IAEA TECDOC SERIES

IAEA-TECDOC-1868

Nuclear Security Assessment Methodologies for Regulated Facilities

Final Report of a Coordinated Research Project

IAEA
International Atomic Energy Agency

IAEA SAFETY STANDARDS AND RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish or adopt standards of safety for protection of health and minimization of danger to life and property, and to provide for the application of these standards.

The publications by means of which the IAEA establishes standards are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety. The publication categories in the series are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides**.

Information on the IAEA's safety standards programme is available on the IAEA Internet site

http://www-ns.iaea.org/standards/

The site provides the texts in English of published and draft safety standards. The texts of safety standards issued in Arabic, Chinese, French, Russian and Spanish, the IAEA Safety Glossary and a status report for safety standards under development are also available. For further information, please contact the IAEA at: Vienna International Centre, PO Box 100, 1400 Vienna, Austria.

All users of IAEA safety standards are invited to inform the IAEA of experience in their use (e.g. as a basis for national regulations, for safety reviews and for training courses) for the purpose of ensuring that they continue to meet users' needs. Information may be provided via the IAEA Internet site or by post, as above, or by email to Official.Mail@iaea.org.

RELATED PUBLICATIONS

The IAEA provides for the application of the standards and, under the terms of Articles III and VIII.C of its Statute, makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety in nuclear activities are issued as **Safety Reports**, which provide practical examples and detailed methods that can be used in support of the safety standards.

Other safety related IAEA publications are issued as **Emergency Preparedness and Response** publications, **Radiological Assessment Reports**, the International Nuclear Safety Group's **INSAG Reports**, **Technical Reports** and **TECDOCs**. The IAEA also issues reports on radiological accidents, training manuals and practical manuals, and other special safety related publications.

Security related publications are issued in the **IAEA Nuclear Security Series**.

The **IAEA Nuclear Energy Series** comprises informational publications to encourage and assist research on, and the development and practical application of, nuclear energy for peaceful purposes. It includes reports and guides on the status of and advances in technology, and on experience, good practices and practical examples in the areas of nuclear power, the nuclear fuel cycle, radioactive waste management and decommissioning.

NUCLEAR SECURITY ASSESSMENT METHODOLOGIES FOR REGULATED FACILITIES

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BARBADOS
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ESWATINI
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GRENADA
GUATEMALA
GUYANA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORTH MACEDONIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAINT LUCIA
SAINT VINCENT AND THE GRENADINES
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
TURKMENISTAN
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VANUATU
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world''.

IAEA-TECDOC-1868

NUCLEAR SECURITY ASSESSMENT METHODOLOGIES FOR REGULATED FACILITIES

FINAL REPORT OF A COORDINATED RESEARCH PROJECT

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2019

COPYRIGHT NOTICE

For further information on this publication, please contact:

Nuclear Security of Materials and Facilities Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Email: Official.Mail@iaea.org

Printed by the IAEA in Austria
April 2019

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Nuclear security assessment methodologies for regulated facilities / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2019. | Series: IAEA TECDOC series, ISSN 1011–4289 ; no. 1868 | Includes bibliographical references.
Identifiers: IAEAL 19-01228 | ISBN 978–92–0–101719–2 (paperback : alk. paper)
Subjects: LCSH: Nuclear industry — Security measures. | Nuclear facilities. | Mathematical models.

FOREWORD

Over the past 30 years, several Member States and organizations have developed nuclear security assessment methodologies and tools to provide assurance that regulated facility protection measures are effective against the threat as defined in the State's threat assessment or design basis threat. Over that period, as analysts have requested the ability to look at more detailed features of nuclear security systems, assessment tools have evolved from simple manual methods to complex modelling and simulation techniques. As these tools have become more complex, the types and amount of data required to conduct an assessment have also increased. Furthermore, as assessment tools and data requirements have evolved, the assessment methodologies themselves have also changed owing to the influence of evolving regulatory requirements of States. As a result, a wide variety of methodologies are in use today in different States, which has made it more difficult for States now embarking on a nuclear programme to decide which methodology and tools to use as part of their regulatory process. To provide Member States with a standard nuclear security assessment methodology and criteria to assist in assessment tool(s) selection, the IAEA recently concluded the coordinated research project (CRP) entitled Development of Nuclear Security Assessment Methodologies (NUSAM) for Regulated Facilities.

The objective of the CRP was to establish a standard risk informed, performance based methodological framework in a systematic, structured, comprehensive and appropriately transparent manner. The framework also had to meet two other requirements. First, it needed to be sufficiently flexible to enable assessment of the nuclear security of a wide range of nuclear and other radioactive materials, as well as associated facilities and activities under regulatory control. Second, any new approaches to nuclear security assessment included in the framework needed to be consistent with the recommendations and guidance provided in current IAEA Nuclear Security Series publications. The present publication includes a description of the completed NUSAM methodology as well as the results of applying that methodology to three case studies covering the following facilities and activities: a nuclear power plant, an irradiator facility and a radioactive material transport.

In accordance with broader IAEA objectives, the CRP also provided an environment for the sharing and transfer of knowledge and experience, and provided guidance on and practical examples of good practices in assessing the security of nuclear and other radioactive materials, as well as associated facilities and activities. The project began in 2013 and was completed in 2017. Two research coordination meetings were held in Vienna to review progress, the first in March 2014, chaired by J. Rivers (United States of America), and the second in June 2016, chaired by M. Snell (United States of America). Their leadership was essential to establishing a risk informed, performance based methodological framework at the IAEA and with the Member States.

The IAEA wishes to thank Member State experts for the organization of the CRP and for the preparation of this publication. The IAEA responsible officer for this publication was D. Shull of the Division of Nuclear Security.

EDITORIAL NOTE

This publication has been prepared from the original material as submitted by the contributors and has not been edited by the editorial staff of the IAEA. The views expressed remain the responsibility of the contributors and do not necessarily represent the views of the IAEA or its Member States.

Neither the IAEA nor its Member States assume any responsibility for consequences which may arise from the use of this publication. This publication does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

The authors are responsible for having obtained the necessary permission for the IAEA to reproduce, translate or use material from sources already protected by copyrights.

The IAEA has no responsibility for the persistence or accuracy of URLs for external or third party Internet web sites referred to in this publication and does not guarantee that any content on such web sites is, or will remain, accurate or appropriate.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

To provide Member States with a standard nuclear security assessment (SA) methodology and criteria to assist in assessment tool(s) selection, the International Atomic Energy Agency (IAEA) initiated a Coordinated Research Project (CRP), Nuclear Security Assessment Methodologies (NUSAM) for Regulated Facilities. The CRP was approved in 2012, began in 2013 and was concluded in 2017. This publication contains the results of the IAEA CRP NUSAM for Regulated Facilities.

1.2. OBJECTIVE

The objective of this publication is to describe a risk informed, performance based methodological framework in a systematic, structured, comprehensive and appropriately transparent manner. The framework could be used to assess the security of nuclear and other radioactive materials within regulatory control, as well as associated facilities and activities. While the NUSAM project explored new approaches to nuclear security assessment, the established framework is consistent with recommendations and guidance provided in current IAEA Nuclear Security Series (NSS) publications.

A secondary objective is to provide an environment for sharing and transferring knowledge and experience, and to provide guidance on, and practical examples of, good practices in assessing the security of nuclear and other radiological materials, as well as associated facilities and activities.

1.3. SCOPE

The methodology assesses the performance of a defined security process. The emphasis is on the methodological aspects of SA and is illustrated by the application of the methodological framework to three example facilities/activities. Facilities and activities of interest included are:

- Those associated with the nuclear fuel cycle;
- Nuclear power plants;
- Those associated with industry, medicine, research and agriculture, including research reactors that use radioactive/nuclear material;
- Those associated with the manufacture, distribution, storage and disposal of radioactive sources;
- Those used for radioactive/nuclear material predisposal and disposition waste management on the short term (e.g. 5–10 years), medium term (e.g. 10–50 years), and long term (e.g. 50–100 years);
- The transport of nuclear and radioactive material.

The NUSAM methodology was applied to three case studies that include the following facilities/activities: a nuclear power plant, an irradiator facility, and a radioactive material transport. The case studies were selected with the expectation that the set of these three case study reports and this publication could be used as a basis for successfully planning and performing an SA of the other facilities and activities on this list.

It is not appropriate to use this methodology where the security risks to materials and facilities are judged as requiring no more security than similar industrial and technological facilities that do not handle nuclear or radioactive materials.

1.4. STRUCTURE

This publication is an assessment methodology; it provides the tools and methods that can be used to assess security performance. It is intended to be a practical reference. Whenever possible, background information has been placed in Appendices to provide more detailed technical discussions and descriptions of different analysis methods. This publication contains two main sections and three

referenced case study publications Ref. [1-3] that were also developed as part of this CRP. The three case study publications are located on a CD-ROM attached to the back cover of this publication.

Section 2.1 provides an overview of the NUSAM Analysis Working Group Report

Section 2.2 provides an overview of the NUSAM methodological framework and process. An SA is described as a standalone project with three phases:

- Planning and preparation;
- Conducting;
- Analysis and reporting.

Section 2.3 discusses the planning requirements for an SA, provides suggestions on managing and controlling the process and introduces some of the test processes.

Section 2.4 discusses the information required for assessment and a process for collecting that information.

Section 2.5 describes and discusses the following three general steps for performing a performance based nuclear SA:

(1) Develop data libraries that indicate the effectiveness of the physical protection measures both individually and as part of systems and subsystems;
(2) Perform path analysis;
(3) Perform scenario analysis.

Section 2.5 further divides scenario analysis into four steps:

(1) Identify scenario sets to analyse;
(2) Develop detailed scenarios;
(3) Review and select final scenarios to evaluate;
(4) Determine effectiveness against final scenarios.

Section 2.6 discusses the overall assessment of security, including:

(1) Prescriptive requirements;
(2) Performance requirements;
(3) Combined assessments;
(4) A summary of assessment tools.

Section 2.7 discusses coordinated research project results and conclusions.

References in this publication provide links to important international publications, standards and other guidance publications relevant to NUSAM.

Appendices I-XIII to this publication provides detailed information concerning the methods and processes documented during the CRP.

2.0 ANALYSIS WORKING GROUP REPORT

2.1. METHODOLOGY OVERVIEW

While the regulatory process is an effective mechanism for developing and maintaining security standards, certain questions recur. This is in part due to differing judgements on the effectiveness of certain measures, in part due to no single security measure on its own will likely be wholly effective, and in part due to it not always being clear on how other measures compensate for any such deficiency. Some questions also arise because of the inevitable compromises that have to be made to accommodate conflicting priorities and because of the complexity of the systems involved. SAs are intended to ensure that security is effective, despite these difficulties.

This publication provides a methodology for a performance based assessment of security systems designed for the protection of nuclear and radiological materials and the processes that produce and/or involve them. This methodology is a risk informed approach and provides a performance based assessment for nuclear security in a systematic, structured, comprehensive and appropriately transparent manner. It is intended for use with both relatively simple installations and with highly regulated complex sites with demanding security requirements. The methodology gives quantitative and/or qualitative results. The methodology framework was developed as part of the NUSAM Coordinated Research Project conducted by the IAEA. Although the methodology is intended to be a practical reference, a SA needs to be understood in the context of regulation; may involve considerable management effort, resources and coordination; and will require expert knowledge and experience.

The methodology is intended to assist regulators and those with security accountabilities and responsibilities to produce a tested and coherent security regime with proven capabilities appropriate to the assets being protected and the threats being faced. Performance based SA is intended to inform users about the strengths and weaknesses of their security system and, at best, to demonstrate that the security measures and systems will work as intended if the threat reveals itself. Less complex security systems do not require as complex or resource intensive SAs.

While this publication describes the context for performance based SAs and outlines the management requirements, it focuses principally on expert methods and outputs. It is beyond the scope of this publication to go into the details of project management and the decision making processes.

The NUSAM methodological framework is consistent with recommendations, requirements and guidance provided in current IAEA Nuclear Security Series publications.

2.1.1. NUSAM summary

The NUSAM CRP held its first meeting in April 2013. Security experts from more than a dozen countries agreed to meet the challenge of developing a performance based, risk informed approach for assessing security effectiveness at a broad range of sites, facilities and activities. Facilities and activities of interest to the NUSAM CRP included those associated with:

- The nuclear fuel cycle;
- Nuclear power plants;
- Industry, medicine, research, and agriculture, including research reactors that use radioactive/nuclear material;
- The manufacture, distribution, storage and disposal of radioactive sources;
- The use for radioactive/nuclear material predisposal and disposition waste management for the short term (e.g. 5 to 10 years), medium term (e.g. 10 to 50 years) and long term (e.g. 50 to 100 years);
- The transport of nuclear and radioactive material.

The organizational structure of the NUSAM project is shown in Fig. 1. The overall project was managed by the Coordinating Group, consisting of the working group leaders, led by a chairperson and supported

by an IAEA Scientific Secretary. The Coordinating Group provided oversight and control of the scope of the project and ensured that the objectives of the project were achieved.

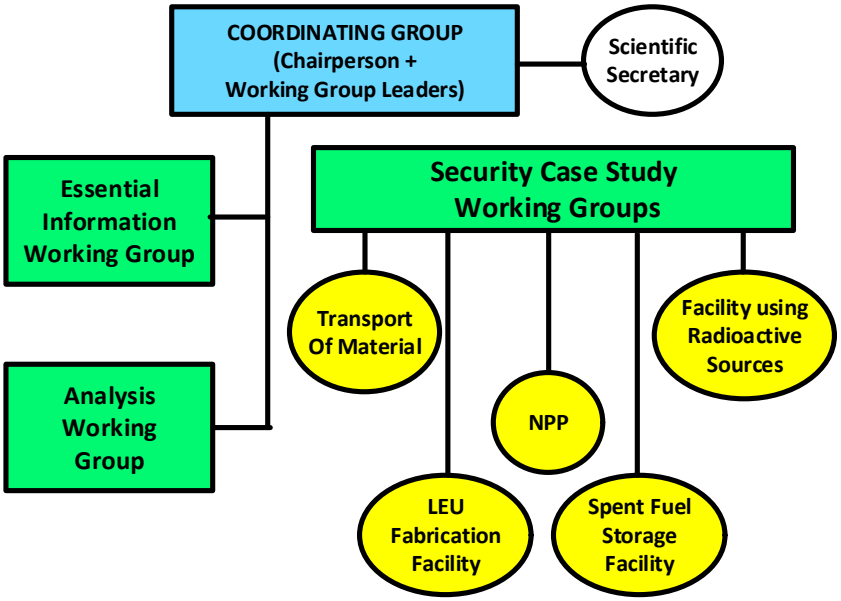


FIG. 1. The NUSAM organizational structure

The NUSAM project was comprised of the following working groups: The essential information working group, the analysis working group and the security case study working groups. Each working group included a leader and project participants.

Participants in the working groups:

- Participated in technical discussions and gave presentations describing the nuclear security assessment related work that they have undertaken within their own national programmes or related projects;
- Shared experiences regarding the content, development and use of nuclear security assessments in decision making through the life cycle of a facility/activity;
- Shared successes and challenges encountered;
- Provided reference information with regard to the approaches used;
- Provided feedback regarding concerns that were specific to the situation in their country or region;
- Contributed to the elaboration, review and improvement of project publications.

The NUSAM CRP developed and validated a methodological framework. It has identified the necessary data required to perform such an analysis, how to collect the data, and how to use it to assess security effectiveness at a range of facilities and activities. It has identified a variety of tools that can be used to implement NUSAM. Those tools range from semi-quantitative tools that assess security at facilities with predominantly prescriptive requirements to complex computerized modelling and simulation tools that address those sites that have performance or outcome based requirements.

The following security assessment methodological framework was proposed, developed and enhanced during the NUSAM project (see Fig. 2). This framework and its application are documented in more detail in the following sections.

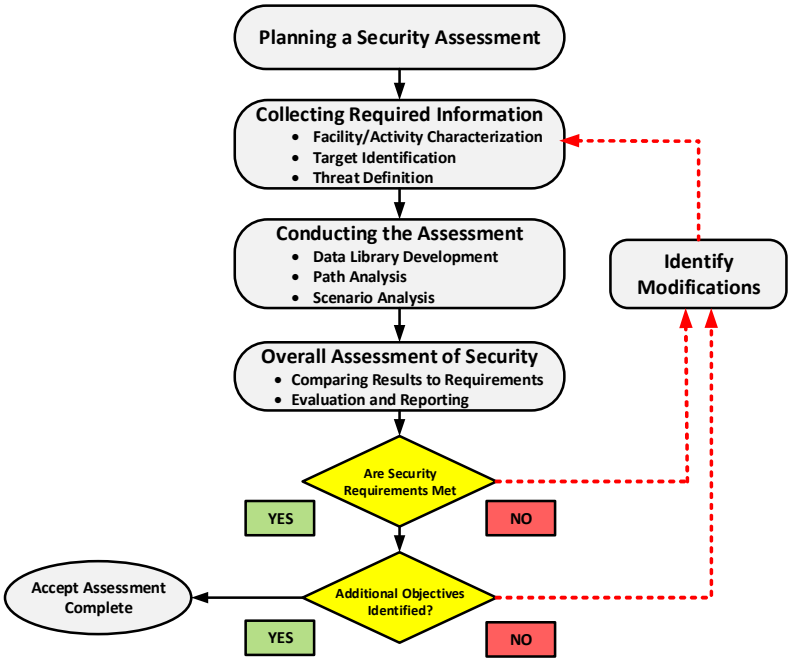


FIG. 2. The NUSAM methodological framework

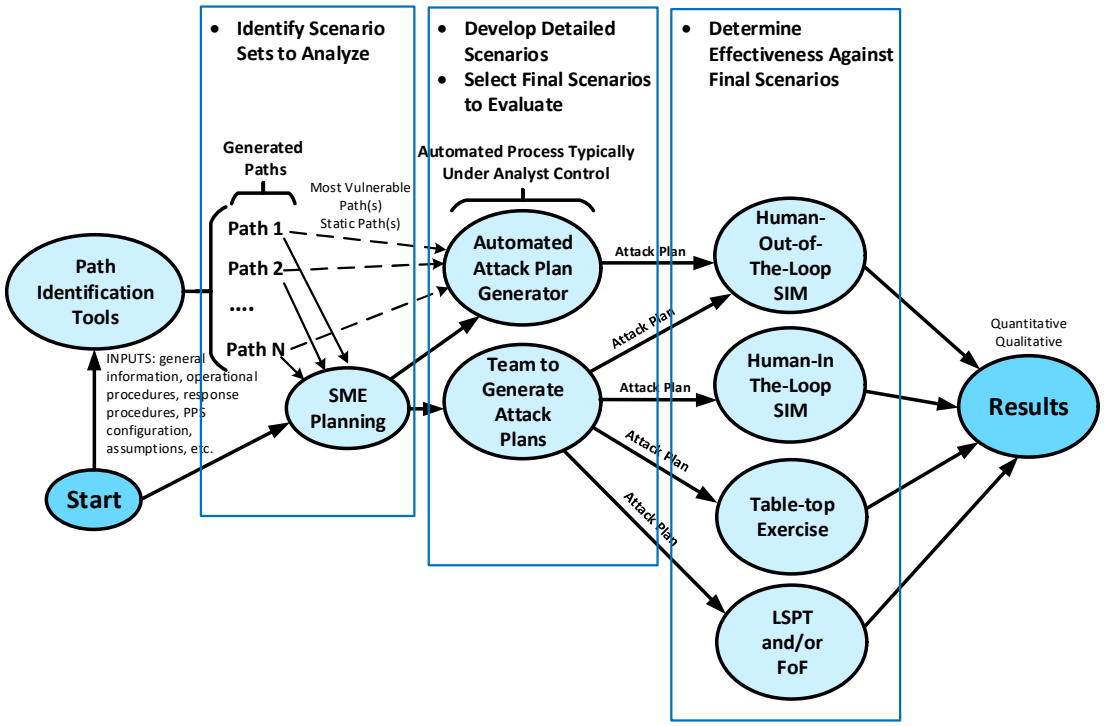
The NUSAM methodology and the associated tools were applied to three case studies that include the following facilities/activities: a nuclear power plant, an irradiator facility, and a radioactive material transport. The case studies were selected with the expectation that the set of these three case study reports and the analysis working group report could be used as a basis for successfully planning and performing a SA of the other facilities and activities on the facilities of interest list. Each case study used the NUSAM methodology to assess the effectiveness of the security arrangements using at least one or more assessment tools or methods.

2.1.2. Scenario analysis process

The sections of the analysis working group report align with the NUSAM Assessment Methodology process shown in Fig. 2.

The scenario analysis process for using software tools and evaluation methods is reflected in Fig. 3. The analysis process begins at the Start Node. If the tool or method uses a path analysis approach, the node ‘path identification tools’ would be highlighted along with the paths Path 1, Path 2, …, Path N. The description of the path can then be used by a subject matter expert (SME) to develop an adversary attack plan or can be used internally to the software to identify an adversary attack plan automatically. Some tools do nothing more than generate paths.

SME developed attack plans can be used in human in the loop simulations, TT exercises, force-on-force (FoF) exercises or as part of limited scope performance tests (LSPTs).



(Courtesy of M. Snell, Sandia National Laboratories)

FIG. 3. How scenario analysis steps correspond to the process for using software tools and evaluation methods

This section addresses a range of mathematical details supporting analysis, insider threat and TT analysis methods, and original research on how to quantify the probability of deterrence.

2.1.3. Comparison of tools

The software tools and methods used in this assessment are listed and compared in the Table 1 below:

TABLE 1. SOFTWARE AND TOOL COMPARISON

Software/Method Name	Tabletop*	VISA	SAVI	ProEv	STAGE	VEGA-2	Simajin	AVERT
Type (S = Software, M = Method)	M	M	S	S	S	S	S	S
Performs Path Analysis	Yes	Yes	Yes	Yes	Yes	Yes	Under development	Yes
Metrics Calculated: P_I	No	Yes	Yes	Yes	Yes	Yes	Under development	Yes
Performs Scenario Analysis	Yes	Yes	No	No	Yes	Yes	Yes	Yes
Metrics Calculated: P_N, P_E	P_N	P_N, P_E	No	No	Yes	Yes	Yes	Yes
Simulation	No	No	No	No	Yes	Yes	Yes	Yes
Human in the Loop					No	No	Yes	Yes
Human out of the Loop (Constructive)					Yes	Yes	Yes	Yes
Facility Representation								
Adversary Sequence Diagram (ASD)	No	Layer	Yes	No	No	No	No	No
Representation of Site and Building Floors	Yes	No	No	2D+	3D	2D + Floors	3D	3D
Path Network on representation Determined:	No	No	ASD	By Mixed Approach	By User	By Mixed Approach	Automatically	Automatically
Adversary Penetration Points on Barriers and Waypoints Are Determined:				Automatically or by user	By User	By User	Mixed	Automatically determined
Input Data								
Detection								
P_D Values	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed or Sampled	Sampled
Sensor/Camera Area Coverage Maps Represented	No	No	No	No	Yes	Yes	Yes	Yes
Delay values for barriers	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed or Sampled	Fixed or Sampled
Probability Hit/Probability Kill (P_H/P_K)	P_H/P_K	No	No	No	P_H/P_K	Physical	P_H/P_K	P_H/P_K
Patrol Routes	No	No	No	No	Yes	Yes	Yes	Yes

TABLE 1. SOFTWARE AND TOOL COMPARISON (CONT.)

Software/Method Name	Tabletop	VISA	SAVI	ProEv	STAGE	VEGA-2	Simajin	AVERT
Path Description	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Scenario Description	Yes	Yes	Tactics	Tactics	Yes	Tactics	Yes	Yes
Scenario Representation on Maps	Yes	No	No	Yes	Yes	Yes	Yes	Yes
Sampled Input Data	No	No	No	No	Yes	Yes	Yes	Yes
Replications performed for each set of input data	No	No	No	No	Yes	Yes	Yes	Yes
Data Analysis Tools	No	No	No	No	Yes	No	Yes	Yes

P_D	Probability of detection
P_E	Probability of system effectiveness
P_I	Probability of interruption
P_N	Probability of neutralization
P_H/P_K	Probability hit/probability kill

*: The tabletop methodology was included for comparative purposes against analysis results from the simulation tools.

Table 2 shows notes explaining the entries in Table 1.

TABLE 2. EXPLANATION OF ENTRIES FOUND TABLE 1 – SOFTWARE AND TOOL COMPARISON

FIELD	DEFINITION/EXPLANATION
Type (S = Software, M = Method)	Approach a method (implemented manually) or a software tool
PERFORMS PATH ANALYSIS	
Metrics Calculated (e.g., P_I)	P_I, Path Delay Time, Path Probability of Detection (P_D), P_N, and/or P_E
PERFORMS SCENARIO ANALYSIS	
Metrics Calculated (e.g., P_N, P_E)	See above
SIMULATION[1]	
Human in the Loop	Human operator makes decisions for and controls entities such as guards, adversaries, vehicles, cameras
Human out of the Loop (Constructive)	Program makes decisions for and controls entities
FACILITY REPRESENTATION	
Adversary Sequence Diagram (ASD)	
Representation of Site and Building Floors	2D means that the site is represented by layers, one being the site and facility ground level, and other layers representing floors. 3D means that buildings and terrain are modelled to some level of fidelity. 2D+ assumes that each 2D layer representation is accurate between adjacent layers (e.g., if floors 2 and 3 are at 10m and 15m, respectively, then the floor 2 layout is valid between 10m and 14.99m). 2D and 2D+ typically assume terrain is flat.
Path Network on representation of Site and Buildings Determined	Paths in 2D or 3D are defined on networks that consist of r nodes (typically specific locations where the adversary can go) and arcs allowing routes to travel between nodes. Nodes are defined by Penetration Points and Waypoints (see next item). Arcs can either be determined automatically by software, by the user, or in a 'mixed approach' where some arcs can be set automatically while the user typically defines others, for example, traversals between layers. ASDs represent the facility in terms of protection layers which otherwise have no association with specific facility locations.
Adversary Penetration Points on Barriers and Waypoints Are Determined	Approach used for placing these penetration points and waypoints for the adversary/defenders to move between. These points may be defined by the user, automatically, or a 'mixed approach' may be used where the user defines penetration points on barriers and the software automatically places waypoints at corners of objects such as walls or terrain obstacles so that entities can move around these objects when moving between penetration points.
INPUT DATA	
Detection	DEFINITION/EXPLANATION
P_D Values	Fixed or Sampled depending upon whether the value is a point values or sampled from a distribution
Sensor/Camera Area Coverage Maps Represented	Does the tool attempt to model the actual coverage map covered by the sensor and/or camera

[1] It should be noted since the conclusion of the NUSAM CRP that advancements in simulation based assessment platforms continue to progress in terms of increased: fidelity of combat simulation, automated capability, graphical representation/ output, and usefulness as VE training platforms.

TABLE 2. EXPLANATION OF ENTRIES FOUND TABLE 1 – SOFTWARE AND TOOL COMPARISON (CONT.)

FIELD	DEFINITION/EXPLANATION
RESULTS	
Delay values for barriers	Fixed or Sampled depending upon whether the value is a point values or sampled from a distribution
P_H/P_K	P_H/P_K =Probability of Hit, Probability of Kill (given hit); Physical = Model actual round fired.
Patrol Routes	Patrol routes specifically defined
Path Description	Yes = describes where the adversary group(s) went and what tactics they used; otherwise: Partial.
Scenario Description	Yes = Tool provides a description of the adversary attack plan (to some level of detail); otherwise: Partial.
Scenario Representation on Maps	Does the tool/approach result in a description of the scenario that specifies where the adversary group(s) go?
Sampled Input Data	Yes if input parameters such as P_D, delay values, response locations, and/or response times that are used in a software tool or method can be chosen (sampled) from probability distributions as opposed to just using point values; otherwise, No.
Replications performed for each set of input data	Two or more simulated adversary attacks are said to be replications if they are based on identical analysis assumptions and input variables are sampled from the same input distributions in such a way that all input variables are statistically independent (meaning that knowing the specific input variable values used in one simulated attack does not improve one's ability to predict the values used in another simulated attack). Yes means that multiple replications can be performed; otherwise, No.
Data Analysis Tools	Yes = Simulation/Method results can be stored in dedicated relational databases; otherwise, No. Note that such databases can then be queried using specialized database analysis and visualization tools to help understand the data.

2.1.4. NUSAM case studies

The security case study working groups developed detailed models of the facilities to demonstrate the use and applicability of the NUSAM methodological framework, along with the recommended information, tools and approaches developed by the methodological working groups. The development of security case studies provided a basis for discussion of the many practical issues encountered when undertaking a nuclear security assessment with the aim to reach broad consensus in as many areas as possible.

2.1.4.1. Nuclear power plants

This case study working group applied a number of assessment methods to a hypothetical nuclear power plant, the Lone Pine Nuclear Power Plant (LPNPP), located in a hypothetical country named the Republic of Lagassi. See Ref. [1].

Nuclear power plants (NPP) have very complex security systems and have potentially extreme consequences as a result of sabotage. They tend to have an on-site guard force, alarm stations and multiple layers of security and access controls.

Target analysis for NPPs is typically complicated because of the process to identify target sets that are combinations of nuclear safety systems that, if disabled, will result in an unacceptable radiological consequence. The target analysis for the LPNPP is not described in this publication; the targets to protect were assumed. Reference [1] includes a very detailed description of LPNPP and its physical protection system (PPS) which served as the basis for the assessment.

Reference [4] recommends performance based assessments of NPPs. To assess the performance of the LPNPP physical protection system, one manual method and seven software tools were used. Reference [1] describes each of these methods/tools, discusses how each was applied to the LPNPP, compares and contrasts them and provides some lessons learned from applying them. The process shown in Fig. 3 was developed based on the joint application of these tools.

No assessment was performed to evaluate the hypothetical LPNPP PPS against IAEA recommendations.

2.1.4.2. Medical irradiator facility

This case study working group applied a range of prescriptive and performance based assessment methodologies to several radiological targets at a hypothetical facility, the University Medical Centre, within a hypothetical country named the Republic of Lagassi. See Ref. [2].

Facilities using radioactive sources, such as medical facilities, are typically less protected than NPPs or sites dedicated to the use of Category I amounts of nuclear material (NM) owing to the smaller societal consequences of malicious acts associated with radioactive sources. For this reason, both prescriptive and performance based assessment methodologies were applied during this case study. The two prescriptive methods were a manual checklist and a software based qualitative tool. The software based qualitative tool compares security goals and objectives for different security levels against requirements for security functions (deterrence, detection, delay, response and security management) of the PPS. Three performance based assessment methods were applied: a simple timeline approach, a TT method and a modelling and simulation software tool.

The case study compares these methods in terms of several factors, including the costs and skills required to perform the assessment, complexity of the assessment, reproducibility of the results and transparency of the approach for checking input data, modelling assumptions and results.

For a facility using radioactive material, the presented methods appear to give realistic results that are considered reasonable.

This case study included eight appendices that describe the University Medical Centre, PPS, targets and hypothetical threat.

The NUSAM project team also performed an experimental manual TT exercise for the University Medical Centre remotely.[2] Despite this limitation, the working group determined that the TT exercise for the irradiator facility was performed effectively. The success of this experiment demonstrates the effectiveness of current communications capabilities to apply these methods.

2.1.4.3. Transport of material

This case study working group applied two manual TT assessment methods to a hypothetical transport of a Category 1 radioactive source via road between two hypothetical sites set in a hypothetical country named the Republic of Lagassi. See Ref. [3].

Transport of radioactive materials poses a different challenge for security than fixed sites containing these materials. While in transport, the adversary can choose any location on the transportation route to attack the transport vehicle and either sabotage the material or steal it. An important part of this case study was determining the set of scenarios to use for evaluation to address both unauthorized removal and sabotage while covering the range of possible attack locations and threat characteristics included in the hypothetical Design Basis Threat (DBT).

---

[2] This was a novel use of this method. TTXs are usually performed with all participants in the same location. The NPP and material transport case studies were not performed remotely.

Reference [3] includes a detailed description of the hypothetical transportation security plan for protecting the shipment. It also documents two manual, performance based TT methodologies: The Oak Ridge National Laboratory (ORNL) "BattleBoard" Tabletop (BattleBoard) Methodology and the Sandia National Laboratories (SNL) Tabletop Exercise (TTX) Methodology, along with the details comprising these methodologies. Despite identified differences in the details, both TT methodologies provided results that were comparable in terms of system wins or losses.

No assessment was performed to evaluate the hypothetical transportation security plan against IAEA recommendations.

2.1.5. Coordinated research project results and conclusions

After three years, the NUSAM CRP has developed and validated a methodological framework. It has identified the necessary data required to perform such an analysis, how to collect the data, and how to use it to assess security effectiveness at a range of facilities and activities. It has identified a variety of tools that can be used to implement NUSAM. Those tools range from semi-quantitative tools that assess security at facilities with predominantly prescriptive requirements to complex computerized modelling and simulation tools that address sites that have performance or outcome based requirements.

In order to test the methodology and the associated tools, the project undertook three hypothetical case studies: a nuclear power plant (NPP) which was developed from example facilities used in IAEA training activities Ref. [1], a medical irradiator facility Ref. [2], and a Category 1 radioactive sources in transit Ref. [3]. Each case study used the NUSAM methodology to assess the effectiveness of the security arrangements using at least one of the assessment tools or methods.

Table 3 summarizes the methods and tools used for the NUSAM CRP case studies. TT exercises were performed for each case study. In addition, the NPP case study was provided to two external vendors who modelled the facility and performed their SAs. These demonstrated how different modelling techniques may produce non-identical results, but are generally consistent in their overall outcomes.

TABLE 3. METHODS AND TOOLS USED FOR THE NUSAM CRP CASE STUDIES

Methods and tools	NPP	Irradiator facility	Transport
Path analysis	X	X	
Computer simulations	X	X	
Tabletops	X	X	X
Checklist		X	

The conclusion of this study revealed that different analysis techniques produce generally consistent results using the NUSAM methodology. Since each type of tool, or analysis technique, has strengths and weaknesses, several tools could be used in a complementary fashion during an assessment to take advantage of the strengths and offset the weaknesses of each type of tool.

The NUSAM project went beyond just developing a strategic methodology by testing the methodology against hypothetical facilities based on realistic situations. The fully documented case studies for a wide range of facilities and activities will be of value for training, specialist skills development and implementation guidance. These case studies validated the use of various analysis tools and methods and the overall NUSAM methodology.

The NUSAM CRP can be considered a success as it met the project objectives and has provided a validated approach for the assessment of security arrangements at a variety of sites, facilities and activities. Section 2.7 provides additional detail concerning the project results and conclusions.

2.1.6. Coordinated research project suggestions for future activities

Based on the successful results of the CRP, three suggestions for future actions were provided for consideration:

The first suggestion is for the development of two methodological publications. One publication could formalize the overall NUSAM methodology for Member State use in higher level facilities assessments and the other publication would address lower level facilities (i.e. irradiator facility) assessments.

The second suggestion is for the development of two additional case studies as described in the original CRP scope. One could consider a low enriched uranium fabrication facility and the other could consider a spent fuel storage facility. Both case studies may be useful for Member State reference for these types of regulated facilities.

The third suggestion is for the NUSAM methodology to be applied during the conduct of the CRP for Nuclear Security for Research Reactors and Associated Facilities (RRAFs).

2.1.7. Using the methodology

An SA is a standalone project with three phases: (1) planning and preparation, (2) conducting and (3) analysis and reporting.

In principle, the methodology is as appropriate to assessing the performance of security surrounding a single source. Carrying out an SA needs to be manageable by such a small undertaking. However, in a complex facility, an SA is likely to be a major undertaking. It often requires considerable information gathering and assessment, detailed planning and extensive resources. Both the decisions to adopt the methodology and to proceed are matters for senior management. It is suggested that the development phase of the assessment leading to a decision to proceed, and the practical assessment, be regarded as a major project requiring appropriate project management expertise and would need to be resourced accordingly.

An SA is not intended to show that certain systems or components do not work. That function is performed through routine maintenance and can be considered as part of the site's own security management and is included in regulatory compliance checks. In general, less will be understood from an SA carried out on a security system already known not to meet regulatory requirements.

2.1.8. Assessments recommended in IAEA publications

This section provides a list of citations that recommends the conduct of evaluations (i.e. assessments) to ensure the effectiveness of a facility's nuclear security measures.

Para. 3.9 of Ref. [5] describes the use of a risk informed approach as an essential element. The risk can be evaluated through SA combined with threat and consequence assessment. The following paragraphs of Ref. [5] also emphasize evaluations:

- Para. 3.3(e), "…evaluating applications and granting *authorizations* or licenses";
- Para. 3.11(b), "Periodically exercising, testing, and evaluating the plans for effectiveness by relevant *competent authorities* and *authorized persons* with the aim of ensuring timely implementation of comprehensive measures";
- Para. 3.12 (e), "Routinely conducting maintenance, training and evaluation to ensure the effectiveness of the *nuclear security systems*."

The following paragraphs of Ref. [4] emphasize evaluations and performance testing:

- Para. 3.13, "The State should ensure that evaluations include exercises to test the *physical protection system,* including the training and readiness of *guards* and/or *response forces*."
- Para. 3.21, "…the State's *competent authority* should ensure that evaluations based on *performance testing* are conducted by *operators* at *nuclear facilities* and, as appropriate, by *shippers* and/or carriers for *transport*. Evaluations should be reviewed by the State's *competent authority*, and should include administrative and technical measures, such as testing of *detection*, assessment, delay and communications systems and reviews of the implementation of physical protection procedures. When deficiencies are identified, the *competent authority* should ensure that corrective action is taken by the *operator, shipper* and/or carrier."

- Para. 3.29, "The *operator* should develop and implement means and procedures for evaluations, including *performance testing* and maintenance of the *physical protection system*."
- Para. 4.35, "Evaluations, including *performance testing*, of the *physical protection measures* and of the *physical protection system*, including timely response of the *guards* and *response forces* should be conducted regularly to determine reliability and effectiveness against the *threat*. These should be carried out with full cooperation between the *operator* and *response forces*. Significant deficiencies and action taken should be reported as stipulated by the *competent authority*."
- Para. 4.49, "*Guards* and *response forces* should provide an effective and timely response to prevent an adversary from completing the *unauthorized removal*. At least annually, *performance testing* of the *physical protection system* should include appropriate exercises, for example *force-on-force exercises*, to determine if the *guards* and the *response forces* can reach this objective."
- Para. 5.41, "Evaluations, including *performance testing*, of the *physical protection measures* and of the *physical protection system*, including timely response of the *guards* and *response forces* should be conducted regularly to determine reliability and effectiveness against the t*hreat*. These should be carried out with full cooperation between the *operator* and *response forces*. *Performance testing* of the *physical protection system* should include appropriate exercises, for example *force-on-force exercises*, to determine if the *response forces* can provide an effective and timely response to prevent *sabotage*. Significant deficiencies and action taken should be reported as stipulated by the *competent authority*."

Paragraph 4.7 of Ref. [6] states:

- "The regulatory body should select a regulatory approach that the operator must follow to meet the required goals and objectives. There are three alternative approaches that the regulatory body may use:
  - A prescriptive approach, in which the *regulatory body* directly specifies the security measures that the *operator* should implement to meet the goals and objectives, or
  - A performance based approach, in which the *regulatory body* requires the *operator* to design the *nuclear security system* and demonstrate to the *regulatory body* that the *nuclear security system* meets the goals and objectives, or
  - A combined approach, in which the *regulatory body* draws on elements of both the prescriptive and performance based approaches."

Two Implementing Guides (Refs [7, 8]) support the recommendation to use SA methodologies found in Ref. [4].

2.2. METHODOLOGICAL FRAMEWORK AND PROCESS

The methodology is an SA of a security system. Figure 2 provides a high level summary of the methodology and of the key milestones in an SA.

The security of nuclear and radiological materials and processes is subject to regulatory assessment and, if appropriate, regulatory oversight. This oversight is designed to ensure that the security system meets the required regulatory standards. This oversight cannot prove that the security system will work against a defined adversary even though that is the intention of the regulations. The starting point of the methodology is, therefore, the existing regulatory framework, policies and guidance on which the security system is based. If, as a result of the assessment, a security system is deemed insufficient, the assessor may consider that the failure may be, at least in part, in the regulations and not just their application.

The activities undertaken during the SA may usually be incorporated into a project plan or other planning document and may include the involvement of different internal or external organizations (see Section 2.3). The essential activities include:

- Deciding the purpose of the assessment and its target;
- Gathering relevant regulations, reports, etc.;
- Gathering any additional information;
- Defining the system to be tested;
- Defining the threat to be used in the scenario;
- Selecting the appropriate security performance test(s);
- Managing and conducting the assessment;
- Measuring and assessing the outcomes;
- Analysing and reporting the results;
- Assessing the implications for the system tested;
- Assessing the implications for the whole security system;
- Responding to the assessment (e.g. do nothing, take corrective measures and retest.).

Many of these steps require specific background information before they can be completed. The evaluation of this information may reveal security shortcomings that need to be addressed before carrying out an SA. Once the regulator is satisfied that regulatory requirements have been met, the SA can then be conducted by the operator. Most of the activity involved in completing the first three processes (understanding the regulations, collecting security relevant information, and evaluating the information) could be completed within normal operator/regulator interactions. However, preparing for an SA using a dedicated team for the purpose may create new insights.

A security and regulatory framework is based on a threat statement (TS) incorporated into regulatory policy. An SA requires a specific scenario (i.e. a description of adversary activity that is more specific than a TS yet is within the limits of the TS). A scenario is a specific and realistic example, albeit fictional, of the general statement of the threat. The SA evaluates the ability of the security system to protect the target from the adversary included in the scenario description. This evaluation draws on the precise description and boundaries of the security system under test. It is not a question of whether the adversary made some progress towards the target but rather if the adversary compromised the target by the successful completion of a malicious act.

2.3. PLANNING A SECURITY ASSESSMENT

This assessment methodology can be applied to evaluations of security measures against unauthorized removal and/or sabotage. The methodology is intended for use with fixed site facilities that handle, store, manage and/or transport nuclear and high activity radiological materials. This methodology can also be adapted for use at facilities where low activity radioactive materials and processes are used. Although not strictly part of the methodology, preparations for other considerations are also necessary to conduct a thorough SA.

2.3.1. Defining the purpose of the assessment

The primary purpose of a security based assessment is to determine if the applicable security requirements for the facility or activity are met. These requirements can be based on prescriptive requirements, performance requirements or a combination of both, as defined by the relevant competent authority or state body. In addition, the purpose of the assessment is to provide insight into the strengths and weaknesses of the physical protection system (PPS) under evaluation. If assessments repeatedly and consistently reveal the same or similar weaknesses in a security system, the results could suggest that the problems are general and best addressed at a strategic or governance level. Where weaknesses are identified, appropriate remedial actions can be taken to rectify the issue. The facility can then be reevaluated.

The license holder (operator/carrier) is responsible and accountable for the security of the facility and its materials. As such, an operator ensures that security measures, as well as being compliant with regulations, are genuinely appropriate and effective. Even if not a regulatory requirement, it is in the operator's interests to carry out periodic performance based SAs since these activities can provide business assurance and strengthen stakeholder confidence.

The competent authority may also wish to initiate SAs to ensure that the physical protection measures in place are effective. The purpose of these assessments is not to evaluate regulatory compliance, which are normally performed through periodic inspections. Both competent authority and the operator have a common interest in identifying which elements of the security system are effective; the operator is also interested in determining how efficient and cost effective these elements are.

It is important that the SA address the targets that have the highest potential radiological consequences or are most vulnerable. It is important to clearly define the principle purpose of the assessment. For example, is the intention to evaluate the PPS that an adversary may have to overcome, or is it to evaluate just the response to the adversary actions? The purpose of the assessment will determine what the evaluators will assess and the methods that they will use.

2.3.2. Identifying requirements for a security assessment

There is extensive documentation on the need for, and methods of achieving, the security of NM and processes from outsider threats (see Appendix I). Publications range from obligations included in International Conventions, to recommendations and guidance based on expert experience that may be available to any State organization. The regulations, policies, and guidelines applicable to a facility will determine the security objectives to be met and the type of assessment to be performed.

It is advisable the competent authority ensures that the current regulations in force in a State are appropriate and reflect both international standards and best practice. An SA takes place within that regulatory framework and there is likely to be a significant amount of preexisting information of direct relevance to the assessment. Nevertheless, it may be beneficial to draw on the wider range of publications detailed in Appendix I (e.g. whether an operator could use internationally accepted guidelines to support the interpretation of state level requirements). A regulator could benefit from the same material as a basis for testing the effectiveness of its regulation.

An SA, whether initiated by the competent authority or by the operator, is likely to clarify the purpose of the assessment and the target(s) to be assessed. These decisions will determine the regulatory basis for the assessment and will direct the assessment team towards:

- Appropriate security requirements and plans;
- Previous security inspection reports;
- Relevant safety and risk mitigation measures;
- Previous operator assessments and facility records.

This information will also direct the assessment team towards any issues which need particular investigation or reinvestigation, and towards the sort of adversary scenario(s) that might be the most informative. This process could be iterative and the purpose and target(s) of the assessment may change as information is acquired and the methods and tools chosen are identified.

The type of information specific to the assessment being conducted may also draw on other State policies and regulations. Some examples of the information to be considered include, but are not limited to:

- Provisions to prevent proliferation;
- Nuclear security laws and regulations;
- National/State threat assessment or design basis threat;
- Responsibilities and legal authority of respective competent authorities to fulfil their assigned roles;
- Nuclear security system requirements;

— Physical protection system requirements;

— Material accounting and control system requirements;

— Radiological/nuclear transport security requirements;

— Requirements for protection of the confidentiality of sensitive information and protecting sensitive information assets;

— Personnel trustworthiness requirements;

— Responsibilities of licensees and operators.

2.3.3. Management of a security assessment

An SA, particularly if it includes a full scope performance test, can be a major and costly project with potentially significant consequences for the operator and the competent authority. It is suggested that the SA be approved and overseen by an appropriate level of management that is responsible for acting on the outcomes of the assessment.

2.3.3.1. Security assessment management

An SA requires the same degree of rigorous management and planning as any other comparable project. This section proposes a project management approach for major SAs. Smaller assessments can be given the same logical approach but may not need such formalized structures. A hierarchy of oversight and control is suggested; Fig. 4 depicts one way to view the organization associated with an SA.

An SA is performed by a team consisting of one or more levels of security management, possibly including the Facility Security Manager for major assessments. This team may report to internal stakeholders (e.g. a board of directors or the facility manager), and may interact with external stakeholders (e.g. the competent authority or regulator). Specifically, it is suggested that an SA involving performance testing at the facility be coordinated with the facility performance testing organization that has the responsibility and authority for performing these tests. It is the project manager's responsibility to ensure that the assessment is performed safely and does not adversely affect facility or plant safety.

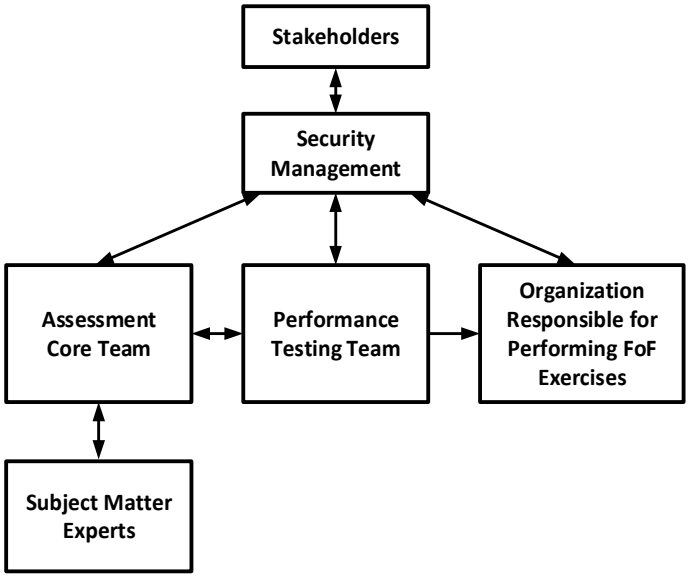


FIG. 4. Project control for security assessment

It is not reasonable to expect all assessment team members involved in an SA to have complete knowledge of all relevant requirements. Therefore, a core team will typically perform the assessment. This core team will have access to one or more subject matter experts (SMEs) either in relevant nuclear security domains or in supporting areas such as intelligence or facility safety. In a performance based assessment, the core team will interact with a performance testing group responsible for planning,

conducting and documenting appropriate limited scope performance test (LSPTs) to collect information such as task times and detection probabilities. If necessary, the assessment may require a FoF exercise, which is typically performed by a specialized group due to the cost and complexity of such exercises.

Clarifying roles is an essential element of an assessment because individuals may be exercising different levels of authority from those they exercise in normal circumstances.

It is suggested that the size and composition of the core team be commensurate with the facility size, complexity of the system(s) being assessed, and the areas to be addressed (such as nuclear material accounting and control, computer security, etc.).

Table 4 lists some examples of roles and expertise that core assessment team members and supporting SMEs may possess.

TABLE 4. EXAMPLE ROLES AND EXPERTISE FOR CORE ASSESSMENT TEAM MEMBERS

Core Team Members	Subject Matter Experts
Team leader (physical protection specialist)	Locksmith
Site/facility liaison member	Nuclear material accounting and control
Security system engineer	Assessment software specialist
Assessment analyst	Threat specialist
Operations representative	Safety representative
Response expert	Site/region security officer
Access delay/explosives expert	Security technicians
Alarm communication and display engineer	Security force personnel
	Construction/structural engineer
	Information technology administrators

2.3.3.2. Planning documents

To support the assessment, a number of planning documents and presentations may be developed:

- An approved work agreement describing the goal(s) of the assessment, an assessment security plan, the scope of the system(s) to be assessed, project management structure, the schedule, budget and resources required;
- An initial briefing to assessment participants describing the information in the work agreement as well as a briefing by assessment team leadership about assumptions used for the nuclear security systems being assessed;
- An assessment participant guide which provides guidance, processes and procedures for performing all phases of the assessment.

2.3.3.3. Security assessment security plan

The existing security plan for the facility or activity is to be evaluated to determine if it gives sufficient support for the purpose of planned assessment activities or if additional elements are necessary. The plan to protect sensitive and confidential information in compliance with security regulations and standards is an important element. Information security is also necessary to prevent unauthorized personnel from knowledge of no notice performance tests and exercises in order to reduce the likelihood of an adversary using the test as an opportunity to conceal or enhance a malicious activity. Further, whenever these tests and exercises are being executed at the facility, they are by nature, an attempt to overcome a facility's security system. However, the facility security effectiveness would need to be effectively maintained throughout the process. This will usually mean using supplementary measures. In particular, special attention needs to be paid to maintaining an effective security response capability and to ensuring that effective security is in place at all times during the assessment.

2.3.3.4. Defining the security assessment

An SA may be an assessment of the security of an entire facility. However, an assessment carried out in certain parts of a facility might be too operationally disruptive or too hazardous. In the interests of efficiency, economy and safety, it is advisable to precisely define the specific boundaries of the SA.

The boundaries of the SA need not correspond to a specific locale but could be a discrete part of the security system (e.g. personnel screening and access control). In such a case, it is imperative to decide the limits of the assessment. For example, it could include how the system responds to a mistake made in granting security clearance or it could include or exclude information security aspects of personnel screening. Similarly, if the SA needs to evaluate the effectiveness up to a particular vital area, the boundary of the assessment will stop at the vital area perimeter. However, decisions may also be necessary as to whether to include parts of distributed systems, such as alarm or access control systems, that are actually located within that vital area.

2.3.3.5. Resources

An effective assessment will demand funding, time and expertise. For the period while the assessment is taking place, it could have an impact on the normal activities of a facility. It is beyond the scope of this methodology to go into further detail, but managers may allocate resources and make provision for any disruptions caused by the assessment.

2.3.3.6. Assessment team guides

The assessment team develops a specific guide which can cover details such as:

- Skills, knowledge and attributes of the team members needed for the assessment team and how they will be selected. The size and composition of the team is dependent on the size and scope of the evaluation;
- Description of the processes and timeframes for acquiring sensitive site information and gaining access to the site;
- Gathering essential information data for the assessment;
- Assessment team management structure.

2.3.3.7. Assessment team management structure

It is advisable that an SA manager be assigned with the responsibility and authority to perform the assessment. Given that most assessments will take place at a facility, the assessment team will also require someone to coordinate with site management. It is the team manager's responsibility to ensure that the assessment activities are coordinated with the site in order to ensure safety is maintained at all times.

The planning of the SA will determine how unplanned external inputs are handled. For example, it may be difficult to determine whether the arrival of fire and rescue services was triggered from within the exercise, by someone outside the exercise who is unaware of it, or by a real event outside the exercise.

2.3.3.8. Assessment documentation

An SA is a complex, iterative and detailed process involving many areas of a facility and involving many people and decisions. It is highly suggested to document all of these factors as well as the uncertainties and assumptions taken into account during scenario development. The threat scoping document discussed in Section 2.4 is an example of such a document.

2.3.3.9. Assessment training

It is advisable that the assessment team involved in planning and performing an SA be trained on how to conduct the assessment according to the documents pertinent to the specific assessment and facility.

Training is also needed for others involved in the assessment, such as the SMEs and stakeholders, so that they understand the purpose of the assessment and their roles in it. It is important for all to understand that a performance based assessment depends upon their cooperation and openness to uncovering and discussing strengths and potential vulnerabilities of the PPS evaluated.

2.4. COLLECTING REQUIRED INFORMATION

Assessment of an effective nuclear security system includes the determination of the nuclear security system objectives, the proposed design or characterization of an existing nuclear security system, the evaluation of the design, and possibly a redesign or refinement of the system.

The process of collecting required information can be divided into four steps:

(1) The assessor begins by performing a facility/activity characterization which involves gathering information about facility/activity operations and conditions, such as a comprehensive description of the facility/activity, operating conditions and nuclear security requirements as well as regulatory requirements. The assessment considers the effectiveness of a system of elements that work together to ensure protection rather than regarding each element separately.

(2) The assessor identifies targets including vital areas based on information collected during facility/activity characterization. Determination of whether nuclear/radioactive materials are attractive targets is based mainly on the type of material and the ultimate goal of the adversary threat. This allows the assessor to know the objectives of the nuclear security system (what to protect against whom).

(3) The assessor defines the threat to be used for the assessment based upon policy as defined by the competent authority and upon other considerations such as local conditions and factors about potential adversaries including intent, motivation, types, capabilities and the range of tactics.

(4) The assessment includes data libraries that are collections of performance test data that can be used as a basis to justify nuclear security element probability of sensing, assessment and detection; delay times and response force (RF) times; and weapons effects for adversary and responders' weapons.

The first three steps generally apply to any type of SA. If the methodology for transportation security or protection of radiative sources is different, additional details are noted within each case study.

The last step concerning data libraries is discussed in Section 2.5 under performance testing.

Additional detail on developing data libraries is beyond the scope of this publication.

2.4.1. Facility/activity characterization

In order to perform a facility/activity characterization, the assessor begins by gathering information about the site. This information includes a **facility/activity description**: structural description of the facility; layout of physical boundaries including fences; building construction (i.e. walls, floors, ceiling, and roofs); internal building floor plans; material storage/activity areas; vital areas; personnel and vehicle access points; as well as windows, doors and other openings. Facility details may also include topography, weather and environmental conditions.

2.4.1.1. Description of the PPS and facility operations

The description of the **intrusion detection** and assessment system consists of sensor types and their locations (including their installation, maintenance and testing); protection of alarm communications lines; redundancy measures of alarm system; adequacy of lighting to assess alarms, assessment system and procedures; and measures for alarm reporting.

Access control descriptions include locations, configurations, types of access control measures, procedures and devices (including their installation, maintenance and testing), access control interface with guards, time and capability to assess access control alarms, methods of alarm assessment and resolution, and search systems.

The **barrier and delay element** descriptions can consist of location and types (including their installation, maintenance and testing), detection location with the respect to the delay and possible failure conditions (e.g. loss of power).

The **guards and response forces** description can consist of the initial personnel locations and deployment positions, types and numbers of guards and responders, their roles and training, weapons, equipment and their capabilities. Guard and response protection strategies as well as their assessment capabilities, communication and deployment times are included. Force-on-force and limited scope exercise reports can be reviewed for input.

Operational details collected would include **facility policies, procedures and training** of personnel to include nuclear security culture and human trustworthiness programmes and how these protection measures are applied for different facility conditions including operations during normal/night/holiday and emergency conditions including contingency plans. Computer security, information security procedures and nuclear material accounting and control procedures would need to be documented and understood, especially when considering protection measures against the insider threat and other mitigation measures.

It is important that **special procedures** for particular activities be addressed; for example, for maintenance activities when more individuals than usual may have access to security sensitive areas or for operational interactions of safety systems and controls (to include safety/security interface).

For the **security of radioactive sources**, the facility/process characterization described above would be similar but less complex as compared to the characterization of a nuclear power plant or nuclear fuel processing facility.

For **radioactive and nuclear material transportation activities**, this information can include modes of transportation such as rail, truck or vessel. For example, for truck transport, a description includes the type of vehicle and details such as open or closed cargo locations and hardened driver compartment. Security feature details include any locks and alarms, delay features, communications and vehicle tracking capabilities, and radioactive source packaging features such as tamper indicating devices or special closure details. Additional details may include drivers, escorts and guards, including local or regional police and response procedures and equipment. Procedures can also address pre-shipment inspections; normal operations; security incidents (especially for unplanned stops); confidentiality of information; command and control during normal and emergency conditions; non tactical and tactical emergency response and response times; incident communications and notification of relevant agencies and contingency plans. It is advisable that primary and secondary route selection (including the identification of safe havens) be documented and consider road quality, distances and other geographic and ergonomic factors.

Other transportation activities information may include movement and vehicle states. These states include those at the originating site for loading and site egress, urban and rural movement, planned stops, safe haven parking and protection, unplanned stops and destination site ingress and unloading. Figure 5 depicts some of these states that correspond to operating states for a nuclear facility (‘rolling’ refers to the shipment moving). Consideration can also include intermodal transportation combinations such as transfers between rail and vehicle.

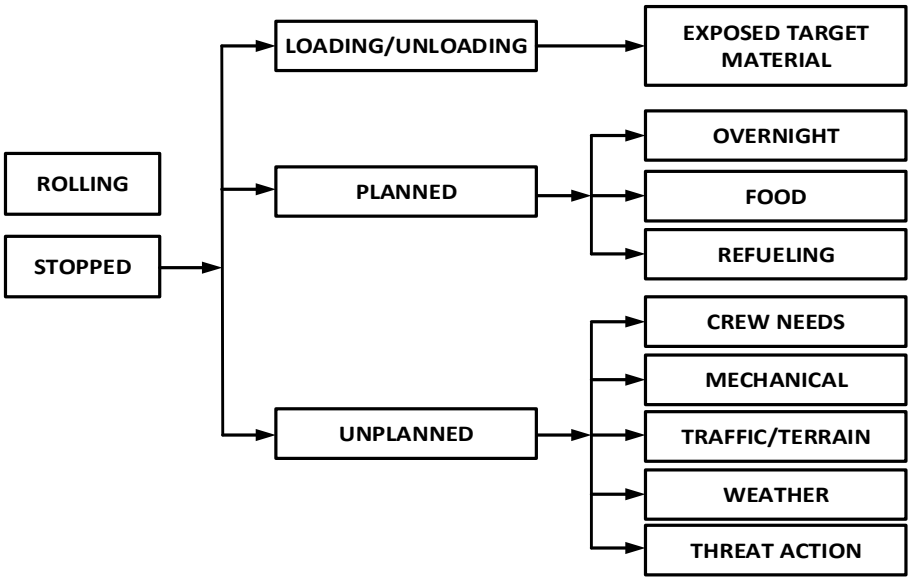


FIG. 5. Potential transportation states

There are various shipment combinations that include inter site and intra site transfers. Figure 6 represents these combinations which are considered, as necessary, during the assessment process.

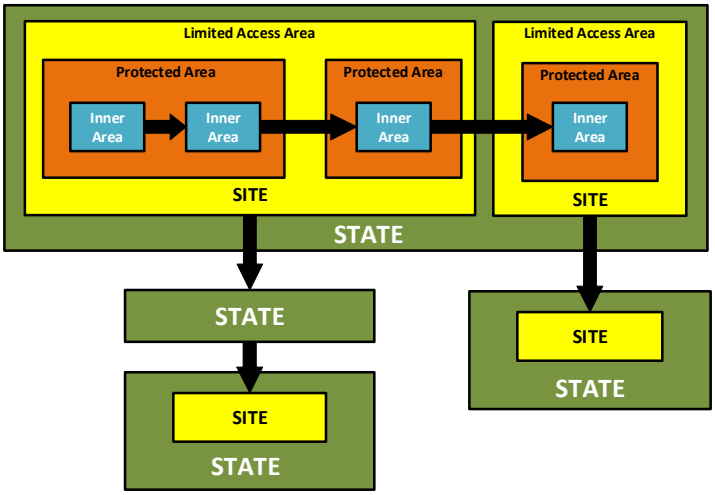


FIG. 6. Combinations of transportation origination points

Consider convoy configuration when collecting information for transportation. The effectiveness of physical protection for a shipment will also depend upon how many vehicles will be involved in the movement, how protected they are against adversary weapons as defined in the TA/DBT, and how vehicles in a convoy are configured (if more than one vehicle is involved), as shown in Fig. 7.

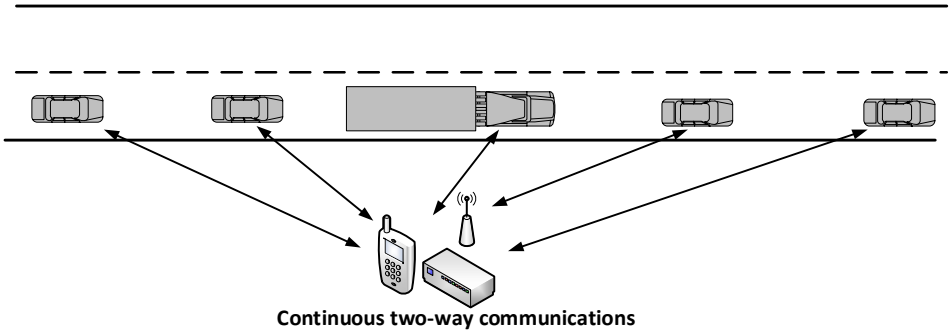


FIG. 7. Possible locations of vehicles in a convoy along a route

Relevant information for facility/activity characterization may be obtained from the following sources: facility or transportation security plans, facility surveys or walk downs, security and contingency plans and PPS test data.

2.4.1.2. Modelling environments – reorganize from simple to more complex environments

Modelling and simulation tools need some capability to create an environment depicting the physical and structural aspects of the nuclear facility, if any, and the topographic elements (e.g. roads, water features, and terrain) as appropriate for the model or simulation tool(s) applied.

For **manual methods**, such as TT and path analysis models, floor maps are typically adequate. Any type of file format, whether in vectored electronic files or in image or PDF files, are adequate.

For **complex modelling and simulation tools**, the topographic elements of the virtual environment (VE) typically require very precise information about the facility which can be gathered from existing geographic information system (GIS) databases along with satellite imagery (e.g. Google Earth, Bing Maps) that provide easy access to texture data to enhance the visual realism of the VE. If the facility has more current geographic information system and/or imagery data, this data can be utilized to improve the accuracy of the resulting VE. As defined above, the VE also includes the structural elements including the buildings and other structures, systems and components on the site. Data for these elements of the VE typically come from engineering drawings. Vectored electronic file formats for the drawings are preferred to eliminate errors and rework by enabling direct data importing.

Because a number of nuclear facilities were constructed some time ago, the analyst may face a situation where vectored electronic files are not available to support a software tool. In such cases, image or PDF files will need to be used, with an understanding that this approach will lengthen the time and cost needed to accurately generate the VE. Scanning technologies, such as light detection and ranging can also be used to assist in creating a VE. In such cases, manual post processing of the resulting 'point cloud' will be needed given that automated technologies that can convert this 'point cloud' to the required solid shapes of a VE are still in their infancy. Depending on the complexity of the facility, creation of a VE can take from two weeks to six months so careful scoping is suggested to ensure the focus is on producing the minimal VE that will support all decisions required of the analysis effort. For example, it is important to carefully weigh the amount of time and cost that will be needed to add visually appealing textures to the VE. Such textures can be impactful for communicating with stakeholders, but will have no impact on the quality of numerical results provided from the physical security modelling and simulation. Another significant factor to cost and schedule is the level of detail included in the VE for building interiors (e.g. floorplans). For some tools, careful attention is necessary to not eliminate features that can impact line of sight for the adversary or protective force or significantly impact the tactical situation during an attack. For example, if a feature does not contain an element of an adversary target set, it can be modelled as just a 'shell' with no interior details. This approach provides for proper line of sight impact from the feature while still allowing the feature to be used tactically (e.g. as a possible sniper position).

A common concern across different tools/methods is representing recent site construction such as new roads or buildings that does not show up on current drawings or electronic files but will impact the quality of the analysis. Site personnel from the engineering/planning organization can assist the assessment team by checking drawings or electronic files against actual construction and correcting drawings and files.

Once the VE is completed, it is then extended to represent the PPS design. Part of this representation includes identifying the location and orientation of the security design features within the current VE. This representation does not require knowledge of how each feature performs during the attack simulation. This guidance is particularly useful because a larger set of site personnel have the knowledge of where the detection, delay and response capabilities of the site are located, while knowledge of the specific performance characteristics (e.g. the likelihood of hit and kill for a particular weapon at a given range) of these capabilities is limited to a much smaller set of individuals.

It can be helpful to think of the VE creation as placing each individual instance of a design feature while the performance data library focuses on the performance of the design feature itself. For example, the site may have many video cameras of a particular make and model and from a specific manufacturer,

each of which needs to be placed on the VE, but only one set of performance data for this camera resides in the performance data library. It is suggested that all features in the PPS design be accounted for when creating the VE. The representation of this design is best split into the three required sections of any PPS—detection, delay and response.

Typically, the facility receives additional benefits from the creation of a physical protection VE beyond just the performance metrics, such as Probability of Interruption (P_I) or Probability of System Effectiveness (P_E), produced during the assessment. These benefits include an interactive communication tool for management and regulators, visualizing new design concepts prior to implementation, and a virtual TT exercise platform to support future TTs, particularly for sustaining protective force capabilities. One final suggestion when scoping and budgeting for initial VE development is to base the level of detail on the next fiscal year of physical protection decisions. Additions to this scope and budget can be made if some of the additional benefits described above are desired. A common mistake is to strive for an overly detailed VE from the beginning.

2.4.2. Target identification

The target is an essential element of the boundary conditions of the security system to be assessed. Defining the target will determine the threat and how the security system will be performance tested. Thus, the actual processes used to identify and evaluate targets can range from the simple to the very complex. The facility targets can include facility/activities, material unauthorized removal and/or material sabotage (direct or indirect targets) resulting in a radiological consequence. For additional information, refer to Refs [4, 7-10].

2.4.3. Threat definition

The assessment uses the threat and associated capabilities defined by the State's competent authority in the form of a TA and, if appropriate, a DBT. The TA or DBT articulates a detailed statement of the threat that draws on, and is bound by, the State's description of the threat considering the State's social, cultural and geopolitical conditions. Conducting a national TA and developing a DBT typically requires the combined efforts of domestic authorities such as intelligence and security agencies, law enforcement and regulatory bodies and operators. Reference [11] provides a detailed description of the information required, stakeholders to be included and process for conducting TA and developing the DBT. The threat description may include the overall State assessments of the significance of the threat from a range of adversaries for both outsider and insider threats (as described Ref. [12]).

The DBT is a tool used to help establish performance requirements for the design of physical protection systems for specific types of facilities or activities. Reference [4] recommends the use of the DBT for State's physical protection requirements related to unauthorized removal of Category I quantities of NM as well as sabotage of NM and nuclear facilities with high radiological consequence (HRC). However, the State may decide to use TA or DBT for other NM, radioactive material and associated facilities. Reference [11] also refers to a threat statement (TS), which is a policy document and can be used the same way as a DBT.

In order to do the assessment, a set of scenario classes is required (e.g. unauthorized removal and sabotage, threats considered from the TA/DBT, use, storage or transportation). In creating scenarios for the purpose of SA, a more detailed description of a specific adversary type may be necessary. Given the considerations built in to the TA/DBT, it is imperative that the threat capabilities for scenario purposes lie within the TA/DBT parameters. When moving from the State/competent authority level to the facility level, or from the facility level to the assessment level, detailed descriptions of the threat are typically required and require a larger policy component.

At the facility level shown in Fig. 8, the TA/DBT may be augmented by assumptions associated with the approved security plan concerning how the threat might be addressed. For example, there may be assumptions about whether the adversary has the expertise to disable certain safety systems or to find the right NM container in a hardened room.

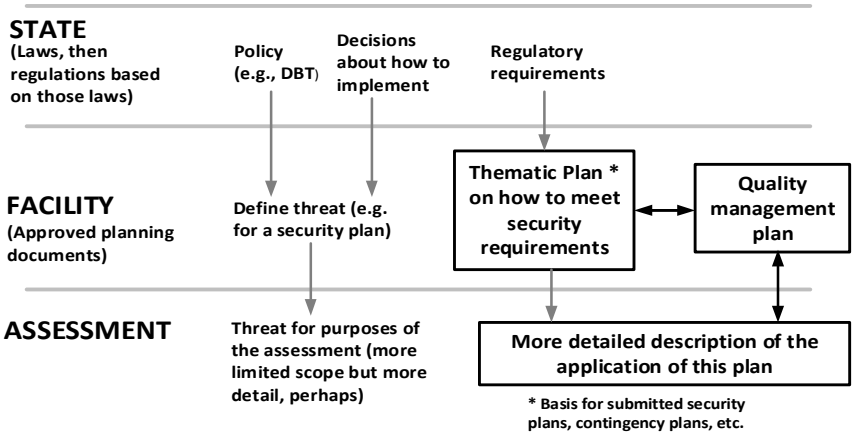


FIG. 8. Hierarchy of threat statements

At the assessment level in Fig. 8, it is advisable to apply adversary capabilities in an intelligent fashion during the evaluation to keep the scenarios credible.

For this reason, a scoping document can be developed at the assessment level to document assumptions, beyond those found in DBT policy documents, about how the threat will employ a particular capability during a scenario. Some of this extra detail can be collected from SMEs and some derived by technical standards developed by the competent authority on the employment of a certain type of adversary capability. For example, the DBT may allow the adversary to use a certain type of weapon, type of explosive, tool or tactic. Issues may arise during an assessment about whether the adversary would employ those capabilities. While there may be experts available to provide guidance on such matters, there may be differences of opinion between those experts or changes in the opinion of a single expert over time. In such cases, the competent authority may include guidance in the scoping document to help the evaluation team consistently select one type of capability and determine whether the novel use of such weapon, tool, explosive or tactic was credible.

There is strong evidence that many attackers are well prepared and have spent a considerable amount of effort in planning and preparation. If the target of concern is deep within a facility and well protected, it is unrealistic to plan a performance based SA based on the assumption that the adversary will be ill prepared. There may be good justification for including an ability to prepare in the threat description and SA. This will assess security effectiveness against covert attack techniques as well as the more usual tests of protection against overt attack. Where it is justified, there may be value in gaining more insight into the effectiveness of a security system, especially its deterrence value, by starting with attack preparation than by assuming that, as a starting condition, planning and preparation have already been completed (see Appendix XIII).

Consideration of insider threats provides insight on how active or passive insiders can perform malicious acts on their own or act in collusion with an outside adversary. These may not be the same as outsider actions. The insider may provide information that assists the outsider adversary in penetrating a security layer, or they may impact a protection mechanism to reduce its ability to detect or delay the adversary, to include removal of the layer from the security system.

2.4.4. Review of security plans and procedures

Security plans identify, describe and account for how the facility's specific security measures satisfy the regulatory requirements. Such plans provide part of the basis for licensing of the nuclear facility by the State and implementation of the security plan is a condition of the authorization to conduct operations at the nuclear facility. Therefore, a security plan describes in detail all aspects of the PPS implemented at that facility, and thus, may include information about the targets at the facility for either unauthorized removal or sabotage; descriptions and locations of security areas; physical protection measures in place and the insider threat mitigation programme. Details about security plans and suggested contents of a security plan can be found in Ref. [7] (see Ref. [6, 8 and 13] for additional information).

Security plans provide information about physical protection measures in place and may also serve as a context for the assessment by indicating what level of performance is needed to confirm that the State's physical protection requirements are being met when the plan is executed.

Security plans also serve as a basis for contingency plans and for implementing procedures. Reference [7] also lists suggested examples of contingency plans, covering such topics as locating and recovering missing NM (to include emergency inventory taking), minimizing and mitigating radiological consequences, countering an insider threat or unauthorized intrusion and responding to a stand-off attack. Implementing procedures are then defined to describe how the PPS will be operated and how the security and contingency plans will be implemented.

Security and/or contingency plans may include information that is useful for performance testing and analysis, such as how much time is planned for RFs to arrive from different off-site organizations. Part of the analysis may address how well the PPS meets these performance requirements.

The assessment team needs to understand the security and contingency plans and the procedures described in the security plan and, in particular, needs to understand the reasons for any deviation from normal licensing conditions. Security inspection reports by the competent authority and by the operator, as well as similar reports (e.g. by RFs) and records of security related incidents, can be studied, as appropriate, for the scope of the analysis.

It is important to demonstrate that the security system is operated in accordance with plans and procedures.

2.5. CONDUCTING ASSESSMENTS

A nuclear SA is composed of three steps:

(1) Develop data libraries that indicate the effectiveness of the physical protection measures both individually and as part of systems and subsystems;

(2) Perform path analysis;

(3) Perform scenario analysis.

Depending upon the nature and objectives of the assessment, not all three of these steps may be performed. For example, at facilities with simple layouts a path analysis may not be necessary.

Each of these steps is described in the following sections.

2.5.1. Develop data libraries

2.5.1.1. Data libraries

Data libraries are a historical collection of performance test data that can be used as a basis to justify nuclear security element probability of detection, assessment or delay times used in modelling and simulation activities. Data libraries can be developed and maintained as part of any assessment programme or process. Data is collected in the initial stages of the assessment process and is essential to the characterization of the facility to provide documented evidence for the facility assessment results. Once established, data libraries can also be used as initial input to other assessments with some confidence that similar nuclear security element configurations will provide comparable detection, assessment and/or delay values for similar installations/configurations. The use of data libraries can also reduce the assessment costs by establishing standard delay, detection and assessment values for use by multiple sites or facilities where common barriers and alarms systems are used. The data libraries can be a manually tabulated list or electronic menu values embedded in an assessment software programme.

Sources where data library values can be derived include the use of state sponsored or other site testing, facility specific performance testing, SME judgement and other sources of data including state law enforcement, military experience and the insurance industry. Manufacturer specifications or testing data may be used initially until other user performance data can be developed.

It is advisable that data libraries be protected based upon the highest level of sensitivity of any data contained in the data library.

The assessment will typically start with existing data and will collect new data if it is needed during the assessment. The assessment scoping document referred to in Section 2.4 can be used to describe the process and criteria for selecting data library values. It is important for the assessor to allocate sufficient time during the assessment process to plan for, collect and document site specific performance data at the facility.

Appendix II describes two techniques (statistical analysis and expert judgement) for characterizing performance measures such as delay times or detection probabilities.

Careful use of the data collected during a FoF and/or a response LSPT is necessary. The primary purpose of a FoF exercise is to provide assessment of training or insight into overall system effectiveness, not to collect data for use in an assessment. There are also typically practical limitations on the time to conduct the exercise and the safety considerations associated with performing each task that limit the realism of the test or exercise. As an example, expert controllers are needed during exercises to assess the effectiveness of area kill weapons, such as grenades, due to safety concerns.

Table 5 provides a list of some of the primary categories of data needed in a data library. As the table indicates, a high degree of dependency exists between the different categories of data. For example, the performance of a barrier cannot be fully determined without knowing the capabilities of the tools that an adversary may use to defeat it. Accounting for this dependency during data collection can speed the process.

TABLE 5. SELECTED PERFORMANCE DATA CATEGORIES

Category	Typical Parameters	Description
Detectors	Assessment delay and sensor sensitivity	Sensing and assessment data to go with each method of detection (e.g. cameras, eyes).
Tools	Weight, effectiveness, defeat and deploy times	Tools used by adversaries (and protective force) to defeat barriers and objectives.
Weapons	Weight, firing rate, hit and kill probabilities	Weapons used to neutralize adversaries (or protective force) or objectives/targets.
Platforms (people, vehicles)	Speeds over barriers and across terrains	Determines how fast adversaries and responders move on foot or in vehicles.
Barriers	Transparency of barriers to sensors and weapons	Determines how sensors and weapons are impacted by the barriers in a security system.
Terrains	Transparency of terrains to sensors and weapons	Determines how sensors and weapons are affected by the terrains at a facility.
Humans	Tools, weapons and vehicles assigned	Defines tools, weapons and vehicles assigned to adversaries and responders.

Regardless of the specific methods used to select and reduce the data, retention of all data is highly suggested for quality control purposes. It is a good practice to record this information on worksheets even if the modelling and simulation tool has its own interface for capturing data. Typically, the data may be reviewed and approved by several organizations, some at the facility and some within the competent authority and it is not reasonable to assume that all of these reviewers have ready access to that tool and the required training on the tool to inspect the database. It is imperative that data collection adhere to quality standards to ensure the confidence given to the accuracy of the data is maintained. It is suggested that data collection and testing programmes be prioritized to focus on those features that give the greatest benefit to the evaluation.

Once a facility has been adequately characterized during the first assessment, future updates can be more straightforward and can even represent a small incremental cost over the original effort.

2.5.1.2. Performance testing

Performance testing by state sponsored testing centres and/or by site resources can be conducted for different types of barriers, sensors, cameras and procedures. Data is based on specific defeat mechanisms associated with barriers, sensors, cameras, procedures and/or personnel. For example, barrier delay times can be tested for defeat over a range of increasing levels of breaching techniques from hand tools, power tools, breaching tools, explosives and vehicles, as applicable. Similarly, probability of sensing levels is determined for personnel walking, running, jumping, crawling, bridging and use of other aids. Typically, multiple iterations of testing can occur on each nuclear security element resulting in a range of test data to ensure a representative sample is collected. Selection of the data library values used for input is then based on either statistical analysis of all test data, professional judgement or a combination of both. Performance testing data can also be derived from state oversight inspection results, routine facility testing organizations or specific testing as requested by the assessment team to validate critical system element assumptions and input. It is important that performance testing methodologies and results are well documented in order to justify the development or revision of assigned values. The use of video and a full explanation of the performance tests can be very useful to document test data.

On-site testing—Due to unique facility design or environmental conditions that may not match assumed conditions for existing library source data, some sites may conduct nuclear security element testing to establish and/or validate assessment input values. If the actual facility is used, detailed coordination is required with facility operations and security to ensure protection measures are maintained during the testing period through compensatory measures. If a deficiency is identified through testing or a protection element is defeated as part of a test (e.g. fence is cut), corrective actions can be initiated as soon as testing is completed. Compensatory measures will remain in place until corrective actions are completed.

Dedicated test bed—Dedicated test beds can be located at the facility location or as part of a state sponsored testing location. The dedicated test bed approach allows for PPS testing under more realistic conditions without impacting facility operations or security. Due to the wide use of certain PPS elements, a dedicated testing facility may be established to determine and/or validate assessment input values over a wide range of PPS elements, conditions and defeat mechanisms. Test beds may include facilities to test interior and exterior PPS systems. It may also include infrastructure to support sensor testing, data gathering and data recording. It is advisable that the test bed also include the efficient installation of sensor platforms, access control systems, delay systems, prohibited items detection, lighting, assessment, power distribution, alarm communications, monitoring, and recording systems. The test bed can be used for determining performance data for assessments and assess new technologies and training personnel on the operation and maintenance of the PPS. The benefit of using a facility based test bed is that it allows for the testing of facility specific physical protection measures under exact climatic conditions to understand how weather and other site conditions affect sensor performance. This approach also helps to identify the proper calibration and/or installation configuration in order to ensure the optimum system performance.

In some cases, defeat testing of a barrier or alarm system may be prohibited due to cost or operational constraints at a site/facility. These constraints can include attempting to performance test sensors or barriers in areas of high radiation or contamination issues where personnel safety is a concern. In these cases, SME judgement can be relied upon for establishing delay times and/or detection/assessment values. The SMEs may perform engineering calculations and/or review historical testing data for similar types of protection elements and assign testing results. If no data exists, SME opinion and manufacturer specifications/testing values can be the initial basis for assigning values.

Other data sources may include manufacturer published data (although they may be conducted under controlled laboratory conditions); national and international standards; web site or widely distributed data for general use, such as ammunition ballistic performance or general explosive characteristics; and national law enforcement or military data and experiences. For example, the use of military handbooks can be a valuable source of information for generic data. An example of such a handbook, that is openly available, is “Soldier in the Field (Sold F)” published in Sweden. It gives guidance on the soldier´s behaviour on and off the battlefield. In addition, there are sections on rules of engagement, weapon types (including general descriptions of their performance), body armour and communications. This type of data source, although it is quite general in nature, has the advantage that its quality has been assessed and found to be sufficient as guidance for military personnel.

There are various reasons to adjust data library values. Site specific conditions for barriers or alarm systems may differ from the previous data library tested configurations. Minor design changes in barrier design may dramatically affect standard adversary delay times and defeat methods. Advances in both physical protection technologies and adversary defeat capabilities are also justifications to adjust historical testing data. In other cases, where testing of a barrier or alarm system is possible, data collected by the site/facility on specific adversary scenarios may invalidate existing data library values. Site specific conditions and protection measures can be different than generic testing conditions performed at a state testing location. As a result, site specific testing of both the site protection capabilities (alarm, assessment, response) and the adversary attack methods is always advisable to justify or confirm assessment model inputs.

One method to document changes or modifications to standard data library values is for the facility/site to develop an annex to the data library that identifies site specific testing results and justifies model inputs in order to properly document assessment inputs for model validation. The benefit of having these test data in a separate annex allows for easy reference and the ability to highlight inputs that deviate from standard historical values.

Table 6 and Table 7 provide some brief examples of detection and delay values and are provided for illustration purposes only.

TABLE 6. HYPOTHETICAL INTRUSION DETECTION SAMPLE DATA

Component type	Component description	No equipment P_D	Hand tools P_D	Power tools P_D	High explosives P_D	Land vehicle P_D
Exterior sensors	Seismic buried cable	0.5	0.5	0.5	0.5	0.9
	Electric field	0.5	0.3	0.3	0.5	0.9
	Infrared	0.8	0.4	0.4	0.5	0.8
	Microwave	0.8	0.7	0.7	0.7	0.9
	Video motion	0.8	0.6	0.6	0.7	0.9
	Multiple non complementary	0.9	0.8	0.8	0.8	0.99
	Multiple complementary	0.99	0.95	0.95	0.99	0.99
Interior Sensors	Sonic	0.5	0.5	0.5	0.5	n.a.*
	Capacitance	0.5	0.5	0.5	0.5	n.a.
	Video Motion	0.5	0.5	0.5	0.5	n.a.
	Infrared	0.5	0.5	0.5	0.5	n.a.
	Ultrasonic	0.5	0.5	0.5	0.5	n.a.
	Microwave	0.5	0.5	0.5	0.5	n.a.
	Multiple non complementary	0.75	0.75	0.75	0.75	n.a.
	Multiple complementary	0.9	0.9	0.9	0.9	n.a.
Position Sensors	Position Switch	0.5	0.2	0.2	0.2	n.a.
	Balanced Magnetic Switch	0.8	0.8	0.8	0.8	n.a.
Fence Sensors	Taut Wire	0.5	0.25	0.25	0.75	0.85
	Vibration	0.5	0.1	0.1	0.75	0.85
	Strain	0.1	0.1	0.1	0.1	0.9
	Electric Field	0.5	0.4	0.4	0.75	0.9
	Multiple Sensors	0.75	0.5	0.5	0.8	0.9

* n.a.: not applicable.

TABLE 7. HYPOTHETICAL PENETRATION TIMES – DOOR SAMPLE DATA

			Penetration time (minutes)			
Barrier description	Penetration equipment	Equipment weight (kg)	Min.	Mean	Max.	Standard deviation
Sheet metal	Explosives (1.0)	1	1.25	1.9	2.8	—*
Standard industrial pedestrian door, 1.6 mm metal, panic hardware, cylinder lock, rim set, butt hinges with removable pins	Cordless drill	2.7	1.5	3.0	4.5	0.61
	Pry bar	7	0.1	0.2	0.3	0.41
	Fire axe	4.5	1.9	3.8	5.7	0.78
	Suction cups, sledge, cutting torch	25	0.5	1.0	1.5	0.20
	Pipe wrench	1	0.2	1.2	2.5	—

* —: data not available.

Types of performance testing

A new performance test can be regarded as a scientific experiment; the hypothesis being tested is that the PPS does not resist the threat at an acceptable level, as determined in the test plan. In this fashion, test error rates control the probability that the measure(s) under testing meet acceptable performance levels against the threat when they actually do not.

Performance testing of technical systems

The functionality of technical security systems (detectors, alarms, communications, etc.) is mostly a matter for routine monitoring and inspection. However, they may also be performance tested, especially with regard to their inputs to analysis systems and controls requiring a human response.

Performance testing of response capability

Response capabilities will nearly always be assessed as part of a whole system SA. However, given the potential importance of response elements in a security system, there is merit in designing performance testing for response elements on their own. Uniquely, these SAs could be incorporated in a training programme especially where the RF has no other responsibilities. This can be readily achieved for a site response capability because it is usually subject to oversight by the regulatory authority and may be also under the control of the operator. However, off-site response is typically provided by law enforcement or the military and is not subject to oversight by the regulatory body. It is suggested in these circumstances the operator, if possible, include the need for SA in the formal arrangements for the RF.

Limited scope performance tests

LSPTs provide an approach to evaluate the effectiveness of portions of the security system without conducting expensive and resource intensive FoF exercises. It can also be used to test system effectiveness of one or more elements of the system.

Force-on-force exercises

FoF exercises allow the testing of the complete system using the full features of the security system, to include the protective force. These activities are very resource intensive, requiring shadow forces, controllers, etc.

Performance testing of security related procedures carried out by personnel

The effectiveness of procedural security measures can also be assessed independently of a whole system assessment. This might include checks on the effectiveness of the two-person rule and searches, etc. However, this may more properly be seen as a training and refresher issue. See Ref. [14] for more information.

Uncertainties

Assessment results will not be precise and will have some uncertainties associated with them given resource limitations on collecting required information described in Section 2.4; limited precision about performance metrics such as delay times and detection probabilities derived from data libraries; imperfect knowledge about the precise status of the PPS and facility during an attack and the unpredictability about how adversaries or responders will react during an attack.

Uncertainties related to the variability that can be discerned from available data are frequently referred to as 'stochastic' or 'aleatory' uncertainties. These aleatory uncertainties are sometimes also referred to as irreducible uncertainties as an indicator that this type of uncertainty generally cannot be decreased. Aleatory uncertainties are accounted for during the assessment by allowing the variables related to detection, delay and response to change over their range based upon a given model/distribution in the assessment data library. In general, the variables given are good examples of where aleatory uncertainties exist.

The area of uncertainty which relates to the shortcoming in analytical or experimentally based modelling is referred to as 'epistemic' or modelling uncertainty. Partly due to the irreducible nature of the aleatory uncertainties, analysts tend to focus the understanding of uncertainty on these epistemic contributors. Such contributors may include uncertainty in the representation of the facility (e.g. the precise design of an ancient door may not be available), in the actual status of the PPS or how adversaries may respond to certain events or how responders may implement tactics. It may also include approved simplifications (e.g. not explicitly including some infrequent operating modes, see Table 7). Therefore, the easiest way to identify epistemic uncertainties is to identify shortcomings and associated alternative models for each of the four types of data described in the introduction to Section 2.4.

Table 8 identifies some significant sources of uncertainty in performing PPS assessments along with how these sources relate to the three data requirement categories.

TABLE 8. SOURCES OF UNCERTAINTY

Source	Data requirement category	Relationship to human performance	Description
Decision making on responder deployment	Facility characterization	This is directly related to human performance.	Details of how responders are deployed can be left to commanders and these commanders can make different decisions all within a given response plan. Given that the number of commanders can be discerned, this uncertainty is really due to insufficient modelling.
Failure of security system components to function as designed	Facility characterization	The failure (i.e. human error) of security forces (for any reason) is directly related to human performance.	Random failure of any system components (including officers). The failure modes for equipment components are generally discernible. This is not failure due to the adversary defeating the components (that failure is integral to the simulation), but rather an unrepaired/latent failure prior to attack.
Operating modes	Facility characterization	Not directly related to human performance	This is the uncertainty in the modelling of the defined operating modes (e.g. full power, refuelling) of the facility. Some operating modes may occur only infrequently, but may represent increased vulnerability due to target set exposure or security design configuration. The number of operating modes is known so this uncertainty is due to insufficient modelling.
Environmental conditions	Facility characterization	Not directly related to human performance	This is uncertainty in the modelling of environmental conditions. Only choosing to model daytime and not night time operations is an example of this insufficient modelling uncertainty.

TABLE 8. SOURCES OF UNCERTAINTY (CONT.)

Source	Data requirement category	Relationship to human performance	Description
Weapon performance (P_H/P_K)	Performance data library	The hit and kill probability data attempts to remove any human performance bias.	Uncertainty in the current model of how weapons (both adversaries and security officers) perform. A ballistics based model would likely reduce these uncertainties. Represents a needed research area since the current state of the art is still using hit and kill probabilities.
Starting locations for adversaries and responders	Scenario specific	Not directly related to human performance but is influenced by adversary and defender preferences.	Uncertainty of where adversary and defenders are located can affect planning assumptions set by attackers and defenders and their decisions during a simulation or exercise. The discrepancy between where these entities actually are versus where they are planned to be could affect the results of the analysis.

2.5.2. Path analysis

2.5.2.1. Introduction

Path analysis is an evaluation method to determine whether the PPS is effective across a wide variety of paths that an adversary might take to cause unauthorized removal or sabotage at a facility. This section provides a general overview definition of path analysis; Appendix V discusses path analysis in more technical depth.

Path analysis is useful primarily by providing insight into the performance of a PPS across many possible paths simultaneously but also serves to very quickly determine which paths have the lowest associated performance against the TA/DBT. Such paths, termed most vulnerable paths, may serve as the basis for building detailed attack plans as part of scenario analysis (see Section 2.5).

This section starts by defining a single adversary path and then describes how P_I is calculated for that path using a timely detection analysis method. Overt attack analysis, as described in the IAEA Introduction to the Evaluation of Physical Protection System Effectiveness course, is examined briefly. Both the traditional P_I and overt analysis methods focus on adversary paths within a stated DBT and account for facility response requirements. Both methods only provide P_I. If the analyst is interested in determining P_E, then some other tool or method is required to determine the corresponding probability of neutralization (P_N).

Finally, an overview of multipath analysis is presented. Multipath analysis examines how PPS effectiveness differs over multiple paths and retains information identifying those paths that have the lowest P_I or P_E effectiveness metric. Software is typically used to perform multipath analysis; examples of such software are provided in Ref. [1]. Advanced software tools measure performance directly, but approximately in terms of total system effectiveness. More commonly, multipath analysis is used to determine minimum P_I paths as part of timely detection analysis.

2.5.2.2. Definition of a path

A path is a time ordered series of adversary tasks or actions along with some description of where those tasks/actions are performed within a nuclear facility (see Appendix V). Figure 9 shows an example of a very simple path drawn in red on a hypothetical facility layout; such a path might be followed by an outsider adversary. In this case, a task might consist of either penetrating an element, such as Door 1 or crossing an area, such as the Hardened Room. Locations associated with these tasks are then defined in spatial coordinates for the elements and for the routes between consecutive elements on the path. Depending on the adversary objective, the adversary may attack one or more targets in different rooms or areas with each target then being included as part of the path definition. Given assumptions about adversary objectives and response protection strategies, the adversary may be assumed to achieve their

objective at the last target (as in sabotage) or when their final task is to exit the facility with nuclear material (as in unauthorized removal). Figure 9 shows an example of a path (in red) where the adversary intent is to perform sabotage at a single target in a hardened room; an example of an unauthorized removal path might contain the same tasks in red down to the target followed by the same tasks in reverse order (with blue arrows) to represent the adversary escaping from the facility.

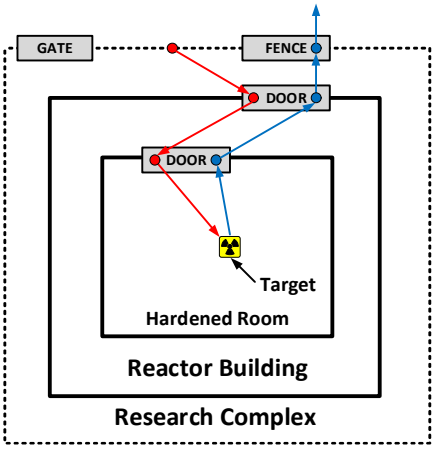


FIG. 9. Path displayed on a hypothetical facility layout

The green boundary is meant to indicate a fence that covers the entire Research Complex boundary except for the gate. The fence may be quite extensive, perhaps several kilometres long. Some simpler evaluation tools treat the entire fence as one location, whereas other tools represent specific locations along the boundary. In this example, the red dot on the perimeter in Fig. 9 is an example of a specific definition of location. The other tasks on the path are through specific doors and at a specific target.

The scenarios discussed in Section 2.5 allow for more generality than paths because scenarios may involve multiple adversaries performing tasks in parallel while paths represent a single sequence of tasks/actions.

Table 9, along with the locations in Fig. 9, defines a hypothetical path that will be used in the rest of this section. The left column of Table 9 lists an ordered set of adversary actions that are associated with the unauthorized removal path in Fig. 9; the delay and detection physical protection measures encountered during each adversary action are shown in the middle and right columns.

TABLE 9. PHYSICAL PROTECTION MEASURES ALONG A PATH WITH GENERAL DESCRIPTIONS OF ADVERSARY ACTIONS

General description of adversary action/task	Delay physical protection measures	Detection physical protection measures
Penetrate fence	Fence fabric	Fence sensor
Cross Research Complex Area	Distance	Guards hearing adversaries
Penetrate door	Door hardness and lock	Door alarms sense cutting a hole or opening door
Cross Reactor Building	Distance	Employees hear adversaries
Penetrate door 1	Door hardness and locks	Door alarms sense cutting a hole or opening door
Cross Hardened Room	Distance	Interior sensors (off)
Open container and gather material	Task complexity to open container	Interior sensors (off)
Escape by same route used on entry	Exit distance; assume other measures defeated	None: assume defeated

The description of each adversary action/task is not specific. For example, in Table 9 it is unclear whether the adversary would use explosives or cutting tools in attempting to penetrate the fence.

2.5.2.3. Timely detection analysis of a single path

This section explains how P_I is traditionally computed for a single path, whether by using software or manual methods. P_I for a path such as the one in Table 9 is calculated using an adversary timeline and a PPS response timeline (see Fig. 10). Fig 10 depicts the adversary timeline at the top, indicating the task time it takes the adversary to complete all of their tasks and also the sensing opportunities along the timeline which may cause the adversary to be detected. Below the adversary timeline, there is a comparison between the PPS response time (PRT) and the adversary task time remaining on the path after the third sensing opportunity shown in red (to simplify this explanation, assume that all task times and probabilities are point values.)

If PRT < adversary task time remaining after first sensing, then the corresponding sensing opportunity is considered timely; if this is not the case, then the opportunity is not timely. The critical detection point (CDP) is the last sensing opportunity on the adversary timeline that is timely, in this case sensing opportunity[3] which is labelled in red.

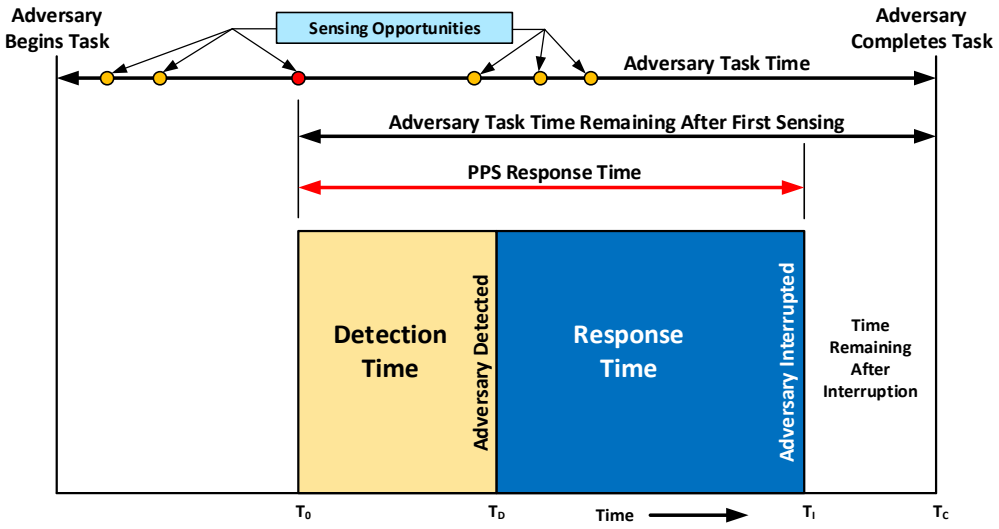
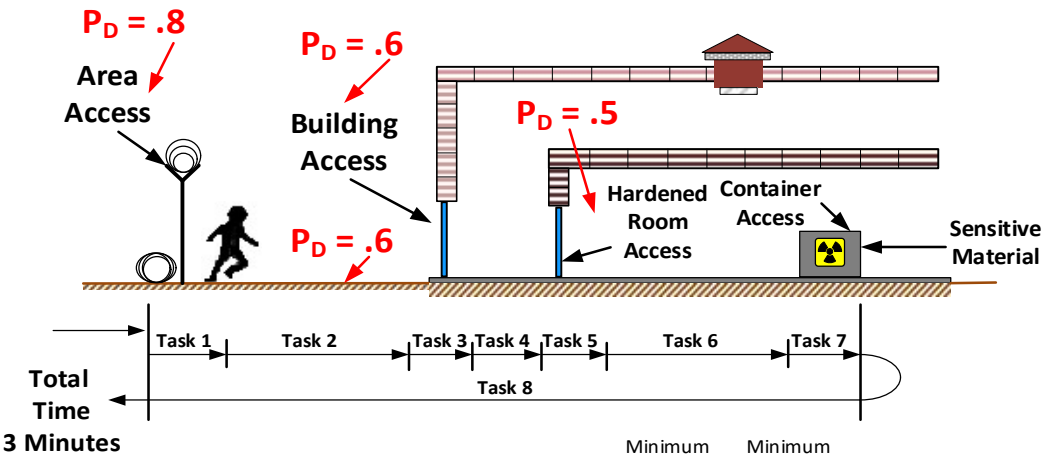


FIG. 10. Adversary and response timelines associated with a path

The data used for creating the adversary timeline are shown in Fig. 11. Each adversary action/task is assigned a delay time and, where appropriate, a probability of detection (P_D) taking into account the capabilities of the threat as defined in the TA/DBT. For this example, assume that detection occurs at the end of the task delay. The CDP for this path is at Task 3 and the adversary task time remaining after first sensing = 108 seconds, which is the sum of the delay times for tasks 4 through 8.

[3] This model is called 'timely detection' and not 'timely sensing' because the timing for the beginning of the detection process is the sensing event; hence, from a timeline perspective, timely detection equates to timely sensing.



Task	General Description of Adversary Actions	Minimum Delay Time	Minimum P_D
1	Penetrate fence	12	0.8
2	Cross Research Complex Area	12	0.6
3	Penetrate door	48	0.6
4	Cross reactor building	24	
5	Penetrate Door 1	12	0.5
6	Cross hardened room to container	6	
7	Open container and gather material	12	
8	Escape by same route used for entry	54	

FIG. 11. Adversary timeline information data with a path

To develop P_D and delay times, two further questions need to be answered for each corresponding general adversary action:

- What P_D and delay time is to be used, given that more than one defeat method might be used to defeat the delay and detection protection measures?
- Where, specifically in the facility, is the adversary located as they perform a task or cross some area?

For example, two adversary defeat methods might be to cut through Door 1 or to cut through its lock. The first defeat method encounters the door hardness and any sensors that determine if the door is being cut open. The second defeat method would encounter the locks and sensors that determine if the door has been opened.

The P_D for a single adversary action, such as those shown in Table 9, is typically assigned as the smallest P_D over all defeat methods; the delay time is typically assigned as the smallest delay time over all defeat methods. The specific defeat method that achieves the lowest P_D does not need to match the defeat method achieving the lowest delay time. The last two columns in the table in Fig. 11 list the minimum P_D and delay times for all tasks; some P_Ds (probability of detections) are left blank to indicate that there is only marginal detection associated with those tasks so none will be taken into account when calculating P_I.

The location of each adversary attack is typically identified prior to determining delay times and perhaps P_D. For example, in Fig. 9, the fence might hypothetically be defeated anywhere over a three kilometres distance, so the actual location (indicated with a red dot) may affect the delay time, and perhaps P_D, associated with moving between the fence and the door to the reactor building.

The response timeline, representing the detection and response times included in the PRT, also needs to be defined. Average values for the components of the PRT are shown in Fig. 12. Assuming an alarm occurs at time zero, thirty seconds are spent receiving the alarm at a central alarm station (CAS) and then assessing that the alarm was caused by an actual intrusion, and sixty seconds are spent by the RF receiving the alert and deploying on-site. The total PPS response time is ninety seconds.

P_I is defined as the probability that the adversary is detected during at least one of the timely sensing opportunities. For this case, where P_D, delay times and PRT are point values, Eq. (1) for P_I is (P_{Dj} refers to the P_D for task j):

$$P_I = 1 - \prod_{j=1}^{CDP} (1 - P_{Dj}) \quad (1)$$

Response Action	Average Times (in seconds)	
Alarm communication time	1	Detection Time
Alarm assessment time	29	
Response force communication time	10	Response Time
Response force preparation time	20	
Response force travel time (vehicle)	15	
On-site deployment time	15	
PPS Response Time (Total)	90	

FIG. 12. Component times for the PPS response times

For the example path in Table 9 and in Figs.10 through 12, the first three sensing opportunities are timely, so Eq. (2) is:

$$P_I = 1 - (1 - P_{D1}) \times (1 - P_{D2}) \times (1 - P_{D3}) = \quad (2)$$

$$1 - (1-.8) \times (1-.6) \times (1-.6) = 0.968 \text{ or } 0.97, \text{ approximately}$$

By using minimum P_Ds and delay times, P_I is calculated as if the adversary attempts to minimize detection down to, and including, the CDP and then minimizes delay, proceeding as quickly as possible, until the end of the path.

2.5.2.4. Overt attack analysis of a single path

This method is described in the IAEA Introduction to the Evaluation of Physical Protection System Effectiveness training course. Unlike traditional path analysis where the focus is minimizing P_I, overt attack analysis is a manual method for determining whether there are paths that are susceptible to overt attacks that reduce P_N and/or increase PRT by attempting to attrite RFs using vehicle bombs, etc., simultaneously with the actual intrusion by an adversary team. Figure 13 shows an example of an overt attack where an adversary detonates a bomb next to a RF post while other adversaries are attempting to defeat the fence. The net result may be that P_D for the fence will increase from 0.8 to perhaps 1 (because the explosion may be heard anywhere) while the number of responders may drop by the number of them incapacitated at the post and this may, in turn, affect P_N. The PRT may also increase if the number of surviving responders at the post can no longer effectively interrupt the adversary. If such is the case here and if the remaining responders are more than 167 seconds away, then detection at the fence will no longer be timely and $P_I = 0$ even if the P_D at the fence is effectively 1.

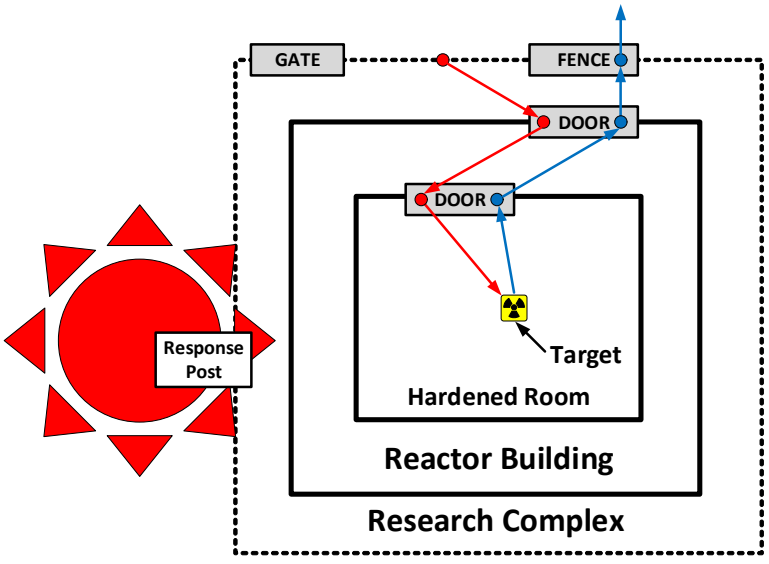


FIG. 13. Overt attack displayed on a hypothetical facility layout

2.5.2.5. Multipath analysis

During path analysis, PPS effectiveness is typically reported as P_I for the most vulnerable path(s) that achieves the lowest P_I[4]. To do this requires some approach to represent all paths, either explicitly or implicitly, and then some method to systematically examine P_I for every path in that representation while keeping information about the most vulnerable path(s).

Multipath analysis is typically performed over some sort of network model that represents the set of paths to analyze. Appendix V discusses several types of networks; this explanation will use a simple network that is based on what is called an adversary sequence diagram (ASD). Figure 14 depicts an example ASD which represents the concentric physical protection areas (in green) around a facility target (in this case a floor enclosure). It also shows the physical protection elements (in yellow), such as doors and walls, that constitute protection layers between areas.

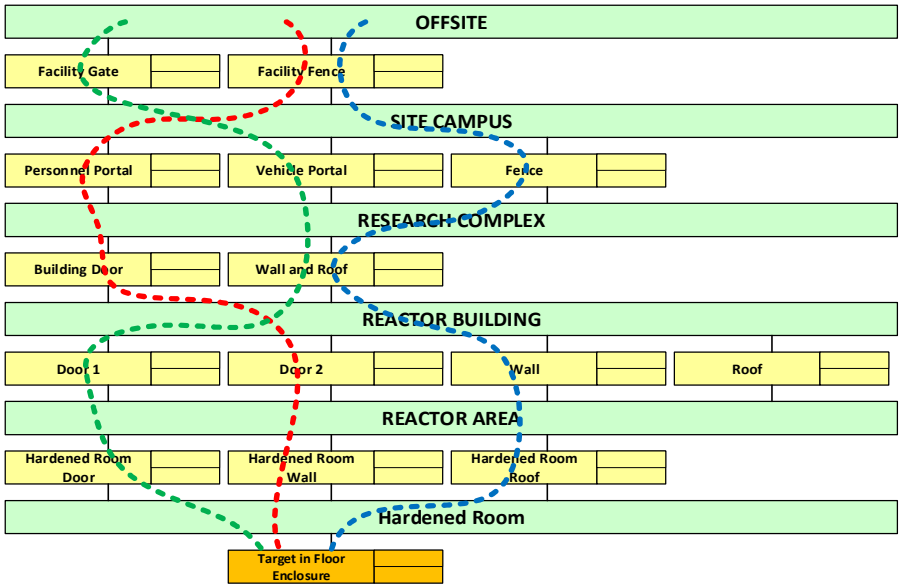


FIG. 14. Sample ASD and P_I comparison

An ASD is used to represent all paths to the floor enclosure target where a path in Fig. 14 is defined as a sequence of elements from the off-site area where there is minimal protection down to the target. The second protection layer consists of a personnel portal, vehicle portal and fence, which represent the three possible options for the adversary to pass through that particular protection layer. The diagram also indicates three paths shown on the diagram; for example, the green line represents a path starting off-site, proceeding through a facility gate, through the vehicle portal, and then passing through the wall and roof. The red and blue lines represent two additional paths to the target location. There are $2 \times 3 \times 2 \times 4 \times 3 = 144$ paths represented in this ASD.

Figure 15 depicts a plot of P_I versus path number. The vertical axis of the graph measures the P_I for each path, while the horizontal axis shows paths 1 through n, where n = 144 for this example. Protection along the three paths shown is not balanced: Path 2 has a $P_I = 0.4$, much less than the P_I for paths 1 and 3. In this example, if Path 2 has the lowest P_I among all paths, then it will be a most vulnerable path. In such a case, physical protection around this floor enclosure would be assigned $P_I = 0.4$.

Although multipath analysis provides helpful information as a standalone analysis when performed during the early stages of scenario development, it can also be used to compare the timeline features of a scenario to the PRT. This comparison determines if the adversary is likely to be interrupted and, if interrupted, likely to be neutralized. The path analysis is based on conservatively low (or worst case) probabilities of detection and delay times. This conservatism leads to a low value of P_I compared to that

[4] The metric would be P_E for those tools that are designed to minimize P_E.

for an actual detailed scenario which typically will have a larger P_I. However, the conservatism can be valuable in the sense that if the conservative P_I is high, then the scenario development team assumes the adversary will be interrupted.

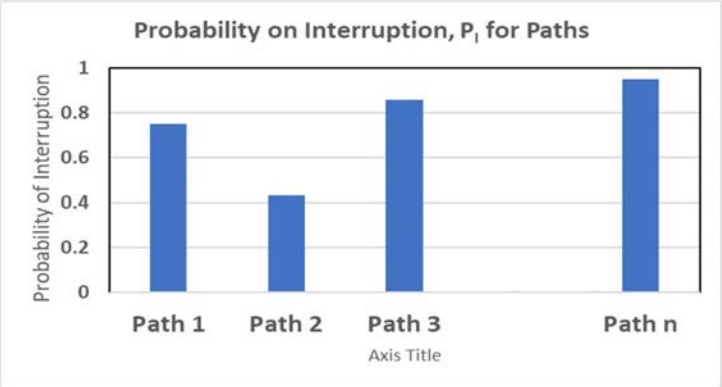


FIG. 15. Plot of P_I versus path number

2.5.3. Scenario analysis

Scenarios are hypothetical sets of conditions and sequences of events constructed for the purpose of focusing attention on causal processes and decision points. They answer two kinds of questions:

- Precisely, how might some hypothetical situation come about, step by step?
- What alternatives exist for each actor, at each step, for preventing, diverting or facilitating the process? See Ref. [15] for information.

Scenarios are commonly used to allow a range of possible future conditions and/or events to be modelled and assessed. A scenario may represent the conditions at a single point in time, a single event, or a time history of conditions and/or events (including processes). Safety analysts use accident scenarios to describe and model plant response to potential accidents. An accident scenario, which usually has an initiating event superimposed on a proposed plant configuration, can be used to model system response, including various operator actions as appropriate. As mentioned in Refs [10 and 16], initiating events that can happen by accident could also be caused by malicious acts.

Nuclear security scenarios can be divided into several component stages, each addressing sub objectives that the adversary has for that stage of the scenario. For example, a ‘pre attack’ or ‘planning’ stage for a scenario before the adversary has attempted to penetrate a controlled or restricted area, or the ‘transportation’ stage of a scenario where material is being taken to some strategic location or major public event to be scattered or detonated. This publication will refer to the scenario as that phase where a facility or transport operation is attacked by adversaries as opposed to the planning phase or what the adversary will do after the attack is successful.

Scenarios can be described as having attributes. Some examples of scenario attributes are the specific type of adversary involved, the target location, the use of special attack methods (e.g. cyber-attack), operating conditions, use of overt versus stealth actions, whether part of the attack is aimed at degrading the PPS through indirect attacks and whether an insider is used as part of the adversary’s hypothetical planning for, or execution of, the scenario.

Scenario classes can be defined in terms of scenario attributes, where each class conceptually includes all individual scenarios that have the corresponding scenario attributes. For example, scenario classes are commonly defined in terms of adversary objective (unauthorized removal or sabotage), operational state during which the attack occurs, the capabilities of the adversary and the adversary avenue of approach (e.g. from the sea versus land).

Scenario Analysis consists of four steps:

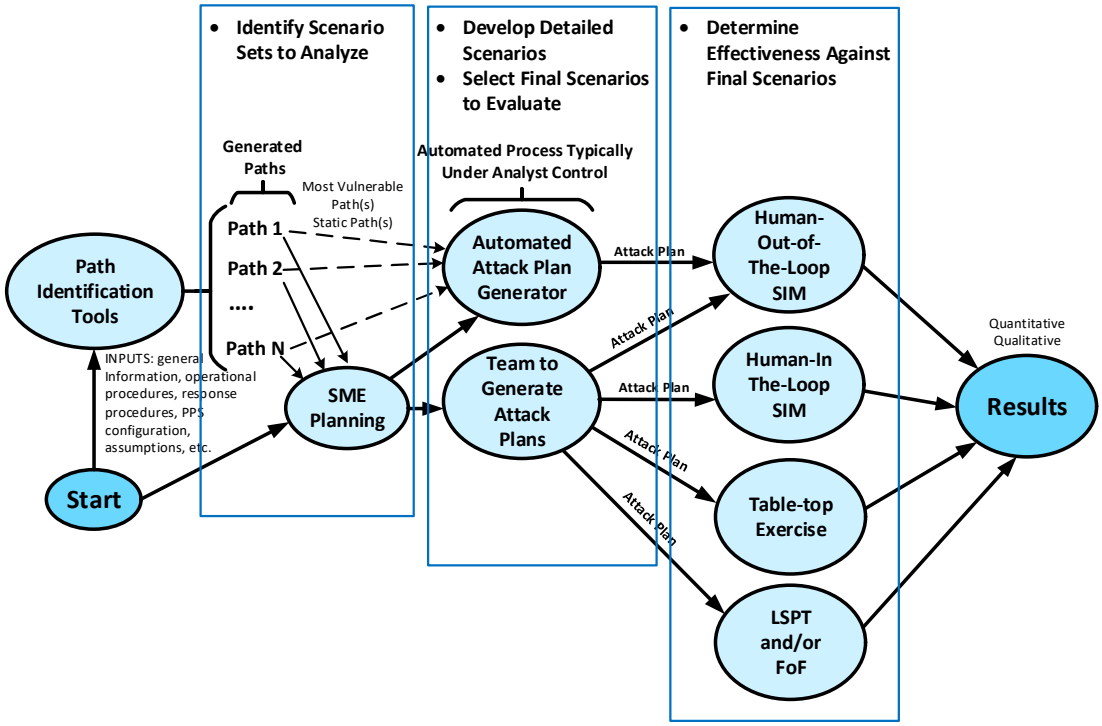
(1) Identify scenario sets to analyse;

(2) Develop detailed scenarios;

(3) Review and select final scenarios to evaluate;

(4) Determine effectiveness against final scenarios.

Figure 16 demonstrates how these steps correspond to the process for using software tools and evaluation methods.



(Courtesy of M. Snell, Sandia National Laboratories)

FIG. 16. How scenario analysis steps correspond to the process for using software tools and evaluation methods

2.5.3.1. Identify scenario sets to analyze

The first step in scenario analysis is to determine the set of scenario classes to be analyzed. A scenario class can be defined in terms of unique combinations of scenario attributes, where each class conceptually includes all individual scenarios that have the corresponding scenario attributes.

It is impractical to attempt to cover all scenario classes during the nuclear SA; hence, it is important to plan the classes to be analyzed before starting to develop scenarios. In some cases, the competent authority or facility management may require that specific scenario classes be addressed during scenario analysis. For example, the competent authority may require that scenarios be developed for all buildings that contain Category I NM, or materials of high radiological consequence. In other cases, the assessment team may develop a planning document specifying which scenario classes will be evaluated.

For the purposes of this publication, the scenario set is an explicit or implicit list of all scenario classes for analyses. Table 10 shows four assessment variables: threat, malicious objective, target, and plant/facility state. From the three types of threat, five malicious objectives for those three malicious capabilities, three targets and three plant/facility states would create forty-five different potential scenarios to evaluate. Some of those scenarios are excluded due to physical or operational considerations, procedural and access limitations or physical robustness. From the remaining scenarios that could be assessed, the table shows the ten scenarios that may have been selected from stakeholder discussions which are the most challenging to the security arrangements.

TABLE 10. HYPOTHETICAL SCENARIO SET TO BE EVALUATED

		Threat				
		Outsider		VBIED*	Insider	
		Objective				
Target	Facility state	Unauthorized removal	Sabotage	Sabotage	Unauthorized removal	Sabotage
A	1	#1	#2	#3	Two-person rule	
	2			#4		
	3					
B	1		#5	#6	#7	#8
	2					
	3					
C	1	Sabotage target only	#9	Vehicle cannot access – stand-off too great	Sabotage target only	#10
	2					
	3					

* VBIED - Vehicle-borne improvised explosive device

2.5.3.2. Develop detailed scenarios

When developing attack scenarios, scenarios are be chosen to challenge the plant security and operations to the maximum extent practicable. The scenario needs to be within the constraints established by a TA/DBT and the scenario class under consideration. Thus, the scenarios selected within each scenario class might be chosen as those for which the facility or transport is judged to be most vulnerable. As shown in Fig. 16, the scenario may be based on a most vulnerable path generated by path analysis software or may be developed by a team of experts. A process for scenario development is outlined below.

Development of detailed scenarios is not necessary for every scenario class in the scenario set. It may be impractical to attempt a scenario based on actual conditions. In other cases, the analysis may run out of time or resources before all the scenario classes can be evaluated.

Identify operational vulnerabilities

In order to identify site vulnerabilities across various operational conditions and states, the SA team may consider different:

— Operational conditions (operational versus nonoperational);

— Target material configurations (reactor lead-out versus operations);

— RF alert levels and personnel ‘crews’;

— Different upgrade packages.

Exploiting the vulnerabilities

When promising vulnerabilities have been identified, an action plan can be developed to describe how each vulnerability will be exploited. The action plan will also have the detail and adversary organization in how the attack will be executed. The following steps can be followed (note that the scenario is hypothetical):

— First, create a list of essential tasks to be accomplished for the attack based on that vulnerability to succeed. Such a list might look like the following for a target:

- Task 1: Enter building XYZ;
- Task 2: Collect 20 kg of ^{235}U in storage containers;
- Task 3: Leave site with material without pursuit by RFs;
- Task 4: Arrive undetected at a safe house in city ABC;
- Task 5: Delay responding units so that Tasks 1–3 are accomplished.

These tasks can be kept as simple as possible.

— Next, create sub plans that describe how one or more teams of attackers can perform each task within resource constraints. These sub plans can describe:
  - Who is involved;
  - What they are doing as a function of time;
  - How they are performing each step;
  - What equipment they are using;
  - How they are transporting the equipment.

— Finally, combine these sub plans into a master attack plan/scenario description, adjusting sub plans to meet overall constraints imposed by the DBT, and perhaps the site, as well as to achieve synchronization between teams.

Adding supporting team sub plans to scenarios

Supporting teams can be assigned to complete other essential tasks or to aid the main team directly. Often, the remaining tasks look like: "Delay responding units so ..." or "Neutralize off-site response..." Thus, one good use of supporting teams is to delay or incapacitate the response through setting ambushes, creating diversions and attempting to confuse the response.

Using path analysis for scenario development

Path analysis can suggest sub plans that serve as the main or direct (going to the target) part of the attack. Such plans might be based on the minimum delay, minimum P_I, or minimum $P_I \times P_N$ paths

Details can be added to these path descriptions to round out the scenario. For example, instead of the step "Penetrate Fence" found in the path analysis, the scenario description might consist of: "Four adversaries bridge fence using ladder carried in from vehicle parked outside at night during a storm. Last adversary monitors radio traffic."

Multiple scenarios can be developed for a single path by slightly varying the method by which the adversary attacks different protection elements along the path.

Be aware, though, the most vulnerable path (MVP) from path analysis may be a poor basis for creating a scenario. This may occur because typically low P_I paths are corrected with upgrades during the path analysis phase. After such upgrades, the MVP may now have a high P_I which would make that path less desirable. At this stage, scenario analysis might more profitably consider factors not found in path analysis: preventing neutralization and employing other teams to prevent interruption.

2.5.3.3. Review and select final scenarios to evaluate

Either while the scenario is being developed or at the end of that process, the scenarios are reviewed to determine which scenarios will be evaluated. This review and selection may involve stakeholders, such as staff from the competent authority or facility management. Documentation of assumptions, including which scenarios and assessment methods are to be analyzed, may be approved by stakeholders.

Part of this review considers whether all objectives for the current assessment have been covered by the set of scenarios selected. Another consideration is whether all selected scenarios appear to be credible and within the capabilities specified in the TA/DBT. If there are issues with either of these concerns, then it may be necessary for the assessment team to revise some of the existing scenarios or develop new ones.

2.5.3.4. Determine effectiveness against scenarios

Figure 16 shows four types of performance assurance methods that can be used singly or in combinations to evaluate scenarios: human in the loop combat simulations, human out of the loop combat simulations, TT exercises, and LSPT/FoF exercises. The choice of which combination to use will depend upon a number of factors, such as the nature and size of the facility and the type of assessment and its objectives. In some instances, it may be sufficient to conduct a TT exercise.

A simple path analysis approach based on scenario timelines can be used to assess detection and delay. This approach assesses the detection and delay elements of the scenario to determine whether the RF can interdict the adversary force.

Note: A simple calculation may show that the response cannot arrive in time so that further detailed scenario simulation/exercises (as described below) are unnecessary.

A simple vulnerability approach can also be used to assess detection and response. This approach assesses the detection and response elements of scenarios where the adversary actions and resulting consequences occur without building a timeline. For example, such an approach may reveal that some insider tampering with safety equipment during the outage period is possible and would lead to core damage in case of a reactor scram.

2.5.4. Selection of performance assurance methods

It is suggested that careful planning be performed before every SA to select the best set of methods and tools to use during that assessment. In particular, the methods and tools to use may be dependent on the State's regulatory requirements for graded protection and details about the TA/DBT.

There are strengths and weaknesses of the three approaches for simulating the interaction between adversaries and the PPS: TT exercises, computer simulations and RF tests.

TT exercises can be used for a couple purposes: to assess the security system effectiveness against a given scenario using expert input and help response organizations better understand how to interact and achieve success in defeating the adversary as part of a contingency plan.

Computer simulations require extensive input and may require several people to play roles in the conflict analysis. It can be noted that the quality of computer tools in general tend to be limited by the quality of the performance data used by the software. Computer simulations also require very detailed descriptions of scenarios such as attack plans. These attack plans can be developed through automated or manual methods.

RF testing including FoF exercises allows the testing of the complete system, using the full features of the PPS, to include the protective force. These activities are very resource intensive, requiring shadow forces, controllers, etc. Because a FoF exercise is resource intensive and contains some artificiality, such as assumed weapons effects or safety constraints, an alternative is to conduct a combination of limited scope performance testing, TTs, or computer modelling/simulation in lieu of FoF exercises. It is a good idea to compare FoF exercise data with results produced by other assessment approaches.

Table 11 indicates that computer simulations and path analysis may not be appropriate for evaluating a spent fuel storage facility. Table 12 indicates the methods and tools that can be used during different stages of the facility life cycle. These methods and types are described in Appendix I.

TABLE 11. SUGGESTIONS OF METHODS AND TOOLS THAT CAN BE USED FOR THE NUCLEAR FACILITY LIFE CYCLE

Performance assurance methods	NPP/Cat I facilities	Irradiator facility	Transport	Low Enriched Uranium fuel fabrication	Spent fuel storage
Checklist against prescriptive requirements	X	X	X	X	X
Observation	X	X	X	X	X
Random sampling	X	X	X	X	X
Tabletops (3 types)	X	X	X	X	X
Computer simulations (human in the loop and out of the loop)	Optional		Optional		
Path analysis (2 types)	X	X	X*	Optional	
Performance testing (4 kinds)	X	X	X	X	X
RF tests (3 types)	X (includes FoF)	Optional	X (includes FoF)	Optional	X

* -Safe haven specific applicable

TABLE 12. METHODS AND TOOLS THAT CAN BE USED DURING DIFFERENT STAGES OF THE FACILITY LIFE CYCLE

Performance assurance methods*	Siting	Design	Operation	Decommissioning	Post-closure
Checklists against prescriptive requirements	X	X	X	X	X
Observation			X	X	X
Random sampling			X	X	
Tabletops (3 types)		X	X	X	
Computer simulations (human in the loop and human out of the loop)		X	X	X	
Path analysis (2 types)	very simple	X	X	X	
Performance testing (4 types)			X	X	
Response tests (3 types)			X	X	

* Methods and tools are described in Appendix I

2.6. OVERALL ASSESSMENT OF SECURITY

The activities included in the key step ‘conducting the assessment’ aim at providing input to the step ‘overall assessment of security’. The main task now is to summarize all relevant evidence in a

comprehensive manner, to be able to answer whether security requirements are met.

There may be many specific requirements to address, but in the overall assessment it may be practical to categorize them as either 'prescriptive requirements' or 'performance based requirements'. These two sets of requirements can be treated separately, after which the partial results are combined into a final conclusion. However, performance based requirements may come as requirements on the performance of distinct **elements** of the PPS or of the PPS as a whole. From a practical point of view, the first case, performance based requirements on distinct elements, may be treated as a special form of **prescriptive** requirement.

2.6.1. Prescriptive requirements

When summarizing the evidence relating to prescriptive requirements, or to performance based requirements on distinct PPS elements, the outcome for each specific requirement may fall into one of a number of predefined types. As an illustration, below is a suggestion for one such set of outcome types:

- It has been demonstrated (to the desired level of confidence) that the requirement is met. No security issues have been identified.
- There is insufficient evidence for demonstrating compliance with the requirement (to the desired level of confidence). One or more **potential** security issues have been identified.
- The assessment has identified cases where the requirement is **not** met. An **actual** security issue has been identified.

2.6.2. Performance based requirements

When summarizing the evidence relating to performance based requirements on the PPS as a whole, the outcome for each scenario or class of scenarios may fall into one of a number of predefined types. Below is a suggestion:

- It has been demonstrated (to the desired level of confidence) that the risk[5] associated with the scenario/scenario class is sufficiently small. No security issue has been identified.
- There is not enough information to demonstrate that the risk is sufficiently small (to the desired level of confidence). One or more potential security issues have been identified.
- The assessment has found that the risk associated with the scenario/scenario class is not sufficiently small (to the desired level of confidence). One or more security issues have been identified.

2.6.3. Combined assessment

If no security issues have been identified, the conclusion is that 'security requirements are met'. For each 'potential' security issue, there is a choice between trying to acquire additional information and remove the uncertainty, or to conservatively decide to treat the potential security issue as if it is an 'actual' one. If there are any 'actual' security issues or potential security issues which will be treated conservatively, the conclusion is that 'security requirements are 'not' met'. In this case, the information on security issues will be used as input to the key step 'identify modifications'.

In addition to the main task for the overall assessment, determining if security requirements are met, there is a secondary task of identifying additional objectives. For example, this could be objectives associated with improving the design for improving nuclear safety for the protection of personnel and the environment. If such objectives are identified through the assessment procedure, it may be convenient to include this information when summarizing evidence relating to prescriptive and

[5] The measure of 'risk' depends on how the requirement is stated, e.g. if the focus is on 'probability of interruption', risk may be represented by $(1-P_I)$. If the probability of neutralization is included, the risk measure may be defined as $(1- (P_I \times P_N))$. More definitions are possible, taking into account, for example, the potential consequences of an attack and/or the assumed frequency of occurrence for it.

performance based requirements. The reason is that a comprehensive summary will facilitate addressing whether additional objectives have been identified. If this is the case, this information will also be used as input to the key step 'identify modifications'.

During a facility´s life cycle, the security programme will not be static, but may be revisited regularly and potentially modified to ensure that it is valid at all times. Reasons for considering such modifications include changes in regulation (e.g. changes in requirements or in the details of the DBT or other prescribed boundary conditions for the assessment) and changes in the security system (e.g. changes in the PPS configuration or how the PPS is operated and maintained).

An effective approach for addressing new information that may have an impact on the security programme is to screen the existing documentation by doing a comparative analysis to identify where the new information would be relevant. Formally, this may be accomplished by retracing the key steps in the assessment methodology then making a decision for each step on whether it is necessary to repeat whole or parts of the activities associated with it or whether the outcomes are still sufficiently valid. If it is decided that the security programme needs to be modified, the comparative analysis will be helpful in limiting the scope of the necessary reassessment. If the current security programme does **not** need any changes, it is sufficient to document the comparative study, thus providing transparency if the decisions are challenged at a later stage.

As an example, an upgrade or modification of the adversary capabilities in the DBT warrants an update of the documentation of the step 'collecting required information'. Looking at the step 'Conducting Assessments', the results may still be valid for its purpose. For example, if any additional capabilities are irrelevant (no corresponding vulnerabilities exist), or if the capability modification may be regarded as a relaxation of the threat (making the current assessment conservative) or if a specific new capability is already included implicitly in the assessment (being a special case of a broader category of capabilities that has already been evaluated). If the assessment results change significantly, the step 'overall assessment' needs to be revisited. Depending upon the outcome, the step 'identify modifications' may also be relevant.

2.6.4. Analysis, evaluation and reporting

The purpose of the assessment, agreed upon during its initial stages, will determine the nature of the results and how they will be evaluated. These will vary in assessment type, but it is suggested the project team have an idea at all times about what they will be reporting to the steering group. If the assessment results reflect that security requirements are met, a more detailed analysis of the assessment outcome(s) may be provided. So far as possible, assessment outcome(s) can focus on the larger issues that could be transferable to other regulated facilities. For example:

- Are there issues of security planning, operation or control at the facility to be addressed?
- Has the assessment suggested a problem with security design concepts?
- Has the assessment suggested a problem with the state regulations or how they are administered?
- Has the assessment suggested a problem with security culture that could be replicated elsewhere?

The project team may report technical and procedural failures but recognize that this is not the main purpose of the assessment. Technical security equipment and systems fail occasionally and some may fail during the assessment. The existence of failures is only a concern to the project team (and the steering group) if they are thought to reflect a significant failure in design or operation or if the facility is failing adequately to monitor and test equipment and failing to have compensatory measures in place.

Bearing in mind the time and resources that the operator and regulator will have committed to the SA, it is important that they get value from it and have confidence in its outcomes. They will want quality assurance and, in particular:

- Verification: The assessment was carried out as designed;
- Validation: The assessment meets operational needs.

2.6.5. Uncertainties and assumptions

It is important to discuss the confidence levels of the SA and of the security system itself. Even if the system meets the requirement, the security system could be degraded by ageing or the DBT could be changed so that the system would no longer meet the requirements. Thus, some margin of effectiveness and backup system is necessary for the system to perform properly under different environments. For example, if a detection system has a very high alarm rate (e.g. nuisance alarms) then it may be better to upgrade it even if it meets current detection requirements.

Quantitative data will have some level of uncertainty and it is important to include a discussion of the uncertainty in the documentation of the analysis. In addition, there is no certainty that the scenario used in the assessment will be that followed by a real adversary. A sensitivity analysis is advisable to study any changes of the overall assessment results (output) when different elements (input) are changed. The purpose of this analysis is testing robustness of the results and increased understanding of the relationships between elements and overall system. It also enables the performance of 'what if' analyses to test various assumptions or alternatives.

2.6.6. Reporting the security assessment

The final assessment report describes the objectives of the assessment including details of the scenarios based upon the DBT, and the expected performance measures and outcome. It also includes information on the assessment methodologies, the management of performance information, an evaluation of the exercise and the lessons learned.

The report details the conclusions and makes recommendations. Those recommendations may address strategic, general and site specific aspects. Where enhancements are identified, they may be prioritized for ease of implementation and return on investment.

2.7 COORDINATED RESEARCH PROJECT RESULTS AND CONCLUSIONS

Performance based, risk informed approaches have been developed and used to assess security effectiveness at facilities with the highest potential radiological consequences. There have been some efforts to similarly assess security of a Category I shipment of NM. In the past several years, the methodologies developed for facilities with Category I NMs have been adapted for nuclear power plants. Generally, the security arrangements at facilities with lower potential radiological consequences have not been as thoroughly or extensively assessed. These facilities have been secured more on the determination that a set of prescriptive requirements were in place and functioning. This approach does not confirm that there is adequate security as designed, nor whether the failure of a component of the security system will be appropriately replaced with the proposed or implemented compensatory measures.

Table 1 compares the methods and tools used for the NUSAM CRP case studies. TT exercises were performed for each case study. In addition, the NPP case study was provided to two external vendors who modelled the facility and performed their SAs. This demonstrated how different modelling techniques may produce non identical results, but are generally consistent in their overall outcomes.

Path analysis tools are used to determine the ordered series of potential adversary actions and calculate the P_I for the most vulnerable paths. Path analysis is based on two sub analyses: timely detection and overt attack analysis. Timely detection analysis determines whether P_I is adequate along all adversary paths. Overt attack analysis determines whether there are paths that are susceptible to overt attacks that reduce P_N. Both analyses focus on adversary paths within a stated threat assessment or DBT and account for facility response requirements. Path analysis tools are useful because they provide insight into the performance of a system across a spectrum of possible paths and scenarios. Path analysis tools typically only provide P_I values; thus, a neutralization tool is needed in order to determine P_E. Note that some path analysis tools combine path searches directly with built in simulations to address this issue. In general, path analysis tools require the use of an alternative analysis method for determining neutralization.

Some computer simulation tools are capable of path analysis as well as neutralization analysis using simulated adversary attack scenarios. These tools are sophisticated enough that they are capable of

running hundreds or thousands of engagement iterations, thereby greatly increasing the amount of data that the analyst can review. However, these tools generally require more training and logistical support than traditional path analysis tools.

Tabletop analyses were conducted to compare results with simple pathway analysis tools and complex modelling and simulation tools. The TT methodology resulted in similar results for PPS effectiveness in comparison with both simple and complex tools/methods. In all, the conclusions of this study revealed that different modelling techniques produce generally consistent results. Complex modelling and simulation tools are capable of generating hundreds of scenarios, considering different pathways, while simple pathway tools produce limited analyses comprised of a few pathways.

The project team also performed TT exercises using two different approaches. A traditional approach of having all participants in the same physical location was used for the material transport and nuclear power plant. However, the team used a novel TT exercise approach for the irradiator facility utilizing participants in four locations on two continents. The success of this experimental approach demonstrates the effectiveness of current communications capabilities to apply these methods.

Due to modelling limitations, the other tools utilized as part of the NPP and irradiator case studies did not lend themselves to application to the transport case study scenarios chosen.

The use of a checklist is a simple and effective method for assessing the security arrangements in place against prescriptive requirements. This approach can be undertaken quickly, usually during a facility walk down, and requires no specialist understanding of the theoretical and mathematical approaches to system effectiveness assessment. It requires no specialist equipment such as computers as it can be done using pencil and paper.

Since each type of tool, or analysis technique, has strengths and weaknesses, several tools could be used in a complementary fashion during an assessment to take advantage of the strengths and offset the weaknesses of each type of tool. For example, path analysis tools are useful because they look across many possible adversary paths. However, if the path analysis tool only addresses P_I, then some approach for estimating P_N or P_E will be necessary.

The NUSAM project has successfully developed a methodology that can be appropriately used across a wide range of NM and other radioactive materials facilities. This enables security managers at most nuclear and radioactive material facilities and activities to perform performance based, risk informed SAs to determine the adequacy of security arrangements and the likely effectiveness of any proposed compensatory measures.

A methodology is only of value if it can be used easily by a practitioner. If the NUSAM project had only focused on developing a strategic methodology as provided in this report, the overall value of the project would be marginal to the stakeholders in nuclear security. The output would be limited to being a good research project for presentation at technical and specialist conferences, but not much more.

The NUSAM project went beyond just developing a strategic methodology by testing the methodology against hypothetical facilities based on realistic situations. The fully documented case studies for a wide range of facilities and activities will be of value for training, specialist skills development and implementation guidance. These case studies validated the use of various analysis tools and methods and the overall NUSAM methodology.

The NUSAM CRP can be considered a success as it met the project objectives and has provided a validated approach for the assessment of security arrangements at a variety of sites, facilities and activities.

Appendix I

PERFORMANCE ASSURANCE METHODS

I.1. INTRODUCTION

There are many types of performance assurance methods ranging from simple to complex, prescriptive based to performance based, limited to full scope, manual methods to computer simulations, as well as combinations of methods. Table I.1 lists types of performance assurance methods with a short description and an example for each method.

TABLE I.1. PERFORMANCE ASSURANCE METHODS

By Hand	Description
Checklists against prescriptive requirements	A checklist is a qualitative tool for determining presence/absence of required features or of adequacy/inadequacy of a required capability (so called because the user checks off whether the presence/absence or adequacy is present). Checklists are valuable for looking at how a system meets requirements from a high level perspective, allowing the user to identify areas that need deeper evaluation. Note that the checklist may also record adjectival scores that are assigned by an expert, such as 'high', 'medium' or 'low' effectiveness of some equipment or security procedure against the DBT based on inspection of the equipment or an analysis of a procedure.
Observation	Watching a process taking place or a procedure being performed to provide insight about how well the process is taking place or procedure is being performed. This method is often used where the evaluator does not want to disrupt the process/procedure with more intrusive methods, say for determining if a two-person rule is being performed correctly. An example of observation is when the evaluator sits in an alarm station to see whether the alarm station operators are assessing alarms correctly.
Random sampling	A method for determining a set of items to examine (selecting intelligently from that set of items) and then assigning some conclusion about the set. Sampling can be used to determine items to inspect (that is to review or examine for certain required features) or to performance test. As an example, the evaluator may select from a set of material transfer forms, see whether each of the forms are filled out correctly, and then make a determination of how well site personnel are adhering to procedures for filling out the forms. As another example, sampling might be used to determine which sensors to test during an audit if that site has many alarms. Sampling may involve selecting all items, either in the complete set itself or in a subset meeting some criteria, or may involve random sampling.
Tabletops	Description
Map exercises	An exercise performed by people using small models of guards, RFs and adversaries performed on one or more maps
Scale model (sand table) exercises	An exercise performed by people using small models of combatants performed on a scale model of a facility or area with terrain features, vegetation, roads and buildings shown in scale. (This is called a sand table exercise because it was historically performed on a table where the terrain was modelled in sand.)
Computer based exercises	An exercise performed by people using icons of guards, RFs and adversaries that are moved on a computer display of a facility

TABLE I.1. PERFORMANCE ASSURANCE METHODS (CONT.)

Computer Simulations	Description
Human in the loop	Humans control activities performed by computer generated adversaries and defenders within an environment modelled in a computer
Constructive simulations (automated behaviour)	Computer generated adversaries and defenders are controlled by software routines (not people) within an environment modelling in a computer
Single path	Calculates P_I for one path
Performance Testing	**Description**
State/competent authority testing laboratories for barrier testing only	Facilities funded and operated to support testing of access delay systems involving either active or passive delay. Such facilities may be run by other State agencies, such as the military. Experts from these facilities develop delay times against the DBT to be used in evaluations and provide guidance for facilities on making upgrades.
State/competent authority testing laboratories for RF equipment	Facilities funded and operated to support testing of RF equipment, such as weapons, protective gear and fighting positions. Such facilities may be run by other State agencies, such as the military. Experts from these facilities provide guidance on RF equipment to use at facilities, training required for such equipment, and may support FoF exercises.
Facility level tests (includes component testing and subsystem testing)	These include functional/operability tests that ensure individual components are working, standardized maintenance performance tests that insure that such components meet performance requirements, simulated adversarial attack tests by skilled testers, and tests of physical protection subsystems to determine, for example, if an alarm generated on the perimeter is acknowledged and assessed properly by alarm station personnel.
Alarm response test	Performance test of RF readiness and response to an alarm by a group of responders that move to a specific location.
Response Tests	**Description**
Limited scope performance test	Tests to determine the level of a single person in performing security force or guard force responsibilities. Examples: effectiveness of searches, assessment of alarms by Central Alarm Station, use of force procedures.
Force-on-force exercises	A performance test of the physical protection system that uses designated personnel in the role of an adversary force to simulate an attack consistent with the threat or the design basis. Typically, this is a full scale field simulation of an attack on a site involving all on-site guards and RFs.

Appendix II

TECHNIQUES FOR CHARACTERIZING PERFORMANCE METRICS

II.1. INTRODUCTION

Effectiveness evaluations depend on performance metrics such as delay times, detection probabilities, and PRT. There are basically three methods for characterizing these performance metrics for systems and components: statistical data, use of expert judgement, and use of models and simulations. This section will focus on the first two topics.

The performance metrics used in evaluations are as follows.

- Detection
  - Probability of detection;
  - Time for communication and assessment;
  - Frequency of nuisance alarms.
- Delay
  - Total delay time;
  - Time after sensing.
- Response
  - Probability of communication to RF;
  - Communication time;
  - Probability of deployment to proper location;
  - Deployment time;
  - Probability of neutralization.

II.1.1. Neutralization time

These metrics are tested, estimated and simulated under various environmental/operational conditions and defeating methods. Since these conditions are very wide, complete test data is impossible to achieve and, hence, SMEs may extrapolate it from known values.

It is advisable that inherent uncertainties of the metrics be considered. Getting a meaningful number of test samples is difficult in many cases for budget limitation: e.g. explosives test and force-on-force exercises. These metrics usually estimate human performances of adversaries, who do not want to be estimated. It is advisable to limit the accuracy of the probability of detection to a first digit or use a conservative approach.

Simulations may need information on the status of the physical protection system at a particular time. A common way to represent this information is using what is called a ‘picture in time’. A ‘picture-in-time’ records information such as where guards and RFs were located, whether they were in vehicles, and the status of alarms, at a specific time that the information was collected.

The settled metrics values may be modified by consequent tests and simulations considering assumptions and extrapolation methods used by SME.

II.1.2. Statistical data

This method records one or more observations or values, typically through statistical sampling. Examples include: delay times for defeating a barrier, times for responders to perform some task, the number of times a central alarm station operator properly identifies someone between perimeter fences and whether an alarm is triggered when someone enters the area that the alarm is supposed to be

monitoring. Where such data exists, classical statistical techniques can be used such as maximum likelihood estimators, confidence intervals and hypothesis tests.

It is common to have only one observation for a barrier defeat time. In such cases, that observation can be treated as a point estimate. If two or more identical tests are performed, then the variance of the defeat time can be estimated.

Typically, when a result is binary (e.g. the alarm successfully triggers or it fails to), the total number of successes, X, out of the total number of tests, N, is assumed to follow a binomial distribution with probability of success p. This information can be used to estimate p as the ratio X/N or to create a confidence interval for p. It is sometimes possible to estimate the components of PRT based on several exercises (e.g. by having guards/RFs on different operational shifts perform the exercises several times per year). In such cases, a conservative approach to setting PRT is to select some percentile (e.g. 75th percentile value) rather than use an average value.

II.1.3. Use of expert judgement

In some cases, either insufficient or no data exists or there is no safe way to correctly collect the data (as might happen when the event is a violent violation of a two-person rule). In such cases, the evaluation would depend on values elicited from experts.

Some models and simulations may only use point values; in such cases, the experts would determine what the values were. In some cases, the model/simulation requires distributions of values. There are several ways to develop such distributions using experts:

- For response or delay times, one approach is to have one or more experts estimate a minimum time and maximum time (or a 5^{th} and 95^{th} percentile time) subjectively. Then the expert(s) would subjectively determine other necessary properties about the distribution, such as the type (triangular, uniform, log normal and beta, etc.) and any variables that are not specified (such as the most likely value (mode) of the triangular distribution).
- For probabilities, it is common to assume that the expert's subjective distribution for the probability can be described by a beta distribution with parameters α and β. There are two approaches to fitting a beta distribution: 1) determine a 5^{th} and 95^{th} percentile for the probability – so that the experts feel 90% sure that the true probability falls between these values – and to determine *a* and *b* from those limits; 2) have the expert determine the probability – call it the value P^* - and how many observations they believe their estimates is worth – call this value M – and then to set Eq. (3) and Eq. (4):

$$\alpha = P \times M \tag{3}$$

and

$$\beta = (1 - P^*) \times M \tag{4}$$

In the 1970s and early 1980s, security simulations developed in the United States assumed a triangular distribution for delay times with the mode set at the (single) observed delay time taken from an actual test with the minimum and the maximum times set by experts. In such cases, statistical data was combined with expert judgement to develop the three parameters needed for the triangular distribution. Other models assumed PRT and delay times follow normal distributions where the standard deviation is some multiple of the mean (e.g. the standard deviation is 0.3 times the mean).

Sampled statistical data can also be combined using Bayesian statistics. As one example binomial counts for numbers of detections, X, out of N tests can be combined with values of α and β for a beta prior distribution determined by an expert to produce a posterior distribution for the probability that would follow a beta distribution as shown in Eq. (5) and Eq. (6):

$$\alpha' = X + \alpha \tag{5}$$

and

$$\beta' = (N - X) + \beta \tag{6}$$

The analyst could then use the posterior distribution to develop an estimate of the probability as well as create tolerance intervals, analogous to confidence intervals developed solely for statistical data.

In some cases, data may exist but may only cover a subset of the required values; this is especially true when using values from a data library. As an example, transit times for adversaries may be collected during exercises but the values would be influenced by what the adversary is carrying, weather conditions, whether they are being fired upon, and how far they were going. In such cases, expert judgement may be used to extrapolate transit times (or transit time distributions) from the data sets that do exist. Similar comments can be made about detection probabilities, delay times, and weapon probability of hit/probability of kill (P_H/P_K) values: the data libraries produce reference values typically based on tests performed under ideal conditions (e.g. weapons fired under ideal weather conditions and nobody shooting back) and an expert is used to modify those values to reflect actual conditions. Note that this use of expert judgement introduces variability due to expert judgement which can be addressed using competent authority guidance about adversary capabilities or by using formal elicitation techniques.

Appendix III

DESCRIPTION OF MATHEMATICAL MODELS FOR USE IN NUCLEAR SECURITY ASSESSMENT

III.1 INTRODUCTION

There are a number of mathematical models that can be used as part of nuclear SAs. Some of these are already described in Section 2.5. This section will briefly describe several other models:

- Communications models;
- Line of sight models between an observer or camera and some entity being observed;
- Hearing models for guards, RFs, and intruders;
- Weapons effects models;
- Probability models used for calculating the probability of several OR'd and/or AND'd events.

III.2. COMMUNICATIONS AND LINE OF SIGHT MODELS

Communications models may be relatively simple and can be used in path analysis and TT exercises for determining if facility alarm stations and guards can communicate with off-site forces; as an example, see Appendix IX. More complex communications models can address RF propagation based on a number of factors; these models are typically used in computer simulations. Such propagation models address the physics involved, with different models typically for propagation inside buildings and exterior to buildings.

Line of sight models relate how much detail (in pixels) is available to the observer given obstacles in the way; requirements for detection, classification and identification of the entity being observed; and the size and lighting of that entity. Detailed line of sight models are primarily used in computer simulations while very simplified models can also be used in TT exercises.

Further details about these models are beyond the scope of this publication.

III.3. HEARING MODELS

In some cases, one significant method of detecting the adversary is through on-site guards and RFs directly hearing adversary activities, especially those activities that are noisy. Modelling guard and response hearing during an adversary attack can then be an important factor in making the results more precise and realistic.

Hearing models can be valuable in determining detection of the following types of events:

- Detection of the intruder's penetration through the separate areas (buildings, premises) of the site through their use of noisy mechanical tools or explosives. Such detection can be treated as equivalent to an alarm from a technical device along with signals from technical devices (sensors, TV cameras, access control and management devices etc.);
- Detection of certain events (explosion, shooting etc.) which may be used in the response modelling (e.g. pro force mission update, their action tactics etc.).

Hearing models depend upon the following types of data:

- Noise characteristics of various mechanical tools (sound level at different distances taking into account the screening effect of sound propagation hindrances);
- Explosion wave propagation characteristics depending on the distance from the sound source and human hearing thresholds;

- On-site and area testing;
- Expert evaluations.

The above aspects may be used to various degrees in various models. Further, the effectiveness of hearing can also be influenced by site specific factors (country, local conditions, temperature, humidity, vegetation, sound propagation factors etc.).

III.4. WEAPONS EFFECTS MODELS

Weapons effects models consider the effect of a number of factors on the ability of responder and adversary weapons to hit and kill their targets. Such models are important in determining whether or not intruders are neutralized either as part of mathematical models, Monte Carlo simulations or computer combat simulations.

The following weapon characteristics may be taken into consideration in such models:

- Weapon type (pistol, submachine gun, grenade, traumatic weapon etc.)
- The probability of hitting a target using small arms weapons as a function of:
  - Weapon type;
  - Distance to target;
  - Target position (standing, crouching, lying);
  - Availability of optical devices (for sniper weapon);
  - Protection devices (armour vest, helmet etc.);
  - Target mobility (fixed, moving);
  - Visibility (time of the day, meteorological conditions);
  - Capacity to perform further actions after being wounded (movements, shooting and deterioration of characteristics).
- Probability of hitting guards or intruder by grenades or explosive device based on:
  - Explosive device type;
  - Distance to explosion epicentre;
  - Armour protection.
- Further factors influencing the modelling results:
  - Ammunition capacity (total cartridges, grenades);
  - Recharge speed (pistol clip change, machine gun dispenser magazine changes etc.)
  - Cover availability (trench etc.);
  - Availability of communication means between all the action participants;
  - Action tactics.

Depending on the applicable effectiveness assessment methods and models, various types of data may be required. Information sources for above characteristics and factors:

- Regulations (manuals, procedures etc.);
- Weapons and auxiliaries record book data;
- Shooting range results;
- Force-on-force exercise results;
- Practical experience;
- Expert evaluations.

Some characteristics may be available at appropriate centralized libraries while some of them will only be obtained locally based on the local particulars (country, external conditions etc.).

The rest of this discussion will focus on two aspects of the weapon:

— The probabilities of hitting and of killing/disabling a target given an unobstructed path between the shooter and target;

— Obstacle penetration by light weapons.

There are two types of models for hitting and killing/disabling a target with an unobstructed path of the round between the shooter and target:

— Probability of hit calculation based on database values. These models take a number of forms. For instance, one model determines a probability of hitting the target (P_H) and a probability of killing a human target given a hit (P_K) (or disabling a vehicle, etc.). The P_H and P_K values typically come from a database based on a number of factors described below. Another model is to include a probability of wounding a human target versus killing that target. Examples of both of these types of models are provided in Appendix XI. These models may differ depending upon whether the weapon is a direct fire weapon such as a rifle or pistol or an area kill weapon such as a grenade.

— Physics based models for probability of hit. The dispersion in the actual path of the bullet or round is determined between the shooter and target and it is directly calculated whether the bullet/round impacts the object. The probability of wounding versus killing/disabling the target given a hit also needs to be determined; the latter probabilities typically come from databases, perhaps modified depending upon the energy still present in the impacting bullet/round.

The following is one general algorithm illustrating how to combine both of these aspects:

(1) Shooter and target coordinates (x, y, h) are identified where h is the height.

(2) The bullet pathway is determined between the shooter location ($X_{shooter}, Y_{shooter}, H_{shooter}$) and the target location ($X_{target}, Y_{target}, H_{target}$). Based on the differences in height, $H_{shooter} - H_{target}$, the final bullet pathway point may be redefined.

(3) Objects intersected by the pathway are identified, sorted out according to their distance from the shooter, and listed.

(4) Each listed object's influence on the bullet pathway and parameters such as energy is consecutively evaluated:

  (a) Based on the current bullet parameters and random number generators, the bullet coordinates relative to the object or target are randomly determined taking into account the object's cross section. The bullet coordinates ($X_{object}, Y_{object}, H_{object}$) are then superposed on the object (obstacle or target) cross section pattern.

  (b) The effect of the bullet's hitting the object is analyzed and a decision is taken concerning its influence on the subsequent bullet pathway and parameters. Three outcomes may follow: the bullet's bypassing the object (with no influence on the bullet parameters), the bullet's running through the object (with an influence on the bullet parameters) and the bullet's sticking in the object.

  (c) Based on the object type and the bullet energy, the influence of the impact on the object is calculated.

(5) A similar approach to step 4 is taken to determine the effect of the bullet on the final target.

III.5. PROBABILITY MODELS

Probability models used in nuclear SAs generally relate to determining the probability of AND'd and OR'd events. Equations for determining probabilities of N events, where $N > 2$, can be inductively determined given equations for 2 events; thus, this section will only describe equations for 2 events.

Let E_1 and E_2 be 2 events and $P\{E_2|E_1\}$ is the conditional probability that E_2 occurs given that E_1 occurs. Further define the complement of E_1, $\overline{E_1}$, as the event that occurs if E_1 does not; then Eq. (7) is:

$$P\{\overline{E_1}\} = (1 - P\{E_1\}). \tag{7}$$

Finally, we can define two events as being independent if the knowledge of one occurring does not change the probability that the other occurs. Mathematically, this means, if events E_1 and E_2 are independent then Eq. (8) is:

$$P\{E_2|E_1\} = P\{E_2|\bar{E}_1\} = P\{E_2\} \tag{8}$$

Then for AND'd events then Eq. (9) is:

$$P\{E_1 AND\ E_2\} = P\{E_2|\ E_1\} \times P\{E_1\} \tag{9}$$

There are two useful relationships for the conditional probability $P\{E_1|E_2\}$:

- If events E_1 and E_2 are independent then Eq. (10) is

$$P\{E_1 AND\ E_2\} = P\{E_2\} \times P\{E_1\} \tag{10}$$

  where $P\{E_2|E_1\} \leq 1$.

It is common to assume that sensing and assessment are independent events so that $P\{Sensing\ AND\ Assessment\} = P\{Sensing\} \times P\{Assessment\}$ models events such as detection which occurs if Sensing AND Assessment occurs.

The bound on $P\{E_2|E_1\}$ implies $P\{E_1 AND\ E_2\} \leq the\ smaller\ of\ P\{E_1\}$ and $P\{\ E_2\}$.

For OR'd events then Eq. (11) is:

$$P\{E_1 OR\ E_2\} = P\{E_1\} + P\{E_2\} - P\{E_1 AND\ E_2\} =$$
$$P\{E_1\} + P\{E_2|\overline{E_1}\} \times P\{\overline{E_1}\} = P\{E_1\} + P\{E_2|\overline{E_1}\} \times (1 - P\{E_1\}) \tag{11}$$

Where $\overline{E_1}$ is the complement of the event E_1, Eq. (12) is:

$$P\{\overline{E_1}\} = (1 - P\{E_1\}) \tag{12}$$

There are two useful relationships for independent events:

- If events E_1 and E_2 are independent then Eq. (13) is:

$$P\{E_1 OR\ E_2\} = P\{E_1\} + (1 - P\{E_1\}) \times P\{E_2\} \tag{13}$$

  where $P\{E_1 OR\ E_2\} \geq the\ larger\ of\ P\{E_1\}$ and $P\{\ E_2\}$.

In general, it is difficult to model dependent events so most probability models assume independence between OR'd events. There are two special cases that are discussed here:

- E_1 and E_2 represent sensing on complementary sensors 1 and 2 respectively. Intuitively this means that the two sensors are configured so that if the adversary is not sensed by the first sensor then the second sensor will be more likely to sense them. In this case, non detection at sensor 1 results in identical or larger conditional probability than assuming independence is reflected in Eq. (14) as:

$$P\{E_2|\overline{E_1}\} \geq P\{E_2\}\ and\ P\{E_1 OR\ E_2\} \geq P\{E_1\} + P\{E_2\} \times (1 - P\{E_1\}) \tag{14}$$

This means that treating sensing at each complementary sensor as independent events will not underestimate probabilities of detection or interruption.

- E_1 and E_2 may represent sensing events for which the probability of event E_2 given $\overline{E_1}$ is lower than the independent model: $P\{E_2|\overline{E_1}\} < P\{E_2\}$. A hypothetical example of this would be two adversaries attempting to get through an entry control point using forged picture badges that are viewed by a guard. If the guard does not notice that the first person's badge is forged (however that was done), then the guard presumably has a lower chance of detecting the second adversary's badge as a forgery either because the guard doesn't recognize the type of forgery that both are

using or perhaps because the guard is fatigued at that time of day. In such a case, one might use the inequality $P\{E_1 OR\ E_2\} \geq P\{E_1\}$. This approach can be taken to estimate the probability that m adversaries are attempting to go through an access control point without being detected: the probability that any of the m are detected is set at the probability that the first adversary is detected.

Appendix IV

CONSEQUENCE ANALYSIS

IV.1 INTRODUCTION

The PPS is to protect essential assets against unauthorized removal and sabotage. In both cases, it may be necessary or useful to determine the maximum radiological consequences for relevant scenarios within, or beyond the boundaries of the DBT.

IV.2. SABOTAGE

In case of a sabotage scenario, the objective is to ensure that the radiological consequences do not exceed certain design limits. For a fixed site facility, different types of consequence analysis may be used (e.g. during the process of identifying vital areas). However, depending on the design strategy for the PPS, radiological consequences may or may not be excluded altogether even with a sufficient protection of the vital areas. If limited radiological consequences may occur as a result of some scenarios included in the DBT, it may be useful to be able to investigate how these consequences depend on the particular assumptions regarding adversary capabilities. This may be useful as a sensitivity study to demonstrate sufficient margin against the design limit (a part of the security case) or it may be used to test for sustainability with respect to future modifications of the DBT (a part of the basis for economic considerations). There may also arise a specific need for such beyond DBT scenarios to respond to an actual threat of a specific nature (e.g. to advise on continued operation or shutdown of an NPP).

To perform consequence analysis, information present in the facility's safety analysis report (SAR) may be useful. For example, does the analysis of internal hazards like fire and flooding contain information on the safety significance of structures, systems and components in fire cells and routes for dispersal of water? Analysis of external hazards like strong winds may contain information that helps in the identification of safety import structures outside protected buildings. In some situations, the information in the safety analysis report may be used directly, in others the existing analysis may need to be modified using security specific boundary conditions.

In addition, severe accident analysis included in the safety analysis report can provide information on expected releases in extreme scenarios where core damage cannot be excluded. Similarly, for transportation of radioactive material, consequence analysis may be used to determine maximum releases following a postulated sabotage.

IV.3. UNAUTHORIZED REMOVAL

Unauthorized removal may result in two primary consequences. The material may be used in a radiological dispersal device or in a nuclear explosive device.

In case of an unauthorized removal scenario for use in a radiological dispersal, radiological consequences can occur. These consequences depend on the lost material and its form, but potentially also on the adversary objective as defined in the DBT. A certain material could be assumed stolen due to its economic value, in which case consequence analysis may not be necessary. In another case, the material is assumed to be stolen for the purpose of building a radiological dispersal device and the potential consequences may be very relevant to assess. In this case, where explosives are involved, it may be necessary to use military type calculation tools.

If Category I quantities of high enriched uranium or plutonium are removed from a facility, much more significant consequences may occur. If this material is removed from a facility, an adversary may construct a nuclear explosive device that could be delivered to a major metropolitan area or a major public event. Such a device could have consequences that are orders of magnitude larger than would be seen from a radiological dispersal device, resulting from a variety of effects from the detonation of such a device.

Appendix V

PATH ANALYSIS

V.1. INTRODUCTION

Path analysis proceeds, in a general way, to determine measures of effectiveness of a physical protection system based on comparison of an adversary timeline and one or more response timelines.

Path analysis primarily focuses on the measure P_I as a key measure of PPS effectiveness against an adversary attack (other such measures will be discussed in a later section).

P_I is defined as the probability that the RFs will arrive and deploy in time before the adversary has completed the attack. P_I is calculated using an adversary timeline and a response timeline. Figure V.1 depicts the adversary timeline at the top, indicating the adversary task time it takes the adversary to complete all of his tasks, and the sensing opportunities along the timeline, which may cause the adversary to be detected. Below the adversary timeline, there is a comparison between the PRT and the adversary task time remaining on the path after first sensing at each possible sensing opportunity.

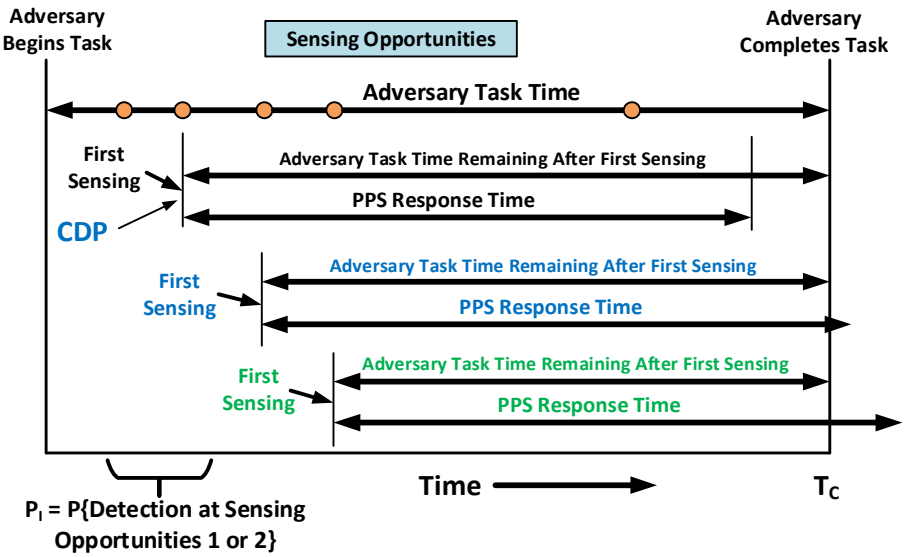


FIG. V.1. Relationship between the adversary timeline and the response timeline

If PRT < adversary task time remaining after first sensing, then the corresponding sensing opportunity is considered timely; if this is not the case, then the opportunity is not timely.[6] P_I is equivalent to the probability that the adversary is detected during at least one of the timely sensing opportunities. For the example in Fig. V.1, the first two sensing opportunities are timely, so P_I = P (detection at sensing opportunity 1 OR sensing opportunity 2). The CDP is the last sensing opportunity on the adversary timeline that is timely, in this case sensing opportunity 2.

The discussion below starts with a definition of adversary and response timelines based on a generalization of a path called an adversary action sequence (AAS). This more general abstraction of a path is used because it accurately describes both insider and outsider attacks and provides a linkage to simulation of an adversary attack plan. The discussion will then present formulas for determining P_I based on the two timelines and will then discuss how path analysis is performed.

[6] This model is called 'timely detection' and not 'timely sensing' because the timing for the beginning of the detection process is the sensing event; hence from a timeline perspective timely detection equates to timely sensing.

V.2. ADVERSARY AND RESPONSE TIMELINES

The adversary timeline is composed of a sequence of times, each associated with a task that an adversary needs to complete to accomplish their objective of unauthorized removal or sabotage. Each time within the timeline represents how long it would take an adversary to complete that task, given characteristics about the adversary that might be specified within a TA/DBT. Thus, the sum of the times represents how much time is required for carrying out all the tasks included in the adversary attack, from the start of the attack in a place where the adversary is not likely to be detected (traditionally termed 'off-site' in evaluation tools) until the last task where their objective is completed.

The adversary timeline will depend on the AAS. The most general definition of an AAS is as a time ordered sequence of *n* tasks that the adversary has to complete. An AAS can be thought of as a detailed plan of what a complete adversary team or a single individual would need to accomplish to effect an unauthorized removal of nuclear or other radiological material or sabotage.

In carrying out the action sequence there are places on the timeline where sensing may occur. Sensing is defined as the generation of some anomaly that could be evidence that an unauthorized adversary action is under way. The places on the timeline where sensing may occur are called 'sensing opportunities'. Each sensing opportunity has an associated probability of sensing (P_S) and an associated probability of assessment (P_A) which is the probability of a correct assessment conditioned on sensing occurring.

Traditionally, it is assumed that each task has an associated sensing opportunity but this not a necessary assumption about AASs. For the discussion below assume that there are N tasks, with times $\tau_1, \tau_2, \ldots \tau_N$ and that there are J sensing opportunities, with probabilities of sensing $P_{S1}, \ldots, P_{Sj}$; J probabilities of assessment $P_{A1}, \ldots, P_{Aj}$; and J probabilities of detection computed as stated in Eq. (15).

$$P_{Dj} = P_{Sj} \times P_{Aj} \tag{15}$$

To keep the discussion general, we will assume that there is a time T_{Rj} (time remaining on the adversary timeline after sensing opportunity j); the time remaining will depend on the task times, τ_n, in a way that will be discussed later.

Once sensing occurs (an alarm is generated or an anomaly is noticed), there are a set of actions that the guard and/or RF will perform to counter the adversary; these actions are depicted on a response timeline. These actions will include 1) assessing the alarm/anomaly to determine if it is indeed due to an unauthorized act, 2) communicating with relevant RFs and 3) deploying those forces to interrupt the adversary before they complete all tasks (see Fig. V.2). The total time from the alarm being generated (at T=0) until sufficient forces arrive to be able to interrupt (in this case, at T_3) is called the PRT.

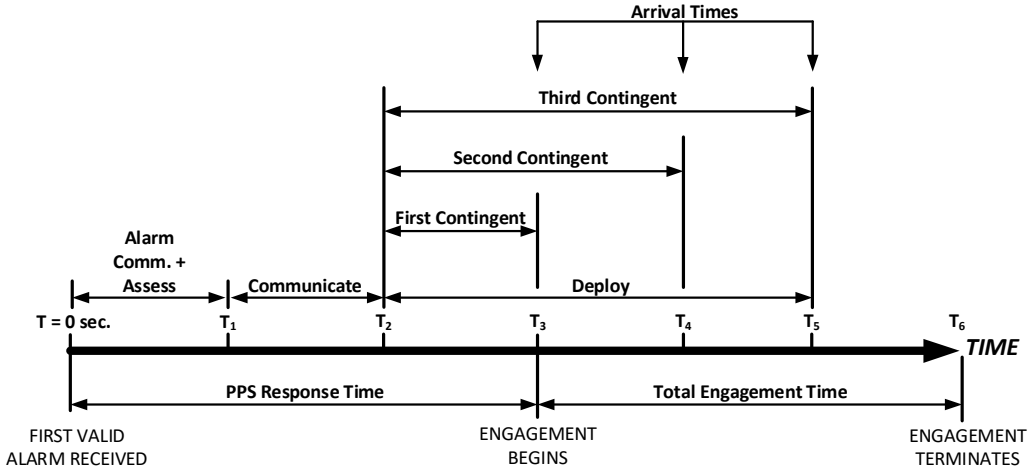


FIG. V.2. Arrival times for the RF

In principle, every sensing opportunity may have its own unique response timeline (and associated PRT).

It can be noted that in some cases different RFs may arrive at different times; in Fig. V.2, forces show up at different times (T_1, T_2, T_3); the forces that show up at each time are called contingents in this figure even if their arrivals at the same time are not coordinated. Three contingents are shown in Fig. V.2 resulting in values PRT_1 (which is the PRT shown), PRT_2 and PRT_3.

From a path analysis perspective, any of the contingent arrival times could be selected within the facility contingency plan as the PRT. Thus, if there are *K* responding contingents, each sensing opportunity *j* could have *K* possible different PRTs. The notation would be PRT_{jk} = the *kth* PPS response time associated with detection occurring due to sensing at sensing location *j*[7].

V.3. OTHER ASSUMPTIONS AND MATHEMATICAL DEFINITIONS

Tasks can be viewed either generally as activities that are to be completed or more specifically as actions against physical protection measures (such as penetrating a wall or defeating a sensor) or as movement from one point to another. There is no requirement, however, that a task be performed in a particular place. For example, a task might be to 'learn the combination to the lock' which might occur in any one of a number of places.

The action sequence is assumed to be taking the adversary towards successfully completing the attack so that it is presumed that the state (however the adversary's 'state' is defined) at the end of a task is 'closer' in some sense to the objective than the state at the beginning of the task. As an example, the adversary could be physically closer to the target at the end of a transit task than at the beginning.

Delays along the AAS may be caused by the need to penetrate barriers or traverse areas but also by armed engagements with guards and RFs.

In the discussion below, probabilities are assumed to be point values while delay times and PRTs can be assumed to be either point values or to follow distributions.

Probability of Interruption (P_I): the probability that the response arrives in time to defeat the adversary before the latter complete their AAS (we will show the equation for just one contingent so the contingent index *k* will not be shown) (See Eq. 16):

$$P_I = \sum_{j=1}^{J} P_{FDj} \times P\left(T_{Rj} - PRT_j > 0 \right) \tag{16}$$

where P_{FDj} = Probability of First Detection at sensing location *j*, defined as Eq. (17):

$$P_{FDj} = P_{Dj} \times \prod_{i=1}^{j} (1 - P_{Di}) \tag{17}$$

Note: The product on the right is assumed to be equal to 1 when *j* =1, so $P_{FD1} = P_{D1}$.

Timely detection: When the time remaining, T_{RJ} and PRT_j are point values, those sensing opportunities, *j*, for which the Time remaining, T_{Rj} exceeds PRT_j are said to be timely meaning that if detection occurs at one of those opportunities interruption will successfully occur before the adversary finishes all of their tasks. When T_{Rj} and PRT_j are point values then sensing opportunity *j* is timely or it is not. If delay times or PRTs follow distributions then sensing opportunity *j* is timely with probability $P\left(T_{Rj} - PRT_j > 0 \right)$ and is not timely with probability *1*- $P\left(T_{Rj} - PRT_j > 0 \right)$.

Critical detection point: When the time remaining, T_{Rj} and PRT_j are point values, the last sensing opportunity in the AAS that is timely is the CDP (see Fig. V.1). This point is considered critical in the

[7] A more general model would define PRT_{jkn}, where n is the task on the adversary timeline associated with sensing opportunity *j*. This case will not be covered here for a number of reasons but a remark will be made about this topic at the end of this section.

sense that if detection does not occur before or at this opportunity then the adversary cannot be interrupted. An AAS does not necessarily have any timely sensing opportunities so there may not be a CDP.

Remark: It is typically assumed that all of the sensing opportunities before the CDP are also timely. While the Time remaining, T_{Rj}, stays the same or decreases further along the AAS, the PRT_js do not necessarily vary in such a way that all opportunities are timely before the CDP. The only simple sufficient condition for achieving this assumption is that $PRT_j \leq \mathrm{PRT_{CDP}}$ for sensing opportunities before the CDP.[8]

If delay times and/or PRTs follow distributions then the selected CDP may or may not actually be timely during a simulation or path analysis. A related issue is that when delays and PRTs are point values, the adversary is assumed to minimize P_D before/at the CDP and minimize delay thereafter. It is not clear how to proceed with choosing defeat methods when delay times and/or PRTs are random variables.

V.4. PROGRESSION FROM ANALYSIS OF TIMELINES TO PATH ANALYSIS

Path analysis looks at effectiveness of the physical protection system against paths as opposed to AASs. A path is a time ordered sequence of adversary tasks or actions with each adversary action/task being associated with a set of facility locations that the adversary moves through as they perform that action/task. The paths may be defined in a general way by a sequence of elements and areas from an adversary sequence diagram or by a sequence of actions performed by an insider from an adversary action sequence diagram. The same type of metrics, such as P_I, can be calculated for paths as are calculated for AASs.

This section will discuss the relationship between paths and AASs starting with adversary action sequences.

In principle, it is possible to find the most vulnerable AAS, defined as an AAS that minimizing the one or more metrics over all possible AASs from some starting point outside the facility to the target(s) and then to the end of the path. This is impractical for a number of reasons:

- One AAS can differ from another by including different numbers of tasks;
- Two AASs can be identical except that the adversary performs a single task against a single physical protection measure (e.g. a fence) using different defeat methods (e.g. cutting through the fence versus climbing over it) or using different tactics such as force, stealth, and deceit;
- The performance data for an AAS (P_{Dj}, t_n, T_{Rj}, and PRT_j) will change depending on specifically where the adversaries are located, where they are going and how quickly;
- Performance data for an AAS may vary based on the time(s) of day, operational conditions(s), weather condition(s), etc., for which the SA is being performed[9].

There are a number of ways of addressing these issues:

- Categorize each task in a AAS by a set of locations that the adversary moves through to carry out that task and perform the search for the best AAS only over each set associated with the AAS. To accomplish this, those AASs that proceed through the same sets of locations would be said to follow the same path. As an example, an adversary path through an ASD might consist of the adversary: penetrating a fence, crossing a protected area (PA), penetrating a door, crossing a building interior, penetrating a certain wall, crossing a vital area and sabotaging a pump. This path 'includes' all AASs that go to these locations however defined by the analyst (e.g. penetrating a fence might refer to crossing a perimeter fence anywhere along a 3 km boundary). Thus, a large

[8] $\mathrm{TR_{CDP}} > \mathrm{PRT_{CDP}}$, which means that $T_{Rj} > \mathrm{PRT_{CDP}}$ for all sensing opportunities before the CDP.

[9] In some AASs the tasks cumulatively may extend over long periods such as hours or days, resulting in multiple times, states and weather conditions encountered during the AAS.

number of AASs are represented by a set of paths that can be searched to find the one with the lowest P_I, etc.;

— Determine conservatively (low) estimates of performance metrics by using minimum probabilities of detection and delay times across defeat methods and operating conditions. These minimum values may be chosen by the analyst but they may also be chosen based on strategies that the adversary might use (such as minimize detection down to a certain task on the AAS and then minimize delay thereafter).

— Perform analyses for each of several facility states, where the 'state' refers to operational condition(s), weather condition(s), etc., and facility targets.

Path analysis, then, includes searching over all paths looking for the one with the lowest P_I, etc. To find the best path, the other two issues need to be addressed. For example, some decision needs to be made about assigning detection and delay times based on all the different defeat methods that the adversary has at each step in the path. Finally, all facility states need to be addressed in some reasonable fashion. These issues will be discussed below.

V.5. PATH SEARCHES OVER NETWORKS

Path searches are typically performed over a network representing the sets of locations that the adversary would need to pass through to achieve their objectives. Several networks in use are described below. For example, paths can be defined on one type of network called an ASD (see Fig. V.3). In this diagram, the long rectangles represent security areas where an adversary can travel while the squares represent security features that the adversary would need to defeat such as gates (GATs) and Doors (DORs).

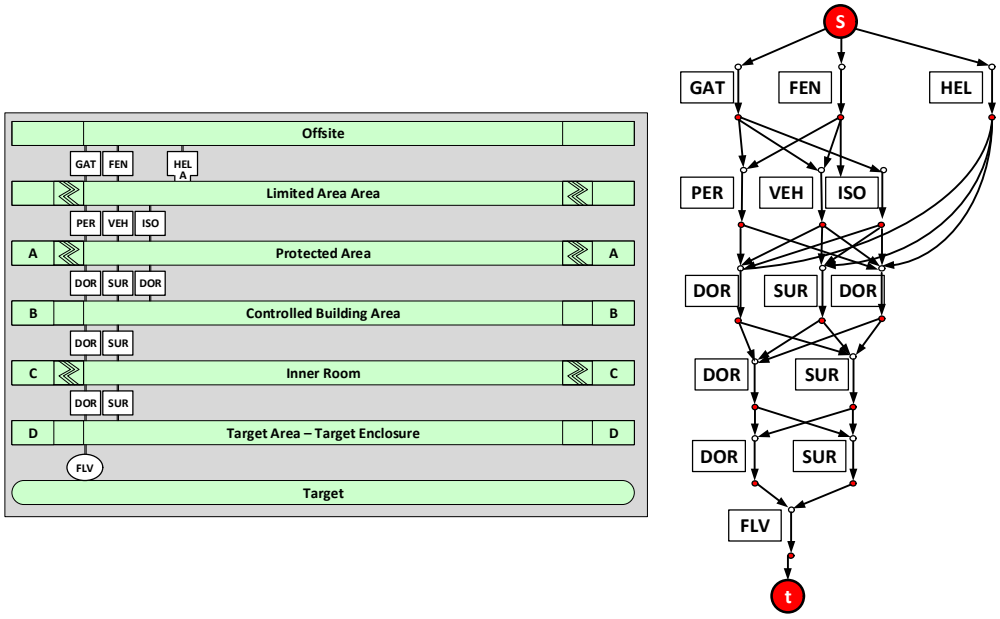


FIG. V.3. Example of an adversary sequence diagram and associated network

This ASD could be simplified just to show the boundaries of formal security areas, such as limited access area, protected area, inner and vital areas.[10] The network equivalent of the ASD is shown on the right side of Fig. V.3. Arcs representing the tasks performed at elements such as the personnel portal (PER), vehicle portal (VEH), and isolation zone (ISO) are indicated with thicker arrows. The narrow arrows represent crossing areas, such as the PA between the PER and the surface (SUR). In this model, all P_D

[10] In this example, everything within the controlled room boundary, between it and the controlled building area, might be in a vital area.

and delay times are assigned to the arcs; the nodes merely serve as transition points between adjacent arcs. The red circle with an 's' is the source node where the adversary starts and 't' is the terminal node where the adversary completes their AAS to achieve their objective.

Alternatively, the paths through the facility can be represented by movement between nodes of a mesh or grid network as shown in Fig. V.4. Note that the mesh may consist of different types of polygons (such as squares, hexagons, and triangles) and the polygons may be regular (that is with identical sides and angles) or irregular where these sides and angles vary between polygons. The mesh or grid may be two dimensional or three dimensional. Two paths could differ merely by passing through different grid points even though the physical protection measures that are attacked, such as walls and sensors, are identical. Alternative types of networks are visibility graphs, quad trees and Voronoi diagrams; all of these are used in robotic path planning.

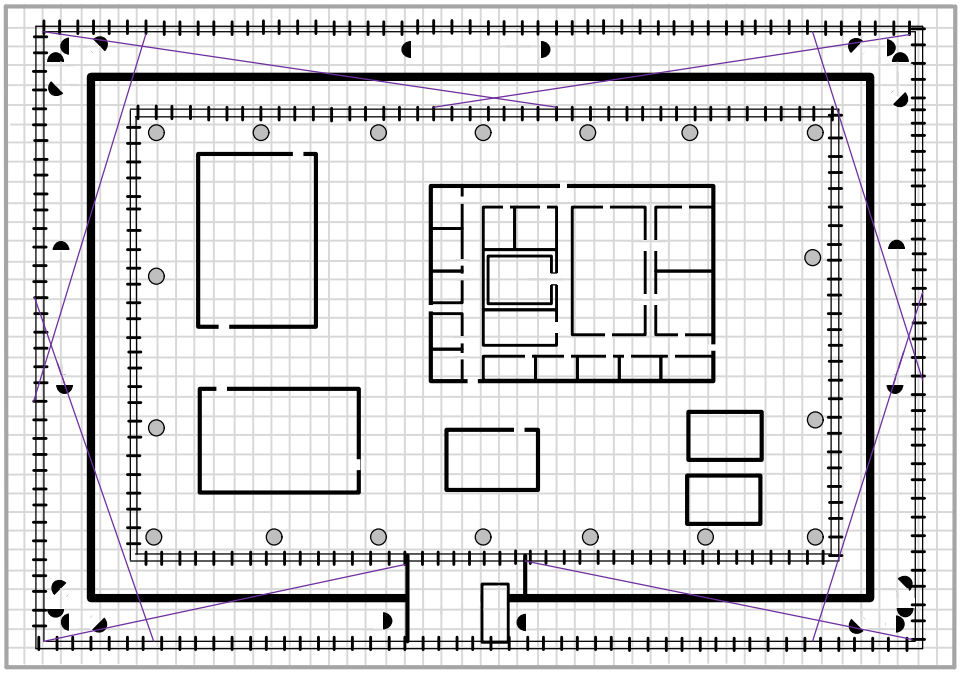


FIG. V.4. Example of a mesh associated with a facility

Two important issues arise with respect to performing path analysis on these networks:

- How does one ensure that the MVP through the network (e.g. from the defenders' concern about low P_I) is identified?
- How does the analyst deal with mobile elements of the physical protection system, such as guards and RFs that might interact with the adversary on the path?

In some cases, shortest path algorithms, such as Dijkstra's or A* methods, can be used to find the MVP. These algorithms can only be used, however, under certain conditions that need to be verified in the underlying model. For example, such algorithms typically require detection probabilities, delay times, and PRTs to be point values (as opposed to following distributions)[11].

[11] It is possible to sample probabilities and times from distributions *N* times and to solve for MVPs through *N* networks treating the values as if they are point values. This approach comes up with *N* MVPs calculated under slightly different assumptions, which can provide information about how the uncertainty in data affects results. This is different, however, from trying to find the MVP through the network taking those same distributions into account.

In other cases, though, such algorithms cannot be proven to work. In such cases, one of several approaches can be taken:

- Have the analyst determine the path;
- Keep the network small enough that an algorithm can review all of the paths by brute force (as has been done with ASDs);
- Perform some global search method that is likely to give the MVP, such as genetic algorithms.

V.6. DETERMINING WORST CASE PROBABILITIES AND TIMES

Even for a single path, there is still the issue of how the adversary performs each task to defeat individual physical protection measures. Several types of decisions come up; for example, if the task is penetrating a fence, does the adversary attempt to climb a fence or cut through it? If they decide to cut through it, what tool(s) might they use, and what delay time against the DBT would be used? If adversaries use wire cutters to cut through the fence what is the associated probability of detection?

There are two main ways of making these decisions:

- Use expert judgement: In this case, one or more experts decide what the best defeat methods are and what the associated delay times and probabilities are.
- Use information about where the CDP is on the path: In this approach, the analyst selects defeat methods that minimize delay starting at the end of the path until a CDP is found; and then minimizes detection back to the start of the path.

As discussed earlier, the CDP can only be defined when detection probabilities and times are point values.

V.7. OTHER METRICS BESIDES PROBABILITY OF INTERRUPTION

Other performance metrics can be used instead of P_I. Two simple metrics are just cumulative P_D along the entire path (whether that detection is healthy or not) and total delay along the entire path.

There are two approaches to attempting to find the path with the lowest P_E:

- Other software attempts to find the path with the lowest estimate of P_E based on a combination of path analysis integrated with some sort of combat simulation. Before using such software, it is useful to find out what metric is actually being modelled and to learn about how closely the software can be shown to find one of the most vulnerable paths in terms of that metric.
- Use Eq. (18)

$$P_E = P_I \times P_N \tag{18}$$

  where both P_I and P_N are calculated assuming a given PRT. In this case, P_I comes from a most vulnerable P_I path while P_N is computed using some other tool, such as a combat simulation.

One complication for determining PRT for this second approach is that, typically, different groups of responders arrive at different times (e.g. on-site forces arrive before off-site forces). An example of this is depicted in Fig. V.2 where RFs arrive in three ‘clumps’ or contingents, each in a slightly different timeframe.

Each arrival time leads to a different PRT, based on the sum of the alarm communications and assessment time, response communications time and the deployment time for that contingent of responders. Figure V.2 shows a PRT based on the arrival of the first contingent but the other two contingents could be used as a basis for PRT. The choice of PRT/contingent is chosen by first determining a PRT for each arrival contingent j as PRT_j, $j = 1,\ldots,J$ and then estimating (see Eq. (19)):

$$P_E(PRT_j) = P_I(PRT_j) \times P_N(PRT_j) \quad (19)$$

where $j = 1,\ldots, J$, where j refers to the jth RF contingent

where $P_I(PRT_j)$ is the probability of interruption for the most vulnerable path when PRT_j is assumed. Then the PRT to report is the value PRT_j* which leads to the highest product $P_E(PRT_j)$. Note that the P_N value needs to be determined assuming the adversary is detected at the last possible timely sensing opportunity, namely the CDP. P_N can be calculated using simulations, such as those found in the NPP Case Study publication, but an alternate simple approach is to use the brief adversary threat loss estimator (BATLE) software code (Ref. [17]) to calculate $P_N(PRT_j)$. The underlying model for P_N in brief adversary threat loss estimator is a continuous time Markov Chain where the transition rates are based on such variables as the number of responders, number of adversaries, their weapons, firing rates, and response/adversary exposure. The model determines P_N by integrating the appropriate differential equations defining the Markov Chain over time using Runge-Kutta numerical integration.

V.8. USE OF SENSING OPPORTUNITIES

One of the issues raised with timeline models (see Fig. V.1) is why the adversary timeline shows sensing opportunities and measure response times from sensing opportunities rather than measure from the points on the path where sensing and assessment occur. Figure V.5 addresses that issue.

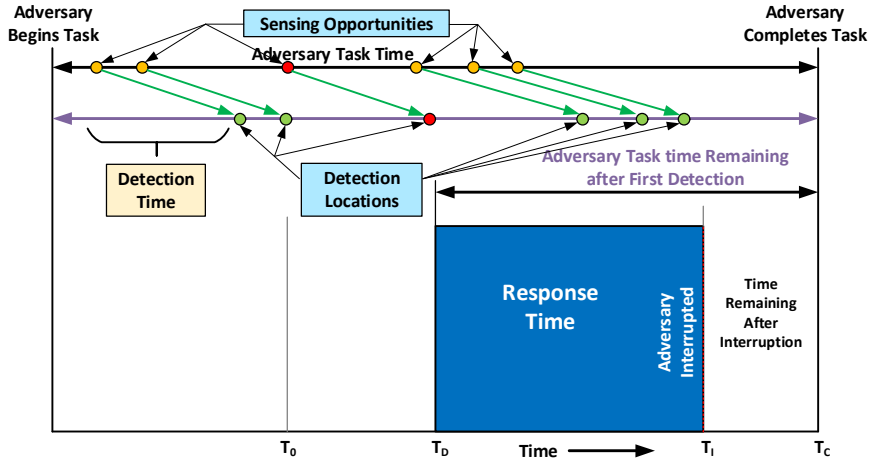


FIG. V.5. Example of a traditional adversary timeline based on sensing opportunities converted in a timeline based on detection locations

In Fig. V.5, a second timeline is displayed below the traditional timeline where the sensing opportunities (in green) on the second timeline have been shifted to the right by the amount of time taken to assess the alarm (detection time). These shifted 'sensing opportunities' are now labelled as 'detection locations' because those are the points on the adversary timeline where assessment is completed. Note that the CDP is the same whether using Fig. V.1 or Fig. V.5 because in Fig. V.5 only the response time is measured after the shifted CDP. The complication here is that the adversary position on the timeline at a particular detection location does not match where the adversary actually was when the corresponding alarm was generated. In the example in Fig. V.5, if sensing occurs at the end of task 3 (the CDP), the detection location is actually depicted in the middle of task 5.

Appendix VI

METHODS FOR DETERMINING CRITICAL SYSTEMS IN EVALUATIONS

VI.1. INTRODUCTION

This section discusses several generic methods for determining how to defeat components, subsystems and entire physical protection systems. These can be classified generally as logic diagrams (which include fault trees, physical protection logic trees, and attack trees) as well as failure mode and effects.

Conceptually, logic diagrams and failure mode and effects are deductive and inductive methods of analysis, respectively. Deductive methods answer the question 'how can some system failure state occur' while inductive methods answer the question 'what happens if…'? Logic diagrams start with some top level undesirable event, such as release of NM (as in vital area identification) or failure of the communications systems with the off-site response, and then represent the combinations of component and subsystem events that can cause that top level event. Inductive methods, such as failure mode and effects, start with some possible event, such as cutting an alarm cable or defeating certain equipment in a vital area and then try to deduce all of the effects that may occur as a result of that event. The two methods are complementary, as logic diagrams can be used to determine what types of adversary defeat methods to apply failure mode and effects analysis to, while failure mode and effects analysis can verify, to a certain extent, the logic diagram. Additional detail can be found in Refs [10 and 16].

VI.2. LOGIC DIAGRAMS

The logic diagram is a useful tool for evaluating security for a nuclear facility. Following a basic discussion of logic diagrams, this section will discuss fault trees, physical protection logic trees and attack trees[12].

VI.2.1. Overview of logic diagrams

The logic diagram is a graphical representation of combinations of events that can result in a specified state or event. For our example, the specified state is a hypothetical release of significant amounts of radioactive material from a notional nuclear plant that causes HRC as a result of sabotage of critical components.

Figure VI.1 illustrates the symbols that are used in logic diagrams. The logic diagram shown represents relationships between events. Each event will have a written description in the large rectangle in the logic diagram. A smaller rectangle placed immediately under the description will show the event name or label. Event names are brief and are formed from combinations of letters and numbers.

[12] In practice, attack trees and fault trees are often used in different ways (e.g. adversary costs/resources might be associated with nodes in attack trees while probabilities might be associated with leaves in fault trees) but, in principle, probabilities could be applied to attack trees while costs/resources could be applied to fault trees.

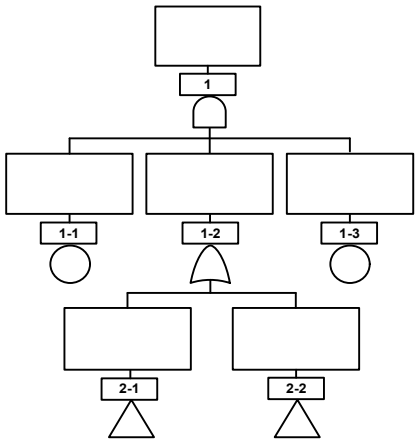


FIG. VI.1. Logic diagram symbols

The symbols of the logic diagram shown in Fig. VI.1 (logic gates, events and transfer options) will be discussed in detail below.

VI.3. LOGIC GATES

Two kinds of logic gates, the AND gate and the OR gate, are used in the logic diagrams. Gates have inputs and may or may not have an output. Inputs enter the bottom of the gate; outputs exit the top of the description rectangle above the gate.

VI.3.1. AND gate

The shape of the AND gate is a round arch with a flat bottom (see Fig. VI.2). For the undesired event described above the AND gate to occur, all of the events that have an input into the AND gate must occur. Thus, if any one of the input events can be prevented, the event described above the AND gate will be prevented. In this example, the top event is generated by an AND gate whose inputs are events 1–1, 1–2 and 1–3. Thus, the top event will only occur if events 1–1, 1–2 and 1–3 all occur.

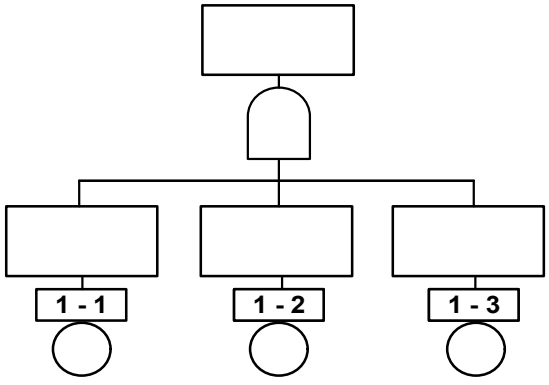


FIG. VI.2. Example of an AND gate

VI.3.2. OR gate

The shape of the OR gate is a pointed arch with a curved bottom (see Fig. VI.3). For the undesired event described above the OR gate to occur, any one (or more) of the events that input to the OR gate must occur. All of the input events must be prevented in order to prevent the event described above the OR gate. For example, in Fig. VI.3, the top event has an OR gate whose inputs are events 1–1, 1–2 and 1–3. Thus, the top event occurs if one or more of events 1–1, 1–2 or 1–3 occur.

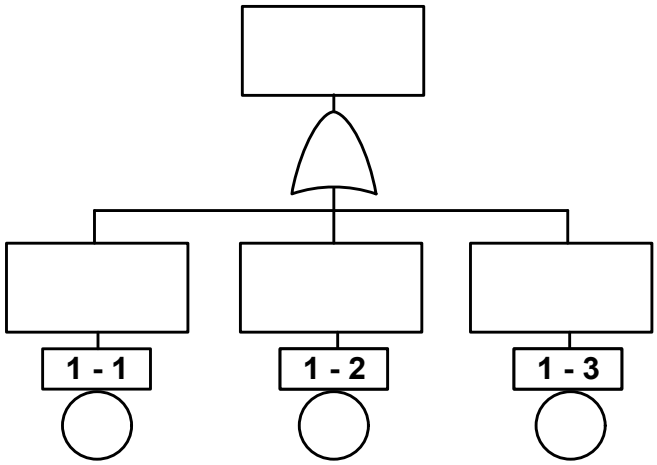


FIG. VI.3. Example of an OR gate

VI.4. EVENTS

There are several types of events in logic diagrams: end events, intermediate events and primary events.

VI.4.1. End events

If an event is not used as input to another gate, it is called an end event. Logic diagrams have only one end event, the topmost event of the tree. In Fig. V.1, event 1 is the end event. Sometimes this event is also called the treetop.

VI.4.2. Intermediate events

Events that have both inputs and outputs are called intermediate events. In Fig. VI.1, event 1–2 is an intermediate event.

VI.4.3. Primary events

Events that do not have an input are called primary events. They represent the start of actions that ultimately generate the end event. Two types of primary events are distinguished by the symbol that appears immediately below the name of the primary event: the basic event and the undeveloped event.

The basic event is symbolized by a circle below the rectangle. A basic event can be understood and evaluated qualitatively or quantitatively, depending on the purpose of the analysis, without further development of the event into causes or specific cases. In Fig. VI.1, events 1–1 and 1–3 are basic events.

The undeveloped event is symbolized by a diamond below the rectangle. An undeveloped event is an event whose causes are insufficiently understood to be included in the logic diagram. For the purpose of evaluation, the undeveloped event is treated as a basic event. The conclusions drawn from the analysis of a tree that contains an undeveloped event are tentative and subject to revision. In Fig. VI.1, event 2–2 is an undeveloped event.

VI.5. TRANSFER OPERATION

The transfer operation is represented by an upright triangle. Event 2–1 in Fig. VI.1 is a transfer operation. The transfer operation is used to make the graphic display of the logic tree more compact and readable. Since many logic diagrams, as they are developed, occupy a wide left to right space across a page, it might be necessary to disconnect the development of an event and place it at a more convenient position on the page or on another page.

VI.6. FAULT TREES

The logic diagram is a useful tool for determining the potential unauthorized removal and sabotage targets for a nuclear facility. One type of logic diagram, called a fault tree, graphically represents the combinations of component and subsystem events that can result in a specified undesired state. Among other things, the fault tree is a useful tool for determining sabotage targets for a nuclear facility.

For the example discussed here, the undesired state (or event) is a release of significant amounts of radioactive material from the plant as a result of sabotage of critical components. The physical protection system is intended to prevent sabotage of these components. Logic diagrams that are intended to identify the sets of components an adversary would have to sabotage to cause the radioactive release are called sabotage fault trees. Sabotage fault trees are used for identifying vital areas. They describe, in this case, the hypothetical actions an adversary would need to accomplish to cause sabotage, and they can be used to identify the areas (locations) to be protected in order to prevent sabotage.

Figure VI.4 shows the top portion of a sabotage fault tree for a hypothetical pressurized water reactor.

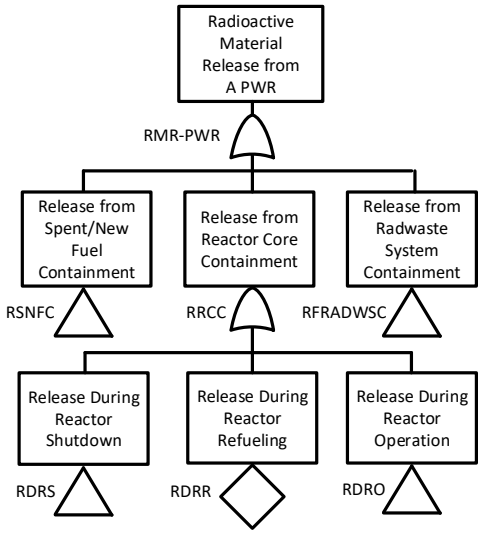


FIG. VI.4. Top portion of a sabotage fault tree for a hypothetical pressurized water reactor

VI.6.1. Physical protection logic trees

Physical protection logic trees were developed to depict all the ways for defeating areas and protection layers of physical protection systems. Figure VI.5 is a logic tree indicating several ways to defeat a perimeter gate using force, stealth or deceit. Traditionally, this tree would be part of a 'boundary' logic tree covering all of the ways to defeat the entire facility perimeter. Note that the tree does not yet describe how the lowest level events are caused. For example, how the adversary will attempt to avoid detection going under the gate is not specified.

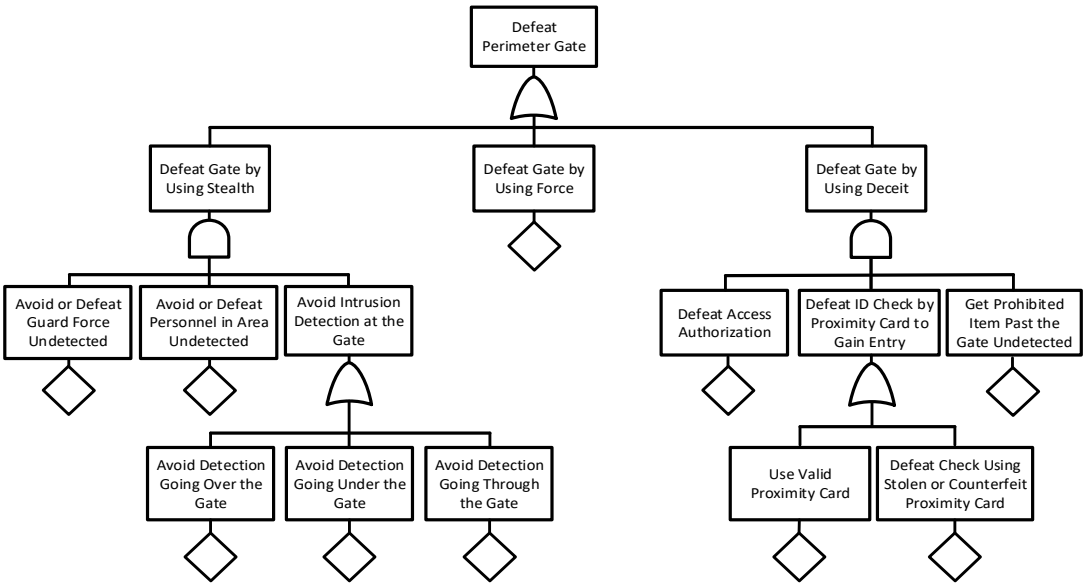


FIG. VI.5. Example of a physical protection logic tree

VI.6.2. Attack trees

Attack Trees are logic diagrams showing how some top level event can be caused (in this sense they are deductive like fault trees). The attack tree has a root representing some undesirable event, child nodes that if true make the direct parent true, ultimately resulting in leaf nodes, which are the lowest level nodes in the tree. In Fig. VI.6, the top node is ‘defeat proximity card authentication’ which organizes possible ways to attack a hypothetical proximity card. To better understand the diagram, note that:

— Any of the child nodes being true causes a parent node in Fig. VI.6, except where an ‘and’ is indicated in the diagram (such as ‘obtain PIN’ AND ‘obtain card’) where all the specified child nodes must be true.

— The colouring in the diagram attempts to convey the same information without having to duplicate subordinate attack trees. For example, the black arrows proceeding into and out of the target user node indicate that the adversary can obtain the card by targeting the user by threatening, bribing or blackmailing them. The red lines indicate that the adversary can target the user to obtain the personal indentification number (PIN) the same way but can also shoulder surf or carry out social engineering, which is impractical for obtaining the card.

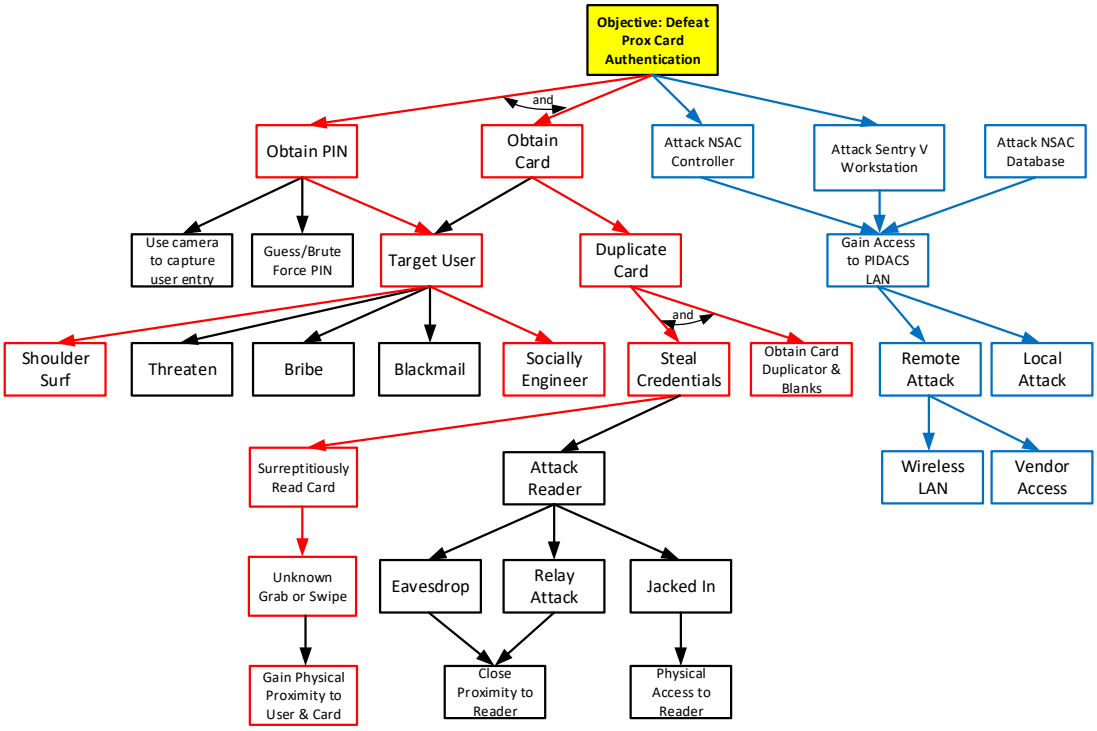


FIG. VI.6. Example of a hypothetical attack tree to defeat proximity card authentication

Notice that the highest level node in this hypothetical attack tree, 'defeat proximity card authentication', is one way to cause the lowest level event 'defeat check using stolen or counterfeit proximity card' in the example hypothetical physical protection logic tree displayed above. Another way to defeat the check with a stolen proximity card is makeup a convincing story why the adversary has a proximity card but cannot get in so that a gullible employee would let the adversary in.

Appendix VII

FAILURE MODES AND EFFECTS

VII.1. INTRODUCTION

Failure modes and effects analysis (FMEA) is an inductive approach that may provide additional information on the importance of different critical structures, systems and components that make up the physical protection system. This information can be of use when developing strategies related to management of failures of non-malicious origin, or of other situations where functionality is degraded.

The critical structures, systems and components themselves may be identified through the use of physical protection logic trees if these are sufficiently detailed. If the level of detail is judged to be too high (e.g. on the systems level in a situation where the desired management strategy is on component level) then the first step involves identification of critical 'objects' at the appropriate level of detail.

The failure modes and effects analysis has two main parts: identification of failure modes and describing the consequences, or effects, if these failure modes are realized.

VII.2. PART 1 – IDENTIFICATION OF FAILURE MODES

- Make a list of critical 'objects' (structures, systems or components depending on the purpose of the FMEA)
- Characterize the critical objects. Characterization may include but is not limited to the following:
  - Function types ('standby' (intrusion detection), 'continuous operation' (video streaming) 'delay' (a fence, …)). Note also that an 'object' may have several functions. For example, a particular physical barrier may have both the function of delaying an adversary and the function of forcing the adversary to carry a specific type of (heavy) tool, thus reducing the capability to carry large amounts of explosives.
  - Possible failure modes (degraded/unavailable/modified function, inadvertent actuation, …).
  - Failure mode probabilities (for standby functions) or failure intensities (i.e. probability per time unit for continuous operation functions) or unavailability time windows (for planned maintenance etc.).
  - Potential for common cause failure (e.g. all video image based verification of perimeter alarms unavailable due to fog).
- Define 'primary events' based on the characterization, one for each unique combination of 'object', function and failure mode (with associated data regarding function unavailability). These 'primary events' will be used as input to the effects analysis in part 2.

As an example, consider the fault tree in Fig. VI.4. The release during reactor operations event is a transfer, and one possible development is to expand that event as in Fig. VII.1.

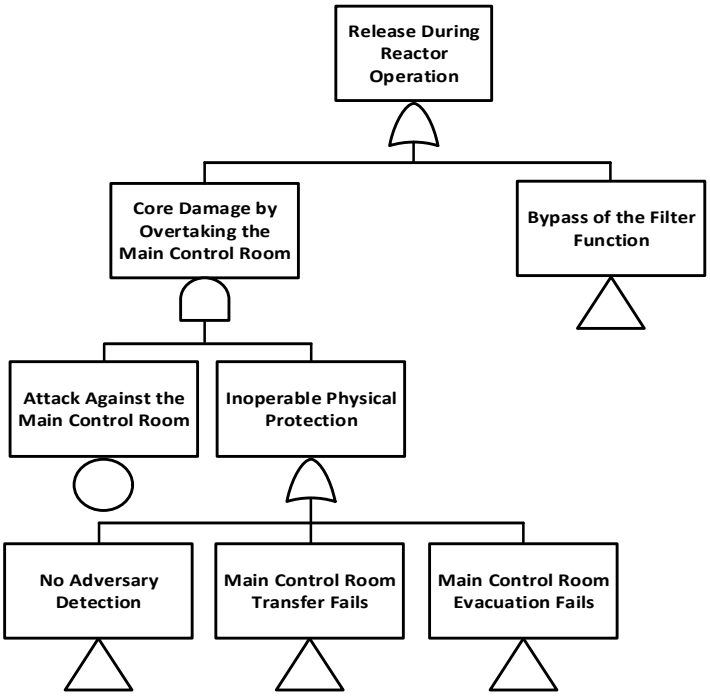


FIG. VII.1. Hypothetical expansion of the Release during reactor operations event

A part of the interpretation of this fault tree is that core damage avoidance cannot be guaranteed if either 'the adversary detection capability' is inadequate or the transfer of the functions of the main control room (MCR) is not operational or the routes for prompt MCR evacuation to a secure location are unavailable.

The definition of the critical 'objects' and how they are characterized is typically, when applicable, based on the assessment of different parts of the physical protection, as indicated below.

The associated critical object for the 'no adversary detection' event could be named 'detector' representing adversary detection capability in general. For the purpose of the failure modes and effects analysis, one possibility is to state that if any detection capability up to and including the CDP remain, this translates as 'detector is available'. The CDP(s) is typically determined along the relevant attack path(s) against the MCR using conventional path analysis.

The event 'MCR transfer fails' is associated with a hypothetical critical 'transfer button' object. For the purpose of the FMEA, one possibility is to state that if a limited scope exercise has demonstrated that the MCR staff is proficient in the procedures leading to timely actuation of the (operational) 'transfer button', this translates as 'transfer button is available'.

The final critical object ('evacuation routes') is related to 'structures'. For the purpose of the FMEA, one possibility is to state that if scheduled inspections are being performed and documented, to ensure that the evacuation routes do not get blocked; this translates as 'evacuation routes are available'.

The above critical objects are characterized below:

— 'Detector' is a standby function (safety community terminology), with the purpose of the detection of an intrusion that may threaten the MCR. An investigation could determine that it has the two relevant (accidental) failure modes 'unavailable' and 'giving intermittent false alarms'.

— 'Transfer Button' is a standby function, with the purpose of reducing the importance, if the MCR would be overtaken. An investigation could conclude that its design is such that it has one failure mode: 'unavailable'.

— 'Evacuation routes' is a standby function, with the purpose of ensuring that a hostage situation can be avoided even if the MCR is overtaken. There is only one failure mode: 'unavailable'.

‘Bypass’ of the filter function is an additional event. Core damage and ‘bypass’ in combination will lead to ‘release’. The critical object associated with ‘bypass’ is the ‘filter’ and is characterized below:

— ‘Filter’ is a standby function, with the purpose of mitigating the radioactive releases in the event of core damage to amounts below the applicable unacceptable radiological consequence (URC) limit. It has only one failure mode - ‘unavailable’.

Based on this identification procedure, five primary events are identified:

(1) Unavailable ‘detector’;

(2) ‘Detector’ giving intermittent false alarms;

(3) Unavailable ‘transfer button’;

(4) Unavailable ‘evacuation routes’;

(5) Unavailable ‘filter’.

This concludes part 1 of the failure modes and effects analysis for this fault tree. All relevant fault trees need to be analyzed in the same manner before proceeding to step 2.

VII.3. PART 2 – EFFECTS ANALYSIS

— Build or modify existing physical protection logic trees, where ‘primary events’ from the failure modes analysis are incorporated;

— Use the logic trees to determine the consequences, or effects, of different combinations of failures;

— Determine the importance of different failures (represented by the new ‘primary events’), either deterministically – are remaining physical protection capability sufficient or not? – or probabilistically – to what extent is the overall effectiveness of the physical protection system influenced? If the importance is different for different classes of adversaries or scenarios, this information may support development of dedicated compensatory measures for each adversary class or scenario.

The fault tree may now be completed to the desired level of detail (see Fig. VII.2). The same five primary events could be present in many fault trees, but for the case of this example it is assumed that there is only one relevant fault tree.

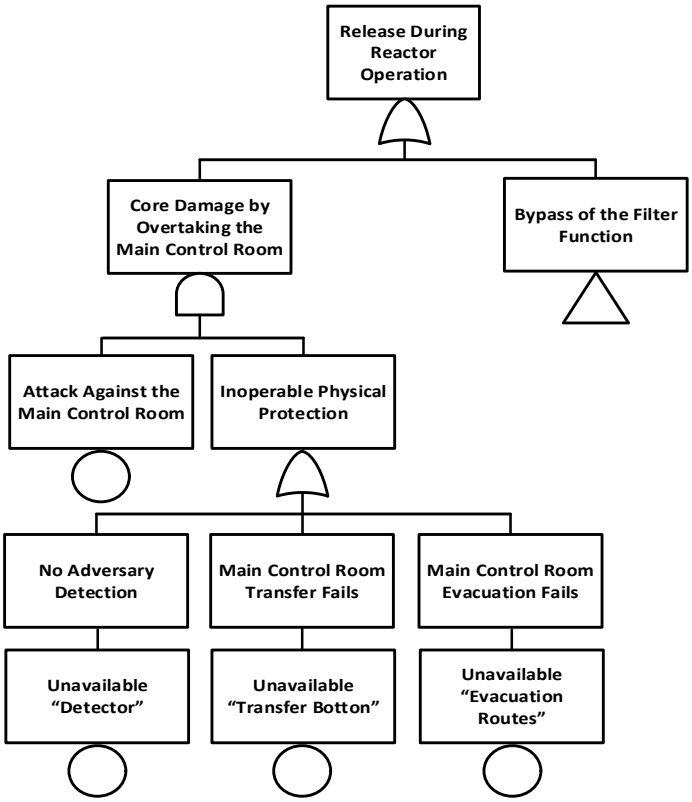


FIG. VII.2. Release during reactor operations fault tree with incorporated primary events

By analyzing the completed fault tree and considering the failure modes, it can be concluded that some combinations of faults will have the consequence 'inoperable physical protection' with respect to sabotage events (attacks) directed towards the MCR. However, the primary event 2, where the detector gives a false alarm, still leaves the physical protection essentially operational. The consequences may be considered to be economic in nature. In summary:

Primary events 1 and 5	⇒	'vulnerable to attack' (potential URC)
Primary events 3 and 5	⇒	'vulnerable to attack' (potential URC)
Primary event 4 and 5	⇒	'vulnerable to attack' (potential URC)
Primary event 2 (false alarms)	⇒	'economic consequences'

It follows that the 'transfer button', the 'evacuation routes' and the 'filter' need to be fully operational. The object 'detector' needs to be able to fulfil its function, but physical protection capability is still sufficient even if the false alarm rate from the 'detector' is elevated compared with specification.

Appendix VIII

DETERMINE EFFECTIVENESS FOR EACH SCENARIO

VIII.1. INTRODUCTION

Metrics are methods for measuring things, in this case some facet of how well the security system performs against an AAS.

VIII.2. PHYSICAL PROTECTION SYSTEM PERFORMANCE MEASURES

Metrics can be categorized by whether they are determined quantitatively or qualitatively.

There are a number of performance measures that may need to be characterized either quantitatively or qualitatively during the assessment:

- P_S
- P_A, given Sensing
- P_D (Sensing AND Assessment) = $(P_S \times P_A)$
- P_I
- P_N, given Interruption
- P_E (Interruption AND Neutralization) = $P_I \times P_N$
- Delay Times, τ,
- PPS Response Time, PRT

These measures can be estimated for each element or task in a path or scenario or can be accumulated for portions of an entire path/scenario, either from the beginning of the path/scenario up to some element/task or from some element/task to the end of the path/scenario.

Quantitative models typically assign a probability, such as P_S, P_A, P_D and P_I. Some models determine P_N (and P_E) quantitatively, while others include qualitative scores as well, assigning Very High, High, Moderate or Low, etc., to describe P_N and P_E

Probability of System Effectiveness, P_{Ej}, can be determined for a particular sensing opportunity j, along the path/scenario in the following way (See Eq. 20):

$$P_{Ej} = P_{Sj} \times P_{Aj} \times P_{Ij} \times P_{Nj} \tag{20}$$

where

- P_{Sj} = probability of sensing at j
- P_{Aj} = probability of assessment given sensing at j
- P_{Ij} = probability of interruption on the rest of the path/scenario given detection at j
- P_{Nj} = probability of neutralization, given interruption on the rest of the path/scenario

Overall P_E, is then related to the individual sensing opportunity P_{Ej} as follows:

Note that we can define $P_{Di} = P_{Si} \times P_{A\mathbf{i}}$ = Probability of detection at the *ith* sensing opportunity (neglecting detection anywhere else on the path)

The P_E equation can be represented a slightly different way (See Eq. (21)):

$$P_E = \sum_{j=1}^{J} P_{FDj} \times P_{Ij} \times P_{Nj} \tag{21}$$

Where P_{FDi} is the probability that the adversary is detected for the first time based on sensing opportunity j (See Eq. (22)):

$$P_{FDj} = P_{Sj} \times P_{Aj} \times \left\{ \prod_{i=1}^{j-1} (1 - P_{Si} \times P_{Ai}) \right\} = P_{Dj} \times \left\{ \prod_{i=1}^{j-1} (1 - P_{Di}) \right\} \tag{22}$$

Cumulative probability of detection is typically accumulated from the beginning of the path:

$P_{DCumulative}(j)$ = Probability of Detection at sensing locations 1,…, j

while delay, τ, is typically accumulated from sensing location j until the end of the path/scenario (See Eq. (23)):

$$T_{Rj} = t_{afj} + \sum_{i=j+1}^{N} \tau_i \tag{23}$$

where t_{afj} is the time after sensing at sensing opportunity j (Fig. VIII.1), which measures the time from when the adversary is sensed at opportunity j until they finish the associated task.

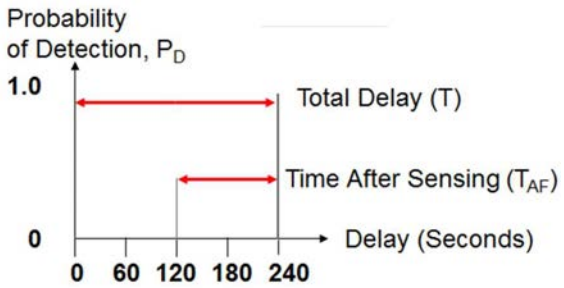


FIG. VIII.1. Time after sensing opportunity j

Probability of interruption: This is the probability that the response arrives in time to defeat the adversary before the latter complete their AAS (we will show the equation for one contingent, also).

There are several approaches for combining quantitative and qualitative metrics, depending upon the need for rigor in the assessment (see Table VIII.1):

- Approach 1: Fully quantitative.
- Approach 2: P_I components quantitative, while P_N (and hence P_E) are qualitative.
- Approach 3: Only delays and response times (which can be tested) are quantitative; all other measures are qualitative.

TABLE H-1. QUANTITATIVE AND QUALITATIVE METRICS

Performance Measure	Approach 1	Approach 2	Approach 3
Probability of Detection	Quantitative	Quantitative	Qualitative
Delay, Response Times	Quantitative	Quantitative	Quantitative
Probability of Interruption	Quantitative	Quantitative	Qualitative
Probability of Neutralization	Quantitative	Qualitative	Qualitative
Probability of Effectiveness	Quantitative	Qualitative	Qualitative

VIII.3. QUANTITATIVE PERFORMANCE MODELS

One purely quantitative performance model is P_I which is calculated as (See Eq. (24)):

$$P_I = \sum_{j=1}^{J} P_{FDj}\, P\big(T_{Rj} - PRT_j > 0\big) \tag{24}$$

Note that PRT_j is the PPS response time given sensing at sensing location j and assuming subsequent detection. This model allows the PRT to vary by where on the path/scenario the adversary is detected.

VIII.4. QUALITATIVE MODELS

Some of the metrics that can be expressed quantitatively also have an equivalent qualitative version. A common approach is to treat probabilities as qualitative values while delays and PRTs are expressed quantitatively). Qualitative probabilities are typically assigned as 'very high' to 'very low'.

For example:

- One can speak about assigning a qualitative probability of sensing and probability of assessment for sensing location j;
- A qualitative probability of detection at a sensing opportunity j would then be some function of the qualitative probability of sensing and a qualitative probability of assessment.
- Instead of trying to calculate $P\big(T_{Rj} - PRT_j > 0\big)$, a qualitative approach might be to assign a qualitative interruption score, indicating whether the response is able to interrupt the adversary somewhere along the AAS, **given** detection at sensing opportunity j. This qualitative interruption score may be based on knowledge about how the time remaining, T_{Rj}, compares to PRT_j, but also may factor in whether it is easy for the response to find the adversary, for example, an issue not explicitly considered when determining quantitative P_Is.
- For neutralization, a qualitative score for neutralization can be assigned assuming interruption has occurred. That is, given that sensing location j generated an alarm that caused a positive assessment AND the response arrived in time to interrupt, how likely is it that the adversary was neutralized?
- The contribution of sensing location j would then be a function of the qualitative scores for sensing, assessment, interruption, and neutralization (given interruption) determined for sensing location j. This would contrast with the qualitative model where the contribution of sensing location j would be $P_{FDj}P_{Nj}$.

Remark: The quantitative P_E Eq. (25) **could** include terms of the form:

$$P\{\textit{Neutralization given } T_{Rj}\text{-}PRT_j > 0 \text{ AND } \textit{detection at sensing opportunity } j\} \tag{25}$$

but this is typically impractical. Instead, a different approach is typically taken, which will be discussed shortly.

Qualitative $P_{Dcumulative}$, $P_{Interruption}$, and P_E can be determined using the metrics for each sensing opportunity as long as there are rules for assigning qualitative probabilities P(A or B) and P(A and B) based on qualitative P(A) and P(B) for events A and B, respectively. At the same time, it is impractical to combine qualitative probabilities with numerical times so there are no qualitative versions of expected time remaining, expected margin or expected deficiency.

VIII.5. TIMELY DETECTION

When delay times and PPS response times are point values then some sensing opportunities are timely in the sense that if detection occurs at one of those opportunities then interruption will successfully occur before the adversary finishes all of their tasks. One can then define P_E as (See Eq. (26)):

$$P_E = \sum_{\substack{j=1,\ldots,J \\ that\ are\ timely}} P_{FDj} P_{Nj} \tag{26}$$

This equation does match more closely with qualitative methods for setting P_E as P_{Nj} is now only counted if interruption occurs.

VIII.6. EXAMPLE OF QUALITATIVE PERFORMANCE MODEL - VISA

Vulnerability of integrated security analysis (VISA) tabletop methodology is a qualitative based assessment modelling tool than can systematically evaluate system effectiveness of nuclear security through the use of SMEs. (See Ref. [18]) The methodology is a scenario based approach based on SME opinion, documented values or a combination of both. The methodology can use either qualitative or quantitative input and can be used for existing and/or future facility analyses and for the base case and upgrade cases to document the nuclear security effectiveness for both insider and/or outsider threats against a TA or DBT.

Facility specific detection, assessment, and delay elements are modelled using the VISA methodology to evaluate the effectiveness of the nuclear security protection system and its components. Input values for detection, assessment and delay elements are based on the scenario specific details. Using site layouts, response procedures, assumed protection element delay values and adversary attack strategies, adversary and protective force response timelines can be estimated and compared to postulate interruption neutralization may be evaluated/assigned using a TT or computer based analysis, expert judgement or any combination of these methods. Through VISA analysis and SME opinion, vulnerable paths for a facility or activity can be determined and evaluated.

VIII.7. EXAMPLE METHODS FOR CONVERTING QUALITATIVE AND QUANTITATIVE PROBABILITIES

During an SA, there may be a need to convert either adjectival ratings or qualitative probabilities to quantitative values and vice versa. Reference [1] describes one method, associated with the VISA methodology, which includes a method for converting adjectival ratings, which are analogous to probabilities, to or from quantitative probabilities. This conversion method is described in columns 2–4 of Table VIII.2. An alternative method, termed the Sandia Qualitative Conversion (SQC) method, developed as part of the CRP, is reflected in columns 5–8; this is another way to convert qualitative probabilities to and from quantitative probabilities.

TABLE VIII.2. TWO METHODS FOR CONVERTING ADJECTIVAL RATINGS/QUALITATIVE PROBABILITIES TO RANGES AND MIDPOINTS FOR QUANTITATIVE PROBABILITIES

	VISA Method			SQC Method			
1	2	3	4	5	6	7	8
Adjectival Rating/Qualitative Probability	Range		Mid-Point	Range		Mid-Point	Rounded Off Mid-Point
	Lower Bound	Upper Bound		Lower Bound	Upper Bound		
Very Low (VL)	0	0.2	0.1	VVL*: 0 VL: 0.12	0.11 0.21	.06 0.16	0.05 0.15
Low (L)	0.21	0.4	0.3	0.22	0.38	0.30	0.30
Moderate (M)	0.41	0.6	0.5	0.39	0.61	0.50	0.50
High (H)	0.61	0.8	0.7	0.62	0.85	0.74	0.75
Very High (VH)	0.81	1	0.9	0.86	1	0.93	0.90

* VVL = Very Very Low

Table VIII.2 is used in the following way:

- Columns 2–4 illustrates the VISA method for determining ranges of quantitative values associated with adjectival ratings. If a P_D is assigned a low (L) adjectival rating, for example, then the corresponding range of quantitative P_D values would be 0.21 to 0.4 and 0.3 of that range would be assigned if a point value was needed. Conversely, a quantitative estimate of P_D of .37 would be assigned the same L adjectival rating.
- Columns 5–8 illustrates the SQC method to convert qualitative probabilities to ranges and midpoints of quantitative probabilities. In this approach, an L qualitative probability is assigned a range 0.22 to 0.38 with a midpoint of 0.30. The numerical ranges for the SQC method were developed to generally have the property that they are consistent with one another when combining two similar qualitative probabilities, *X*, *Y*, to assign a qualitative probability for P(*X* OR *Y*). As an example, if *X* and *Y* are both assigned an L qualitative probability, meaning that the associated quantitative probabilities are each assumed to fall into the range 0.22 to 0.38, then P(*X* OR *Y*) will fall in the range 0.39 and 0.61, which is very close to (due to round off error) the range for a moderate (M) qualitative probability. This corresponds to an assumption that two L qualitative probabilities OR'd together would be equivalent to an M qualitative probability.

The SQC method also includes an extra qualitative probability, very, very low (VVL) that is not found in the VISA method. The range associated with VVL is 0 to 0.11.

The SQC method ranges are defined to be used as part of the Sandia Qualitative (SQ) approach shown in Table VIII.2. To be complete, the SQ approach needs some rules for assigning qualitative P(*X* AND *Y*), where *X* and *Y* are qualitative probabilities. The SQ rule, in general, is to OR two similar qualitative probabilities by reducing the category one level, that is P(high AND high) = M, P(M AND M) = low and P(L AND L) = VL. With this rule the AND'd ranges are no longer consistent with one another: for example, P(high AND high) falls between 0.38 and 0.72 which includes the M range along with part of the high (H) range. The SQ approach described in Table K.1 also assigns: P(VL AND VL) = VVL and P(VH AND VH) = P(VH), where VH = very high. Note that a combination of the VISA method and the SQC method could be devised that includes all of the VISA intervals, except moving the boundary between the H and VH categories from 0.8 to 0.85. This approach might have some merit (for example, the midpoint for the H rating of 0.75 which is exactly the probability if two 0.5 probabilities are OR'd together) but this approach was not investigated due to project time constraints.

Comparing the two methods, the methods differ in that the VISA method does not include a VVL score. Of the other scores/probabilities, how close the midpoints are and how close the cut off points between ranges, with the exception of the cut off between H and VH that is higher for the SQC method, are to be noted. The ranges for the VISA method have been shown to work well as part of the VISA analysis approach, are straightforward to use, are evenly sized and do not require an extra qualitative category. The SQC method has the relative benefit that it was developed to be used as part of the SQ analysis approach. From this perspective, the analysis approach selected would typically determine which of these methods to use (e.g. the VISA method would be used if the VISA approach is used in the SA).

Appendix IX

DESCRIPTION OF TABLETOP METHODOLOGIES

IX.1. INTRODUCTION

Two TT exercise methodologies were utilized during the NUSAM assessment process. The two TT exercise methods used were the ORNL BattleBoard Methodology and the SNL TTX Methodology. Since both methods are being utilized and taught in various international training courses and technical exchanges, it was decided to compare the two methods as part of this research project.

IX.2. OVERVIEW OF A TABLETOP EXERCISE

The concept of the TT exercise will be familiar to anyone who has engaged in combat oriented board games. This analytical methodology is a low cost methodology ideal for modelling and analysis of small unit tactics, neutralization analysis, impacts of PPS systems on adversary scenarios and more. The methodology is suitable for most industries where protection may involve a combat or tactical engagement between opposing forces.

The TT exercise is a simulation that moves from start to finish and is largely a discussion by the two opposing forces (protective force and the adversary force) guided by the moderator to carry out baseline and upgraded systems and tactics.

Common uses of TT methodologies include:

- Evaluating fixed-site or transport protection systems;
- Evaluating system performance of current configurations (baseline);
- Evaluating system performance of an upgraded or changed system;
- Optimizing potential changes to procedures and system components;
- Developing and optimizing protective force tactical plans;
- Training physical security personnel on procedures and system capabilities;
- Evaluating procedural changes in the safeguards and security programme;
- Contingency planning.

The TT methodology is designed to simulate the use of protective forces to defend or respond to any event that has a protection consequence including the fire, spills, criticality or natural disasters. While a TT is not the same as a live action practice scenario or a FoF simulation, TTs can help increase communication between the various divisions responsible for protecting the material work together, familiarize people with the technology used to protect the material, and establish solid lines of communication between the various groups.

Most exercises begin with some type of TT. The TTs use scaled drawing, model, map, etc. with terrain features. The exercise uses movable tokens to represent people, protective forces, vehicles, buildings etc. to replicate actual conditions as closely as possible. All models used are evaluated for applicability and realism. The board is setup each time to model specific scenarios, and completely sanitized by removing all components and features after each play.

There are a defined set of rules for TT exercises that sets a common application of decisions to ensure fair and consistent outcomes.

Key points in the preparation and conduct of a TT include the following:

- The objectives of the TT exercise are well defined;
- A clear scenario is prepared, which includes all associated data needed to meet the objectives of the simulation;
- All logistics requirements are clearly identified and prepared (e.g. data presentation, communications, tools required by the players, etc.);
- The physical meeting location of the TT is organized to ensure the exercise can be conducted in an environment allowing all players to do their jobs efficiently. Typically, at least two rooms are needed (one for protective forces and one for adversary forces to plan and conduct the analysis). When all players are visible to the opposing side, all activities are moved to a single model to complete the analysis;
- Players are introduced and their roles and responsibilities are clearly understood by all;
- The goal of the TT is clearly explained to assess and make decisions. These decisions will be used for improving the overall response to a nuclear security event;
- All players know that they are accountable for their contribution;
- Only realistic resources are brought to the analysis.

IX.3. PARTICIPANT ROLES AND RESPONSIBILITIES

A simulation is conducted utilizing a disciplined approach that includes the roles and responsibilities of all participants. Both TT methods discussed generally utilize four categories or functions of participants during the conduct of the exercise.

- **Facilitator** – person/team responsible for running the entire exercise to ensure an accurate and unbiased outcome of the simulation. Ensures all parties act in accordance with the agreed upon rules. The facilitator has final decision making authority when parties do not agree on an issue. This person may also record all movements and engagement outcomes.
- **Protective force team** – responsible for laying out the initial positions for each response element as well as managing all response actions and reactions during the simulation according to approved defence plans, training and tactics; without personal compromise, strives to achieve system success.
- **Adversary team** – responsible for ensuring that adversary teams make plans in accordance with agreed threat and capabilities and is responsible for managing all the adversary actions and reactions throughout the simulation; without personal compromise, strives to achieve the adversary objective.
- **Arbitration team** – acts as the judges or honest brokers of the exercise. This person/team is responsible for determining a final answer to issues that cannot be resolved by the facilitator and the players which may include adjudicating the effects of all engagements using the P_H/P_K tool (explained later in this publication), defining and implementing practical detection points, communication protocols, effectiveness of closed circuit television camera, and other aspects of the PPS. **If the facilitator chooses, this person/team may be assigned the responsibility to record all movements and engagement outcomes.**

IX.4. SETTING UP THE TABLETOP EXERCISE

Prior to beginning a simulation, a number of activities are needed to confirm that everyone is planning with a consistent set of data. This process is fundamentally the same process as conducting any vulnerability analysis and reflected in Fig. I-1. These steps are fully described in Section 2.4 and 2.5.

FIG. IX.1. Planning process for a TT

IX.5. CHARACTERISTICS OF THE TABLETOP EXERCISE

Tabletop exercises are conducted in a room with a large table where a scaled model (ideally a 3-dimentional (3D) model) is used to carry out attack scenarios. These models reflect as much detail as practical to ensure accuracy of the results. Details include terrain features, movable units (people and vehicles), vegetation, buildings and roads etc.

Ideally, two TT models may be used. One TT model setup showing the protective force and another for the adversary team. This precludes the players from having a 'god's view' which will influence their command and control actions. Facilitator's place tokens on the respective boards only when they have been seen by the other side through the moves of the players.

To begin the exercise, the facilitator will facilitate discussion on defining the target, threat, facility characterization, barrier delay times and scenario development. The modelling rules of the exercise are in line with typical modelling characteristics for probability of detection, response times, engagements and weapons effects.

The protective force and adversary teams will separate and develop detailed protection plans and attack strategies to defend/attack the site or convoy. After the defend/attack plans are defined, the two teams rejoin around a table with the scaled model to be analyzed. Beginning with the adversary team, the 'players' announce their scenario moves then the protective force team announces their moves. The analysis is dynamic in that the outcomes in a scenario will change in response to the actions of the players as they implement their plans.

Both the adversary and protective forces are controlled to ensure they conduct realistic actions. Protective forces are constrained by:

- Actual procedures, tactics, tactical plans and training. Players are not permitted to make moves that are not consistent with their training.
- Equipment carried by the RFs (unless an upgrade is being modelled).

Adversary forces are constrained by an agreed upon design basis threat with:

- Force numbers;
- Insider numbers;
- Level of aggression (passive/active);
- Equipment (tool kit);
- Realistic tactics and movements.

The exercise continues until one of the following conditions is met:

- Adversaries have met their objective;
- Adversaries are no longer capable of meeting objective. Typical reasons:
  - Attrition – not enough people to complete remaining tasks;
  - Loss of an essential capability such as explosives, vehicle or tools.

Weapon effect P_H/P_K tables are an important element used in any TT analysis. The hypothetical P_H/P_K tables used in the respective methodologies were developed for training and demonstration purposes only. It is advisable to develop and validate P_H/P_K tables by each State or organization based on the weapons capabilities and proficiency of its protective forces and the anticipated adversary force.

IX.6. DOCUMENTING THE ANALYSIS

Table methodologies provide for a disciplined approach to collecting data to form the evidence file for the outcomes of the analysis and simulation. When conducting a baseline assessment, documentation for the normal operations can be referenced and used as the basis of the analysis and need not be documented again. However, when analyzing initial designs or modifications of new designs, additional documentation is needed for reference and agreement by the stakeholders to understand the characterization of the system being evaluated. In Table IX.1, the details of the scenarios evaluated are shown to provide contexts of the types of information recorded during a TT exercise.

TABLE IX.1. EXAMPLE OF DETAILS CAPTURED DURING THE TABLETOP EXERCISE

BattleBoard Analysis Timeline				
Time (seconds)	Marker ID	Marker Action	Dice Roll	Result (Miss, Wound, Kill)
0-30	Adv 1/Adv2/Adv 3	Crash into escort vehicle and wedge the vehicle into the guard rail		
	PF-1	Remains in vehicle assessing the situation		
	PF-2	Radio communication of accident to dispatch		
	Cargo Driver	Brings vehicle to a stop 10m from the accident		
	Cargo Passenger	Begins radio communication to the TCC		
30-60	Adv 1/Adv2/Adv 3	Exits the vehicle with weapons ready		
	Cargo Driver	Backs vehicle 100m in reverse		
	Cargo Passenger	Finishes communications to the TCC		
60-90	Adv 1	Engages PF1		Wounded (Combat effective)
	Adv 2	Engages PF2		Wounded (Not combat effective)
	PF1	Engages Adv 1		Wounded (Combat effective)
90-120	Adv 1	Engages PF1		Kill
	Adv 2	Engages PF1		Kill
	Cargo Driver	Stays in cargo vehicle		
	Cargo Passenger	Communicates with TCC		
120-150	Adv 1/Adv 2	Engages Cargo Driver at 90 m		Kill
	Cargo Passenger	Exits vehicle and leaves scene		
150-180	Adv 1/Adv 2	Runs 90 m to cargo vehicle		
180-210	Adv 1/Adv 2	Enters cargo vehicle and departs the scene		

The following sections will describe the two TT methods used and the validation of the differences between the two models for comparative purposes. The two TT methods are very similar during the planning, organization, conduct and documentation of the exercises as described above. The sections below will provide an overview of the methods and then discuss specific details concerning each method, primarily concerning rules associated with event outcome determination.

IX.7. ORNL BATTLEBOARD METHODOLOGY

The ORNL BattleBoard tabletop methodology was originally developed by the United States Army for theatre wide battle planning. That method was later modified by the United States Department of Energy to reflect small unit tactics, engagements and conflicts. The ORNL BattleBoard tabletop is a turn based (adversary then protective force) simulation designed to evaluate the protection system's capability in response to an attack by an adversary force. The ORNL BattleBoard tabletop helps stakeholders to identify whether or not weaknesses are present in a physical protection system that could result in a loss of material by unauthorized removal or by sabotage.

IX.7.1. ORNL BattleBoard P_H/P_K

An important decision to determine is the use of a representative P_H/P_K table. Many of the decisions made in a ORNL BattleBoard tabletop are made based on the outcomes of dice rolls which correspond to a percentage of success or failure. The most common decision is whether a shot from one team upon the other results in a miss, wound or kill. Outcomes of weapons engagements are decided based upon P_H/P_K tables based on shooter weapon, tactics proficiency, weapon type, distance, training effectiveness and environmental factors.

IX.7.2. How the simulation progresses

The following provides a brief description for each 'turn' played on the ORNL BattleBoard tabletop:

- The simulation begins with the adversary force. The adversary force will initiate each game turn by moving any, all or none of their markers. All other forces will then move any, all or none of their markers. Normally, the protective force has the second move. Each adversary and protective force turn represents activities happening in the same time increment being modelled.

- Time increments are typically played as 30 second real time intervals. This means that each time a turn has been played, 30 seconds have elapsed on scenario timeline.
- A five minute time limit is allotted to each team to make their moves on their turn.
- Once a player makes a move and that move would be observed, such as during an engagement, all tokens that are involved in that move are moved to the board so that the opposing side can see them.
- All preplanned movements and engagements will be announced to, and concurred by, the facilitator prior to beginning the simulation.
- After all movements have been completed, results of engagements will be determined and the results will be recorded on the documentation forms included below.

The rules of the TT methodologies are easy to understand and most participants are well versed in the methodology after a single simulation. However, the skill of the facilitator can greatly promote a successful process. With the rules as a basis and the ability to draw upon the expertise of the players as well as to reach out to others for technical analysis, the results can be achieved which accurately reflect an actual situation. Poorly managed simulations can result in poor data and a loss of confidence in the analysis by everyone involved.

IX.7.3. ORNL BattleBoard tabletop methodology rules

Below are the ORNL BattleBoard tabletop methodology rules.

IX.7.3.1. Engagement between forces

- Tokens represent people. Each token is uniquely identified for documentation and tracking purposes (i.e. PF 1 for Protective Force number 1);
- Adversary plans that include hidden traps, explosives, snipers, etc. are to be announced to the facilitator prior to the simulation beginning;
- A token may engage only one other token per turn;
- A token firing from a hidden position becomes visible to those in line of sight and may be engaged in that same turn;

- Multiple tokens may engage a single token during the same turn;
- Variation of success of firearm engagements is determined by the roll of two six sided dice (see the random sampling method in Appendix I). Possible outcomes of an engagement:
  - Miss;
  - Wound (wounded tokens cannot move but can communicate; dice roll to determine whether combat effective or not);
  - Kill.
- Engagement outcomes are determined by P_H/P_K tables based on:
  - Type of weapon;
  - Distance from target;
  - Observation capability;
  - Firing from armoured position;
  - Armour type if employed of the targeted token.

IX.7.3.2. Modelling armour

- Vehicles
  - No protection against explosives or rocket propelled grenades unless designed against those threats;
  - Armour piercing rounds' effectiveness based on type of armour deployed;
  - Firing small arms from a moving vehicle will not result in neutralization of tokens;
  - Soft vehicles offer no protection for tokens inside.
- Personnel
  - No protection achieved with body armour. Basis of the simulation is that both the adversary and the protective forces have the appropriate information to plan and select appropriate ammunition.
- Hardened fighting positions
  - No protection against explosives or rocket propelled grenades unless designed against those threats;
  - Armour piercing rounds' effectiveness based on type of armour deployed.

IX.7.3.3. Special weapons and equipment

- Bulk explosives:
  - Expert analysis is used to determine the amounts of explosives needed for each type of barrier to be explosively breached. Players may not attempt to use more explosives than is approved in the design basis threat. Players are to document their use of explosives in the scenario planning phase of the ORNL BattleBoard.
  - Thirty seconds of task time is required to complete a breach. This time includes:
    - Setting charge on barrier;
    - Retreat to safe location;
    - Detonate the charge;
    - Fifteen seconds to clear debris;
    - Fifteen seconds to enter breach.

- Fragmentation grenades
  - Deployed accurately a maximum of thirty metres;
  - Neutralization radius of five metres;
  - Casualty radius is fifteen metres. Roll dice for tokens 5–15 m from device to decide if combat effective;
  - Probability of neutralization is 50% (dice roll of 7 or better);
  - Dice roll for each person in the radius.
- Rocket propelled grenades
  - Not possible for targets less than twenty-five metres away;
  - One round per thirty second turn;
  - Engagement table used to determine hit or miss;
  - Controller makes decisions on combat effectiveness of tokens based on how the rocket propelled grenade(s) is used (against vehicles or structures).
- Distraction and disorientation devices
  - Maximum accurate range of throw is thirty metres;
  - Effective range is a five metres radius;
  - Tokens are combat ineffective for one turn.
- Smoke grenades
  - Maximum accurate range of throw is thirty metres;
  - Smoke dispenses for maximum of sixty seconds;
  - Effective obscure distance is twenty metres;
  - One game turn to become effective cover;
  - Effective only when wind is less than forty km/h.

IX.7.3.4. Movement of tokens

- Tokens may move ½ distance and engage a token in the same turn
- Movement distances are based on:
  - Walking;
  - Running – defensive standard;
  - Running – offensive standard;
  - Tokens encumbered with weight (more than twenty kg) or awkward items will be slowed to at least half of maximum.
- Movements of tokens will be slowed based on barriers in their path. For example:
  - A token can move 100 metres in thirty seconds (offensive standard);
  - If that token would need to overcome a fence, which takes fifteen seconds, then the movement will be limited to fifty metres.
- Vehicle movements
  - Thirty seconds for tokens to mount and start vehicle;
  - Distance travelled based on actual speed assessed as realistic for conditions;
  - Fifteen seconds for tokens to exit a vehicle and ready weapons.

IX.7.3.5. Observation capabilities

- Tokens may be observed:
  - Up to 300 m during daylight (clear) if line of sight is possible and no optics are used;
  - Up to 150 m in dark but lighted conditions;
  - Up to twenty metres during darkness;
  - Vehicles may be observed:
    - 600 m during daylight and at night with headlights on;
    - 200 m at night in lighted conditions, no headlights;
    - Fifty metres at night, no headlights.

IX.7.3.6. Other considerations

- Casualties (wounded)
  - A wounded token is laid on its side so that everyone knows the status of that position;
  - A wounded token may not move;
  - After a token has been wounded, a decision is made to determine the combat effectiveness of the token:
    - Dice role of seven or better will permit the token to be combat effective (shoot);
    - Token can only communicate with dice roles of six or less.
  - Becomes neutralized (dead) after five turns;
  - Two hits result in the death of a token.
- Man portable
  - Items less than seventy kg is considered man portable by one person.
- Other considerations
  - An advantage of the ORNL BattleBoard tabletop is its flexibility and ease to introduce new strategies for both protection as well as how a system might be attacked. When players devise a strategy not specifically governed by the rules, the facilitator will take measures to ensure adequate understanding of the proposed action by conferring with the players involved and other experts at the site or elsewhere to determine the credible application of the approach and any outcomes derived from the use of the approach. Examples may include: use of radio jamming, explosive breaching techniques, force multipliers as well as others.

Table I-2 through Table I-5 are for use during the ORNL BattleBoard tabletop analysis. These hypothetical values were developed for training and demonstration purposes only.

TABLE IX.2. ORNL BATTLEBOARD MOVEMENT TIMES

Personnel Movement Table - Defensive															
All Times in Seconds															
Metres	20	40	60	80	100	120	140	160	180	200	220	240	260	280	300
Hard Surface	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
Mixed Surface	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75

Personnel Movement Table - Offensive															
All Times in Seconds															
Metres	20	40	60	80	100	120	140	160	180	200	220	240	260	280	300
Hard Surface	3	6	9	12	15	18	22	25	28	31	34	37	40	43	46
Mixed Surface	4	7	11	15	18	22	25	29	33	36	40	44	47	51	55

TABLE IX.3. ORNL BATTLEBOARD PROBABILITY OF WOUND AND PROBABILITY OF KILL DATA FOR HANDGUNS/PISTOLS AND 9 MM SUBMACHINE GUN

Handgun/Pistol					
	Range				
Yards	7	15	25	50	60
Metres	6.4	13.7	22.9	45.7	54.9
DAY	Total Dice Roll				
Miss	2-4	2-6	2-8	2-10	2-11
Wound	5-8	7-10	9-10	11	12
Kill	9-12	11-12	11-12	12	-
NIGHT					
Miss	2-6	2-8	2-10	2-12	-
Wound	7-10	9-10	11	-	-
Kill	11-12	11-12	12	-	-
From Armoured Vehicle					
DAY					
Miss	2-6	2-7	2-12	2-12	2-12
Wound	7-11	8-12	-	-	-
Kill	12	-	-	-	-
NIGHT					
Miss	2-7	2-10	2-12	2-12	2-12
Wound	8-11	11-12	-	-	-
Kill	12	-	-	-	-

9mm Submachine Gun					
	Range				
Yards	10	25	50	75	100
Metres	9.1	22.9	45.7	68.6	91.4
DAY	Total Dice Roll				
Miss	2-4	2-5	2-6	2-8	2-10
Wound	5-8	6-10	7-10	9-10	11
Kill	9-12	11-12	11-12	11-12	12
NIGHT					
Miss	2-5	2-6	2-8	2-10	2-12
Wound	6-10	7-10	9-11	11	-
Kill	11-12	11-12	12	12	-
From Armoured Vehicle					
DAY					
Miss	2-5	2-6	2-7	2-12	2-12
Wound	6-11	7-12	8-12	-	-
Kill	12	-	-	-	-
NIGHT					
Miss	2-6	2-7	2-10	2-12	2-12
Wound	7-11	8-12	11-12	-	-
Kill	12	-	-	-	-

TABLE IX.4. ORNL BATTLEBOARD PROBABILITY OF WOUND AND PROBABILITY OF KILL DATA FOR SHOTGUNS AND 5.56 MM RIFLES

Shotgun					
	Range				
Yards	7	15	25	40	60
Metres	6.4	13.7	22.9	36.6	54.9
DAY	Total Dice Roll				
Miss	2-4	2-6	2-8	2-10	2-11
Wound	5-8	7-10	9-10	11	12
Kill	9-12	11-12	11-12	12	-
NIGHT					
Miss	2-6	2-8	2-10	-	-
Wound	7-10	9-10	11	-	-
Kill	11-12	11-12	12	-	-
From Armoured Vehicle					
DAY					
Miss	2-6	2-7	2-12	2-12	2-12
Wound	7-11	8-12	-	-	-
Kill	12	-	-	-	-
NIGHT					
Miss	2-7	2-10	2-12	2-12	2-12
Wound	8-11	11-12	-	-	-
Kill	12	-	-	-	-

5.56 mm Rifle												
	Range											
Yards	25	50	75	100	125	150	175	200	225	250	275	300
Metres	23	46	69	91	114	137	160	183	206	229	251	274
DAY	Total Dice Roll											
Miss	2-3	2-4	2-6	2-6	2-6	2-7	2-8	2-9	2-10	2-11	2-11	2-11
Wound	4-8	5-10	7-10	7-10	7-10	8-10	9-10	10-11	11	12	12	12
Kill	9-12	11-12	11-12	11-12	11-12	11-12	11-12	12	12	-	-	-
NIGHT												
Miss	2-6	2-7	2-8	2-9	2-9	2-10	2-11	2-11	-	-	-	-
Wound	7-9	8-10	9-11	10-11	10-11	11	12	12	-	-	-	-
Kill	10-12	11-12	12	12	12	12	-	-	-	-	-	-
From Armoured Vehicle												
DAY												
Miss	2-5	2-6	2-7	2-7	2-7	2-9	2-10	2-12	-	-	-	-
Wound	6-11	7-12	8-12	8-12	8-12	10-12	11-12	-	-	-	-	-
Kill	12	-	-	-	-	-	-	-	-	-	-	-
NIGHT												
Miss	2-7	2-9	2-10	2-12	-	-	-	-	-	-	-	-
Wound	8-12	10-12	11-12	-	-	-	-	-	-	-	-	-
Kill	-	-	-	-	-	-	-	-	-	-	-	-

TABLE IX.5. ORNL BATTLEBOARD PROBABILITY OF WOUND AND PROBABILITY OF KILL DATA FOR ROCKET PROPELLED GRENADES, SNIPER RIFLES, AND 7.62 MM RIFLES

Rocket Propelled Grenade				
	Range			
Yards	50	100	150	200
Metres	46	91	137	183
	Total Dice Roll			
Stationary Vehicles (Lightly Armoured)	7-12	9-12	11-12	12
Moving Vehicle	8-12	10-12	12	-
No Effect if Total Dice Roll is less than the lower range of values shown				
1 Round Per Engagement, 1 Round per turn				

M24 Sniper Rifle					
	Range				
Yards	50	100	150	200	300
Metres	46	91	137	183	274
	Total Dice Roll				
Personnel	4-12	6-12	7-12	8-12	-
Vehicle (non-armoured)	8-12	8-12	9-12	9-12	9-12
From armoured vehicle					
Personnel	6-12	8-12	9-12	10-12	-
Vehicle (non-armoured)	10-12	10-12	12	12	12
M24 vs Armoured Vehicle -- PK = 0.0 (can roll to cause a flat tire)					
No Effect if Total Dice Roll is less than the lower range of the values shown					
1 Round per engagement, 1 Engagement per turn					

7.62 mm Rifle							
	Range						
Yards	50	100	200	300	400	500	600
Metres	46	91	183	274	366	457	549
DAY	Total Dice Roll						
Miss	2	2-4	2-5	2-6	2-8	2-10	2-11
Wound	3-6	5-8	6-10	7-10	9-10	11	12
Kill	7-12	9-12	11-12	11-12	11-12	12	-
NIGHT							
Miss	2-4	2-6	2-8	2-10	2-12	-	-
Wound	5-8	7-10	9-11	11	-	-	-
Kill	9-12	11-12	11-12	12	-	-	-
From Armoured Vehicle							
DAY							
Miss	2-5	2-6	2-6	2-7	2-10	2-12	-
Wound	6-8	7-11	7-12	8-12	11-12	-	-
Kill	9-12	12	-	-	-	-	-
NIGHT							
Miss	2-6	2-7	2-10	2-12	-	-	-
Wound	7-11	8-12	11-12	-	-	-	-
Kill	12	-	-	-	-	-	-

The following forms (Tables IX.6 through IX.8) can be used during the TT analysis:

TABLE IX.6. ORNL BATTLEBOARD PROTECTIVE FORCE AND ADVERSARY DATA RECORDING FORMS

Protective Force Unit Assignment				
Controller Name:				Page ____ of ____
ID Number	Assignment	Equipment	Action	Turn

Adversary Assignments				
Controller Name:				Page ____ of ____
ID Number	Assignment	Equipment	Action	Turn

TABLE IX.7. ORNL BATTLEBOARD MODELLING SCENARIO DESCRIPTION FORMS

Tabletop Modelling Scenario Description
Scenario Description (Scenario #____)
Protective Force
Configuration:

Tabletop Modelling Scenario Description
Scenario Description (Scenario #____)
Adversary Force
Configuration:

TABLE IX.8. ORNL BATTLEBOARD ANALYSIS TIMELINE FORM

BattleBoard Analysis Timeline				
Time (seconds)	Marker ID	Marker Action	Dice Roll	Result (Miss, Wound, Kill)

IX.8. SNL TTX EXERCISE

The following describes the process used to conduct a scenario based SNL TTX methodology.

IX.8.1. SNL TTX P_H/P_K

The hypothetical P_H/P_K calculation chart tool resolves engagements and other events between the adversary and the RF. In instances in which engagements occur, the P_H chart(s) are consulted to determine the statistical probability of an event outcome based upon the weapon type, distance and rate of fire using a roll of a ten sided die. Tables IX.9 and IX.10 show the hypothetical P_H calculation charts used for human targets and armoured vehicles, respectively.

TABLE IX.9. SNL TTX P_H CHART FOR HUMAN TARGETS

Step 1	Find base P_H cross-referencing weapon type and range to target (rounds down range)								
	Weapons P_H Table								
Weapon Type	RANGE ->	10m	20m	30m	40m	50m	60m	70m	Max Eff.
	Rate of fire in 10 seconds # rounds fired								
Pistol (9mm)	2	7	5	3	1	x	x	x	50m
Assault Rifle (9mm)	2	7	5	3	3	2	1	1	100m
Weapon Type	RANGE ->	100m	300m	500m	700m	900m	1100m	1300m	Max Eff.
	Rate of fire in 10 seconds # rounds fired								
Assault Rifle (5.56)	2	7	5	3	1	x	x	x	600m
Light Machine Gun (5.56)	3	6	4	2	1	x	x	x	600m
Heavy Machine Gun (7.62)	3	6	4	2	2	1	1	x	1000m
Heavy Machine Gun (50 cal.)	3	5	5	5	3	3	3	1	1800m
Sniper Rifle (7.62)	2	7	7	5	3	1	1	x	1000m
Sniper Rifle (50 cal.)	1	7	7	5	3	3	3	1	1800m
Rocket Propelled Granade-7	1	6	3	1	x	x	x	x	500m
40 mm	1	6	3	x	x	x	x	x	350m
40 mm belted	3	6	4	4	3	3	2	2	1600m
Spotting only	n.a.	5	3	1	0	0	0	0	0
Modified spotting P_H +1 for target firing, +1 for target moving, +1 for large target, +1 fpr pos rep from friendly unit: all modifiers are cumulative. Example: P_H to spot a moving vehicle ay 700 metres is 0 + 1 + 1 = 2									

* n.a.: not applicable.

TABLE IX.10. SNL TTX P_K CHART FOR ARMOURED VEHICLES

Vehicle P_K Table							
Die Roll:	Vs. Armour*	5.56mm	7.62mm	.50 cal	40mm HEDP	RPG	9 mm (No effect on Armour)
1	Vk	Vk	VK 1 KIA	VK 2 KIA	VK 2 KIA	VK all KIA	1 KIA
2-3	1 KIA	1 KIA	VK	VK 1 KIA	VK 2 KIA	VK 2 KIA	1 KIA
4-5	No effect	1 KIA	VK	VK 1 KIA	VK 1 KIA	VK 2 KIA	No effect
6-7	No effect	1 KIA	1 KIA	VK 1 KIA	VK 1 KIA	VK 1 KIA	No effect
8-9	No effect	No effect	1 KIA	VK	VK	VK 1 KIA	No effect
10	No effect	No effect	1 KIA	1 KIA	1 KIA	VK 0 KIA	No effect

VK = Vehicle Kill (or vehicle disabled)

KIA = Personnel in vehicle killed

— Movement table – movement of humans and vehicles are an important element for any time based analysis or analysis tool. There are various factors that determine the speed for which a TTX entity moves, such as the rate of speed (slow, medium, fast, very fast), position (crawling or crouching) or method of movement (tactical). Movement speeds are disregarded in instances in which an individual is traversing large distances on foot or is carrying a heavy load. Table IX.11 is a movement table consisting of hypothetical data used during a TTX.

TABLE IX.11. SNL TTX MOVEMENT RATES

TTX Movement Rate Table						
	10 Seconds		30 Seconds		60 Seconds	
	Personnel	Vehicle	Personnel	Vehicle	Personnel	Vehicle
Slow	7 m 2 kph (crawling or crouch)	27 m 10 kph	20 m 2 kph (crawling or crouch)	80 m 10 kph	40 m 2 kph (crawling or crouch)	160 m 10 kph
Medium	13 m 5 kph (tactical movement)	133 m 48 kph	40 m 5 kph (tactical movement)	400 m 48 kph	80 m 5 kph (tactical movement)	800 m 48 kph
Fast	26 m 10 kph (running)	266 m 97 kph	80 m 10 kph (running)	800 m 97 kph	160 m 10 kph (running)	1600 m 97 kph
Very Fast	N/A	400 m 145 kph	N/A	1200 m 145 kph	N/A	2400 m 145 kph

IX.8.2. SNL TTX methodology process

The facilitator will initiate the assessment by asking the protective force team to lay the RF positions out on the map in a typical configuration and dispersion for the facility. Initially, the adversary team adversary positions will not be identified on the map. The facilitator will start the simulation by

examining the first ten seconds of the attack beginning with the adversary team's intentions. The adversary team will state each adversary element's intentions for this block of time to the facilitator. The facilitator will tell the protective force team what each RF element is going to experience during this block of time and what each element will be able to see and hear as a result of the adversary's actions. Next, the facilitator will ask the protective force team to state RF element's reactions and intentions for the same ten second block of time. The facilitator will note all individual and vehicle movements, potential engagements and other stated intentions on the white board for both teams. Once both commanders' intentions are fully understood, they are noted on the map and the facilitator looks for any adversary/protective force interactions or engagements that need to be further examined and evaluated. The arbitration team will examine each potential engagement individually and determine the following for each:

- Engagement feasibility
  - Line of site between shooter and target;
  - Range of weapon system (distance in Table IX.9).
- Characteristics of the shooter
  - Standing still, walking, running, prone, kneeling, in vehicle;
  - Type of weapon and round, number of rounds, mounted, bipod, supported.
- Characteristics of target
  - In/out of vehicle, level of armour on vehicle, speed of vehicle;
  - Body armour/level, behind cover, in prepared fighting position;
  - Prone, kneeling, standing, walking, running, low crawling.
- Run P_H/P_K calculations and declare the results of the engagement. (Tables IX.9 and IX.10)

Personnel casualties, personnel suppressed from fire and vehicle kills are recorded for both teams. The facilitator along with the green team will decide which adversary positions were exposed to the RF as a result of actions during the previous ten seconds. Those adversary positions will be noted on the map and pointed out to RF team elements that would have seen them.

The facilitator will briefly recap the actions and engagements of the previous ten seconds to the adversary and protective force teams, describing what each element would have experienced. Depending on how fast the scenario is moving, the facilitator will decide the amount of time to examine in each subsequent evolution. Typically, the initial moments of the simulation are examined in small time slices of 10 or 20 seconds. As the action of the scenario starts to slow, the facilitator may increase the time increments to a longer duration of 30 seconds up to several minutes depending on progress of the assessment.

The facilitator will ask the adversary team to state each individual adversary element's intentions for the next time period being examined. The facilitator will then explain to the protective force team what each RF element is experiencing and ask for that element's actions or reactions for the time period being examined and the process repeats itself.

The assessment will continue until the facilitator and green team decide that the analysis objectives have been met.

It is important to review necessary information so all stakeholders and supporting personnel thoroughly understand how the stage is set and what the parameters are prior to starting the TTX.

IX.9. AN APPROACH FOR VALIDATION OF TT COMBAT MODELS

IX.9.1. Background

A TT is not a real time simulation. Instead, the adversary and defender teams take turns in executing their actions. This simplified approach could potentially introduce unrealistic properties, making it more difficult to draw relevant conclusions from an exercise.

One way to evaluate this potential disadvantage is to compare simulations of situations that may occur in a TT exercise using a turn by turn approach with simulations of the same situations using a real time approach. For example, if the timeline or consequences can be demonstrated to be similar (on average) between the two approaches, this indicates that the simplified approach is valid for timeline or consequence analysis. If the evaluation identifies significant differences between the two approaches these insights can be used to facilitate the post analysis of TT exercises and/or to modify the rules of the particular TT method.

To demonstrate this evaluation strategy, two TT exercise methods were compared with a real time representation of a specific situation: symmetric combat between two groups (the adversaries and the defenders). The two TT exercise methods were the SNLTTX and the ORNL BattleBoard. The real-time representation was an analytical combat model. Two different aspects were studied, the defender win probability and the average number of remaining (combat effective) adversaries after the completed combat simulation.

IX.9.2. Method and assumptions

IX.9.2.1. Analytical model

The analytical combat model uses combat states defined by the number of defenders (D) and adversaries (A) at a particular moment, and describes the probabilities that the combat transits from one state to another. Under symmetric conditions (e.g. battle geometry, weapons, armour, etc.) defender win probability and the average number of remaining adversaries only depend on the initial number of defenders and adversaries (Tables IX.12 and IX.13).

TABLE IX.12. PROBABILITY THAT 'D' DEFENDERS WIN OVER 'A' ADVERSARIES

A \ D	1	2	3	4	5
1	50%	83%	96%	99%	100%
2	17%	50%	78%	92%	98%
3	4%	22%	50%	74%	89%
4	1%	8%	26%	50%	72%
5	0%	2%	11%	28%	50%

TABLE IX.13. AVERAGE NUMBER OF REMAINING ADVERSARIES AFTER COMPLETED BATTLE BETWEEN 'D' DEFENDERS AND 'A' ADVERSARIES UNDER SYMMETRIC CONDITIONS

A \ D	1	2	3	4	5
1	0.5	0.2	0.0	0.0	0.0
2	1.5	0.8	0.4	0.1	0.0
3	2.6	1.9	1.1	0.6	0.2
4	3.7	3.1	2.3	1.4	0.8
5	4.8	4.3	3.5	2.6	1.7

IX.9.2.2. Monte Carlo simulations

The two TT exercise methods were analyzed using Monte Carlo simulation of turn by turn actions (shooting) according to the two sets of TT rules. Defender win probability and average number of remaining adversaries were calculated based on 1000 simulated battles (500 with adversary initiative (first turn) and 500 with defender initiative). For the simulations, it was assumed that the weapon type used, both by the defenders and the adversaries, was an AK-47. The shooting distance was assumed to be 100 metres.

IX.9.3. SNL TTX rules

For each engagement (one defender/adversary shoots at one opponent) three 10 sided dice are thrown. '7 or lower' on one or more of the dice is 'a kill'. Three engagements per turn (3 × 10 seconds = 30 seconds) are allowed.

IX.9.4. ORNL BattleBoard Tabletop rules

For each engagement, two 6 sided dice are thrown. A total of '9 or higher' is 'a kill'. A sum in the range 5 to 8 is 'a wound'. '4 or lower' is 'a miss'. If the outcome is 'a wound', the two dice are thrown again to determine if the wounded fighter is combat effective or not. '6 or lower' means that the fighter is 'combat effective', and may continue shooting. If a fighter takes two 'wounds' this is defined as 'a kill'. Only one engagement per turn is allowed.

IX.9.5. Simplifications in the Monte Carlo representation

In these Monte Carlo simulations, the fighters have no identity. Within the ORNL BattleBoard rules, to be able to take the possibility of a 'wound' into account, a wound was defined as a '20% kill'[13]. In addition, since 'a wound', where the fighter is not 'combat effective' has the same effect as 'a kill' (for the purpose of determining defender win probabilities and average number of remaining adversaries), both outcomes are regarded as 'a kill'.

IX.9.6. Results

The following initial (D, A) states were evaluated:

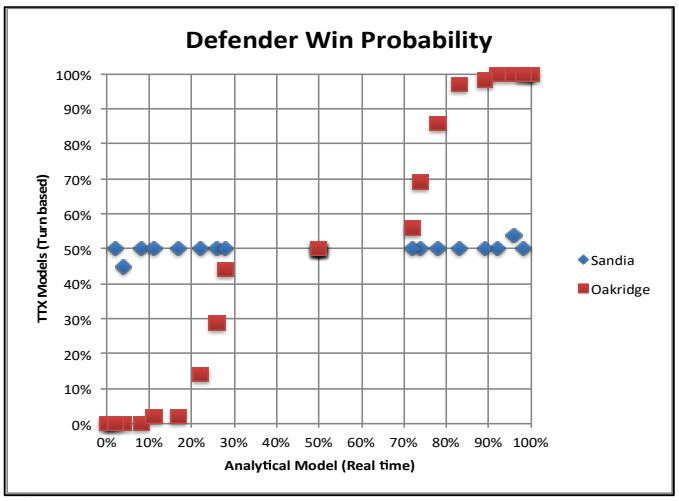
(1,1) (1,2) (1,3) (1,4) (1,5)
(2,1) (2,2) (2,3) (2,4) (2,5)
(3,1) (3,2) (3,3) (3,4) (3,5)
(4,1) (4,2) (4,3) (4,4) (4,5)
(5,1) (5,2) (5,3) (5,4) (5,5)

The results are presented as plots (see Figs. IX.2 and IX.3), where defender win probability and average number of remaining adversaries respectively for the two TT methods are plotted against the results for the real time (analytical) method.

For the SNL TTX method, the result indicated that the team who gets the initiative will most likely win, irrespective of the number of adversaries and defenders (in the studied range). This assumption was verified by repeating the simulation twice, first with adversary initiative and then with defender initiative (sees Fig. IX.4). Who gets the initiative, the adversary or the defender team, does influence the defender win probability for the ORNL BattleBoard method as well; but the effect is not as 'binary' as for the SNL TTX method (see Fig. IX.5).

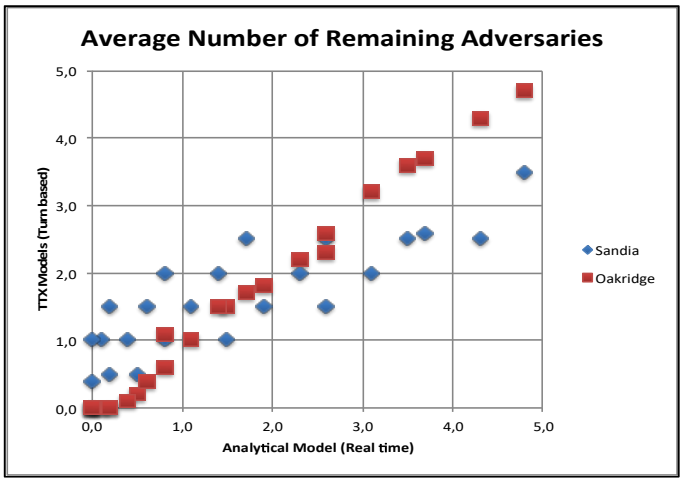
To increase resemblance with the two other methods, the SNL TTX rules were modified so that only one engagement was allowed per turn. The results before and after the modification are presented in Fig. IX.6 for defender win probabilities and Fig. IX.7 for average number of remaining adversaries.

[13] 20% was a value determined through separate simulations where fighters **did** have identity.



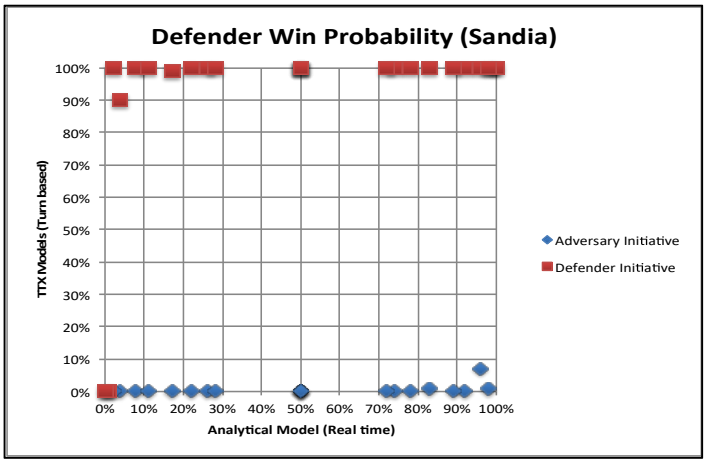
(Courtesy of P. Lindahl, OKG AB, Sweden)

FIG. IX.2. Defender win probability ('SNL TTX' and 'ORNL BattleBoard' versus 'Analytical')



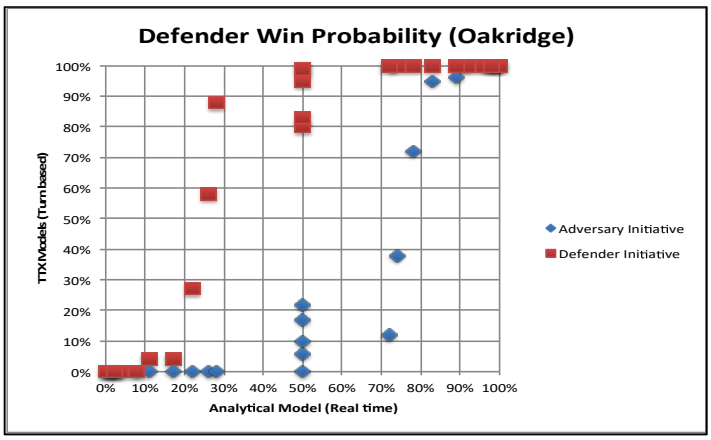
(Courtesy of P. Lindahl, OKG AB, Sweden)

FIG. IX.3. Average number of remaining adversaries ('SNL TTX' and 'ORNL BattleBoard' versus 'Analytical')



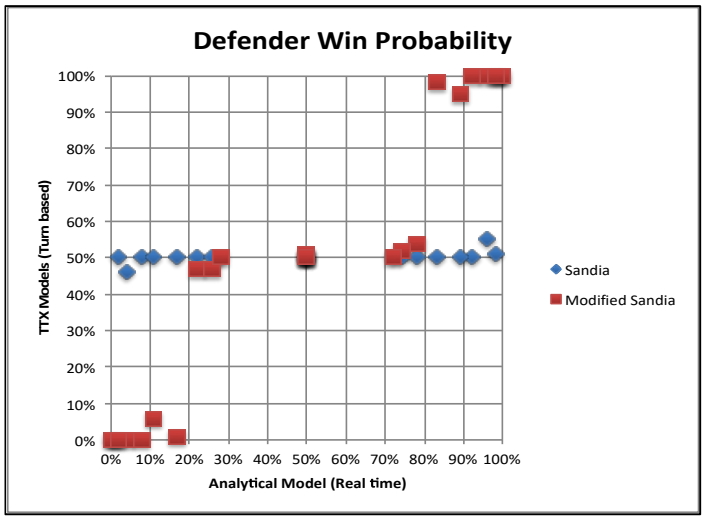
(Courtesy of P. Lindahl, OKG AB, Sweden)

FIG. IX.4. SNL TTX method effect on defender win probability versus who has the initiative (who fires first) .



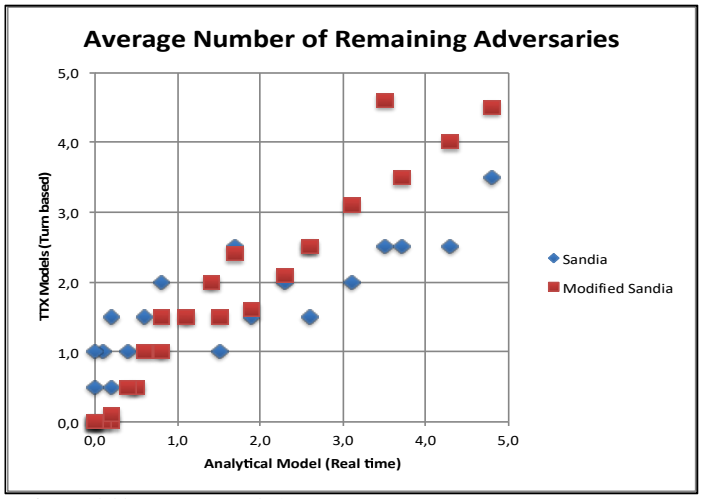
(Courtesy of P. Lindahl, OKG AB, Sweden)

FIG IX.5. ORNL BattleBoard method effect on defender win probability versus who has the initiative (who fires first)



(Courtesy of P. Lindahl, OKG AB, Sweden)

FIG IX.6. Defender win probability ('SNL TTX' and 'Modified SNL TTX' versus 'Analytical')



(Courtesy of P. Lindahl, OKG AB, Sweden)

FIG. IX.7. Average number or remaining adversaries ('SNL TTX' and 'Modified SNL TTX' versus 'Analytical')

IX.9.7. Conclusions

The ORNL BattleBoard method was essentially consistent with the real time method. For the SNL TTX method, the large number of dice thrown per turn made the probability of 'a kill' very high compared with the Oak Ridge and real time methods. The modified approach, with only one third the number of dice throws, made the SNL TTX method essentially consistent with the other two methods.

The example demonstrates how a comparative study may be used to validate TT exercise assumptions for specific applications (assuming in this case that the analytical model is the more realistic one), and how the validation results may be used in an iterative fashion to improve the applicability of the method.

Appendix X

SAFETY APPROACH FOR SECURITY ASSESSMENT

X.1. SAFETY AND SECURITY CONSIDERATIONS

It is not uncommon that **physical protection** and **nuclear safety** are managed much as separate issues with different, sometimes contradicting, objectives. One possible approach to integrate these two aspects is to recognize the physical protection as being an important part of the protection against nuclear accidents. By integrating physical protection within the well-established framework of nuclear safety, it is possible to resolve many of the difficulties associated with traditional management of security and safety.

X.2. ANALYSIS METHODOLOGY EXAMPLE

Reference [19] contains an example (see pp 105–113) of a DBT based analysis methodology that has been used to design and assess the performance of the protection against malicious acts using a nuclear safety perspective. The DBT has been interpreted and transformed into a set of specific scenarios, potentially challenging nuclear safety. The scenarios are considered to be precursors, which may result in initiating events (e.g. if an action triggers the need to shut down the reactor). Such an initiating event is not associated with a specific event class – these event classes are used in deterministic analysis to characterize the expected event frequency – since the DBT consists of postulated threats not actual ones. However, acceptance criteria are harmonized with the ones used for different event classes in the deterministic safety analysis. It is reasonable to require that less serious threats (e.g. non-violent demonstrations) may only lead to small consequences (e.g. similar to the ones accepted for the event class 'anticipated events'). More serious threats (e.g. terrorist attacks) could lead to larger but acceptable consequences (e.g. similar to the ones accepted for 'improbable events' or 'highly improbable events'). As the security analysis follows the format of deterministic safety analysis, all tools for design and assessment with respect to safety becomes applicable also for design and assessment with respect to security. By format, the two aspects have been merged into one single aspect.

To harmonize the documentation of the security and safety case, the final design of the physical protection was introduced as a new section in the safety analysis report. This documentation included a comprehensive description of the design and a summary of the results of the DBT based analysis. Based on the documentation of the physical protection in the safety analysis report, the technical specifications were also updated with sufficient requirements for safe operation. These requirements were readily acquired from the DBT analysis results using failure modes and effects analysis (see Appendix VII).

The referred example demonstrates a way to integrate safety and security in a systematic manner through performing design, implementation and finally giving support for management and operation.

Appendix XI

INSIDER THREAT ANALYSIS METHODOLOGIES

XI.1 INTRODUCTION

The NUSAM case studies have not discussed the use of assessment methodologies specific to the insider threat. There are several methods that have been used for insider threat analysis:

- The VISA method described in Ref. [1];
- A variant of the VISA method using insider adversary action sequences;
- PPS Efficiency Assessment Model for an internal threat discussed in Ref. [20].

Each method will be briefly described below after a general introduction to insider threat assessment methodologies.

XI.2. THE VISA METHOD

The VISA tabletop methodology is a qualitative based assessment modelling tool than can systematically evaluate system effectiveness of nuclear security through the use of SMEs. The methodology is a scenario based approach based on SME opinion, documented values or a combination of both. The methodology can use either qualitative or quantitative input to document the nuclear security effectiveness against the defined insider threats.

XI.3. A GENERAL APPROACH TO INSIDER THREAT ANALYSIS

The overall P_E for a PPS against an active insider scenario can be expressed using the following equation (see Eq. (27)):

$$P_E = 1 - (1 - P_{DS}) \times (1 - P_{EO}) \quad (27)$$

where P_{DS} represents probability of detection of the adversary during a protracted stage of the scenario and P_{EO} (probability of system effectiveness for an abrupt unauthorized removal) measures effectiveness of the PPS with timely detection (in some sense) of the adversary attack over a more limited time frame. P_{EO} would be estimated assuming any adversary protracted actions defined in the scenario had been successfully completed with no detection before the start of the abrupt phase. However, protracted adversary activities would incur the risk of being detected with probability P_{DS} resulting in a tradeoff between performing protracted actions that would increase P_{DS} but potentially decrease P_{EO}.

For a non-violent active insider, P_{EO} would be measured by P_I; if the active insider is violent, then P_{EO} would incorporate the effectiveness of both interruption and neutralization. By comparison, the formula for P_E assumes that the insider is both interrupted and neutralized if detection occurs during the protracted phase even if the adversary is armed and violent.

The protracted phase consists of one or more adversary actions such as those provided as examples below (any combination of these types of activities might be included in the scenario as deemed practical for the insider threat by the analyst):

- Introducing prohibited items covertly through access points into areas that they have normal access to;
- Gaining access to tools and equipment in areas that they have normal access to;
- Tampering with safety equipment in different vital areas they have normal access to;
- Removing NM in a number of steps out of a hardened room, inner area, and/or PA;
- Tampering with physical protection measures or systems so that they will not function effectively during the abrupt phase of an adversary attack;

— Tampering with physical protection measures or corrupting access control databases to allow them to covertly move from an area they have authorized access to into other areas that they do not have authorized access to.

Any one of these types of adversary actions might be performed multiple times spread over multiple insider visits to the facility. Note that the last type of protracted activity, if successfully completed without detection, might allow the adversary to possibly introduce prohibited items to or gain access to tools and equipment in areas beyond those that they have authorized access to.

The quantity P_{DS} will include one or more detection probabilities and combine them using the general formula (See Eq. (28)):

$$P(E_1\ OR\ E_2) = P(E_1) + P(E_2) - P(E_1\ AND\ E_2) = 1 - \big(1 - P(E_1)\big) \times \big(1 - P(E_2)\big) \qquad (28)$$

The insider might also have the option to perform protracted phase activities in different temporal sequences. For example, if adversary actions *A*, *B* and *C* need to be performed during a protracted phase, then the adversary might perform them in one or more of the following orders: *A, B, C* or *A, C, B* or *B, A, C* or *B, C, A* or *C, A, B* or *C, B, A.* This could be an important consideration in determining how to represent that scenario in an exercise or computer simulation of the attack as performance may vary according to the sequence selected.

A similar approach can be used as a basis for evaluating the effectiveness of the physical protection system against an active insider performing protracted phase attacks to prepare for an attack with a colluding outsider threat.

In principle, a separate, independent insider threat analysis could be performed for each person who potentially has access to the facility. This is usually impractical so that it is common to first categorize potential insider threats in terms of their (common) access, authority and knowledge and then to perform an analysis for one or more categories of potential insider threats.

This same formula can be used to include protracted adversary cyber-attacks on the access control and physical protection system, safety equipment and the nuclear material accounting and control system.

Some of the insider threat analysis methods have versions that use qualitative probabilities. Such methods then require rules for determining qualitative probabilities for AND'd (multiplied) events, such as detection occurs only if sensing and assessment occurs, and for OR'd (added) events, such as detection at protection layer 1 or layer 2. Table XI.1 indicates the results of AND and OR functions for 2 different approaches for determining AND'd and OR'd qualitative probabilities.

TABLE XI.1. QUALITATIVE PROBABILITY RESULTS FOR AND'D AND OR'D COMBINATIONS OF ADJECTIVAL SCORES/QUALITATIVE PROBABILITIES - TWO APPROACHES

		VISA Approach		SQ Approach	
P_1, Probability of Event E_1	P_2, Probability of Event E_2	Probability of E_1 AND E_2	Probability of E_1 OR E_2	Probability of E_1 AND E_2	Probability of E_1 OR E_2
VVL = Very Very Low	VVL	Not used	Not used	VVL	VVL
VVL	VL, L, M, H, VH*	Not used	Not used	VVL	VL, L, M, H, VH*
VL = Very Low	VL	VL	VL	VL	***L***
VL	L, M, H, VH*	VL	L, M, H, VH*	VL	L, M, H, VH*
L = Low	L	L	L	L	***M***
L	M, H, VH*	L	M, H, VH*	L	M, H, VH*
M = Moderate	M	M	M	***L***	***H***
M	H, VH*	M	H, VH*	M	H, VH*
H = High	H	H	H	***M***	***VH***
H	VH	H	VH	H	VH
VH = Very High	VH	VH	VH	VH	VH

* Indicates solution is stated in the same order as the combination: e.g. M AND H = H, M AND VH = VH.

The first approach, which is used as part of the VISA analysis methodology, is easily described:

- The adjectival rating for Event E_1 AND E_2 = Minimum of the rating for the Event E_1 and the rating for Event E_2.
- The adjectival rating for Event E_1 OR E_2 = Maximum of the rating for the Event E_1 and the rating for Event E_2.

The SQ approach, developed for this CRP, uses qualitative probabilities rather than adjectival scores. The OR and AND rules are similar to those for the VISA approach except for three important differences: 1) the SQ approach has an additional category, VVL, 2) where the combination H AND H has a different answer (M) and 3) the combinations VL OR VL, L OR L, M OR M and H OR H have different answers which are indicated in bold italics in the table above.

These qualitative probabilities can be equated by the analyst to ranges of quantitative probabilities. For example, moderate might equate to a probability between 0.39 and 0.61, with a 'central' value at 0.5. The rationale for using the SQ approach is tied to the fact that it may increase at least some OR'd probabilities and possibly decrease some AND'd probabilities, while the VISA method takes no credit for OR'd scores and reflects no decreases for AND'd scores.

To compare the two approaches with quantitative calculations, if 4 M adjectival scores are AND'd together, the VISA approach result is assigned an M score. If we assign the range of probabilities (0.41 to 0.6) to an M rating, the quantitative probability of all events ranges between 0.03 and 0.13, which is not very consistent with the assigned M VISA range (0.4 to 0.6). For the SQ approach, the 4 M's are combined two at a time to get 2 L's based on Table XI.1; these 2 L's are then AND'd together to get L. The SQ approach uses the SQC method found in Table H.2 to convert qualitative probabilities to quantitative ranges. Based on the SQC method, L equates to the range (0.22 to .038), which closer to the quantitative range (0.03 to 0.13) determined by treating each of the four probabilities as falling between the 0.39 to 0.61 range associated with an M rating. Thus, the VISA approach tends to overestimate ratings compared with the corresponding quantitative probability calculations. Note that the SQ approach is somewhat better but still only reduces the answers if the two qualitative probabilities are the same: for example, H AND M = M. Conversely, the SQ approach can also result in what appear to be low probabilities. For example, the SQ approach assigns a L qualitative probability, with the range (0.22 to 0.38), to the combination of 4 H's AND'd together. This result appears to be a significant reduction considering each H by itself would seem to be a relatively high probability.

On the other hand, the VISA approach tends to give less credit to OR'd scores than the corresponding quantitative probabilities would. For example, the VISA approach assigns 4 Ms OR'd together an M rating, while the probability of seeing the OR'd event ranges between 0.88 and 0.98 when an individual M rating is equivalent to the probability being between 0.88 and 0.97. For the SQ approach 4 M's AND'd together can be combined using Table XI.1 to 2 Hs AND'd together, which then results in a VH quantitative probability (with a range 0.86 to 1.00) which is fairly close to the quantitative probability range. Another example of this effect is demonstrated in the VISA tabletop results found in Table 3 (Ref. [1]): system effectiveness includes one VL step score or rating, one L, one M and 4 H step scores yet the P_E is only assigned a H.

The SQ approach tends to give more credit for OR'd probabilities and less than for AND'd probabilities than the VISA approach. Thus, the SQ approach will give higher qualitative answers when there are four or more facility layers with H qualitative answers, as is the case for the NPP Case Study VISA Example. On the other hand, the SQ approach will tend to give lower answers if there are 4 AND'd terms on a layer (as is also the case for the Nuclear Power Plant Case Study VISA example). Therefore, one might use the SQ approach if there are expected to be several highly effective security layers in the facility and it would be desirable to take credit for this defence in depth.

The VISA approach has the additional merit that it can handle correlated quantitative probabilities in a very easy and straightforward way. The quantitative probability of the Event E_1 AND E_2 is, at most, the smaller of the quantitative probabilities P_1 and P_2 independently of how the two events are correlated while the quantitative probability of the Event E_1 OR E_2 is at least the larger of the quantitative probabilities P_1 and P_2 whatever the correlation between events E_1 and E_2.

These are theoretical considerations. In practice, the difference between the answers provided by the VISA qualitative approach and quantitative calculations are typically not very great because VISA's

property of overestimating AND'd scores at a single step is often offset by its property of underestimating OR'd terms across multiple steps. The exception may be when scenarios are expected to includes 4 or more steps with M or H step scores. If this latter case is suspected, VISA may underestimate P_E compared to using SQ approach or quantitative probability calculations.

The VISA approach has the significant advantage of being used widely and successfully worldwide to evaluate nuclear security events while the SQ approach is only used in training courses.

XI.4. INSIDER ADVERSARY ACTION SEQUENCES

This approach is based on adversary action sequence diagrams that are similar in concept to adversary sequence diagrams except the elements on a layer may represent adversary actions as opposed to physical locations on a protection layer. An example of such an action might be: 'get combination to hardened room that the insider is not authorized to know' which could be accomplished in multiple ways across many physical locations. Figure XI.1 shows an adversary action sequence diagram for a violent insider attack in a reactor control room (the example is notional and does not apply to the nuclear power plant in Ref. [1].):

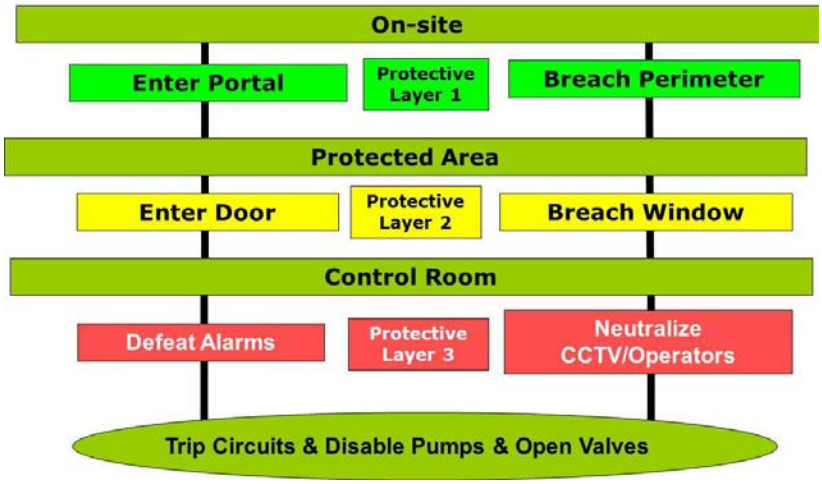


FIG. XI.1. Example of an adversary action sequence diagram

This approach is conducted in several phases:

(1) For a selected target and insider threat category, define a general sequence of actions for that target;

(2) Identify measures to protect against these actions;

(3) Estimate the effectiveness of each measure;

(4) Develop most vulnerable scenarios;

(5) Incorporate response and mitigation measures;

(6) Determine overall effectiveness.

Table XI.2 explains the process.

Phase 1: For a selected target and insider threat category, define a general sequence of actions for that target.

During this phase, the analyst determines what actions are to occur so that the adversary succeeds and to determine in what protection layers or areas those actions are completed and the options that the adversary has to perform those actions at each area or protection layer or area.

For this example, we will assume that the potential insider is a reactor operator and the target is a control room in a generic nuclear power plant. As a reactor operator, this person is allowed access into the control room.

There are five actions that makeup the adversary's scenario:

- Step 1: Enter and traverse the NPP PA;
- Step 2: Enter the Control Room;
- Step 3: In the Control Room, trip one or more pumps;
- Step 4: In the Control Room, disable other pumps;
- Step 5: In the Control Room, open a valve.

Note that the operator would need to perform actions 3–5 in order to hypothetically cause some sort of unacceptable damage to the plant. In this sense, the AAS is a generalization of an ASD since the latter considers elements or areas to be single steps.

The second phase is to identify administrative and technical measures to protect against these actions. Table XI.3 shows the results of these two phases: first, it lists the actions and where the action takes place in the first two columns. In the third column, it describes the adversary options for performing that action (e.g. the insider either goes through an entry portal or breach a perimeter in the PA boundary) and the physical protection and other measures associated with that option.

Note that these options can be displayed in an adversary action sequence diagram such as the one shown in Table XI.1.

TABLE XI.2. EXAMPLE VIOLENT INSIDER THREAT ANALYSIS

Step	Action	Measures along path	Defeat Strategies	P_S	P_A	P_D	Time Required
1	Enter and traverse the NPP PA	Enter portal: Entry control and general observation	Normal entry, no prohibited items	None	NA	None	30 seconds
			Normal entry, weapon in briefcase	High	Very High	High	30 seconds
			OR				
		Breach perimeter: Perimeter and general observation	Cut or climb fence	Moderate	Low	Low	1 minute (10 sec to cross fence and 50 sec to cross area)
2	Enter the control room	Enter poor: Key card access control and general observation	Normal entry	None	NA	None	20 seconds
			OR				
		Breach window: Window or door and general observation	Breach one of surfaces using tool acquired elsewhere on plant	Very High	Very High	Very High	90 seconds
3, 4, 5	Trip, disable pump, open valve	Neutralize closed circuit television (CCTV)/operators: Observations by operators and CAS	Wait until distracted	Low	High	Low	1 minute
			Disable CCTV and overpower operators	Very High	Low	Low	10 minutes
			AND				
		Defeat operational alarms	Disable alarms and displays or	High	High	High	45 minutes prior
			Act confused and claim he didn't do anything wrong, or	High	Very High	High	30 sec
			Overpower operators	Very High	Low	Low	10 minutes

TABLE XI.3. MEASURES ASSOCIATED WITH EACH ADVERSARY ACTION

Step	Action	Measures along path
1	Enter and traverse NPP PA	Enter portal: Entry control and general observation OR Breach perimeter fence: Perimeter and general observation
2	Enter the control room	Enter door: Key card access control and general observation OR Breach window: Window or door and general observation
3	Trip pumps in the control room	Neutralize CCTV/operators: Observations by operators and CAS AND Defeat operational alarms
4	Disable pumps in the control room	Neutralize CCTV/operators: Observations by operators and CAS AND Defeat operational alarms
5	Open valve in the control room	Neutralize CCTV/operators: Observations by operators and CAS AND Defeat operational alarms

The next phase is to estimate the effectiveness of each measure. To accomplish this, first the possible adversary defeat strategies for countering each measure needs to be identified and then various performance measures need to be estimated. As an example of this, consider the entry control and physical protection measures associated with the adversary attempting to enter the PA. The insider is allowed access into the PA so normal entry without prohibited items is one adversary defeat strategy while another might be to enter with a weapon in a briefcase.

There are three qualitative probabilities (P_S, P_A, and P_D) and one time required (essentially a delay time) needed for each strategy. The probabilities as assigned as VL, L, M, etc., while the time required will typically be assigned as minutes or seconds, although, protracted activities, such as 'covertly obtain combinations to vault locks' might take hours or days to complete. Note that we will assign P_D as P_S AND P_A using Table XI.1.

For the 'normal entry, no prohibited items' defeat strategy through the entry portal, the insider bypasses all countermeasures as they are allowed entry and are not bringing any prohibited items. In this case, P_S is assigned as none or zero. The P_A is not applicable (n.a.) because there is no sensing, therefore P_D = none. The time required is estimated as 30 seconds. For the 'normal entry, weapon in the briefcase' defeat strategy, it is assumed that the search procedures are effective against that type of weapon so that P_S = High; P_A might be set to be Very High based on the searcher knowing the item is a weapon and knowing that a reactor operator is not authorized to have such a weapon. The resulting P_D = High AND Very High = High. The time required for going through this process is also assumed to be 30 seconds.

Assigning P_A depends upon who assesses the alarm – security or operations – and whether they want to identify the insider and interrupt them as opposed to wanting to undo the damage caused by the insider. In the first case, the responders need to identify who did it and be able to respond properly either by intercepting the insider or moving to protect targets; in the second case, the operations responders need to identify what the damage is so that they can respond correctly to that damage.

Phase 4 consists of developing most vulnerable scenarios. To do so, for each step of the action sequence, and for each protection measure that would need to be defeated, select the defeat strategy with the most advantage to the adversary considering the adversary's capabilities, the probability of detection, the complexity of the action and the time required to defeat the protection measure(s). Select the measures based on logic, for example, (a) when parallel measures have differing levels of detection, select the lowest detection unless the times are significantly different and (b) when all the measures need to be encountered in the same step select the highest detection likelihood of all the measures.

In Table XI.3, the adversary's best scenario appears to consist of using the 'normal entry' adversary strategy for the first two steps. Since there is no detection at either of these steps, the times are not relevant. The adversary then uses 'disabling the CCTV to the central alarm station and overpowering the operators' as a common defeat strategy to accomplish Steps 3, 4 and 5 simultaneously. The rationale: the adversary would have to defeat the operational alarms so that they would need to overpower the operators. The associated P_D is low but would require 10 minutes to complete. Note that this last strategy would only be credible if the adversary is allowed to be active and violent. Depending upon the situation the adversary might also need to get a weapon or tool at the facility to overpower the operators, too.

The resulting scenario can be summarized as shown in Table XI.4.

TABLE XI.4. SCENARIO SUMMARY

Step	Action	Defeat Strategy	P_D	Time Required
1	Enter and traverse the NPP PA	Normal entry with no prohibited items through the entry personnel portal	None	30 sec.
2	Enter the control room	Normal entry	None	20 sec.
3	Trip pumps	Common Defeat Strategy: Disable CCTV and overcome operators	High	10 minutes
4	Disable pumps			
5	Open valve			

The fifth phase is to incorporate response and mitigation measures. These can be divided into two classes: 1) the security response to prevent successful sabotage and 2) the operations personnel and safety systems acting to either prevent successful sabotage or to mitigate consequences (the latter typically also involves emergency management).

Given the many uncertainties about responding to insider threats, RF times may be given as ranges, as shown as an example in Table XI.5 where the RF requires 20–150 seconds intervening to stop the insider perhaps because they are unarmed guards who use batons, etc.

TABLE XI.5. PPS RESPONSE TIME CALCULATIONS FOR A VIOLENT INSIDER THREAT SCENARIO

Response action	Minimum time taken (seconds)	Maximum time taken (seconds)
Identify malicious action	30	60
Communicate	10	30
Response prep time	10	60
Travel	15	310
Intervene	20	150
PPS response time (total)	85	610

Similar approaches would be used, perhaps based on drills or exercises, to determine an Operational Response Time. That process is not described here.

The sixth and final phase is to determine overall effectiveness. This involves several activities:

(1) Determine cumulative detection probability qualitatively from the start of the scenario;

(2) Determine cumulative time required from the end of the path;

(3) Use the minimum and maximum PPS response time to determine where in the action sequence that the adversary is be detected to allow the malicious action to be stopped (this is essentially a CDP);

(4) Determine the cumulative likelihood of detection before or at this CDP. This is the P_I. If neutralization is required, $P_E = P_I \times P_N$; otherwise $P_E = P_I$.

Table XI.6 shows the results of determining the cumulative P_D from the front of the scenario and cumulative time required from the end of the scenario.

TABLE XI.6. CUMULATIVE VALUES OF P_D AND TIME REQUIRED BY THE INSIDER THREAT

Step	Action	Defeat Strategy	P_D	Cumulative P_D	Time Required	Cumulative Time
1	Enter and traverse the NPP PA	Normal entry with no prohibited items through the personnel portal	None	None	30 sec.	650 sec.
2	Enter the control room	Normal entry	None	None	20 sec.	620 sec.
3	Trip pumps	Common Defeat Strategy: Disable CCTV and overcome operators	High	High	10 minutes	600 sec.
4	Disable pumps					
5	Open valve					

The cumulative time required sums the time required for all actions at that step and afterward. In this sense, this column shows time remaining assuming that detection occurs at the beginning of the delay. In practice, the analyst will verify that assumption for each step. As an example, at the minimum PPS response time of 100 seconds, the CDP is at simultaneous steps 3, 4, and 5 if detection occurs early enough during those actions that at least 100 seconds are left in order to respond. If this is the case then these steps are the CDP and P_I is the cumulative P_D up to and including these steps: High. If detection at steps 3, 4 and 5 occurs too late, so that less than 100 seconds is left in order to respond, the CDP is at Step 2 and P_I is essentially zero.

Qualitative P_I and P_N values are AND'd together to derive P_E: $P_E = P_I$ AND P_N. For this example, assume that neutralization is certain given interruption (that is, $P_N = 1$), resulting in P_E = High for a PPS response time of 100 seconds and 'none' for a PPS response time of 610 seconds. Given the wide range of qualitative P_E values – None to High – more information about the PPS response time is needed and/or security upgrades likely need to be made to this system.

Timelines for both the adversary and response times for physical protection or operations response organizations can be built based on the AAS (see Fig. XI.2). This figure shows response timelines for the security system, with an associated PRT, and for a system controlled by operations with an associated operations response time (ORT). Potentially, additional response organizations might participate and consequently have their own timelines represented.

The adversary timeline and (possibly multiple) response timeline(s) can be compared to determine something analogous to P_I, for the outsider threats. In this more general approach, sensing opportunities on the adversary timeline would be considered timely if they were timely against at least one of the response timelines. Note that P_{EO} would include a term analogous with P_N, to go with this more general P_I. In practice, any approach to characterize P_{EO} would probably be based on a simulation of some kind rather than attempt to determine P_I and P_N individually.

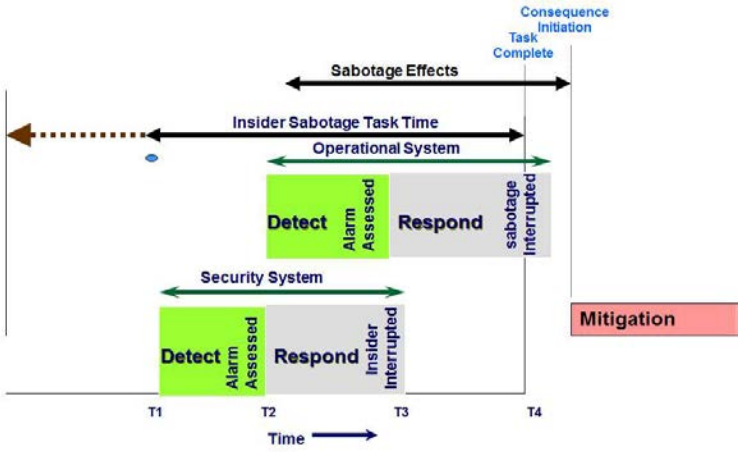


FIG. XI.2. Adversary, security response and operational response timelines

A different example scenario is provided to allow where the insider first tampers with an off-site power feed to the NPP and then would need to perform sabotage in two rooms to complete the malicious act. The evaluation assumes that the PRT being between 100 and 420 seconds (see Table XI.7).

TABLE XI.7. PPS RESPONSE TIME CALCULATIONS FOR A THREE TARGET VIOLENT INSIDER THREAT SCENARIO

Response Action	Minimum Time Taken (Seconds)	Maximum Time Taken (Seconds)
Identify malicious action	30	60
Communicate	10	30
Response prep time	10	60
Travel	30	120
Intervene	20	150
PPS Response Time (Total)	100	420

Table XI.8. shows how the effectiveness of this scenario is performed against this response.

TABLE XI.8. P_I EFFECTIVENESS CALCULATIONS FOR A THREE TARGET VIOLENT INSIDER THREAT SCENARIO

Step	Action	P_D	Cumulative P_D	Time Required (sec)	Cumulative Delay (sec)	Effectiveness (Min PRT = 100 sec)	Effectiveness (Max PRT = 420 sec)
1	Tamper with plant power feed	Very Low	Very Low	300	810		CDP: Very Low
2	Enter and traverse the PA	None	Very Low	300	510		
3	Enter Room #1	None	Very Low	30	210		–
4	Disable item A in Room #1	Moderate	Moderate	60	180	CDP: Moderate	–
5	Enter Room #2	None	Moderate	60	120		–
6	Disable item B in Room #2	Very High	Very High	60	60	–	–

In this example, depending upon where detection occurs within steps 2 and 5, the CDP could be at steps 1 or 2 when PPS response time = 420 seconds and at steps 4 or 5 when the PPS response time = 100 seconds. In either case, P_I = Moderate if the PPS response time = 100 seconds and Very Low if the PPS response time = 420 seconds. In summary, then P_I ranges between Very Low and Moderate depending upon the PPS response time. If $P_N = 1$, P_E also ranges between the P_I qualitative limits.

This evaluation raises a number of issues. For one, it is assumed that if the insider is detected while tampering with the power feed then the response would be sent to protect one or both of the other target rooms. Further, there is an assumption that if the insider is first detected at Room #1, then the response is able to effectively respond to Room #2 to prevent the rest of the attack. Finally, the insider is assumed to try to enter the PA immediately after they tamper with the plant power feed.

The effects of some alternate assumptions can be reflected in a new analysis shown in Table XI.9:

- Alternative assumption 1: The insider is interrupted in a particular room by the response getting to that specific room before the adversary disables the item.
- Alternative assumption 2: the insider could theoretically attempt to tamper with the power feed hours or days before proceeding further along the scenario. This would allow them to wait to see if anyone had noticed the damage to the power feed before they entered the facility and could abort the attack if the damage had been detected either by security or by operations.

TABLE XI.9. P_I EFFECTIVENESS CALCULATIONS FOR A THREE TARGET VIOLENT INSIDER THREAT SCENARIO UNDER ALTERNATIVE ASSUMPTION 1

Step	Action	P_D	Cumulative P_D	Time Required (sec)	Cumulative Delay (sec)	Effectiveness (Min PRT = 100 sec)	Effectiveness (Max PRT = 420 sec)
1	Tamper with plant power feed	Very Low	Very Low	300	600	CDP: Very Low	CDP: Very Low
2	Enter and traverse the PA	None	Very Low	300	300		
3	Enter Room #1	None	Very Low	30	90	–	–
4	Disable item A in Room #1	Moderate	Moderate	60	60	–	–
5	Enter Room #2	None	Very Low	60	120		–
6	Disable Item B in Room #2	Very High	Very High	60	60	–	–

If only alternative assumption 1 is true, there is a Very Low qualitative probability that the insider tampering with the power feed will be detected. The response would then identify the malicious action, communicate properly and prepare for responding to that event, all of which would take 50–150 seconds. The response would then proceed to an appropriate location to assess and begin to intervene to stop that action, which would be accomplished within 80–270 seconds after the alarm was generated. Depending upon where the sensing occurs within the first step, the response might arrive within that 300 second delay or they might not. If the response did not arrive while the insider was still performing step 1, more information would be required about response plans to see if interruption would occur (for simplicity we will assume that it does). On the other hand, if the insider was **not** detected at step 1, then the next opportunity to detect the insider would be at step 4. In this case, there would be a Moderate probability of detection but the insider would be gone by the time the response arrived at Room #1; subsequent detection would occur only during step 6 leaving at most 60 seconds for the response to now proceed to Room #2 and to intervene against the insider. Travel to that room (which is assumed to take 30–120 seconds) and intervention time (which takes 20–150 seconds) adds up to 50–270 seconds of new PRT. Sensing at step 6 is likely not timely for any PRT between 50 and 270 since the entire task delay is only 60 seconds.

Thus, with alternative assumption 1, P_I is Very Low for all PRT between 100 and 420 seconds because if the insider is not detected during step 1, then steps 2–6 can be completed before the response arrives at where the insider actually is carrying out the sabotage.

For alternative assumption 2, the adversary attack would be interrupted with a Very Low probability if their tampering during Step 1 was detected. If the insider was not detected during Step 1, retracing the logic associated with Tables XI.8 or XI.9 would result in additional timely detection ranging between None to Moderate, resulting in P_I ranging between Very Low to Moderate.

A final case to be discussed is the discontinuous insider threat attack in Fig. XI.3.

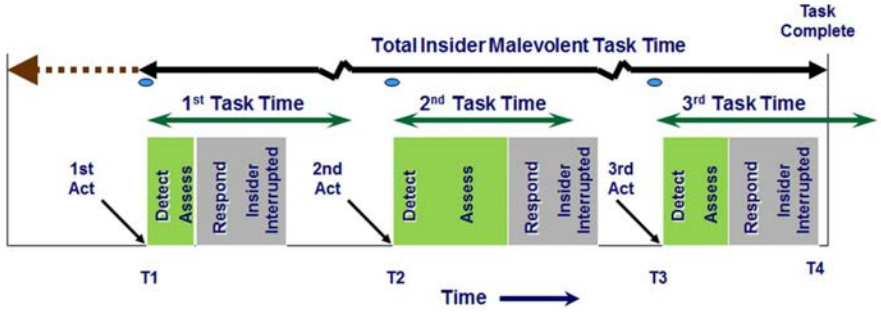


FIG. XI.3. Insider discontinuous attack sequence

In this type of attack, the insider may carry out a first task and if they get away, then waits to perform a second task, and so on. Figure XI.3 shows three planned insider tasks, with an indefinite time between tasks 1 and 2 and the time between tasks 2 and 3.

Figure XI.3 suggests that if the adversary is detected but not assessed during the first task, then the insider is free to wait to perform the second task. This is not very credible given the seriousness of sabotage or tampering of safety or security equipment or unauthorized removal of NM. It is more realistic to assume that the insider threat will be interrupted if detected during completion of all tasks except the last one. The last task would then be evaluated as if it were a single continuous attack, comparing detection before a CDP on that last timeline for the corresponding PPS response time.

There are three potential outcomes for all tasks during discontinuous attacks:

— Insider threat completes task *j* without security or operations knowing about it;

— The insider threat is assessed as attempting to complete task *j* maliciously and both security and operations respond;

— The sabotage or tampering is discovered but is not assumed to be malicious; operations fixes the effect of the sabotage/tampering (assumed to be ineffective for the last task).

Assuming that P_{Sj} is the probability that operations or security senses or discovers the effects of the sabotage/tampering and that P_{Aj} is the probability that the effects are assessed to be caused by a malicious act, the following probabilities can be assigned to the three outcomes:

— Insider threat completes task *j* without security or operations knowing about it: $1\text{-}P_{Sj}$;

— The insider threat is assessed as attempting to complete task *j* maliciously; both security and operations respond: $P_{Sj} \times P_{Aj}$;

— The sabotage or tampering is discovered but is not assumed to be malicious; operations fixes the effect of the sabotage/tampering: $P_{Sj} \times (1\text{-}P_{Aj})$.

The 3-task discontinuous attack in Fig. XI.3 can be analyzed using a Markov Chain, as shown in the Fig. XI.4.

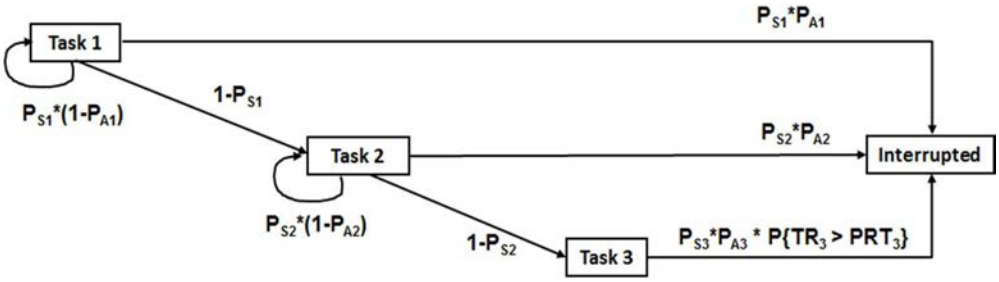


FIG. XI.4. Markov chain representation of example insider discontinuous attack sequence

To interpret Fig. XI.4, the insider starts with Task 1. If the insider completes that task without sensing $(1 - P_{S1})$, the insider can move on to Task 2. Alternatively, the insider might be detected as an insider with probability $P_{S1} \times P_{A1}$; in such a case the insider would be interrupted due to the long time on the rest of the path. The third outcome is that the insider's damage will be discovered but will be fixed without realizing that the effect was caused by an insider. Potentially, the insider could continue trying to complete their attack until they were either detected as insiders or have completed Task 1 without discovery.

Task 2 would be evaluated the same way, while for Task 3, the probability of detection, $P_{S3} \times P_{A3}$ would be multiplied by the probability that detection at Task 3 would be timely, that is, the time remaining (TR_3) would be greater than the PPS response time (PRT_3).

If the insider could continue to attempt Tasks 1 and 2 until they were detected as an insider or had completed the task without discovery, then P_I would be (See Eq. (29)):

$$P_I = \left\{\frac{P_{S1} \times P_{A1}}{1-P_{S1} \times (1-P_{A1})}\right\} + \left(\frac{1-P_{S1}}{1-P_{S1} \times (1-P_{A1})}\right) \times \left[\frac{P_{S2} \times P_{A2}}{1-P_{S2} \times (1-P_{A2})}\right] + \left(\frac{1-P_{S1}}{1-P_{S1} \times (1-P_{A1})}\right) \times \left[\frac{1-P_{S2}}{1-P_{S2} \times (1-P_{A2})}\right] \times P_{S3} \times P_{A3} \times P\{TR_3 > PRT_3\} \quad (29)$$

Conversely, if the insider could not try Tasks 1 or 2 again, given sensing/discovery of any kind, then the formula for P_I would be (See Eq. (30)):

$$P_I = P_{S1} + (1 - P_{S1}) \times P_{S2} + (1 - P_{S1}) \times (1 - P_{S2}) \times P_{S3} \times P_{A3} \times P\{TR_3 > PRT_3\} \quad (30)$$

XI.5. PPS EFFICIENCY ASSESSMENT MODEL FOR AN INSIDER THREAT

As mentioned earlier, this method is described on pg. 469 of Ref. [20]:

> "It is assumed that the insider, to defeat each PPS layer, may choose any of the following two options:
>
> Option 1 – the insider clears a (physical protection) PP layer by virtue of his/her capability using authorized access routes. In doing this, for a lower probability of the act suppression, the insider may attempt to throw prohibited items out of/into the PP area via channels not accessible to humans (piping, upper story windows, mesh holes and so on);
>
> Option 2 – the insider defeats a PP layer 'by force' using the same unauthorized intrusion channels as the external intruder. It is assumed that the attacker defeats the subsequent PP layers also 'by force.'"

The following discussion provides a summary overview of the equations that form the basis of this methodology.

Assuming that there are I categories of on-site personnel groups associated with a particular target; these categories could be defined in terms of access, authority and knowledge or other factors.

For insider threat category *i*, then the probability of interruption for this category is calculated using the following equation (See Eq. (31)):

$$P_I(i) = 1 - \left\{\prod_{l=1}^{L}(1 - P_{int\ il})\right\} \times (1 - P_{iL}) \quad (31)$$

where:

- L is the number of PP layers that the insider threat category *i* has access to;
- P_{iL} is the probability of interruption for insider threat category *i* using force/stealth beyond the *Lth* layer;
- $P_{int\ il}$ is the probability of detection for insider threat category *i* trying to smuggle prohibited items through layer *l*.

The probability of interruption P_{iL} is calculated using any of the outsider threat analysis methods described in this publication, presumably allowing the adversary to use force, stealth or deceit tactics.

The probability of detection for insider threat category i trying to smuggle prohibited items or materials through an access control point on layer i, $P_{\text{int } il}$ is calculated using the following expression (See Eq. (32)):

$$P^{*}_{int} = 1 - (1 - P_{search1} \times P_{search2}) \times (1 - P_{met1} \times P_{met2}) \times \left(1 - P_{exp1} \times P_{exp2}\right) \times (1 - P_{NM} \times P_{NM2}) \quad (32)$$

where:

- $P_{search1}$ = Probability of the insider being searched;
- $P_{search2}$ = Probability of prohibited items being detected by the search;
- P_{met1} = Probability of the insider being searched using a metal detector;
- P_{met2} = Probability of metallic items being detected with the aid of a metal detector;
- P_{exp1} = Probability of the insider being searched using an explosive detector;
- P_{exp2} = Probability of explosives being detected with the aid of an explosive detector;
- P_{NM1} = Probability of the insider being searched using a NM detector;
- P_{NM2} = Probability of NM being detected with the aid of a NM detector.

These formulas are used with the understanding that P_{search} = 0 if the prohibited material or item is not present.

Note: This model assumes that detection before or at Layer L is timely, presumably because the insider is detected while they are being searched.

While not discussed in Ref. [20], a similar model for cumulative probability of detection $P_I(i)$ could be based on the following equation (See Eq. (33)):

$$P_I(i) = 1 - \left\{\prod_{l=1}^{L}(1 - P_{int\ il})\right\} \times (1 - P_{DiL}) \quad (33)$$

where P_{DiL} is the cumulative probability of detection for insider threat category i using force/stealth beyond the Lth layer. This probability can be determined using any of the outsider threat analysis methods for calculating P_I that are described in this publication, with the assumption that the PPS response time is negligible.

Appendix XII

QUANTIFYING RISK

XII.1 INTRODUCTION

This appendix will discuss how risk can be semi-qualitatively quantified.

XII.2. RISK INFORMED DECISION MAKING

In an integrated approach as discussed in this section, risk can be defined in a semi-quantitative manner based on the method described in Ref. [21]. The purpose of this method is to be able to rank the risk associated with different 'safety issues' into 'Low', 'Medium' or 'High' risk, based on assessment of the frequency of 'issue related' initiating events, the vulnerability of the protection against these initiating events and of the resulting consequences of them.

- The frequencies of 'initiating events' are categorized into four classes: 'expected', 'possible', 'unlikely' and 'remote';
- The vulnerability with respect to each initiating event is categorized into three classes: 'robust' (protection effectiveness in compliance with regulations and good practices), 'adequate' (protection effectiveness is fair, but needs improvement) and 'inadequate' (non-effective protection);
- Consequences are categorized into three categories: 'tolerable' (consequences resulting from plant transients and on-site radiological exposures associated with accidents, typically 'expected' and 'possible' initiating events), 'significant' (consequences resulting from design basis accidents, 'unlikely' initiating events and off-site radiological exposures associated with such accidents) and 'intolerable' (consequences resulting from accidents beyond the design basis with off-site radiological exposures, 'remote' initiating events).

This risk measure is not a numeric function, but is defined by a matrix (see Table XII.1). Note that in this table there is one more additional category labelled 'drop'. It may be interpreted as 'negligible' risk.

TABLE XII.1. DECISION MATRIX FOR EVALUATION OF SAFETY ISSUES. Ref. [21]

Potential Consequences	Tolerable			Significant			Intolerable		
Safety Function Capability / Event Frequency	Robust	Adequate	Inadequate	Robust	Adequate	Inadequate	Robust	Adequate	Inadequate
Expected	Low	Low	Medium	Medium	High	High	High	High	High
Possible	Drop	Drop	Low	Low	Medium	High	Medium	Medium	High
Unlikely	Drop	Drop	Drop	Drop	Low	Low	Low	Low	Medium
Remote	Drop	Drop	Drop	Drop	Drop	Drop	Drop	Low	Low

* Risk classes are 'drop' = negligible risk, 'low' risk, 'medium' risk and 'high' risk

This risk concept may be used as a management tool to prioritize between measures to address safety issues. This is also useful when conflicts of interest between different aspects of safety need to be resolved. For this purpose, Ref. [21] defines generic recommendations (for NPPs) associated with the different classes of safety risk.

- **Low**: "Plant operation can continue without the need for interim corrective measures. Corrective measures may be implemented within a specified time schedule if shown to be reasonably practicable."

- **Medium**: "Some interim corrective measures are usually necessary in the short term. Plant operation may continue for some limited time, depending on the risk after implementation of the interim corrective measures. Cost effective permanent corrective measures should be implemented."
- **High**: "Immediate corrective measures are necessary to reduce the risk, and plant shutdown should be considered. If immediate corrective measures cannot reduce the risk, the plant may need to be shut down until interim or permanent corrective measures which will reduce the risk are implemented."

Considering that many sabotage events in a DBT or TA may involve some radiological consequences, it is possible to harmonize the definition of different levels of security related URCs with the categorization scheme in the safety case. There are two key decisions by the competent authority required to achieve this approximate harmonization:

1. Create an equivalence of URC levels with safety consequence levels, such as equating at/above HRC as "intolerable," at/above URC but less than HRC as" Significant" and less than URC as "tolerable." Note that this is a very simple way to setup the equivalence; more complex approaches may be used depending upon the preferences of the competent authority.

2. Assign an event frequency class for security related initiating events of malicious origin. For example, the competent authority could assign either an "Expected" frequency class or a "Possible" frequency class to all security related initiating events of malicious origin that are consistent with the DBT or TA.

As an example, assume the competent authority has decided to assign a "Possible" event frequency class to initiating events of malicious origins and to equate "intolerable" to at/above HRC, etc., as described under decision 1. In such a case, a facility would pose a HIGH security risk if their Security function capability was Inadequate but a MEDIUM risk if security capability was Robust or Adequate. Note that the risks for above URC (equated to Significant Potential Consequences) would be similar except when the Security capability was robust. Also, if the Security Event Frequency was equated to "Expected" all URC/HRC facilities would essentially have a HIGH security risk except for one case. If these results are not satisfactory, Table XII.1 itself could be modified, too, for security purposes. For example, the combination of "Possible" Security event frequency, "Significant" consequences, and "Adequate" security capability could be assigned a MEDIUM risk rather than HIGH as shown in Table XII.1.

Appendix XIII

DETERRENCE

XIII.1. INTRODUCTION

This section is based on research aimed at expanding the scope for performance based methods compared with currently accepted practices. Before the use of this approach as a basis for design and assessment of a facility's PPS, the applicability of this method needs to be carefully verified against the legal framework of the Member State for that facility.

The risk associated with each scenario may formally be represented by Eq. (34).

$$R = F \times (1 - P_{Det}) \times (1 - P_E) \times C \quad (34)$$

- R: Measure of risk
- F: Frequency of occurrence
- P_{Det}: Probability of deterrence
- P_E: Probability of system effectiveness
- C: Measure of consequence (in case of unsuccessful defence)

Earlier portions of Section 2 illustrate how to determine P_E. But in Eq. (34), the probability of deterrence is a measure of equal weighting, since increasing P_{Det} will reduce the risk in the same way as increasing P_E will. Therefore, to balance the earlier NUSAM discussion of risk, this section presents an outline on how P_{Det} may be measured under certain circumstances.

Deterrence is achieved when potential adversaries regard a facility as an unattractive target and decide not to attack it. From Eq. (30), it is tempting to draw the conclusion that an effective set of deterrence measures would automatically reduce the risk. This is not necessarily true since P_{Det} and P_E may in some cases be negatively correlated, such that, increasing P_{Det} may result in a reduction of P_E.

If a facility is to be perceived to be an unattractive target, it is necessary to convince the potential adversary of one or both of two facility impressions:

- The facility by itself is not a suitable target in relation to the adversary objective;
- The adversary perceives the facility protection measures are very difficult or too 'costly' to penetrate.

To convey these impressions to the adversary, it may be necessary to make some information concerning facility security measures public knowledge. This information may otherwise have been protected as sensitive (e.g. to make planning an attack more difficult). It is therefore important to select a balanced information protection strategy with respect to the measure of risk. To this end, when using a quantitative approach to measure P_E, it is helpful if one can also use a quantitative approach for measuring P_{Det}.

More generally, if both P_E and P_{Det} are included as part of the assessment, it is possible to compare proposed protection strategies with similar P_E values but different values for P_{Det}.

XIII.2. QUANTIFYING THE PROBABILITY OF DETERRENCE

XIII.2.1. Characterizing the adversary

Quantification of P_{Det} is performed based on what is known or assumed about the adversary's objective, motivation and capabilities. Of special importance is the adversary level of knowledge about the facility and its physical protection measures. This type of information regarding the adversary is preferably extracted from the applicable DBT or TA, but other sources of intelligence may also be used.

XIII.2.2. Selecting the theoretical approach

Taking a 'game theory' approach, where the players of the game may be called the '**attacker**' and the '**defender**', it is assumed that each player makes rational decisions and selects the course of action that maximizes the average '**utility**' – '**benefits**' minus '**costs**' – given the opponent's selected course of action. The aim for the defender is to introduce deterrence in order to convince the attacker that a '**non-attack**' is the optimal decision.

XIII.2.3. Building an analytical model

To demonstrate the modelling approach, the simplest case where the attacker has two options, to '**attack**' or a '**non-attack**', has been used. But having a set of multiple attack options will not change the modelling principles.

If the **attack** option is selected, the potential outcomes may be characterized in different ways. Here, it is assumed that there are two aspects to consider. Firstly, the attacker may be successful or unsuccessful in achieving the intended objective and secondly the attacker may suffer acceptable or unacceptable costs. Typically, '**unacceptable costs**' are defined in the DBT (e.g. for an economically motivated adversary, 'being killed' could be defined as an unacceptable **cost**). To determine the **average utility**, the specific utilities for all four outcome combinations need to be calculated: **'success** + **acceptable costs'**, **'success** + **unacceptable costs'**, **'non-success** + **acceptable costs'** and **'non-success** + **unacceptable costs'**.

- Benefits: In the utility calculations, the benefit of '**success**' may arbitrarily be set to 1, while the benefit of '**non-success**' may conservatively be assumed to be 0 (i.e. equivalent to the benefit of non-attack). The '**benefit**' of '**unacceptable costs**' is conservatively set to -1, assuming that the word '**unacceptable**' means that these costs outweigh the benefits of success.

- Probabilities: From the attacker's perspective, the probability of **success** is $(1\text{-}P_E^*)$, where P_E^* is the **perceived** P_E. The **perceived conditional probability** (P^*) of '**unacceptable costs**' (uc) given '**success**' (s) is denoted $P^*(uc \mid s)$, and the P* of '**unacceptable costs**' given '**non-success**' (ns) is denoted $P^*(uc \mid ns)$.

- Utilities: Under these assumptions, a conservative estimate of average utility (U) is given by Eq. (35).

$$U = (1 - P_E^*) \times [1 - P^*(uc|s)] - P_E^* \times P^*(uc|ns) \quad (35)$$

If it can be demonstrated for a specific scenario that the conservative estimate $U \leq 0$, this implies that the **rational adversary** will select the '**non-attack**' option (be deterred from attack). The problem of determining P_{Det}, is then reduced to determining the probability that the adversary perceives the situation according to model assumptions. This probability may sometimes be measured or estimated in another way. Below are a few examples:

- Measure the awareness probability of certain site specific information by using a survey or a written exam, directed at the facility employee population as a whole or a subset of employees that more closely represent the characterization of a potential insider threat adversary;
- Use human reliability analysis for determining the probability that an attacker would see and understand a warning sign along the assumed attack path, thus estimating the effect of 'in action' deterrence, where the adversary has an incentive to abort the attack;
- Apply DBT based assumptions regarding how well regulatory requirements are known and understood, thus ensuring consistent use of design basis information.

XIII.3. HYPOTHETICAL EXAMPLE

XIII.3.1. Scope

Based on the DBT, a specific insider adversary scenario has been developed. To reduce the risk associated with this scenario, deterrence measures are being considered. To justify the decision to implement these measures, P_{Det} needs to be estimated.

XIII.3.2. Adversary characterization

The adversary is a discontent nuclear power plant employee, who considers a malicious act of causing a reactor scram. The goal of the act would be to inflict damage to the company in the form of loss of power production capability, increased administrative costs and loss of the public trust.

The employee has authorized access to a postulated target area, where there are sensors or instrumentation that could be manipulated to cause a reactor scram.

A complete adversary success would be to cause a scram without being identified as the perpetrator. It would be considered an 'unacceptable cost' by the adversary if he or she was identified, arrested, and fined and/or imprisoned.

XIII.3.3. Analytical model

The adversary's intent is to install a homemade scram actuation device, which may either have a delayed actuation or be operated by a remote control. Having authorized access to the target area, the adversary is assumed to have identified an authorized activity that would allow the device to be installed with a very low (**perceived**) P_E^* for defeating the adversary malicious act.

Using expert judgement, it can be assumed as a 'low' (**perceived**) $P_E^* \approx 0.10$, the probability of the adversary being caught in the act (and thereby identified) during installation of the device. If this happens, the adversary is unsuccessful in the attempt to cause a reactor scram and will also suffer 'unacceptable consequences'. If the adversary is **not** caught, scram is assumed to be unavoidable, and there is no simple way to identify the perpetrator. Thus, in this case $P^*(uc/s) \approx 0$ and $P^*(uc/ns) = 1$. Now, the conservative U estimate may be calculated using Eq. (35).

$$U_{\text{Base Case}} = (1 - 0.10) \times (1 - 0) - 0.10 \times 1 = 0.80,$$

and the attack option is **not** ruled out.

To change the adversary perception regarding the utility of an attack, it is proposed that surveillance cameras are installed in the target area, and that their presence is advertised in an appropriate manner. One way of making it clear that any suspicious activities in that area will be monitored is to give a short course for relevant staff categories regarding 'code of conduct in the facility'. The course will contain general information on security, making it clear that all activities in critical areas are being monitored, and that the video recordings are stored for potential post event analysis. This disclosure would be somewhat sensitive, but does not reveal any information on which specific areas fall into the 'sensitive area' category. If the disclosure has the intended effect, it is judged that this trade-off will be an acceptable compromise.

By expert judgement, the proposed measures will significantly increase the adversary's perceived probability of being identified as the perpetrator in a post event analysis; this is interpreted as $P^*(uc/s) = 0.90$. However, the probability of being detected and identified during installation of the scram actuation device may only be perceived by the adversary as slightly higher than without the proposed measures; this is interpreted as $P_E^* \approx 0.25$. As before $P^*(uc/ns) = 1$. Now, the conservative U estimate may be calculated using Eq. (35).

$$U_{\text{Upgrade Case}} = (1 - 0.25) \times (1 - 0.90) - 0.25 \times 1 = -0.175 < 0,$$

and the attack option **is** ruled out, given that the adversary is aware of the deterrence measures.

XIII.3.4. Probability of deterrence

If the new equipment is installed, P_{Det} is now given by the probability that the adversary knows about them. This probability may be measured using a knowledge test. One possible test strategy is to require the test be taken first in conjunction with the code of conduct course and then again at random intervals in the future (failure to pass the test will result in having to attend a refreshment course). The average test result (for relevant questions in the test) based on the randomized examinations gives the final estimate of the P_{Det}. Experience suggests that an average score of ~75% (hypothetical assumption) is to be expected. This score may be sufficient justification for implementing the proposed deterrence measures.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Coordinated Research Project, J02004, Nuclear Power Plant Case Study for the Nuclear Security Assessment Methodologies for Regulated Facilities, IAEA, Vienna (2019)

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Coordinated Research Project, J02004, Medical Irradiator Facility Case Study for the Nuclear Security Assessment Methodologies for Regulated Facilities, IAEA, Vienna (2019)

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Coordinated Research Project, J02004, Transport of Radioactive Material Case Study for the Nuclear Security Assessment Methodologies for Regulated Facilities, IAEA, Vienna (2019)

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Rev. 5), Nuclear Security Series No. 27-G, IAEA, Vienna (2018).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Material in Transport, IAEA Nuclear Security Series No. 26-G, IAEA, Vienna (2015).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Security in the Transport of Radioactive Material, IAEA Nuclear Security Series No. 9, IAEA, Vienna (2008).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2012).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures Against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources, IAEA Nuclear Security Series No. 11, IAEA, Vienna (2009).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

[15] H. Kahn and A. Wiener, The Year 2000: A Framework for Speculation on the Next Thirty-Three Years, Macmillan, New York, (1967).

[16] M. L. Garcia, (2007) Design and Evaluation of Physical Protection Systems, 2nd Edition. Elsevier Science.

[17] Brief Adversary Threat Loss Estimator (BATLE) User's Guide, Dennis Engi and Charlene P. Harlan, Sandia National Laboratories, SAND80-0952/Nureg/CR-1432, May 1981.

[18] H. Donnelly, Fullwood, R., and Glancy, J. et al,. VISA – A Method for Evaluating the Performance of Integrated Safeguards Systems at Nuclear Facilities, NUREG-0317, Vol. 1 and 2, Science Applications, Inc., (1977)

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, International Conference on Topical Issues in Nuclear Installation Safety: Defence in Depth — Advances and Challenges for Nuclear Installation Safety, *Proceedings of an International Conference Held in Vienna, Austria, 21–24 October 2013* IAEA-TECDOC-CD-1749 Vienna (2014).

[20] A.V. Bushuev, V.B. Glebov, N.I. Geraskin, A.V. Izmaylov, E.F. Krychuckov, V.V. Kondakov, Fundamentals of Nuclear Materials Physical Protection, Control and Accountability, Department of Education and Science of the Russian Federation, National Research Nuclear University “MEPhI”, Moscow, (2011).

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of the Safety of Operating Nuclear Power Plants Built to Earlier Standards - A Common Basis for Judgement, Safety Reports Series No. 12, IAEA, Vienna (1998).

ABBREVIATIONS

3D	Three dimensional
AAS	Adversary action sequence
ASD	Adversary sequence diagram
BATLE	Brief adversary threat loss estimator
C	Measure of consequence
CCTV	Closed circuit television
CDP	Critical detection point
CRP	Coordinated research project
DBT	Design basis threat
DOR	Door
FoF	Force-on-force
GAT	Gate
H	High
HRC	High radiological consequence
IAEA	International Atomic Energy Agency
ISO	Isolation zone
KIA	Killed in action
L	Low
LPNPP	Lone Pine Nuclear Power Plant
LSPT	Limited scope performance testing
M	Moderate
MCR	Main control room
MVP	Most vulnerable path
NM	Nuclear material
NPP	Nuclear power plant
NSS	Nuclear Security Series
NUSAM	Nuclear security assessment methodologies
P_A	Probability of assessment
P_D	Probability of detection
P_{DET}	Probability of deterrence
P_E	Probability of system effectiveness
P_I	Probability of interruption
P_N	Probability of neutralization
P_S	Probability of sensing
PA	Protected area
PER	Personnel portal
P_H/P_K	Probability hit/probability kill
PPS	Physical protection system
PRT	PPS response time
RF	Response force
SA	Security assessment
SME	Subject matter expert
STAGE	Simulation toolkit and generation environment

SNL TTX	Sandia National Laboratories Tabletop Exercise
SUR	Surface element
TA	Threat assessment
TS	Threat statement
TT	Tabletop
URC	Unacceptable radiological consequences
VE	Virtual environment
VEH	Vehicle portal element
VH	Very high
VISA	Vulnerability to intrusion system analysis
VL	Very low
VVL	Very very low

LIST OF PARTICIPANTS

Alam, B	Bangladesh Atomic Energy Commission, Bangladesh
Brüecher, W.	GRS, Germany
Chetaine, A.	University of Mohammad V Rabat, Morocco
Contri, A	Rhino Corps, United States of America
Edwards, J.	National Nuclear Laboratory, United Kingdom of Great Britain and Northern Ireland
Garrett, A.	International Atomic Energy Agency
Greenhalgh, D.	Oak Ridge National Laboratory, United States of America
Hall, C.	Expert, United States of America
Hill, S.	Sandia National Laboratories, United States of America
Hogan, T.	Sandia National Laboratories, United States of America
Hwang, M.	Korea Atomic Energy Research Institute, Republic of Korea
Iwuala, E.	Nigerian Nuclear Regulatory Authority, Nigeria
Izmaylov, A.	State Co. Scientific Production Union “Eleron”, Russian Federation
Jang, S.	International Atomic Energy Agency
Jones, B.	Rhino Corps, United States of America
Jung, W.	Korea Atomic Energy Research Institute, Republic of Korea,
Kawata, N.	Japan Atomic Energy Agency, Japan
Kibria, F.	Bangladesh Atomic Energy Commission, Bangladesh
Knight, J.	ARES Security Corporation, United States of America
Leach, J.	Sandia National Laboratories, United States of America
Lee, J.	Korea Institute of Nuclear Nonproliferation and Control, Republic of Korea,
Legoux, P.	World Institute for Nuclear Security
Lindahl, P.	OKG AB, Sweden
Little, R.	Quintessa Ltd., United Kingdom
Mahmood, R.	Pakistan Nuclear Regulatory Agency, Pakistan
Malach, J.	EBIS, Czech Republic
Malachova, T.	EBIS, Czech Republic
Mahdi, A.	Iraqi National Monitoring Authority
Malik, S.	National Nuclear Laboratory, United Kingdom of Great Britain and Northern Ireland
Martin, K.	Oak Ridge National Laboratory, United States of America
Naoko, N.	Japan Atomic Energy Agency, Japan
Norichika, T.	Japan Atomic Energy Agency, Japan
Reynolds, J.	National Nuclear Laboratory, United Kingdom of Great Britain and Northern Ireland
Rivers, J.	Nuclear Regulatory Commission, United States of America
Rodger, R.	National Nuclear Laboratory, United Kingdom of Great Britain and Northern Ireland
Scott, J.	National Nuclear Laboratory, United Kingdom of Great Britain and Northern Ireland
Sergovantsev, P.	State Co. Scientific Production Union “Eleron”, Russian Federation
Shaheen, H.	Egyptian Nuclear and Radiological Regulatory Authority, Egypt
Shakoor, A.	Pakistan Nuclear Regulatory Agency, Pakistan
Shridhar, A.	Bhabha Atomic Research Centre, India
Shull, D.	International Atomic Energy Agency
Snell, M.	Sandia National Laboratories, United States of America
Stangebye, J.	SKB, Sweden
Stefanka, Z.	Hungarian Atomic Energy Authority, Hungary
Terao, N.	Japan Atomic Energy Agency, Japan
Vaclav, J.	UJD SR, Slovakia
Yamaguchi, T	Japan Atomic Energy Agency, Japan
Zahnle, P	ARES Security Corporation, United States of America
Zielman, B	URENCO Nederland B.V., Netherlands

Coordinated Research Project Meetings

Vienna, Austria: 6–8 March 2013, 3–4 February 2014, 17–21 March 2014, 2–3 September 2014, 13–17 October 2014, 16–20 March 2015, 13–17 April 2015, 10–14 August 2015, 27 June–1 July 2016

Preston, United Kingdom: 9–13 February 2015

Albuquerque, New Mexico, United States of America: 2–6 November 2015

Daejeon, Republic of Korea: 14–18 March 2016

IAEA
International Atomic Energy Agency

No. 25

ORDERING LOCALLY

In the following countries, IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

CANADA

Renouf Publishing Co. Ltd

22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Telephone: +1 613 745 2665 • Fax: +1 643 745 7660
Email: order@renoufbooks.com • Web site: www.renoufbooks.com

Bernan / Rowman & Littlefield

15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Tel: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com Web site: www.rowman.com/bernan

CZECH REPUBLIC

Suweco CZ, s.r.o.

Sestupná 153/11, 162 00 Prague 6, CZECH REPUBLIC
Telephone: +420 242 459 205 • Fax: +420 284 821 646
Email: nakup@suweco.cz • Web site: www.suweco.cz

FRANCE

Form-Edit

5 rue Janssen, PO Box 25, 75921 Paris CEDEX, FRANCE
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: formedit@formedit.fr • Web site: www.form-edit.com

GERMANY

Goethe Buchhandlung Teubig GmbH

Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, GERMANY
Telephone: +49 (0) 211 49 874 015 • Fax: +49 (0) 211 49 874 28
Email: kundenbetreuung.goethe@schweitzer-online.de • Web site: www.goethebuch.de

INDIA

Allied Publishers

1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA
Telephone: +91 22 4212 6930/31/69 • Fax: +91 22 2261 7928
Email: alliedpl@vsnl.com • Web site: www.alliedpublishers.com

Bookwell

3/79 Nirankari, Delhi 110009, INDIA
Telephone: +91 11 2760 1283/4536
Email: bkwell@nde.vsnl.net.in • Web site: www.bookwellindia.com

ITALY

Libreria Scientifica "AEIOU"

Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALY
Telephone: +39 02 48 95 45 52 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Web site: www.libreriaaeiou.eu

JAPAN

Maruzen-Yushodo Co., Ltd

10-10 Yotsuyasakamachi, Shinjuku-ku, Tokyo 160-0002, JAPAN
Telephone: +81 3 4335 9312 • Fax: +81 3 4335 9364
Email: bookimport@maruzen.co.jp • Web site: www.maruzen.co.jp

RUSSIAN FEDERATION

Scientific and Engineering Centre for Nuclear and Radiation Safety

107140, Moscow, Malaya Krasnoselskaya st. 2/8, bld. 5, RUSSIAN FEDERATION
Telephone: +7 499 264 00 03 • Fax: +7 499 264 28 59
Email: secnrs@secnrs.ru • Web site: www.secnrs.ru

UNITED STATES OF AMERICA

Bernan / Rowman & Littlefield

15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Tel: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

Renouf Publishing Co. Ltd

812 Proctor Avenue, Ogdensburg, NY 13669-2205, USA
Telephone: +1 888 551 7470 • Fax: +1 888 551 7471
Email: orders@renoufbooks.com • Web site: www.renoufbooks.com

Orders for both priced and unpriced publications may be addressed directly to:

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 2600 29302 or +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/books

19-00231

International Atomic Energy Agency
Vienna
ISBN 978–92–0–101719–2
ISSN 1011–4289