APPLICATIONS OF NUCLEAR SAFETY PROBABILISTIC RISK ASSESSMENT TO NUCLEAR SECURITY FOR OPTIMIZED RISK MITIGATION

S.K. Donnelly and S.B. Harvey
Amec Foster Wheeler, Toronto, Ontario, Canada
sean.donnelly@amecfw.com, stan.harvey@amecfw.com

Abstract

Critical infrastructure assets such as nuclear power generating stations are potential targets for malevolent acts. Probabilistic methodologies can be applied to evaluate the real-time security risk based upon intelligence and threat levels. By employing this approach, the application of security forces and other protective measures can be optimized. Existing probabilistic safety analysis (PSA) methodologies and tools employed in the nuclear industry can be adapted to security applications for this purpose. Existing PSA models can also be adapted and enhanced to consider total plant risk, due to nuclear safety risks as well as security risks. By creating a Probabilistic Security Model (PSM), safety and security practitioners can maximize the safety and security of the plant while minimizing the significant costs associated with security upgrades and security forces.

1. Introduction

Risk informed decision making processes are applied in many industries. More sophisticated applications utilize a probabilistic assessment methodology, allowing for quantification of residual risk. WhileProbabilistic Safety Assessments (PSA) are commonly used in highly regulated industries such as the nuclear power generating industry to quantify risks to public safety, many other industries and organizations employ a Threat and Risk Assessment (TRA) to identify and quantify security risk. The Harmonized TRA of the Communications Security Establishment (CSE) and Royal Canadian Mounted Police (RCMP) [1] provides a comprehensive TRA methodology. Most organizations will utilize a more basic approach, tailored to the complexity of their operating environment.

A TRA is typically divided into a number of phases, which are presented inFigure 1. While a TRA is intended to identify and quantify threats, evaluate their frequencyof occurrence, the consequences, residual risk and mitigation measures, it does not typically consider optimization of human interactions (e.g., security forces or operations staff) to mitigate the risk. This paper focuses on this aspect, namely the optimization of the complex interactions associated with security forces, inherent safety and security design features. This activity has been termed a Probabilistic Security Model (PSM) and aims to increase the efficacy of a security force and minimize operational cost and complexity.

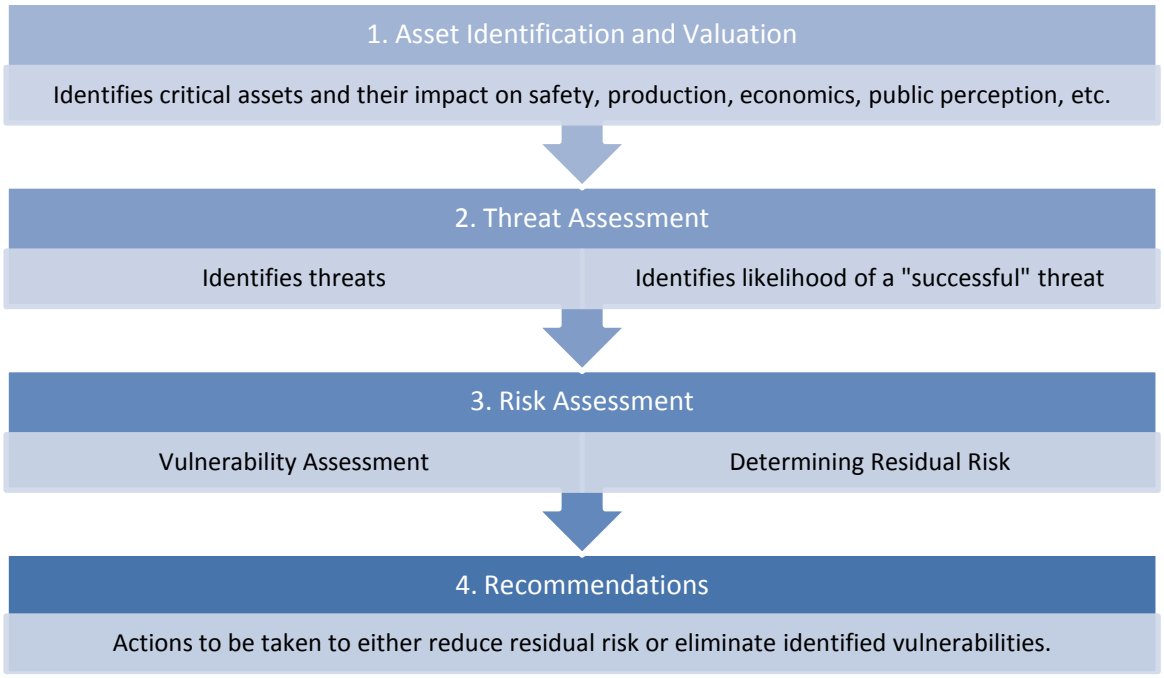

Figure 1: Typical phases of a Threat and Risk Assessment.

2. Background

PSAs and TRAs are common in many industries. Utilities and particularly large electrical generating stations utilize such tools to minimize public and economic risk. Substantial financial investments have been made to develop the PSAs for Nuclear Power Plants (NPPs); a basic PSA is likely to cost several millions of dollars. However, utilities and regulators worldwide recognize the benefits of such studies in reducing public risk by identifying and quantifying risk, thereby allowing for the reduction of risk.

NPP PSAs are used to support a wide variety of design, maintenance, operational, and safety analysis aspects; however, security-related applications are not one of the typical uses and are not considered in international guidance such as Reference [2]. Most other PSA-related guidance and regulatory documents are also silent on security applications. This absence in readily available guidance can at least be partially be attributed to the fact that practitioners of PSA and those responsible for nuclear security are organizationally separated. Further, the potentially sensitive nature of both focus areas does not lend well to information sharing; hence, there may not be an awareness of the potential interactions of the two areas.

Probabilistic tools represent a valuable tool for enhancing protection from threats such as malevolent acts, particularly security events with the potential to impact public safety for which NPP PSAs were intended. Of note is that in some jurisdictions, the NPP PSA is classified as security sensitive due to the potential to identify vulnerabilities that could be used to exploit sensitive aspects.

2.1 Overall vulnerability assessment

A PSM can identify the relative strengths and weaknesses of both the overall and individual parts of the security systems including alarm functions, video threat assessment, and communication, through to various layers of security responder intervention.

A PSM can be used to identify attack locations in terms of attractiveness of the targets and the specifics of the security measures which may be effective to mitigate the risk of such sequences (e.g., protective devices, security forces, alarms). However, by combining a PSM with the plant PSA, the consequences of such an event should it occur can be explicitly evaluated and the risk reduction associated with security improvements can be evaluated. The use of the PSM along with the PSA provides the most comprehensive solution for optimizing protection and response.

Depending on how a PSM is built, it may be possible to identify implications of adversary damage done in geographic areas. For example PSAs used to assess fire damage can predict for a given fire location which components and sub-systems may be affected. Such affects consider both direct damage due to fire and indirect damage such as compromising electrical cables to remote equipment that run through the area affected. Similar approaches have been used in security studies to assess impact of postulated aircraft crashes or explosions of specified magnitudes and consequent damage radii.

The overall PSM assessment process is shown in Figure 2. The subsequent sections describe each of these stages in more detail.

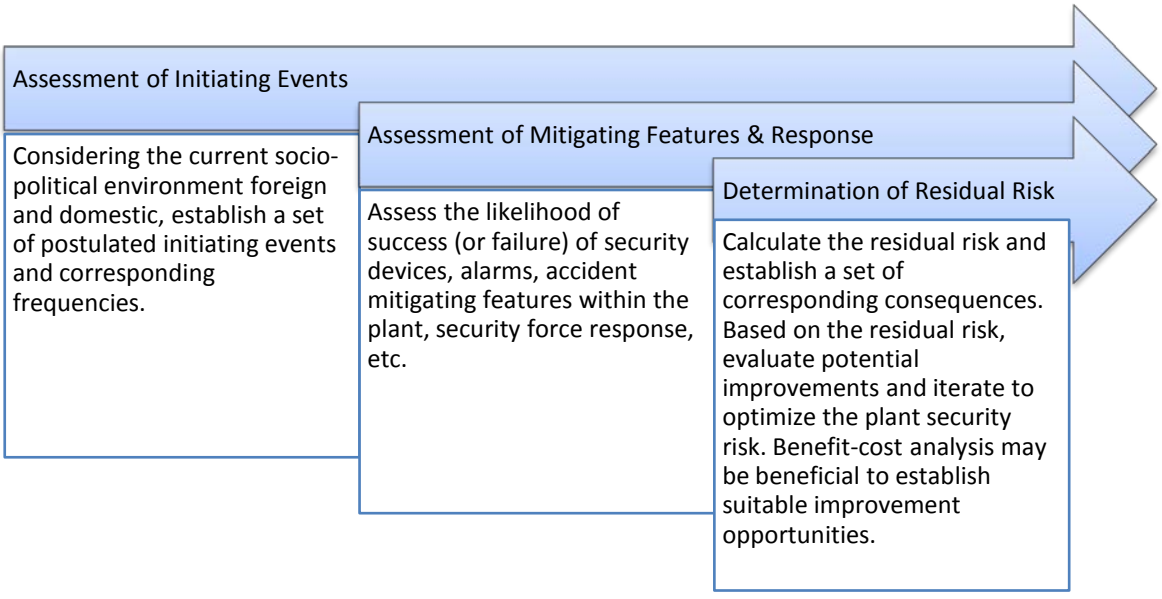

Figure 2: Concept of PSM Assessment

2.1.1 Assessment inputs

A PSM requires sufficient information pertaining to the threat and the expected probability of success of various robustness features or mitigation actions.

The threat itself must be established with sufficient clarity to define the characteristics of the threat (e.g., adversary capability). Security threats for a nuclear facility could involve a wide spectrum of adversary capabilities. For example, a more likely threat would be that of an environmental activist group wishing to vandalize a portion of the plant for media attention. The frequency of occurrence of a threat can be established through assessment of similar events worldwide and an assessment of the domestic "environmental terrorist" threat. A less likely, but potentially much more harmful threat could entail a terrorist cell with access to significant funding, insider knowledge, and the means to carry out a significant attack. In addition to use of the PSM with a range of assessed threat frequencies, the PSM can alternately be used with a given threat set as a certainty, and then the likelihood of various adverse consequences as a result of mitigation measures can be assessed.

Once the threat is established and a suitable security "initiating event" frequency is established, the PSM requires that the analyst evaluate the various barriers which would mitigate the potential consequences. Such barriers may include factors such as physical barriers (e.g., delay barriers), civil/structural factors (e.g., target hardening, wall thicknesses), intrusion detection and other alarm systems, response force personnel, and the physical facility layout. Each of these factors must be systematically assessed to determine the likelihood of success of the protective features or measures.

Although this approach can be adopted using a static plant condition, use of actual operational conditions, and real-time threat levels can allow security and PSA practitioners to assess the specific security risk profile of the plant in any condition at any point in time. This is highly effective at addressing changing risk levels due to political and world events. For example, the terrorist risk rating can be used as an input to the model to evaluate the change in plant risk due to a change in terrorist activity or chatter.

2.1.2 Assessment tools

Tools developed for PSAs can be adapted to use with a PSM. These include the Fussell-Vesely(FV) importance measure which represents the ratio of the decreased risk level if a component (in the case of a PSM this would be an element of the security system) is assumed never to fail to the reference risk calculated from the PSM. Risk Achievement Worth (RAW)is another PSA importance tool that could be applied to a PSM. RAW assesses the impact on system reliability of a component of the system that is assumed to be failed. It is a measure of the worth or importance of a given component in achieving the system's macroscopic reliability. In essence, a component is shown as being failed in the PSM and then the model is solved to assess the impact on the security system. The Risk Reduction Worth (RRW) can also be utilized, signifying the reduction in overall risk if the component failure was to never occur.

There are other importance measures beyond the three described above that can be applied to specific applications. In all cases, use of importance measures requires a degree of expertise since it is both possible to misinterpret individual importance measures, and importance measures can be computationally challenging unless carefully chosen simplifying assumptions are applied.

Depending on the type of protective feature or measure, one or more of these PSA tools may be better suited to characterize the significance. For example, a large FV will indicate that improving the robustness or effectiveness of a particular protective feature or response will have a significant effect on mitigating the residual risk. Other importance measures can provide similar insights.

2.2 Minimizing Risk

2.2.1 Mitigation following failures

Security systems typically have established processes to be appliedfollowing failure of one part of the system. For example if an alarm system is failed, a security officer may be posted to provide oversight that the alarm would otherwise provide. A PSM can be used to identify strategies to cater to component failures that provide the largest security benefit at the lowest cost. This could be useful if a new vulnerability is identified through operating experience at other facilities or if the Design Basis Threat is changed. The PSM can identify what parts of the security system are most important given a particular new or increased likelihood of an existing threat is postulated.

2.2.2 Human reliability

One of the significant advancements in the field of PSA is the understanding of the impact of humans on system reliability. This is important to any risk assessment since humans have a dominant effect on the effectiveness of detection and mitigation functions, whether in the plant reliability context or in the security context. The methodologies to model human performance developed for plant level risk assessments can be directly applied to security. They involve assessing factors such as the complexity of decision making, the nature of information presented, the complexity of the human-machine interface, and the time demands in which decisions and reactions must occur.

As an example, similar approaches to the modelling of plant operator reliability in the context of a PSA could be applied to modeling of security staff in Security Monitoring Rooms. Like the plant control room, security staff in the Security Monitoring Rooms are absolutely essential to the outcome of a security event. A human reliability model as part of a PSM can identify areas where staff in the Security Monitoring Rooms would benefit from improvements that increase their ability to process information in a high-stress situation and to perform their role as a critical link in the ability of responders to defend where needed.

2.2.3 Optimization of use of existing assets; identifying impact of changes to assets

For a given existing set of security systems and resources, it is possible to use a PSM to optimize deployment. For example, the deployment of security foot or vehicle patrols by geographic sector can be optimizedbased on risk to the plant posed by intrusion in various sectors. A probabilistic model would show that a sector that is inherently protected by geographic features or which is remote from sensitive plant areas, would get less benefit from patrols than areas that do not have the same inherent security advantages. A randomized patrol schedule could then bias upward patrol time spent in the more sensitive sectors to optimize the risk profile across all sectors.

Depending on the detail of the PSM, it could also be possible to compare the relative importance of foot patrols, vehicle patrols, and automated systems to optimize the resourcing.

The PSM can be used to assess the security value of expenditures. This could include assessing the security risk reduction as a result of adding an armoured vehicle patrol, or adding an additional Security Monitoring Room operator. Similarly the adverse impact of resource reductions can be assessed and the least impactful areas to make reductions can be identified.

Reliability targets for safety systems are typically established in a nuclear plant to identify during system design, the amount of redundancy required and the required reliability of individual components or sub-systems. Targets also influence the frequency of testing that must be performed and flag when repeated component or system failure is reaching a level where improvements are required. Historically such targets were developed deterministically but it is now possible to develop system targets based on the plant risk model. The same is possible for security systems based on the use of a PSM. Such targets can be used to specify or validate testing frequencies of components. Over-testing is a waste of resources and can cause premature wearout of components. Under-testing reduces reliability. Targets allow for an appropriate response to individual failures by identifying when such failures are within bounds of anticipated failure rates or are indicative of components that are entering end of life and need to be replaced.

3. Conclusions

The approach to nuclear safety continues to evolve with the use of probabilistic methods in addition to classical deterministic approaches. This shift acknowledges that all scenarios cannot be fully postulated and that bounding design basis events are not always representative of the worst case due to unknowns. As security risks continue to change, the design basis threat approach becomes more complex and requires frequent change to adapt to changing security risks. Furthermore, as with nuclear safety, design basis threats may not fully reflect the worst case due to unknowns and the development of more and more complex aggressorstrategies.

Probabilistic methods provide options for the evaluation of these threats: directly from existing PSA for identification of security vulnerabilities or the use of PSA methods to develop a separate or complimentary PSM. A PSM can be used to determine the dynamic security risk profile and adapt security forces and mitigation measures to minimize risk.

The benefits of well-established PSA tools have been proven for nuclear safety applications and help to improve plant nuclear safety and therefore public safety. These tools can be adapted and applied in the nuclear security context to further improve nuclear safety and public safety from the perspective of security. Many of the benefits of PRA for enhancing Nuclear Safety can be achieved using a stand-alone PSMor a PSM and PSA together to enhance Nuclear Security. These models provide new capability to enhance and optimize the security design and response capability for the facility.

4. References

[1] Communications Security Establishment & Royal Canadian Mounted Police, “Harmonized Threat and Risk Assessment Methodology”, TRA-1, 23 October 2007.

[2] International Atomic Energy Agency, “Applications of probabilistic safety assessment (PSA) for nuclear power plants”, IAEA-TECDOC-1200, February 2001.