GIF/PRPPWG/2006/005

Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems

Revision 5

November 30, 2006

Prepared by:

The Proliferation Resistance and Physical Protection
Evaluation Methodology Expert Group
Of the Generation IV International Forum

Printed by the OECD Nuclear Energy Agency
for the Generation IV International Forum

DISCLAMER

This report was prepared by the Proliferation Resistance and Physical Protection Evaluation Methodology Expert Group of the Generation IV International Forum (GIF). Neither GIF nor any of its members, nor any GIF member’s national government agency or employee thereof, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by GIF or its members, or any agency of a GIF member’s national government. The views and opinions of authors expressed therein do not necessarily state or reflect those of GIF or its members, or any agency of a GIF member’s national government.

Proliferation Resistance and Physical Protection Evaluation Methodology Expert Group

Members

Robert Bari	Co-chair	Brookhaven National Laboratory, US
Richard Nishimura	Co-chair	Atomic Energy of Canada Limited, Canada
Per Peterson	Co-chair	University of California, Berkeley, US
Ike Therios	Technical Director	Argonne National Laboratory, US
Evelyne Bertel	Secretary	OECD Nuclear Energy Agency, France
Trond Bjornard		Idaho National Laboratory, US
Dennis Bley		Buttonwood Consulting, Inc., US
Roger Brunt		Office for Civil Nuclear Security, UK
Jean Cazalet		Commissariat a l'Energie Atomique, France
Jor-Shan Choi		Lawrence Livermore National Laboratory, US
Giacomo Cojazzi		EC DG Joint Research Centre-Ispra, Euratom
Philippe Delaune		Commissariat a l'Energie Atomique, France
Michael Ehinger		Oak Ridge National Laboratory, US
Michael Golay		Massachusetts Institute of Technology, US
Eckhard Haas		International Atomic Energy Agency, Austria
Joseph Pilat		Los Alamos National Laboratory, US
Eric Pujol		International Atomic Energy Agency, Austria
Gary Rochau		Sandia National Laboratories, US
Masao Senzaki		Japan Atomic Energy Agency, Japan
Neil Tuley		Department of Trade and Industry, UK
Myung Seung Yang		Korea Atomic Energy Research Institute, Republic of Korea
Michael Zentner		Pacific Northwest National Laboratory, US

Other Contributors

Burrus Carnahan	Observer	Department of State, US
Lap-Yan Cheng		Brookhaven National Laboratory, US
Hussein Khalil	Liaison	Generation IV National Director for Generation IV Design and Evaluation Methods, Argonne National Laboratory, US
John Murphy	Liaison	Project Manager, Nuclear Safeguards Office of International Regimes and Agreements (NA-243), National Nuclear Security Administration (NNSA), US
Guido Renda		EC DG Joint Research Centre-Ispra, Euratom
Filippo Sevini		EC DG Joint Research Centre-Ispra, Euratom
Rob Versluis	Liaison	Program Manager, Generation IV Nuclear Energy Systems Initiative, Department of Energy, Office of Nuclear Energy, Science and Technology (DOE-NE), US
Jeremy Whitlock		Atomic Energy of Canada Limited, Canada
Edward Wonder	Liaison	Project Manager, NA-243, NNSA, US
David York		Sandia National Laboratories, US
Meng Yue		Brookhaven National Laboratory, US

Former Group Members and Past Contributors

Michael Buckland-Smith		Office for Civil Nuclear Security, UK
David Beck		Sandia National Laboratories
Kory Budlong-Sylvester		Los Alamos National Laboratory, US
Scott DeMuth		Los Alamos National Laboratory, US
Ragnar Dworschak		Atomic Energy of Canada Limited, Canada
Jean-Claude Gauthier		Commissariat a l'Energie Atomique, France
James Hassberger		Lawrence Livermore National Laboratory, US
Glenn Hawkins		Department of Trade and Industry, UK
John Herczeg	Liaison	Former Technical Manager, Generation IV Design and Evaluation Methods, DOE-NE, US
Keiichiro Hori		JNC, Japan
Ed Jones		Lawrence Livermore National Laboratory, US
Daryl Kalenchuk		Atomic Energy of Canada Limited, Canada
Junichi Kurakami		JNC, Japan
Pierre Legoux		International Atomic Energy Agency, Austria
Tracia Love		Sandia National Laboratories, US
Steve Mladineo		Pacific Northwest National Laboratory, US
Michael Modro		Idaho National Engineering and Environmental Laboratory, US
Keun-Bae Oh		Korea Atomic Energy Research Institute, Republic of Korea
Ioannis Papazoglou		Brookhaven National Laboratory Consultant, US
Jon Phillips	Liaison	Former Program Director, NA-243, NNSA, US
Andre Poucet		EC DG Joint Research Centre-Ispra, Euratom
John Reynolds		Office for Civil Nuclear Security, UK
Jordi Roglans	Technical Director	Argonne National Laboratory, US
Thomas Shea		International Atomic Energy Agency, Austria
Steven Stein	Observer	Nuclear Regulatory Commission, US
David Tregunno		Atomic Energy of Canada Limited, Canada

(This page has been intentionally left blank.)

TABLE OF CONTENTS

List of Figures

List of Tables

(This page has been intentionally left blank.)

ABSTRACT

This report presents an evaluation methodology for proliferation resistance and physical protection (PR&PP) of Generation IV nuclear energy systems (NESs). For a proposed NES design, the methodology defines a set of challenges, analyzes system response to these challenges, and assesses outcomes. The challenges to the NES are the threats posed by potential actors (proliferant States or sub-national adversaries). The characteristics of Generation IV systems, both technical and institutional, are used to evaluate the response of the system and determine its resistance against proliferation threats and robustness against sabotage and terrorism threats. The outcomes of the system response are expressed in terms of six measures for PR and three measures for PP, which are the high-level PR&PP characteristics of the NES. The methodology is organized to allow evaluations to be performed at the earliest stages of system design and to become more detailed and more representative as design progresses. Uncertainty of results are recognized and incorporated into the evaluation at all stages. The results are intended for three types of users: system designers, program policy makers, and external stakeholders. Program policy makers will be more likely to be interested in the high-level measures that discriminate among choices, while system designers will be more interested in measures that directly relate to design options that will improve PR&PP performance of the NES.

(This page has been intentionally left blank.)

EXECUTIVE SUMMARY

The Technology Goals for Generation IV nuclear energy systems (NESs) highlight Proliferation Resistance and Physical Protection (PR&PP) as one of the four goal areas along with Sustainability, Safety and Reliability, and Economics:

> *Generation IV nuclear energy systems will increase the assurance that they are a very unattractive and the least desirable route for diversion or theft of weapons-usable materials, and provide increased physical protection against acts of terrorism.*

Proliferation resistance is that characteristic of an NES that impedes the diversion or undeclared production of nuclear material or misuse of technology by the Host State seeking to acquire nuclear weapons or other nuclear explosive devices.

Physical protection (robustness) is that characteristic of an NES that impedes the theft of materials suitable for nuclear explosives or radiation dispersal devices (RDDs) and the sabotage of facilities and transportation by sub-national entities and other non-Host State adversaries.

The Generation IV Roadmap recommended the development of an evaluation methodology to assess NESs with respect to PR&PP. Accordingly, the Generation IV International Forum formed an Expert Group in December 2002 to develop a methodology. This report presents the PR&PP methodology.

Figure ES.1 illustrates the methodological approach at its most basic. For a given system, analysts define a set of ***challenges***, analyze ***system response*** to these challenges, and assess ***outcomes***. The challenges to the NES are the threats posed by potential proliferant States and by sub-national adversaries. The technical and institutional characteristics of the Generation IV systems are used to evaluate the response of the system and determine its ***resistance*** to proliferation threats and ***robustness*** against sabotage and terrorism threats. The outcomes of the system response are expressed in terms of PR&PP ***measures*** and assessed.

The evaluation methodology assumes that an NES has been at least conceptualized or designed, including both the intrinsic and extrinsic protective features of the system. Intrinsic features include the physical and engineering aspects of the system; extrinsic features include institutional aspects such as safeguards and external barriers. A major thrust of the PR&PP evaluation is to elucidate the interactions between the intrinsic and the extrinsic features, study their interplay, and then guide the path toward an optimized design.

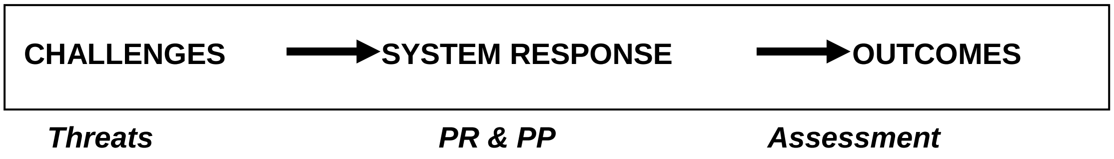

Figure ES.1: Basic Framework for the PR&PP Evaluation Methodology

The structure for the PR&PP evaluation can be applied to the entire fuel cycle or to portions of an NES. The methodology is organized as a *progressive* approach to allow evaluations to become more detailed and more representative as system design progresses. PR&PP evaluations should be performed at the earliest stages of design when flow diagrams are first developed in order to systematically integrate proliferation resistance and physical protection robustness into the designs of Generation IV NESs along with the other high-level technology goals of sustainability, safety and reliability, and economics. This approach provides early, useful feedback to designers, program policy makers, and external stakeholders from basic process selection (e.g., recycling process and type of fuel), to detailed layout of equipment and structures, to facility demonstration testing.

Figure ES.2 provides an expanded outline of the methodological approach. The first step is *threat definition*. For both PR and PP, the threat definition describes the challenges that the system may face and includes characteristics of both the actor and the actor's strategy. For PR, the actor is the Host State for the NES, and the threat definition includes both the proliferation objectives and the capabilities and strategy of the Host State. For PP threats, the actor is a sub-national group or other non-Host State adversary. The PP actors' characteristics are defined by their objective, which may be either theft or sabotage, and their capabilities and strategies.

To facilitate the comparison of different evaluations, a standard Reference Threat Set (RTS) can be defined, covering the anticipated range of actors, capabilities, and strategies for the time period being considered. Reference Threat Sets should evolve through the design and development process of nuclear fuel cycle facilities, ultimately becoming Design Basis Threats (DBTs) upon which regulatory action is based.

For PR, the threats include

- Concealed diversion of declared materials
- Concealed misuse of declared facilities
- Overt misuse of facilities or diversion of declared materials
- Clandestine dedicated facilities.

For PP the threats include

- Radiological sabotage
- Material theft
- Information theft.

The PR&PP methodology does not determine the probability that a given threat might or might not occur. Therefore, the selection of what potential threats to include is performed at the beginning of a PR&PP evaluation, preferably with input from a peer review group organized in coordination with the evaluation sponsors. The uncertainty in the system response to a given threat is then evaluated independently of the probability that the system would ever actually be challenged by the threat. In other words, PR&PP evaluations are contingent on the challenge occurring.

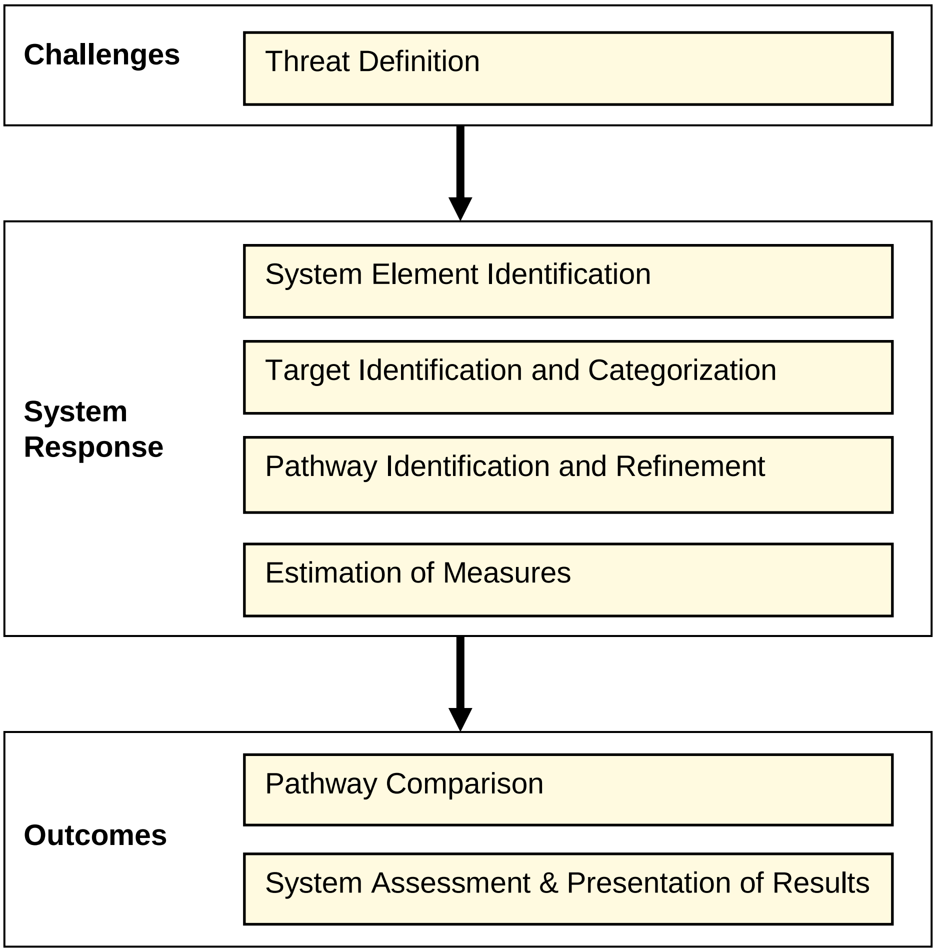

Figure ES.2: Detailed Framework for the PR&PP Evaluation Methodology

The detail with which threats can and should be defined depends on the level of detail of information available about the NES design. In the earliest stages of conceptual design, where detailed information is likely limited, relatively stylized but reasonable threats must be selected. Conversely, when design has progressed to the point of actual construction, detailed and specific characterization of potential threats becomes possible.

When threats have been sufficiently detailed for the particular evaluation, analysts assess system response, which has four components:

1. **System Element Identification**. The NES is decomposed into smaller elements or subsystems at a level amenable to further analysis. The elements can comprise a facility (in the systems engineering sense), part of a facility, a collection of facilities, or a transportation system within the identified NES where acquisition (diversion) or processing (PR) or theft/sabotage (PP) could take place.

2. **Target Identification and Categorization.** Target identification is conducted by systematically examining the NES for the role that materials, equipment, and processes in each element could play in each of the strategies identified in the

threat definition. PR targets are nuclear material, equipment, and processes to be protected from threats of diversion and misuse. PP targets are nuclear material, equipment, or information to be protected from threats of theft and sabotage. Targets are categorized to create representative or bounding sets for further analysis.

3. **Pathway Identification and Refinement.** Pathways are potential sequences of events and actions followed by the actor to achieve objectives. For each target, individual pathways are divided into segments through a systematic process, and analyzed at a high level. Segments are then connected into full pathways and analyzed in detail. Selection of appropriate pathways will depend on the scenarios themselves, the state of design information, the quality and applicability of available information, and the analyst's preferences.

4. **Estimation of Measures.** The results of the system response are expressed in terms of PR&PP measures. Measures are the high-level characteristics of a pathway that affect the likely decisions and actions of an actor and therefore are used to evaluate the actor's likely behavior and the outcomes. For each measure, the results for each pathway segment are aggregated as appropriate to compare pathways and assess the system so that significant pathways can be identified and highlighted for further assessment and decision making.

For PR, the measures are

- *Proliferation Technical Difficulty* – The inherent difficulty, arising from the need for technical sophistication and materials handling capabilities, required to overcome the multiple barriers to proliferation.
- *Proliferation Cost* – The economic and staffing investment required to overcome the multiple technical barriers to proliferation including the use of existing or new facilities.
- *Proliferation Time* – The minimum time required to overcome the multiple barriers to proliferation (i.e., the total time planned by the Host State for the project)
- *Fissile Material Type* – A categorization of material based on the degree to which its characteristics affect its utility for use in nuclear explosives.
- *Detection Probability* – The cumulative probability of detecting a proliferation segment or pathway.
- *Detection Resource Efficiency* – The efficiency in the use of staffing, equipment, and funding to apply international safeguards to the NES.

For PP, the measures are

- *Probability of Adversary Success* – The probability that an adversary will successfully complete the actions described by a pathway and generate a consequence.
- *Consequences* – The effects resulting from the successful completion of the adversary's action described by a pathway.

- *Physical Protection Resources* – the staffing, capabilities, and costs required to provide PP, such as background screening, detection, interruption, and neutralization, and the sensitivity of these resources to changes in the threat sophistication and capability.

By considering these measures, system designers can identify design options that will improve system PR&PP performance. For example, designers can reduce or eliminate active safety equipment that requires frequent operator intervention.

The final steps in PR&PP evaluations are to integrate the findings of the analysis and to interpret the results. Evaluation results should include best estimates for numerical and linguistic descriptors that characterize the results, distributions reflecting the uncertainty associated with those estimates, and appropriate displays to communicate uncertainties.

The information is intended for three types of users: system designers, program policy makers, and external stakeholders. Thus, the analysis of the system response must furnish results easily displayed with different levels of detail. Program policy makers and external stakeholders are more likely to be interested in the high-level measures, while system designers will be interested in measures and metrics that more directly relate to the optimization of the system design.

(This page has been intentionally left blank.)

1 INTRODUCTION

The Technology Goals for Generation IV nuclear energy systems (NESs) (DOE 2002a) highlight Proliferation Resistance and Physical Protection (PR&PP) as one of the four goal areas along with Sustainability, Safety and Reliability, and Economics. Giving this PR&PP goal such high visibility emphasizes the need for a sound evaluation methodology to guide future system evaluation and development. The PR component of the PR&PP goal focuses on providing strong assurance that Generation IV NESs are the least desirable sources for the diversion or undeclared production of nuclear materials. The PP portion of the goal ensures that Generation IV NESs will be robustly resistant to theft and sabotage.

The Evaluation Methodology Group developed a PR&PP methodology during the Generation IV Roadmap (DOE 2002b), but the approach was limited in its depth. Although incomplete information available about the systems contributed uncertainty to evaluations for all goals, the PR&PP evaluation was particularly restricted because of the lack of accepted metrics or figures of merit that could provide a comprehensive representation of the PR or the robustness of nuclear facilities against security threats. As a result, the criteria and metrics used in the final screening evaluations provided only a high-level representation of system performance in this goal area.

The Generation IV Roadmap resulted in a recommendation to develop an improved evaluation methodology to assess NESs with respect to PR&PP and that PR&PP evaluations should be performed during the earliest phases of design. This report presents the methodology developed by the PR&PP Expert Group, which was convened by the Generation IV International Forum in December 2002.

1.1 Overview of the Report

This report is intended for several audiences. The Executive Summary and Chapter 1 are intended for program policy makers, the broad membership of the Generation IV International Forum, and external stakeholders. Section 1.3, which reviews previous work, will also be relevant to technical experts and decision makers who wish to have a more specific understanding of the methodological approach presented in this report. Section 1.4 provides a high-level description of the methodological approach. Section 1.5 gives the reader a glimpse of the steps involved in a formal implementation of the methodology.

Chapter 2 is intended for the analysts who will perform evaluations, and describes the evaluation methodology in detail. The PR&PP evaluation process adopts specific guidelines for defining the threat space (Section 2.1), for performing evaluations of specific system elements and threat definitions (Section 2.2), and for comparing and presenting the results in a format that is of use to system designers and policy makers (Section 2.3).

The report also contains a list of references, as well as a glossary of terms and a list of acronyms as they are used in this document. In addition, a separate companion document serves as a technical addendum to this report. The addendum report, entitled “Addendum to the Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems”, contains several technical appendices which provide supporting details to the material in the present document. In the addendum report, Appendix A summarizes the metrics used in past PR assessments, and Appendix B reviews past assessments of PP robustness. Appendix C contains a more detailed discussion of defining the threat space. Appendix D has four parts:

- D1 is concerned with "Safeguardability Estimation." Safeguardability is defined as the ease with which a system can be effectively [and efficiently] put under international safeguards.
- D2 discusses how an analyst might design a hypothetical safeguards approach for a system and test the system against it.
- D3 summarizes the detection goals of the International Atomic Energy Agency (IAEA).
- D4 deals with aspects of fissile material quality and attractiveness.

Appendix E contains an overview of system analysis techniques applicable to PR&PP.

1.2 Context

The methodology documented in this report covers PR&PP of Generation IV NESs in a comprehensive manner. The PR&PP Expert Group has based its specification of the evaluation methodology scope on the definition of the Generation IV PR&PP Goal. The Generation IV Technology Roadmap (DOE 2002b) formally defined the following PR&PP goal for future NESs:

> *Generation IV nuclear energy systems will increase the assurance that they are a very unattractive and the least desirable route for diversion or theft of weapons-usable materials, and provide increased physical protection against acts of terrorism.*

Clear definitions of PR&PP are important to set the scope of the evaluation methodology. The definition of PR adopted by the Expert Group agrees with the definition established at the international workshop sponsored by the IAEA in Como, Italy, in 2002 (IAEA 2002b).

The following definitions have been adopted:

- ***Proliferation resistance*** is that characteristic of an NES that impedes the diversion or undeclared production of nuclear material and the misuse of technology by the Host State seeking to acquire nuclear weapons or other nuclear explosive devices.

- ***Physical protection (robustness)*** is that characteristic of an NES that impedes the theft of materials suitable for nuclear explosives or radiation dispersal devices (RDDs) and the sabotage of facilities and transportation by sub-national entities or other non-Host State adversaries.

The PR&PP Technology Goal for Generation IV NESs, when combined with the definitions of PR&PP, is therefore as follows:

> A Generation IV NES is to be the least desirable route to proliferation by hindering the diversion of nuclear material from the system and hindering the misuse of the NES and its technology in the production of nuclear weapons or other nuclear explosive devices.
>
> A Generation IV NES is to provide enhanced protection against theft of materials suitable for nuclear explosives or RDDs and enhanced protection against sabotage of facilities and transportation.

The PR&PP methodology provides the means to assess Generation IV NESs with respect to the following categories of PR and PP threats:

Proliferation Resistance – Resistance to a Host State's acquisition of nuclear weapons by:

- Concealed diversion of material from declared flows and inventories
- Overt diversion of material from declared flows and inventories.
- Concealed material production or processing in declared facilities
- Overt material production or processing in declared facilities.
- Concealed material production or processing by replication of declared equipment in clandestine facilities.

Physical Protection (robustness)

- Theft of nuclear weapons-usable material from facilities or transportation
- Theft of hazardous radioactive material from facilities or transportation for use in a dispersion weapon (RDD or "dirty bomb")
- Sabotage at a nuclear facility or during transportation with the objective to release radioactive material to harm the public, damage facilities, or disrupt operations.

1.3 Review of Previous Work and Concurrent Activities

Considerable work has been done to assess PR and PP robustness. The two subjects have traditionally been studied separately. Proliferation is commonly viewed as an international concern, and past work on a wide range of PR assessments is widely available. However, because PP is regarded as a State's security and sovereignty concern, much of the work is controlled or classified. Despite this, systematic analytical assessment similar to the evaluation framework discussed in this report is more mature for PP than for PR.

Since publication of the methodology developed by the Evaluation Methodology Group during the Generation IV Technology Roadmap (DOE 2002b), systematic work has improved evaluation methods. One example of such work is the study *Guidelines for the Performance of Nonproliferation Assessments,* issued by the U.S. Department of Energy (DOE) National Nuclear Security Administration (Denning et al. 2002, NPAM 2003), which provides the basis for the current PR&PP methodology. More detailed background information is included in Appendix A, which summarizes the metrics used in past assessments of PR, and Appendix B, which reviews past assessments of PP. The following sections summarize those studies.

1.3.1 Previous Work on Proliferation Resistance

Consideration of PR began in the 1970s with the International Nuclear Fuel Cycle Examination (INFCE) carried out by the IAEA and the Non-proliferation Alternative Systems Assessment Program (NASAP) carried out by DOE. Both NASAP and INFCE were more focused on identifying positive directions for fuel cycle development to minimize proliferation risks rather than on developing comprehensive means for evaluating that risk. The conclusion of these studies was that no technological arrangements would be immune to proliferation in the face of a State determined to obtain a weapons capability (INFCE 1980, NASAP 1980, Office of Technology Assessment 1977).

Studies of PR have covered a wide scope, including considering dedicated and civilian facilities and assessing individual facilities and entire fuel cycles. A comprehensive review of past work and examination of PR assessment can be found in documents by Krakowski (2001), NPAM (2003) and Cojazzi and Renda (2005).[1]

Past assessments of PR were based on either a decision or risk analysis approach. Work occurred in two main phases. Following INFCE and NASAP, a round of early assessment work was conducted from the late 1970s through the 1980s. The current focus on PR assessment follows a resurgence of interest in the mid-1990s during the U.S. National Academy of Science (NAS) plutonium disposition studies (NAS 1995).

In the most significant early analysis, Papazoglou et al. (1978) applied Multi-Attribute Utility (MAU) analysis to examine proliferation by Host States with different nuclear capabilities and objectives. Following on this work, Heising (1979), Silvennoinen and Vira (1981), and Ahmed and Husseiny (1982) also applied MAU approaches to rank alternative proliferation pathways. Krakowski (1999) performed a more recent application of MAU analysis, which attempts to include additional dynamic and geo-political considerations in the assessment. Ko et al. (2000) draws an analogy between PR and electrical resistance to suggest a novel heuristic for quantifying the PR of nuclear fuel cycles.

Another form of decision analysis based on the assessment of barriers to proliferation emerged in 1996 with the Proliferation Vulnerability Red Team (Hinton et al. 1996). A similar approach was taken by the Task Force on Technological Opportunities to Increase the Proliferation Resistance of Global Civilian Nuclear Power Systems (TOPS) of the U.S. DOE, Nuclear Energy Research Advisory Council (NERAC). The TOPS task force formulated a set of qualitative attributes (barriers) relevant to PR but made no attempt to perform quantitative or comparative assessment based on these attributes (Taylor et al. 2000).

---

[1] In 2003, in a draft review of methodologies for assessing nuclear proliferation resitance (UCRL-ID-153928-DR), E.D. Jones of Lawrence Livermore National Laboratory concluded that no consensus approach existed to assess PR. Rather, past assessments had many different analytical objectives, resulting in a focus on different factors that contribute to proliferation and application of different analytical methods.

Although early probabilistic assessments of nuclear material diversion were published in the late 1980s, systematic probabilistic evaluations of threats and vulnerabilities remained in the background until the latter half of the 1990s, and formal probabilistic risk analysis approaches were not proposed until the new millennium. Elaborating on Safeguards Logic Trees developed by Hill (1998), Cojazzi and Renda (2005) investigated the potential of the fault tree technique to identify all possible acquisition pathways in a given nuclear fuel cycle and their quantification in terms of non-detection probability (Cojazzi, Renda, and Contini 2004).[2] Appendix E gives an overview of systems analysis methods applicable to the PR domain.

Recently, the Blue Ribbon Panel of the Advanced Fuel Cycle Initiative examined the PR of a number of different alternative fuel cycles (PUREX/MOX, UREX, DUPIC, and Inert Matrix Fuel) involving current light-water reactors (Baron et al. 2004). The assessment relied on a MAU analysis methodology developed by Charlton. (An overview of the method is given in Appendix C of Baron et al. 2004.)

In parallel with these activities, complementary efforts have aimed to assess the effectiveness of international safeguards. The assessment of safeguard performance and detection probability is a subcomponent of a complete PR assessment. A number of review studies on safeguards performance assessment have been carried out, but most remain at the level of internal reports. A review study on safeguard assessment methodologies (Cojazzi and Renda 2004) was carried out recently at the European Commission Joint Research Center.

1.3.2 Previous Work on Physical Protection

Unlike PR, PP is not unique to the nuclear industry. Although the assets to be protected, consequences of a successful attack, and means to detect, delay, and respond to an attack may differ, the same basic principles are applied to protect a facility against sabotage or theft, whether it is an NES, petrochemical infrastructure, water treatment plant, financial center, or military site. Consequently, early development of methods for assessing PP predates the nuclear industry. Although probably not recognized as such in early times, scenario analysis has been used for centuries to plan defenses. With the advent of modern analytical techniques, the evaluation of PP has become structured and formalized.

The systematic analytical basis of PP is more mature than that of PR, relying on the principles of probabilistic risk assessment. In this treatment, the fault tree structure is commonly used to define threats, evaluate system response, identify system vulnerabilities, and rank risks. As with PR, much of the data involved are obtained subjectively. Thus, the resulting analyses are sometimes qualitative and reflect belief rather than objective analyses. However, they provide an integrated summary of the competing threats and risks and have led to the use of metrics to compare alternative facility designs and threat responses. The analysis has also provided a framework to specify, in a technology-neutral fashion, the performance requirements of the systems examined (Garcia 2001, IAEA 1999, IAEA 2002a).

---

[2] Rochau and colleagues at Sandia National Laboratories have described a probabilistic risk analysis approach based on threat, preventative barriers, assets, mitigating barriers, and consequences. The approach, called Risk-Informed Proliferation Analysis, identifies the pathways with the least PR.

Historically, assessments have considered a PP system consisting of a combination of intrinsic features and institutional framework designed to do the following:

- Minimize and control access to nuclear material, radioactive material, facilities, and transportation systems
- Minimize the vulnerability of plant systems to postulated attack
- Provide adequate response to postulated threats.

Current practice in the evaluation of the potential consequences of hypothetical threats to a facility is to postulate a Design Basis Threat (DBT), which is believed to provide a bounding characterization of the possible challenges to the facility. This DBT approach has been taken because it is difficult to define a realistic set of threats and obtain reliable estimates of their likelihoods. The DBT concept was developed in the 1970s in work by Sandia National Laboratories (SNL) for the U.S. DOE and U.S. Nuclear Regulatory Commission (NRC). SNL, in conjunction with representatives from Germany, the United Kingdom, France, and the IAEA, has conducted numerous workshops on the creation and use of the DBT since 1999. In October 2000, representatives from these States met under the coordination of the IAEA and created an international standard model for the development and use of a DBT (Blankenship 2002).

The established paradigm for threat assessment and management is based on the notions of deterring, detecting, delaying, and responding to the adversary. Further discussion of these concepts can be found in Appendix B of this report.

After September 11, 2001 broader attempts to apply systems analysis and Probabilistic Risk Assessment (PRA) techniques to security and counter terrorism have been increasingly proposed. (For example, see Garrick, et al. 2004).

1.3.3 Concurrent Related International Activities

The International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO) is an IAEA driven concurrent initiative. INPRO is developing a methodology for the *holistic* assessment of NESs. The INPRO assessment methodology (IAEA, 2004) is based on a hierarchical structure of Basic Principles, User Requirements, and Criteria consisting of Indicators and Acceptance Limits. Indicators are compared with corresponding acceptance limits, and judgment is made regarding the NES's capability to meet or exceed the criteria and user requirements. An INPRO assessment covers several different areas: Economics, Environment, Waste Management, Safety, Infrastructure, and Proliferation Resistance. Implementation manuals are under development in all these areas, including the new area of Physical Protection. Although the GIF PR&PP and INPRO evaluation methodologies differ in their implementation, GIF and INPRO share in their objectives to ensure that NESs of the 21st century are sustainable, safe and reliable, and economically viable while minimizing their risk of contributing to nuclear weapons proliferation and maximizing their robustness against theft and sabotage. The development of both approaches benefits from the exchange of information and the links provided by participants in both efforts.

1.4 Evaluation Methodology Approach

The basic evaluation approach developed by the Expert Group comprises **definition of a set of threats** or challenges, evaluation of the system's **response** to these challenges, and expression of **outcomes** in terms of measures.

A progressive approach permits broad application of the PR&PP evaluation to Generation IV NESs. NESs assessed for PR&PP can range from systems under development to fully designed and operating systems. The scope and complexity of the assessment should be appropriate to the level of detailed design information available and the level of detail with which the threats can be specified. In some cases, particularly for PP, the system analysis may involve the use or generation of *sensitive information* (see text box below). The main steps to be performed in each component of the approach are illustrated in Figure 1.1 and discussed in the following sections.

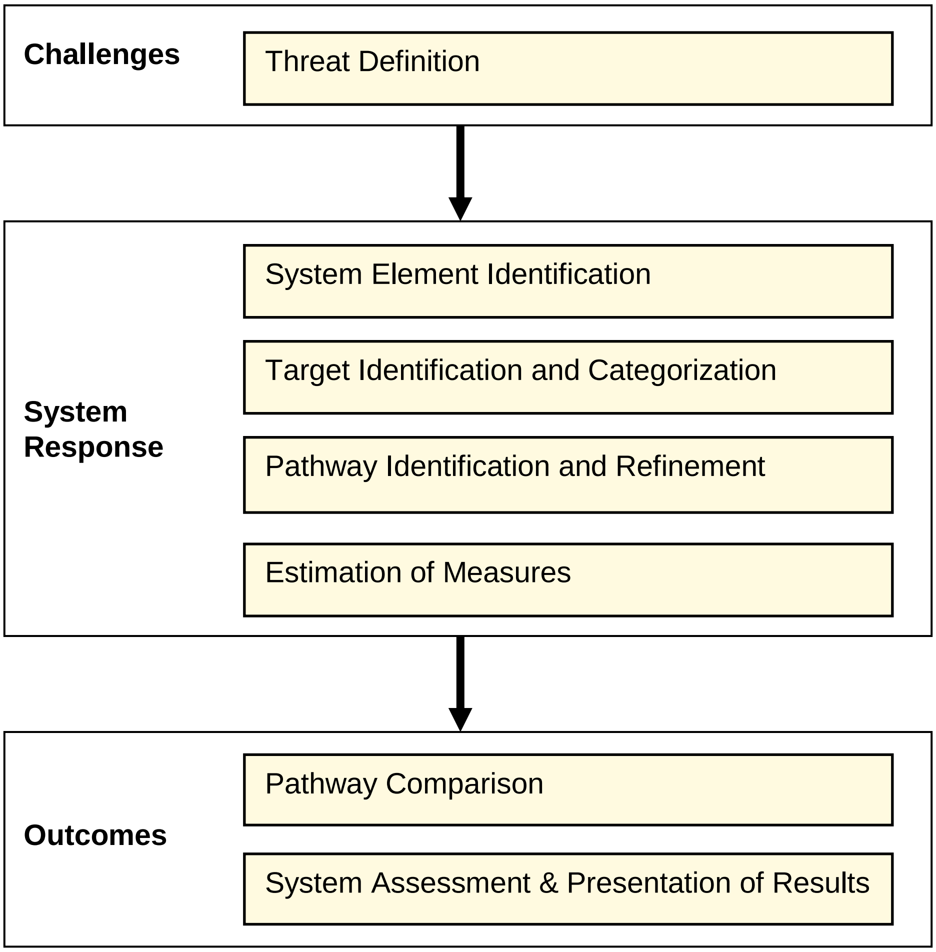

Figure 1.1: PR&PP Main Methodology Steps

Box 1.1 Sensitive Information

For PR&PP assessments of Generation IV NESs, some detailed pathway descriptions may include sensitive information. For example, the IAEA treats as “safeguards confidential” the concealment strategies it has assumed to design a safeguards system for specific facilities. Weapons laboratories treat as classified information on the specific approaches for fabricating nuclear explosives and the information about optimal approaches for processing nuclear materials using clandestine facilities. Likewise, national regulatory authorities treat as classified specific information about the sabotage and theft threats that current facilities are designed to defeat; methods, difficulty, and time required to overcome barriers to accessing facility vital areas; and complete equipment target sets that, if disabled, could result in radiological releases. For these reasons, PR&PP evaluations that use or create sensitive information must be performed by organizations that have the appropriate capabilities to control such information.

In many cases, the need to use and manage sensitive information can be reduced in PR&PP assessments, particularly at the coarse-path level, by the use of categories to characterize different PR and PP targets. Chapter 2 presents three tables for this purpose: a table of *area accessibility* categories that ranks types of areas by the relative difficulty of gaining access to equipment and materials, a table of *material attractiveness* categories that ranks types of materials by the relative difficulty of processing and fabricating nuclear explosives, and a table of *equipment fragility* categories that ranks types of equipment by the relative difficulty of disabling key functions.

Because ranked categories conceal detailed information, conclusions based on indexes are inherently approximate. In many cases these conclusions remain useful. When they do not prove useful, more specific studies must be performed with appropriate protection of sensitive information.

1.4.1 Definition of Challenges

The initial step in the PR&PP assessment is the definition of the challenges i.e. of the threats considered within the scope of the evaluation. To be comprehensive, a full suite of potential threats, referred to as the *Reference Threat Set* (RTS), must be recognized and evaluated. If a subset of the threat space is to be the focus of a specific case study, the subset must be explicitly defined. Threats evolve over time; therefore system designs must be based on reasonable assumptions about the spectrum of threats to which facilities and materials in the system could be subjected over their full lifecycles. The level of detail in threat definition must be appropriate to the level of information available regarding design and deployment.

The definition of a specific PR&PP threat requires information both about the actor and the actor's strategy. Here, actor is defined by the following factors:

- type (e.g., Host State, sub-national, etc.)
- capabilities
- objectives.

1.4.2 System Response

To evaluate the response of a Generation IV NES to proliferation, theft, and sabotage threats, analysts consider both technical and institutional characteristics of the NES. The system response is evaluated using a pathway analysis method. Pathways are defined as potential sequences of events followed by actors to achieve their objectives of proliferation, theft, or sabotage.

Before analyzing pathways, it is important to define the system under consideration and identify its main elements. After identification of the system elements, it is possible to identify and categorize potential targets for each of the threats and identify pathways for those targets. The steps used to evaluate the system response are illustrated in Figure 1.2 and discussed below.

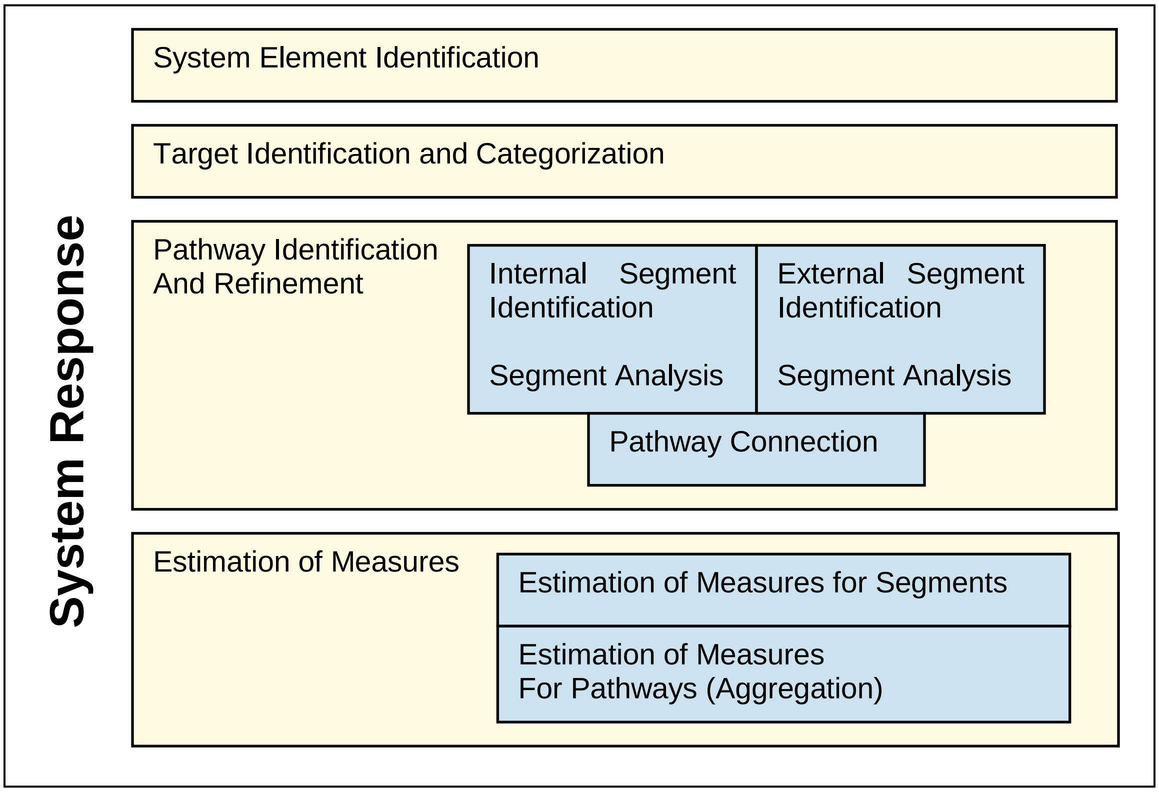

Figure 1.2: System Response Steps

System element identification – The boundaries of the system, which will limit the scope of the evaluation, must be clearly defined. Then the analyst must identify the system elements. The term *system element* is formally defined as a subsystem of the NES; at the analyst's discretion a system element can comprise a facility (not just a building, but a facility in the systems engineering sense), part of a facility, a collection of facilities, or transportation within the identified NES.

Target identification and categorization – Targets are the interface between the actors and the NES and are the basis for the definition of pathways. Clear, comprehensive target identification is an essential part of a PR or PP assessment. Targets can include nuclear or radiological material, as well as processes, equipment, and information.

Pathway identification and refinement – Pathways are built around targets and are composed of segments. For coarse pathway analysis, a *segment* consists of the *action* to be performed on the system. A complete PR pathway includes all of the actions for acquisition of material from the NES, processing of the material into a form directly usable in weapons, and fabrication of the weapon. Each of these three general segments may comprise multiple refined segments. A PP pathway would involve similar general segments for theft of fissile or radiological material. For sabotage, general segments would include access to the target equipment, damaging or disabling the equipment, and the subsequent system response potentially resulting in a radioactive release.

To generate a credible set of pathways, a systematic method comprehensible to subject matter experts must be used. The analysts must provide confidence that all credible pathways are identified. However, the analysts must also avoid or dismiss pathways, after proper justification and documentation, that are obviously not credible or that do not contribute to the overall evaluation of the NES.

Progressive refinement can proceed in two ways: Segments representing actions can be broken down into smaller actions, and characteristics can be added to segment descriptions to facilitate more accurate estimates of the measures.

Estimation of measures – The outcomes of the system's response are expressed in high-level measures for PR&PP, defined as follows:

> <u>*Proliferation Resistance*</u>
>
> *Proliferation Technical Difficulty* – The inherent difficulty arising from the need for technical sophistication, including material-handling capabilities, required to overcome the multiple barriers to proliferation
>
> *Proliferation Cost* – The economic and staffing investment required to overcome the multiple technical barriers to proliferation, including the use of existing or new facilities
>
> *Proliferation Time* – The minimum time required to overcome the multiple barriers to proliferation (i.e., the total time planned by the Host State for the project)
>
> *Fissile Material Type* – A categorization of material based on the degree to which its characteristics affect its utility for use in nuclear explosives

Detection Probability – The cumulative probability of detecting the action described by a segment or pathway

Detection Resource Efficiency – The staffing, equipment, and funding required to apply international safeguards to the NES.

These measures are similar to those adopted in most assessments of PR (see detailed discussion in Appendix A). Furthermore, they are also essentially the measures adopted by Papazoglou et al. (1978). Appendix D of that report provides a rather elaborate and exhaustive discussion of why these measures are complete and non-redundant.

Physical Protection

Probability of Adversary Success – The probability that an adversary will successfully complete a pathway and generate a consequence

Consequences – The effects resulting from the successful completion of the adversary's intended action described by a pathway, including the effects of mitigation measures.

Physical Protection Resources – The staffing, capabilities, and costs required to provide PP, such as background screening, detection, interruption, and neutralization, and the sensitivity of these resources to changes in the threat sophistication and capability.

Measures can be estimated with qualitative and quantitative approaches, which can include documented engineering judgment and formal expert elicitation (as has been successfully applied in a wide range of fields by Budnitz et al. 1998; Cojazzi et al. 2001; Forester et al. 2004; Pilat, Budlong-Sylvester and Stanbro 2002; Siu et al. 1998; and Wreathall et al. 2003). Measures can also be estimated using probabilistic methods (such as Markov chains and event trees) and two-sided simulation methods (such as war-gaming techniques, see NPAM 2003). Appendix E reviews a number of system analysis techniques relevant for PR&PP studies.

Metrics that can be used to estimate the measures are included in Chapter 2 of this report.

1.4.3 Outcomes

To determine the outcomes of the system's response to a threat, analysts compare pathways and assess the system to integrate findings and interpret results.

Pathway comparison – Analysts perform a pathway analysis by considering multiple pathway segments. In general, measures are estimated for the individual segments of a pathway and must then be aggregated to yield a net measure for the pathway. Although measures for different pathways may be aggregated, it is generally more valuable to use the measures to identify the most vulnerable pathways. The objective of the system evaluation is then the identification of the most vulnerable pathways and the measures associated with them.

System assessment & Presentation of Results – The final steps in PR&PP evaluations are to integrate the findings of the analysis and interpret the results in order to arrive at an assessment of the NES. Results include best estimates for descriptors that characterize the results, distributions reflecting the uncertainty associated with those estimates, and appropriate displays to communicate uncertainties.

1.5 Implementation of the Methodology

Evaluating PR&PP for a particular NES requires a mix of management, organizational, and technical skills that must be integrated to effectively develop a thorough, defensible, and understandable evaluation. The process is implemented under nine specific tasks that are organized under four main activities:

- M – Managing the process
- D – Defining the work
- P – Performing the work
- R – Reporting the work.

Each of the steps is primarily associated with one of these activities. The nine steps of the process are more thoroughly explained in Figure 1.3 and the accompanying text. Some level of management is associated with each of the steps; reporting cannot all be done at the end, but draft material must be generated as the work progresses; and the process is iterative and, sometimes, concurrent.

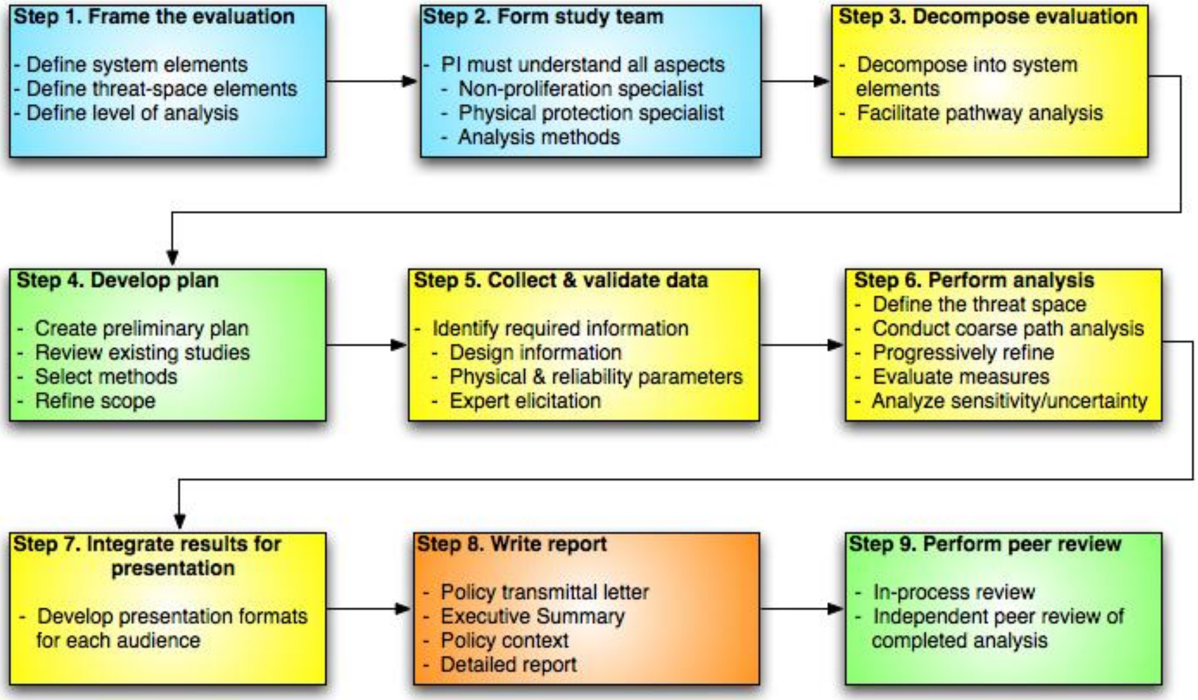

Figure 1.3: Steps in the PR&PP Evaluation Process

1.5.1 Managing the Process/Defining the Work

(Process steps 1, 2, 4, and 9 in Figure 1.3)

Structuring the problem systematically, assembling an expert analysis team, and ensuring competent peer review are important aspects to enhance completeness and adequacy of the results. The steps in the process are sketched in Figure 1.3 and described below. They will be detailed in the *Implementation Guide* for the methodology, a computer-based tool for the evaluation process with extensive examples and assistance. Note that the steps in the process are numbered in the order they are first performed but are grouped for discussion under the four main activities, as shown in Figure 1.3.

Step 1. Frame the evaluation clearly and concisely. – D[3]

The process of framing a PR&PP evaluation requires close interaction between the analysts and the evaluation sponsors to specify the scope, in particular to specify the system elements (facilities, processes, materials) and the range and definition of threats. The institutional context in which safeguards and other international controls would be implemented must also be specified in sufficient detail.

The process allows for analysis to be performed at many levels, depending on the needs of the sponsor. From pre-conceptual design to a fully operational facility, the PR&PP analysis can and must become more detailed. Timeframe can also dictate depth of analysis; quick and coarse evaluations may be needed when answers are required in weeks or months—and for some types of problems, potentially shorter time periods. Such shortcuts, however, entail a higher degree of uncertainty in the results.

Step 2. Form a study team that provides the required expertise. – M

The team should include experts in all required technical areas, including those areas from which expert judgment will be elicited, as well as expertise in carrying out the elicitation in an unbiased manner, with full expression of consensus uncertainty (Budnitz et al. 1998; Cojazzi et al (2001), Forester et al. 2004; Pilat, Budlong-Sylvester, and Stanbro 2002; Siu and Kelly 1998; Wreathall et al. 2003). The team should include the following expertise:

- Nonproliferation and/or safeguards, if the evaluation scope includes PR
- Physical protection, if the evaluation scope includes PP
- Analysis methods
- All relevant aspects of the NES design
- System design and operations.

---

[3] Each step in the PR&PP evaluation process is linked and color (shading)-coded to one of the four main activities:

- M – Managing the process (green)
- D – Defining the work (blue)
- P – Performing the work (yellow)
- R – Reporting the work (orange).

The principle investigator must understand all the technical areas at a level that permits integration and overall control. The PI must be able to speak for the analysis, explaining and defending the integrity of the work.

Step 4. Develop a plan describing the approach and desired results. – M

Before undertaking this major analysis effort, the evaluation plan should be thoroughly developed, reviewed, and documented. Additionally the staff resources, costs, schedule, and the form of the results and documentation must be clearly defined. Milestones should be developed particularly for regular reporting to sponsors. A detailed plan for the conduct and use of peer reviews is important to ensure quality. In developing the plan and in carrying out many of the information gathering and analysis tasks, coordination with safety evaluation, safeguards and physical security work for the NES could provide significant benefits.

Step 9. Commission peer reviews. – M

For any PR&PP evaluation that will be used to support decision-making or will receive wide exposure, a peer review should be performed to ensure the quality of the product. Two types of peer review have been widely used and provide different types of support to the project:

- In-process peer review/steering committee
- Independent peer review of the completed analysis.

In-process peer review brings an expert group of practitioners and decision-makers into the process at regular intervals – perhaps once per quarter – to be fully briefed on the status of the work and any known problem areas. Independent peer review allows objectivity through the review of the finished product by independent outside experts who have not been involved in the evaluation.

1.5.2 Performing the Work

(Process steps 3, 5, 6, and 7)

There are four steps involved in the main activity, performing the work. Steps 3 and 4 prepare for the required analyses, while the bulk of the analysis occurs under Step 6.

Step 3. Decompose the problem into manageable elements. – M

This step decomposes the NES into a tractable number of system elements and PR&PP threats to permit pathways analysis. Expert judgment may be used to identify system elements and threats that will be covered under qualitative, coarse pathway analysis and those that will then be subjected to progressive refinement with quantitative analysis.

Step 5. Collect and validate input data. – P

The quantities and sources of input data depend on the scope of analysis. Validation of input data implies either the independent review of the data sources or examination of the consistency and bases for expert elicitation. To the extent that information and input data used in the analysis come from classified or sensitive sources, the analyst must ensure that this information is protected appropriately, including the possibility of classification of the evaluation results. Most important is a strong interface with designers. Designers should be key members of the PR&PP evaluation team. Later, when the evaluation is applied to operating facilities, members of the operations team should be included.

Step 6. Perform analysis. – P

The actual analysis of PR&PP risks and capabilities is a multi-stage process. It addresses the **system response** and **outcomes** parts of the PR&PP methodological approach. System response is modeled using a pathways approach, which identifies the specific tasks required for the PR&PP evaluation. At a high level, these tasks are identical for structuring both the PR evaluation and the PP evaluation. At the detailed level, specific analyses differ. These differences are documented in Chapter 2. The outcomes are provided in terms of the estimation of a set of well-defined measures, also illustrated in Chapter 2.

Step 7. Integrate results for presentation. – P

Until several example analyses have been performed, the aggregation of results must be done carefully. In this process, the analysts should reference and consider previous studies, and apply the best available analysis tools to aggregate results and prepare the output in an optimal form for presentation to designers, program policy makers, and external stakeholders.

1.5.3 Reporting the Work

(Process step 8)

Step 8. Write the report. – R

The analysts must provide the results in a form that can be understood by the user and enable the user to draw appropriate conclusions. If the report contains classified or sensitive information, it may be necessary to abstract an unclassified summary. Section 2.3 describes ways in which the form of the results can be adapted to best communicate with specific audiences.

(This page has been intentionally left blank.)

2 EVALUATION METHODOLOGY

The major elements of the PR&PP methodology are discussed below in more detail. As summarized in Chapter 1, these elements comprise definition of challenges, system response, and outcomes and presentation of results.

2.1 Challenges

To evaluate PR and PP, analysts must first determine against whom and against what actions the NES is being protected. The results of the assessment can only be properly understood in this context. Thus, it is important to agree with evaluation sponsors at the outset of the assessment on what the *threats* are within the scope of the evaluation. To be comprehensive, a full suite of potential threats, referred to as the *Reference Threat Set* (RTS), must be recognized and evaluated. Rigor in threat definition avoids the potential problem of ascribing results of an assessment to a threat that was never considered in the analysis. Reference Threat Sets should evolve through the design and development process of nuclear fuel cycle facilities, which ultimately may be considered in formulating Design Basis Threats (DBTs) on which regulatory action is based.

The definition of a specific PR&PP threat requires information about the *actor*, the actor's *strategy*, and the actor's *objectives*. Table 2.1 summarizes the major dimensions of the RTS developed for use in the PR&PP evaluation methodology. Each of the elements in Table 2.1 is described in more detail below and in Appendix C, which also presents a method to assess and incorporate future PR and PP threats into facility design considerations.

2.1.1 Host-State Threat Definition (PR)

Traditionally, proliferation has been defined as any acquisition of a nuclear explosive device by a Host State. The following sections describe the actors, capabilities, objectives, and strategies associated with this threat space. Acquisition by a sub-national actor is countered by the physical protection system (PPS) and is addressed in Section 2.1.2. The threat of a proliferant State stealing material from a Host State is a special case, but because this threat would also be countered by the Host State's PPS, it is also discussed in Section 2.1.2.

2.1.1.1 PR Actors, Capabilities, and Objectives

The motives of Host States to acquire nuclear weapons will influence the PR threat definition by determining urgency, types and quantity of weapons sought, resources committed, and risks deemed acceptable (all of which may change over time). Regardless of the Host State's ultimate ambitions, the acquisition of the first weapon constitutes a fundamental threshold, and thus the acquisition of the first weapon is normally treated as a key endpoint of the analysis.

For PR, the type of **actor** is a non-nuclear weapons State assumed to have physical control over the facility and materials being evaluated and to be subject to international safeguards, i.e., the "Non-Proliferation Treaty" (NPT), INFCIRC/140, IAEA 1970; the "Acceptance of Safeguards Agreement" for Non-Nuclear Weapons States (NNWS) within the NPT, INFCIRC/153 (Corrected), IAEA, 1972; and the "Additional Protocol" to the NPT, INFCIRC/540 (Corrected), IAEA, 1998.

Table 2.1: Summary of the PR&PP Threat Dimensions

	Proliferation Resistance	**Physical Protection**
Actor Type	• Host State	• Outsider • Outsider with insider • Insider alone • Above and non-Host State
Actor Capabilities	• Technical skills • Resources (money and workforce) • Uranium and Thorium resources • Industrial capabilities • Nuclear capabilities	• Knowledge • Skills • Weapons and tools • Number of actors • Dedication
Objectives (relevant to the nuclear fuel cycle)	Nuclear weapon(s): • Number • Reliability • Ability to stockpile • Deliverability • Production rate	• Disruption of operations • Radiological release • Nuclear explosives • Radiation Dispersal Device • Information theft
Strategies	• Concealed diversion • Overt diversion • Concealed facility misuse • Overt facility misuse • Independent clandestine facility use	• Various modes of attack • Various tactics

The overall proliferation **capability** of a Host State is shaped by its capabilities in several key areas: general technical skills/knowledge, general resources (workforce and capital), uranium and thorium resources (particularly if indigenous), general industrial capabilities, and specific nuclear capabilities (for example, nuclear physics and engineering knowledge and nuclear facilities, particularly for enrichment and reprocessing). Typical values for state capabilities can be found in a variety of public sources including [IAEA, 2003].[4]

---

[4] Host State capabilities considered before the deployment of an NES may change considerably with the deployment of an NES. For example, introduction of a reprocessing facility into a State which previously had no reprocessing capability could potentially create significant new proliferation pathways which the analyst may consider important to take into account. On the other hand, there could be cases in which these capabilities would not be substantially modified. For this reason it is necessary to clearly specify the assumptions of any PR study, i.e., if the assumed capabilities are those possessed by the State before a possible deployment of a new NES or whether they will be estimated on the basis of a deployed new NES. This allows the analyst to consider how such deployment may affect a Host State's capabilities and whether to consider capabilities before or after deployment.

The ultimate **objectives** of the Host State for its nuclear weapons arsenal (size, reliability, ability to stockpile, deliverability, and production/deployment rate) will affect how a proliferant Host State may choose to misuse the civilian nuclear fuel cycle. For example, in terms of technical requirements, several attributes affect the utility of nuclear materials for use in explosives, including bare-sphere critical mass, heat generation rate, spontaneous neutron generation rate, and gamma radiation emission.

2.1.1.2 PR Strategies

A proliferant Host State may follow different strategies, depending on its particular circumstances, including the following:

- *Concealed diversion from declared flows and inventories.* This strategy may involve the direct extraction of materials from the facility in their typical composition or diversion of declared materials after they have been altered in order to either avoid detection or produce more attractive fissile material.
- *Concealed facility misuse, undeclared material production, or processing in declared facilities.* This strategy attempts to hide weapons material processing or production in a nuclear power program. An example is the undeclared irradiation of uranium targets in a power reactor.
- *Overt diversion of declared material and/or facility misuse for undeclared production.* In this case, the Host State does not care about detection and seeks to use the material and facilities available to it in its weapons program without attempting to conceal its activities.
- *Production using dedicated clandestine facilities alone.* Rather than directly using either the material or services provided by a declared fuel cycle, the Host State decides to produce weapons-usable material by building clandestine dedicated facilities (possibly replicas of declared facilities).

2.1.2 Non-Host State Threat Definition (PP)

The importance of specific PP threat dimensions depends on facility characteristics and the level of design detail available. However, each threat dimension specified in the sections below should be reviewed as a part of the evaluation process. As presented in Table 2.1, the definition of a PP threat has two components: a description of the actor (which includes type, objectives, and capabilities); and a description of the actor's strategy. The threat space is defined by considering an appropriate range of combinations of actors and strategies.

2.1.2.1 PP Actors, Capabilities, and Objectives

Three types of **actors** must be considered to define the PP threat space:

- Outsiders
- Outsiders in collusion with insiders
- Insiders alone.

Outsiders can include armed terrorist groups, agents of proliferant States, advocacy group, organized criminal gangs, and lone individuals. Insiders can be sympathetic with outsiders but may also include disaffected, anti-social, mentally unstable, or suborned employees or contract staff.

The PP assessment should consider a mixture of non-Host State and sub-national threats. This mixture can lead to complicated analyses but is necessary to consider the synergism between categories. The level of detail to which the actor is defined should be appropriate to the assessment goals. For system assessments where operations would start decades in the future, the definition of the actor types will be qualitative and stylized. Where operations would occur in the present or near future, the actor definitions will likely be specific and detailed.

Five categories of actor **capabilities** must be considered to define the PP threat space:

- Knowledge (including outsider access to insider knowledge)
- Skills
- Weapons and tools (commercial, military, or improvised)
- Number of actors
- Commitment and dedication (risk tolerance up to self-sacrifice).

Five categories of actor **objectives** must be considered to define the PP threat space:

- Sabotage intended to disrupt normal operations
- Sabotage intended to cause radiological release
- Theft for production of nuclear explosives
- Theft for production of RDDs
- Theft of technical information.

2.1.2.2 PP Strategies

The strategies of the PP actor can be defined as a set of tactics and modes of attack. Five potential **modes of attack**, employed singly or in combination, should be considered when defining the strategy for a given threat:

- *Ground-based* (may entail a mix of overt and covert activities and/or the help of an insider)
- *Waterborne* (many NESs are situated by a large body of water)
- *Standoff* (direct or diversionary attack using light anti-tank weapons or rocket-propelled grenades)
- *Aircraft* (as weapon itself or as transport for explosives or personnel)
- *Cyber* (hacking of alarm, sensor, or assessment software or direct attack of reactor safety software).

In addition, three categories of **tactics**, employed singly or in combination, may be considered when defining the strategy for a given threat:

- Stealth (avoiding or inactivating components of a PPS)
- Deceit (using false identification or authorization)
- Overt force (from advocacy group trying to gain access to fully armed assault).

2.2 System Response

The first step in evaluating system response is to identify system elements to be studied, as described below. In addition, analysts must identify and categorize targets, identify and refine pathways, and estimate evaluation measures.

2.2.1 System Element Identification

The goal of system element identification is to decompose the nuclear energy system into a tractable number of elements to permit the identification, refinement, and analysis of pathways to targets. Nuclear systems can be very extensive and complex and contain multiple facilities and operations. Furthermore, a Generation IV NES will not exist by itself but will likely be deployed in the context of an existing fuel cycle architecture, and the interactions with the existing fuel cycle may be significant. For a PR&PP evaluation, therefore, the boundaries and interfaces with other system elements outside the study must be clearly identified.

The system will in general be composed of facilities, controls, etc. For some Host States (i.e., “reactor states”), this system may only comprise reactors, associated storage for fresh and spent fuel, and possibly nuclear research facilities. For other states (i.e., “fuel supplier states” or “fuel cycle states”), an element (e.g., an enrichment facility) or multiple elements of a fuel cycle may also be included.

The evaluation of the system response is facilitated by subdividing the system into discrete elements at the facility level. However, depending on the detail and objectives of the analysis, the analyst may further subdivide facilities into finer elements, to the level of a distinct process or operation. To decide how to define system elements, the analyst may consider the location of the operations and materials, their accessibility and characteristics, and the potential methods used to define Material Balance Areas (MBAs), determine Key Measurement Points (KMPs), and apply safeguards and physical protection. Transportation between facilities can also provide a point for material diversion or theft, and important transportation links must be identified as either separate elements or as part of system elements.

2.2.2 Target Identification

A *PR target* is nuclear material that can be diverted, equipment and processes that can be misused to process undeclared nuclear materials, or equipment and technology that can be replicated in an undeclared facility. A *PP target* is nuclear material to be protected from theft, information to be protected from theft, or a set of equipment to be protected from sabotage. The primary goal of target identification is *completeness*, that is, to ensure that all possible targets and pathways have been identified. At the same time that initial hazard identification is performed for safety analysis, initial target identification can also be performed, typically at the earliest phases of conceptual design when process flow diagrams are first created to define system processes and material stocks and flows. In fact, target identification for various categories of threats in PR&PP evaluations has many similarities with the hazard identification process used in safety analysis (Box 2.1). To ensure completeness, target identification should be updated regularly, along with safety hazard identification, as design progresses and the system processes, stocks, and flows (including waste streams) are defined in progressively greater detail.

Box 2.1 Commonalities Between Safety Analysis and PR&PP

The Generation IV program established four primary goals for Sustainability, Economics, Safety and Reliability, and Proliferation Resistance and Physical Protection. This PR&PP Methodology Report describes the process used to establish the approach to evaluate PR&PP. Similar processes are used to evaluate and compare safety and reliability; it is recommended that the analyses be done in parallel.

The following familiar graphic defines the PR/PP methodological approach:

THREATS → SYSTEM RESPONSE → OUTCOMES

The accident analysis process can be defined in a similar way:

ACCIDENT INITIATORS → SYSTEM RESPONSE → CONSEQUENCES

As these paradigms illustrate, each of the two types of assessments requires similar system information to be collected and analyzed at various stages of facility design, development, and construction. Parallel evaluations in these areas complement each other, and the results of these studies and their implementation interrelate and affect each other.

For a PR&PP evaluation, the appropriate time for early system element and target identification is at the time the facility hazard evaluation (safety assessment) is done as a part of the accident analysis process. The hazard evaluation

- Establishes the maximum quantity of material involved, including its form and possible locations
- Identifies potential initiating events that could affect the hazardous material and lead to a release
- Describes structures, systems, or components that serve to prevent the release of hazardous material in an accident scenario
- Identifies structures, systems, or components that serve to mitigate the consequences of a release of hazardous materials in an accident scenario.

There are obvious parallels in this process to identifying and categorizing targets for both the PP and the PR assessment processes.

Each target or target set associated with a threat category must have at least one pathway. Pathways can be categorized based on specific attributes of the targets and the threat strategy or objective. The potential targets in a system element will also depend on the threat objectives and strategy. The types of pathways that require analysis are established by the threat definition.

For PR threats, PR pathways can be placed into high-level threat types by strategy, using Table 2.1:

- Concealed diversion (material targets)
- Overt diversion (break out) (material targets)
- Concealed facility misuse (process/equipment targets)
- Overt facility misuse (break out) (process/equipment targets)
- Clandestine facility use (process/equipment targets).

For PP threats, PP pathways can be placed into high-level threat types by objective, using Table 2.1:

- Disruption of operations
- Sabotage to cause radiological release (process/equipment targets)
- Theft for nuclear explosives (material targets)
- Theft for RDDs (material targets)
- Information theft (process/equipment targets).

Unless the threat definition more specifically describes objectives and strategies, these high-level PR&PP threat types can be used to organize the process of target identification and to identify material, process, and equipment targets.

Identification of *material targets* for concealed or overt diversion for nuclear explosives (PR) and for theft for nuclear explosives or RDDs (PP) is relatively straight forward, because it can be performed by enumerating all materials entering, residing in, and leaving the system element. Because flow diagrams are usually produced at the earliest stages of design, information on material inventories and flows is usually readily available. However, during target identification all materials containing fissile or fertile elements must be identified, including all waste streams, regardless of concentration or other attributes. This identification is particularly important for waste streams with normally small concentrations of fissile or fertile elements, as the undeclared or unauthorized transfer of additional material into waste streams may provide a pathway for diversion or theft.

Identification of *process and equipment targets* for concealed or overt undeclared misuse (PR) and for radiological sabotage or information theft (PP) involves greater complexity. Seldom can a single process or equipment function be misused (undeclared production) or disabled (sabotage). These acts require the use of a combination of processes and equipment functions, and the adversary may introduce into the system element additional materials, equipment, and tools. Therefore systematic analysis is required to identify all possible process and equipment targets in the system element, for each of the high-level threat pathway threat types.

The identification of process and equipment targets that could be replicated or transferred for use in a clandestine facility requires analysis of potential processes that could be carried out in such facilities. Equipment that creates high technical difficulty in the construction and operation of a clandestine facility would typically have the highest potential for information theft (PP, for transfer to another State) or replication or transfer (PR). The identification of potential targets for information theft and replication can assist in the design of export control systems to monitor for and detect imports of specific components and materials. Such export controls have proven to be one of the more effective methods for detecting clandestine production facilities.

For undeclared production using declared facilities, the identification of target sets must consider the potential rerouting of flows in the declared facility, the addition of undeclared materials and equipment to the system, and performance of some portions of the process outside the system element in undeclared, clandestine facilities. For radiological sabotage, the identification of target "cut" sets must consider all potential combinations of equipment failures that could result in a radiological release.

After all target sets have been identified, it is then possible to identify *success sets*; that is, minimum sets of equipment functions that, if protected, result in adversary failure for all possible target sets. For undeclared production, the identification of such success sets can assist in the design of the safeguards approach for the system element. For sabotage, the identification of success sets can assist in the design of the PPS.

2.2.2.1 PR Target Identification

Identification of PR targets proceeds in two steps. Each step examines a different type of target.

1. For concealed and overt (break out) diversion strategies:

    - *Nuclear material stocks* are examined one at a time to identify inventories that could be targets.
    - *Nuclear material flows* are examined one at a time to identify movement of nuclear material that could be diverted.

    If the proliferant State's strategies include concealed, protracted diversion, then even small material inventories and flows must be considered because they may be targets that contribute to meeting the proliferant State's objectives.

2. For concealed and overt (break out) misuse strategies, system elements are examined one at a time to identify the following targets:

    - *Any declared equipment that is consistent with the strategies and objectives in the threat definition and that could be misused for materials processing*. Targets are identified on the basis of the service the equipment provides (e.g., irradiation, plutonium separation, enrichment), without consideration of details such as capacity, technical difficulty, or cost. At this stage of the evaluation, facilities outside of the normal operating envelope must be included. Details such as how clandestine materials are inserted into the process and products extracted, including off-normal operation such as inadvertent material hold up, are considered during analysis of pathway segments.

- *Technology (information and equipment) that is consistent with the strategies and objectives in the threat space and that could be misused for proliferation in clandestine facilities*. This technology could include, for example, equipment that could be replicated (cloned) in a clandestine facility, information that could assist a proliferant State in designing or constructing a clandestine facility, or critical equipment that could be used in a clandestine facility after being declared lost or damaged. This step requires expert judgment to identify technology that is provided by the system elements and that would otherwise not be generally available to the proliferant State for a weapons program. Note that these targets could also be targets for theft for transfer to a proliferant State. Information theft is covered under PP pathway analysis but may use the same target identification process.

Target identification and subsequent segment identification typically requires iterative review and revision to consider different aspects of the proliferant State's strategy.

2.2.2.2 PP Target Identification

PP evaluation considers two broad classes of targets: *material targets* for theft of nuclear material and *equipment targets* for sabotage or theft of information. Because a system may contain a large number of targets with similar characteristics, targets are then systematically categorized, sorted, and possibly ranked, allowing a representative subset of the targets to be selected for further detailed analysis.

Because flow sheets are normally generated early in the design process, information about materials stocks and flows is usually readily available to the analyst. To identify PP material targets for nuclear explosives, the same target identification process described above to identify PR diversion targets can be applied. For theft of materials for RDDs, all radioactive materials in the system elements must be considered, including, for example, low- and high-level waste streams. A similar method to that for nuclear explosives materials can be used to provide a comprehensive identification of RDD material targets.

The identification of equipment targets for sabotage requires a more complex and analytical process. Typically, for successful sabotage resulting in radiological release, an adversary must disable the functions of a number of different pieces of equipment. An equipment target set is defined as a minimum set of equipment that must be disabled to successfully sabotage a facility. A facility will often contain multiple possible equipment target sets. The number and diversity of equipment functions in each equipment target set provide a measure of the system's redundancy and diversity.

While the goal of an attacker is to disable a complete equipment target set, the goal of the PPS is to protect at least one element of each possible equipment target set. A success set can then be defined as the minimum set of equipment functions that would include at least one element from each possible equipment target set.

Equipment target set identification is performed routinely during the design of PPSs for nuclear facilities. The approach is similar to that used in probabilistic safety assessment

(PSA) to identify combinations of equipment functions (cut sets) that, if failed, could generate radiological releases. PSA studies can provide a starting point for the identification of potential radiological sabotage targets but must be modified in two ways. First, the probability of multiple, simultaneous failures of diverse and redundant components may be increased substantially. Second, the probability of failure for passive components that normally have high reliability (walls, fire barriers, doors, vessels, etc.) can also increase.

Target identification for sabotage involves three steps: (1) the systematic search for sets of equipment with functions that, if disabled, could result in the subsequent release of radionuclides (complete equipment target sets); (2) the selection of a subset of each equipment target set to be protected (vital equipment identification), and (3) the definition of vital areas associated with these vital equipment sets to identify access paths, allowing the accessibility of the equipment to be evaluated.

Various analytical approaches can identify equipment target sets, and analysts' preferences play a role in approach selection. For initial screening, target identification trees can be used, where at the top level, the main high-level sabotage targets are identified, and the bottom-most nodes contain equipment target sets that if disabled would lead to the consequence at the top of the tree.

2.2.3 Target Categorization

For any given category of threat objective and strategy, systematic target identification is expected to result in a large number of targets or target sets, many of which will share substantial similarities. For each category of the threat objective and strategy, *target categorization* applies a taxonomy based on *target attributes* to group targets into a manageable number of bins (categories) with common characteristics. This binning helps to reduce the number of pathways that must then be considered in detail, by aggregating targets and pathways together to allow the identification of *representative* targets and pathways.

The categorization approach uses attributes selected based on the threat objective and strategy and the major segments of its pathways. For example, for the PR threat strategy of covert material diversion, material targets can be categorized by the attributes that are important to the acquisition, processing, and fabrication segments. Likewise, for the PP threat strategy of radiological sabotage, process and equipment targets are categorized by attributes that are important to the access, exploitation, and consequence generation segments.

Categorization allows targets to be grouped into categories where a representative or "bounding" target can be selected from each category. "Representative" means that, for a given type of threat objective and strategy, similar safeguards or PPSs can be employed to protect the target and approximately similar system response and outcomes could be expected for any target in the category. "Bounding" means that the target is expected to have the worst outcome of the various targets in the category. Therefore, target categorization allows the number of targets and pathways selected for detailed pathway analysis to be reduced to a more tractable number. It also allows designers to determine the availability of off-the-shelf safeguards and PPS designs or the need to develop these designs.

As with all taxonomies where individual items are grouped based on attributes, target categorization will be inherently approximate. If very large differences in outcomes are found to be possible for different targets and pathways grouped into a single category, then an important target attribute has been missed. For this reason, there is no “perfect” categorization method, and target categorization methods are expected to, and should, evolve as analysts gain experience, and therefore it is important that analysts reference and consider earlier studies.

Target attributes may include both physical attributes and location attributes. Physical attributes used for target categorization will often be known relatively early in the design process. For material targets, these attributes include property characteristics that can be determined from process flow sheets, such as isotopic compositions, physical forms, inventories, and flow rates. For equipment targets, these attributes include basic characteristics of the equipment functions.

Somewhat later in the design process, physical arrangement drawings are produced, which will help to define the location attributes of targets. For example, physical location will have important effects on the accessibility of PP targets and the ability to safeguard PR targets. Indeed, it is expected that designers will find target categorization tools helpful in the physical arrangement design by providing guidance in selecting location attributes to achieve uniform reduction of overall vulnerability, for example by locating PP equipment targets with higher fragility in locations with lower accessibility.

In addition, some target attributes are determined only during detailed design and/or following the development of detailed operation and maintenance procedures. Examples include the following:

- Design features to harden an equipment function to resist sabotage damage
- Design features that would generate detectable signatures if undeclared fertile material were introduced into a reactor for irradiation
- Operational procedures to implement a two-person rule for maintenance/operation activities.

Where important target attributes are determined only after detailed design, analysts can introduce reasonable assumptions about detailed design and operation and maintenance procedures by specifying system *performance objectives* or by referencing specific safeguards or PPS designs developed for previous applications. For example, when an area accessibility category is assigned to a PP target location, the area category may have an associated set of performance objectives related to access control. Likewise, when a safeguards assessment shows that a well-developed safeguards system design already exists for a given category of target, this design may be referenced for use in the new system under development. Performance objectives introduced into target categorization must be documented and a *performance evaluation* conducted following detailed design to ensure that the objectives have been met. References to existing safeguards or PPS designs must be tracked to ensure that the design is properly implemented.

2.2.3.1 PR Target Categorization

For material targets, categorization is performed by examining the range of combinations of physical attributes and location attributes for each material target identified. In general, the analyst should employ a systematic process, including reviewing earlier studies, to ensure that all important attributes have been identified and considered in categorizing targets.

2.2.3.2 PP Target Categorization and Sorting

For PP targets the target identification process can yield large numbers of targets. To facilitate analysis and to gain insight, it is valuable to categorize targets by their key attributes: for material targets, accessibility and attractiveness; and for equipment targets, accessibility and fragility. Sorting in this manner simplifies the selection of a representative subset of targets for detailed pathway analysis and gains the analyst significant insights about the most important PP strengths and vulnerabilities in a system.

Accessibility is one of the key attributes of PP targets. Table 2.2 provides an example of seven accessibility categories that can be used to sort PP targets. In general, access control is a highly developed concept in PP. In nuclear facilities, access to nuclear materials and vital equipment is controlled using a set of multiple access areas, each of which includes detection and delay elements. Specific requirements and recommendations for controlling access into nuclear facilities using multiple controlled access barriers are found in U.S. and international documents (10 CFR 73, U.S. Code of Federal Regulations 2006; INFCIRC/274/Rev.1, *The Convention on the Physical Protection of Nuclear Material*, IAEA 1980[5]; and INFCIRC/225/Rev.4 (Corrected), *The Physical Protection of Nuclear Material and Nuclear Facilities*, IAEA 1999[6]). In this categorization, a protected area (Type 3 and greater in Table 2.2) is surrounded by a perimeter. A protected area can then contain secondary areas with additional access barriers (Types 4, 5, and 6 in Table 2.2).[7] These secondary areas are of two basic types: *material access areas*, where nuclear material to be protected from theft is in use or stored; and *vital areas*, containing equipment to be protected from sabotage.

---

[5] The Convention is the only international legally binding undertaking in the area of physical protection of nuclear material. It establishes measures related to the prevention, detection and punishment of offenses relating to nuclear material.

[6] In INFCIRC/225/Rev.4, the IAEA provides a set of non-binding recommendations on requirements for the physical protection of nuclear facilities and nuclear material in use, in storage, and during transport.

[7] The term "secondary area" is only used in this report to describe a generic security system. This term is not found in IAEA documents or CFRs. For example, IAEA material access areas are described by terms such as inner areas and storage areas, with protection requirements varying with material category.

Table 2.2: Example Area Accessibility Categories
(from most accessible to least accessible)

Area Category	Description	Examples
(Type 1) Public area	Area open to the public	Visitor's center
(Type 2) Controlled area	Area with limited access control inside a plant site's gates	Storage warehouses, parking lots, and training centers.
(Type 3) Protected area	Area protected by double fences and other intrusion detection; access restricted to screened plant workers and visitors, and access portals detect the introduction of weapons or explosives	Turbine buildings, maintenance shops, and transformer areas.
(Type 4) Vital area—high frequency access	Vital or material access area (e.g., inside a protected area, with additional portals to delay unauthorized access) with frequent access by plant personnel	Control room, spent-fuel pool, glove boxes for mixed-oxide fuel fabrication, and areas with equipment requiring frequent routine surveillance
(Type 5) Vital area—moderately frequent controlled access	Vital or material access area for moderately frequent access, with a robust active portal and provisions for augmented PP during access periods	An enclosure for reactor control logic and battery power, with a vault-like door; material storage vaults; and a reactor primary containment structure during reactor operation
(Type 6) Vital area—infrequent controlled access	Vital or material access area for infrequent access, with a robust passive portal and provisions for augmented PP during access periods	Passive decay-heat removal equipment space under a crane-movable hatch, reactor cavity, interior of a dry-cask storage container, interior of a hot cell, and interior of a reprocessing canyon
(Type 7) Highly inaccessible area	Area never accessed during normal operation and with a high difficulty of gaining access	Soil around a buried reactor cavity silo, soil around a buried spent-fuel pool wall, and interior of a closed and backfilled geologic repository

For theft, an adversary must gain access to material, successfully remove the material from the facility, and exploit the material to achieve the objective. In addition to accessibility (Table 2.2), material targets can be sorted by *attractiveness*. Materials are routinely sorted by attractiveness[8] and *category* levels during PPS design. Categories of

---

[8] It is important to note that the PR&PP definition of material type (MT) is quite different from the attractiveness concept. Attractiveness considerations apply to the material in the form in which it exists at any point in a system element. On the other hand, the PR&PP material type applies to the processed material in its final, weapons usable metal form.

nuclear material identified in DOE's graded physical protection[9] program are shown in Table 2.3 (DOE M 470.4-6, *Nuclear Material Control and Accountability*, 2005). In the DOE system there are five material attractiveness levels (A to E, based on physical form, radiation level, chemical composition, and isotopic content), and four physical protection categories (I to IV, based on quantity of material present). The table is used by the U.S. DOE in specifying the physical protection requirements for materials that could be potential theft targets for use in nuclear explosives. In the DOE graded physical protection hierarchy, materials that are highly irradiated, as well as all forms of uranium with enrichment below 20%, are assigned the lowest attractiveness level: Level E. All Level E materials fall under the least protective safeguards requirements of Category IV. In general, these materials are both intrinsically difficult to handle and remove from a facility, (i.e., they are bulky and/or radioactive), and they are difficult to process into weapons-usable forms after removal. Materials within attractiveness levels A to D in quantities within category levels I to III have more restrictive physical protection requirements.

For sabotage, an adversary must first gain access to equipment and then successfully disable the equipment’s function. In addition to accessibility (Table 2.2), equipment targets can be sorted by *fragility*. Table 2.4 presents an example of three equipment-function fragility categories that highlight the relative difficulty of disabling an equipment function in a manner that cannot be easily mitigated.

Some types of equipment can be readily located in areas of low accessibility, and some equipment functions can be difficult to disable or can be easily repaired if disabled. Equipment with low accessibility or low fragility (for example passive safety equipment that does not require routine surveillance) can be called *resilient*. In general, resilient equipment is more difficult for an adversary to defeat, particularly if sets of resilient equipment also have redundancy and/or diversity.

For sabotage, it may not be possible or necessary to completely identify all the equipment in every possible equipment target set at the conceptual-design and qualitative analysis levels. Instead, analysts may choose to simply show that each equipment target set includes some resilient equipment. For the adversary, the difficulty of defeating the equipment target set will depend primarily on the difficulty of defeating this resilient equipment, and of defeating the additional equipment functions in the equipment target set for which the adversary will likely have only uncertain information (information describing complete equipment target sets is sensitive and protected).

From the designer’s perspective, it is valuable to identify potential equipment target sets and to ensure that the system design introduces resilient equipment into each equipment target set. Additionally, benefits can come from redundancy and diversity in equipment target sets (e.g., the fact that an equipment target set has a large number of different elements).

---

[9] Graded physical protection, which is sometimes called “graded [*domestic*] safeguards,” is the concept of providing the greatest relative amount of physical protection (control and effort) to the types and quantities of nuclear material that can be most effectively exploited for use in a nuclear explosive device.

Table 2.3: DOE Safeguards Categories I to IV for Physical Protection of Nuclear Materials Which Can Be Used in a Nuclear Explosive Device
(based on the Graded Safeguards Table of DOE Manual 470.4-6)

	Attractiveness Level	**Category (quantities in kilograms)**							
		Pu or U-233 [g]				**U-235 or Np-237**			
		I	**II**	**III**	**IV**	**I**	**II**	**III**	**IV**
Weapons [a]	A	All Quantities	NA	NA	NA	All Quantities	NA	NA	NA
Pure products [b]	B	≥2	0.4-2	0.2-0.4	<0.2	≥5	1-5	0.4-1	<0.4
High-grade materials [c]	C	≥6	2-6	0.4-2	<0.4	≥20	6-20	2-6	<2
Low-grade materials [d]	D	NA	≥16	3-16	<3	NA	≥50	8-50	<8
All other materials [e]	E	Any reportable quantity [f] is Category IV							

NOTES: NA indicates not applicable.

[a] Assembled weapons and test devices (Category I for any quantity).

[b] Weapons components, buttons, ingots, recastable metal, and directly convertible materials.

[c] Carbides, oxides, solutions of ≥25 g/L, nitrates, fresh fuel elements and assemblies, alloys and mixtures, UF_4 or UF_6 at ≥50% enrichment.

[d] Solutions of 1-25 g/L, process residues requiring extensive reprocessing, moderately irradiated material (i.e., radiation dose equivalent rate >0.15 to 1 Sv/hr at 1 meter, where 1 Sv (sievert) ≡ 1 J/kg = 100 rem), Pu-238 (except in waste), and UF_4 or UF_6 at ≥20% <50% enrichment.

[e] Highly irradiated forms (i.e., radiation dose equivalent rate >1 Sv/hr at 1 meter, e.g., spent fuel), solutions <1 g/L, and uranium in any form and quantity containing <20% U-235 or <10% U-233.

[f] A reportable quantity is 1 g or more of Pu-239 to Pu-242 and enriched uranium, and 0.1 g of Pu-238.

[g] Total quantity of U-233 = [Contained U-233 + Contained U-235].

Table 2.4: Example Equipment Function Fragility Categories
(from most fragile to least fragile)

Equipment Function Category	Description	Examples
(Type 1) High fragility	Equipment functions can be disabled rapidly using simple, readily available tools	Operability of electronic circuit boards, power and control wiring, pump motors, valve actuators, and circuit breakers; and combustion of flammable materials
(Type 2) Intermediate fragility	Equipment functions can be disabled with some time delay with readily accessible tools, or rapidly with tools that are normally not permitted or are controlled in the plant, such as small explosive charges	Operability of electronics inside locked cabinets; leak-integrity of tanks, pipes and heat exchangers; and operability of mechanically actuated reactivity control mechanisms
(Type 3) Low fragility	Equipment functions require large explosive charges, large missiles, or other heavy tools (e.g., cranes) to be disabled	Structural integrity of reinforced concrete walls and structures; gross leak integrity of lined reinforced concrete structures; thermal inertia of liquids, solid materials and structures; and negative core temperature reactivity coefficients

Following a sabotage attempt, *mitigation measures* may be taken to reduce attack consequences. For adversaries to achieve their objective, their equipment target set and attack strategy must also prevent mitigation measures. Therefore, system characteristics that enable mitigation can contribute to the resilience of a equipment target set. For example, reactor cores with very large thermal inertia can generate long delays for decay-heat thermal damage.

After equipment target sets and targets have been identified and categorized, equipment target sets can be sorted and ranked to aid subsequent target pathway analysis based on the presence of resilient equipment, the redundancy and diversity of equipment, and system characteristics that would facilitate mitigation if the equipment target set were disabled.

Likewise for theft, targets can be categorized, sorted, and ranked based on the accessibility and attractiveness of the targets.

While target categorization and sorting can provide important insights for PP robustness by identifying potential strengths and vulnerabilities, it also has important limitations because it does not consider details of the threat definition and system design that may have important effects on the system response. Furthermore, categorization alone provides insufficient information to evaluate the PP measures except in a qualitative way.

Thus, at the coarse-pathway level, it is expected that pathway analysis will also be performed for a representative subset of targets in the system. For material targets, pathway analysis should include targets that have high accessibility and/or attractiveness, and, for sabotage, pathway analysis should include the most resilient equipment in the potential equipment target sets.

2.2.4 Pathway Identification and Refinement

Pathways are potential sequences of events or actions followed by a proliferant State or adversary to achieve objectives. Figure 2.1 depicts the major stages of the pathway analysis for both PR and PP, highlighting the strong parallels between the methodologies. The figure also suggests how intermediate results can readily be reported from each stage. (An additional parallel can be drawn to safety evaluation by replacing the "threat" with "accident initiator" and then defining stages of movement of the radiological source term; also see Box 2.1.)

For PR, the full pathway by which a proliferant State obtains a nuclear explosive device can be divided into three major stages:

> **Acquisition**: *Activities carried out to acquire nuclear material in any form, starting with the decision to acquire the material and ending with the availability of the material.* Unless ready-to-use material is acquired (e.g., separated plutonium in metallic form), further processing will be needed before beginning the fabrication stage.
>
> **Processing**: *Activities carried out to convert the nuclear material obtained in the acquisition stage into material ready for use in a nuclear weapon.* Processing may include such activities as irradiation of targets, plutonium separation, uranium enrichment, and reduction of oxides or fluorides to metal.
>
> **Fabrication:** *Activities carried out to manufacture and assemble nuclear explosive devices.* Fabrication starts from the processing stage, or in some cases directly from the acquisition stage, with nuclear material that is ready for use in a nuclear explosive device (e.g., plutonium in metallic form) and ends with the availability of one or more nuclear explosive devices.

Similarly, for PP, the full pathway by which an adversary steals a theft target or damages a sabotage target can also be divided into three major stages:

> **Target access**: *Activities carried out to gain access to a target or an equipment target set.* Target access may include such activities as disabling intrusion detection systems and breaching protective barriers to access material or equipment.
>
> **Target exploitation**: *Activities carried out to remove a theft target from a facility or transportation system or to damage an equipment target set.*
>
> **Consequence generation**: *Sequence of events following target exploitation that result in release, damage, or disruption.*

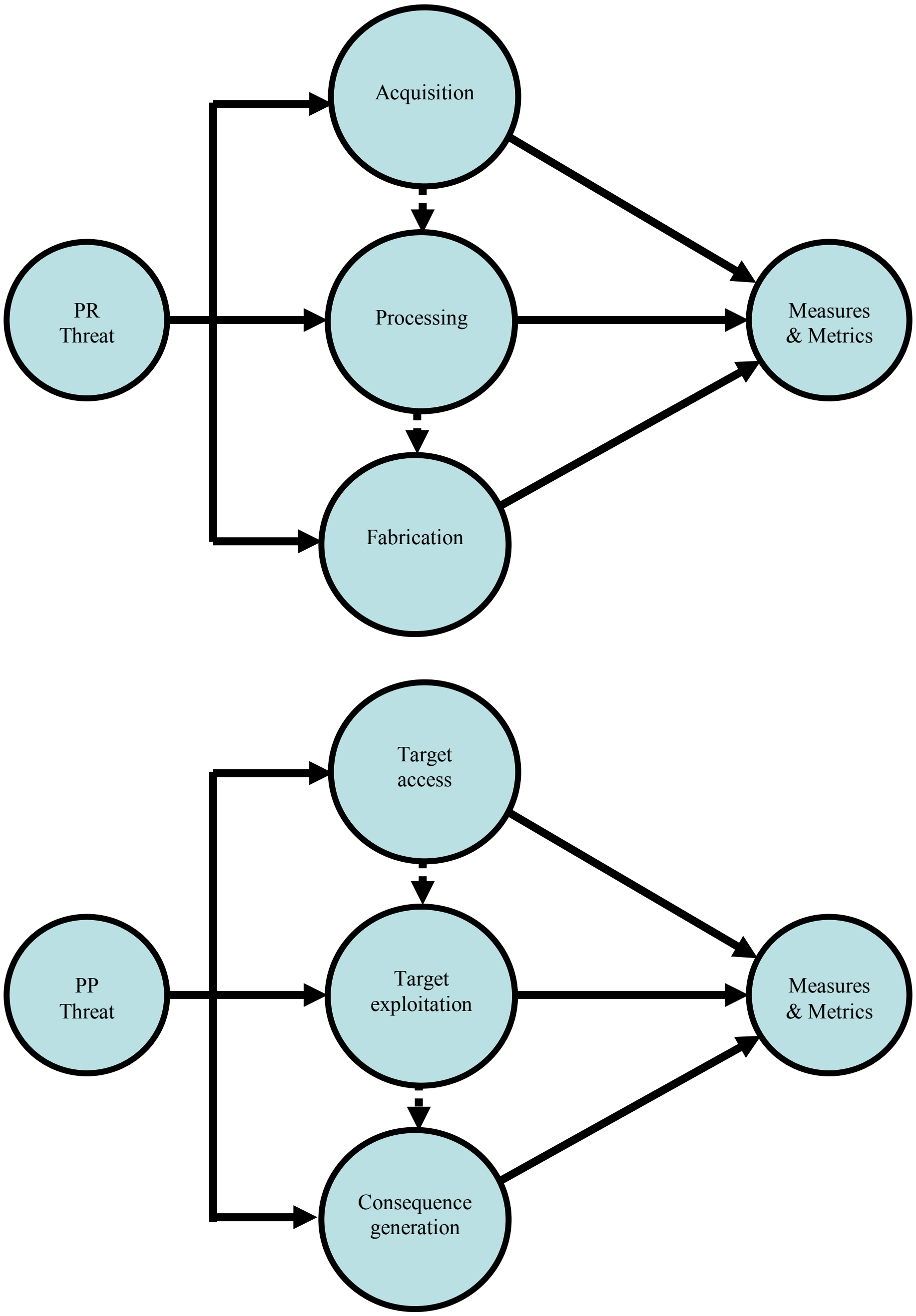

Figure 2.1: Major Stages of Pathway Analysis for PR and PP

Pathways are composed of segments. Segments are built around targets. For coarse path analysis, a *segment* describes the *action* to be performed. A complete proliferation pathway requires acquisition, processing, and fabrication, and a complete theft or sabotage pathway requires target access, exploitation, and consequence generation. Each of these stages may be composed of one or more segments.

Segments carried out within the boundaries of the declared NES are called *internal segments*; all others are called *external segments*. External segments may describe such things as plutonium extraction, uranium enrichment, or target production performed in undeclared facilities. Pathways are constructed by linking together segments in logical sequences that result in a final outcome.

In every PR segment, a safeguards system may detect anomalies, while in every PP segment, the PPS may detect, delay, and neutralize unauthorized actions. The use of the segment and pathway formulation helps system designers to interact with safeguards and PP experts, identify opportunities to introduce effective safeguards and PP measures, and refine the safeguards and PP approaches for the system. The safeguards and PP approaches comprise the specific measurements made by the safeguards and PP monitoring systems. The monitoring systems detect anomalies that would be generated by the action performed in a pathway segment but could also be generated by other sources (false alarms). Following the detection of an anomaly, the safeguards and PP approaches also specify the subsequent actions that are performed to determine whether a false alarm has been received. The PP approach also comprises the specific system design features and PP force strategies that contribute to the delay and neutralization of an adversary following detection.

At the conceptual design stage, often safeguards and PP approaches will not be available, except for cases where their design is obvious (e.g., safeguards for a sealed-core reactor) or easily available (off the shelf). Before a safeguards or PP approach is defined, the detection probability and false alarm rate for a pathway segment (and the delay and neutralization probabilities for PP) can be specified as *performance objectives* for each pathway segment to permit pathway analysis.

The approach used to generate the pathways affects the methods that can be used to cope with the large number of pathways expected in a comprehensive analysis. The method used to generate pathways must

- Be tractable, natural, and comprehensible to subject matter experts
- Create a robust, credible, and representative set of pathways
- Provide confidence that all credible pathways are covered but avoid or dismiss pathways that are obviously not credible, that are sufficiently similar that they can be treated using a representative target and pathway, or that don’t contribute to the overall evaluation of the NES.

For coarse pathway analysis, the number of segments may initially be limited. Limiting pathways makes it possible in some cases to manually generate a number of potential pathways, categorize these pathways, and then select a representative set of pathways for qualitative descriptive analysis to evaluate measures.

While such a qualitative exploration of pathways is useful, and even desirable, in a preliminary PR&PP evaluation, analysts require a structured method for pathway generation to ensure the completeness of a comprehensive analysis. Both PR and PP evaluations should consider all lifecycle stages (e.g., design, construction, commissioning, operation, transients, accidents, shutdown, and decommissioning). Because very large numbers of similar pathways may exist, representative pathways must be identified to keep the analysis tractable.

The PR&PP methodology does not prescribe the type of analytical tool to use in pathway analysis. The various approaches to pathway analysis include methods based on event trees, influence diagrams, success trees, dynamic probabilistic methods such as Markov chains, and two-sided simulation methods, among others. These methods directly incorporate and facilitate the aggregation of pathway segments.

2.2.4.1 PR Pathway Refinement

The first step in generating pathways for a specific target is to construct internal and external segments by assigning an action to be performed or initiated by the proliferant State related to the target.

Internal segments are identified by reviewing each target and its location. At a coarse pathway level the action for material targets is diversion. For each process target, the action is misuse, and the undeclared material that must be introduced into the system to misuse the process is identified.

External segments represent actions that the adversary must conduct in facilities outside the declared NES to complete a pathway leading to a nuclear explosive device. Generation of external segments challenges the analyst to creatively search for ways in which internal segments can be credibly combined with actions in facilities outside of the NES.

A proliferant State may also choose to replicate declared equipment or processes in an undeclared facility, so that the replicated equipment or processes in the undeclared facility can be used without detection by safeguards. Replication pathways can be attractive because activity at the declared facility can reduce the probability that acquisition of undeclared equipment and components will be detected by export controls and national technical means and can reduce the technical difficulty of successfully implementing the undeclared process.

Segment refinement occurs after initial segment identification. At the coarse pathway level, a segment includes a minimal set of characteristics necessary to estimate PR measures. Refinement may lead to a rapid increase in the number of pathways. Figure 2.2 illustrates a generic PR pathway consisting of one segment for each stage (acquisition, processing, fabrication), and the subsequent expansion of each segment into a number of segments as refinement progresses. This growth in the number of segments and pathways presents an analytical challenge.

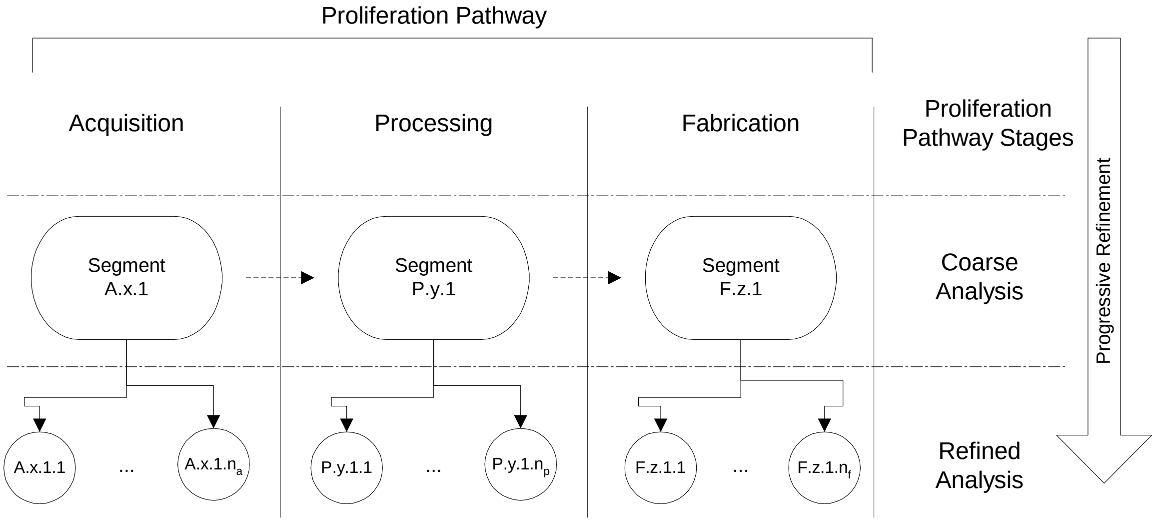

Figure 2.2: Refinement of Pathways
(In most PR assessments, it is not necessary to analyze the fabrication stage in detail.)

At a coarse pathway level, the characteristics used to refine each segment include the material type, the location in which the action occurs, the quantity of material involved, and the general types and effectiveness of safeguard detection measures that may be applied to detect actions occurring in the segment. During subsequent refinement, additional characteristics are considered, such as the mode of facility operation during the diversion, material characteristics, penetrations utilized, specific safeguard instruments and methods applied to detect undeclared actions, false alarm frequencies for anomalies detected by safeguards, and additional details regarding the proliferant State's concealment strategy. This information then allows systematic analysis of the pathway segments to generate increasingly accurate estimates of the pathway outcome.

A descriptive presentation can be valuable in presenting the sequence of segments that constitute a given pathway. Graphical representations can also be useful to visualize pathways and the segments from which they are constructed and to identify the various ways that segments can be combined to create pathways. Two alternate but equivalent graphical representations that can be useful at a coarse pathway level are network diagrams and event trees.

2.2.4.2 PP Pathway Refinement

After a PP threat definition has been specified and representative PP targets have been identified, scenario methods can be used to determine the various possible sequences of events following an attack on the target. These event sequences can be diagramed with several different approaches: logic diagrams, event trees, adversary sequence diagrams, or even a verbal description. All such event sequences should be diagramed from the perspective of the adversaries as a tactical map of activities and events necessary to achieve their objective. For sequential or serial activities, the same type of logic structure as the pathway diagrams in PR can be used. However, the entire equipment target set must be addressed from the adversary's perspective for a sabotage objective to be complete, and this may require activities to be accomplished in parallel with a more complex diagramming tool. In general, a segmentation of the complete pathway aids in the analysis.

PP pathways are typically composed of multiple segments or a subset of events that contribute to an attack on the NES. In the earliest stages, the assessment can be organized in coarse pathway diagrams that serve as the basis for judgmental quantification. As more design detail becomes available, more detail is added to the pathways through pathway segments, and engineering analysis replaces judgment in assessing the probabilities and measures. The specific analytical tools that can provide the most efficient and effective solution to the pathway model will depend on the specifics of each pathway.

For example, the action of gaining access to a portion of the facility can be divided into pathway segments that detail the exact movement through the facility and specific barriers to be defeated. This segmentation can be repeatedly used in the analysis. For example, a specific type of portal may provide a barrier for several different types of targets. A segment that represents gaining access through this type of portal can be used repeatedly for all these targets.

Some segments can happen in parallel, while others must occur serially. Detailed pathways must be constructed to be consistent with the capabilities defined for the threat. For example, the number of segments that can be pursued in parallel must be consistent with the number and capability of the adversaries.

2.2.5 Estimation of Measures

Once pathways have been identified and analyzed, analysts determine measures for the evaluation. The measures differ for PR and PP evaluations.

2.2.5.1 PR Measures

The PR measures introduced in Section 1.4.2 can be categorized into two groups: those that result primarily from intrinsic features of a system and those that result from a combination of intrinsic features of a system and extrinsic measures applied to the system. For example, the measure of Detection Probability is affected by intrinsic features like the accessibility to nuclear material, uniqueness of material signature, and hardness of radiation signature. However, it is also affected by extrinsic measures, such as the international safeguards agreements to which the Host State is a party.

PR measures determined primarily by intrinsic features of a system include

- Proliferation Technical Difficulty (TD)
- Proliferation Cost (PC)
- Proliferation Time (PT)
- Fissile Material Type (MT).

PR measures determined by both intrinsic features of a system and extrinsic features applied to the system include

- Detection Probability (DP)
- Detection Resource Efficiency (DE).

Of the measures, MT is estimated for complete pathways, whereas the remaining measures are estimated for each segment. The DP measure is evaluated when sufficient information is available about the safeguards approach. If the safeguards approach is not available, then an appropriately large uncertainty is assigned to the DP measure. The pathway value of each of these measures is obtained by aggregating the estimates for each segment in the pathway.

The analyst must employ a systematic process to ensure that all system attributes that might affect the measure value have been identified and considered in the pathway modeling, for example by reviewing earlier studies and employing the “safeguardability” analysis discussed in Appendix D.1. For qualitative pathway analysis, segment measures can be estimated directly from the segment characteristics using expert judgment. Qualitative pathway analysis can be further simplified by recognizing that certain measures for certain segments typically dominate the difficulty of proliferation. For example, for some threats and pathways the TD, PC, and PT measures may be weak barriers for material diversion compared with DP, and hence that measure takes paramount importance. In a more refined analysis, the measure values are estimated using more structured techniques allowing formal methods for aggregation.

After measures have been estimated for pathways, pathways must be compared and ranked (Section 2.3) relative to the Generation IV goal (DOE, 2002a) to provide “a very unattractive and least desirable route” for diversion or undeclared production. Therefore, to facilitate pathway comparison, quantitative metrics are applied to the TD, PC, PT, MT, and DP measures to relate them to linguistic values, from very low to very high, that would suggest the likely decision-making by a proliferant State. Likewise, for the DE measure, a quantitative metric is applied to reflect the magnitude of required resources, relative to the resources that the IAEA commonly applies to safeguard facilities. The analyst may select other quantitative metrics appropriate for comparing pathways for the specific threat being considered. As a starting point, the analyst may choose to apply the approximate, representative metrics given in Table 2.5.

Each of the PR measures and corresponding metrics are discussed in greater detail below.

Proliferation Technical Difficulty (TD) Measure

The TD measure is estimated using a metric scale as shown in the example given in Table 2.5. Technical difficulty arises from inherent characteristics of the pathway that create difficulty and thus a potential for failure from technical problems. When scaled to reflect the State’s capability, the TD measure assists in distinguishing pathways a proliferant State would judge to have higher risk of technical problems and to have the potential to greatly increase the time and resources to complete a pathway or to result in the failure to complete a pathway.

Estimation of TD uses expert judgment to identify the sources of intrinsic difficulty in completing a pathway segment, such as difficulty from criticality hazards, radiation, lack of design information, lack of access, or inability to fabricate or produce equipment or materials covered by export controls. Estimation of TD for a complete pathway uses the combined sources of difficulty for all segments.

Table 2.5: Example Quantitative Metrics and Scales for PR Measures (qualitative PR ranking [Very Low → Very High], numerical range for bins, and median numerical values)

Measures and Metrics	Metric Scales Bins (Median)	Proliferation Resistance
Proliferation Resistance Measures Determined by Intrinsic Features		
Proliferation Technical Difficulty (TD) Example metric: Probability of pathway failure from inherent technical difficulty considering threat capabilities	0-5% (2%)	Very Low
	5-25% (10%)	Low
	25-75% (50%)	Medium
	75-95% (90%)	High
	95-100% (98%)	Very High
Proliferation Cost (PC) Example metric: Fraction of national resources for military capabilities	0-5% (2%)	Very Low
	5-25% (10%)	Low
	25-75% (50%)	Medium
	75-100% (90%)	High
	>100% (>100%)	Very High
Proliferation Time (PT) Example metric: Total time to complete pathway	0-3 mon (2 mon)	Very Low
	3 mon-1 yr (8 mon)	Low
	1-10 yr (5 yr)	Medium
	10 yr-30 yr (20 yr)	High
	>30 yr (>30 yr)	Very High
Fissile Material Type (MT) Example metric: Dimensionless ranked categories (HEU, WG-Pu, RG-Pu, DB-Pu, LEU); interpolation based on material attributes	HEU	Very Low
	WG-Pu	Low
	RG-Pu	Medium
	DB-Pu	High
	LEU	Very High

Table 2.5: Example Quantitative Metrics and Scales for PR Measures (continued)

Measures and Metrics	**Metric Scales Bins (Median)**	**Proliferation Resistance**
Proliferation Resistance Measures Determined by Extrinsic Measures and Intrinsic Features		
Detection Probability (DP) Example metric: Cumulative detection probability	a	Very Low
	b	Low
	c	Medium
	d	High
	e	Very High
Detection Resource Efficiency (DE) Example metric: GW(e) years of capacity supported (or other normalization variable) per Person Days of Inspection (PDI) (or inspection $)	<0.01 (0.005 GWyr/PDI)	Very Low
	0.01-0.04 (0.02 GWyr/PDI)	Low
	0.04-0.1 (0.07 GWyr/PDI)	Medium
	0.1-0.3 (0.2 GWyr/PDI)	High
	>0.3 (1.0 GWyr/PDI)	Very High

NOTES:
HEU = high-enriched uranium, nominally 95% ^{235}U;
WG-Pu = weapons-grade plutonium, nominally 94% fissile Pu isotopes;
RG-Pu = reactor-grade plutonium, nominally 70% fissile Pu isotopes;
DB-Pu = deep burn plutonium, nominally 43% fissile Pu isotopes;
LEU = low-enriched uranium, nominally 5% ^{235}U.

a Significantly lower cumulative detection probability than the IAEA detection probability and timeliness goal for depleted, natural, and low-enriched uranium.
b 50% in 1 year (This equates to IAEA detection probability and timeliness goal for 1 significant quantity of depleted, natural, and LEU uranium).
c 20% in 3 months, 50% in 1 year (This equates to IAEA detection probability and timeliness goal for 1 significant quantity of spent fuel/irradiated material).
d 50% in 1 month, 90% in 1 year (This equates to IAEA detection probability and timeliness goal for 1 significant quantity HEU/separated Pu).
e Significantly greater cumulative detection probability than the IAEA detection probability and timeliness goal for HEU/separated Pu.

The metric scale for the TD measure reflects the probability that a pathway will end in failure and thus depends on the resources and capabilities available to a proliferant State. Thus, for example, the TD of an external segment to construct and operate a concealed centrifuge enrichment plant may become lower if a State has an operating commercial enrichment capability or can access expert guidance. However, the TD for manufacturing specific components for centrifuges, such as frequency invertors, may remain high if a State does not have a domestic commercial capability to manufacture these components. Most of the nuclear components that have high TD to manufacture are monitored by international export controls and by national intelligence services. The evaluation of the DP measure may include the potential for export controls to detect the acquisition of such equipment.

The use of probabilistic methods can facilitate aggregation of the TD measure associated with each segment in a pathway. Examples based on Markov models are contained in Yue, Cheng, Papazoglou, Azarm, and Bari (2005). Table 2.6 summarizes key characteristics of the TD measure.

Table 2.6: Summary of Characteristics for the
Proliferation Technical Difficulty (TD) Measure

Characteristic	Description
Definition	Inherent difficulty of the segment
Typical attributes to be considered for estimation	Criticality hazards Radioactivity levels Availability of open information Access to specialized export-controlled components or materials
Example metric	Probability of pathway failure from inherent technical difficulty considering threat capabilities
Segments-to-pathway aggregation method	Calculate the probability of pathway failure on the basis of the segments involved.

Proliferation Cost (PC) Measure

The PC measure is estimated in dollars and can be scaled with the total resources available to a proliferant State for military expenditures, which may be on the order of $2 billion per year for a reactor state or $20 billion per year for a fuel cycle state. Table 2.5 provides an index for scaling the value of PC from low (< 10%) to very high (> 100%). This measure expresses the economic and staffing investment required to overcome the multiple barriers that impede completion of the action associated with the segment.

The PC measure is aggregated over a pathway by summing the value of the measure for each segment in the pathway. In many cases, this measure will be dominated by one segment. Note that this measure does not include the cost of the declared Generation IV NES but does include the cost of modifications made to that system to complete the segment. These modifications may include process modifications as well as modifications intended to defeat safeguard verification activities. Table 2.7 summarizes key characteristics of the PC measure.

Table 2.7: Summary of Characteristics for the Proliferation Cost (PC) Measure

Characteristic	Description
Definition	Total cost of segment
Typical attributes to be considered for estimation	Minimum cost for setting up the minimum needed infrastructure to complete the segment Cost from misuse of civilian infrastructure/personnel
Example metric	Fraction of national resources for military capabilities
Segments-to-pathway aggregation method	Sum of segment estimates. Can be normalized to national resources for military capabilities.

Proliferation Time (PT) Measure

The PT measure is estimated in units of time, as shown in Table 2.5, and ranges from very low (< 3 months) to very high (> 30 years). The proliferation time is the minimum time required to overcome the multiple barriers that impede completion of the action associated with the acquisition and processing segments. Typically, PT is measured from the time that the proliferant State initiates its first detectable activity (e.g., its first action to divert material or misuse a declared facility). However, the analyst may select other initiation times, such as the time when the proliferant State's planning starts if the analyst judges this to be important in affecting the State's preferences between pathways. The analyst should state explicitly, the basis used for selecting an initiation time and use it consistently. Typically PT is estimated at the end of the processing segment and does not include the weapon fabrication time (which is subsumed in the MT measure). In practice, though, weapon fabrication time can be expected to be short (a few weeks) compared to the PT, so this distinction is not important.

For example, abrupt diversion of spent fuel from a storage facility might require less than 1 month. Extraction of plutonium from irradiated targets might require 3 to 12 months, assuming that the extraction facility (whether clandestine or obtained through misuse of a declared facility) is already available. In making these estimates, the analyst must clearly state assumptions. These assumptions include what preparations the proliferant State has completed before initiating the action associated with the segment (e.g., an assumption that the proliferant State constructed and commissioned a clandestine plutonium extraction facility before initiating this segment and assumed throughput).

For a pathway, the PT measure is aggregated by summing serial activities and taking into account parallel activities. Parallel and serial activities depend on the details of each pathway. Table 2.8 summarizes key characteristics of the PT measure.

Table 2.8: Summary of Characteristics for the Proliferation Time (PT) Measure

Characteristic	**Description**
Definition	Total time required to complete segment
Typical attributes to be considered for estimation	Maximum diversion or production rate Storage duration Extent of required equipment modifications
Example metric	Total time to complete pathway (e.g., months, years)
Segments-to-pathway aggregation method	Appropriate aggregation of parallel and serial activities

Fissile Material Type (MT) Measure

The MT measure ranks types of fissile material produced by the processing segment—typically metal—based on their utility for use in fabrication of a nuclear explosive and the relative preference of a proliferant State. As such, the MT measure is only estimated for pathways; it is not estimated for segments. It is, however, of interest to report MT at the end of major stages as defined in Section 2.2.4. For, example, as an intermediate result, a designer may want to know the various possible MTs emerging from the acquisition stage.

The specific design tradeoffs that arise from fissile material properties will affect several areas that would be important to the objectives of a proliferant State: technical performance (e.g., reliability of yield, both in achieving a successful first test and in achieving reliable performance after a sequence of tests), the ability to stockpile the material, and deliverability.

Because detailed information on the relationship between MT and weapons design is sensitive, the PR methodology applies an approximate ranking (Table 2.5) of nuclear material types. This ranking reflects relative PR based on the preferences of a proliferant State in attempting to acquire its first few weapons. The ranking ranges from material like high-enriched uranium (HEU), for which design and fabrication of nuclear explosives has very low difficulty (very low PR ranking), to low-enriched uranium (LEU), for which fabrication of a workable nuclear explosive is essentially impossible (very high PR ranking). The basic range is as follows:

- very low PR – HEU
- low PR – weapons-grade plutonium (WG-Pu)
- medium PR – reactor-grade plutonium (RG-Pu)
- high PR – “deep-burn” plutonium (DB-Pu)
- very high PR – LEU.

The very low PR ranking for HEU results primarily from the extremely low spontaneous neutron emission rate compared to all plutonium compositions. This difference substantially simplifies weapons design and gives a proliferant State high confidence in obtaining reliable performance on the first test or use of nuclear weapons.

For plutonium, a very wide range of isotopic compositions can be generated depending on the conditions of reactor operation and recycle of spent fuel. The basis for categorizing the attractiveness of different plutonium compositions is complex and, when presented in detail, is sensitive and classified. Here the MT PR ranking for plutonium compositions is based on the study of the U.S. National Research Council on the spent-fuel standard (National Research Council 2000):

> "If it is assumed that proliferators in all categories will ultimately be capable of obtaining reasonably pure plutonium metal…then the main intrinsic barriers in this category are those associated with deviation of the plutonium's isotopic composition from 'weapons grade.' …"
>
> "In the case of…a proliferant State we rate the barrier [from reactor-grade plutonium] as 'moderate' in importance: such a state would probably prefer to avoid if possible the burdens posed by isotopic deviations for design, fabrication, and maintenance of nuclear weapons, but it would also probably have the capabilities to cope with the burdens in ways that achieved a level of weapon performance adequate for the proliferant State's initial purposes."

When plutonium is recycled, it is possible to further degrade the isotopic composition. For the MT measure, such degraded plutonium is listed as DB-Pu, which would have high concentrations of Pu-238 and thus high heat generation rates. A proliferant State would be expected to expend great effort to identify proliferation pathways that would result in acquiring material with a lower MT PR ranking, and thus the MT PR ranking of DB-Pu is listed as high. Appendix D.4 provides a more detailed discussion regarding the level of preference that a proliferant State would display between materials of higher and lower MT ranking.

In many cases, the simple MT ranking, along with the qualitative discussion of MT provided above and in Appendix D.4, will be sufficient to allow pathways to be compared and ranked. Where this is not the case, additional expert guidance in nuclear weapons design and fabrication should be obtained. If expert guidance is not available, then the designer and analyst should apply appropriately conservative assumptions about the relative importance that a proliferant State would place on the MT measure. Table 2.9 summarizes key characteristics of the MT measure.

Table 2.9: Summary of Characteristics for the Fissile Material Type (MT) Measure

Characteristic	Description
Definition	Characteristics of metal for weapons fabrication
Typical attributes to be considered for estimation	Spontaneous neutron emission rate Heat generation rate Gamma radiation activity Bare-sphere critical mass
Example metric	Dimensionless ranked categories (HEU, WG-Pu, RG-Pu, DB-Pu, LEU); interpolation based on material attributes
Segments-to-pathway aggregation method	Not applicable

Detection Probability (DP) Measure

The DP measure expresses the probability that action described by a pathway segment is detected. DP results from measurements that (1) detect anomalies generated during the execution of pathway segments and (2) are performed to assess that anomalies originate from actions in actual pathway segments rather than legitimate, inadvertent sources. DP is generally expressed as a cumulative probability function. If a defined safeguards approach is not available, however, DP can only be expressed by a very wide uncertainty band.

In addition, a variety of concealment strategies may affect DP. The effects of a concealment strategy are determined by analyzing pathways that include the strategy, not by assigning an arbitrary DP uncertainty for assumed effects of concealment methods.

Safeguards involve continuously evolving technology. A number of system attributes can affect both the optimal approach for the application of safeguards and the effectiveness of that approach in providing high DP. Systematically considering these system attributes, as is done with “safeguardability” assessment (Appendix D.1), can guide designers in selecting design options that facilitate the application of effective safeguards and identifying an optimal combination of safeguard methods to provide high DP.

To detect *internal material diversion segments*, measurements may be combined to detect the material transfer and the resulting change in material inventory. Uncertainty in detection arises from three sources: (1) instrument measurement uncertainty; (2) the possibility that a measured anomaly has a legitimate origin, such as inadvertent hold up of material, inadvertent operator destruction of a seal, or inadvertent delay of an inspection due to legitimate safety or access restrictions; and (3) uncertainty that the actual facility configuration is the same as that assumed in the design of the safeguards system, where, for example, an undeclared penetration may exist in or be added to a facility.

To detect *internal facility misuse segments*, measurements to detect misuse must be tailored to detect anomalies that the action of a segment would generate. Uncertainties in detection of misuse have similar origins to those listed above for internal material diversion segments.

To detect *external segments*, methods include the use of tools such as commercial satellite photography and environmental sampling, as well as the use of various types of information that may be supplied by third party sources, such as information from national export control programs, which monitor and detect purchases or transfers of sensitive or dual purpose equipment and technologies, and information gathered by national technical means.[10] External segments that use equipment diverted from declared facilities, such as frequency invertors in enrichment plants, could also be detected by monitoring the inventory of this equipment in declared facilities. Although the IAEA does not currently have goals for detection of clandestine activities and facilities, the IAEA utilizes information obtained from a variety of sources, including non-safeguards databases, open sources and third parties.

Under modern integrated safeguards, safeguards detection resources such as the frequency of inspections are increased progressively as anomalies are detected. This provides a higher cumulative confidence of detection with lower detection resources. Likewise, safeguards approaches that provide multiple and diverse measurements capable of detecting the actions described by a pathway segment increase the DP.

For internal pathway segments, the reference metric scale for the DP measure, shown in Table 2.5, is based on a comparison with the applicable IAEA safeguards detection goals contained in the IAEA safeguards criteria. A “medium” DP meets the IAEA safeguards detection goals for spent fuel and irradiated materials. A “high” DP meets IAEA goals for HEU and separated plutonium, and a “low” DP meets IAEA goals for depleted uranium, natural uranium, and LEU.

For external pathway segments, DP may have large uncertainty unless the segment generates obvious visual, thermal, or other signatures. If detection uncertainty is large, it may be useful to provide decision makers with a qualitative, general description of the methods available to detect the external segment, particularly if the actual DP cannot be readily evaluated and presented on a metric scale like that of Table 2.5. Table 2.10 summarizes key characteristics of the DP measure.

Detection Resource Efficiency (DE) Measure

The DE measure is estimated for each pathway segment by summing estimates of the manpower (e.g., Person Days of Inspection, PDI) or the cost (in $) required to implement the detection methods for the segment. Safeguards resources are then aggregated for all segments of a pathway, using logical assumptions (e.g., a single instrument may provide detection capabilities for multiple segments). Estimates of time or cost will necessarily be based on currently accepted safeguards approaches but anticipated changes to safeguards approaches and safeguards technology (e.g., increased use of remote monitoring) should be considered that could occur over the multi-decade life cycle for most nuclear facilities The DE measure is normalized by a variable such as the energy production supported by the system element, and is presented as the ratio of that

---

[10] Although the IAEA doesn't have direct access to national technical means, Article VIIIa of the IAEA Statute states that "*Each member should make available such information as would, in the judgement of the member, be helpful to the Agency*".

normalization variable divided by the inspection time or cost (for example, in units of gigawatt years per PDI). Table 2.11 summarizes key characteristics of the DE measure.

Table 2.10: Summary of Characteristics for the Detection Probability (DP) Measure

Characteristic	Description
Definition	Cumulative probability and confidence level for detection of a pathway segment
Typical attributes to be considered for estimation	Attributes important to design information verification Transparency of layout Possibility to use 3-d scenario reconstruction models Possibility to have visual access to equipment while operational Comprehensiveness of facility documentation and data Attributes important to nuclear material accounting Uniqueness of material signature Hardness of radiation signature Possibility of applying passive measurement methods Item/bulk Throughput rate Batch/continuous process Nuclear material heat generation rate Attributes important to containment and surveillance Operational practice Extent of automation Standardization of items in transfer Possibility to apply visual monitoring Number of possible transfer routes for items in transit
Example metric	Cumulative detection probability.
Segments-to-pathway aggregation method	Calculate the probability of pathway detection on the basis of the segments involved. (e.g. the probability of pathway detection will be $P(d) = 1 - P(nd)$, where the probability of pathway non-detection, $P(nd) = \Pi(1-P_i(d))$, with $P_i(d)$ being the probability of detection of the i^{th} segment, under the hypothesis of the independence of detection events).

Table 2.11: Summary of Characteristics for the Detection Resource Efficiency (DE) Measure

Characteristic	Description
Definition	Total inspector time or cost of safeguarding the segment
Typical attributes to be considered for estimation	See Table 2.10
Example metric	GW(e) years of capacity supported (or other normalization variable) per Person Days of Inspection (PDI) (or inspection $)
Segments-to-pathway aggregation method	Aggregation to total inspection time or safeguards cost, normalized to an appropriate scale, such as nuclear energy production supported [GW(e) year]

2.2.5.2 PP Measures

The design of PPS generally follows a tailored systems engineering process (Garcia 2001, IAEA 2002b, U.S. Army 2001). The three PP measures—probability of adversary success (PAS), consequences (C), and physical protection resources (PPR)—provide a basis for sorting and comparing pathways. These three measures allow assessment of the pathway risk (the product of the probability of adversary success multiplied by the consequences). Investments to reduce this risk can then be evaluated using the PPR measure. Risks and investment needs can also be compared broadly across critical infrastructure and key assets, allowing optimal investments to identify and reduce the largest sources of vulnerability.

At the level of scenario analysis, detailed information is generally required about the effectiveness and delay provided by different types of barriers against various adversary capabilities, methods for disabling equipment and handling materials, the detailed design of detection and alarm systems, and the strategies of PP forces. All of this information is sensitive, and thus, in general, *scenario and two-sided analysis of PP pathways must be performed by organizations possessing the ability to manage sensitive information.* These organizations—national regulatory authorities, national laboratories, military organizations, and some commercial organizations—typically possess substantial expertise and specialized analytical and computational tools for performing scenario-based and two-sided analyses. In general, it is valuable and important to involve security specialists in concept and facility design at an early stage. For Generation IV PP evaluations, when scenario analysis is performed an organization with these specialized capabilities must be commissioned to provide analytical support. Feedback between this organization and system designers can provide an important additional contribution to improving the overall PP performance of facilities and systems.

The evaluation of PP measures shares many general features with the evaluation of PR measures. In some cases, coarse pathway analysis descriptions can be used to express the value of these measures for each pathway. The aggregation of measures for multiple pathway segments is also similar to PR.

The three measures for PP evaluations are as follows:

Probability of Adversary Success (PAS). This measure assesses the probability that an adversary will successfully complete the actions described by a pathway and generate a consequence. If the actions required to complete the pathway are within the resources and capability of the adversary, then the probability of adversary success depends on the capability of the PPS to detect the actions, delay the adversary, and neutralize the adversary before the actions can be completed. The PAS measure is commonly used in the design and analysis of PPSs, and various tools are available to quantitatively evaluate the measure. For some pathways, the PAS may be controlled by a small number of segments, such as the physical difficulty in obtaining access to safety equipment in attempting to sabotage passively safe nuclear reactors and the difficulty of removing and processing spent-fuel assemblies in attempting to steal plutonium.

Consequences (C). Consequences are defined as the effects resulting from the successful completion of the adversary's intended action described by a pathway. This measure reflects both the attractiveness to the adversary and the relative importance of a pathway in generating adverse effects. Theft consequences can be expressed in terms of the quantity and quality of the material removed. Appendix D.4 discusses fissile material quality of materials for nuclear explosives, in relationship to sub-national threats. Sabotage consequences can be measured by the number of physical quantities, acute fatalities, latent fatalities, quantities of material per unit area, etc. Perhaps the most meaningful measurement of sabotage consequences at the coarse pathway level is whether a release is contained, kept to the plant site, or released offsite.

Physical Protection Resources (PPR). This measure reflects the resources devoted to provide extrinsic features—a PPS—to detect, delay, and neutralize an adversary. At the lowest end, in system elements that provide very long intrinsic delay times, this measure may involve the cost of alarm systems and offsite police response. At the high end, this measure may involve extensive investments in maintaining large, armed security forces and in detection, delay, and response systems. The PPR measure quantifies the staff, capabilities, and costs (both infrastructure and operation) required to provide a level of PP for a given NES. As with the DE measure for PR, the PPR measure for a given pathway is evaluated for each pathway segment and then aggregated appropriately, noting that some PPS elements can provide responses to multiple segments. PPR for targets can be evaluated by aggregating resources for all pathways associated with the target. Likewise PPR for a system element can be evaluated by aggregating the resources required for all targets in the system element. The PPR measure can also be expressed as a cost per unit of energy (TWh) produced.

The three measures for PP are consistent with those commonly used by national programs to make efficient investments to protect critical infrastructure and key assets. PP is a national responsibility and thus involves national policies. The goal is to optimally allocate resources to limit risk to a uniform level across both nuclear and non-nuclear critical infrastructure and key assets. Quantitative analysis for PAS, C, and PPR will also be required to support licensing and deployment decisions for new nuclear infrastructure.

In decision making at a national level, lower-probability, high-consequence events may be given more weight than higher-probability, low-consequence events. Also, synergistic investments may be more efficient. For example, investments making it more difficult to hijack aircraft reduce the probability of success for attacks against both nuclear and non-nuclear key assets. Investments in emergency response provide capabilities to respond to multiple types of terrorist attacks and natural disasters.

For the design of new NESs, such as those envisioned in the Generation IV program, the goals are to

- Reduce resources (PPR) required to limit risk (PAS x C) for a complete NES for a spectrum of threats
- Focus design attention on sources of highest risk (greatest vulnerability) in a system
- Increase transparency of PP system effectiveness to increase confidence of all stakeholders and increase deterrence of adversaries.

During conceptual and detailed design, the primary objective is the identification and selection between design options that affect the relative resources required to achieve a given level of risk.

Analysis of individual pathway segments can be used to estimate measures for each pathway segment. The individual measures can then be aggregated for the entire pathway. This approach requires a well-defined metric for each measure so that judgment and the effect of assumptions can be identified. Metrics are estimated at the segment level even at the conceptual design stage, where it is easier to identify the sources of uncertainty through the refinement of pathway segments because sources of uncertainty can be more easily characterized at the segment level. It may also be easier at the segment level to specify assumptions and identify intrinsic features that are useful to the designer.

Tools such as Estimate of Adversary Sequence Interruption (EASI) can be used as a quantitative method to evaluate the effectiveness of PPR investments for each segment and the PPS in whole against the adversary's pathway. These tools are discussed in Appendix B.

2.3 Outcomes

The goal of PR&PP assessment is, by comparing pathways, to identify those that a proliferant State or adversary might most likely pursue and to provide a basis for decision makers to prioritize investments in safeguards and PP resources.

The process of pathway comparison is ultimately a process of decision analysis. The PR&PP methodology therefore adopts a cautious but reasonable approach to pathway comparison. Caution is required to avoid embedding significant assumptions about the preferences of a proliferant State or adversary into the system evaluation, unless these preferences are provided explicitly in the threat definition. For example, the analyst should not assume how strong a proliferant State's desire would be to avoid detection by safeguards, unless this preference is specified in the threat definition. Thus, the analyst cannot normally assume the relative weight a State would place on the DP measure. However, the methodology is sufficiently rich to allow such input when quantified.

Pathways can be compared to identify representative and dominant pathways and to explore the sensitivity of pathway outcomes to various system design parameters. This comparison process is important to gain insights from pathway evaluations and ultimately to identify a set of representative pathway outcomes that can be used in the summary of the study results. Thus, similar tools are used for pathway comparison and for the presentation of study results. A detailed PR&PP study may involve the comparison of very large numbers of pathway outcomes, while the presentation of results will typically focus on a summary of dominant pathways or the sensitivity of pathway outcomes to various system design parameters.

2.3.1 Pathway Comparison

The PR&PP methodology does not use weighting functions to aggregate pathway measures. While aggregating to a single outcome value might appear to facilitate the comparison of pathway outcomes, the use of simplified weighting functions requires very strong and potentially inaccurate assumptions about the preferences of proliferant States and adversaries. Instead, the PR&PP methodology uses pair-wise and group comparisons (Denning et al. 2002, NPAM 2003) of pathway outcomes to characterize and, where appropriate, rank pathways. This allows those pathways that lie on the *efficient frontier* to be identified, consisting of the set of pathways that remain after unambiguously inferior pathways are rejected.

Measure values can be presented in two basic ways: by binned metric values (e.g., the VL-L-M-H-VH bins) or by the metric values on a continuous scale ranging from 0 to 1. In the second case, the qualitative descriptors are assigned the metric values: VL = 0-0.2, L = 0.2-0.4, M = 0.4-0.6, H = 0.6-0.8, and VH = 0.8-1.0. For qualitative analysis based on expert judgment, binned values can be the most practical because uncertainty is expressed by regarding the value to be equally likely within the range of the given bin or multiple bins. For quantitative methods, results are generated from point estimates first and then sensitivity studies and uncertainty analyses are performed over continuous scales. Table 2.5 provides suggested metrics and scales, however it is emphasized that the methodology does not prescribe specific metrics and instead permits analysts to select metrics appropriate to the specific threat and decision problem.

Because the multiple measures provide a multi-dimensional result, analysts should use convenient and suggestive display mechanisms to aid pathway comparisons and present study results. Tabular displays can present numerical results directly. Graphic displays (e.g., bar charts or spider and wind rose graphs) can also be helpful, particularly if they capture the overall result. Graphical and tabular displays can be used to compare and report the following types of information:

- Representative or dominant pathways/scenarios for a given threat and system element
- The relative ranking of each pathway/scenario
- Estimates of pathway/scenario consequences in terms of acquisition, processing, and fabrication; or sabotage, theft, damage to property, number of injuries or fatalities, and dollar loss

- Factors affecting each pathway and associated measures (often a qualitative description)
- Measures of relative importance
- Uncertainties associated with various estimates
- Technical knowledge gaps responsible for significant uncertainties in pathway endpoints and measure values.

Table 2.12 provides a simple example comparing four different pathway outcomes for PR. Cell entries can include qualitative descriptive information, probability distributions, statistics of distributions, or a combination of these. This type of table allows a program policy maker, external stakeholder, or a system designer to compare a number of options.

Figure 2.3 presents the same measures as Table 2.12 in the form of a bar chart. The bar chart format provides a convenient method to present uncertainty information. Table 2.13 provides a similar example for PP. The presentation of information is quite simple, and more complex presentations can readily be envisioned. Alternate graphical presentation methods, such as spider graphs and wind rose diagrams, are available and can be employed. Likewise, for the results of specific measures, specialized presentation methods may be valuable.

Table 2.12: Comparison of PR Pathway Measures Using Binned Values
(Numerical values from a continuous metric scale may also be used.)

Pathway	Proliferation Technical Difficulty	Proliferation Cost	Proliferation Time	Fissile Material Type	Detection Probability	Detection Resource Efficiency
Pathway # 1:	L	VL	VL	VL	VL	L
Pathway # 2:	L	VL	L	VL	VL-L	L
Pathway # 3:	VL	L	H-VH	M	MH	L-H
Pathway # 4:	VL	L	L-M	L-M	H-VH	M-H

NOTES: L = low; V = very; M = medium; H = high.

The PR&PP methodology does not prescribe a specific presentation method, leaving these decisions to the analysts and study peer reviewers. Tools to compare pathways and present results will likely evolve over time, and thus analysts are encouraged to review the methods used in previous studies.

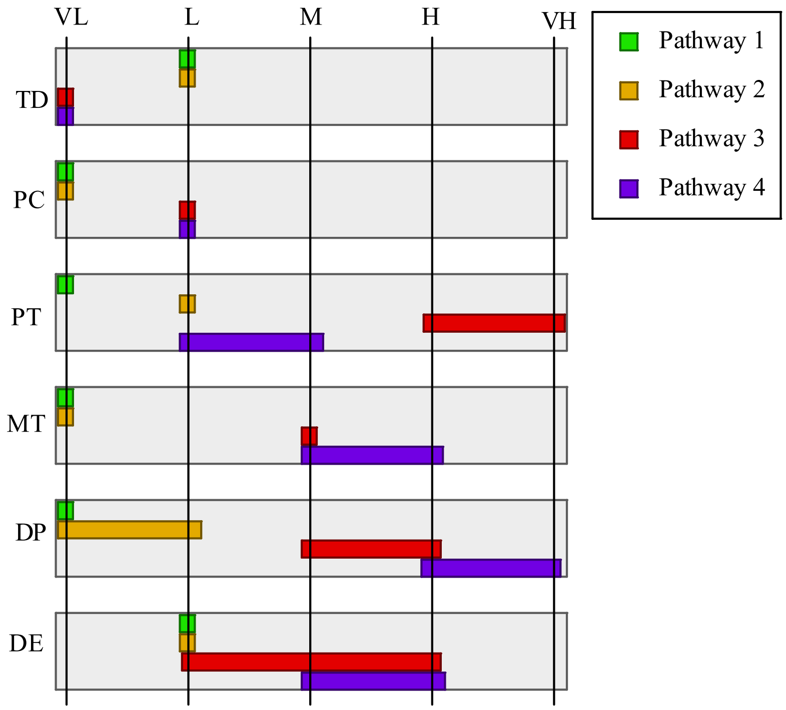

Figure 2.3: Comparison of Binned Measure Values for Four Pathways Using Data From Table 2.12

Table 2.13: Comparison of PP Pathway Measures Using Binned Values (Numerical values from a continuous metric scale may also be used.)

Pathway	**Probability of Adversary Success**	**Consequences**	**Physical Protection Resources**
Pathway #1:	M	H	M
Pathway # 2:	L	M	H
Pathway # 3:	M	L	H
Pathway # 4:	L	L	VH

NOTES: L = low; V = very; M = medium; H = high.

2.3.2 System Assessment and Presentation of Results

System assessment uses the results of pathway comparison to provide insight and reach conclusions about PR and PP. The presentation of system assessment results is central to the effective use of information generated by a PR&PP evaluation and must support decision making by three basic types of users:

1. System designers
2. Policy makers
3. External stakeholders.

System designers are likely to be more interested in identifying specific design options that improve their system response to PR&PP threats, commonly at the facility, target, and the pathway-segment levels, so that they can factor the assessment results into the design process. Policy makers are likely to be more interested in high-level measures for dominant pathways in a system. The level of detail and the form in which the results are presented should be defined when planning the assessment and must be suited to the needs of the assessment user.

The assessment of the system response should be presented with different levels of detail, depending on the purpose of the evaluation. Intermediate results will be useful in gaining insight into the contributors to the final results. For example, analysts may want to know how material acquisition affects processing as the two aspects contribute to overall PR. The presentation must maintain a transparent relationship between the detailed results compiled for system designers and the high-level measures representing the outcomes for policy users.

Results will also be calculated and presented in different forms through the approach discussed in Section 2.2. At early stages, the methodology provides qualitative and quantitative outcomes based heavily on expert judgment. The methodology then progresses toward more quantitative results as the design matures and the analysis becomes more detailed. The results, while different in the level of their quantification, should be presented in a consistent format to facilitate understanding.

Of paramount importance to the expression of the results is the role of uncertainty. Both lack of knowledge and inherent randomness of processes/events should be incorporated into the expression of uncertainty. Lack of knowledge may relate to design information, procedures, and policies (imprecisely known) or to physical behavior. (Inherent randomness refers to stochastic events.) Evaluation results should include best estimates for numerical and linguistic descriptors that characterize the results, distributions reflecting the uncertainty associated with those estimates, and appropriate displays to communicate uncertainties.

Assessments may involve PR&PP robustness for multiple threats and multiple facilities or options. The many dimensions of the results must be captured and summarized as a manageable set while preserving all critical information necessary for the end user. As part of the ability to use and interpret the results and performing peer reviews, it is important that well-defined terminology be used in the reporting of results.

Remember that the results are conditional on the specific threats studied. Frequencies have not been assigned to the possible threats in this methodology, nor does it prescribe a weighting system to be used to combine contributors to the high-level measures. Thus, in all cases, final results are presented on a per threat basis. Therefore, analysts cannot aggregate end results over pathways resulting from different threats. Likelihoods could be denoted for the threats, but their actual probabilistic quantification falls outside the scope of this methodology.

For some end users, particular measures may overshadow others in decision making. A focus on a subset of measures can simplify the comparison of pathways and limit information-overload for the user. Hence, the users of the PR&PP methodology may select a subset of the parameters or measures of interest for specific decisions. However, even if only one or two threats are of interest to the end user, the outcomes should still be expressed in terms of the six measures for PR and the three measures for PP.

The results must be reported in a credible manner and carefully checked for accuracy. To provide focus for the assessment, the results should include identification of system and institutional features that are the most significant contributors to PR and PP robustness. Insights into relative importance of various features of the systems and institutions, and the relative importance of various modeling assumptions, may be developed from uncertainty and sensitivity analyses. A discussion of these insights is needed to provide the proper interpretation of the conclusions presented in the tables or figures. These insights should include an appreciation of the overall degree of uncertainty in the results and an understanding of their magnitude and effect. The level of detail and the style of presentation of results depend on the assessment objectives. Besides the quantitative discussion, a qualitative description is often needed. The results section should also communicate the assessment's motivations and objectives in a way that shows how the results meet those objectives.

2.3.2.1 Credibility

One section of the results should highlight the key characteristics of the PR&PP evaluation that make the results credible. Types of information that should be presented include the following:

- Clear definition of the scope and objective of the analysis
- Definition of the boundary conditions
- Insights into how various systems/institutions interact with one another
- Insights into the relationship between mode of facility operation and scenarios
- Results of activities undertaken to ensure completeness of the pathways
- Clear and concise tabulation of all known limitations and constraints associated with the analysis
- Clear and concise tabulation of all assumptions used in the assessment, especially with respect to success criteria and selection of certain pathways
- Key parameters that greatly influence the numerical results of the assessment

- Activities undertaken (e.g., sensitivity analyses) to ensure that the results would not be negated if an alternative parameter value or modeling assumption were to be employed
- Activities undertaken to ensure technical quality.

2.3.2.2 Accuracy

It is also important to check the results for accuracy. This checking ensures that the assessment provides a technically reasonable representation of the Generation IV NES being evaluated. Assume that the assessment will undergo independent review. Sufficient material should be provided within the report or appendices and reference citations that would allow the independent reviewer to reproduce results. Similarly, intermediate and low-level results should be provided to allow the policy maker to trace the underlying foundations of high-level results. The numerical results need only be accurate enough to allow the decision maker to distinguish significant contributors.

2.3.2.3 Significant Pathways

Each significant pathway should be described. If there is no single most significant pathway, then the set of pathways on the efficient frontier should be displayed. Selected inferior pathways that are not on the efficient frontier may also be displayed because they provide insight to potential vulnerabilities. Pathways that lie away from the efficient frontier may also be presented to illustrate design features that can reduce system vulnerabilities. The narrative should discuss the nature of the threat space and system failures, such as breached barriers. For PR, the information should also mention the point at which material is acquired and whether it was done covertly or overtly. The major events occurring in each pathway should be described.

Because the methodology does not aggregate results across threats, the top-level results should be regarded on a per threat basis. Even for a given threat, if there are multiple pathways, the end user may want to regard them as equally likely (absent further information on the proliferant State’s strategy). A separate pathway list (in tabular or graphical format) could be created for each threat and used to compare a range of options against each threat.

2.3.2.4 Uncertainty

The degree of uncertainty about the results of the analysis must be communicated clearly. During initial assessment, rough order-of-magnitude uncertainty should be estimated where possible. The NPAM Report (2003) explores a number of approaches to the display of uncertainty in results. The manner in which the uncertainty is displayed may depend on the type of uncertainty analysis. In a very detailed uncertainty analysis using Monte Carlo techniques, it may be possible to display the 5th percentile, 95th percentile, mean, and median of a distribution. More typically, a range of uncertainty is displayed qualitatively without a rigorous interpretation of its meaning. The semantics, however, should be clear.

PR&PP assessments are affected by several sources of uncertainty. Assumptions should be stated as qualitative descriptors for the initial attempts at uncertainty characterization. Uncertainties for threat descriptions, system characteristics and institutional factors that are contributors to the pathways must also be stated and displayed. Where alternate pathways emerge, the uncertainties associated with these should be noted. Appendix E provides a more detailed discussion of uncertainty.

2.3.2.5 Sensitivity Analyses

The final results of the analysis must be presented in a way that allows an understanding of the sensitivity of analysis assumptions. For example, in characterizing the threat space for PP, a given sabotage threat may be assumed to have a specified objective. It may be interesting to know the impact on the results if the objective were different. Thus, the least resistant pathways for a given country and energy system should be displayed. Similar concepts apply to PR analysis.

Other sensitivity results could also be generated, depending on the interest of the end user. In preparing the results, the analyst should take care to clearly state the given conditions of each sensitivity analysis and parameter that is being varied. Assumptions, data, and models that do not impact the final results significantly must also be investigated and reported.

2.3.2.6 Qualitative Discussion of Results: Insights and Conclusions

In addition to the technical (quantitative) presentation of the results of the assessment, there must be a clear discussion of the main conclusions of the effort. The analysts should state the four or five main, high-level results of the assessment, putting such information in perspective with other results, studies, and anticipated trends. New insights should especially be noted. The type of information needed to reduce uncertainty should also be discussed. Finally, the results should be discussed in terms of the PR&PP goals for Generation IV NESs.

3 SUMMARY AND CONCLUSIONS

The PR&PP methodology provides a framework to answer a wide variety of security-related questions for NESs and to optimize these systems to enhance their ability to withstand the threats of proliferation, theft, and sabotage. The PR&PP methodology provides the tools to assess NESs with respect to the security-related goals for Generation IV technologies to be "*a very unattractive and the least desirable route for diversion or theft of weapons-usable materials, and provide increased physical protection against acts of terrorism."*

PR&PP analysis is intended to be performed, at least at a qualitative level, from the earliest stages of system design, at the level where initial flow diagrams and physical arrangement drawings are developed, and simultaneously with initial hazards identification and safety analysis. The methodology facilitates the early consideration of security and safety because the structure of the PR&PP methodology bears strong similarity to safety analysis.

The PR&PP methodology adopts the structure of systematically identifying the security challenges a system may face, evaluating the system response to these challenges, and comparing outcomes. The outcomes are expressed in terms of measures, which reflect the primary information that a proliferant State or an adversary would consider in selecting strategies and pathways to achieve their objectives. By understanding those features of a facility or system that could provide more attractive pathways, the designer can introduce barriers that systematically make these pathways less attractive. When this reduction may not be possible, for example in reducing the attractiveness of the proliferation pathways provided by uranium enrichment, the analyst can highlight where special institutional measures such as assured fuel supply and return regimes may be required to provide appropriate levels of security.

Beyond requiring that a systematic process be used to identify threats, analyze the system response, and compare the resulting outcomes, the PR&PP methodology provides a high degree of flexibility to the analyst, subject to the requirement that the results of studies receive appropriate peer review. For this reason, it is anticipated that approaches to performing PR&PP evaluations will evolve over time, as the literature and examples of PR&PP assessments expand. Different tools for identifying targets, assessing system response and uncertainty, comparing pathway outcomes, and presenting results can be expected to increase in number, as will the range of questions that can be answered and insights gained from PR&PP studies.

(This page has been intentionally left blank.)

4 REFERENCES

Ahmed, S., and A.A. Husseiny. 1982. "Risk Assessment of Alternative Proliferation Routes." *Nuclear Technology* 56:507

Baron, P., C. Brown, B. Kaiser, B. Matthews, T. Mukaiyama, R. Omberg, L. Peddicord, M. Salvatores, and A. Waltar. 2004. *An Evaluation of the Proliferation Resistant Characteristics of Light Water Reactor Fuel with the Potential for Recycle in the United States*, A. Waltar and R. Omberg, eds.
Available at: http://www.ne.doe.gov/nerac/BlueRibbonCommFinRprtNov2004.pdf.

Blankenship, J. 2002. "International Standard for Design Basis Threat (DBT)." International Conference on Physical Protection, Strengthening Practices for Protecting Nuclear Material, Salzburg, Austria, Sept 8-13, 2002.

Budnitz, R.J., G. Apostolakis, D.M. Boore, L.S. Cluff, K.J. Coppersmith, C.A. Cornell, and P.A. Morris. 1998. "Use of Technical Expert Panels: Applications to Probabilistic Seismic Hazard Analysis." *Risk Analysis* 18(4):463-9.

Cojazzi, G.G.M., and G. Renda. 2004. *Safeguards Assessment Methodologies: Review and Perspectives from a Systems Analysis Point of View*. EUR 21307, Joint Research Center of the European Commission, Brussels.

Cojazzi, G.G.M., and G. Renda. 2005. "Proliferation Resistance Characteristics for Civilian Nuclear Fuel Cycles Assessments." 27th ESARDA Annual Meeting Symposium on Safeguards and Nuclear Material Management, London, May 10-12, 2005.

Cojazzi, G.G.M., G. Renda, and S. Contini. 2004. "Qualitative and Quantitative Analysis of Safeguards Logic Trees." In *Probabilistic Safety Assessment and Management 2004*, C. Spitzer, U. Schmocker, and V.N. Dang, eds., pp. 1083. Springer, Cambridge, Massachusetts.

Cojazzi, G.G.M., D. Fogli, G. Grassini, P. De Gelder, D. Gryffroy, R. Bolado, E. Hofer, R. Virolanen, I.M. Coe, A. Bassanelli, A.I Puga, I. Papazoglou, O. Zuchuat, E. Cazzoli, J. Eyink, G. Guida, L. Pinola, U. Pulkkinen, K. Simola, D. Von Winterfeldt, and A. Valeri. 2001. "Benchmark Exercise on Expert Judgment Techniques in PSA Level 2." *Nuclear Engineering & Design* 209:211-221.

R. Denning, R., et al. 2002. "Guidelines for the Performance of Nonproliferation Assessments." *Transactions of the American Nuclear Society* 87:365-366.

DOE (U.S. Department of Energy), Nuclear Energy Research Advisory Committee and the Generation IV International Forum. December 2002a. *A Technology Roadmap for Generation IV Nuclear Energy Systems.* GIF002-00, DOE Nuclear Energy Research Advisory Committee and the Generation IV International Forum, Washington, D.C.

DOE (U.S. Department of Energy), Nuclear Energy Research Advisory Committee and the Generation IV International Forum. December 2002b. *Generation IV Roadmap: Viability and Performance Evaluation Methodology Report.* GIF002-13, DOE Nuclear Energy Research Advisory Committee and the Generation IV International Forum, Washington, D.C.

DOE (U.S. Department of Energy), Manual DOE M 470.4-6, *Nuclear Material Control and Accountability*, Approved August 26, 2005.

Forester, J., D. Bley, S. Cooper, E. Lois, N. Siu, A. Kolaczkowski, and J. Wreathall. 2004. “Expert Elicitation Approach for Performing ATHEANA Quantification.” *Reliability Engineering and System Safety* 83:207-220.

Garcia, M.L. 2001. *The Design and Evaluation of Physical Protection Systems*. Butterworth-Heinemann, Boston.

Garrick, B.J, J.E. Hall, M. Kilger, J.C. McDonald, T. O’Toole, P.S. Probst, E.R. Parker, R. Rosenthal, A.W. Trivelpiece, L.A. Van Arsdale, and E.L. Zebroski. 2004. "Confronting the Risks of Terrorism: Making the Right Decisions." *Reliability Engineering & System Safety* 86(2):119-176.

Heising, C.D. 1979. *A Comparative Assessment of the LMFBR and Advanced Converter Fuel Cycles with Quantification of Relative Diversion Resistance*. Final Report, MIT-NE-238, Massachusetts Institute of Technology Energy Laboratory, Boston.

Hill, J. 1998. *Logic Trees and Integrated Safeguards*. ASAP-9802, Australian Safeguards and Non-Proliferation Office, Barton, Australia.

Hinton, J.P., et al. 1996. *Proliferation Vulnerability Red Team Report*. SAND97-8203, Sandia National Laboratories, Albuquerque, New Mexico.

IAEA (International Atomic Energy Agency). 1970. *Treaty on the Non-Proliferation of Nuclear Weapons*, INFCIRC/140, IAEA, Vienna.

IAEA (International Atomic Energy Agency). 1972. *The Structure and Content of Agreements Between the Agency and States Required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons*, INFCIRC/153 (Corrected), IAEA, Vienna.

IAEA (International Atomic Energy Agency). 1980. *The Convention on the Physical Protection of Nuclear Material*, INFCIRC/274/Rev.1, IAEA, Vienna.

IAEA (International Atomic Energy Agency). 1998. *Model Protocol Additional to the Agreement(s) between State(s) and the International Atomic Energy Agency for the Application of Safeguards*, INFCIRC/540 (Corrected), IAEA, Vienna.

IAEA (International Atomic Energy Agency). 1999. *The Physical Protection of Nuclear Materials and Nuclear Facilities*. IAEA-INFCIRC/225/Rev. 4 (Corrected), IAEA, Vienna.

IAEA (International Atomic Energy Agency). 2002a. *Handbook on the Physical Protection of Nuclear Materials and Facilities.* IAEA-TECDOC-1276, IAEA, Vienna.

IAEA (International Atomic Energy Agency). 2002b. *Proliferation Resistance Fundamentals for Future Nuclear Energy Systems.* IAEA Department of Safeguards, IAEA, Vienna.

IAEA (International Atomic Energy Agency). 2002c. *IAEA Safeguards Glossary*, *2001 Edition*, International Nuclear Verification Series n. 3, IAEA, Vienna.

IAEA (International Atomic Energy Agency). 2003. *Country Nuclear Power Profiles* Web site. Available at:
http://www-pub.iaea.org/MTCD/publications/PDF/cnpp2003/CNPP_Webpage/pages/countryprofiles.htm

IAEA (International Atomic Energy Agency). 2004. *Methodology for the Assessment of innovative nuclear reactors and fuel cycles*, IAEA-TECDOC-1434, IAEA, Vienna.

INFCE (International Nuclear Fuel Cycle Examination). 1980. *Report of the First Plenary Conference of the International Nuclear Fuel Cycle Examination (INFCE)*. International Atomic Energy Agency, Vienna.

Ko, W.I., et al. 2000. “Electrical Circuit Model for Quantifying the Proliferation Resistance of Nuclear Fuel Cycles.” *Annals of Nuclear Energy* 27:1399.

Krakowski, R.A. 1999. *A Multi-attribute Utility Approach to Generating Proliferation Risk Metrics*. LA-UR-96-3620, Los Alamos National Laboratory, Los Alamos New Mexico.

Krakowski, R.A. 2001. "Review of Approaches for Quantitative Assessment of the Risks of and Resistance to Nuclear Proliferation from the Civilian Nuclear Fuel Cycle." LA-UR-01-169, Los Alamos National Laboratory, Los Alamos, New Mexico.

NAS (National Academy of Sciences), Committee on International Security and Arms Control, Panel on Reactor-Related Options. 1995. *Management and Disposition of Excess Plutonium: Reactor-Related Options.* National Academy Press, Washington, D.C.

NASAP (Nonproliferation Alternative Systems Assessment Program). 1980. *Nuclear Proliferation and Civilian Nuclear Power*, Report of the Nonproliferation Alternative Systems Assessment Program, Vols. I-IX. U.S. Department of Energy, Washington, D.C.

National Research Council, Office of International Affairs. 2000. *The Spent-Fuel Standard for Disposition of Excess Weapon Plutonium: Application to Current DOE Options*. National Academy Press, Washington, D.C. Available online at http://www.nap.edu/books/0309073200/html/

NPAM (Nonproliferation Assessment Methodology) Working Group, National Nuclear Security Administration (NA-241). 2003. *Guidelines for the Performance of Nonproliferation Assessments.* PNNL-14294, Pacific Northwest National Laboratory, Richland, Washington.

Office of Technology Assessment. 1977. *Nuclear Proliferation and Safeguards*. OTA-E-48, Office of Technology Assessment, Washington, D.C.

Papazoglou, I.A., E.P. Gyftopoulos, N.C. Rasmussen, M.M. Miller, and H. Raiffa. 1978. *A Methodology for the Assessment of the Proliferation Resistance of Nuclear Power Systems*. MIT-EL-78-021, Massachusetts Institute of Technology Energy Laboratory, Boston.

Pilat, J.F., K. Budlong-Sylvester, and W. Stanbro. 2002. *Expert Elicitation and the Problem of Detecting Undeclared Activities: A Report on Three Illustrative Elicitations Undertaken in Support of The International Atomic Energy Agency*. LA-UR-02-6875, ISPO-492, Los Alamos National Laboratory, Los Alamos, New Mexico.

Silvennoinen, P., and J. Vira. 1981. "An Approach to Quantitative Assessment of Relative Proliferation Risks from Nuclear Fuel Cycles." *Journal of Operations Research* 32:457.

Siu, N.O., and D.L. Kelly. 1998. "Bayesian Parameter Estimation in Probabilistic Risk Assessment. *Reliability Engineering and System Safety* 62:89-116.

Taylor, J., et al. 2000. *The Technological Opportunities to Increase the Proliferation Resistance of Global Civilian Nuclear Power Systems*. Report by the Nuclear Energy Research Advisory Council of the U.S. Department of Energy, "TOPS" Task Force, Washington, D.C.

U.S. Government Printing Office via GPO Access, *Code of Federal Regulations*, 10 CFR 73 (2006). Title 10—Energy, Chapter I—Nuclear Regulatory Commission (continued), Part 73:_Physical Protection of Plants and Materials.

Wreathall, J., E. Roth, D. Bley, J. and Multer. 2003. *Human Reliability Analysis in Support of Risk Assessment for Positive Train Control*. Report No. DOT/FRA/ORD-03/15, U.S. Department of Transportation, Washington, D.C.

Yue, M., L. Cheng, I.A. Papazoglou, M.A. Azarm, and R. Bari. 2005. "Calculations of Proliferation Resistance for Generation III Nuclear Energy Systems." Global 2005, Japan, October 9-13 2005.

5 GLOSSARY

Acquisition	A high-level stage of a PR pathway, considering the set of activities carried out to acquire nuclear material in any form. Acquisition starts with the decision to acquire nuclear material and ends with the availability of nuclear material.
Actor	For PR, the actor is the Host State for the nuclear energy system. For PP, the actor (or adversary) is an individual or group composed of some combination of outsiders and/or insiders. The group might be backed by a non-Host State. Actors are further characterized by their objective (or objectives) and capabilities.
Adversary delay (PP)	The time required by the PP actor to overcome intrinsic barriers to accessing and disabling a vital equipment target set (sabotage) or to removing materials (theft).
Analysis	The consideration in detail to discover essential features or meaning; the break-down into components or essential features.
Assessment	The classification of something with respect to its worth; the act of judging or assessing a situation or event.
Barrier	A characteristic of a nuclear energy system that impedes proliferation (PR) or sabotage or theft of nuclear material/information (PP).
Capabilities	The elements the actor can draw on to carry out the necessary steps inherent in each pathway. For PR actors, capabilities are characterized in terms of general technical skills/knowledge, general resources, uranium resources, general industrial capabilities, and specific nuclear capabilities. For PP actors, capabilities are characterized in terms of knowledge, skills, weapons and tools, number of adversaries, and commitment and dedication.
Consequences (C)	A PP measure capturing the effects resulting from successful completion of the adversary's intended action described by a pathway.
Consequence generation	A PP pathway stage, considering the sequence of events following target exploitation that result in radiological release, damage, or disruption.
Design-Basis Threat	A bounding characterization of the possible challenges to the facility to aid design.
Detection Probability (DP)	A PR measure that expresses the cumulative probability of detecting the action described by a pathway or segment. At coarse analysis level, it is a performance objective rather than a measure to be estimated. IAEA (1998) defines detection Probability as: "The probability, if diversion of a given amount of nuclear material has occurred, that IAEA safeguards activities will lead to detection."
Detection Resource Efficiency (DE)	A PR measure capturing the staffing, equipment, and funding required to apply international safeguards to the nuclear energy system. Detection resource efficiency can be only qualitatively estimated at coarse analysis level but can be quantitatively estimated at a refined level on the basis of safeguards system design.

Efficient frontier	The set of different pathways that cannot be differentiated with respect to their attractiveness without value tradeoffs among high-level measures.
Equipment target set	Minimum set of equipment that must be disabled to successfully sabotage a facility or to gain access to a theft target.
Evaluation methodology	The overall process of examining a nuclear energy system or a system element to determine its PR and/or PP robustness.
Extrinsic (Institutional)	Extrinsic – Adjective relating to the actions undertaken to impede proliferation, sabotage or theft, by States or other Institutions. These actions may be institutional, legal or operational in nature. The noun ‘measures’ is popularly used in this context, e.g. ‘extrinsic measures’ to enhance proliferation resistance. Such use is not to be confused with the differing PR&PP use of ‘Measures’ as found in this report to mean bases or standards of comparison. Due to the different use of the term measures PR&PP talks of intrinsic and extrinsic *features*. Examples of extrinsic features to combat proliferation are international laws, treaties, protocols, import/export agreements, and the application of international safeguards and verification activities (including any safeguards measurement equipment employed). An example of extrinsic features for physical protection would be the deployment of a physical security force to protect nuclear material.
Fabrication	A high-level stage of a PR pathway considering the activities carried out to manufacture and assemble nuclear explosive devices. Fabrication starts with the availability of nuclear weapons material ready for use in a nuclear explosive device (e.g. plutonium in metallic form) resulting from the processing stage or from direct acquisition and ends with the availability of one or more nuclear explosive devices.
Facility	(i) A reactor, critical facility, conversion plant, enrichment plant, fabrication plant, reprocessing plant, isotope separation plant, or separate storage installation; or (ii) any location where nuclear material in amounts greater than one effective kilogram is customarily used (IAEA, 1998).
Fissile Material Type (MT)	A PR measure categorizing the material based on the degree to which its characteristics affect its utility for use in nuclear explosives. MT is estimated on metal material immediately prior to fabrication stage.
Generation IV nuclear energy system	A Generation IV Nuclear Power Producing Plant and the facilities necessary to implement its related fuel cycle.
Graded Safeguards	A domestic safeguards system designed to provide varying degrees of physical protection, accountability, and material control to different types, quantities, physical forms, and chemical and isotopic compositions of nuclear materials consistent with the risks associated with malevolent acts and varying levels of attractiveness and convenience to potential adversaries.

Intrinsic	Intrinsic – Adjective relating to the inherent properties or physical design features of a nuclear energy system or component. An intrinsic feature is likely very difficult or impossible to alter, is therefore very robust and desirable, and the term may be applied both to PR and to PP. Intrinsic proliferation resistance features impede proliferation, while intrinsic physical protection features deter sabotage or theft. The beneficial action of an intrinsic proliferation resistance property may be indirect, i.e. by enabling the application of a more cost-effective or robust extrinsic feature. An example of an intrinsic PR feature would be such a high heat rate so as to render a material unusable for a weapon. The placement of a facility completely underground would be an example of an intrinsic PP feature.
Measures	The few, high-level parameters that can be used to express PR or PP robustness. Use of this term must not be confused with another frequent use (e.g., safeguards measures) to indicate the set of extrinsic actions or procedures for material and facility control and protection.
Metric	A quantitative or qualitative scale and method that can be used to estimate the value of a system characteristic or measure.
Objectives	The desired end point for the actor (i.e., the goal to be achieved). For example, in proliferation evaluation the objective can be expressed in terms of a number of nuclear explosive devices with specified characteristics. For PR actors, objectives are limited to acquisition of nuclear weapons and further characterized in terms of number of nuclear weapons, reliability of nuclear weapons, the ability to stockpile nuclear weapons, deliverability of nuclear weapons, and production rate of nuclear weapons. For PP actors, objectives can be disruption of operation, radiological release, acquisition of nuclear explosives, radiation dispersal devices, and information theft. Use of this term must not be confused with the term safeguards objectives, which are used to indicate the goals established by the IAEA to detect diversion of nuclear material.
Outcomes	In the context of a PR&PP evaluation, the results of system response analysis.
Pathway analysis	For a given set of threats, identification of potential sequences of events that lead to the undesirable outcome (proliferation, sabotage, or theft) and the estimation of the system response. For PR, according to the scope of the evaluation, pathway analysis may involve the complete set of proliferation stages (acquisition, processing, and fabrication) or only a subset. Each proliferation stage may be composed of one or more segments. For PP, pathway analysis may also involve proliferation stages (for theft of fissile material).
Pathways	Potential sequences of events/actions followed by adversaries to achieve objectives (proliferation for PR, theft or sabotage for PP). A pathway is composed of segments.

Pathway segment	A distinct part of a pathway.
Physical Protection (PP) Robustness	That characteristic of a nuclear energy system that impedes the theft of materials suitable for nuclear explosives or radiation dispersal devices and the sabotage of facilities and transportation by sub-national entities and/or non-Host States.
Physical Protection Resources (PPR)	A PP measure capturing the staffing, capabilities, and costs (for both infrastructure and operations) required to provide a given level of physical protection robustness and the sensitivity of these resources to changes in the threat sophistication and capabilities.
Probability of Adversary Success (PAS)	A PP measure capturing the probability that an adversary will successfully complete the action described by a pathway and generate a consequence.
Processing	A high-level stage of a PR pathway, considering the set of activities carried out to convert the nuclear material obtained in the acquisition stage into material ready for use in a nuclear weapon.
Progressive approach	A progressive evaluation approach allowing evaluations to become more detailed and more representative as more detailed information becomes available.
Proliferation Resistance (PR)	That characteristic of a nuclear energy system that impedes the diversion or undeclared production of nuclear material or misuse of technology by the Host State seeking to acquire nuclear weapons or other nuclear explosive devices.
Proliferation Cost (PC)	A PR measure capturing the economic and staffing resources required to overcome the multiple barriers to proliferation. The measure is estimated in dollars and might be scaled (e.g., against the total resources available to a proliferant State for military expenditures).
Proliferation Technical Difficulty (TD)	A PR measure capturing the inherent difficulty, arising from the need for technical sophistication and materials handling capabilities, required to overcome the multiple barriers to proliferation.
Proliferation Time (PT)	A PR measure capturing the time to overcome the multiple barriers to proliferation.
Reference Threat Set	A collection of well-defined threats that is to be consistently considered and is the foundation for any level of PR or PP assessment. Reference Threat Sets should evolve through the design and development process of nuclear fuel cycle facilities. Once the facility is constructed, Reference Threat Sets become Design Basis Threats.
Sabotage	A deliberate act intended to lead to a radiological release or disruption of operation.
Safeguards	Activities conducted by an independent agency to verify that commitments made by States under safeguards agreements are fulfilled. Verification agencies include the IAEA, Euratom, and the Agencia Brasileño Argentina de Contabilidad y Control de Materiales Nucleares (ABACC).
Safeguardability	The ease with which a system can be effectively and efficiently put under international safeguards. "Safeguardability" is a property of the whole nuclear system and is estimated for targets on the basis

	of characteristics related to the involved nuclear material, process implementation, and facility design.
Strategy	A description, in general terms, of the ways in which the actor may achieve its objective.
System elements	Facilities to be included in the assessment. For PR, system elements are the collection of facilities inside the identified nuclear energy system where diversion/acquisition, and/or processing, and/or fabrication could take place. For PP, system elements are facilities in the nuclear energy system that can be or can contain targets for physical protection threats.
System response	In the context of PR, the resistance that a nuclear energy system provides against proliferation. In the context of PP, the robustness that a nuclear energy system provides against theft and sabotage.
Target	For PR, nuclear material that can be diverted or equipment/processes that can be misused to process undeclared nuclear materials or can be replicated in an undeclared facility. For PP, nuclear material or information to be protected from theft and transfer or equipment to be protected from sabotage.
Target access	A PP pathway stage considering the activities carried out to gain access to a target or an equipment target set.
Target exploitation	A PP pathway stage considering the activities carried out to remove a theft target from a facility or transportation system or to damage an equipment target set.
Technology Readiness Level	Level of a safeguards method development relative to that required for fully functional deployment.
Theft	Unlawful removal of nuclear material, radioactive material, or information.
Threat	A description of a potential menace consisting of information about the actor and the actor's strategy. A PR threat can be described by defining the objectives, capabilities, and strategy of a proliferant State. A PP threat is similarly described for a sub-national actor or non-Host State.
Threat space	A full suite of potential threats.
Vital area	Locations in a nuclear facility containing equipment, systems, or devices or nuclear/radioactive material the sabotage of which could directly or indirectly lead to unacceptable radiological consequences or disruption of operations.

(This page has been intentionally left blank.)

6 LIST OF ACRONYMS

10 CFR 73	U.S. Code of Federal Regulations
ABACC	Agencia Brasileño Argentina de Contabilidad y Control de Materiales Nucleares.
C	Consequences
CANDU	Canada Deuterium Uranium nuclear reactor
DB-Pu	deep burn plutonium
DBT	Design Basis Threat
DOE	U.S. Department of Energy
DOS	U.S. Department of State
DP	Detection Probability
DE	Detection Resource Efficiency
DUPIC	Direct Use of spent PWR fuel in CANDU
EASI	Estimate of Adversary Sequence Interruption
GEN IV	Generation IV
GIF	Generation IV International Forum
H	High
HEU	High-enriched uranium
IAEA	International Atomic Energy Agency
INFCE	International Nuclear Fuel Cycle Examination
INFCIRC	Information Circular (IAEA publication)
L	Low
LEU	Low-enriched uranium
LWR	Light Water Reactor
M	Medium
MAU	Multi-attribute utility
MC&A	Material Control and Accounting
MOX	Mixed Oxide
MQ	(Fissile) Material Quality
NAS	U.S. National Academy of Sciences
NASAP	Nonproliferation Alternative Systems Assessment Program
NERAC	Nuclear Energy Research Advisory Council of the DOE
NES	Nuclear energy system
NNSA	National Nuclear Security Administration
NNWS	Non-Nuclear Weapon State
NPAM	Non-Proliferation Assessment Methodology (Working Group)
NPT	Non-Proliferation Treaty
NWS	Nuclear Weapon State
PC	Proliferation Cost
PDI	Person-Days of Inspection
PP	Physical Protection (Robustness)
PPR	Physical Protection Resources
PPS	Physical Protection System
PR	Proliferation Resistance
PRA	Probabilistic Risk Analysis
PR&PP	Physical Protection and Proliferation Resistance
PAS	Probability of Adversary Success
PSA	Probabilistic Safety Assessment

PUREX	Plutonium and Uranium Recovery by EXtraction
PT	Proliferation Time
PWR	Pressurized Water Reactor
RDD	Radiation dispersal device
RG-Pu	Reactor-grade plutonium
RTS	Reference Threat Set
SNL	Sandia National Laboratories
SQ	Significant Quantity (of nuclear material)
TD	Proliferation Technical Difficulty
TOPS	Technological Opportunities to Increase the Proliferation Resistance of Global Civilian Nuclear Power Systems
UREX	Uranium Recovery by EXtraction
WG-Pu	Weapons-grade plutonium