean 3</th>
<th>STD-1</th>
<th>STD-2</th>
<th>STD-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>11.1</td>
<td>11.1</td>
<td>11.1</td>
<td>3.33</td>
<td>3.33</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>4.5</td>
<td>4.5</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Inner Burglar Gate</td>
<td>Open Door 4</td>
<td>Open Door 3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>84</td>
<td>85.5</td>
<td>85.5</td>
<td>16.95</td>
<td>16.95</td>
<td>16.95</td>
</tr>
<tr>
<td>4</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
<td>0.8</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>148.5</td>
<td>150.3</td>
<td>150.3</td>
<td>47.84</td>
<td>47.84</td>
<td>47.84</td>
</tr>
<tr>
<td>5</td>
<td>Run to Controlled Area</td>
<td>Run to Controlled Area</td>
<td>Run to Controlled Area</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>159.9</td>
<td>7.6</td>
<td>7.6</td>
<td>2.28</td>
<td>2.28</td>
<td>2.28</td>
</tr>
<tr>
<td>6</td>
<td>Walk through Maze</td>
<td>Open Inner Burglar Gate A</td>
<td>Open Inner Burglar Gate A</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>10.2</td>
<td>159.8</td>
<td>159.8</td>
<td>47.94</td>
<td>47.94</td>
<td>47.94</td>
</tr>
<tr>
<td>7</td>
<td>Sabotage Target (Equipment)</td>
<td>Sabotage Target (Equipment)</td>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>110</td>
<td>148.2</td>
<td>148.2</td>
<td>44.25</td>
<td>44.25</td>
<td>44.25</td>
</tr>
<tr>
<td>8</td>
<td>Walk through Maze</td>
<td>Walk through Maze</td>
<td>Walk through Maze</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>19.5</td>
<td>19.5</td>
<td>19.5</td>
<td>3.98</td>
<td>3.98</td>
<td>3.98</td>
</tr>
<tr>
<td>9</td>
<td>Sabotage Target (Equipment)</td>
<td>Sabotage Target (Equipment)</td>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>110</td>
<td>110</td>
<td>110</td>
<td>35.4</td>
<td>35.4</td>
<td>35.4</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 4.81: Sabotage evaluation result for pathways 1-2-3C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD-1</th>
<th>PD-2</th>
<th>PD-3</th>
<th>Location 1</th>
<th>Location 2</th>
<th>Location 3</th>
<th>Mean 1</th>
<th>Mean 2</th>
<th>Mean 3</th>
<th>STD-1</th>
<th>STD-2</th>
<th>STD-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>11.1</td>
<td>11.1</td>
<td>11.1</td>
<td>3.33</td>
<td>3.33</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>4.5</td>
<td>4.5</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Inner Burglar Gate</td>
<td>Open Door 4</td>
<td>Open Door 3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>84</td>
<td>85.5</td>
<td>85.5</td>
<td>16.95</td>
<td>16.95</td>
<td>16.95</td>
</tr>
<tr>
<td>4</td>
<td>Open Door 1</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
<td>0.8</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>148.5</td>
<td>150.3</td>
<td>150.3</td>
<td>47.84</td>
<td>47.84</td>
<td>47.84</td>
</tr>
<tr>
<td>5</td>
<td>Run to Controlled Area</td>
<td>Run to Controlled Area</td>
<td>Run to Controlled Area</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>159.9</td>
<td>7.6</td>
<td>7.6</td>
<td>2.28</td>
<td>2.28</td>
<td>2.28</td>
</tr>
<tr>
<td>6</td>
<td>Walk through Maze</td>
<td>Open Inner Burglar Gate A</td>
<td>Open Inner Burglar Gate A</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>10.2</td>
<td>159.8</td>
<td>159.8</td>
<td>47.94</td>
<td>47.94</td>
<td>47.94</td>
</tr>
<tr>
<td>7</td>
<td>Sabotage Target (Equipment)</td>
<td>Sabotage Target (Equipment)</td>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>110</td>
<td>148.2</td>
<td>148.2</td>
<td>44.25</td>
<td>44.25</td>
<td>44.25</td>
</tr>
<tr>
<td>8</td>
<td>Walk through Maze</td>
<td>Walk through Maze</td>
<td>Walk through Maze</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>19.5</td>
<td>19.5</td>
<td>19.5</td>
<td>3.98</td>
<td>3.98</td>
<td>3.98</td>
</tr>
<tr>
<td>9</td>
<td>Sabotage Target (Equipment)</td>
<td>Sabotage Target (Equipment)</td>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>110</td>
<td>110</td>
<td>110</td>
<td>35.4</td>
<td>35.4</td>
<td>35.4</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 4.82: Sabotage evaluation result for pathways 1-4-14C.

137
Figure 4. 83: Sabotage evaluation result for pathways 3-8-13C.

Figure 4. 84: Sabotage evaluation result for pathways 4-5-6C.
### Figure 4. 85: Sabotage evaluation result for pathways 7-8-5C.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD-1</th>
<th>PD-2</th>
<th>PD-3</th>
<th>Location-1</th>
<th>Location-2</th>
<th>Location-3</th>
<th>Mean-1</th>
<th>STD-1</th>
<th>Mean-2</th>
<th>STD-2</th>
<th>Mean-3</th>
<th>STD-3</th>
<th>Probability of Guard Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>11.1</td>
<td>11.1</td>
<td>11.1</td>
<td>3.33</td>
<td>3.33</td>
<td>3.33</td>
<td>0.93</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>4.5</td>
<td>4.5</td>
<td>4.5</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Door 3</td>
<td>Open Door 4</td>
<td>Open Door 10</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>56.5</td>
<td>56.5</td>
<td>56.5</td>
<td>16.95</td>
<td>16.95</td>
<td>16.95</td>
<td>0.93</td>
</tr>
<tr>
<td>4</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
<td>Break Wall</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>159.8</td>
<td>159.8</td>
<td>159.8</td>
<td>98.93</td>
<td>98.93</td>
<td>98.93</td>
<td>0.93</td>
</tr>
<tr>
<td>5</td>
<td>Run to Controlled Area</td>
<td>Run to Controlled Area</td>
<td>Break Ceiling</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>7.6</td>
<td>7.6</td>
<td>7.6</td>
<td>3.00</td>
<td>3.00</td>
<td>3.00</td>
<td>0.93</td>
</tr>
<tr>
<td>6</td>
<td>Open Door 1</td>
<td>Enter Wash Rooms</td>
<td>Jump into Room</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>56.5</td>
<td>56.5</td>
<td>56.5</td>
<td>18.3</td>
<td>18.3</td>
<td>18.3</td>
<td>0.93</td>
</tr>
<tr>
<td>7</td>
<td>Break Double Ceiling</td>
<td>Break Double Ceiling</td>
<td>Walk through Maze</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>159.8</td>
<td>159.8</td>
<td>159.8</td>
<td>10.3</td>
<td>10.3</td>
<td>10.3</td>
<td>0.93</td>
</tr>
<tr>
<td>8</td>
<td>Jump into Room</td>
<td>Jump into Room</td>
<td>Sabotage Target (Equipment)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>18.3</td>
<td>18.3</td>
<td>18.3</td>
<td>5.40</td>
<td>5.40</td>
<td>5.40</td>
<td>0.93</td>
</tr>
<tr>
<td>9</td>
<td>Sabotage Target (Equipment)</td>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>118</td>
<td>118</td>
<td>118</td>
<td>58.4</td>
<td>58.4</td>
<td>58.4</td>
<td>0.93</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Figure 4. 86: Sabotage evaluation result for pathways 10-11-13C.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD-1</th>
<th>PD-2</th>
<th>PD-3</th>
<th>Location-1</th>
<th>Location-2</th>
<th>Location-3</th>
<th>Mean-1</th>
<th>STD-1</th>
<th>Mean-2</th>
<th>STD-2</th>
<th>Mean-3</th>
<th>STD-3</th>
<th>Probability of Guard Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>11.1</td>
<td>11.1</td>
<td>11.1</td>
<td>3.33</td>
<td>3.33</td>
<td>3.33</td>
<td>0.93</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>4.5</td>
<td>4.5</td>
<td>4.5</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Door 3</td>
<td>Open Door 4</td>
<td>Open Door 10</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>56.5</td>
<td>56.5</td>
<td>56.5</td>
<td>16.95</td>
<td>16.95</td>
<td>16.95</td>
<td>0.93</td>
</tr>
<tr>
<td>4</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
<td>Break Wall</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>159.8</td>
<td>159.8</td>
<td>159.8</td>
<td>98.93</td>
<td>98.93</td>
<td>98.93</td>
<td>0.93</td>
</tr>
<tr>
<td>5</td>
<td>Run to Controlled Area</td>
<td>Run to Controlled Area</td>
<td>Break Ceiling</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>7.6</td>
<td>7.6</td>
<td>7.6</td>
<td>3.00</td>
<td>3.00</td>
<td>3.00</td>
<td>0.93</td>
</tr>
<tr>
<td>6</td>
<td>Open Door 1</td>
<td>Enter Wash Rooms</td>
<td>Jump into Room</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>56.5</td>
<td>56.5</td>
<td>56.5</td>
<td>18.3</td>
<td>18.3</td>
<td>18.3</td>
<td>0.93</td>
</tr>
<tr>
<td>7</td>
<td>Break Double Ceiling</td>
<td>Break Double Ceiling</td>
<td>Walk through Maze</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>159.8</td>
<td>159.8</td>
<td>159.8</td>
<td>10.3</td>
<td>10.3</td>
<td>10.3</td>
<td>0.93</td>
</tr>
<tr>
<td>8</td>
<td>Jump into Room</td>
<td>Jump into Room</td>
<td>Sabotage Target (Equipment)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>18.3</td>
<td>18.3</td>
<td>18.3</td>
<td>5.40</td>
<td>5.40</td>
<td>5.40</td>
<td>0.93</td>
</tr>
<tr>
<td>9</td>
<td>Sabotage Target (Equipment)</td>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>118</td>
<td>118</td>
<td>118</td>
<td>58.4</td>
<td>58.4</td>
<td>58.4</td>
<td>0.93</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Probability of Interruption
- Figure 4. 85: 0.93
- Figure 4. 86: 0.73
Figures 4.87 to 4.92 show evaluation results of multiple adversary pathways for building F2C using the EASIM code for the proposed design – theft scenario.

Figure 4. 87: Theft evaluation result for pathways 1-2-3C.

Figure 4. 88: Theft evaluation result for pathways 1-4-14C.
Figure 4. 89: Theft evaluation result for pathways 4-5-6C.

Figure 4. 90: Theft evaluation result for pathways 7-8-5C.
### Table 4.91: Theft evaluation result for pathways 9-10-12C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD_1</th>
<th>PD_2</th>
<th>PD_3</th>
<th>Location_1</th>
<th>Location_2</th>
<th>Location_3</th>
<th>Mean_1</th>
<th>Mean_2</th>
<th>Mean_3</th>
<th>STD_1</th>
<th>STD_2</th>
<th>STD_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>11.1</td>
<td>11.1</td>
<td>11.1</td>
<td>3.33</td>
<td>3.33</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>4.5</td>
<td>4.5</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Door 4</td>
<td>Open Door 3</td>
<td>Remove Outer Window Bars</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>4.5</td>
<td>4.5</td>
<td>4.5</td>
</tr>
<tr>
<td>4</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
<td>Break Window Glass</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>15.8</td>
<td>15.8</td>
<td>15.8</td>
<td>9</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>Run to Controlled Area</td>
<td>Enter Wash Room</td>
<td>Remove Inner Window Bars</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>7.6</td>
<td>6</td>
<td>18.1</td>
<td>1.8</td>
<td>2.18</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Open Inner Burglar Gate A</td>
<td>Break Double Ceiling</td>
<td>Jump into Room</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>15.8</td>
<td>15.8</td>
<td>15.8</td>
<td>5.49</td>
<td>4.7</td>
<td>4.74</td>
</tr>
<tr>
<td>7</td>
<td>Open Door 5</td>
<td>Jump into Room</td>
<td>Walk through LAB</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>148.5</td>
<td>18.3</td>
<td>12.4</td>
<td>3.72</td>
<td>5.49</td>
<td>44.55</td>
</tr>
<tr>
<td>8</td>
<td>Remove Target (Equipment)</td>
<td>Remove Target (Equipment)</td>
<td>Remove Target (Equipment)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>201.3</td>
<td>201.3</td>
<td>201.3</td>
<td>84.39</td>
<td>84.39</td>
<td>84.39</td>
</tr>
</tbody>
</table>

### Table 4.92: Theft evaluation result for pathways 11-8-13C.

<table>
<thead>
<tr>
<th>Task</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD_1</th>
<th>PD_2</th>
<th>PD_3</th>
<th>Location_1</th>
<th>Location_2</th>
<th>Location_3</th>
<th>Mean_1</th>
<th>Mean_2</th>
<th>Mean_3</th>
<th>STD_1</th>
<th>STD_2</th>
<th>STD_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>11.1</td>
<td>11.1</td>
<td>11.1</td>
<td>3.33</td>
<td>3.33</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>4.5</td>
<td>4.5</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Remove Outer Burglar Bars</td>
<td>Open Door 10</td>
<td>Open Door 10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>128.4</td>
<td>35.5</td>
<td>35.5</td>
<td>16.95</td>
<td>16.95</td>
<td>16.95</td>
</tr>
<tr>
<td>4</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
<td>Break Double Wall</td>
<td>0.9</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>30</td>
<td>159.8</td>
<td>644.3</td>
<td>193.86</td>
<td>47.94</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>Remove Inner Burglar Bars</td>
<td>Run to Controlled Area</td>
<td>Walk through Mine</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>10.1</td>
<td>7.6</td>
<td>10.3</td>
<td>3.39</td>
<td>2.28</td>
<td>26.73</td>
</tr>
<tr>
<td>6</td>
<td>Remove Target (Equipment)</td>
<td>Remove Target (Equipment)</td>
<td>Remove Target (Equipment)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>183</td>
<td>6</td>
<td>201.3</td>
<td>84.39</td>
<td>84.39</td>
<td>84.39</td>
</tr>
<tr>
<td>7</td>
<td>Open Door 5</td>
<td>Break Double Ceiling</td>
<td>Jump into Room</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>148.5</td>
<td>18.3</td>
<td>12.4</td>
<td>3.72</td>
<td>5.49</td>
<td>44.55</td>
</tr>
<tr>
<td>8</td>
<td>Open Door 2</td>
<td>Jump into Room</td>
<td>Remove Target (Equipment)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>148.5</td>
<td>18.3</td>
<td>12.4</td>
<td>3.72</td>
<td>5.49</td>
<td>44.55</td>
</tr>
</tbody>
</table>

### Figure 4.91: Theft evaluation result for pathways 9-10-12C.

### Figure 4.92: Theft evaluation result for pathways 11-8-13C.
Figures 4.93 to 4.98 show validation results of the proposed design implementation of building F2C by the global threat reduction initiative using the EASIM code - sabotage scenario.

Figure 4.93: Sabotage evaluation result of GTRI for pathways 1-2-3C.

Figure 4.94: Sabotage evaluation result of GTRI for pathways 1-4-14C.
### Figure 4.95: Sabotage evaluation result of GTRI for pathways 3-8-13C.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD-1</th>
<th>PD-2</th>
<th>PD-3</th>
<th>Location-1</th>
<th>Location-2</th>
<th>Location-3</th>
<th>Location-4</th>
<th>Location-5</th>
<th>Mean-1</th>
<th>Mean-2</th>
<th>STD-1</th>
<th>STD-2</th>
<th>STD-3</th>
<th>STD-4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>11.1</td>
<td>11.1</td>
<td>3.33</td>
<td>3.33</td>
<td>3.33</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>15</td>
<td>15</td>
<td>4.5</td>
<td>4.5</td>
<td>4.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Open Door 1</td>
<td>Open Door 2</td>
<td>Open Door 3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>58.5</td>
<td>58.5</td>
<td>16.95</td>
<td>16.95</td>
<td>16.95</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Run to Controlled Area</td>
<td>Open Inner Bargal Gate</td>
<td>Break Double Wall</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>7.6</td>
<td>519.0</td>
<td>646.2</td>
<td>193.36</td>
<td>47.94</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Open Door 2</td>
<td>Run to Controlled Area</td>
<td>Walk through Mason</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>148.3</td>
<td>7.6</td>
<td>10.3</td>
<td>3.69</td>
<td>2.28</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Walk through Mason</td>
<td>Enter Wash Room</td>
<td>Sabotage Target (Equipment)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>10.3</td>
<td>6</td>
<td>118</td>
<td>35.4</td>
<td>1.18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Sabotage Target (Equipment)</td>
<td>Break Double Ceiling</td>
<td>Sabotage Target (Equipment)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>118</td>
<td>159</td>
<td>47.3</td>
<td>25.4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Jump into Room</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>118</td>
<td>159</td>
<td>47.3</td>
<td>25.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>118</td>
<td>159</td>
<td>47.3</td>
<td>25.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Figure 4.96: Sabotage evaluation result of GTRI for pathways 4-5-6C.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD-1</th>
<th>PD-2</th>
<th>PD-3</th>
<th>Location-1</th>
<th>Location-2</th>
<th>Location-3</th>
<th>Location-4</th>
<th>Location-5</th>
<th>Mean-1</th>
<th>Mean-2</th>
<th>STD-1</th>
<th>STD-2</th>
<th>STD-3</th>
<th>STD-4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>11.1</td>
<td>11.1</td>
<td>3.33</td>
<td>3.33</td>
<td>3.33</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>15</td>
<td>15</td>
<td>4.5</td>
<td>4.5</td>
<td>4.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Open Door 1</td>
<td>Open Door 2</td>
<td>Open Door 3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>58.5</td>
<td>58.5</td>
<td>16.95</td>
<td>16.95</td>
<td>16.95</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Run to Controlled Area</td>
<td>Open Inner Bargal Gate</td>
<td>Break Double Wall</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>7.6</td>
<td>519.0</td>
<td>646.2</td>
<td>193.36</td>
<td>47.94</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Open Door 2</td>
<td>Run to Controlled Area</td>
<td>Walk through Mason</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>148.3</td>
<td>7.6</td>
<td>10.3</td>
<td>3.69</td>
<td>2.28</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Walk through Mason</td>
<td>Enter Wash Room</td>
<td>Sabotage Target (Equipment)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>10.3</td>
<td>6</td>
<td>118</td>
<td>35.4</td>
<td>1.18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Sabotage Target (Equipment)</td>
<td>Break Double Ceiling</td>
<td>Sabotage Target (Equipment)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>118</td>
<td>159</td>
<td>47.3</td>
<td>25.4</td>
<td>2.28</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Jump into Room</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>118</td>
<td>159</td>
<td>47.3</td>
<td>25.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>118</td>
<td>159</td>
<td>47.3</td>
<td>25.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Probability of Interruption:** 0.01
Figure 4.97: Sabotage evaluation result of GTRI for pathways 7-8-5C.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD-1</th>
<th>PD-2</th>
<th>PD-3</th>
<th>Location-1</th>
<th>Location-2</th>
<th>Location-3</th>
<th>Mean-1</th>
<th>Mean-2</th>
<th>Mean-3</th>
<th>STD-1</th>
<th>STD-2</th>
<th>STD-3</th>
<th>STD-4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0 0 0 0 E E</td>
<td></td>
<td></td>
<td></td>
<td>11.1 11.1 11.1</td>
<td>3.33 3.33 3.33</td>
<td>4.5 4.5 4.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0 0 0 0 E E</td>
<td></td>
<td></td>
<td></td>
<td>15 15 15</td>
<td>4.5 4.5 4.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Open Door 3</td>
<td>Open Door 4</td>
<td>Open Door 10</td>
<td>0 0 0 0 E E</td>
<td>56.5</td>
<td>56.5</td>
<td>56.5</td>
<td>16.95 16.95 16.95</td>
<td>2.21 2.21 2.21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Run to Controlled Area</td>
<td>Open Inner Burglar Gate</td>
<td>Break Wall</td>
<td>0 0 0 0 E E</td>
<td>7.6</td>
<td>159.1</td>
<td>32.1</td>
<td>0.94 0.94 0.94</td>
<td>7.21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Open Door 7</td>
<td>Run to Controlled Area</td>
<td>Break Ceiling</td>
<td>0 0 0 0 E E</td>
<td>56.5</td>
<td>7.6 79.5</td>
<td>22.85 22.85 22.85</td>
<td>16.95</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 Break Double Ceiling</td>
<td>Enter Wash Rooms</td>
<td>Jump into Room</td>
<td>0 0 0 0 E E</td>
<td>159 6</td>
<td>183.3</td>
<td>5.49 5.49 5.49</td>
<td>1.8 1.8 1.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 Jump into Room</td>
<td>Break Double Ceiling</td>
<td>Walk through Maze</td>
<td>0 0 0 0 E E</td>
<td>10.3</td>
<td>19.9</td>
<td>10.3</td>
<td>3.9 3.9 3.9</td>
<td>5.49 5.49 5.49</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8 Sabotage Target (Equipment)</td>
<td>Jump into Room</td>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>118 118</td>
<td>33.4</td>
<td>5.49 5.49 5.49</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>118</td>
<td>33.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 4.98: Sabotage evaluation result of GTRI for pathways 10-11-13C.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD-1</th>
<th>PD-2</th>
<th>PD-3</th>
<th>Location-1</th>
<th>Location-2</th>
<th>Location-3</th>
<th>Mean-1</th>
<th>Mean-2</th>
<th>Mean-3</th>
<th>STD-1</th>
<th>STD-2</th>
<th>STD-3</th>
<th>STD-4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0 0 0 0 E E</td>
<td></td>
<td></td>
<td></td>
<td>11.1 11.1 11.1</td>
<td>3.33 3.33 3.33</td>
<td>4.5 4.5 4.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0 0 0 0 E E</td>
<td></td>
<td></td>
<td></td>
<td>15 15 15</td>
<td>4.5 4.5 4.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Open Door 3</td>
<td>Open Door 4</td>
<td>Open Door 10</td>
<td>0 0 0 0 E E</td>
<td>56.5</td>
<td>56.5</td>
<td>56.5</td>
<td>16.95 16.95 16.95</td>
<td>2.21 2.21 2.21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Run to Controlled Area</td>
<td>Open Inner Burglar Gate</td>
<td>Break Wall</td>
<td>0 0 0 0 E E</td>
<td>7.6</td>
<td>159.1</td>
<td>32.1</td>
<td>0.94 0.94 0.94</td>
<td>7.21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Open Door 7</td>
<td>Run to Controlled Area</td>
<td>Break Ceiling</td>
<td>0 0 0 0 E E</td>
<td>56.5</td>
<td>7.6 79.5</td>
<td>22.85 22.85 22.85</td>
<td>16.95</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 Break Double Ceiling</td>
<td>Enter Wash Rooms</td>
<td>Jump into Room</td>
<td>0 0 0 0 E E</td>
<td>159 6</td>
<td>183.3</td>
<td>5.49 5.49 5.49</td>
<td>1.8 1.8 1.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 Jump into Room</td>
<td>Break Double Ceiling</td>
<td>Walk through Maze</td>
<td>0 0 0 0 E E</td>
<td>10.3</td>
<td>19.9</td>
<td>10.3</td>
<td>3.9 3.9 3.9</td>
<td>5.49 5.49 5.49</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8 Sabotage Target (Equipment)</td>
<td>Jump into Room</td>
<td>Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>118 118</td>
<td>33.4</td>
<td>5.49 5.49 5.49</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 Sabotage Target (Equipment)</td>
<td>0.9</td>
<td>118</td>
<td>33.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Probability of Intermittent: 0.15

Figure 4.98: Sabotage evaluation result of GTRI for pathways 10-11-13C.
Figures 4.99 to 4.104 show validation results of the proposed design implementation of building F2C by the global threat reduction initiative using the EASIM code - theft scenario.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD-1</th>
<th>PD-2</th>
<th>PD-3</th>
<th>Location 1</th>
<th>Location 2</th>
<th>Location 3</th>
<th>Mean 1</th>
<th>Mean 2</th>
<th>Mean 3</th>
<th>STD-1</th>
<th>STD-2</th>
<th>STD-3</th>
<th>DIs (in seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>11.1</td>
<td>11.1</td>
<td>11.1</td>
<td>3.33</td>
<td>3.33</td>
<td>3.33</td>
<td>20.1</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>4.5</td>
<td>4.5</td>
<td>4.5</td>
<td>8.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Outer Burglar Gate</td>
<td>Open Door 1</td>
<td>Open Door 3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>94</td>
<td>56.5</td>
<td>56.5</td>
<td>18.95</td>
<td>18.95</td>
<td>18.95</td>
<td>20.1</td>
</tr>
<tr>
<td>4</td>
<td>Open Door 1</td>
<td>Open Inner Burglar Gate</td>
<td>Run to Controlled Area</td>
<td>0.9</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>140.5</td>
<td>150.1</td>
<td>7.8</td>
<td>2.20</td>
<td>4.94</td>
<td>44.35</td>
<td>1.9</td>
</tr>
<tr>
<td>5</td>
<td>Walk through Maze</td>
<td>Run to Controlled Area</td>
<td>Open Door 2</td>
<td>0</td>
<td>0</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>10.3</td>
<td>7.6</td>
<td>140.5</td>
<td>44.35</td>
<td>2.20</td>
<td>3.09</td>
<td>1.9</td>
</tr>
<tr>
<td>6</td>
<td>Remove Target (Equipment)</td>
<td>Open Door 1</td>
<td>Walk through Maze</td>
<td>0</td>
<td>0</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>201.3</td>
<td>140.5</td>
<td>10.3</td>
<td>3.09</td>
<td>44.55</td>
<td>84.39</td>
<td>1.9</td>
</tr>
<tr>
<td>7</td>
<td>Walk through Maze</td>
<td>Remove Target (Equipment)</td>
<td>0</td>
<td>0</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>10.3</td>
<td>201.3</td>
<td>84.39</td>
<td>3.09</td>
<td>1.9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>181.3</td>
<td>3.09</td>
<td>1.9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 4.99:** Theft evaluation result of GTRI for pathways 1-2-3C.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD-1</th>
<th>PD-2</th>
<th>PD-3</th>
<th>Location 1</th>
<th>Location 2</th>
<th>Location 3</th>
<th>Mean 1</th>
<th>Mean 2</th>
<th>Mean 3</th>
<th>STD-1</th>
<th>STD-2</th>
<th>STD-3</th>
<th>DIs (in seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>11.1</td>
<td>11.1</td>
<td>11.1</td>
<td>3.33</td>
<td>3.33</td>
<td>3.33</td>
<td>20.1</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>4.5</td>
<td>4.5</td>
<td>4.5</td>
<td>8.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Outer Burglar Gate</td>
<td>Open Door 1</td>
<td>Open Door 3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>94</td>
<td>56.5</td>
<td>56.5</td>
<td>18.95</td>
<td>18.95</td>
<td>18.95</td>
<td>20.1</td>
</tr>
<tr>
<td>4</td>
<td>Open Door 1</td>
<td>Open Inner Burglar Gate</td>
<td>Run to Controlled Area</td>
<td>0.9</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>140.5</td>
<td>150.1</td>
<td>7.8</td>
<td>2.20</td>
<td>4.94</td>
<td>44.35</td>
<td>1.9</td>
</tr>
<tr>
<td>5</td>
<td>Walk through Maze</td>
<td>Run to Controlled Area</td>
<td>Open Door 2</td>
<td>0</td>
<td>0</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>10.3</td>
<td>7.6</td>
<td>140.5</td>
<td>44.35</td>
<td>2.20</td>
<td>3.09</td>
<td>1.9</td>
</tr>
<tr>
<td>6</td>
<td>Remove Target (Equipment)</td>
<td>Open Door 1</td>
<td>Walk through Maze</td>
<td>0</td>
<td>0</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>201.3</td>
<td>140.5</td>
<td>10.3</td>
<td>3.09</td>
<td>44.55</td>
<td>84.39</td>
<td>1.9</td>
</tr>
<tr>
<td>7</td>
<td>Walk through Maze</td>
<td>Remove Target (Equipment)</td>
<td>0</td>
<td>0</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>10.3</td>
<td>201.3</td>
<td>84.39</td>
<td>3.09</td>
<td>1.9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>E</td>
<td>181.3</td>
<td>3.09</td>
<td>1.9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 4.100:** Theft evaluation result of GTRI for pathways 1-4-14C.

146
Figure 4. 101: Theft evaluation result of GTRI for pathways 4-5-6C.

Figure 4. 102: Theft evaluation result of GTRI for pathways 7-8-5C.
### Figure 4.103: Theft evaluation result of GTRI for pathways 9-10-12C.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD 1</th>
<th>PD 2</th>
<th>PD 3</th>
<th>Location 1</th>
<th>Location 2</th>
<th>Location 3</th>
<th>Mean 1</th>
<th>Mean 2</th>
<th>Mean 3</th>
<th>STD 1</th>
<th>STD 2</th>
<th>STD 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>11.1</td>
<td>11.1</td>
<td>11.1</td>
<td>3.33</td>
<td>3.33</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>4.5</td>
<td>4.5</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Door 1</td>
<td>Open Door 3</td>
<td>Reserved Outer Window Bars</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>58.5</td>
<td>58.5</td>
<td>58.5</td>
<td>128.4</td>
<td>38.52</td>
<td>16.95</td>
</tr>
<tr>
<td>4</td>
<td>Open Inner Burglar Gate</td>
<td>Enter Wash Room</td>
<td>Break Window Glass</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>118.6</td>
<td>6</td>
<td>30</td>
<td>6</td>
<td>26.3</td>
<td>45.47</td>
</tr>
<tr>
<td>5</td>
<td>Run to Controlled Area</td>
<td>Break Double Ceiling</td>
<td>Reserve Inner Window Bars</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>7.8</td>
<td>25</td>
<td>53</td>
<td>8.1</td>
<td>26.3</td>
<td>47.94</td>
</tr>
<tr>
<td>6</td>
<td>Open Door 5</td>
<td>Jump into Room</td>
<td>Jump into Room</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>201.3</td>
<td>201.3</td>
<td>12.4</td>
<td>3.72</td>
<td>84.19</td>
<td>84.19</td>
</tr>
<tr>
<td>7</td>
<td>Remove Target (Equipment)</td>
<td>Remove Target (Equipment)</td>
<td>Walk through LAB</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>201.3</td>
<td>201.3</td>
<td>12.4</td>
<td>3.72</td>
<td>84.19</td>
<td>84.19</td>
</tr>
</tbody>
</table>

### Figure 4.104: Theft evaluation result of GTRI for pathways 11-8-13C.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD 1</th>
<th>PD 2</th>
<th>PD 3</th>
<th>Location 1</th>
<th>Location 2</th>
<th>Location 3</th>
<th>Mean 1</th>
<th>Mean 2</th>
<th>Mean 3</th>
<th>STD 1</th>
<th>STD 2</th>
<th>STD 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>11.1</td>
<td>11.1</td>
<td>11.1</td>
<td>3.33</td>
<td>3.33</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>4.5</td>
<td>4.5</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Remove Outer Burglar Bars</td>
<td>Open Door 4</td>
<td>Open Door 10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>128.4</td>
<td>56.5</td>
<td>56.5</td>
<td>160.5</td>
<td>45.52</td>
<td>16.95</td>
</tr>
<tr>
<td>4</td>
<td>Break Window Glass</td>
<td>Open Inner Burglar Gate</td>
<td>Break Double Wall</td>
<td>0.9</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>30</td>
<td>159.8</td>
<td>645.2</td>
<td>183.88</td>
<td>47.94</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>Reserve Inner Burglar Bars</td>
<td>Run to Controlled Area</td>
<td>Walk through Maze</td>
<td>0</td>
<td>0</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>80.3</td>
<td>7.6</td>
<td>10.3</td>
<td>3.09</td>
<td>2.38</td>
<td>26.73</td>
</tr>
<tr>
<td>6</td>
<td>Jump into Room</td>
<td>Enter Wash Rooms</td>
<td>Reserve Target (Equipment)</td>
<td>0</td>
<td>0</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>18.6</td>
<td>6</td>
<td>381.5</td>
<td>84.59</td>
<td>44.49</td>
<td>1.1</td>
</tr>
<tr>
<td>7</td>
<td>Open Door 5</td>
<td>Break Double Ceiling</td>
<td>0.9</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>148.5</td>
<td>159</td>
<td>47.7</td>
<td>44.55</td>
<td>48.19</td>
<td>44.55</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Open Door 2</td>
<td>Jump into Room</td>
<td>0.9</td>
<td>0.9</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>148.5</td>
<td>18.3</td>
<td>3.49</td>
<td>44.55</td>
<td>84.19</td>
<td>84.19</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Remove Target (Equipment)</td>
<td>Remove Target (Equipment)</td>
<td>0.9</td>
<td>0.9</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>201.3</td>
<td>201.3</td>
<td>12.4</td>
<td>3.72</td>
<td>84.19</td>
<td>84.19</td>
<td></td>
</tr>
</tbody>
</table>

Probability of Interruption: 0.10

Probability of Interruption: 0.31

148
Figures 4.105 to 4.110 show evaluation results of multiple adversary pathways for building F2A using the EASIM code for the proposed design – theft scenario

Figure 4.105: Theft evaluation result for pathways 1-2-6A.

Figure 4.106: Theft evaluation result for pathways 2-5-1A.
### Figure 4.107: Theft evaluation result for pathways 3-6-8A.

<table>
<thead>
<tr>
<th>Task</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD 1</th>
<th>PD 2</th>
<th>PD 3</th>
<th>Location 1</th>
<th>Location 2</th>
<th>Location 3</th>
<th>Mean 1</th>
<th>Mean 2</th>
<th>Mean 3</th>
<th>STD 1</th>
<th>STD 2</th>
<th>STD 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>11.1</td>
<td>11.1</td>
<td>11.1</td>
<td>3.33</td>
<td>3.33</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>4.5</td>
<td>4.5</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Outer Burglar Bars</td>
<td>Open Outer Burglar Gate</td>
<td>Open Outer Burglar Gate</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>128.4</td>
<td>94</td>
<td>94</td>
<td>28.2</td>
<td>20.2</td>
<td>38.52</td>
</tr>
<tr>
<td>4</td>
<td>Break Window Glass</td>
<td>Open Door 7</td>
<td>Open Door 1</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>30</td>
<td>56.5</td>
<td>56.5</td>
<td>16.95</td>
<td>16.95</td>
<td>4.5</td>
</tr>
<tr>
<td>5</td>
<td>Reserve Inner Burglar Bars</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>10.3</td>
<td>159.8</td>
<td>159.8</td>
<td>47.94</td>
<td>47.94</td>
<td>26.73</td>
</tr>
<tr>
<td>6</td>
<td>Jump into Room</td>
<td>Open Door 6</td>
<td>Walk to Door 6</td>
<td>0.9</td>
<td>0</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>18.3</td>
<td>148.5</td>
<td>9.2</td>
<td>2.78</td>
<td>46.23</td>
<td>5.49</td>
</tr>
<tr>
<td>7</td>
<td>Open Door 4</td>
<td>Walk to Office G01</td>
<td>Open Door 6</td>
<td>0</td>
<td>0</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>56.3</td>
<td>9.2</td>
<td>24.5</td>
<td>4.5</td>
<td>16.95</td>
<td>2.76</td>
</tr>
<tr>
<td>8</td>
<td>Walk to Office G07</td>
<td>Open Door 2</td>
<td>Open Door 3</td>
<td>0</td>
<td>0</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>9.2</td>
<td>148.5</td>
<td>56.5</td>
<td>16.95</td>
<td>44.55</td>
<td>2.76</td>
</tr>
<tr>
<td>9</td>
<td>Open Door 5</td>
<td>Reserve Target (Stationary)</td>
<td>Reserve Target (Equipment)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>56.5</td>
<td>40</td>
<td>281.2</td>
<td>8.49</td>
<td>14.95</td>
<td>14.95</td>
</tr>
<tr>
<td>10</td>
<td>Reserve Target (Equipment)</td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>281.2</td>
<td>8.49</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Probability of Interruption:** 0.75

### Figure 4.108: Theft evaluation result for pathways 3-7-9A.

<table>
<thead>
<tr>
<th>Task</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD 1</th>
<th>PD 2</th>
<th>PD 3</th>
<th>Location 1</th>
<th>Location 2</th>
<th>Location 3</th>
<th>Mean 1</th>
<th>Mean 2</th>
<th>Mean 3</th>
<th>STD 1</th>
<th>STD 2</th>
<th>STD 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>11.1</td>
<td>11.1</td>
<td>11.1</td>
<td>3.33</td>
<td>3.33</td>
<td>3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>4.5</td>
<td>4.5</td>
<td>4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Outer Burglar Bars</td>
<td>Open Outer Burglar Gate</td>
<td>Climb Building</td>
<td>0</td>
<td>0</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>128.4</td>
<td>94</td>
<td>94</td>
<td>28.2</td>
<td>20.2</td>
<td>38.52</td>
</tr>
<tr>
<td>4</td>
<td>Break Window Glass</td>
<td>Open Door 7</td>
<td>Remove Roof</td>
<td>0.9</td>
<td>0.9</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>30</td>
<td>56.5</td>
<td>368.7</td>
<td>92.91</td>
<td>16.95</td>
<td>4.5</td>
</tr>
<tr>
<td>5</td>
<td>Open Inner Burglar Bars</td>
<td>Open Inner Burglar Gate</td>
<td>Break Collar</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>80.1</td>
<td>159.8</td>
<td>70.3</td>
<td>23.93</td>
<td>47.94</td>
<td>26.73</td>
</tr>
<tr>
<td>6</td>
<td>Jump into Room</td>
<td>Open Door 8</td>
<td>Jump into Room</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>18.3</td>
<td>56.5</td>
<td>18.3</td>
<td>5.49</td>
<td>16.95</td>
<td>2.76</td>
</tr>
<tr>
<td>7</td>
<td>Open Door 4</td>
<td>Reserve Target (Equipment)</td>
<td>Walk to Office G01</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>56.3</td>
<td>281.2</td>
<td>9.2</td>
<td>2.78</td>
<td>46.23</td>
<td>5.49</td>
</tr>
<tr>
<td>8</td>
<td>Walk to Office G07</td>
<td>Open Door 2</td>
<td>Open Door 3</td>
<td>0</td>
<td>0</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>9.2</td>
<td>148.5</td>
<td>56.5</td>
<td>16.95</td>
<td>44.55</td>
<td>2.76</td>
</tr>
<tr>
<td>9</td>
<td>Open Door 5</td>
<td>Reserve Target (Stationary)</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>56.6</td>
<td>40</td>
<td>12</td>
<td>16.95</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Reserve Target (Equipment)</td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>281.2</td>
<td>8.49</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Probability of Interruption:** 0.74

150
Figure 4. 109: Theft evaluation result for pathways 4-5-9A.

Figure 4. 110: Theft evaluation result for pathways 4-9-10A.
Figures 4.111 to 4.116 show evaluation results of multiple adversary pathways for building F2E using the EASIM code for the proposed design – theft scenario.

### Table: Evaluation Results

| Tasks       | Path 1          | Path 2          | Path 3          | PD-1 | PD-2 | PD-3 | Location-1 | Location-2 | Location-3 | Location-4 | Mean-1 | Mean-2 | Mean-3 | STD-1 | STD-2 | STD-3 | STD-4 | STD-5 |
|-------------|-----------------|-----------------|-----------------|------|------|------|------------|------------|------------|------------|--------|--------|--------|-------|-------|-------|-------|-------|-------|
| 1           | Jump Fence      | Jump Fence      | Jump Fence      | 0    | 0    | E    | E          | E          | E          | 11.1      | 11.1   | 11.1   | 3.33   | 3.33  | 3.33  | 3.33  | 3.33  | 3.33  |
| 2           | Run to Building | Run to Building | Run to Building | 0.9  | 0.9  | 0.9  | E          | E          | E          | 15        | 15     | 15     | 4.5    | 4.5   | 4.5   | 4.5   | 4.5   | 4.5   |
| 3           | Open Outer Burglar Gate | Open Outer Burglar Gate | Open Outer Burglar Gate | 0    | 0    | E    | E          | E          | E          | 94        | 94     | 94     | 38.3   | 38.3  | 38.3  | 38.3  | 38.3  | 38.3  |
| 4           | Open Door 9     | Open Door 11    | Open Door 1     | 0.9  | 0.9  | 0.9  | E          | E          | E          | 56.5      | 56.5   | 56.5   | 16.95  | 16.95 | 16.95 | 16.95 | 16.95 | 16.95 |
| 5           | Open Inner Burglar Gate | Open Inner Burglar Gate | Open Inner Burglar Gate | 0    | 0    | E    | E          | E          | E          | 159.8     | 159.8  | 159.8  | 47.94  | 47.94 | 47.94 | 47.94 | 47.94 | 47.94 |
| 6           | Open Door 8     | Walk to Office G11 | Walk to Office G11 | 0    | 0    | E    | E          | E          | E          | 12.4      | 12.4   | 12.4   | 3.72   | 3.72  | 3.72  | 3.72  | 3.72  | 3.72  |
| 7           | Walk through LAB | Open Door 10    | Open Door 10    | 0    | 0    | E    | E          | E          | E          | 14.8      | 14.8   | 14.8   | 16.95  | 16.95 | 16.95 | 16.95 | 16.95 | 16.95 |
| 8           | Reserve Target (Equipment) | Walk to Office G11 | Remove Target (Equipment) | 0    | 0    | E    | E          | E          | E          | 20.3      | 20.3   | 20.3   | 6.13   | 6.13  | 6.13  | 6.13  | 6.13  | 6.13  |
| 9           | Open Door 10    | 0                | E              | 36.5 | 36.5 | 36.5 | 16.95      | 16.95      | 16.95      | 36.5      | 36.5   | 36.5   | 16.95  | 16.95 | 16.95 | 16.95 | 16.95 | 16.95 |
| 10          | Reserve Target (Chemicals) | 0                | E              | 40    | 40    | 40    | 16.95      | 16.95      | 16.95      | 40    | 40     | 40     | 16.95  | 16.95 | 16.95 | 16.95 | 16.95 | 16.95 |

**Figure 4.111:** Theft evaluation result for pathways 1-2-3E.

**Figure 4.112:** Theft evaluation result for pathways 2-5-10E.
Figure 4.113: Theft evaluation result for pathways 3-7-9E.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD-1</th>
<th>PD-2</th>
<th>PD-3</th>
<th>Locations</th>
<th>Mean-1</th>
<th>Mean-2</th>
<th>Mean-3</th>
<th>Delay (in seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>11.1</td>
<td>11.1</td>
<td>5.33, 3.33, 3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>15</td>
<td>15</td>
<td>4.5, 4.5, 4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Outer Burglar Gate</td>
<td>Open Outer Burglar Gate</td>
<td>Break Window Glass</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>94</td>
<td>94</td>
<td>9, 9, 9, 9, 9, 9</td>
</tr>
<tr>
<td>4</td>
<td>Open Door 11</td>
<td>Open Door 11</td>
<td>Remove Inner Burglar Bars</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>56.5</td>
<td>56.5</td>
<td>89.1, 56.5, 56.5</td>
</tr>
<tr>
<td>5</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
<td>Jump into Room</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>159.8</td>
<td>159.8</td>
<td>183.3, 5.49, 5.49</td>
</tr>
<tr>
<td>6</td>
<td>Walk to G11</td>
<td>Walk to Door 4</td>
<td>Walk to Door 4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>92.2</td>
<td>92.2</td>
<td>2.78, 2.78, 2.78</td>
</tr>
<tr>
<td>7</td>
<td>Open Door 10</td>
<td>Walk to Office G11</td>
<td>Open Door 4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>56.5</td>
<td>56.5</td>
<td>148.5, 44.55, 44.55</td>
</tr>
<tr>
<td>8</td>
<td>Remove Target (Equipment)</td>
<td>Open Door 10</td>
<td>Walk to Door 6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>281.3</td>
<td>281.3</td>
<td>16.95, 16.95, 16.95</td>
</tr>
<tr>
<td>9</td>
<td>Remove Target (Equipment)</td>
<td>Open Door 6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>281.3</td>
<td>281.3</td>
<td>16.95, 16.95, 16.95</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Open Door 7</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>56.5</td>
<td>16.95, 16.95, 16.95</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Remove Target (Chemicals)</td>
<td>0</td>
<td>E</td>
<td>40</td>
<td>12</td>
<td>40</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 4.114: Theft evaluation result for pathways 4-5-6E.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Path 1</th>
<th>Path 2</th>
<th>Path 3</th>
<th>PD-1</th>
<th>PD-2</th>
<th>PD-3</th>
<th>Locations</th>
<th>Mean-1</th>
<th>Mean-2</th>
<th>Mean-3</th>
<th>Delay (in seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>11.1</td>
<td>11.1</td>
<td>5.33, 3.33, 3.33</td>
</tr>
<tr>
<td>2</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>15</td>
<td>15</td>
<td>4.5, 4.5, 4.5</td>
</tr>
<tr>
<td>3</td>
<td>Open Outer Burglar Gate</td>
<td>Open Outer Burglar Gate</td>
<td>Open Outer Burglar Gate</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>94</td>
<td>94</td>
<td>9, 9, 9, 9, 9, 9</td>
</tr>
<tr>
<td>4</td>
<td>Open Door 11</td>
<td>Open Door 9</td>
<td>Open Door 12</td>
<td>0.9</td>
<td>0.9</td>
<td>0.9</td>
<td>E</td>
<td>E</td>
<td>56.5</td>
<td>56.5</td>
<td>16.95, 16.95, 16.95</td>
</tr>
<tr>
<td>5</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>159.8</td>
<td>159.8</td>
<td>183.3, 5.49, 5.49</td>
</tr>
<tr>
<td>6</td>
<td>Walk through LAB</td>
<td>Open Door 8</td>
<td>Open Door 13</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>92.2</td>
<td>92.2</td>
<td>2.78, 2.78, 2.78</td>
</tr>
<tr>
<td>7</td>
<td>Remove Target (Equipment)</td>
<td>Open Door 7</td>
<td>Walk through LAB</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>281.3</td>
<td>281.3</td>
<td>16.95, 16.95, 16.95</td>
</tr>
<tr>
<td>8</td>
<td>Open Door 6</td>
<td>Remove Target (Equipment)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>E</td>
<td>E</td>
<td>281.3</td>
<td>281.3</td>
<td>16.95, 16.95, 16.95</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Open Door 5</td>
<td>0</td>
<td>E</td>
<td>56.5</td>
<td>56.5</td>
<td>16.95, 16.95, 16.95</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Remove Target (Computers)</td>
<td>0</td>
<td>E</td>
<td>40</td>
<td>12</td>
<td>40</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Figure 4. 115: Theft evaluation result for pathways 4-6-10E.

Figure 4. 116: Theft evaluation result for pathways 7-8-9E.
Tables 4.6 to 4.11 present the possible adversary paths identified for the three buildings, their probability of interruption values for sabotage and theft attack scenarios, probability of neutralization values and probability of effectiveness values for the study and the implementation of the PPS in the context of GTRI using the EASI code.

The detailed probability of neutralization values can be found in appendix D from figure D1 to D36.

Table 4. 6: Adversary paths and their $P_I$, $P_N$ and $P_E$ values for the proposed PPS design for building F2C using EASI (sabotage scenario)

<table>
<thead>
<tr>
<th>Adversary Paths</th>
<th>($P_I$) for Sabotage, Study</th>
<th>($P_N$) for Sabotage, Study</th>
<th>($P_E$) for System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path 1C</td>
<td>0.51</td>
<td>0.99</td>
<td>0.50</td>
</tr>
<tr>
<td>Path 2C</td>
<td>0.77</td>
<td>0.83</td>
<td>0.64</td>
</tr>
<tr>
<td>Path 3C</td>
<td>0.77</td>
<td>0.83</td>
<td>0.64</td>
</tr>
<tr>
<td>Path 4C</td>
<td>0.81</td>
<td>0.85</td>
<td>0.69</td>
</tr>
<tr>
<td>Path 5C</td>
<td>0.68</td>
<td>0.84</td>
<td>0.57</td>
</tr>
<tr>
<td>Path 6C</td>
<td>0.65</td>
<td>0.88</td>
<td>0.57</td>
</tr>
<tr>
<td>Path 7C</td>
<td>0.64</td>
<td>0.81</td>
<td>0.52</td>
</tr>
<tr>
<td>Path 8C</td>
<td>0.53</td>
<td>0.98</td>
<td>0.52</td>
</tr>
<tr>
<td>Path 9C</td>
<td>0.76</td>
<td>0.84</td>
<td>0.64</td>
</tr>
<tr>
<td>Path 10C</td>
<td>0.52</td>
<td>0.96</td>
<td>0.50</td>
</tr>
<tr>
<td>Path 11C</td>
<td>0.79</td>
<td>0.96</td>
<td>0.76</td>
</tr>
<tr>
<td>Path 13C</td>
<td>0.84</td>
<td>0.95</td>
<td>0.80</td>
</tr>
<tr>
<td>Path 14C</td>
<td>0.62</td>
<td>0.96</td>
<td>0.60</td>
</tr>
</tbody>
</table>
Table 4.7: Adversary paths and their $P_I$, $P_N$ and $P_E$ values of the proposed PPS design for building F2C using EASI (theft scenario)

<table>
<thead>
<tr>
<th>Adversary Paths</th>
<th>($P_I$) for Theft, Study</th>
<th>($P_N$) for Theft, Study</th>
<th>($P_E$) for System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path 1C</td>
<td>0.76</td>
<td>0.93</td>
<td>0.71</td>
</tr>
<tr>
<td>Path 2C</td>
<td>0.89</td>
<td>0.93</td>
<td>0.83</td>
</tr>
<tr>
<td>Path 3C</td>
<td>0.89</td>
<td>0.93</td>
<td>0.83</td>
</tr>
<tr>
<td>Path 4C</td>
<td>0.90</td>
<td>0.94</td>
<td>0.85</td>
</tr>
<tr>
<td>Path 5C</td>
<td>0.85</td>
<td>0.94</td>
<td>0.80</td>
</tr>
<tr>
<td>Path 6C</td>
<td>0.84</td>
<td>0.90</td>
<td>0.76</td>
</tr>
<tr>
<td>Path 7C</td>
<td>0.84</td>
<td>0.92</td>
<td>0.77</td>
</tr>
<tr>
<td>Path 8C</td>
<td>0.79</td>
<td>0.96</td>
<td>0.76</td>
</tr>
<tr>
<td>Path 9C</td>
<td>0.89</td>
<td>0.92</td>
<td>0.82</td>
</tr>
<tr>
<td>Path 10C</td>
<td>0.78</td>
<td>0.83</td>
<td>0.65</td>
</tr>
<tr>
<td>Path 11C</td>
<td>0.89</td>
<td>0.87</td>
<td>0.77</td>
</tr>
<tr>
<td>Path 12C</td>
<td>0.55</td>
<td>0.92</td>
<td>0.51</td>
</tr>
<tr>
<td>Path 13C</td>
<td>0.90</td>
<td>0.94</td>
<td>0.85</td>
</tr>
<tr>
<td>Path 14C</td>
<td>0.82</td>
<td>0.96</td>
<td>0.79</td>
</tr>
</tbody>
</table>
Table 4.8: Adversary paths and their $P_I$, $P_N$ and $P_E$ values of the implementation by GTRI for building F2C using EASI (sabotage scenario)

<table>
<thead>
<tr>
<th>Adversary Paths</th>
<th>($P_I$) for Sabotage, GTRI</th>
<th>($P_N$) for Sabotage, GTRI</th>
<th>($P_E$) for System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path 1C</td>
<td>0.01</td>
<td>0.99</td>
<td>0.01</td>
</tr>
<tr>
<td>Path 2C</td>
<td>0.01</td>
<td>0.83</td>
<td>0.01</td>
</tr>
<tr>
<td>Path 3C</td>
<td>0.01</td>
<td>0.83</td>
<td>0.01</td>
</tr>
<tr>
<td>Path 4C</td>
<td>0.01</td>
<td>0.85</td>
<td>0.01</td>
</tr>
<tr>
<td>Path 5C</td>
<td>0.01</td>
<td>0.84</td>
<td>0.01</td>
</tr>
<tr>
<td>Path 6C</td>
<td>0.01</td>
<td>0.88</td>
<td>0.01</td>
</tr>
<tr>
<td>Path 7C</td>
<td>0.01</td>
<td>0.81</td>
<td>0.01</td>
</tr>
<tr>
<td>Path 8C</td>
<td>0.01</td>
<td>0.98</td>
<td>0.01</td>
</tr>
<tr>
<td>Path 9C</td>
<td>0.01</td>
<td>0.84</td>
<td>0.01</td>
</tr>
<tr>
<td>Path 10C</td>
<td>0.01</td>
<td>0.96</td>
<td>0.01</td>
</tr>
<tr>
<td>Path 11C</td>
<td>0.52</td>
<td>0.96</td>
<td>0.50</td>
</tr>
<tr>
<td>Path 13C</td>
<td>0.01</td>
<td>0.95</td>
<td>0.01</td>
</tr>
<tr>
<td>Path 14C</td>
<td>0.01</td>
<td>0.96</td>
<td>0.01</td>
</tr>
</tbody>
</table>
Table 4.9: Adversary paths and their $P_I$, $P_N$ and $P_E$ values of the implementation by GTRI for building F2C using EASI (theft scenario)

<table>
<thead>
<tr>
<th>Adversary Paths</th>
<th>($P_I$) for Theft, GTRI</th>
<th>($P_N$) for Theft, GTRI</th>
<th>($P_E$) for System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path 1C</td>
<td>0.10</td>
<td>0.93</td>
<td>0.10</td>
</tr>
<tr>
<td>Path 2C</td>
<td>0.10</td>
<td>0.93</td>
<td>0.10</td>
</tr>
<tr>
<td>Path 3C</td>
<td>0.10</td>
<td>0.93</td>
<td>0.10</td>
</tr>
<tr>
<td>Path 4C</td>
<td>0.10</td>
<td>0.94</td>
<td>0.10</td>
</tr>
<tr>
<td>Path 5C</td>
<td>0.10</td>
<td>0.94</td>
<td>0.10</td>
</tr>
<tr>
<td>Path 6C</td>
<td>0.10</td>
<td>0.90</td>
<td>0.10</td>
</tr>
<tr>
<td>Path 7C</td>
<td>0.09</td>
<td>0.92</td>
<td>0.10</td>
</tr>
<tr>
<td>Path 8C</td>
<td>0.09</td>
<td>0.96</td>
<td>0.10</td>
</tr>
<tr>
<td>Path 9C</td>
<td>0.09</td>
<td>0.92</td>
<td>0.10</td>
</tr>
<tr>
<td>Path 10C</td>
<td>0.09</td>
<td>0.83</td>
<td>0.10</td>
</tr>
<tr>
<td>Path 11C</td>
<td>0.77</td>
<td>0.87</td>
<td>0.67</td>
</tr>
<tr>
<td>Path 12C</td>
<td>0.09</td>
<td>0.92</td>
<td>0.10</td>
</tr>
<tr>
<td>Path 13C</td>
<td>0.09</td>
<td>0.94</td>
<td>0.10</td>
</tr>
<tr>
<td>Path 14C</td>
<td>0.10</td>
<td>0.96</td>
<td>0.10</td>
</tr>
</tbody>
</table>
Table 4.10: Adversary paths and their $P_I$, $P_N$ and $P_E$ values of the proposed PPS design for building F2A using EASI (theft scenario)

<table>
<thead>
<tr>
<th>Adversary Paths</th>
<th>($P_I$) for Theft, Study</th>
<th>($P_N$) for Theft, Study</th>
<th>($P_E$) for System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path 1A</td>
<td>0.51</td>
<td>0.98</td>
<td>0.50</td>
</tr>
<tr>
<td>Path 2A</td>
<td>0.58</td>
<td>0.93</td>
<td>0.54</td>
</tr>
<tr>
<td>Path 3A</td>
<td>0.72</td>
<td>0.81</td>
<td>0.58</td>
</tr>
<tr>
<td>Path 4A</td>
<td>0.50</td>
<td>0.99</td>
<td>0.50</td>
</tr>
<tr>
<td>Path 5A</td>
<td>0.60</td>
<td>0.97</td>
<td>0.58</td>
</tr>
<tr>
<td>Path 6A</td>
<td>0.75</td>
<td>0.94</td>
<td>0.71</td>
</tr>
<tr>
<td>Path 7A</td>
<td>0.73</td>
<td>0.90</td>
<td>0.66</td>
</tr>
<tr>
<td>Path 8A</td>
<td>0.87</td>
<td>0.92</td>
<td>0.80</td>
</tr>
<tr>
<td>Path 9A</td>
<td>0.73</td>
<td>0.94</td>
<td>0.67</td>
</tr>
<tr>
<td>Path 10A</td>
<td>0.67</td>
<td>0.84</td>
<td>0.56</td>
</tr>
</tbody>
</table>

Table 4.11: Adversary paths and their $P_I$, $P_N$ and $P_E$ values of the proposed PPS design for building F2E using EASI (theft scenario)

<table>
<thead>
<tr>
<th>Adversary Paths</th>
<th>($P_I$) for Theft, Study</th>
<th>($P_N$) for Theft, Study</th>
<th>($P_E$) for System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path 1E</td>
<td>0.74</td>
<td>0.92</td>
<td>0.68</td>
</tr>
<tr>
<td>Path 2E</td>
<td>0.62</td>
<td>0.97</td>
<td>0.60</td>
</tr>
<tr>
<td>Path 3E</td>
<td>0.74</td>
<td>0.94</td>
<td>0.70</td>
</tr>
<tr>
<td>Path 4E</td>
<td>0.66</td>
<td>0.84</td>
<td>0.55</td>
</tr>
<tr>
<td>Path 5E</td>
<td>0.79</td>
<td>0.96</td>
<td>0.76</td>
</tr>
<tr>
<td>Path 6E</td>
<td>0.74</td>
<td>0.83</td>
<td>0.61</td>
</tr>
<tr>
<td>Path 7E</td>
<td>0.87</td>
<td>0.92</td>
<td>0.80</td>
</tr>
<tr>
<td>Path 8E</td>
<td>0.70</td>
<td>0.88</td>
<td>0.62</td>
</tr>
<tr>
<td>Path 9E</td>
<td>0.59</td>
<td>0.84</td>
<td>0.50</td>
</tr>
<tr>
<td>Path 10E</td>
<td>0.82</td>
<td>0.92</td>
<td>0.75</td>
</tr>
</tbody>
</table>
Tables 4.12 to 4.17 present the possible adversary paths identified for the three buildings, their probability of interruption values for sabotage and theft attack scenarios, probability of neutralization values and probability of effectiveness values for the study and the implementation of the PPS in the context of GTRI using EASIM code.

The detailed probability of neutralization values can be found in appendix D from figure D1 to D36.

Table 4.12: Multiple adversary pathways and their $P_I$, $P_N$ and $P_E$ values of the proposed PPS design for building F2C using EASIM (sabotage scenario)

<table>
<thead>
<tr>
<th>Multiple Adversary Pathways</th>
<th>$(P_I)$ for Sabotage, Study</th>
<th>$(P_N)$ for Sabotage, Study</th>
<th>$(P_E)$ for System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pathways 1-2-3C</td>
<td>0.69</td>
<td>0.88</td>
<td>0.61</td>
</tr>
<tr>
<td>Pathways 1-4-14C</td>
<td>0.63</td>
<td>0.93</td>
<td>0.59</td>
</tr>
<tr>
<td>Pathways 3-8-13C</td>
<td>0.72</td>
<td>0.92</td>
<td>0.66</td>
</tr>
<tr>
<td>Pathways 4-5-6C</td>
<td>0.71</td>
<td>0.86</td>
<td>0.61</td>
</tr>
<tr>
<td>Pathways 7-8-5C</td>
<td>0.62</td>
<td>0.88</td>
<td>0.55</td>
</tr>
<tr>
<td>Pathways 10-11-13C</td>
<td>0.72</td>
<td>0.96</td>
<td>0.69</td>
</tr>
</tbody>
</table>

Table 4.13: Multiple adversary pathways and their $P_I$, $P_N$ and $P_E$ values of the proposed PPS design for building F2C using EASIM (theft scenario)

<table>
<thead>
<tr>
<th>Multiple Adversary Pathways</th>
<th>$(P_I)$ for Theft, Study</th>
<th>$(P_N)$ for Theft, Study</th>
<th>$(P_E)$ for System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pathways 1-2-3C</td>
<td>0.85</td>
<td>0.93</td>
<td>0.80</td>
</tr>
<tr>
<td>Pathways 1-4-14C</td>
<td>0.81</td>
<td>0.94</td>
<td>0.76</td>
</tr>
<tr>
<td>Pathways 4-5-6C</td>
<td>0.86</td>
<td>0.93</td>
<td>0.80</td>
</tr>
<tr>
<td>Pathways 7-8-5C</td>
<td>0.83</td>
<td>0.94</td>
<td>0.78</td>
</tr>
<tr>
<td>Pathways 9-10-12C</td>
<td>0.75</td>
<td>0.89</td>
<td>0.67</td>
</tr>
<tr>
<td>Pathways 11-8-13C</td>
<td>0.86</td>
<td>0.92</td>
<td>0.79</td>
</tr>
</tbody>
</table>
Table 4.14: Multiple adversary pathways and their $P_I$, $P_N$ and $P_E$ values of the implementation by GTRI for building F2C using EASIM (sabotage scenario)

<table>
<thead>
<tr>
<th>Multiple Adversary Pathways</th>
<th>($P_I$) for Sabotage, GTRI</th>
<th>($P_N$) for Sabotage, GTRI</th>
<th>($P_E$) for System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pathways 1-2-3C</td>
<td>0.01</td>
<td>0.88</td>
<td>0.01</td>
</tr>
<tr>
<td>Pathways 1-4-14C</td>
<td>0.01</td>
<td>0.93</td>
<td>0.01</td>
</tr>
<tr>
<td>Pathways 3-8-13C</td>
<td>0.01</td>
<td>0.92</td>
<td>0.01</td>
</tr>
<tr>
<td>Pathways 4-5-6C</td>
<td>0.01</td>
<td>0.86</td>
<td>0.01</td>
</tr>
<tr>
<td>Pathways 7-8-5C</td>
<td>0.01</td>
<td>0.88</td>
<td>0.01</td>
</tr>
<tr>
<td>Pathways 10-11-13C</td>
<td>0.18</td>
<td>0.96</td>
<td>0.17</td>
</tr>
</tbody>
</table>

Table 4.15: Multiple adversary pathways and their $P_I$, $P_N$ and $P_E$ values of the implementation by GTRI for building F2C using EASIM (theft scenario)

<table>
<thead>
<tr>
<th>Multiple Adversary Pathways</th>
<th>($P_I$) for Theft, GTRI</th>
<th>($P_N$) for Theft, GTRI</th>
<th>($P_E$) for System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pathways 1-2-3C</td>
<td>0.10</td>
<td>0.93</td>
<td>0.10</td>
</tr>
<tr>
<td>Pathways 1-4-14C</td>
<td>0.10</td>
<td>0.94</td>
<td>0.10</td>
</tr>
<tr>
<td>Pathways 4-5-6C</td>
<td>0.10</td>
<td>0.93</td>
<td>0.10</td>
</tr>
<tr>
<td>Pathways 7-8-5C</td>
<td>0.10</td>
<td>0.94</td>
<td>0.10</td>
</tr>
<tr>
<td>Pathways 9-10-12C</td>
<td>0.10</td>
<td>0.89</td>
<td>0.10</td>
</tr>
<tr>
<td>Pathways 11-8-13C</td>
<td>0.31</td>
<td>0.92</td>
<td>0.29</td>
</tr>
</tbody>
</table>
Table 4.16: Multiple adversary pathways and their $P_I$, $P_N$ and $P_E$ values of the proposed PPS design for building F2A using EASIM (theft scenario)

<table>
<thead>
<tr>
<th>Multiple Adversary Pathways of F2A</th>
<th>$(P_I)$ for Theft, Study</th>
<th>$(P_N)$ for Theft, Study</th>
<th>$(P_E)$ for System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pathways 1-2-6A</td>
<td>0.61</td>
<td>0.95</td>
<td>0.58</td>
</tr>
<tr>
<td>Pathways 2-5-1A</td>
<td>0.56</td>
<td>0.96</td>
<td>0.54</td>
</tr>
<tr>
<td>Pathways 3-6-8A</td>
<td>0.79</td>
<td>0.89</td>
<td>0.70</td>
</tr>
<tr>
<td>Pathways 3-7-9A</td>
<td>0.74</td>
<td>0.88</td>
<td>0.65</td>
</tr>
<tr>
<td>Pathways 4-5-9A</td>
<td>0.61</td>
<td>0.97</td>
<td>0.59</td>
</tr>
<tr>
<td>Pathways 4-9-10A</td>
<td>0.63</td>
<td>0.92</td>
<td>0.58</td>
</tr>
</tbody>
</table>

Table 4.17: Multiple adversary pathways and their $P_I$, $P_N$ and $P_E$ values of the proposed PPS design for building F2E using EASIM (theft scenario)

<table>
<thead>
<tr>
<th>Multiple Adversary Pathways of F2E</th>
<th>$(P_I)$ for Theft, Study</th>
<th>$(P_N)$ for Theft, Study</th>
<th>$(P_E)$ for System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pathways 1-2-3E</td>
<td>0.71</td>
<td>0.94</td>
<td>0.67</td>
</tr>
<tr>
<td>Pathways 2-5-10E</td>
<td>0.74</td>
<td>0.95</td>
<td>0.70</td>
</tr>
<tr>
<td>Pathways 3-7-9E</td>
<td>0.67</td>
<td>0.90</td>
<td>0.60</td>
</tr>
<tr>
<td>Pathways 4-5-6E</td>
<td>0.72</td>
<td>0.88</td>
<td>0.63</td>
</tr>
<tr>
<td>Pathways 4-6-10E</td>
<td>0.74</td>
<td>0.86</td>
<td>0.64</td>
</tr>
<tr>
<td>Pathways 7-8-9E</td>
<td>0.72</td>
<td>0.88</td>
<td>0.63</td>
</tr>
</tbody>
</table>
Figures 4.117 to 4.124 show the evaluation results from the EASI and EASIM codes for the research’s RFT and a lower RFT of 300 seconds with standard deviation of 90 for the sabotage or theft attack scenarios for the study and the GTRI implementation to show the relevance of a quick response in a PPS.

Figure 4.117: Adversary paths and their $P_E$ values for a lower RFT using EASI – sabotage scenario for building F2C study and implementation by GTRI.

Figure 4.118: Adversary paths and their $P_E$ values for a lower RFT using EASI – theft scenario for building F2C study and implementation by GTRI.
Figure 4.119: Adversary paths and their $P_E$ values for a lower RFT using EASI – theft scenario for building F2A.

Figure 4.120: Adversary paths and their $P_E$ values for a lower RFT using EASI – theft scenario for building F2E.

164
Figure 4. 121: Adversary pathways and their $P_E$ values for a lower RFT using EASIM – sabotage scenario for building F2C study and implementation by GTRI.

Figure 4. 122: Adversary pathways and their $P_E$ values for a lower RFT using EASIM – theft scenario for building F2C study and implementation by GTRI.
Figure 4.123: Adversary pathways and their $P_E$ values for a lower RFT using EASIM – theft scenario for building F2A.

Figure 4.124: Adversary pathways and their $P_E$ values for a lower RFT using EASIM – theft scenario for building F2E.
CHAPTER 5 Discussions

This chapter presents the discussions of the results obtained in this research work.

5.1 Discussions of Results

This research was to ascertain the possibility of the existing PPS at the Centre for Applied Radiation Science and Technology of the North West University (Mafikeng Campus) to provide the necessary protection for the 444 TBq $^{60}$Co irradiation source and upgrade, redesign and evaluate for PPS effectiveness in accordance to the changing threats.

The use of radioactive sources comes with safety and security responsibilities, including protecting personnel, the public and the environment from unwarranted radiation exposure; preventing or reducing the risk of theft or sabotage of radioactive sources, nuclear facilities and associated activities in use, storage or in transport. In order to take up these responsibilities, adequate physical security is needed for the sources, facilities and activities. This research was particularly relevant in light of the infiltrations of the Pelindaba nuclear research facility outside Pretoria. These infiltrations occurred in 2005, 2007 and 2012. The crime rates in surrounding towns where the CARST facility is located are very high, and represent additional threats to the facility.

The schematic diagram in figure 3.5 gives details of the methodology undertaken for the research.

The vulnerability of the PPS was derived from the preliminary evaluation which resulted in the $P_E$ being 0 due to the fact that $P_1$ was also 0.

The risk assessment to the $^{60}$Co source was assessed. The results gave the A/D ratios to be 83 for the 2.5 TBq source and 14800 for the maximum activity of 444 TBq $^{60}$Co source. These ratios indicated the categories and the required security measures to be put in place.
A DBT was developed based on the threat assessment of the facility’s assets and radioactive sources.

The designs of the PPS for the three Buildings were then proposed. In designing the PPS, a performance-based design was considered. The detection, delay and response stages of the design, make use of various detection devices including CCTV Cameras, Balanced Magnetic Switches, Duress Buttons, and Dual Technology PIR/Doppler Microwave motion detector, Radiation Detector, Proximity Card Reader requiring PIN, Glass Break Sensors and Arm/Disarm Keypad. Delays include the use of Electric Strike Locks, Tamper Devices, High Security Padlocks, Exit Buttons, Security-Harden Doors and inner Burglar Bar Gates. Response consisted of communication devices like the conventional narrow-band frequency modulated (FM) and clear-voice radio systems, landlines, pagers, cellular phones, intercoms, hand signals, lights, whistles and spread-spectrum systems.

The devices used in the design were described and their functions explained in detail and administrative procedures governing the mode of operation of the Center was drafted to include certain requirements of employees to obtain good safety and security.

EASI and ASSESS codes were proposed for the evaluation of the PPS but by the time the study reached the evaluation stage, ASSESS was still not ready for release to African countries including South Africa. Therefore EASI and a new code EASIM was created from the EASI algorithm for evaluation of multiple paths simultaneously were used.

In this research, the risks associated with providing potential adversaries with the security information given in this thesis raises concern since this is an academic exercise and could be published in journals. On the other hand, the benefits of discussing the security arrangements so that other specialists can critique it and learn from it, outweighs the potential risks to telling the “bad guys” or potential adversaries how the security works.

The problems and limitations of this research were, the security company contracted by the global threat reduction initiative not putting in place early detection features, before or on
entrance doors of the Buildings in the Center. This will be recommended to be done for the security effectiveness to be achieved. The other limitation, is the unavailability of the ASSESS code which is an enhanced version of SAVI with additional insider attack analysis and neutralization modules. Assess could have analyzed the insider adversaries and how to neutralize such personnel.

Figure 5: 1: EASI $P_E$ values of the existed PPS, the proposed PPS and the GTRI implementation for building F2C.

Figure 5.1 represents the probability of effectiveness values for the existing PPS, sabotage and theft scenarios for the proposed PPS and the GTRI implementation of Building F2C. The EASI evaluation for the existing PPS gave a $P_E$ of 0 for all identified paths. This result indicates that, the existing system was unable to successfully interrupt and neutralize any attack on the facility. The implementation by the GTRI resulted in $P_E$ values ranging from 0.01 – 0.50 for sabotage attacks and 0.09 – 0.77 for theft attacks. This means that, for 13 paths of sabotage and theft, the system cannot successfully interrupt and neutralize an attack. The system will only have a chance of 9% - 10% of effectiveness but 50% success for sabotage attack and 77% success for theft attack for the remaining path.
The $P_E$ values for the proposed PPS ranges from 0.50 – 0.80 for sabotage and 0.51 – 0.85 for theft. This signifies the system’s success of 50% - 80% interrupting and neutralizing a sabotage attack and a 51% - 85% against a theft attack. It should be noted that, these ranges of success are for specific path at a time.

Figure 5.2 above shows the EASI $P_E$ evaluation results for theft attacks for the existing PPS and the proposed PPS of Buildings F2A and F2E. Both buildings had $P_E$ value of 0 for the existed PPS which indicates no chance of interrupting and neutralizing an attack on the facility at all identified 10 paths. $P_E$ values for the proposed PPS of the two Buildings again ranges from 0.50 – 0.80 given the system successful interruption and neutralization at 50% – 80%. This means on any of the individual identified paths, the system’s effectiveness against threats or attacks falls in the percentage bracket.
Figure 5.3 illustrates the $P_E$ values resulting from the EASIM code for the existed PPS together with the sabotage and theft attack scenarios of the proposed PSS and the GTRI implementation for Building F2C. As indicated in the EASI code, the EASIM code also gave a PE value of 0 for the existed PPS as a result of the absence of detection elements on the possible identified paths of Building F2C. This result means the system cannot be effective in interrupting and neutralizing any attack be it sabotage or theft.

For the implementation in the context of the PPS by the GTRI, $P_E$ values ranges from 0.01 – 0.17 for sabotage attack scenarios and 0.10 – 0.29 for theft attack scenarios. This is indicative of the fact that, the system has a chance of 1% – 17% interruption and neutralization success against sabotage attack scenarios and 10% – 29% success against theft attack scenarios. This ranges of multiple paths of three at the same time.

PE values for the proposed PPS ranges from 0.55 – 0.69 for sabotage attack scenarios and 0.67 – 0.80 for theft attack scenarios. This suggests that, in an event an attack in respect to sabotage occurs, the system is able to interrupt and neutralize the attack before the adversary succeeds by 55% – 69% and 67% – 80% in respect to theft occurring. These results from the EASIM code are
success of effectiveness against a threat or attack for multiple paths i.e., three paths at the same time.

Figure 5.4 demonstrates the EASIM’s $P_E$ values for both the existed PPS and the proposed PPS for Buildings F2A and F2E. Again, the $P_E$ value for the existed PPS was 0 for both Buildings indicating the lack of detection features, sufficient delays and a quick response. The $P_E$ values of Building F2A ranges from 0.54 – 0.70 against theft attack scenarios giving the system the capability to interrupt and neutralize these attacks by 54% – 70%. Building F2E’s $P_E$ values on the hand ranges from 0.60 – 0.70 against theft attack scenarios enabling the system to interrupt and neutralize at 60% – 70%.

The results from both the EASI and EASIM codes for the three Buildings, show significant increase in the probability of effectiveness for the new proposed PPS compared to the existed PPS $P_E$ of 0. On the other hand, the results for the implementation in the context of the PPS by the Global Threat Reduction Initiative for sabotage and theft scenarios of Building F2C, however show marginal increase in the $P_E$ values compared to the existed PPS $P_E$ of 0. This was a result of lack of early detection on the adversary paths, little delay tasks for adversaries to overcome and detection too close to the target.
The EASIM code evaluates three paths simultaneously and therefore, each path contributes to the overall result depending on early detection, sufficient delays and quicker response.

Some of the lessons in evaluating physical protection systems with security models or computer codes, emphasized detection as a vital feature in the evaluation. Because the PPS works collectively with detection, delay and response, the models and codes do not function well on only delay and response. Another lesson learnt, was the fact that, after early detection and sufficient delays in the paths of adversary, a quicker response adds to the overall security effectiveness. This is shown in figures 4.117 to 4.124, where bar charts represent probability of effectiveness values with the RFT of the research and a lower RFT. It was evident that, the lower RFT’s $P_E$ values were higher.

This research could have been done better if the analytical system and software for evaluating safeguards and security code which is an enhanced version of the System Analysis of Vulnerability to Intrusion with additional insider attack analysis and neutralization modules was available for the evaluations. This would have analyzed the insider adversaries and how to neutralize such personnel.

Future work needs to be done on the proposed design, such as conducting vulnerability assessment of the PPS and identify the weak links or vulnerabilities of the system. These vulnerabilities should be corrected by upgrading the PSS. This process is essential since adversaries are a step ahead, finding weak links of systems to attack, and also threat changes as technology advances and with the trend of technology advances, security measures should change with respect to the change in identified threat.
CHAPTER 6 Conclusions and Recommendations

This chapter presents the conclusions drawn from the research, along with appropriate recommendations to the management of the Centre for Applied Radiation Science and Technology of the North-West University (Mafikeng Campus), South Africa.

6.1 Conclusions

A new physical protection system was designed and proposed for the Centre for Applied Radiation Science and Technology at the North-West University, Mafikeng Campus. The design resulted from first establishing the basis for such a design. The Center has acquired a $^{60}$Co irradiation source from the iThemba Laboratories in South Africa to be used for research. The source is to be used for sterilization of medical equipment, preservation of food items and irradiating municipal waste for the production of fertilizers. The Center also houses equipment worth millions of South African Rands which need to be secured against unauthorized access or removal.

A Risk Assessment of the Center and the risk due to the $^{60}$Co irradiation source were undertaken to ascertain the security measures needed. A graded approach was used in the design so that the risk received its corresponding security measures.

An integrated system of detection, delay and response was proposed for the new PPS. The proposed PPS was then evaluated with the Estimate of Adversary Sequence Interruption code for the measurement of effectiveness, as well as the Estimation of Adversary Sequence Interruption for Multiple Pathways code with respect to simultaneous, multiple attacks. The evaluations were done for the existed PPS and the proposed designed PPS for 14 potential adversary paths inside Building F2C, 10 paths inside Building F2A and 10 paths inside Building F2E. An evaluation was also undertaken for the PPS implementation based on the Global Threat Reduction Initiative for 14 paths inside Building F2C using EASI. Similar evaluations were done for the existed PPS and the proposed designed PPS for 6 pathways inside Building F2C, 6 pathways inside Building F2A and 6 pathways inside Building F2E. An evaluation was also done for the PPS
implementation based on the Global Threat Reduction Initiative for the 6 pathways inside Building F2C using EASIM.

The overall effectiveness of the proposed PPS for the paths increased from zero (0) to a minimum of 0.50 and a maximum of 0.80 for sabotage scenario for Building F2C and a minimum of 0.50 and a maximum of 0.85 for theft scenario for Buildings F2C, F2A and F2E using the EASI evaluation code. The EASIM code’s results increased from zero (0) to a minimum of 0.55 and a maximum of 0.69 for sabotage scenario for Building F2C and a minimum of 0.54 and a maximum of 0.80 for theft scenario for Buildings F2C, F2A and F2E increasing the overall effectiveness of the PPS of the Center and therefore adversaries can be interrupted and neutralized in the course of their attack by as high as 80% effectiveness.

6.2 Recommendations

1. An effective PPS has early detection, substantial delay for the adversary after detection and a quick response. It is recommended that the Center or the GTRI team take steps to do the following:

   ❖ Add detection features before or on entrance doors and the windows of Building F2C. This will serve as early detection for various adversary paths.

   ❖ Add enough delay tasks after detection in all pathways, especially installing an inner burglar gate A between doors D5 and D6 leading to the 2.5 TBq $^{60}$Co source room in Building F2C. Inner burglar gates should also be installed after all entrance doors for Building F2E, door D7 of Building F2A, doors D3 and D1 of Building F2C. An outer burglar gate should also be installed in front of door D1 of Building F2A.

   ❖ Management of the Center together with the GTRI team should implement all the elements proposed in the PPS of Buildings F2A and F2E since the only implementation was for Building F2C which was inadequate to perform the three principles of an effective PPS, early detection, sufficient delay tasks on the path of adversaries and a quick response.
2. For faster responses to any security incident, management should take steps to relocate the control room for the intrusion detection system from the security office to a convenient location where response can be swifter. This recommendation arises from the results presented on the bar charts of figures 4.117 to 4.124, where a lower RFT used in the evaluation in both EASI and EASIM resulted in higher probability of effectiveness values.
REFERENCES


42. Kim, J., K., (South Korea’s ambassador to India, writing on the eve of the Seoul NSS). (2012). Beyond security towards peace. Times of India. India.


76. Ithemba Laboratory, National Research Fund of South Africa, (2013). Transfer document of the Eldorado 78 Therapy Head to North-West University Mafikeng Campus.


### APPENDICES

Table A1: Recommended Categorization of Sources used in Practices [44].

<table>
<thead>
<tr>
<th>Category</th>
<th>Practices</th>
<th>Activity Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Radioisotope thermoelectric generators (RTGs)</td>
<td>A/D ≥ 1000</td>
</tr>
<tr>
<td></td>
<td>Irradiators</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Teletherapy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fixed, multi-beam teletherapy (gamma knife)</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Industrial gamma radiography</td>
<td>1000 &gt; A/D ≥ 10</td>
</tr>
<tr>
<td></td>
<td>High/medium dose rate brachytherapy</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Fixed industrial gauges</td>
<td>10 &gt; A/D ≥ 1</td>
</tr>
<tr>
<td></td>
<td>Level gauges</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dredger gauges</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Conveyor gauges containing high activity sources</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spinning pipe gauges</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Well logging gauges</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Low dose rate brachytherapy (except eye plaques and permanent implant sources)</td>
<td>1 &gt; A/D ≥ 0.01</td>
</tr>
<tr>
<td></td>
<td>Thickness/fill-level gauges</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Portable gauges (e.g. moisture/density gauges)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bone densitometers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Static eliminators</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Low dose rate brachytherapy eye plaques and permanent implant sources</td>
<td>0.01 &gt; A/D ≥ Exempt/D [94].</td>
</tr>
<tr>
<td></td>
<td>X-ray fluorescence devices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Electron capture devices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mossbauer spectrometry</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Positron Emission Tomography (PET) checking</td>
<td></td>
</tr>
</tbody>
</table>
Table A2: Recommended Security Levels for Common Practices [27].

<table>
<thead>
<tr>
<th>Practices</th>
<th>Activity Ratio</th>
<th>Security Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radioisotope thermoelectric generators (RTGs)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Irradiators</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Teletherapy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fixed, multi-beam teletherapy (gamma knife)</td>
<td>$A/D \geq 1000$</td>
<td>A</td>
</tr>
<tr>
<td>Industrial gamma radiography</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High/medium dose rate brachytherapy</td>
<td>$1000 &gt; A/D \geq 10$</td>
<td>B</td>
</tr>
<tr>
<td>Fixed industrial gauges</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level gauges</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dredger gauges</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conveyor gauges containing high activity sources</td>
<td>$10 &gt; A/D \geq 1$</td>
<td>C</td>
</tr>
<tr>
<td>Spinning pipe gauges</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Well logging gauges</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low dose rate brachytherapy (except eye plaques and permanent implant sources)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thickness/fill-level gauges</td>
<td>$1 &gt; A/D \geq 0.01$</td>
<td></td>
</tr>
<tr>
<td>Portable gauges (e.g. moisture/density gauges)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bone densitometers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Static eliminators</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low dose rate brachytherapy eye plaques and permanent implant sources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X-ray fluorescence devices</td>
<td>$0.01 &gt; A/D \geq$ Exempt/D [94].</td>
<td></td>
</tr>
<tr>
<td>Electron capture devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mossbauer spectrometry</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Positron Emission Tomography (PET) checking</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Apply measures as described in the Basic Safety Standards [94].
<table>
<thead>
<tr>
<th>GOALS</th>
<th>SECURITY LEVEL A</th>
<th>SECURITY LEVEL B</th>
<th>SECURITY LEVEL C</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Prevent unauthorized removal of the radioactive material</td>
<td>Minimize the likelihood of unauthorized removal of radioactive material</td>
<td>Reduce the likelihood of unauthorized removal of radioactive material</td>
</tr>
<tr>
<td></td>
<td>Provide immediate detection of any attempted unauthorized removal of the</td>
<td>Provide detection of any attempted unauthorized removal of the radioactive</td>
<td>Provide detection of unauthorized removal of the radioactive material</td>
</tr>
<tr>
<td></td>
<td>radioactive material by an insider or outsider adversary</td>
<td>material</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Provide immediate assessment of detection</td>
<td>Provide immediate communication to the response force</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Provide immediate assessment of detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Provide immediate communication to the response force</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Provide immediate communication to the response force</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Provide a means to detect loss of material through verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delay</td>
<td>Provide delay after detection sufficient for the response team to interrupt the</td>
<td>Provide delay to minimize the likelihood of unauthorized removal</td>
<td>Provide delay to reduce the likelihood of unauthorized removal</td>
</tr>
<tr>
<td></td>
<td>unauthorized removal</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Response</td>
<td>Provide immediate response to assessed alarm with sufficient resources to</td>
<td>Provide immediate initiation of response to interrupt the unauthorized removal</td>
<td>Implement appropriate actions in the event of unauthorized removal</td>
</tr>
<tr>
<td></td>
<td>interrupt and prevent the unauthorized removal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Provide access controls to material locations that effectively restrict access to</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>authorized persons only</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ensure trustworthiness of authorized personnel</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identify and protect sensitive information</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Provide a security plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ensure a capability to manage security events covered by security contingency</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Establish a security event reporting system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Applicable Occupational dose limit</td>
<td>Public dose limit applicable to persons other than employees</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Effective dose</strong></td>
<td>20 mSv per annum, averaged over five years and not more than 50 mSv in any one year</td>
<td>1 mSv per annum</td>
<td></td>
</tr>
<tr>
<td><strong>Annual equivalent dose to the</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eye</td>
<td>150 mSv</td>
<td>15 mSv</td>
<td></td>
</tr>
<tr>
<td>skin</td>
<td>500 mSv</td>
<td>50 mSv</td>
<td></td>
</tr>
<tr>
<td>hands and feet</td>
<td>500 mSv</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>
Table B1: Mean and Standard Deviation Values for Response Force Times (RFT) in seconds.

<table>
<thead>
<tr>
<th>X</th>
<th>$x_i - x_{avg}$</th>
<th>X</th>
<th>$x_i - x_{avg}$</th>
<th>X</th>
<th>$x_i - x_{avg}$</th>
<th>X</th>
<th>$x_i - x_{avg}$</th>
<th>X</th>
<th>$x_i - x_{avg}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>241</td>
<td>-180.2</td>
<td>771</td>
<td>292.8</td>
<td>243</td>
<td>-209.6</td>
<td>666</td>
<td>185.2</td>
<td>415</td>
<td>-44.4</td>
</tr>
<tr>
<td>659</td>
<td>237.8</td>
<td>543</td>
<td>64.8</td>
<td>710</td>
<td>257.4</td>
<td>354</td>
<td>-126.8</td>
<td>277</td>
<td>-182.4</td>
</tr>
<tr>
<td>300</td>
<td>-121.2</td>
<td>420</td>
<td>-58.2</td>
<td>534</td>
<td>81.4</td>
<td>481</td>
<td>0</td>
<td>362</td>
<td>-97.4</td>
</tr>
<tr>
<td>421</td>
<td>-0.2</td>
<td>302</td>
<td>-176.2</td>
<td>358</td>
<td>-94.6</td>
<td>605</td>
<td>124.2</td>
<td>567</td>
<td>107.6</td>
</tr>
<tr>
<td>485</td>
<td>63.8</td>
<td>355</td>
<td>-123.2</td>
<td>418</td>
<td>-34.6</td>
<td>298</td>
<td>-182.8</td>
<td>676</td>
<td>216.6</td>
</tr>
<tr>
<td>421.2</td>
<td>164.15</td>
<td>478.2</td>
<td>186.78</td>
<td>452.6</td>
<td>178.16</td>
<td>480.8</td>
<td>157.50</td>
<td>459.4</td>
<td>160.64</td>
</tr>
<tr>
<td>424</td>
<td>-59.2</td>
<td>709</td>
<td>200.8</td>
<td>477</td>
<td>55.6</td>
<td>588</td>
<td>71.4</td>
<td>399</td>
<td>-119.6</td>
</tr>
<tr>
<td>650</td>
<td>166.8</td>
<td>544</td>
<td>35.8</td>
<td>410</td>
<td>-11.4</td>
<td>551</td>
<td>34.4</td>
<td>343</td>
<td>-175.6</td>
</tr>
<tr>
<td>483.2</td>
<td>120.17</td>
<td>508.2</td>
<td>133.58</td>
<td>421.4</td>
<td>128.61</td>
<td>516.6</td>
<td>129.04</td>
<td>518.6</td>
<td>196.99</td>
</tr>
<tr>
<td>360</td>
<td>-56.8</td>
<td>599</td>
<td>47.6</td>
<td>663</td>
<td>109</td>
<td>367</td>
<td>168.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>465</td>
<td>48.2</td>
<td>480</td>
<td>71.4</td>
<td>547</td>
<td>7</td>
<td>620</td>
<td>84.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>294</td>
<td>-122.8</td>
<td>533</td>
<td>-18.4</td>
<td>382</td>
<td>-172</td>
<td>778</td>
<td>242.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>398</td>
<td>-18.8</td>
<td>425</td>
<td>-126.4</td>
<td>497</td>
<td>-57</td>
<td>429</td>
<td>-106.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>567</td>
<td>150.2</td>
<td>720</td>
<td>168.6</td>
<td>681</td>
<td>127</td>
<td>485</td>
<td>50.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>416.8</td>
<td>104.33</td>
<td>551.4</td>
<td>114.13</td>
<td>554</td>
<td>123.38</td>
<td>535.8</td>
<td>164.49</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers. Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B2: Mean and Standard Deviation Values for Delay Times (T_{Delay}) in seconds – Jump Fence

<table>
<thead>
<tr>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>-0.4</td>
<td>15</td>
<td>3.8</td>
<td>13</td>
<td>0</td>
<td>11</td>
<td>0.8</td>
<td>16</td>
<td>2.2</td>
<td>11</td>
<td>1.2</td>
<td>7</td>
<td>-4</td>
</tr>
<tr>
<td>13</td>
<td>0.6</td>
<td>8</td>
<td>-3.2</td>
<td>15</td>
<td>2</td>
<td>9</td>
<td>-1.2</td>
<td>8</td>
<td>-5.8</td>
<td>5</td>
<td>-4.8</td>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>4.6</td>
<td>10</td>
<td>-1.2</td>
<td>9</td>
<td>-4</td>
<td>14</td>
<td>3.8</td>
<td>13</td>
<td>-0.8</td>
<td>11</td>
<td>1.2</td>
<td>15</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>-3.4</td>
<td>14</td>
<td>2.8</td>
<td>17</td>
<td>4</td>
<td>7</td>
<td>-3.2</td>
<td>15</td>
<td>1.2</td>
<td>9</td>
<td>-0.8</td>
<td>9</td>
<td>-2</td>
</tr>
<tr>
<td>11</td>
<td>-1.4</td>
<td>9</td>
<td>-2.2</td>
<td>11</td>
<td>-2</td>
<td>10</td>
<td>-0.2</td>
<td>17</td>
<td>3.2</td>
<td>13</td>
<td>3.2</td>
<td>13</td>
<td>2</td>
</tr>
<tr>
<td>12.4</td>
<td>2.97</td>
<td>11.2</td>
<td>3.11</td>
<td>13</td>
<td>3.16</td>
<td>10.2</td>
<td>2.59</td>
<td>13.8</td>
<td>3.56</td>
<td>9.8</td>
<td>3.03</td>
<td>11</td>
<td>3.16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>-3.8</td>
<td>10</td>
<td>0.4</td>
<td>11</td>
<td>-1</td>
<td>10</td>
<td>-0.8</td>
<td>12</td>
<td>0.8</td>
<td>15</td>
<td>4.8</td>
<td>14</td>
<td>3</td>
</tr>
<tr>
<td>13</td>
<td>2.2</td>
<td>11</td>
<td>1.4</td>
<td>16</td>
<td>4</td>
<td>13</td>
<td>2.2</td>
<td>14</td>
<td>2.8</td>
<td>5</td>
<td>-5.2</td>
<td>10</td>
<td>-1</td>
</tr>
<tr>
<td>15</td>
<td>4.2</td>
<td>7</td>
<td>-2.6</td>
<td>8</td>
<td>-4</td>
<td>9</td>
<td>-1.8</td>
<td>8</td>
<td>-3.2</td>
<td>14</td>
<td>3.8</td>
<td>8</td>
<td>-3</td>
</tr>
<tr>
<td>9</td>
<td>-1.8</td>
<td>14</td>
<td>4.4</td>
<td>10</td>
<td>-2</td>
<td>14</td>
<td>3.2</td>
<td>15</td>
<td>3.8</td>
<td>11</td>
<td>0.8</td>
<td>17</td>
<td>6</td>
</tr>
<tr>
<td>10</td>
<td>-0.8</td>
<td>6</td>
<td>-3.6</td>
<td>15</td>
<td>3</td>
<td>8</td>
<td>-2.8</td>
<td>7</td>
<td>-4.2</td>
<td>6</td>
<td>-4.2</td>
<td>6</td>
<td>-5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>2.4</td>
<td>9</td>
<td>-1.6</td>
<td>15</td>
<td>5</td>
<td>15</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>-2.6</td>
<td>14</td>
<td>3.4</td>
<td>8</td>
<td>-2</td>
<td>10</td>
<td>-1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>4.4</td>
<td>11</td>
<td>0.4</td>
<td>6</td>
<td>-4</td>
<td>8</td>
<td>-3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>-3.6</td>
<td>7</td>
<td>-3.6</td>
<td>11</td>
<td>1</td>
<td>15</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>-0.6</td>
<td>12</td>
<td>1.4</td>
<td>10</td>
<td>0</td>
<td>7</td>
<td>-4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.6</td>
<td>3.36</td>
<td>10.6</td>
<td>2.70</td>
<td>10</td>
<td>3.39</td>
<td>11</td>
<td>3.81</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

|                 |                 |                 |                 |
|                 |                 |                 |                 |
| 11.10          | 3.33            |

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers
Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B3: Mean and Standard Deviation Values for Delay Times (T\textsubscript{Delay}) in seconds – Run to Building

<table>
<thead>
<tr>
<th>x</th>
<th>x\textsubscript{i} – x\textsubscript{avg} x</th>
<th>x\textsubscript{i} – x\textsubscript{avg} x</th>
<th>x\textsubscript{i} – x\textsubscript{avg} x</th>
<th>x\textsubscript{i} – x\textsubscript{avg} x</th>
<th>x\textsubscript{i} – x\textsubscript{avg} x</th>
<th>x\textsubscript{i} – x\textsubscript{avg} x</th>
<th>x\textsubscript{i} – x\textsubscript{avg} x</th>
<th>x\textsubscript{i} – x\textsubscript{avg} x</th>
<th>x\textsubscript{i} – x\textsubscript{avg} x</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>-2</td>
<td>15</td>
<td>1.4</td>
<td>13</td>
<td>-1.8</td>
<td>19</td>
<td>4.4</td>
<td>16</td>
<td>0.2</td>
</tr>
<tr>
<td>15</td>
<td>1</td>
<td>7</td>
<td>-6.6</td>
<td>15</td>
<td>0.2</td>
<td>16</td>
<td>1.4</td>
<td>9</td>
<td>-6.8</td>
</tr>
<tr>
<td>21</td>
<td>7</td>
<td>13</td>
<td>-0.6</td>
<td>21</td>
<td>6.2</td>
<td>14</td>
<td>-0.6</td>
<td>20</td>
<td>4.2</td>
</tr>
<tr>
<td>9</td>
<td>-5</td>
<td>19</td>
<td>5.4</td>
<td>17</td>
<td>2.2</td>
<td>6</td>
<td>-8.6</td>
<td>15</td>
<td>-0.8</td>
</tr>
<tr>
<td>13</td>
<td>-1</td>
<td>14</td>
<td>0.4</td>
<td>8</td>
<td>-6.8</td>
<td>18</td>
<td>3.4</td>
<td>19</td>
<td>3.2</td>
</tr>
<tr>
<td>14</td>
<td><strong>4.47</strong></td>
<td><strong>13.6</strong></td>
<td><strong>4.34</strong></td>
<td><strong>14.8</strong></td>
<td><strong>4.82</strong></td>
<td><strong>14.6</strong></td>
<td><strong>5.18</strong></td>
<td><strong>15.8</strong></td>
<td><strong>4.32</strong></td>
</tr>
<tr>
<td>18</td>
<td>3.8</td>
<td>19</td>
<td>4.2</td>
<td>14</td>
<td>-1.2</td>
<td>20</td>
<td>5.6</td>
<td>20</td>
<td>3.6</td>
</tr>
<tr>
<td>10</td>
<td>-4.2</td>
<td>17</td>
<td>2.2</td>
<td>20</td>
<td>4.8</td>
<td>13</td>
<td>-1.4</td>
<td>15</td>
<td>-1.4</td>
</tr>
<tr>
<td>16</td>
<td>1.8</td>
<td>7</td>
<td>-7.8</td>
<td>9</td>
<td>-6.2</td>
<td>16</td>
<td>1.6</td>
<td>9</td>
<td>-7.4</td>
</tr>
<tr>
<td>17</td>
<td>2.8</td>
<td>14</td>
<td>-0.8</td>
<td>17</td>
<td>1.8</td>
<td>14</td>
<td>-0.4</td>
<td>21</td>
<td>4.6</td>
</tr>
<tr>
<td>10</td>
<td>-4.2</td>
<td>16</td>
<td>1.2</td>
<td>16</td>
<td>0.8</td>
<td>9</td>
<td>-5.4</td>
<td>17</td>
<td>0.6</td>
</tr>
<tr>
<td>14.2</td>
<td><strong>3.90</strong></td>
<td><strong>14.6</strong></td>
<td><strong>4.62</strong></td>
<td><strong>15.2</strong></td>
<td><strong>4.09</strong></td>
<td><strong>14.4</strong></td>
<td><strong>4.04</strong></td>
<td><strong>16.4</strong></td>
<td><strong>4.77</strong></td>
</tr>
<tr>
<td>13</td>
<td>-2.8</td>
<td>17</td>
<td>1.2</td>
<td>17</td>
<td>1.4</td>
<td>21</td>
<td>7.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>5.2</td>
<td>20</td>
<td>4.2</td>
<td>8</td>
<td>-7.6</td>
<td>9</td>
<td>-4.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>3.2</td>
<td>14</td>
<td>-1.8</td>
<td>13</td>
<td>-2.6</td>
<td>11</td>
<td>-2.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>-6.8</td>
<td>13</td>
<td>-2.8</td>
<td>19</td>
<td>3.4</td>
<td>7</td>
<td>-6.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>1.2</td>
<td>15</td>
<td>-0.8</td>
<td>21</td>
<td>5.4</td>
<td>18</td>
<td>4.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>15.8</strong></td>
<td><strong>4.82</strong></td>
<td><strong>15.8</strong></td>
<td><strong>2.77</strong></td>
<td><strong>15.6</strong></td>
<td><strong>5.18</strong></td>
<td><strong>13.2</strong></td>
<td><strong>6.02</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 15.00 | 4.50 |

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers. Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B4: Mean and Standard Deviation Values for Delay Times ($T_{\text{Delay}}$) in seconds – Run to Control Area

<table>
<thead>
<tr>
<th>X</th>
<th>x - x_avg</th>
<th>X</th>
<th>x - x_avg</th>
<th>X</th>
<th>x - x_avg</th>
<th>X</th>
<th>x - x_avg</th>
<th>X</th>
<th>x - x_avg</th>
<th>X</th>
<th>x - x_avg</th>
<th>X</th>
<th>x - x_avg</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>-1</td>
<td>8</td>
<td>0.6</td>
<td>10</td>
<td>2</td>
<td>11</td>
<td>3.8</td>
<td>10</td>
<td>2.2</td>
<td>6</td>
<td>-1</td>
<td>9</td>
<td>0.8</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>6</td>
<td>-1.4</td>
<td>6</td>
<td>-2</td>
<td>5</td>
<td>-2.2</td>
<td>9</td>
<td>1.2</td>
<td>7</td>
<td>0</td>
<td>6</td>
<td>-2.2</td>
</tr>
<tr>
<td>4</td>
<td>-3</td>
<td>9</td>
<td>1.6</td>
<td>7</td>
<td>-1</td>
<td>5</td>
<td>-2.2</td>
<td>8</td>
<td>0.2</td>
<td>9</td>
<td>2</td>
<td>11</td>
<td>2.8</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>10</td>
<td>2.6</td>
<td>8</td>
<td>0</td>
<td>8</td>
<td>0.8</td>
<td>7</td>
<td>-0.8</td>
<td>8</td>
<td>1</td>
<td>5</td>
<td>-3.2</td>
</tr>
<tr>
<td>10</td>
<td>3</td>
<td>4</td>
<td>-3.4</td>
<td>9</td>
<td>1</td>
<td>7</td>
<td>-0.2</td>
<td>5</td>
<td>-2.8</td>
<td>5</td>
<td>-2</td>
<td>10</td>
<td>1.8</td>
</tr>
<tr>
<td>7</td>
<td>2.24</td>
<td>7.4</td>
<td>2.41</td>
<td>8</td>
<td>1.58</td>
<td>7.2</td>
<td>2.49</td>
<td>7.8</td>
<td>1.92</td>
<td>7</td>
<td>1.58</td>
<td>8.2</td>
<td>2.59</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>X</th>
<th>x - x_avg</th>
<th>X</th>
<th>x - x_avg</th>
<th>X</th>
<th>x - x_avg</th>
<th>X</th>
<th>x - x_avg</th>
<th>X</th>
<th>x - x_avg</th>
<th>X</th>
<th>x - x_avg</th>
<th>X</th>
<th>x - x_avg</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>1.4</td>
<td>11</td>
<td>3.6</td>
<td>10</td>
<td>2.4</td>
<td>7</td>
<td>0</td>
<td>11</td>
<td>3.6</td>
<td>7</td>
<td>-0.4</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>-1.6</td>
<td>7</td>
<td>-0.4</td>
<td>6</td>
<td>-1.6</td>
<td>6</td>
<td>-1</td>
<td>7</td>
<td>-0.4</td>
<td>9</td>
<td>1.6</td>
<td>7</td>
<td>-1</td>
</tr>
<tr>
<td>5</td>
<td>-2.6</td>
<td>6</td>
<td>-1.4</td>
<td>8</td>
<td>0.4</td>
<td>8</td>
<td>1</td>
<td>4</td>
<td>-3.4</td>
<td>5</td>
<td>-2.4</td>
<td>7</td>
<td>-1</td>
</tr>
<tr>
<td>11</td>
<td>3.4</td>
<td>9</td>
<td>1.6</td>
<td>9</td>
<td>1.4</td>
<td>4</td>
<td>-3</td>
<td>6</td>
<td>-1.4</td>
<td>6</td>
<td>-1.4</td>
<td>6</td>
<td>-2</td>
</tr>
<tr>
<td>7</td>
<td>-0.6</td>
<td>4</td>
<td>-3.4</td>
<td>5</td>
<td>-2.6</td>
<td>10</td>
<td>3</td>
<td>9</td>
<td>1.6</td>
<td>10</td>
<td>2.6</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>7.6</td>
<td>2.41</td>
<td>7.4</td>
<td>2.70</td>
<td>7.6</td>
<td>2.07</td>
<td>7</td>
<td>2.24</td>
<td>7.4</td>
<td>2.70</td>
<td>7.4</td>
<td>2.07</td>
<td>8</td>
<td>1.87</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>X</th>
<th>x - x_avg</th>
<th>X</th>
<th>x - x_avg</th>
<th>X</th>
<th>x - x_avg</th>
<th>X</th>
<th>x - x_avg</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>2.8</td>
<td>9</td>
<td>1</td>
<td>10</td>
<td>2.8</td>
<td>7</td>
<td>-1.2</td>
</tr>
<tr>
<td>6</td>
<td>-2.2</td>
<td>6</td>
<td>-2</td>
<td>9</td>
<td>1.8</td>
<td>5</td>
<td>-3.2</td>
</tr>
<tr>
<td>9</td>
<td>0.8</td>
<td>8</td>
<td>0</td>
<td>4</td>
<td>-3.2</td>
<td>9</td>
<td>0.8</td>
</tr>
<tr>
<td>7</td>
<td>-1.2</td>
<td>12</td>
<td>4</td>
<td>5</td>
<td>-2.2</td>
<td>12</td>
<td>3.8</td>
</tr>
<tr>
<td>8</td>
<td>-0.2</td>
<td>5</td>
<td>-3</td>
<td>8</td>
<td>0.8</td>
<td>8</td>
<td>-0.2</td>
</tr>
<tr>
<td>8.2</td>
<td>1.92</td>
<td>8</td>
<td>2.74</td>
<td>7.2</td>
<td>2.59</td>
<td>8.2</td>
<td>2.59</td>
</tr>
</tbody>
</table>

| 7.60 | 2.28 |

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers. Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B5: Mean and Standard Deviation Values for Delay Times ($T_{delay}$) in seconds – Enter Wash Rooms

<table>
<thead>
<tr>
<th>x</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{avg}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>-0.8</td>
<td>8</td>
<td>2.6</td>
<td>4</td>
<td>-1.4</td>
<td>4</td>
<td>-2.2</td>
<td>4</td>
<td>-2.2</td>
<td>9</td>
<td>2.4</td>
</tr>
<tr>
<td>6</td>
<td>0.2</td>
<td>5</td>
<td>-0.4</td>
<td>8</td>
<td>2.6</td>
<td>4</td>
<td>-0.2</td>
<td>6</td>
<td>-0.2</td>
<td>6</td>
<td>-2.6</td>
</tr>
<tr>
<td>4</td>
<td>-1.8</td>
<td>6</td>
<td>0.6</td>
<td>4</td>
<td>-1.4</td>
<td>9</td>
<td>2.8</td>
<td>7</td>
<td>0.8</td>
<td>8</td>
<td>1.4</td>
</tr>
<tr>
<td>9</td>
<td>3.2</td>
<td>4</td>
<td>-1.4</td>
<td>5</td>
<td>-0.4</td>
<td>7</td>
<td>0.8</td>
<td>9</td>
<td>2.8</td>
<td>5</td>
<td>-1.6</td>
</tr>
</tbody>
</table>

| 5.8 | 1.92 | 5.4 | 1.67 | 5.4 | 1.67 | 6.2 | 1.92 | 6.2 | 1.92 | 6.6 | 2.07 | 6.6 | 1.95 | 5.4 | 2.19 |

<table>
<thead>
<tr>
<th>x</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{avg}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>-1.2</td>
<td>6</td>
<td>-0.2</td>
<td>8</td>
<td>1.6</td>
<td>7</td>
<td>1.4</td>
<td>7</td>
<td>1.2</td>
<td>6</td>
<td>0.4</td>
</tr>
<tr>
<td>8</td>
<td>1.8</td>
<td>7</td>
<td>0.8</td>
<td>9</td>
<td>2.6</td>
<td>4</td>
<td>-1.6</td>
<td>8</td>
<td>2.2</td>
<td>8</td>
<td>2.4</td>
</tr>
<tr>
<td>7</td>
<td>0.8</td>
<td>6</td>
<td>-0.2</td>
<td>4</td>
<td>-2.4</td>
<td>5</td>
<td>-0.6</td>
<td>6</td>
<td>0.2</td>
<td>6</td>
<td>0.4</td>
</tr>
<tr>
<td>4</td>
<td>-2.2</td>
<td>8</td>
<td>1.8</td>
<td>6</td>
<td>-0.4</td>
<td>4</td>
<td>-1.6</td>
<td>4</td>
<td>-1.8</td>
<td>4</td>
<td>-1.6</td>
</tr>
<tr>
<td>7</td>
<td>0.8</td>
<td>4</td>
<td>-2.2</td>
<td>5</td>
<td>-1.4</td>
<td>8</td>
<td>2.4</td>
<td>4</td>
<td>-1.8</td>
<td>4</td>
<td>-1.6</td>
</tr>
</tbody>
</table>

| 6.2 | 1.64 | 6.2 | 1.48 | 6.4 | 2.07 | 5.6 | 1.82 | 5.8 | 1.79 | 5.6 | 1.67 | 6.4 | 1.82 | 5.6 | 1.52 |

<table>
<thead>
<tr>
<th>x</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{avg}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>1.2</td>
<td>9</td>
<td>3</td>
<td>7</td>
<td>1.2</td>
<td>6</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>-0.8</td>
<td>5</td>
<td>-1</td>
<td>4</td>
<td>-1.8</td>
<td>4</td>
<td>-2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0.2</td>
<td>7</td>
<td>1</td>
<td>1</td>
<td>1.2</td>
<td>7</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>2.2</td>
<td>4</td>
<td>-2</td>
<td>6</td>
<td>0.2</td>
<td>5</td>
<td>-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>-2.8</td>
<td>5</td>
<td>-1</td>
<td>5</td>
<td>-0.8</td>
<td>8</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.8</td>
<td>1.92</td>
<td>6</td>
<td>2.00</td>
<td>5.8</td>
<td>1.30</td>
<td>6</td>
<td>1.58</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers. Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B6: Mean and Standard Deviation Values for Delay Times ($T_{\text{Delay}}$) in seconds – Jump into Room

<table>
<thead>
<tr>
<th>X</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>X</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>X</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>X</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>X</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>X</th>
<th>$x_i - \bar{x}_{avg}$</th>
<th>X</th>
<th>$x_i - \bar{x}_{avg}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>-7.6</td>
<td>13</td>
<td>-5.6</td>
<td>20</td>
<td>1.4</td>
<td>27</td>
<td>8.8</td>
<td>25</td>
<td>6.4</td>
<td>25</td>
<td>4.6</td>
<td>14</td>
<td>-4.8</td>
</tr>
<tr>
<td>22</td>
<td>4.4</td>
<td>21</td>
<td>2.4</td>
<td>14</td>
<td>-4.6</td>
<td>11</td>
<td>-7.2</td>
<td>12</td>
<td>-6.6</td>
<td>20</td>
<td>-0.4</td>
<td>20</td>
<td>1.2</td>
</tr>
<tr>
<td>13</td>
<td>-4.6</td>
<td>24</td>
<td>5.4</td>
<td>18</td>
<td>-0.6</td>
<td>19</td>
<td>0.8</td>
<td>20</td>
<td>1.4</td>
<td>18</td>
<td>-2.4</td>
<td>15</td>
<td>-3.8</td>
</tr>
<tr>
<td>18</td>
<td>0.4</td>
<td>12</td>
<td>-6.6</td>
<td>15</td>
<td>-3.6</td>
<td>12</td>
<td>-6.2</td>
<td>17</td>
<td>-1.6</td>
<td>24</td>
<td>3.6</td>
<td>19</td>
<td>0.2</td>
</tr>
<tr>
<td>25</td>
<td>7.4</td>
<td>23</td>
<td>4.4</td>
<td>26</td>
<td>7.4</td>
<td>22</td>
<td>3.8</td>
<td>19</td>
<td>0.4</td>
<td>15</td>
<td>-5.4</td>
<td>26</td>
<td>7.2</td>
</tr>
<tr>
<td>17.6</td>
<td>6.19</td>
<td>18.6</td>
<td>5.68</td>
<td>18.6</td>
<td>4.77</td>
<td>18.2</td>
<td>6.76</td>
<td>18.6</td>
<td>4.72</td>
<td>20.4</td>
<td>4.16</td>
<td>18.8</td>
<td>4.76</td>
</tr>
<tr>
<td>18</td>
<td>-0.4</td>
<td>24</td>
<td>4.8</td>
<td>14</td>
<td>-4.2</td>
<td>20</td>
<td>3.4</td>
<td>20</td>
<td>3.8</td>
<td>21</td>
<td>2.8</td>
<td>11</td>
<td>-5</td>
</tr>
<tr>
<td>10</td>
<td>-8.4</td>
<td>18</td>
<td>-1.2</td>
<td>25</td>
<td>6.8</td>
<td>10</td>
<td>-6.6</td>
<td>10</td>
<td>-6.2</td>
<td>11</td>
<td>-7.2</td>
<td>26</td>
<td>10</td>
</tr>
<tr>
<td>25</td>
<td>6.6</td>
<td>20</td>
<td>0.8</td>
<td>19</td>
<td>0.8</td>
<td>18</td>
<td>1.4</td>
<td>11</td>
<td>-5.2</td>
<td>25</td>
<td>6.8</td>
<td>15</td>
<td>-1</td>
</tr>
<tr>
<td>19</td>
<td>0.6</td>
<td>11</td>
<td>-8.2</td>
<td>10</td>
<td>-8.2</td>
<td>23</td>
<td>6.4</td>
<td>21</td>
<td>4.8</td>
<td>20</td>
<td>1.8</td>
<td>17</td>
<td>1</td>
</tr>
<tr>
<td>20</td>
<td>1.6</td>
<td>23</td>
<td>3.8</td>
<td>23</td>
<td>4.8</td>
<td>12</td>
<td>-4.6</td>
<td>19</td>
<td>2.8</td>
<td>14</td>
<td>-4.2</td>
<td>11</td>
<td>-5</td>
</tr>
<tr>
<td>18.4</td>
<td>5.41</td>
<td>19.2</td>
<td>5.17</td>
<td>18.2</td>
<td>6.22</td>
<td>16.6</td>
<td>5.46</td>
<td>16.2</td>
<td>5.26</td>
<td>18.2</td>
<td>5.63</td>
<td>16</td>
<td>6.16</td>
</tr>
<tr>
<td>24</td>
<td>5.2</td>
<td>17</td>
<td>-3.4</td>
<td>16</td>
<td>-2.8</td>
<td>21</td>
<td>1.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>2.2</td>
<td>23</td>
<td>2.6</td>
<td>25</td>
<td>6.2</td>
<td>17</td>
<td>-2.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>1.2</td>
<td>26</td>
<td>5.6</td>
<td>12</td>
<td>-6.8</td>
<td>9</td>
<td>-10.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>-8.8</td>
<td>12</td>
<td>-8.4</td>
<td>18</td>
<td>-0.8</td>
<td>26</td>
<td>6.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>0.2</td>
<td>24</td>
<td>3.6</td>
<td>23</td>
<td>4.2</td>
<td>23</td>
<td>3.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18.8</td>
<td>5.26</td>
<td>20.4</td>
<td>5.77</td>
<td>18.8</td>
<td>5.26</td>
<td>19.2</td>
<td>6.57</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>18.30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5.49</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers. Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B7: Mean and Standard Deviation Values for Delay Times ($T_{\text{Delay}}$) in seconds – Walk through Maze

<table>
<thead>
<tr>
<th>x</th>
<th>$x_i - \overline{x}_{\text{avg}}$ x</th>
<th>$x_i - \overline{x}_{\text{avg}}$ x</th>
<th>$x_i - \overline{x}_{\text{avg}}$ x</th>
<th>$x_i - \overline{x}_{\text{avg}}$ x</th>
<th>$x_i - \overline{x}_{\text{avg}}$ x</th>
<th>$x_i - \overline{x}_{\text{avg}}$ x</th>
<th>$x_i - \overline{x}_{\text{avg}}$ x</th>
<th>$x_i - \overline{x}_{\text{avg}}$ x</th>
<th>$x_i - \overline{x}_{\text{avg}}$ x</th>
<th>$x_i - \overline{x}_{\text{avg}}$ x</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>-2</td>
<td>15</td>
<td>4</td>
<td>15</td>
<td>2.2</td>
<td>12</td>
<td>2</td>
<td>15</td>
<td>1.4</td>
<td>11</td>
</tr>
<tr>
<td>14</td>
<td>2</td>
<td>8</td>
<td>-3</td>
<td>7</td>
<td>-5.8</td>
<td>8</td>
<td>-2</td>
<td>8</td>
<td>-5.6</td>
<td>9</td>
</tr>
<tr>
<td>15</td>
<td>3</td>
<td>10</td>
<td>-1</td>
<td>9</td>
<td>-3.8</td>
<td>14</td>
<td>4</td>
<td>9</td>
<td>-4.6</td>
<td>11</td>
</tr>
<tr>
<td>9</td>
<td>-3</td>
<td>7</td>
<td>-4</td>
<td>11</td>
<td>-1.8</td>
<td>7</td>
<td>-3</td>
<td>10</td>
<td>-3.6</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>-4</td>
<td>11</td>
<td>0</td>
<td>10</td>
<td>-2.8</td>
<td>12</td>
<td>2</td>
<td>9</td>
<td>-4.6</td>
<td>12</td>
</tr>
<tr>
<td><strong>11.2</strong></td>
<td><strong>3.11</strong></td>
<td><strong>10.2</strong></td>
<td><strong>3.11</strong></td>
<td><strong>10.4</strong></td>
<td><strong>2.97</strong></td>
<td><strong>10.6</strong></td>
<td><strong>2.97</strong></td>
<td><strong>10.2</strong></td>
<td><strong>2.77</strong></td>
<td><strong>10</strong></td>
</tr>
<tr>
<td>x</td>
<td>$x_i - \overline{x}_{\text{avg}}$ x</td>
<td>$x_i - \overline{x}_{\text{avg}}$ x</td>
<td>$x_i - \overline{x}_{\text{avg}}$ x</td>
<td>$x_i - \overline{x}_{\text{avg}}$ x</td>
<td>$x_i - \overline{x}_{\text{avg}}$ x</td>
<td>$x_i - \overline{x}_{\text{avg}}$ x</td>
<td>$x_i - \overline{x}_{\text{avg}}$ x</td>
<td>$x_i - \overline{x}_{\text{avg}}$ x</td>
<td>$x_i - \overline{x}_{\text{avg}}$ x</td>
<td>$x_i - \overline{x}_{\text{avg}}$ x</td>
</tr>
<tr>
<td>8</td>
<td>-2.2</td>
<td>12</td>
<td><strong>2.4</strong></td>
<td>14</td>
<td>1.8</td>
<td>12</td>
<td>1.8</td>
<td>13</td>
<td>3.2</td>
<td>14</td>
</tr>
<tr>
<td>13</td>
<td>2.8</td>
<td>11</td>
<td><strong>1.4</strong></td>
<td>5</td>
<td>-7.2</td>
<td>13</td>
<td>2.8</td>
<td>8</td>
<td>-1.8</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>-3.2</td>
<td>7</td>
<td><strong>-2.6</strong></td>
<td>9</td>
<td>-3.2</td>
<td>10</td>
<td>-0.2</td>
<td>9</td>
<td>-0.8</td>
<td>13</td>
</tr>
<tr>
<td>9</td>
<td>-1.2</td>
<td>9</td>
<td><strong>-0.6</strong></td>
<td>12</td>
<td>-0.2</td>
<td>14</td>
<td>3.8</td>
<td>13</td>
<td>3.2</td>
<td>9</td>
</tr>
<tr>
<td>6</td>
<td>-4.2</td>
<td>14</td>
<td><strong>4.4</strong></td>
<td>15</td>
<td>2.8</td>
<td>8</td>
<td>-2.2</td>
<td>6</td>
<td>-3.8</td>
<td>6</td>
</tr>
<tr>
<td><strong>8.6</strong></td>
<td><strong>2.70</strong></td>
<td><strong>10.6</strong></td>
<td><strong>2.70</strong></td>
<td><strong>11</strong></td>
<td><strong>4.06</strong></td>
<td><strong>11.4</strong></td>
<td><strong>2.41</strong></td>
<td><strong>9.8</strong></td>
<td><strong>3.11</strong></td>
<td><strong>10</strong></td>
</tr>
<tr>
<td>x</td>
<td>$x_i - \overline{x}_{\text{avg}}$ x</td>
<td>$x_i - \overline{x}_{\text{avg}}$ x</td>
<td>$x_i - \overline{x}_{\text{avg}}$ x</td>
<td>$x_i - \overline{x}_{\text{avg}}$ x</td>
<td>$x_i - \overline{x}_{\text{avg}}$ x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>1.8</td>
<td>8</td>
<td>-1.6</td>
<td>7</td>
<td>-3.2</td>
<td>11</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>2.8</td>
<td>6</td>
<td>-3.6</td>
<td>13</td>
<td>2.8</td>
<td>8</td>
<td>-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>-2.2</td>
<td>11</td>
<td>1.4</td>
<td>6</td>
<td>-4.2</td>
<td>10</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>3.8</td>
<td>9</td>
<td>-0.6</td>
<td>15</td>
<td>4.8</td>
<td>15</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>-6.2</td>
<td>14</td>
<td>4.4</td>
<td>10</td>
<td>-0.2</td>
<td>6</td>
<td>-4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>11.2</strong></td>
<td><strong>4.15</strong></td>
<td><strong>9.6</strong></td>
<td><strong>3.05</strong></td>
<td><strong>10.2</strong></td>
<td><strong>3.83</strong></td>
<td><strong>10</strong></td>
<td><strong>3.39</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>10.30</strong></td>
<td><strong>3.09</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers. Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B8: Mean and Standard Deviation Values for Delay Times (T_{delay}) in seconds – Break Window Glass

<table>
<thead>
<tr>
<th>x</th>
<th>x_{i \text{--}} x_{\text{avg}}</th>
<th>x</th>
<th>x_{i \text{--}} x_{\text{avg}}</th>
<th>x</th>
<th>x_{i \text{--}} x_{\text{avg}}</th>
<th>x</th>
<th>x_{i \text{--}} x_{\text{avg}}</th>
<th>x</th>
<th>x_{i \text{--}} x_{\text{avg}}</th>
<th>x</th>
<th>x_{i \text{--}} x_{\text{avg}}</th>
</tr>
</thead>
<tbody>
<tr>
<td>42</td>
<td>12.6</td>
<td>29</td>
<td>2.8</td>
<td>29</td>
<td>-3.4</td>
<td>26</td>
<td>-5.6</td>
<td>22</td>
<td>-7.8</td>
<td>35</td>
<td>3.6</td>
</tr>
<tr>
<td>33</td>
<td>3.6</td>
<td>39</td>
<td>12.8</td>
<td>45</td>
<td>12.6</td>
<td>44</td>
<td>12.4</td>
<td>41</td>
<td>11.2</td>
<td>18</td>
<td>-13.4</td>
</tr>
<tr>
<td>25</td>
<td>-4.4</td>
<td>18</td>
<td>-8.2</td>
<td>28</td>
<td>-4.4</td>
<td>37</td>
<td>5.4</td>
<td>29</td>
<td>-0.8</td>
<td>28</td>
<td>-3.4</td>
</tr>
<tr>
<td>24</td>
<td>-5.4</td>
<td>20</td>
<td>-6.2</td>
<td>36</td>
<td>3.6</td>
<td>28</td>
<td>-3.6</td>
<td>37</td>
<td>7.2</td>
<td>34</td>
<td>2.6</td>
</tr>
<tr>
<td>23</td>
<td>-6.4</td>
<td>25</td>
<td>-1.2</td>
<td>24</td>
<td>-8.4</td>
<td>23</td>
<td>-8.6</td>
<td>20</td>
<td>-9.8</td>
<td>42</td>
<td>10.6</td>
</tr>
</tbody>
</table>

29.4 \text{minimum} \ 8.08 \text{average} \ 8.35 \text{standard deviation} \ 8.26 \text{minimum} \ 8.68 \text{average} \ 31.6 \text{maximum} \ 8.99 \text{standard deviation} \ 32.2 \text{minimum} \ 8.44 \text{average} \ 31.6 \text{maximum} \ 8.47 \text{standard deviation}

<table>
<thead>
<tr>
<th>x</th>
<th>x_{i \text{--}} x_{\text{avg}}</th>
<th>x</th>
<th>x_{i \text{--}} x_{\text{avg}}</th>
<th>x</th>
<th>x_{i \text{--}} x_{\text{avg}}</th>
<th>x</th>
<th>x_{i \text{--}} x_{\text{avg}}</th>
<th>x</th>
<th>x_{i \text{--}} x_{\text{avg}}</th>
<th>x</th>
<th>x_{i \text{--}} x_{\text{avg}}</th>
</tr>
</thead>
<tbody>
<tr>
<td>38</td>
<td>7.4</td>
<td>20</td>
<td>-8</td>
<td>35</td>
<td>3.4</td>
<td>21</td>
<td>-9.6</td>
<td>20</td>
<td>-10.6</td>
<td>20</td>
<td>-7.4</td>
</tr>
<tr>
<td>28</td>
<td>-2.6</td>
<td>38</td>
<td>10</td>
<td>21</td>
<td>-10.6</td>
<td>39</td>
<td>8.4</td>
<td>29</td>
<td>-1.6</td>
<td>37</td>
<td>9.6</td>
</tr>
<tr>
<td>26</td>
<td>-4.6</td>
<td>40</td>
<td>12</td>
<td>36</td>
<td>4.4</td>
<td>29</td>
<td>-1.6</td>
<td>25</td>
<td>-5.6</td>
<td>26</td>
<td>-1.4</td>
</tr>
<tr>
<td>19</td>
<td>-11.6</td>
<td>17</td>
<td>-11</td>
<td>24</td>
<td>-7.6</td>
<td>23</td>
<td>-7.6</td>
<td>40</td>
<td>9.4</td>
<td>18</td>
<td>-9.4</td>
</tr>
<tr>
<td>42</td>
<td>11.4</td>
<td>25</td>
<td>-3</td>
<td>42</td>
<td>10.4</td>
<td>41</td>
<td>10.4</td>
<td>39</td>
<td>8.4</td>
<td>36</td>
<td>8.6</td>
</tr>
</tbody>
</table>

30.6 \text{minimum} \ 9.32 \text{average} \ 10.46 \text{standard deviation} \ 8.79 \text{minimum} \ 9.10 \text{average} \ 30.6 \text{maximum} \ 8.73 \text{standard deviation} \ 27.4 \text{minimum} \ 8.82 \text{average} \ 29.8 \text{maximum} \ 8.29 \text{standard deviation} \ 29 \text{minimum} \ 8.94 \text{standard deviation}

<table>
<thead>
<tr>
<th>x</th>
<th>x_{i \text{--}} x_{\text{avg}}</th>
<th>x</th>
<th>x_{i \text{--}} x_{\text{avg}}</th>
<th>x</th>
<th>x_{i \text{--}} x_{\text{avg}}</th>
<th>x</th>
<th>x_{i \text{--}} x_{\text{avg}}</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>-5.2</td>
<td>39</td>
<td>10.2</td>
<td>18</td>
<td>-11</td>
<td>18</td>
<td>-14.8</td>
</tr>
<tr>
<td>37</td>
<td>9.8</td>
<td>19</td>
<td>-9.8</td>
<td>29</td>
<td>0</td>
<td>37</td>
<td>4.2</td>
</tr>
<tr>
<td>20</td>
<td>-7.2</td>
<td>26</td>
<td>-2.8</td>
<td>44</td>
<td>15</td>
<td>28</td>
<td>-4.8</td>
</tr>
<tr>
<td>18</td>
<td>-9.2</td>
<td>39</td>
<td>10.2</td>
<td>25</td>
<td>-4</td>
<td>37</td>
<td>4.2</td>
</tr>
<tr>
<td>39</td>
<td>11.8</td>
<td>21</td>
<td>-7.8</td>
<td>29</td>
<td>0</td>
<td>44</td>
<td>11.2</td>
</tr>
</tbody>
</table>

27.2 \text{minimum} \ 9.98 \text{average} \ 9.65 \text{standard deviation} \ 9.51 \text{minimum} \ 32.8 \text{average} \ 10.03 \text{standard deviation}

30.00 \text{maximum} \ 9.00 \text{minimum}

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers

Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B9: Mean and Standard Deviation Values for Delay Times ($T_{\text{Delay}}$) in seconds – Walk to Offices

<table>
<thead>
<tr>
<th>$x_i$</th>
<th>$x_{i-} X_{\text{avg}}$</th>
<th>$x_{i-} X_{\text{avg}}$</th>
<th>$x_{i-} X_{\text{avg}}$</th>
<th>$x_{i-} X_{\text{avg}}$</th>
<th>$x_{i-} X_{\text{avg}}$</th>
<th>$x_{i-} X_{\text{avg}}$</th>
<th>$x_{i-} X_{\text{avg}}$</th>
<th>$x_{i-} X_{\text{avg}}$</th>
<th>$x_{i-} X_{\text{avg}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>2.2</td>
<td>12</td>
<td>3.2</td>
<td>11</td>
<td>2.2</td>
<td>10</td>
<td>1.2</td>
<td>13</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>-3.8</td>
<td>5</td>
<td>-3.8</td>
<td>7</td>
<td>-1.8</td>
<td>8</td>
<td>-0.8</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>4.2</td>
<td>11</td>
<td>2.2</td>
<td>6</td>
<td>-2.8</td>
<td>9</td>
<td>0.2</td>
<td>7</td>
<td>-3</td>
</tr>
<tr>
<td>8</td>
<td>-0.8</td>
<td>7</td>
<td>-1.8</td>
<td>8</td>
<td>-0.8</td>
<td>5</td>
<td>-3.8</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>-1.8</td>
<td>9</td>
<td>0.2</td>
<td>12</td>
<td>3.2</td>
<td>12</td>
<td>3.2</td>
<td>9</td>
<td>-1</td>
</tr>
</tbody>
</table>

| 8.8   | **3.19**       | 8.8            | **2.86**       | 8.8            | **2.59**       | 8.8            | **2.59**       | 10             | **2.24**       |
|       |                |                |                |                |                |                |                |                |                |

| 8     | -1             | 12             | 1.6            | 11             | 2              | 12             | 3              | 10             | 1              |
| 10    | 1              | 13             | 2.6            | 8              | -1             | 8              | -1             | 5              | -3.8           |
| 12    | 3              | 7              | -3.4           | 6              | -3             | 6              | -3             | 12             | 3              |
| 9     | 0              | 11             | 0.6            | 13             | 4              | 8              | -1             | 6              | -3             |
| 6     | -3             | 9              | -1.4           | 7              | -2             | 11             | 2              | 9              | 0              |
| 9     | **2.24**       | **10.4**       | **2.41**       | **9**          | **2.92**       | **9**          | **2.45**       | **9**          | **2.24**       |
|       |                |                |                |                |                |                |                |                |                |

| 13    | 2              | 9              | -0.6           | 7              | -2.2           | 13             | 3.2            |
| 9     | -2             | 7              | -2.6           | 11             | 1.8            | 8              | -1.8           |
| 8     | -3             | 12             | 2.4            | 6              | -3.2           | 12             | 2.2            |
| 14    | 3              | 7              | -2.6           | 13             | 3.8            | 9              | -0.8           |
| 11    | 0              | 13             | 3.4            | 9              | -0.2           | 7              | -2.8           |
| 11    | **2.55**       | **9.6**        | **2.79**       | **9.2**        | **2.86**       | **9.8**        | **2.59**       |

| 11    | **2.55**       | **9.6**        | **2.79**       | **9.2**        | **2.86**       | **9.8**        | **2.59**       |
|       |                |                |                |                |                |                |                |

| NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers |
| Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final |
| Standard Deviation for the entire distribution. |

200
Table B10: Mean and Standard Deviation Values for Delay Times ($T_{\text{Delay}}$) in seconds – Walk through LAB

<table>
<thead>
<tr>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>-3.8</td>
<td>15</td>
<td>3</td>
<td>12</td>
<td>0</td>
<td>12</td>
<td>-0.2</td>
<td>16</td>
<td>3.4</td>
<td>14</td>
<td>1.2</td>
<td>12</td>
<td>-0.2</td>
</tr>
<tr>
<td>15</td>
<td>3.2</td>
<td>8</td>
<td>-4</td>
<td>7</td>
<td>-5</td>
<td>7</td>
<td>-5.2</td>
<td>9</td>
<td>-3.6</td>
<td>15</td>
<td>2.2</td>
<td>11</td>
<td>-1.2</td>
</tr>
<tr>
<td>13</td>
<td>1.2</td>
<td>16</td>
<td>4</td>
<td>16</td>
<td>4</td>
<td>10</td>
<td>-2.2</td>
<td>15</td>
<td>2.4</td>
<td>16</td>
<td>3.2</td>
<td>17</td>
<td>4.8</td>
</tr>
<tr>
<td>9</td>
<td>-2.8</td>
<td>7</td>
<td>-5</td>
<td>15</td>
<td>3</td>
<td>17</td>
<td>4.8</td>
<td>9</td>
<td>-3.6</td>
<td>7</td>
<td>-5.8</td>
<td>13</td>
<td>0.8</td>
</tr>
<tr>
<td>14</td>
<td>2.2</td>
<td>14</td>
<td>2</td>
<td>10</td>
<td>-2</td>
<td>15</td>
<td>2.8</td>
<td>14</td>
<td>1.4</td>
<td>12</td>
<td>-0.8</td>
<td>8</td>
<td>-4.2</td>
</tr>
<tr>
<td>11.8</td>
<td>3.11</td>
<td>12</td>
<td>4.18</td>
<td>12</td>
<td>3.67</td>
<td>12.2</td>
<td>3.96</td>
<td>12.6</td>
<td>3.36</td>
<td>12.8</td>
<td>3.56</td>
<td>12.2</td>
<td>3.27</td>
</tr>
<tr>
<td>18</td>
<td>4.8</td>
<td>12</td>
<td>-0.2</td>
<td>13</td>
<td>0.2</td>
<td>12</td>
<td>-0.8</td>
<td>11</td>
<td>-1</td>
<td>9</td>
<td>-1.8</td>
<td>14</td>
<td>-0.4</td>
</tr>
<tr>
<td>9</td>
<td>-4.2</td>
<td>13</td>
<td>0.8</td>
<td>17</td>
<td>4.2</td>
<td>16</td>
<td>3.2</td>
<td>17</td>
<td>5</td>
<td>15</td>
<td>4.2</td>
<td>18</td>
<td>3.6</td>
</tr>
<tr>
<td>12</td>
<td>-1.2</td>
<td>7</td>
<td>-5.2</td>
<td>15</td>
<td>2.2</td>
<td>7</td>
<td>-5.8</td>
<td>12</td>
<td>0</td>
<td>12</td>
<td>1.2</td>
<td>15</td>
<td>0.6</td>
</tr>
<tr>
<td>11</td>
<td>-2.2</td>
<td>15</td>
<td>2.8</td>
<td>12</td>
<td>-0.8</td>
<td>18</td>
<td>5.2</td>
<td>7</td>
<td>-5</td>
<td>8</td>
<td>-2.8</td>
<td>9</td>
<td>-5.4</td>
</tr>
<tr>
<td>16</td>
<td>2.8</td>
<td>14</td>
<td>1.8</td>
<td>7</td>
<td>-5.8</td>
<td>11</td>
<td>-1.8</td>
<td>13</td>
<td>1</td>
<td>10</td>
<td>-0.8</td>
<td>16</td>
<td>1.6</td>
</tr>
<tr>
<td>13.2</td>
<td>3.70</td>
<td>12.2</td>
<td>3.11</td>
<td>12.8</td>
<td>3.77</td>
<td>12.8</td>
<td>4.32</td>
<td>12</td>
<td>3.61</td>
<td>10.8</td>
<td>2.77</td>
<td>14.4</td>
<td>3.36</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>9</td>
<td>-3.2</td>
<td>7</td>
<td>-6</td>
<td>6</td>
<td>-6.6</td>
<td>12</td>
<td>4.36</td>
<td>12.2</td>
<td>2.59</td>
<td>13</td>
<td>5.24</td>
</tr>
<tr>
<td>12</td>
<td>4.36</td>
<td>12.2</td>
<td>2.59</td>
<td>13</td>
<td>5.24</td>
<td>12.6</td>
<td>5.13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.40</td>
<td></td>
<td></td>
<td>3.72</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers. Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B11: Mean and Standard Deviation Values for Delay Times ($T_{\text{Delay}}$) in seconds – Walk to Underground Room

<table>
<thead>
<tr>
<th>X</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>X</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>X</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>X</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>X</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>X</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>X</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>1.4</td>
<td>12</td>
<td>3.2</td>
<td>11</td>
<td>2.4</td>
<td>10</td>
<td>1.2</td>
<td>13</td>
<td>4</td>
<td>13</td>
<td>4.4</td>
<td>14</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>-3.6</td>
<td>8</td>
<td>-0.8</td>
<td>7</td>
<td>-1.6</td>
<td>6</td>
<td>-2.8</td>
<td>8</td>
<td>-1</td>
<td>5</td>
<td>-3.6</td>
<td>5</td>
<td>-4</td>
</tr>
<tr>
<td>13</td>
<td>4.4</td>
<td>11</td>
<td>2.2</td>
<td>5</td>
<td>-3.6</td>
<td>11</td>
<td>2.2</td>
<td>7</td>
<td>-2</td>
<td>8</td>
<td>-0.6</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>-2.6</td>
<td>7</td>
<td>-1.8</td>
<td>8</td>
<td>-0.6</td>
<td>5</td>
<td>-3.8</td>
<td>11</td>
<td>2</td>
<td>6</td>
<td>-2.6</td>
<td>8</td>
<td>-1</td>
</tr>
<tr>
<td>9</td>
<td>0.4</td>
<td>6</td>
<td>-2.8</td>
<td>12</td>
<td>3.4</td>
<td>12</td>
<td>3.2</td>
<td>6</td>
<td>-3</td>
<td>11</td>
<td>2.4</td>
<td>7</td>
<td>-2</td>
</tr>
<tr>
<td>10</td>
<td>6.1</td>
<td>13</td>
<td>3</td>
<td>9</td>
<td>0.4</td>
<td>8</td>
<td>-0.4</td>
<td>11</td>
<td>0.4</td>
<td>10</td>
<td>2.4</td>
<td>9</td>
<td>0.4</td>
</tr>
</tbody>
</table>

**NB:** Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers. Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B12: Mean and Standard Deviation Values for Delay Times ($T_{\text{Delay}}$) in seconds – Open Door 1, 2, 5(F2C), 2, 6(F2A), 4, 9(F2E)

<table>
<thead>
<tr>
<th></th>
<th>$x_i - x_{\text{avg}}$</th>
<th></th>
<th>$x_i - x_{\text{avg}}$</th>
<th></th>
<th>$x_i - x_{\text{avg}}$</th>
<th></th>
<th>$x_i - x_{\text{avg}}$</th>
<th></th>
<th>$x_i - x_{\text{avg}}$</th>
<th></th>
<th>$x_i - x_{\text{avg}}$</th>
<th></th>
<th>$x_i - x_{\text{avg}}$</th>
<th></th>
<th>$x_i - x_{\text{avg}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>110</td>
<td>-39.6</td>
<td>195</td>
<td>45.6</td>
<td>118</td>
<td>-31.2</td>
<td>189</td>
<td>39.8</td>
<td>112</td>
<td>-35</td>
<td>186</td>
<td>37.4</td>
<td>120</td>
<td>-31.2</td>
<td>112</td>
<td>-33.2</td>
</tr>
<tr>
<td>113</td>
<td>-36.6</td>
<td>112</td>
<td>-37.4</td>
<td>111</td>
<td>-38.2</td>
<td>123</td>
<td>-26.2</td>
<td>182</td>
<td>35</td>
<td>120</td>
<td>-28.6</td>
<td>119</td>
<td>-32.2</td>
<td>185</td>
<td>39.8</td>
</tr>
<tr>
<td>198</td>
<td>48.4</td>
<td>121</td>
<td>-28.4</td>
<td>197</td>
<td>47.8</td>
<td>114</td>
<td>-35.2</td>
<td>114</td>
<td>-33</td>
<td>110</td>
<td>-38.6</td>
<td>187</td>
<td>35.8</td>
<td>110</td>
<td>-35.2</td>
</tr>
<tr>
<td>207</td>
<td>57.4</td>
<td>208</td>
<td>58.6</td>
<td>206</td>
<td>56.8</td>
<td>110</td>
<td>-39.2</td>
<td>119</td>
<td>-28</td>
<td>210</td>
<td>61.4</td>
<td>207</td>
<td>55.8</td>
<td>116</td>
<td>-29.2</td>
</tr>
<tr>
<td>120</td>
<td>-29.6</td>
<td>111</td>
<td>-38.4</td>
<td>114</td>
<td>-35.2</td>
<td>210</td>
<td>60.8</td>
<td>208</td>
<td>61</td>
<td>117</td>
<td>-31.6</td>
<td>123</td>
<td>-28.2</td>
<td>203</td>
<td>57.8</td>
</tr>
<tr>
<td>149.6</td>
<td><strong>48.53</strong></td>
<td><strong>149.4</strong></td>
<td><strong>47.94</strong></td>
<td><strong>149.2</strong></td>
<td><strong>47.91</strong></td>
<td><strong>149.2</strong></td>
<td><strong>46.75</strong></td>
<td>147</td>
<td><strong>44.84</strong></td>
<td><strong>148.6</strong></td>
<td><strong>46.03</strong></td>
<td><strong>151.2</strong></td>
<td><strong>42.43</strong></td>
<td><strong>145.2</strong></td>
<td><strong>45.05</strong></td>
</tr>
<tr>
<td>184</td>
<td>39</td>
<td>185</td>
<td>36</td>
<td>120</td>
<td>-24.4</td>
<td>110</td>
<td>-46</td>
<td>118</td>
<td>-27.4</td>
<td>110</td>
<td>-35.4</td>
<td>151</td>
<td>-1.2</td>
<td>110</td>
<td>-41.2</td>
</tr>
<tr>
<td>204</td>
<td>59</td>
<td>115</td>
<td>-34</td>
<td>181</td>
<td>36.6</td>
<td>189</td>
<td>33</td>
<td>197</td>
<td>51.6</td>
<td>120</td>
<td>-25.4</td>
<td>198</td>
<td>45.8</td>
<td>185</td>
<td>33.8</td>
</tr>
<tr>
<td>110</td>
<td>-35</td>
<td>130</td>
<td>-19</td>
<td>117</td>
<td>-27.4</td>
<td>165</td>
<td>9</td>
<td>111</td>
<td>-34.4</td>
<td>175</td>
<td>29.6</td>
<td>111</td>
<td>-41.2</td>
<td>120</td>
<td>-31.2</td>
</tr>
<tr>
<td>115</td>
<td>-30</td>
<td>205</td>
<td>56</td>
<td>112</td>
<td>-32.4</td>
<td>203</td>
<td>47</td>
<td>189</td>
<td>43.6</td>
<td>209</td>
<td>63.6</td>
<td>110</td>
<td>-42.2</td>
<td>131</td>
<td>-20.2</td>
</tr>
<tr>
<td>112</td>
<td>-33</td>
<td>110</td>
<td>-39</td>
<td>192</td>
<td>47.6</td>
<td>113</td>
<td>-43</td>
<td>112</td>
<td>-33.4</td>
<td>113</td>
<td>-32.4</td>
<td>191</td>
<td>38.8</td>
<td>210</td>
<td>58.8</td>
</tr>
<tr>
<td>145</td>
<td><strong>45.32</strong></td>
<td>149</td>
<td><strong>43.21</strong></td>
<td>144.4</td>
<td><strong>38.73</strong></td>
<td>156</td>
<td><strong>42.85</strong></td>
<td>145.4</td>
<td><strong>43.63</strong></td>
<td>145.4</td>
<td><strong>44.35</strong></td>
<td>152.2</td>
<td><strong>42.08</strong></td>
<td>151.2</td>
<td><strong>43.81</strong></td>
</tr>
<tr>
<td>113</td>
<td>-33.8</td>
<td>199</td>
<td>51.2</td>
<td>121</td>
<td>-30.2</td>
<td>189</td>
<td>42.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>115</td>
<td>-31.8</td>
<td>188</td>
<td>40.2</td>
<td>197</td>
<td>45.8</td>
<td>193</td>
<td>46.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>189</td>
<td>42.2</td>
<td>116</td>
<td>-31.8</td>
<td>119</td>
<td>-32.2</td>
<td>128</td>
<td>-18.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>110</td>
<td>-36.8</td>
<td>124</td>
<td>-23.8</td>
<td>112</td>
<td>-39.2</td>
<td>110</td>
<td>-36.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>207</td>
<td>60.2</td>
<td>112</td>
<td>-35.8</td>
<td>207</td>
<td>55.8</td>
<td>111</td>
<td>-35.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>146.8</td>
<td><strong>47.20</strong></td>
<td>147.8</td>
<td><strong>42.12</strong></td>
<td>151.2</td>
<td><strong>46.63</strong></td>
<td>146.2</td>
<td><strong>41.54</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers. Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B13: Mean and Standard Deviation Values for Delay Times ($T_{\text{Delay}}$) in seconds – Open Door all Other Doors

<table>
<thead>
<tr>
<th>$x_i$</th>
<th>$x_i - \bar{x}_i$</th>
<th>$x_i$</th>
<th>$x_i - \bar{x}_i$</th>
<th>$x_i$</th>
<th>$x_i - \bar{x}_i$</th>
<th>$x_i$</th>
<th>$x_i - \bar{x}_i$</th>
<th>$x_i$</th>
<th>$x_i - \bar{x}_i$</th>
<th>$x_i$</th>
<th>$x_i - \bar{x}_i$</th>
<th>$x_i$</th>
<th>$x_i - \bar{x}_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td>-26</td>
<td>70</td>
<td>15.2</td>
<td>28</td>
<td>-32.2</td>
<td>33</td>
<td>-8.8</td>
<td>24</td>
<td>-30.4</td>
<td>86</td>
<td>22.2</td>
<td>48</td>
<td>-9.8</td>
</tr>
<tr>
<td>69</td>
<td>14</td>
<td>52</td>
<td>-2.8</td>
<td>55</td>
<td>-5.2</td>
<td>64</td>
<td>22.2</td>
<td>71</td>
<td>16.6</td>
<td>68</td>
<td>4.2</td>
<td>34</td>
<td>-23.8</td>
</tr>
<tr>
<td>64</td>
<td>9</td>
<td>68</td>
<td>13.2</td>
<td>85</td>
<td>24.8</td>
<td>22</td>
<td>-19.8</td>
<td>67</td>
<td>12.6</td>
<td>39</td>
<td>-24.8</td>
<td>75</td>
<td>17.2</td>
</tr>
<tr>
<td>45</td>
<td>-10</td>
<td>49</td>
<td>-5.8</td>
<td>69</td>
<td>8.8</td>
<td>40</td>
<td>-1.8</td>
<td>50</td>
<td>-4.4</td>
<td>54</td>
<td>-9.8</td>
<td>59</td>
<td>1.2</td>
</tr>
<tr>
<td>68</td>
<td>13</td>
<td>35</td>
<td>-19.8</td>
<td>64</td>
<td>3.8</td>
<td>50</td>
<td>8.2</td>
<td>60</td>
<td>5.6</td>
<td>72</td>
<td>8.2</td>
<td>73</td>
<td>15.2</td>
</tr>
<tr>
<td>55</td>
<td>17.48</td>
<td>54.8</td>
<td>14.48</td>
<td>60.2</td>
<td>21.04</td>
<td>41.8</td>
<td>16.07</td>
<td>54.4</td>
<td>18.77</td>
<td>63.8</td>
<td>17.95</td>
<td>57.8</td>
<td>17.25</td>
</tr>
<tr>
<td>58</td>
<td>-5</td>
<td>70</td>
<td>6.2</td>
<td>51</td>
<td>-3.6</td>
<td>47</td>
<td>-18.6</td>
<td>60</td>
<td>6</td>
<td>57</td>
<td>0.8</td>
<td>70</td>
<td>16.2</td>
</tr>
<tr>
<td>32</td>
<td>-31</td>
<td>48</td>
<td>-15.8</td>
<td>61</td>
<td>6.4</td>
<td>90</td>
<td>24.4</td>
<td>49</td>
<td>-5</td>
<td>67</td>
<td>10.8</td>
<td>63</td>
<td>9.2</td>
</tr>
<tr>
<td>74</td>
<td>11</td>
<td>80</td>
<td>16.2</td>
<td>77</td>
<td>22.4</td>
<td>56</td>
<td>-9.6</td>
<td>55</td>
<td>1</td>
<td>33</td>
<td>-23.2</td>
<td>46</td>
<td>-7.8</td>
</tr>
<tr>
<td>69</td>
<td>6</td>
<td>67</td>
<td>3.2</td>
<td>28</td>
<td>-26.6</td>
<td>74</td>
<td>8.4</td>
<td>27</td>
<td>-27</td>
<td>48</td>
<td>-8.2</td>
<td>31</td>
<td>-22.8</td>
</tr>
<tr>
<td>82</td>
<td>19</td>
<td>54</td>
<td>-9.8</td>
<td>56</td>
<td>1.4</td>
<td>61</td>
<td>-4.6</td>
<td>79</td>
<td>25</td>
<td>76</td>
<td>19.8</td>
<td>59</td>
<td>5.2</td>
</tr>
<tr>
<td>63</td>
<td>19.39</td>
<td>63.8</td>
<td>12.81</td>
<td>54.6</td>
<td>17.78</td>
<td>65.6</td>
<td>16.77</td>
<td>54</td>
<td>18.81</td>
<td>56.2</td>
<td>16.69</td>
<td>53.8</td>
<td>15.45</td>
</tr>
<tr>
<td>53</td>
<td>-2.6</td>
<td>34</td>
<td>-6.8</td>
<td>67</td>
<td>0.6</td>
<td>69</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>67</td>
<td>11.4</td>
<td>68</td>
<td>27.2</td>
<td>48</td>
<td>-18.4</td>
<td>78</td>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>-10.6</td>
<td>25</td>
<td>-15.8</td>
<td>82</td>
<td>15.6</td>
<td>54</td>
<td>-5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>-17.6</td>
<td>37</td>
<td>-3.8</td>
<td>50</td>
<td>-16.4</td>
<td>67</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>75</td>
<td>19.4</td>
<td>40</td>
<td>-0.8</td>
<td>85</td>
<td>18.6</td>
<td>27</td>
<td>-32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>55.6</td>
<td>15.29</td>
<td>40.8</td>
<td>16.21</td>
<td>66.4</td>
<td>17.30</td>
<td>59</td>
<td>19.84</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NB: Iitalicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers. Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B14: Mean and Standard Deviation Values for Delay Times ($T_{\text{Delay}}$) in seconds – Open Outer Burglar Bar Gate

<table>
<thead>
<tr>
<th>x</th>
<th>$x_i - \bar{x}$</th>
<th>x</th>
<th>$x_i - \bar{x}$</th>
<th>x</th>
<th>$x_i - \bar{x}$</th>
<th>x</th>
<th>$x_i - \bar{x}$</th>
<th>x</th>
<th>$x_i - \bar{x}$</th>
<th>x</th>
<th>$x_i - \bar{x}$</th>
<th>x</th>
<th>$x_i - \bar{x}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>52</td>
<td>48.2</td>
<td>75</td>
<td>16.8</td>
<td>58</td>
<td>41.6</td>
<td>109</td>
<td>8.6</td>
<td>131</td>
<td>35</td>
<td>86</td>
<td>3.8</td>
<td>54</td>
<td>45.2</td>
</tr>
<tr>
<td>147</td>
<td>46.8</td>
<td>55</td>
<td>36.8</td>
<td>102</td>
<td>2.4</td>
<td>94</td>
<td>6.4</td>
<td>75</td>
<td>21</td>
<td>118</td>
<td>28.2</td>
<td>137</td>
<td>37.8</td>
</tr>
<tr>
<td>95</td>
<td>5.2</td>
<td>138</td>
<td>46.2</td>
<td>89</td>
<td>10.6</td>
<td>120</td>
<td>19.6</td>
<td>137</td>
<td>41</td>
<td>61</td>
<td>28.8</td>
<td>120</td>
<td>20.8</td>
</tr>
<tr>
<td>84</td>
<td>16.2</td>
<td>86</td>
<td>5.8</td>
<td>99</td>
<td>0.6</td>
<td>83</td>
<td>17.4</td>
<td>57</td>
<td>39</td>
<td>74</td>
<td>15.8</td>
<td>98</td>
<td>1.2</td>
</tr>
<tr>
<td>123</td>
<td>22.8</td>
<td>105</td>
<td>13.2</td>
<td>150</td>
<td>50.4</td>
<td>96</td>
<td>-4.4</td>
<td>80</td>
<td>-16</td>
<td>110</td>
<td>20.2</td>
<td>87</td>
<td>-12.2</td>
</tr>
<tr>
<td>100.2</td>
<td><strong>36.48</strong></td>
<td>91.8</td>
<td><strong>31.54</strong></td>
<td>99.6</td>
<td><strong>33.13</strong></td>
<td>100.4</td>
<td><strong>14.33</strong></td>
<td>96</td>
<td><strong>35.79</strong></td>
<td>89.8</td>
<td><strong>23.96</strong></td>
<td>99.2</td>
<td><strong>31.84</strong></td>
</tr>
<tr>
<td>119</td>
<td>17.8</td>
<td>71</td>
<td>-5</td>
<td>99</td>
<td>-1.2</td>
<td>83</td>
<td>-11.2</td>
<td>60</td>
<td>-30.6</td>
<td>59</td>
<td>-45.8</td>
<td>71</td>
<td>-21.8</td>
</tr>
<tr>
<td>79</td>
<td>22.2</td>
<td>84</td>
<td>8</td>
<td>131</td>
<td>30.8</td>
<td>91</td>
<td>-3.2</td>
<td>94</td>
<td>3.4</td>
<td>96</td>
<td>-8.8</td>
<td>100</td>
<td>7.2</td>
</tr>
<tr>
<td>64</td>
<td>37.2</td>
<td>63</td>
<td>-13</td>
<td>89</td>
<td>-11.2</td>
<td>106</td>
<td>11.8</td>
<td>91</td>
<td>0.4</td>
<td>133</td>
<td>28.2</td>
<td>146</td>
<td>53.2</td>
</tr>
<tr>
<td>149</td>
<td>47.8</td>
<td>100</td>
<td>24</td>
<td>126</td>
<td>25.8</td>
<td>125</td>
<td>30.8</td>
<td>127</td>
<td>36.4</td>
<td>149</td>
<td>44.2</td>
<td>88</td>
<td>-4.8</td>
</tr>
<tr>
<td>95</td>
<td>6.2</td>
<td>62</td>
<td>-14</td>
<td>56</td>
<td>-44.2</td>
<td>66</td>
<td>-28.2</td>
<td>81</td>
<td>-9.6</td>
<td>87</td>
<td>-17.8</td>
<td>59</td>
<td>-33.8</td>
</tr>
<tr>
<td>101.2</td>
<td><strong>33.60</strong></td>
<td>76</td>
<td><strong>16.05</strong></td>
<td>100.2</td>
<td><strong>30.39</strong></td>
<td>94.2</td>
<td><strong>22.47</strong></td>
<td>90.6</td>
<td><strong>24.32</strong></td>
<td>104.8</td>
<td><strong>36.20</strong></td>
<td>92.8</td>
<td><strong>33.63</strong></td>
</tr>
<tr>
<td>58</td>
<td>36.4</td>
<td>122</td>
<td>25.6</td>
<td>67</td>
<td>12.6</td>
<td>96</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>76</td>
<td>18.4</td>
<td>88</td>
<td>-8.4</td>
<td>84</td>
<td>4.4</td>
<td>78</td>
<td>-11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>141</td>
<td>46.6</td>
<td>65</td>
<td>-31.4</td>
<td>102</td>
<td>22.4</td>
<td>114</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>108</td>
<td>13.6</td>
<td>137</td>
<td>40.6</td>
<td>55</td>
<td>-24.6</td>
<td>87</td>
<td>-2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>89</td>
<td>5.4</td>
<td>70</td>
<td>-26.4</td>
<td>90</td>
<td>10.4</td>
<td>70</td>
<td>-19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>94.4</td>
<td><strong>31.82</strong></td>
<td>96.4</td>
<td><strong>31.85</strong></td>
<td>79.6</td>
<td><strong>18.66</strong></td>
<td>89</td>
<td><strong>17.03</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers. Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B15: Mean and Standard Deviation Values for Delay Times ($T_{\text{Delay}}$) in seconds – Open Inner Burglar Bar Gate

| X     | $x_i - \bar{x}_{avg}$ | X     | $x_i - \bar{x}_{avg}$ | X     | $x_i - \bar{x}_{avg}$ | X     | $x_i - \bar{x}_{avg}$ | X     | $x_i - \bar{x}_{avg}$ | X     | $x_i - \bar{x}_{avg}$ | X     | $x_i - \bar{x}_{avg}$ | X     | $x_i - \bar{x}_{avg}$ | X     | $x_i - \bar{x}_{avg}$ |
|-------|------------------------|-------|------------------------|-------|------------------------|-------|------------------------|-------|------------------------|-------|------------------------|-------|------------------------|-------|------------------------|
| 150   | 2.2                    | 177   | 10.2                   | 165   | 0                      | 60    | -93.2                  | 161   | 2.4                    | 186   | 27.8                   | 156   | -1.8                   | 191   | 24.8                   |
| 79    | -68.8                  | 208   | 41.2                   | 202   | 37                     | 205   | 51.8                   | 200   | 41.4                   | 153   | -5.2                   | 207   | 49.2                   | 89    | -77.2                  |
| 210   | 62.2                   | 183   | 16.2                   | 89    | -76                    | 180   | 26.8                   | 150   | -8.6                   | 68    | -90.2                  | 161   | 3.2                    | 202   | 35.8                   |
| 147   | -0.8                   | 197   | 30.2                   | 199   | 34                     | 155   | 1.8                    | 102   | -56.6                  | 174   | 15.8                   | 189   | 31.2                   | 188   | 21.8                   |
| 153   | 5.2                    | 69    | -97.8                  | 170   | 5                      | 166   | 12.8                   | 180   | 21.4                   | 210   | 51.8                   | 76    | -81.8                  | 161   | -5.2                   |
| 147.8 | 46.46                  | 166.8 | 55.99                  | 165   | 45.62                  | 153.2 | 55.35                  | 158.6 | 36.93                  | 157.8 | 54.47                  | 166.2 | 45.71                  |
| 146   | -8.8                   | 171   | 5.2                    | 197   | 37.6                   | 183   | 23.6                   | 160   | -2.8                   | 71    | -85.8                  | 179   | 20.8                   | 189   | 27.2                   |
| 73    | -81.8                  | 204   | 38.2                   | 143   | -16.4                  | 191   | 31.6                   | 194   | 31.2                   | 178   | 21.2                   | 200   | 41.8                   | 70    | -91.8                  |
| 209   | 54.2                   | 210   | 44.2                   | 86    | -73.4                  | 201   | 41.6                   | 167   | 4.2                    | 190   | 33.2                   | 164   | 5.8                    | 163   | 1.2                    |
| 157   | 2.2                    | 78    | -87.8                  | 206   | 46.6                   | 157   | -2.4                   | 172   | 9.2                    | 157   | 0.2                    | 89    | -69.2                  | 187   | 25.2                   |
| 189   | 34.2                   | 166   | 0.2                    | 165   | 5.6                    | 65    | -94.4                  | 121   | -41.8                  | 188   | 31.2                   | 159   | 0.8                    | 200   | 38.2                   |
| 154.8 | 52.16                  | 165.8 | 52.79                  | 159.4 | 48.15                  | 159.4 | 55.23                  | 162.8 | 26.60                  | 156.8 | 49.72                  | 158.2 | 41.84                  | 161.8 | 53.06                  |
| 183   | 20.8                   | 159   | 3.6                    | 167   | 6.2                    | 196   | 31                     |
| 87    | -75.2                  | 168   | 12.6                   | 184   | 23.2                   | 178   | 13                     |
| 207   | 44.8                   | 67    | -88.4                  | 200   | 39.2                   | 161   | -4                     |
| 166   | 3.8                    | 176   | 20.6                   | 160   | -0.8                   | 82    | -83                    |
| 168   | 5.8                    | 207   | 51.6                   | 93    | -67.8                  | 208   | 43                     |
| 162.2 | 45.12                  | 155.4 | 52.61                  | 160.8 | 40.96                  | 165   | 49.71                  |

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers. Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B16: Mean and Standard Deviation Values for Delay Times (T\text{Delay}) in seconds – Remove Outer Window Burglar Bars

<table>
<thead>
<tr>
<th>X</th>
<th>x_i - \bar{x}_\text{avg}</th>
<th>X</th>
<th>x_i - \bar{x}_\text{avg}</th>
<th>X</th>
<th>x_i - \bar{x}_\text{avg}</th>
<th>X</th>
<th>x_i - \bar{x}_\text{avg}</th>
<th>X</th>
<th>x_i - \bar{x}_\text{avg}</th>
<th>X</th>
<th>x_i - \bar{x}_\text{avg}</th>
<th>X</th>
<th>x_i - \bar{x}_\text{avg}</th>
<th>X</th>
<th>x_i - \bar{x}_\text{avg}</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>-61.4</td>
<td>71</td>
<td>-53.4</td>
<td>168</td>
<td>36.6</td>
<td>121</td>
<td>1</td>
<td>160</td>
<td>22.8</td>
<td>86</td>
<td>-39.6</td>
<td>154</td>
<td>28.4</td>
<td>65</td>
<td>-64</td>
</tr>
<tr>
<td>147</td>
<td>25.6</td>
<td>152</td>
<td>27.6</td>
<td>120</td>
<td>-11.4</td>
<td>63</td>
<td>-57</td>
<td>73</td>
<td>-64.2</td>
<td>180</td>
<td>54.4</td>
<td>173</td>
<td>47.4</td>
<td>179</td>
<td>50</td>
</tr>
<tr>
<td>103</td>
<td>-18.4</td>
<td>176</td>
<td>51.6</td>
<td>129</td>
<td>-2.4</td>
<td>149</td>
<td>29</td>
<td>176</td>
<td>38.8</td>
<td>63</td>
<td>-62.6</td>
<td>125</td>
<td>-0.6</td>
<td>87</td>
<td>-42</td>
</tr>
<tr>
<td>174</td>
<td>52.6</td>
<td>98</td>
<td>-26.4</td>
<td>90</td>
<td>-41.4</td>
<td>157</td>
<td>37</td>
<td>157</td>
<td>19.8</td>
<td>174</td>
<td>48.4</td>
<td>100</td>
<td>-25.6</td>
<td>145</td>
<td>16</td>
</tr>
<tr>
<td>123</td>
<td>1.6</td>
<td>125</td>
<td>0.6</td>
<td>150</td>
<td>18.6</td>
<td>110</td>
<td>-10</td>
<td>120</td>
<td>-17.2</td>
<td>125</td>
<td>-0.6</td>
<td>76</td>
<td>-49.6</td>
<td>169</td>
<td>40</td>
</tr>
<tr>
<td>121.4</td>
<td>43.40</td>
<td>124.4</td>
<td>41.75</td>
<td>131.4</td>
<td>29.73</td>
<td>120</td>
<td>37.28</td>
<td>137.2</td>
<td>41.34</td>
<td>125.6</td>
<td>51.94</td>
<td>125.6</td>
<td>39.27</td>
<td>129</td>
<td>50.54</td>
</tr>
<tr>
<td>128</td>
<td>-12.2</td>
<td>74</td>
<td>-54.8</td>
<td>119</td>
<td>-5</td>
<td>163</td>
<td>42.2</td>
<td>160</td>
<td>30</td>
<td>73</td>
<td>-61.2</td>
<td>60</td>
<td>-63.6</td>
<td>138</td>
<td>7.4</td>
</tr>
<tr>
<td>177</td>
<td>36.8</td>
<td>119</td>
<td>-9.8</td>
<td>133</td>
<td>9</td>
<td>105</td>
<td>-15.8</td>
<td>104</td>
<td>-26</td>
<td>180</td>
<td>45.8</td>
<td>130</td>
<td>6.4</td>
<td>69</td>
<td>-61.6</td>
</tr>
<tr>
<td>67</td>
<td>-73.2</td>
<td>163</td>
<td>34.2</td>
<td>79</td>
<td>-45</td>
<td>140</td>
<td>19.2</td>
<td>171</td>
<td>41</td>
<td>133</td>
<td>-1.2</td>
<td>146</td>
<td>22.4</td>
<td>124</td>
<td>-6.6</td>
</tr>
<tr>
<td>149</td>
<td>8.8</td>
<td>120</td>
<td>-8.8</td>
<td>126</td>
<td>2</td>
<td>125</td>
<td>4.2</td>
<td>127</td>
<td>-3</td>
<td>149</td>
<td>14.8</td>
<td>125</td>
<td>1.4</td>
<td>151</td>
<td>20.4</td>
</tr>
<tr>
<td>180</td>
<td>39.8</td>
<td>168</td>
<td>39.2</td>
<td>163</td>
<td>39</td>
<td>71</td>
<td>-49.8</td>
<td>88</td>
<td>-42</td>
<td>136</td>
<td>1.8</td>
<td>157</td>
<td>33.4</td>
<td>171</td>
<td>40.4</td>
</tr>
<tr>
<td>140.2</td>
<td>46.16</td>
<td>128.8</td>
<td>38.35</td>
<td>124</td>
<td>30.23</td>
<td>120.8</td>
<td>34.99</td>
<td>130</td>
<td>35.46</td>
<td>134.2</td>
<td>38.94</td>
<td>123.6</td>
<td>37.77</td>
<td>130.6</td>
<td>38.54</td>
</tr>
<tr>
<td>X</td>
<td>\bar{x}_\text{avg}</td>
<td>X</td>
<td>\bar{x}_\text{avg}</td>
<td>X</td>
<td>\bar{x}_\text{avg}</td>
<td>X</td>
<td>\bar{x}_\text{avg}</td>
<td>X</td>
<td>\bar{x}_\text{avg}</td>
<td>X</td>
<td>\bar{x}_\text{avg}</td>
<td>X</td>
<td>\bar{x}_\text{avg}</td>
<td>X</td>
<td>\bar{x}_\text{avg}</td>
</tr>
<tr>
<td>153</td>
<td>15.6</td>
<td>167</td>
<td>40.2</td>
<td>117</td>
<td>5.2</td>
<td>175</td>
<td>29.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>137</td>
<td>-0.4</td>
<td>80</td>
<td>-46.8</td>
<td>125</td>
<td>13.2</td>
<td>128</td>
<td>-17.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>145</td>
<td>7.6</td>
<td>171</td>
<td>44.2</td>
<td>76</td>
<td>-35.8</td>
<td>159</td>
<td>13.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>179</td>
<td>41.6</td>
<td>97</td>
<td>-29.8</td>
<td>133</td>
<td>21.2</td>
<td>97</td>
<td>-48.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>73</td>
<td>-64.4</td>
<td>119</td>
<td>-7.8</td>
<td>108</td>
<td>-3.8</td>
<td>167</td>
<td>21.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>137.4</td>
<td>39.30</td>
<td>126.8</td>
<td>40.95</td>
<td>111.8</td>
<td>22.06</td>
<td>145.2</td>
<td>32.30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers
Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution

207
Table B17: Mean and Standard Deviation Values for Delay Times (T_{Delay}) in seconds – Remove Inner Window Burglar Bars

<table>
<thead>
<tr>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
<th>x</th>
<th>x_i - x_{avg}</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>-58.4</td>
<td>45</td>
<td>-41.4</td>
<td>41</td>
<td>-45</td>
<td>109</td>
<td>14.6</td>
<td>47</td>
<td>-33.6</td>
<td>36</td>
<td>-45.4</td>
<td>79</td>
<td>-0.4</td>
<td>81</td>
<td>-6.2</td>
</tr>
<tr>
<td>134</td>
<td>45.6</td>
<td>75</td>
<td>-11.4</td>
<td>102</td>
<td>16</td>
<td>57</td>
<td>-37.4</td>
<td>71</td>
<td>-9.6</td>
<td>108</td>
<td>26.6</td>
<td>41</td>
<td>-38.4</td>
<td>102</td>
<td>14.8</td>
</tr>
<tr>
<td>79</td>
<td>-9.4</td>
<td>128</td>
<td>41.6</td>
<td>85</td>
<td>-1</td>
<td>120</td>
<td>25.6</td>
<td>106</td>
<td>25.4</td>
<td>69</td>
<td>-12.4</td>
<td>120</td>
<td>40.6</td>
<td>55</td>
<td>-32.2</td>
</tr>
<tr>
<td>86</td>
<td>-2.4</td>
<td>86</td>
<td>-0.4</td>
<td>82</td>
<td>-4</td>
<td>90</td>
<td>-4.4</td>
<td>81</td>
<td>0.4</td>
<td>84</td>
<td>5.6</td>
<td>89</td>
<td>9.6</td>
<td>88</td>
<td>9.8</td>
</tr>
<tr>
<td>113</td>
<td>24.6</td>
<td>98</td>
<td>11.6</td>
<td>120</td>
<td>34</td>
<td>96</td>
<td>1.6</td>
<td>98</td>
<td>17.4</td>
<td>110</td>
<td>28.6</td>
<td>68</td>
<td>-14.4</td>
<td>110</td>
<td>22.8</td>
</tr>
<tr>
<td>88.4</td>
<td>39.34</td>
<td>86</td>
<td>30.45</td>
<td>86</td>
<td>29.39</td>
<td>94.4</td>
<td>23.92</td>
<td>80.6</td>
<td>23.29</td>
<td>81.4</td>
<td>30.61</td>
<td>79.4</td>
<td>28.92</td>
<td>87.2</td>
<td>21.30</td>
</tr>
<tr>
<td>119</td>
<td>23.8</td>
<td>57</td>
<td>-31.8</td>
<td>99</td>
<td>11</td>
<td>45</td>
<td>-46.2</td>
<td>80</td>
<td>-5.8</td>
<td>71</td>
<td>-28</td>
<td>79</td>
<td>-3.6</td>
<td>123</td>
<td>31.4</td>
</tr>
<tr>
<td>51</td>
<td>-44.2</td>
<td>84</td>
<td>-4.8</td>
<td>41</td>
<td>-47</td>
<td>91</td>
<td>-0.2</td>
<td>49</td>
<td>-36.8</td>
<td>96</td>
<td>-3</td>
<td>101</td>
<td>18.4</td>
<td>69</td>
<td>-22.6</td>
</tr>
<tr>
<td>86</td>
<td>-9.2</td>
<td>81</td>
<td>-7.8</td>
<td>88</td>
<td>0</td>
<td>106</td>
<td>14.8</td>
<td>88</td>
<td>2.2</td>
<td>133</td>
<td>34</td>
<td>68</td>
<td>-14.6</td>
<td>110</td>
<td>18.4</td>
</tr>
<tr>
<td>135</td>
<td>39.8</td>
<td>100</td>
<td>11.2</td>
<td>126</td>
<td>38</td>
<td>125</td>
<td>33.8</td>
<td>127</td>
<td>41.2</td>
<td>104</td>
<td>5</td>
<td>86</td>
<td>3.4</td>
<td>58</td>
<td>-33.6</td>
</tr>
<tr>
<td>85</td>
<td>-10.2</td>
<td>122</td>
<td>33.2</td>
<td>86</td>
<td>-2</td>
<td>89</td>
<td>-2.2</td>
<td>85</td>
<td>-0.8</td>
<td>91</td>
<td>-8</td>
<td>79</td>
<td>-3.6</td>
<td>98</td>
<td>6.4</td>
</tr>
<tr>
<td>95.2</td>
<td>32.76</td>
<td>88.8</td>
<td>24.10</td>
<td>88</td>
<td>30.73</td>
<td>91.2</td>
<td>29.58</td>
<td>85.8</td>
<td>27.80</td>
<td>99</td>
<td>22.57</td>
<td>82.6</td>
<td>12.14</td>
<td>91.6</td>
<td>27.41</td>
</tr>
<tr>
<td>54</td>
<td>-40.4</td>
<td>121</td>
<td>24.8</td>
<td>51</td>
<td>-34</td>
<td>96</td>
<td>-4.4</td>
<td>58</td>
<td>-2.8</td>
<td>78</td>
<td>-22.4</td>
<td>120</td>
<td>19.6</td>
<td>102</td>
<td>10.6</td>
</tr>
<tr>
<td>98</td>
<td>3.6</td>
<td>79</td>
<td>-17.2</td>
<td>84</td>
<td>-1</td>
<td>78</td>
<td>-22.4</td>
<td>120</td>
<td>19.6</td>
<td>102</td>
<td>10.6</td>
<td>112</td>
<td>3.4</td>
<td>115</td>
<td>10.6</td>
</tr>
<tr>
<td>79</td>
<td>-15.4</td>
<td>93</td>
<td>-3.2</td>
<td>115</td>
<td>30</td>
<td>120</td>
<td>19.6</td>
<td>102</td>
<td>10.6</td>
<td>112</td>
<td>3.4</td>
<td>115</td>
<td>10.6</td>
<td>115</td>
<td>10.6</td>
</tr>
<tr>
<td>94.4</td>
<td>29.11</td>
<td>96.2</td>
<td>30.29</td>
<td>85</td>
<td>24.95</td>
<td>100.4</td>
<td>16.04</td>
<td>85</td>
<td>24.95</td>
<td>100.4</td>
<td>16.04</td>
<td>89.4</td>
<td>26.73</td>
<td>89.4</td>
<td>26.73</td>
</tr>
</tbody>
</table>

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers. Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B18: Mean and Standard Deviation Values for Delay Times ($T_{\text{Delay}}$) in seconds – Remove Targets (Computers, Test Sources and Stationary)

<table>
<thead>
<tr>
<th>x</th>
<th>$x_i - \overline{x}$</th>
<th>x</th>
<th>$x_i - \overline{x}$</th>
<th>x</th>
<th>$x_i - \overline{x}$</th>
<th>x</th>
<th>$x_i - \overline{x}$</th>
<th>x</th>
<th>$x_i - \overline{x}$</th>
<th>x</th>
<th>$x_i - \overline{x}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>-16.2</td>
<td>53</td>
<td>10.6</td>
<td>26</td>
<td>-12.2</td>
<td>52</td>
<td>13.6</td>
<td>56</td>
<td>17</td>
<td>34</td>
<td>-6</td>
</tr>
<tr>
<td>32</td>
<td>-9.2</td>
<td>32</td>
<td>-10.4</td>
<td>32</td>
<td>-6.2</td>
<td>28</td>
<td>-10.4</td>
<td>49</td>
<td>10</td>
<td>29</td>
<td>-11</td>
</tr>
<tr>
<td>55</td>
<td>13.8</td>
<td>27</td>
<td>-15.4</td>
<td>53</td>
<td>14.8</td>
<td>32</td>
<td>-6.4</td>
<td>27</td>
<td>-12</td>
<td>36</td>
<td>-4</td>
</tr>
<tr>
<td>51</td>
<td>9.8</td>
<td>51</td>
<td>8.6</td>
<td>29</td>
<td>-9.2</td>
<td>31</td>
<td>-7.4</td>
<td>33</td>
<td>-6</td>
<td>41</td>
<td>1</td>
</tr>
<tr>
<td>43</td>
<td>1.8</td>
<td>49</td>
<td>6.6</td>
<td>51</td>
<td>12.8</td>
<td>49</td>
<td>10.6</td>
<td>30</td>
<td>-9</td>
<td>60</td>
<td>20</td>
</tr>
<tr>
<td>41.2</td>
<td>12.62</td>
<td>42.4</td>
<td>11.99</td>
<td>38.2</td>
<td>12.79</td>
<td>38.4</td>
<td>11.19</td>
<td>39</td>
<td>12.75</td>
<td>40</td>
<td>11.98</td>
</tr>
<tr>
<td>34</td>
<td>-6.6</td>
<td>33</td>
<td>-7.6</td>
<td>57</td>
<td>15.6</td>
<td>25</td>
<td>-13.8</td>
<td>35</td>
<td>-7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>16.4</td>
<td>58</td>
<td>17.4</td>
<td>31</td>
<td>-10.4</td>
<td>36</td>
<td>-2.8</td>
<td>27</td>
<td>-15</td>
<td>51</td>
<td>10.6</td>
</tr>
<tr>
<td>29</td>
<td>-11.6</td>
<td>36</td>
<td>-4.6</td>
<td>28</td>
<td>-13.4</td>
<td>29</td>
<td>-9.8</td>
<td>55</td>
<td>13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>7.4</td>
<td>49</td>
<td>8.4</td>
<td>38</td>
<td>-3.4</td>
<td>54</td>
<td>15.2</td>
<td>37</td>
<td>-5</td>
<td>25</td>
<td>-15.4</td>
</tr>
<tr>
<td>35</td>
<td>-5.6</td>
<td>27</td>
<td>-13.6</td>
<td>53</td>
<td>11.6</td>
<td>50</td>
<td>11.2</td>
<td>56</td>
<td>14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>40.6</td>
<td>11.55</td>
<td>40.6</td>
<td>12.62</td>
<td>41.4</td>
<td>13.01</td>
<td>38.8</td>
<td>12.76</td>
<td>42</td>
<td>12.88</td>
<td></td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>14.8</td>
<td>51</td>
<td>6.6</td>
<td>45</td>
<td>6.4</td>
<td>31</td>
<td>-10.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>8.8</td>
<td>56</td>
<td>11.6</td>
<td>30</td>
<td>-8.6</td>
<td>55</td>
<td>13.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>-12.2</td>
<td>36</td>
<td>-8.4</td>
<td>33</td>
<td>-5.6</td>
<td>51</td>
<td>9.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>-5.2</td>
<td>34</td>
<td>-10.4</td>
<td>26</td>
<td>-12.6</td>
<td>32</td>
<td>-9.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>-6.2</td>
<td>45</td>
<td>0.6</td>
<td>59</td>
<td>20.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>39.2</td>
<td>11.30</td>
<td>44.4</td>
<td>9.45</td>
<td>38.6</td>
<td>13.43</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers. Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B19: Mean and Standard Deviation Values for Delay Times ($T_{\text{Delay}}$) in seconds – Remove Targets (Equipment)

<table>
<thead>
<tr>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>210</td>
<td>-74.6</td>
<td>213</td>
<td>-69</td>
<td>365</td>
<td>80</td>
<td>217</td>
<td>-67.4</td>
<td>344</td>
<td>66.4</td>
<td>388</td>
<td>99.8</td>
<td>221</td>
<td>-58.6</td>
</tr>
<tr>
<td>233</td>
<td>-51.6</td>
<td>231</td>
<td>-51</td>
<td>234</td>
<td>-51</td>
<td>236</td>
<td>-48.4</td>
<td>230</td>
<td>-47.6</td>
<td>221</td>
<td>-67.2</td>
<td>390</td>
<td>110.4</td>
</tr>
<tr>
<td>221</td>
<td>-63.6</td>
<td>361</td>
<td>79</td>
<td>390</td>
<td>105</td>
<td>380</td>
<td>95.6</td>
<td>222</td>
<td>-55.6</td>
<td>215</td>
<td>-73.2</td>
<td>211</td>
<td>-68.6</td>
</tr>
<tr>
<td>370</td>
<td>85.4</td>
<td>229</td>
<td>-53</td>
<td>224</td>
<td>-61</td>
<td>223</td>
<td>-61.4</td>
<td>216</td>
<td>-61.6</td>
<td>387</td>
<td>98.8</td>
<td>340</td>
<td>60.4</td>
</tr>
<tr>
<td>389</td>
<td>104.4</td>
<td>376</td>
<td>94</td>
<td>212</td>
<td>-73</td>
<td>366</td>
<td>81.6</td>
<td>376</td>
<td>98.4</td>
<td>230</td>
<td>-58.2</td>
<td>236</td>
<td>-43.6</td>
</tr>
<tr>
<td>284.6</td>
<td>87.27</td>
<td>282</td>
<td>79.45</td>
<td>285</td>
<td>85.26</td>
<td>284.4</td>
<td>81.32</td>
<td>277.6</td>
<td>76.23</td>
<td>288.2</td>
<td>90.81</td>
<td>279.6</td>
<td>80.43</td>
</tr>
<tr>
<td>212</td>
<td>-63.2</td>
<td>229</td>
<td>-48.2</td>
<td>350</td>
<td>71.4</td>
<td>222</td>
<td>-61.8</td>
<td>215</td>
<td>-64.2</td>
<td>211</td>
<td>-70.4</td>
<td>210</td>
<td>-74</td>
</tr>
<tr>
<td>351</td>
<td>75.8</td>
<td>335</td>
<td>57.8</td>
<td>220</td>
<td>-58.6</td>
<td>212</td>
<td>-71.8</td>
<td>387</td>
<td>107.8</td>
<td>386</td>
<td>104.6</td>
<td>223</td>
<td>-61</td>
</tr>
<tr>
<td>220</td>
<td>-55.2</td>
<td>222</td>
<td>-55.2</td>
<td>216</td>
<td>-62.6</td>
<td>232</td>
<td>-51.8</td>
<td>220</td>
<td>-59.2</td>
<td>224</td>
<td>-57.4</td>
<td>221</td>
<td>-63</td>
</tr>
<tr>
<td>213</td>
<td>-62.2</td>
<td>389</td>
<td>111.8</td>
<td>223</td>
<td>-55.6</td>
<td>365</td>
<td>81.2</td>
<td>362</td>
<td>82.8</td>
<td>365</td>
<td>83.6</td>
<td>389</td>
<td>105</td>
</tr>
<tr>
<td>380</td>
<td>104.8</td>
<td>211</td>
<td>-66.2</td>
<td>384</td>
<td>105.4</td>
<td>388</td>
<td>104.2</td>
<td>212</td>
<td>-67.2</td>
<td>221</td>
<td>-60.4</td>
<td>377</td>
<td>93</td>
</tr>
<tr>
<td>275.2</td>
<td>83.12</td>
<td>277.2</td>
<td>79.99</td>
<td>278.6</td>
<td>81.63</td>
<td>283.8</td>
<td>85.31</td>
<td>279.2</td>
<td>87.49</td>
<td>281.4</td>
<td>86.36</td>
<td>284</td>
<td>90.61</td>
</tr>
<tr>
<td>211</td>
<td>-71</td>
<td>375</td>
<td>100.2</td>
<td>220</td>
<td>-63.8</td>
<td>348</td>
<td>68.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>216</td>
<td>-66</td>
<td>355</td>
<td>80.2</td>
<td>390</td>
<td>106.2</td>
<td>210</td>
<td>-69.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>221</td>
<td>-61</td>
<td>220</td>
<td>-54.8</td>
<td>231</td>
<td>-52.8</td>
<td>226</td>
<td>-53.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>379</td>
<td>97</td>
<td>214</td>
<td>-60.8</td>
<td>222</td>
<td>-61.8</td>
<td>223</td>
<td>-56.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>383</td>
<td>101</td>
<td>210</td>
<td>-64.8</td>
<td>356</td>
<td>72.2</td>
<td>389</td>
<td>109.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>282</td>
<td>90.45</td>
<td>274.8</td>
<td>82.72</td>
<td>283.8</td>
<td>82.41</td>
<td>279.2</td>
<td>83.02</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers. Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B20: Mean and Standard Deviation Values for Delay Times (T_{Delay}) in seconds – Sabotage Target

<table>
<thead>
<tr>
<th></th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>-44.4</td>
<td>167</td>
<td>47</td>
<td>165</td>
<td>42</td>
<td>137</td>
<td>15</td>
<td>162</td>
<td>34.8</td>
<td>91</td>
<td>-22.6</td>
<td>167</td>
<td>49.2</td>
<td>88</td>
<td>-26.6</td>
<td></td>
</tr>
<tr>
<td>92</td>
<td>-32.4</td>
<td>82</td>
<td>-38</td>
<td>119</td>
<td>-4</td>
<td>83</td>
<td>-39</td>
<td>131</td>
<td>3.8</td>
<td>150</td>
<td>36.4</td>
<td>83</td>
<td>-34.8</td>
<td>168</td>
<td>53.4</td>
<td></td>
</tr>
<tr>
<td>125</td>
<td>0.6</td>
<td>97</td>
<td>-23</td>
<td>95</td>
<td>-28</td>
<td>149</td>
<td>27</td>
<td>166</td>
<td>38.8</td>
<td>88</td>
<td>-25.6</td>
<td>110</td>
<td>-7.8</td>
<td>93</td>
<td>-21.6</td>
<td></td>
</tr>
<tr>
<td>170</td>
<td>45.6</td>
<td>94</td>
<td>-26</td>
<td>81</td>
<td>-42</td>
<td>154</td>
<td>32</td>
<td>86</td>
<td>-41.2</td>
<td>80</td>
<td>-33.6</td>
<td>88</td>
<td>-29.8</td>
<td>84</td>
<td>-30.6</td>
<td></td>
</tr>
<tr>
<td>155</td>
<td>30.6</td>
<td>160</td>
<td>40</td>
<td>155</td>
<td>32</td>
<td>87</td>
<td>-35</td>
<td>91</td>
<td>-36.2</td>
<td>159</td>
<td>45.4</td>
<td>141</td>
<td>23.2</td>
<td>140</td>
<td>25.4</td>
<td></td>
</tr>
</tbody>
</table>

**Total:** 124.4 38.85 120 40.18 123 36.58 122 34.37 127.2 37.88 113.6 37.69 117.8 35.77 114.6 37.44

<table>
<thead>
<tr>
<th></th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
</tr>
</thead>
<tbody>
<tr>
<td>86</td>
<td>-25.6</td>
<td>98</td>
<td>-21.4</td>
<td>93</td>
<td>-24.2</td>
<td>161</td>
<td>52.8</td>
<td>80</td>
<td>-42.2</td>
<td>92</td>
<td>-30</td>
<td>87</td>
<td>-23.6</td>
<td>95</td>
<td>-21.8</td>
<td></td>
</tr>
<tr>
<td>133</td>
<td>21.4</td>
<td>139</td>
<td>19.6</td>
<td>137</td>
<td>19.8</td>
<td>88</td>
<td>-20.2</td>
<td>151</td>
<td>28.8</td>
<td>163</td>
<td>41</td>
<td>130</td>
<td>19.4</td>
<td>99</td>
<td>-17.8</td>
<td></td>
</tr>
<tr>
<td>82</td>
<td>-29.6</td>
<td>110</td>
<td>-9.4</td>
<td>147</td>
<td>29.8</td>
<td>85</td>
<td>-23.2</td>
<td>166</td>
<td>43.8</td>
<td>133</td>
<td>11</td>
<td>80</td>
<td>-30.6</td>
<td>143</td>
<td>26.2</td>
<td></td>
</tr>
<tr>
<td>164</td>
<td>52.4</td>
<td>80</td>
<td>-39.4</td>
<td>126</td>
<td>8.8</td>
<td>126</td>
<td>17.8</td>
<td>120</td>
<td>-2.2</td>
<td>81</td>
<td>-41</td>
<td>92</td>
<td>-18.6</td>
<td>83</td>
<td>-33.8</td>
<td></td>
</tr>
<tr>
<td>93</td>
<td>-18.6</td>
<td>170</td>
<td>50.6</td>
<td>83</td>
<td>-34.2</td>
<td>81</td>
<td>-27.2</td>
<td>94</td>
<td>-28.2</td>
<td>141</td>
<td>19</td>
<td>164</td>
<td>53.4</td>
<td>164</td>
<td>47.2</td>
<td></td>
</tr>
</tbody>
</table>

**Total:** 111.6 35.64 119.4 35.51 117.2 27.90 108.2 34.61 122.2 36.50 122 34.44 110.6 35.59 116.8 34.82

<table>
<thead>
<tr>
<th></th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
<th>x</th>
<th>x_{i} - x_{avg}</th>
</tr>
</thead>
<tbody>
<tr>
<td>154</td>
<td>39.4</td>
<td>160</td>
<td>43.6</td>
<td>81</td>
<td>-27.8</td>
<td>168</td>
<td>38.4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>-17.6</td>
<td>100</td>
<td>-16.4</td>
<td>152</td>
<td>43.2</td>
<td>100</td>
<td>-29.6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>146</td>
<td>31.4</td>
<td>80</td>
<td>-36.4</td>
<td>83</td>
<td>-25.8</td>
<td>129</td>
<td>-0.6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>-34.6</td>
<td>150</td>
<td>33.6</td>
<td>133</td>
<td>24.2</td>
<td>94</td>
<td>-35.6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>96</td>
<td>-18.6</td>
<td>92</td>
<td>-24.4</td>
<td>95</td>
<td>-13.8</td>
<td>157</td>
<td>27.4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Total:** 114.6 33.13 116.4 36.12 108.8 31.94 129.6 33.05

**Total:** 118.00 35.40

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers. Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B21: Mean and Standard Deviation Values for Delay Times (T_{Delay}) in seconds – Break Ceiling

<table>
<thead>
<tr>
<th>x</th>
<th>x_{i - x_{avg}}</th>
<th>x</th>
<th>x_{i - x_{avg}}</th>
<th>x</th>
<th>x_{i - x_{avg}}</th>
<th>x</th>
<th>x_{i - x_{avg}}</th>
<th>x</th>
<th>x_{i - x_{avg}}</th>
<th>x</th>
<th>x_{i - x_{avg}}</th>
<th>x</th>
<th>x_{i - x_{avg}}</th>
</tr>
</thead>
<tbody>
<tr>
<td>55</td>
<td>-27.8</td>
<td>104</td>
<td>19.8</td>
<td>57</td>
<td>-22.8</td>
<td>65</td>
<td>-18.2</td>
<td>56</td>
<td>-24.8</td>
<td>93</td>
<td>10.8</td>
<td>68</td>
<td>-19</td>
</tr>
<tr>
<td>97</td>
<td>14.2</td>
<td>71</td>
<td>-13.2</td>
<td>116</td>
<td>36.2</td>
<td>97</td>
<td>13.8</td>
<td>66</td>
<td>-14.8</td>
<td>74</td>
<td>-8.2</td>
<td>112</td>
<td>25</td>
</tr>
<tr>
<td>125</td>
<td>42.2</td>
<td>69</td>
<td>-15.2</td>
<td>64</td>
<td>-15.8</td>
<td>59</td>
<td>-24.2</td>
<td>71</td>
<td>-9.8</td>
<td>68</td>
<td>-14.2</td>
<td>55</td>
<td>-32</td>
</tr>
<tr>
<td>70</td>
<td>-12.8</td>
<td>119</td>
<td>34.8</td>
<td>70</td>
<td>-9.8</td>
<td>121</td>
<td>37.8</td>
<td>92</td>
<td>11.2</td>
<td>57</td>
<td>-25.2</td>
<td>118</td>
<td>31</td>
</tr>
<tr>
<td>82.8</td>
<td>28.15</td>
<td>84.2</td>
<td>25.96</td>
<td>79.8</td>
<td>24.11</td>
<td>83.2</td>
<td>25.60</td>
<td>80.8</td>
<td>25.07</td>
<td>82.2</td>
<td>24.37</td>
<td>87</td>
<td>27.37</td>
</tr>
<tr>
<td>63</td>
<td>-16.2</td>
<td>90</td>
<td>11</td>
<td>62</td>
<td>-11.8</td>
<td>57</td>
<td>-24.6</td>
<td>73</td>
<td>-3.6</td>
<td>62</td>
<td>-16.6</td>
<td>64</td>
<td>-9.4</td>
</tr>
<tr>
<td>114</td>
<td>34.8</td>
<td>117</td>
<td>38</td>
<td>69</td>
<td>4.8</td>
<td>74</td>
<td>7.6</td>
<td>68</td>
<td>8.6</td>
<td>56</td>
<td>22.6</td>
<td>70</td>
<td>-3.4</td>
</tr>
<tr>
<td>70</td>
<td>-9.2</td>
<td>59</td>
<td>-20</td>
<td>112</td>
<td>38.2</td>
<td>96</td>
<td>14.4</td>
<td>58</td>
<td>18.6</td>
<td>115</td>
<td>36.4</td>
<td>60</td>
<td>-13.4</td>
</tr>
<tr>
<td>55</td>
<td>-24.2</td>
<td>69</td>
<td>-10</td>
<td>56</td>
<td>-17.8</td>
<td>117</td>
<td>35.4</td>
<td>118</td>
<td>41.4</td>
<td>66</td>
<td>-12.6</td>
<td>63</td>
<td>-10.4</td>
</tr>
<tr>
<td>94</td>
<td>14.8</td>
<td>60</td>
<td>-19</td>
<td>70</td>
<td>3.8</td>
<td>64</td>
<td>17.6</td>
<td>66</td>
<td>10.6</td>
<td>94</td>
<td>15.4</td>
<td>110</td>
<td>36.6</td>
</tr>
<tr>
<td>79.2</td>
<td>24.30</td>
<td>79</td>
<td>24.63</td>
<td>73.8</td>
<td>22.10</td>
<td>81.6</td>
<td>24.66</td>
<td>76.6</td>
<td>23.77</td>
<td>78.6</td>
<td>25.04</td>
<td>73.4</td>
<td>20.78</td>
</tr>
<tr>
<td>63</td>
<td>-17.4</td>
<td>65</td>
<td>-14</td>
<td>80</td>
<td>0.2</td>
<td>71</td>
<td>-4.8</td>
<td>68</td>
<td>-12.2</td>
<td>61</td>
<td>-14.8</td>
<td>111</td>
<td>35.2</td>
</tr>
<tr>
<td>98</td>
<td>17.6</td>
<td>71</td>
<td>-8</td>
<td>70</td>
<td>0.6</td>
<td>111</td>
<td>35.2</td>
<td>68</td>
<td>-12.2</td>
<td>61</td>
<td>-14.8</td>
<td>111</td>
<td>35.2</td>
</tr>
<tr>
<td>64</td>
<td>-16.4</td>
<td>81</td>
<td>2</td>
<td>68</td>
<td>-12.2</td>
<td>61</td>
<td>-14.8</td>
<td>64</td>
<td>-15.2</td>
<td>72</td>
<td>-3.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>111</td>
<td>30.6</td>
<td>116</td>
<td>37</td>
<td>118</td>
<td>37.8</td>
<td>64</td>
<td>11.8</td>
<td>66</td>
<td>14.4</td>
<td>64</td>
<td>21.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>66</td>
<td>-14.4</td>
<td>62</td>
<td>-17</td>
<td>65</td>
<td>-15.2</td>
<td>72</td>
<td>-3.8</td>
<td>64</td>
<td>21.4</td>
<td>64</td>
<td>21.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>80.4</td>
<td>22.50</td>
<td>79</td>
<td>21.92</td>
<td>80.2</td>
<td>21.87</td>
<td>75.8</td>
<td>20.22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers
Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution

212
<table>
<thead>
<tr>
<th>X</th>
<th>x_i - X_avg</th>
<th>X</th>
<th>x_i - X_avg</th>
<th>X</th>
<th>x_i - X_avg</th>
<th>X</th>
<th>x_i - X_avg</th>
<th>X</th>
<th>x_i - X_avg</th>
<th>X</th>
<th>x_i - X_avg</th>
</tr>
</thead>
<tbody>
<tr>
<td>188</td>
<td>-146.8</td>
<td>183</td>
<td>-137.8</td>
<td>315</td>
<td>10.8</td>
<td>276</td>
<td>-39.4</td>
<td>410</td>
<td>96.4</td>
<td>226</td>
<td>-63.8</td>
</tr>
<tr>
<td>275</td>
<td>-59.8</td>
<td>442</td>
<td>121.2</td>
<td>477</td>
<td>151.2</td>
<td>348</td>
<td>32.6</td>
<td>319</td>
<td>5.4</td>
<td>440</td>
<td>150.2</td>
</tr>
<tr>
<td>377</td>
<td>42.2</td>
<td>339</td>
<td>18.2</td>
<td>355</td>
<td>29.2</td>
<td>445</td>
<td>129.6</td>
<td>381</td>
<td>67.4</td>
<td>192</td>
<td>-97.8</td>
</tr>
<tr>
<td>480</td>
<td>145.2</td>
<td>299</td>
<td>-21.8</td>
<td>193</td>
<td>-132.8</td>
<td>190</td>
<td>-125.4</td>
<td>194</td>
<td>-119.6</td>
<td>341</td>
<td>51.2</td>
</tr>
<tr>
<td>354</td>
<td>19.2</td>
<td>341</td>
<td>20.2</td>
<td>289</td>
<td>-36.8</td>
<td>318</td>
<td>2.6</td>
<td>264</td>
<td>-49.6</td>
<td>250</td>
<td>-39.8</td>
</tr>
<tr>
<td>334.8</td>
<td><strong>109.95</strong></td>
<td>320.8</td>
<td><strong>93.40</strong></td>
<td>325.8</td>
<td><strong>103.47</strong></td>
<td>315.4</td>
<td><strong>93.73</strong></td>
<td>313.6</td>
<td><strong>87.51</strong></td>
<td>289.8</td>
<td><strong>100.50</strong></td>
</tr>
<tr>
<td>433</td>
<td>109.2</td>
<td>411</td>
<td>100</td>
<td>324</td>
<td>-18.8</td>
<td>381</td>
<td>45.4</td>
<td>325</td>
<td>2.4</td>
<td>437</td>
<td>106</td>
</tr>
<tr>
<td>254</td>
<td>-69.8</td>
<td>320</td>
<td>9</td>
<td>419</td>
<td>76.2</td>
<td>457</td>
<td>121.4</td>
<td>478</td>
<td>155.4</td>
<td>320</td>
<td>-11</td>
</tr>
<tr>
<td>314</td>
<td>-9.8</td>
<td>344</td>
<td>33</td>
<td>344</td>
<td>1.2</td>
<td>351</td>
<td>15.4</td>
<td>291</td>
<td>-31.6</td>
<td>419</td>
<td>88</td>
</tr>
<tr>
<td>409</td>
<td>85.2</td>
<td>229</td>
<td>-82</td>
<td>400</td>
<td>57.2</td>
<td>272</td>
<td>-63.6</td>
<td>331</td>
<td>8.4</td>
<td>284</td>
<td>-47</td>
</tr>
<tr>
<td>209</td>
<td>-114.8</td>
<td>251</td>
<td>-60</td>
<td>227</td>
<td>-115.8</td>
<td>217</td>
<td>-118.6</td>
<td>188</td>
<td>-134.6</td>
<td>195</td>
<td>-136</td>
</tr>
<tr>
<td>323.8</td>
<td><strong>96.61</strong></td>
<td>311</td>
<td><strong>73.30</strong></td>
<td>342.8</td>
<td><strong>75.57</strong></td>
<td>335.6</td>
<td><strong>93.74</strong></td>
<td>322.6</td>
<td><strong>104.09</strong></td>
<td>331</td>
<td><strong>99.76</strong></td>
</tr>
<tr>
<td>347</td>
<td>32.2</td>
<td>391</td>
<td>65.6</td>
<td>447</td>
<td>122.4</td>
<td>307</td>
<td>-8</td>
<td>164</td>
<td>96</td>
<td>437</td>
<td>105.75</td>
</tr>
<tr>
<td>317</td>
<td>2.2</td>
<td>233</td>
<td>-92.4</td>
<td>323</td>
<td>-1.6</td>
<td>388</td>
<td>73</td>
<td>199</td>
<td>-115.8</td>
<td>189</td>
<td>-135.6</td>
</tr>
<tr>
<td>314.8</td>
<td><strong>109.85</strong></td>
<td>325.4</td>
<td><strong>105.75</strong></td>
<td>324.6</td>
<td><strong>124.78</strong></td>
<td>315</td>
<td><strong>121.87</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers.Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B23: Mean and Standard Deviation Values for Delay Times ($T_{\text{Delay}}$) in seconds – Remove Roof

<table>
<thead>
<tr>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - \bar{x}_{\text{avg}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>215</td>
<td>-106.2</td>
<td>427</td>
<td>137.2</td>
<td>258</td>
<td>-53.6</td>
<td>347</td>
<td>60.4</td>
<td>245</td>
<td>-58.4</td>
<td>235</td>
<td>-78.8</td>
<td>315</td>
<td>11.2</td>
</tr>
<tr>
<td>433</td>
<td>111.8</td>
<td>331</td>
<td>41.2</td>
<td>249</td>
<td>-62.6</td>
<td>230</td>
<td>-56.6</td>
<td>305</td>
<td>1.6</td>
<td>310</td>
<td>-3.8</td>
<td>450</td>
<td>146.2</td>
</tr>
<tr>
<td>236</td>
<td>-85.2</td>
<td>213</td>
<td>-76.8</td>
<td>435</td>
<td>123.4</td>
<td>405</td>
<td>118.4</td>
<td>262</td>
<td>-41.4</td>
<td>433</td>
<td>119.2</td>
<td>230</td>
<td>-40.4</td>
</tr>
<tr>
<td>416</td>
<td>94.8</td>
<td>237</td>
<td>-52.8</td>
<td>235</td>
<td>-76.6</td>
<td>251</td>
<td>-52.4</td>
<td>245</td>
<td>36.8</td>
<td>238</td>
<td>-65.8</td>
<td>234</td>
<td>-55.8</td>
</tr>
<tr>
<td>306</td>
<td>-15.2</td>
<td>241</td>
<td>-48.8</td>
<td>381</td>
<td>69.4</td>
<td>241</td>
<td>-45.6</td>
<td>454</td>
<td>150.6</td>
<td>346</td>
<td>32.2</td>
<td>283</td>
<td>-20.8</td>
</tr>
<tr>
<td>321.2</td>
<td><strong>100.32</strong></td>
<td>289.8</td>
<td><strong>88.87</strong></td>
<td>311.6</td>
<td><strong>90.42</strong></td>
<td>286.6</td>
<td><strong>84.88</strong></td>
<td>303.4</td>
<td><strong>87.40</strong></td>
<td>313.8</td>
<td><strong>80.94</strong></td>
<td>303.8</td>
<td><strong>88.42</strong></td>
</tr>
<tr>
<td>431</td>
<td>128.2</td>
<td>400</td>
<td>89.2</td>
<td>322</td>
<td>15.2</td>
<td>351</td>
<td>55</td>
<td>237</td>
<td>-75.8</td>
<td>437</td>
<td>139.6</td>
<td>213</td>
<td>-106.2</td>
</tr>
<tr>
<td>210</td>
<td>-92.8</td>
<td>300</td>
<td>-10.8</td>
<td>302</td>
<td>-4.8</td>
<td>245</td>
<td>-51</td>
<td>391</td>
<td>78.2</td>
<td>250</td>
<td>-47.4</td>
<td>231</td>
<td>-88.2</td>
</tr>
<tr>
<td>267</td>
<td>-35.8</td>
<td>238</td>
<td>-72.8</td>
<td>234</td>
<td>-72.8</td>
<td>210</td>
<td>-86</td>
<td>240</td>
<td>-72.8</td>
<td>223</td>
<td>-74.4</td>
<td>320</td>
<td>0.8</td>
</tr>
<tr>
<td>234</td>
<td>-68.8</td>
<td>217</td>
<td>-93.8</td>
<td>455</td>
<td>148.2</td>
<td>441</td>
<td>145</td>
<td>433</td>
<td>120.2</td>
<td>342</td>
<td>44.6</td>
<td>376</td>
<td>56.8</td>
</tr>
<tr>
<td>372</td>
<td>69.2</td>
<td>399</td>
<td>88.2</td>
<td>221</td>
<td>-85.8</td>
<td>233</td>
<td>-63</td>
<td>263</td>
<td>-49.8</td>
<td>235</td>
<td>-62.4</td>
<td>456</td>
<td>136.8</td>
</tr>
<tr>
<td>302.8</td>
<td><strong>94.67</strong></td>
<td>310.8</td>
<td><strong>86.53</strong></td>
<td>306.8</td>
<td><strong>93.38</strong></td>
<td>296</td>
<td><strong>97.49</strong></td>
<td>312.8</td>
<td><strong>92.32</strong></td>
<td>297.4</td>
<td><strong>91.04</strong></td>
<td>319.2</td>
<td><strong>101.24</strong></td>
</tr>
<tr>
<td>247</td>
<td>-68.6</td>
<td>226</td>
<td>-90</td>
<td>345</td>
<td>18.2</td>
<td>237</td>
<td>-78.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>432</td>
<td>116.4</td>
<td>237</td>
<td>-79</td>
<td>412</td>
<td>85.2</td>
<td>452</td>
<td>136.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>254</td>
<td>-61.6</td>
<td>305</td>
<td>-11</td>
<td>229</td>
<td>-97.8</td>
<td>255</td>
<td>-60.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>420</td>
<td>104.4</td>
<td>370</td>
<td>54</td>
<td>422</td>
<td>95.2</td>
<td>413</td>
<td>97.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>225</td>
<td>-90.6</td>
<td>442</td>
<td>126</td>
<td>226</td>
<td>-100.8</td>
<td>222</td>
<td>-93.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>315.6</td>
<td><strong>101.44</strong></td>
<td>316</td>
<td><strong>91.18</strong></td>
<td>326.8</td>
<td><strong>95.37</strong></td>
<td>315.8</td>
<td><strong>108.05</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers. Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table B24: Mean and Standard Deviation Values for Delay Times ($T_{\text{Delay}}$) in seconds – Climb Building

<table>
<thead>
<tr>
<th>x</th>
<th>$x_i - x_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - x_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - x_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - x_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - x_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - x_{\text{avg}}$</th>
<th>x</th>
<th>$x_i - x_{\text{avg}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>48</td>
<td>13</td>
<td>43</td>
<td>7.8</td>
<td>35</td>
<td>0.6</td>
<td>47</td>
<td>12</td>
<td>22</td>
<td>-13.4</td>
<td>39</td>
<td>4</td>
<td>44</td>
<td>9.4</td>
</tr>
<tr>
<td>37</td>
<td>2</td>
<td>39</td>
<td>3.8</td>
<td>46</td>
<td>11.6</td>
<td>45</td>
<td>10</td>
<td>47</td>
<td>11.6</td>
<td>20</td>
<td>-15</td>
<td>25</td>
<td>-9.6</td>
</tr>
<tr>
<td>25</td>
<td>-10</td>
<td>22</td>
<td>-13.2</td>
<td>27</td>
<td>-7.4</td>
<td>37</td>
<td>2</td>
<td>48</td>
<td>12.6</td>
<td>29</td>
<td>-6</td>
<td>41</td>
<td>6.4</td>
</tr>
<tr>
<td>41</td>
<td>6</td>
<td>26</td>
<td>-9.2</td>
<td>39</td>
<td>4.6</td>
<td>26</td>
<td>-9</td>
<td>38</td>
<td>2.6</td>
<td>42</td>
<td>7</td>
<td>39</td>
<td>4.4</td>
</tr>
<tr>
<td>24</td>
<td>-11</td>
<td>46</td>
<td>10.8</td>
<td>25</td>
<td>-9.4</td>
<td>20</td>
<td>-15</td>
<td>22</td>
<td>-13.4</td>
<td>45</td>
<td>10</td>
<td>24</td>
<td>-10.6</td>
</tr>
<tr>
<td>35</td>
<td>10.37</td>
<td>35.2</td>
<td>10.62</td>
<td>34.4</td>
<td>8.65</td>
<td>35</td>
<td>11.77</td>
<td>35.4</td>
<td>12.84</td>
<td>35</td>
<td>10.32</td>
<td>34.6</td>
<td>9.40</td>
</tr>
<tr>
<td>40</td>
<td>4.4</td>
<td>26</td>
<td>-8.6</td>
<td>33</td>
<td>-4</td>
<td>22</td>
<td>-13.8</td>
<td>20</td>
<td>-14.8</td>
<td>43</td>
<td>8.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>-9.6</td>
<td>44</td>
<td>9.4</td>
<td>47</td>
<td>10</td>
<td>44</td>
<td>8.2</td>
<td>39</td>
<td>4.2</td>
<td>39</td>
<td>4.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>10.4</td>
<td>43</td>
<td>8.4</td>
<td>38</td>
<td>1</td>
<td>48</td>
<td>12.2</td>
<td>45</td>
<td>10.2</td>
<td>22</td>
<td>-12.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>-13.6</td>
<td>37</td>
<td>2.4</td>
<td>21</td>
<td>-16</td>
<td>24</td>
<td>-11.8</td>
<td>40</td>
<td>5.2</td>
<td>29</td>
<td>-5.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>8.4</td>
<td>23</td>
<td>-11.6</td>
<td>46</td>
<td>9</td>
<td>41</td>
<td>5.2</td>
<td>30</td>
<td>-4.8</td>
<td>40</td>
<td>5.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>35.6</td>
<td>10.90</td>
<td>34.6</td>
<td>9.66</td>
<td>37</td>
<td>10.65</td>
<td>35.8</td>
<td>11.97</td>
<td>34.8</td>
<td>9.88</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>-13.4</td>
<td>40</td>
<td>5.8</td>
<td>46</td>
<td>12.2</td>
<td>40</td>
<td>4.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>4.6</td>
<td>46</td>
<td>11.8</td>
<td>27</td>
<td>-6.8</td>
<td>38</td>
<td>2.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>10.6</td>
<td>23</td>
<td>-11.2</td>
<td>47</td>
<td>13.2</td>
<td>23</td>
<td>-12.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>-8.4</td>
<td>41</td>
<td>6.8</td>
<td>24</td>
<td>-9.8</td>
<td>34</td>
<td>-1.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>6.6</td>
<td>21</td>
<td>-13.2</td>
<td>25</td>
<td>-8.8</td>
<td>44</td>
<td>8.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>34.4</td>
<td>10.33</td>
<td>34.2</td>
<td>11.39</td>
<td>33.8</td>
<td>11.65</td>
<td>35.8</td>
<td>8.01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>35.10</td>
<td>10.53</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NB: Italicized values are Mean values of each set of numbers and bold values are Standard Deviation values for each set of numbers. Italicized and underlined value is the final Mean value for the entire distribution and bold and italicized value is the final Standard Deviation for the entire distribution.
Table C1: Identified Adversary Paths for Building F2C.

<table>
<thead>
<tr>
<th>Path 1C</th>
<th>Path 2C</th>
<th>Path 3C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
</tr>
<tr>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
</tr>
<tr>
<td>Open Outer Burglar Gate</td>
<td>Open Door 4</td>
<td>Open Door 3</td>
</tr>
<tr>
<td>Open Door 1</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
</tr>
<tr>
<td>Open Inner Burglar Gate</td>
<td>Run to Controlled Area</td>
<td>Run to Controlled Area</td>
</tr>
<tr>
<td>Walk through Maze</td>
<td>Open Inner Burglar Gate A</td>
<td>Open Inner Burglar Gate A</td>
</tr>
<tr>
<td>Remove or Sabotage Target</td>
<td>Open Door 2</td>
<td>Open Door 2</td>
</tr>
<tr>
<td></td>
<td>Walk through Maze</td>
<td>Walk through Maze</td>
</tr>
<tr>
<td></td>
<td>Remove or Sabotage Target</td>
<td>Remove or Sabotage Target</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Path 4C</th>
<th>Path 5C</th>
<th>Path 6C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
</tr>
<tr>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
</tr>
<tr>
<td>Remove Outer Window Bars</td>
<td>Open Door 10</td>
<td>Open Door 8</td>
</tr>
<tr>
<td>Break Window Glass</td>
<td>Break Wall</td>
<td>Remove Roof</td>
</tr>
<tr>
<td>Remove Inner Window Bars</td>
<td>Break Ceiling</td>
<td>Break Ceiling</td>
</tr>
<tr>
<td>Jump into Room</td>
<td>Jump into Room</td>
<td>Jump into Room</td>
</tr>
<tr>
<td>Run to Controlled Area</td>
<td>Walk through Maze</td>
<td>Walk through Maze</td>
</tr>
<tr>
<td>Open Inner Burglar Gate A</td>
<td>Remove or Sabotage Target</td>
<td>Remove or Sabotage Target</td>
</tr>
<tr>
<td></td>
<td>Open Door 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Walk through Maze</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remove or Sabotage Target</td>
<td></td>
</tr>
</tbody>
</table>
Table C2: Continuation of Identified Adversary Paths for Building F2C.

<table>
<thead>
<tr>
<th>Path 7C</th>
<th>Path 8C</th>
<th>Path 9C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
</tr>
<tr>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
</tr>
<tr>
<td>Open Door 3</td>
<td>Open Door 4</td>
<td>Open Door 4</td>
</tr>
<tr>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
</tr>
<tr>
<td>Run to Controlled Area</td>
<td>Run to Controlled Area</td>
<td>Run to Controlled Area</td>
</tr>
<tr>
<td>Open Door 7</td>
<td>Enter Wash Rooms</td>
<td>Open Inner Burglar Gate A</td>
</tr>
<tr>
<td>Break Double Ceiling</td>
<td>Break Double Ceiling</td>
<td>Open Door 5</td>
</tr>
<tr>
<td>Jump into Room</td>
<td>Jump into Room</td>
<td>Remove or Sabotage Target</td>
</tr>
<tr>
<td>Remove or Sabotage Target</td>
<td>Remove or Sabotage Target</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Path 10C</th>
<th>Path 11C</th>
<th>Path 12C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
</tr>
<tr>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
</tr>
<tr>
<td>Open Door 3</td>
<td>Remove Outer Window Bars</td>
<td>Break Window Glass</td>
</tr>
<tr>
<td>Open Inner Burglar Gate</td>
<td>Break Window Glass</td>
<td>Remove Inner Window Bars</td>
</tr>
<tr>
<td>Enter Wash Room</td>
<td>Remove Inner Window Bars</td>
<td>Jump into Room</td>
</tr>
<tr>
<td>Break Double Ceiling</td>
<td>Jump into Room</td>
<td>Walk through LAB</td>
</tr>
<tr>
<td>Jump into Room</td>
<td>Open Door 5</td>
<td>Remove Target</td>
</tr>
<tr>
<td>Remove or Sabotage Target</td>
<td>Open Door 2</td>
<td></td>
</tr>
<tr>
<td>Walk through Maze</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Path 13C</th>
<th>Path 14C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>Jump Fence</td>
</tr>
<tr>
<td>Run to Building</td>
<td>Run to Building</td>
</tr>
<tr>
<td>Open Door 10</td>
<td>Climb Building</td>
</tr>
<tr>
<td>Break Double Wall</td>
<td>Break Ceiling</td>
</tr>
<tr>
<td>Walk through Maze</td>
<td>Jump into Room</td>
</tr>
<tr>
<td>Remove or Sabotage Target</td>
<td>Walk through Maze</td>
</tr>
<tr>
<td></td>
<td>Remove or Sabotage Target</td>
</tr>
</tbody>
</table>
Table C3: Identified Adversary Paths for Building F2A.

<table>
<thead>
<tr>
<th>Path 1A</th>
<th>Path 2A</th>
<th>Path 3A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
</tr>
<tr>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
</tr>
<tr>
<td>Open Outer Burglar Gate</td>
<td>Remove Outer Window Bars</td>
<td>Remove Outer Window Bars</td>
</tr>
<tr>
<td>Open Door 1</td>
<td>Break Window Glass</td>
<td>Break Window Glass</td>
</tr>
<tr>
<td>Open Inner Burglar Gate</td>
<td>Remove Inner Window Bars</td>
<td>Remove Inner Window Bars</td>
</tr>
<tr>
<td>Jump Fence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Walk through LAB</td>
<td>Jump into Room</td>
<td>Jump into Room</td>
</tr>
<tr>
<td>Walk to Office G02</td>
<td>Walk through LAB</td>
<td>Open Door 4</td>
</tr>
<tr>
<td>Open Door 2</td>
<td>Remove Target</td>
<td>Walk to Office G07</td>
</tr>
<tr>
<td>Remove Target</td>
<td></td>
<td>Open Door 5</td>
</tr>
<tr>
<td>Path 5A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Path 4A</td>
<td>Jump Fence</td>
<td></td>
</tr>
<tr>
<td>Jump Fence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Run to Building</td>
<td>Open Outer Burglar Gate</td>
<td>Jump Fence</td>
</tr>
<tr>
<td>Open Outer Burglar Gate</td>
<td>Open Door 7</td>
<td>Run to Building</td>
</tr>
<tr>
<td>Open Door 1</td>
<td>Open Inner Burglar Gate</td>
<td>Open Outer Burglar Gate</td>
</tr>
<tr>
<td>Open Inner Burglar Gate</td>
<td>Open Door 6</td>
<td>Open Door 7</td>
</tr>
<tr>
<td>Walk to Door 6</td>
<td>Walk to Office G07</td>
<td>Open Inner Burglar Gate</td>
</tr>
<tr>
<td>Open Door 6</td>
<td>Open Door 5</td>
<td>Open Door 6</td>
</tr>
<tr>
<td>Run to Underground Room</td>
<td>Remove Target</td>
<td>Walk to Office G02</td>
</tr>
<tr>
<td>Remove Target</td>
<td></td>
<td>Open Door 2</td>
</tr>
<tr>
<td>Path 7A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Path 6A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jump Fence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Run to Building</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Outer Burglar Gate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Door 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Inner Burglar Gate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Door 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove Target</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table C4: Continuation of Identified Adversary Paths for Building F2A.

<table>
<thead>
<tr>
<th>Path 8A</th>
<th>Path 9A</th>
<th>Path 10A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
</tr>
<tr>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
</tr>
<tr>
<td>Open Outer Burglar Gate</td>
<td>Climb Building</td>
<td>Open Outer Burglar Gate</td>
</tr>
<tr>
<td>Open Door 1</td>
<td>Remove Roof</td>
<td>Open Door 7</td>
</tr>
<tr>
<td>Open Inner Burglar Gate</td>
<td>Break Ceiling</td>
<td>Open Inner Burglar Gate</td>
</tr>
<tr>
<td>Walk to Door 6</td>
<td>Jump into Room</td>
<td>Run to Underground Room</td>
</tr>
<tr>
<td>Open Door 6</td>
<td>Walk to Office G02</td>
<td>Remove Target</td>
</tr>
<tr>
<td>Open Door 8</td>
<td>Open Door 2</td>
<td></td>
</tr>
<tr>
<td>Remove Target</td>
<td>Remove Target</td>
<td></td>
</tr>
</tbody>
</table>

Table C5: Identified Adversary Paths for Building F2E.

<table>
<thead>
<tr>
<th>Path 1E</th>
<th>Path 2E</th>
<th>Path 3E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
</tr>
<tr>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
</tr>
<tr>
<td>Open Outer Burglar Gate</td>
<td>Open Outer Burglar Gate</td>
<td>Open Outer Burglar Gate</td>
</tr>
<tr>
<td>Open Door 9</td>
<td>Open Door 1</td>
<td>Open Door 11</td>
</tr>
<tr>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
</tr>
<tr>
<td>Open Door 8</td>
<td>Walk to Door 4</td>
<td>Walk to Office G11</td>
</tr>
<tr>
<td>Walk through LAB</td>
<td>Open Door 4</td>
<td>Open Door 10</td>
</tr>
<tr>
<td>Remove Target</td>
<td>Walk to Office G11</td>
<td>Remove Target</td>
</tr>
<tr>
<td></td>
<td>Open Door 10</td>
<td>Remove Target</td>
</tr>
<tr>
<td></td>
<td>Remove Target</td>
<td></td>
</tr>
</tbody>
</table>
Table C6: Continuation of Identified Adversary Paths for Building F2E.

<table>
<thead>
<tr>
<th>Path 4E</th>
<th>Path 5E</th>
<th>Path 6E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>Jump Fence</td>
<td>Jump Fence</td>
</tr>
<tr>
<td>Run to Building</td>
<td>Run to Building</td>
<td>Run to Building</td>
</tr>
<tr>
<td>Open Outer Burglar Gate</td>
<td>Open Outer Burglar Gate</td>
<td>Open Outer Burglar Gate</td>
</tr>
<tr>
<td>Open Door 11</td>
<td>Open Door 9</td>
<td>Open Door 12</td>
</tr>
<tr>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
<td>Open Inner Burglar Gate</td>
</tr>
<tr>
<td>Walk through LAB</td>
<td>Open Door 8</td>
<td>Open Door 13</td>
</tr>
<tr>
<td>Remove Target</td>
<td>Open Door 7</td>
<td>Walk through LAB</td>
</tr>
<tr>
<td></td>
<td>Open Door 6</td>
<td>Remove Target</td>
</tr>
</tbody>
</table>

Path 7E: Open Door 3

<table>
<thead>
<tr>
<th>Path 7E</th>
<th>Path 8E</th>
<th>Path 9E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>Remove Target</td>
<td>Jump Fence</td>
</tr>
<tr>
<td>Run to Building</td>
<td>Remove Target</td>
<td></td>
</tr>
<tr>
<td>Open Outer Burglar Gate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Door 1</td>
<td>Jump Fence</td>
<td>Run to Building</td>
</tr>
<tr>
<td>Open Inner Burglar Gate</td>
<td>Run to Building</td>
<td>Remove Inner Window Bars</td>
</tr>
<tr>
<td>Open Door 4</td>
<td>Open Outer Burglar Gate</td>
<td>Jump into Room</td>
</tr>
<tr>
<td>Walk to Office G12</td>
<td>Open Door 12</td>
<td>Walk to Door 4</td>
</tr>
<tr>
<td>Open Door 14</td>
<td>Open Inner Burglar Gate</td>
<td>Open Door 4</td>
</tr>
<tr>
<td>Remove Target</td>
<td>Open Door 13</td>
<td>Walk to Door 6</td>
</tr>
<tr>
<td></td>
<td>Walk to Door 4</td>
<td>Open Door 6</td>
</tr>
</tbody>
</table>

Path 10

<table>
<thead>
<tr>
<th>Path 10</th>
<th>Path 11</th>
<th>Path 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump Fence</td>
<td>Open Door 4</td>
<td>Open Door 7</td>
</tr>
<tr>
<td>Run to Building</td>
<td>Open Door 2</td>
<td>Remove Target</td>
</tr>
<tr>
<td>Climb Building</td>
<td>Remove Target</td>
<td></td>
</tr>
<tr>
<td>Remove Roof</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Break Ceiling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jump into Room</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Walk through LAB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove Target</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Figure D1: Neutralisation result for an activist, weapons and corresponding number of guards.

Figure D2: Neutralisation result for two activists, weapons and corresponding number of guards.

Figure D3: Neutralisation result for three activists, weapons, and corresponding number of guards.
**Figure D4**: Neutralisation result for an activist, weapons, and corresponding number of guards.

<table>
<thead>
<tr>
<th>Threats</th>
<th>Type</th>
<th>Number</th>
<th>Weapons</th>
<th>Delay (min/sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>activist</td>
<td>1</td>
<td>baton</td>
<td></td>
</tr>
</tbody>
</table>

**Guards**

<table>
<thead>
<tr>
<th>Type</th>
<th>Number</th>
<th>Weapons</th>
<th>Delay (min/sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st post</td>
<td>2</td>
<td>baton</td>
<td>10</td>
</tr>
<tr>
<td>2nd Alarm Response Team</td>
<td>1</td>
<td>baton</td>
<td>8</td>
</tr>
<tr>
<td>3rd Special Response Team</td>
<td>5</td>
<td>automatic rifle</td>
<td>5</td>
</tr>
<tr>
<td>4th Special Response Team</td>
<td>5</td>
<td>automatic rifle</td>
<td>8</td>
</tr>
<tr>
<td>5th Officer</td>
<td>5</td>
<td>automatic rifle</td>
<td>30</td>
</tr>
</tbody>
</table>

**Results**

<table>
<thead>
<tr>
<th>Probability of Neutralization:</th>
<th>Total Guards engaging:</th>
<th>Total Threats engaging:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.825</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

**Figure D5**: Neutralisation result for two activists, weapons, and corresponding number of guards.

<table>
<thead>
<tr>
<th>Threats</th>
<th>Type</th>
<th>Number</th>
<th>Weapons</th>
<th>Delay (min/sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>activist</td>
<td>2</td>
<td>baton</td>
<td></td>
</tr>
</tbody>
</table>

**Guards**

<table>
<thead>
<tr>
<th>Type</th>
<th>Number</th>
<th>Weapons</th>
<th>Delay (min/sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st post</td>
<td>2</td>
<td>baton</td>
<td>10</td>
</tr>
<tr>
<td>2nd Alarm Response Team</td>
<td>2</td>
<td>baton</td>
<td>8</td>
</tr>
<tr>
<td>3rd Special Response Team</td>
<td>5</td>
<td>automatic rifle</td>
<td>5</td>
</tr>
<tr>
<td>4th Special Response Team</td>
<td>5</td>
<td>automatic rifle</td>
<td>8</td>
</tr>
<tr>
<td>5th Officer</td>
<td>5</td>
<td>automatic rifle</td>
<td>30</td>
</tr>
</tbody>
</table>

**Results**

<table>
<thead>
<tr>
<th>Probability of Neutralization:</th>
<th>Total Guards engaging:</th>
<th>Total Threats engaging:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.825</td>
<td>4</td>
<td>2</td>
</tr>
</tbody>
</table>

**Figure D6**: Neutralisation result for three activists, weapons, and corresponding number of guards.

<table>
<thead>
<tr>
<th>Threats</th>
<th>Type</th>
<th>Number</th>
<th>Weapons</th>
<th>Delay (min/sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>activist</td>
<td>3</td>
<td>baton</td>
<td></td>
</tr>
</tbody>
</table>

**Guards**

<table>
<thead>
<tr>
<th>Type</th>
<th>Number</th>
<th>Weapons</th>
<th>Delay (min/sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st post</td>
<td>2</td>
<td>baton</td>
<td>10</td>
</tr>
<tr>
<td>2nd Alarm Response Team</td>
<td>3</td>
<td>baton</td>
<td>8</td>
</tr>
<tr>
<td>3rd Special Response Team</td>
<td>5</td>
<td>automatic rifle</td>
<td>5</td>
</tr>
<tr>
<td>4th Special Response Team</td>
<td>5</td>
<td>automatic rifle</td>
<td>8</td>
</tr>
<tr>
<td>5th Officer</td>
<td>5</td>
<td>automatic rifle</td>
<td>30</td>
</tr>
</tbody>
</table>

**Results**

<table>
<thead>
<tr>
<th>Probability of Neutralization:</th>
<th>Total Guards engaging:</th>
<th>Total Threats engaging:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.806</td>
<td>5</td>
<td>3</td>
</tr>
</tbody>
</table>
Figure D7: Neutralisation result for an activist, weapons, and corresponding number of guards.

Figure D8: Neutralisation result for two activists, weapons, and corresponding number of guards.

Figure D9: Neutralisation result for three activists, weapons, and corresponding number of guards.
Figure D10: Neutralisation result for an activist, weapons, and corresponding number of guards.

Figure D11: Neutralisation result for two activists, weapons, and corresponding number of guards.

Figure D12: Neutralisation result for three activists, weapons, and corresponding number of guards.
Figure D13: Neutralisation result for a criminal, weapons, and corresponding number of guards.

Figure D14: Neutralisation result for two criminals, weapons, and corresponding number of guards.

Figure D15: Neutralisation result for three criminals, weapons, and corresponding number of guards.
Figure D16: Neutralisation result for four criminals, weapons, and corresponding number of guards.

Figure D17: Neutralisation result for a criminal, weapons, and corresponding number of guards.

Figure D18: Neutralisation result for two criminals, weapons, and corresponding number of guards.
Figure D19: Neutralisation result for three criminals, weapons, and corresponding number of guards.

Figure D20: Neutralisation result for four criminals, weapons, and corresponding number of guards.

Figure D21: Neutralisation result for a criminal, weapons, and corresponding number of guards.
Figure D22: Neutralisation result for two criminals, weapons, and corresponding number of guards.

Figure D23: Neutralisation result for three criminals, weapons, and corresponding number of guards.

Figure D24: Neutralisation result for four criminals, weapons, and corresponding number of guards.
Figure D25: Neutralisation result for a terrorist, weapons, and corresponding number of guards.

Figure D26: Neutralisation result for two terrorists, weapons, and corresponding number of guards.

Figure D27: Neutralisation result for three terrorists, weapons, and corresponding number of guards.
Figure D28: Neutralisation result for four terrorists, weapons, and corresponding number of guards.

Figure D29: Neutralisation result for a terrorist, weapons, and corresponding number of guards.

Figure D30: Neutralisation result for two terrorists, weapons, and corresponding number of guards.
Figure D31: Neutralisation result for three terrorists, weapons, and corresponding number of guards.

<table>
<thead>
<tr>
<th>Threats</th>
<th>Type</th>
<th>Number</th>
<th>Weapons</th>
<th>Delay (min:sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>terrorist</td>
<td>3</td>
<td>pistol</td>
<td>11:25</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Guards</th>
<th>Type</th>
<th>Number</th>
<th>Weapons</th>
<th>Delay (min:sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>post</td>
<td>2</td>
<td>baton</td>
<td>2:30</td>
</tr>
<tr>
<td>2nd</td>
<td>Alarm Response Team</td>
<td>4</td>
<td>pistol</td>
<td>8:5</td>
</tr>
<tr>
<td>3rd</td>
<td>Special Response Team</td>
<td>1</td>
<td>automatic rifle</td>
<td>8:5</td>
</tr>
<tr>
<td>4th</td>
<td>Special Response Team</td>
<td>5</td>
<td>automatic rifle</td>
<td>8:20</td>
</tr>
<tr>
<td>5th</td>
<td>Officer</td>
<td>5</td>
<td>automatic rifle</td>
<td>30:0</td>
</tr>
</tbody>
</table>

Results

- Probability of Neutralization: 0.936
- Total Guards engaging: 7
- Total Threats engaging: 3

Figure D32: Neutralisation result for four terrorists, weapons, and corresponding number of guards.

<table>
<thead>
<tr>
<th>Threats</th>
<th>Type</th>
<th>Number</th>
<th>Weapons</th>
<th>Delay (min:sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>terrorist</td>
<td>4</td>
<td>pistol</td>
<td>11:15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Guards</th>
<th>Type</th>
<th>Number</th>
<th>Weapons</th>
<th>Delay (min:sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>post</td>
<td>2</td>
<td>baton</td>
<td>2:30</td>
</tr>
<tr>
<td>2nd</td>
<td>Alarm Response Team</td>
<td>5</td>
<td>pistol</td>
<td>8:5</td>
</tr>
<tr>
<td>3rd</td>
<td>Special Response Team</td>
<td>1</td>
<td>automatic rifle</td>
<td>8:5</td>
</tr>
<tr>
<td>4th</td>
<td>Special Response Team</td>
<td>5</td>
<td>automatic rifle</td>
<td>8:20</td>
</tr>
<tr>
<td>5th</td>
<td>Officer</td>
<td>5</td>
<td>automatic rifle</td>
<td>30:0</td>
</tr>
</tbody>
</table>

Results

- Probability of Neutralization: 0.903
- Total Guards engaging: 6
- Total Threats engaging: 4

Figure D33: Neutralisation result for a terrorists, weapons, and corresponding number of guards.

<table>
<thead>
<tr>
<th>Threats</th>
<th>Type</th>
<th>Number</th>
<th>Weapons</th>
<th>Delay (min:sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>terrorist</td>
<td>1</td>
<td>automatic rifle</td>
<td>13:50</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Guards</th>
<th>Type</th>
<th>Number</th>
<th>Weapons</th>
<th>Delay (min:sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>post</td>
<td>2</td>
<td>baton</td>
<td>2:30</td>
</tr>
<tr>
<td>2nd</td>
<td>Alarm Response Team</td>
<td>2</td>
<td>pistol</td>
<td>8:5</td>
</tr>
<tr>
<td>3rd</td>
<td>Special Response Team</td>
<td>1</td>
<td>automatic rifle</td>
<td>8:5</td>
</tr>
<tr>
<td>4th</td>
<td>Special Response Team</td>
<td>5</td>
<td>automatic rifle</td>
<td>8:20</td>
</tr>
<tr>
<td>5th</td>
<td>Officer</td>
<td>5</td>
<td>automatic rifle</td>
<td>30:0</td>
</tr>
</tbody>
</table>

Results

- Probability of Neutralization: 0.922
- Total Guards engaging: 5
- Total Threats engaging: 1
Figure D34: Neutralisation result for two terrorists, weapons, and corresponding number of guards.

<table>
<thead>
<tr>
<th>Threats</th>
<th>Number</th>
<th>Weapons</th>
<th>Delay (min:sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
<td>automatic rifle</td>
<td>11</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Guards</th>
<th>Type</th>
<th>Number</th>
<th>Weapons</th>
<th>Delay (min:sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>post</td>
<td>2</td>
<td>baton</td>
<td>20</td>
</tr>
<tr>
<td>2nd</td>
<td>Alarm Response Team</td>
<td>3</td>
<td>pistol</td>
<td>20</td>
</tr>
<tr>
<td>3rd</td>
<td>Special Response Team</td>
<td>3</td>
<td>automatic rifle</td>
<td>20</td>
</tr>
<tr>
<td>4th</td>
<td>Special Response Team</td>
<td>3</td>
<td>automatic rifle</td>
<td>20</td>
</tr>
<tr>
<td>5th</td>
<td>Offsite</td>
<td>3</td>
<td>automatic rifle</td>
<td>20</td>
</tr>
</tbody>
</table>

Results:
- Probability of Neutralization: 0.938
- Total Guards engaging: 7
- Total Threats engaging: 2

Figure D35: Neutralisation result for three terrorists, weapons, and corresponding number of guards.

<table>
<thead>
<tr>
<th>Threats</th>
<th>Number</th>
<th>Weapons</th>
<th>Delay (min:sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3</td>
<td>automatic rifle</td>
<td>11</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Guards</th>
<th>Type</th>
<th>Number</th>
<th>Weapons</th>
<th>Delay (min:sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>post</td>
<td>2</td>
<td>baton</td>
<td>20</td>
</tr>
<tr>
<td>2nd</td>
<td>Alarm Response Team</td>
<td>3</td>
<td>pistol</td>
<td>20</td>
</tr>
<tr>
<td>3rd</td>
<td>Special Response Team</td>
<td>3</td>
<td>automatic rifle</td>
<td>20</td>
</tr>
<tr>
<td>4th</td>
<td>Special Response Team</td>
<td>3</td>
<td>automatic rifle</td>
<td>20</td>
</tr>
<tr>
<td>5th</td>
<td>Offsite</td>
<td>3</td>
<td>automatic rifle</td>
<td>20</td>
</tr>
</tbody>
</table>

Results:
- Probability of Neutralization: 0.916
- Total Guards engaging: 8
- Total Threats engaging: 3

Figure D36: Neutralisation result for four terrorists, weapons, and corresponding number of guards.

<table>
<thead>
<tr>
<th>Threats</th>
<th>Number</th>
<th>Weapons</th>
<th>Delay (min:sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4</td>
<td>automatic rifle</td>
<td>10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Guards</th>
<th>Type</th>
<th>Number</th>
<th>Weapons</th>
<th>Delay (min:sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>post</td>
<td>2</td>
<td>baton</td>
<td>20</td>
</tr>
<tr>
<td>2nd</td>
<td>Alarm Response Team</td>
<td>3</td>
<td>pistol</td>
<td>20</td>
</tr>
<tr>
<td>3rd</td>
<td>Special Response Team</td>
<td>3</td>
<td>automatic rifle</td>
<td>20</td>
</tr>
<tr>
<td>4th</td>
<td>Special Response Team</td>
<td>3</td>
<td>automatic rifle</td>
<td>20</td>
</tr>
<tr>
<td>5th</td>
<td>Offsite</td>
<td>3</td>
<td>automatic rifle</td>
<td>20</td>
</tr>
</tbody>
</table>

Results:
- Probability of Neutralization: 0.972
- Total Guards engaging: 14
- Total Threats engaging: 4