SANDIA REPORT

SAND2013-8616
Unlimited Release
Printed October 2013

Analysis of Alternatives for Risk Assessment Methodologies and Tools

Noel M. Nachtigal, Julia A. Fruetel, Nathaniel J. Gleason, Jovana Helms,
Dennis R. Imbro, and Matthew C. Sumner

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2013-8616
Unlimited Release
Printed October 2013

Analysis of Alternatives for Risk Assessment Methodologies and Tools

Noel M. Nachtigal[1], Julia A. Fruetel[2], Nathaniel J. Gleason[2], Jovana Helms[2], Dennis R. Imbro[2], and Matthew C. Sumner[2]

[1]System Analytics (8958)
[2]Systems Research and Analysis (8110, 8114, and 8116)

Sandia National Laboratories
P.O. Box 969, Livermore, California 94551-0969

Abstract

This document reviews common risk-analysis methodologies and associated tools and considers their strengths and weakness for performing cybersecurity risk analysis.

CONTENTS

FIGURES

TABLES

SELECTED NOMENCLATURE

DHS	Department of Homeland Security
I^2S	Integrated Infrastructure Security
MARA	Multi-attribute risk analysis
MORA	Multi-object risk analysis
N/A	Not applicable
NAS	National Academy of Sciences
PRA	Probabilistic risk assessment
RIMES	Risk-Informed Management of Enterprise Security
SECIR	Stakeholder Engagement and Cyber Infrastructure Resilience
SME	Subject-matter expert
SNL	Sandia National Laboratories
T, V, C	Threat, vulnerability, and consequence

EXECUTIVE SUMMARY

The purpose of this document is to provide a basic overview and understanding of risk assessment methodologies and tools from the literature and to assess the suitability of these methodologies and tools for cyber risk assessment. Sandia National Laboratories (SNL) performed this review in support of risk modeling activities performed for the Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) division of the Department of Homeland Security (DHS) Office of Cybersecurity and Communications (CS&C).

The set of methodologies and tools covered in this document is not intended to be exhaustive; instead, it focuses on those that are commonly used in the risk assessment community. The classification of methodologies and tools was performed by a group of analysts with experience in risk analysis and cybersecurity, and the resulting analysis of alternatives has been tailored to address the needs of a cyber risk assessment.

The remainder of this document is organized as follows.

- Chapter 1 gives a brief overview of this document and introduces some basic definitions and terminology. It also defines the threat, vulnerability, and consequence framework.
- Chapter 2 provides descriptions of the identified risk assessment methodologies.
- Chapter 3 describes tools that are commonly used in conjunction with these methodologies.
- Chapter 4 offers concluding remarks.

1 INTRODUCTION

1.1 Identification of Risk assessment Methodologies and Tools

This document seeks to provide a basic understanding of risk assessment by summarizing the most commonly used methodologies and tools. It also briefly considers the pros and cons of each of these methodologies and discusses their applicability to cybersecurity risk assessment.

For the purposes of this document, the distinction between a "methodology" and a "tool" is that a risk assessment methodology is a standalone technique that can be used to assess risk. In contrast, a risk assessment tool is a technique that can be used to support a risk assessment, but does not serve to directly assess risk on its own. (Additional terminology used in this document is primarily based on the *DHS Risk Lexicon* [3] and summarized in Figure 2.)

The identification of major classes of risk-assessment methodologies and tools relied heavily upon a National Academy of Sciences (NAS) report, *Review of the Department of Homeland Security's Approach to Risk Analysis* [4]. In particular, the table shown in Figure 1 provides a useful overview that served as a starting point for this analysis and was supplemented by discussions with experts and a variety of literature and Internet searches. This work resulted in the identification of the following common risk assessment methodologies:

- Adherence to best practices,
- Reputational or historical analysis,
- Expert judgment,
- Risk factors,

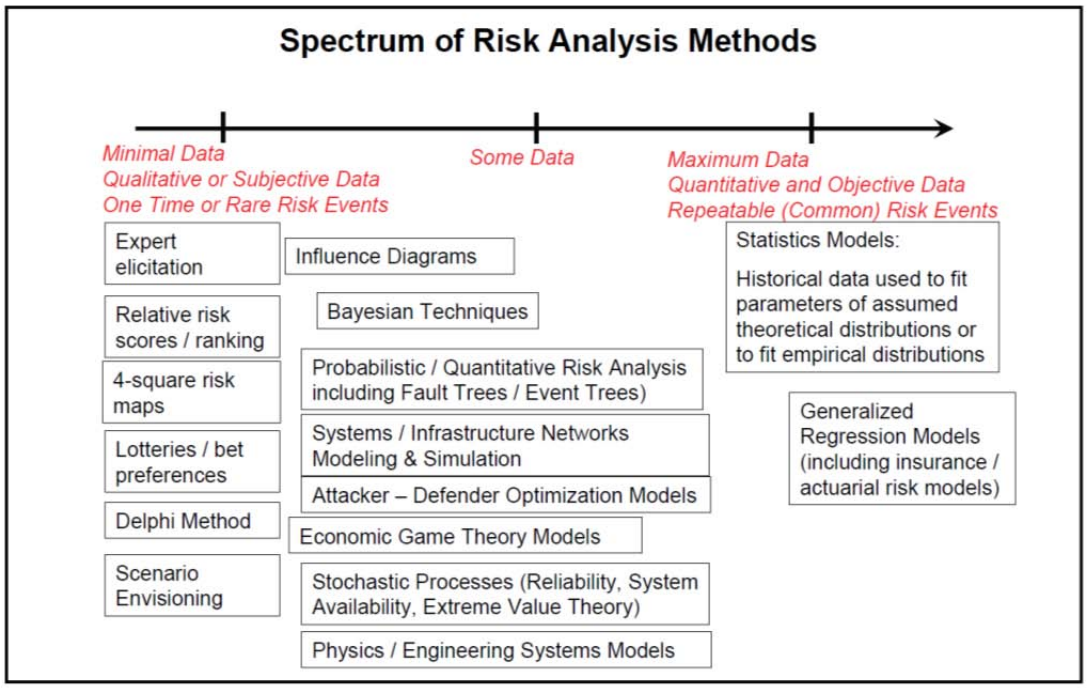


Figure 1: Table of risk methodologies from NAS report

Source: Figure 5-1 from [4]

- Risk factors with regression analysis,
- Multi criteria risk analysis,
- Risk-Informed Management of Enterprise Security, and
- Probabilistic risk assessment.

The following tools were also identified:

- Casual loop diagrams (systems dynamics),
- Expert elicitation,
- Fuzzy logic,
- Game theory,
- Bayesian statistics,
- Fault trees,
- Event trees,
- Attack graphs,
- Prediction markets,
- Scenario planning,
- Sensitivity analysis, and
- Reliability analysis.

Each of the methodologies is discussed in more detail in Chapter 2. Overview of risk assessment tools is given in chapter 3, while Chapter 4 contains summary comparisons of methodologies and our concluding remarks.

1.2 Threat, Vulnerability and Consequence Framework

Risk assessments often use a framework in which risk can be decomposed into threat, vulnerability and consequence, based on the following definitions [3]:

> **Threat (T)**: "Natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property" [3].
>
> **Vulnerability (V)**: "Physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard" [3].
>
> **Consequence (V)**: "Effect of an event, incident, or occurrence" [3].

Using the T, V, C framework, risk can be calculated as a function of these three parameters (e.g., [11]):

$$\text{RISK} = f\,(\text{T, V, C}).$$

1.3 Report Card Definitions

Each of the descriptions of risk assessment methodologies includes a "Report Card" that provides a quick overview of the methodology and its main characteristics. The categories and rating system used in the report cards are defined in Table 1.

Risk: potential for unwanted outcome resulting from an incident, event, or occurrence as determined by its likelihood and the associated consequences.

Absolute risk: level of risk expressed with standard units of measurement that allows for independent interpretation without comparison to estimates of other risks.

Relative risk: measure of risk that represents the ratio of risks when compared to each other or a control.

Non-adaptive risk: category of risk that includes threats caused by natural and technological hazards.

Adaptive risk: category of risk that includes threats intentionally caused by humans.

Risk analysis: systematic examination of the components and characteristics of risk.

Risk assessment: product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.

Risk assessment methodology: set of methods, principles or rules used to identify and assess risks and to form priorities, develop courses of action and inform decision making.

Risk assessment tool: activity, item, or program that contributes to determining and evaluating risks.

Qualitative risk assessment methodology: set of methods, principles, or rules for assessing risk based on non-numerical categories or levels.

Quantitative risk assessment methodology: set of methods, principles or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment.

Semi-quantitative risk assessment methodology: set of methods, principles, or rules to assess risk that uses bins, scales or representative numbers whose values and meanings are not maintained in other contexts.

Subject matter expert: individual with in-depth knowledge in a specific area or field.

Threat (T): natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Vulnerability (V): physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard.

Consequence (C): effect of an event, incident, or occurrence.

T, V, C framework: a model in which risk can be understood as a function of threat, vulnerability, and consequence so that RISK = f (T, V, C).

Figure 2: Definitions and terminology used in this document

Definitions adapted from [3].

Table 1: Description of Entries in Methodology Report Cards

Methodology Name	
NAS Category	This entry identifies the corresponding category from the NAS report (Figure 1) or "N/A" if the NAS report did not include this approach.
Input	This entry describes the type of data needed for input to the methodology. • **Data:** Inputs consist of directly measurable and objective data. • **SME:** Inputs consist of subjective data provided by SMEs. • **Both:** Method can accommodate objective data and/or SME feedback.
Aggregation	This entry describes whether the methodology produces an aggregated score (e.g., a single value representing the risk associated with each scenario). • **Yes:** Method inherently produces an aggregated score. • **No:** Method is not capable of producing an aggregated score or is not typically used in that fashion. • **Optional:** Method can support the creation of an aggregated score if desired.
Weighting	If the methodology assesses risk by considering multiple components (e.g., by calculating a weighted sum), this entry describes how these components are weighted. • **Subjective:** Weights are defined through a subjective method, such as SME feedback. • **Data-based:** Relative weighting is defined through a data-driven, objective approach, such as regression analysis. • **None:** All risk factors and/or data points are weighted equally.
Output	This entry categorizes the type of output produced by the methodology. • **Quantitative:** (See Figure 2.) • **Semi-quantitative:** (See Figure 2.) • **Qualitative:** (See Figure 2.) • **Any:** Methodology can produce any of the three types of outputs
Scenario Based	This entry describes whether the methodology assesses risk by considering particular adversary attack scenarios. • **Yes:** Method inherently requires scenarios to be defined. • **No:** Method does not incorporate attack scenarios. • **Optional:** Method can incorporate attack scenarios if desired, but they are not required for the assessment.
T, V, C	This entry describes whether the methodology incorporates the threat vulnerability and consequence (T, V, C) framework as described in Section 1.2. • **Yes:** Method explicitly incorporates the T, V, C framework. • **No:** Method is inconsistent with the T, V, C framework. • **Optional:** Method can use the T, V, C framework if desired, but this is not required to complete the risk assessment.
Tools	This entry lists tools, if any, that are frequently used in conjunction with the methodology.
Implementation Challenges in Cyber	If the analysis team identified any challenges that might make it difficult to apply a particular methodology to understanding cybersecurity risks, those challenges are listed here.
Examples	This entry lists particular implementations of the general methodology.
Illustration	This entry points to a figure associated with each methodology.

2 RISK ANALYSIS TECHNIQUES
2.1 Adherence to Best Practices

The establishment of best practices is a commonly used technique for addressing potential security risks, and the degree to which a facility adheres to best practices can serve as a simple form of risk assessment. A best practices list identifies a set of recommended risk-mitigation steps, which are typically based on analysis of prior negative outcomes and/or reflect common sense in a given industry. By removing the "low-hanging fruit," such practices block many of the adversary's easiest attack options. If an adversary is not committed to attacking a particular target, this level of security may be sufficient to cause them to look elsewhere for systems that have not yet implemented the best practices [12].

Wyss et al. offer the following description of best-practices [12]:

> A commonly used tool for identifying potential security risks, especially for low-consequence facilities, is the list of "security best practices." Many such lists exist, which are often specifically tailored to particular industries, trade groups, or types of facilities. A best practice list represents a valuable first step in security risk management because it concisely identifies common security mistakes and vulnerabilities, and provides concrete steps for their mitigation. Since these lists have often been developed from the postmortem analysis for security events that have actually occurred, it is easy to view these lists as recipes to mitigate high risk security problems and, thus, reduce and manage security risks. Indeed, security analysts may decide that failure to implement basic security best practices leaves a target so vulnerable to attack that performing a more detailed or intrusive security analysis is a waste of time and money.[5] Thus, while best practice lists do not explicitly calculate a value for risk, they are valuable risk management tools. [Inline footnote 5 refers to [13]].

Table 2: Report Card for Adherence to Best Practices

Adherence to Best Practices	
NAS Category	N/A
Input	Both (SME and/or Data)
Aggregation	No
Weighting	None
Output	Qualitative
Scenario Based	No
T, V, C	No
Tools	N/A
Implementation Challenges in Cyber	• Does not directly assess risk • Difficult to implement for all risks and less common attacks • Recommendations are often very general and may not be applicable across a broad range of system types
Examples	• SANS "Twenty Critical Security Controls for Effective Cyber Defense" • Australian Defense Signals Directorate "Strategies to Mitigate Targeted Cyber Intrusions"
Illustration	Figure 3: Food pyramid

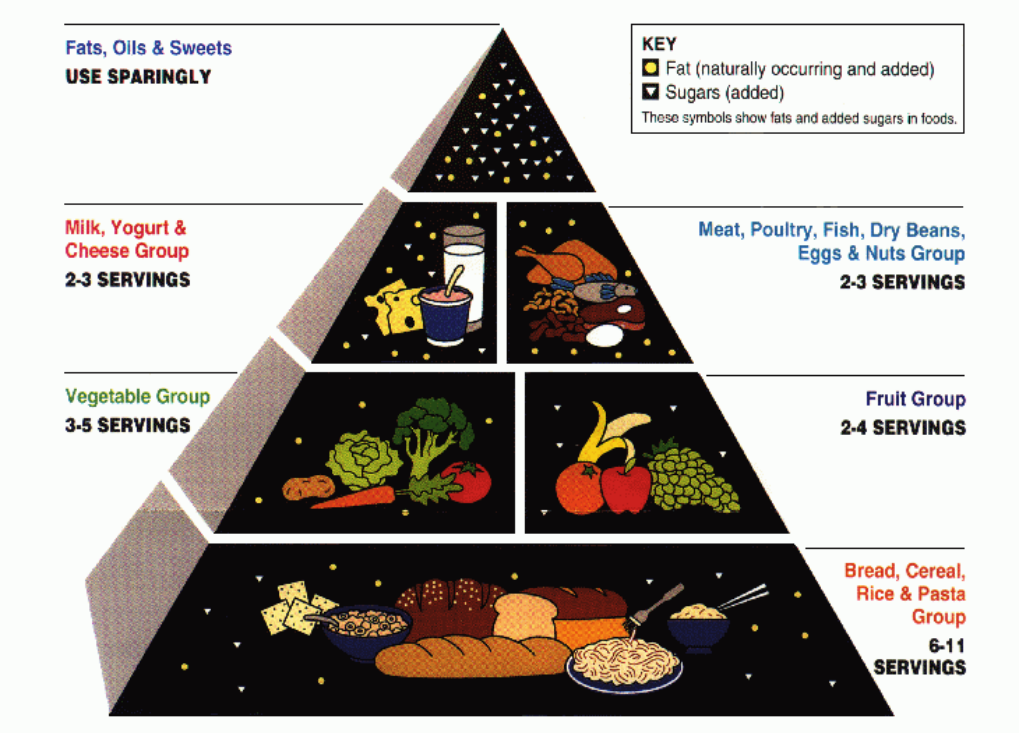


Figure 3: Food pyramid

Source: [1], as reproduced in [7]

A list of best practices can help establish common standards within a community, allowing members to agree on what needs to be done to make systems safer and more secure. They also may be used to provide some measure of quantification for reduction in security risk. For example, the "Twenty Critical Security Controls for Effective Cyber Defense" represent the consensus guidance of broad range of cybersecurity experts. The automation of these controls is anticipated to lower the cost of security while improving its effectiveness. The SANS Institute reports that the U.S. State Department has achieved an "88% reduction in vulnerability-based risk" through the rigorous automation and enforcement of the Twenty Critical Security Controls [12, 14, 15].

Although best practices help to set a baseline level of safety and security, representing the most basic level of risk mitigation, they are usually general in nature, rather than focusing on a specific system or a particular set of threats. Less common attacks may not be addressed adequately. Also, because it is often based on analysis of prior negative outcomes, this technique may not protect well against attacks that have yet to be observed.

Strengths:

- Leverages real-world experiences within a community, capturing common vulnerabilities and use cases.
- Establishes a baseline, foundational level of security upon which more advanced risk-mitigation can be constructed.
- Typically provides actionable, operationally relevant advice that is relatively straightforward to implement.

- Implicitly accounts for likelihood and consequences by addressing the risks that are perceived to be most important in a community and/or by analyzing case studies of attacks perceived to have high severity or likelihood.
- May provide some quantitative measure of security risk reduction.

Weaknesses:

- Usually nonspecific and may not address all risks particular to a given system; since the recommendations are not based on a system-specific risk assessment, the largest risk drivers may be overlooked.
- Often based on analysis of the most common attacks or broad classes of attacks; however, may not protect against attacks that are less commonly observed.
- Largely focused on retrospective analysis, so may not protect against attacks that have not yet been observed but could be identified through a more structured risk analysis.
- May not be applicable across a broad range of systems or may be perceived as “one-size-fits-all.”

2.2 Reputational or Historical Analysis

This technique leverages historical data from prior transactions and/or experiences with a given product or company to provide insight regarding the current acquisition decision. While it is not always predictive, past performance does provide an intuitively appealing basis for decision-making.

One method of performing historical analysis is social rating system, which is very popular among commercial websites, such as Amazon, Netflix, eBay, and Yelp (see Figure 4 and Figure 5). This method relies on users' ratings and feedback on products and services they have purchased. The data can be collected with respect to different criteria (e.g., shipping speed, packaging, customer service, and the quality of the product) or as an overall rating. The most basic form of social ratings is giving a "thumbs up" or "thumbs down" review or assigning a single numerical score to a resource (e.g., a product, a vendor, or a service) [16]. The ratings can also be extended to include reviews and discussions. The data is aggregated and averaged resulting in each resource being assigned one or more scores that can be used to sort resources by relevance, importance, trustworthiness, etc.

One of the main disadvantages of this method is that meaningful risk assessment requires a large sample size, typically involving data collected over an extended period of time. Consequently, risk assessments cannot be performed for new products or companies that have not yet received many reviews. Also, it can be difficult to verify the validity of results, particularly in social scoring systems [17, 18], so user reviews should be vetted to ensure the feedback is coming from trustworthy sources. Finally, vendors or manufacturers may develop strategies to influence their reputational scores (e.g., [19, 20]), potentially making them less reliable.

Table 3: Report Card for Reputational or Historical Analysis

Historical Analysis	
NAS Category	N/A
Input	Both (SME and/or Data)
Aggregation	Optional
Weighting	Optional
Output	Any
Scenario Based	No
T, V, C	No
Tools	N/A
Implementation Challenges in Cyber	• Assessments are retrospective, so there is a time lag
Examples	• Social systems on consumer website (eBay, Amazon, Netflix, Yelp) • Common Vulnerability Scoring System (CVSS) repository of software vulnerabilities • Better Business Bureau review system for businesses • NASA PimeSupplier tool (includes historical data, as well as other factors)
Illustration	Figure 4: Amazon social rating system

Figure 4: Amazon social rating system

Source: Amazon.com

Another form of historical analysis can be based on expert reviews, in which an expert user reviews a product to determine its suitability for different customer use cases. In security analysis, such reviews can be particularly useful, as security experts may be able to find vulnerabilities that normal users would be unlikely to identify. If a vulnerability is found, communicating its existence to current users and potential purchasers can provide an important element of a risk-management process.

By definition, any form of historical analysis must be retrospective. If a resource has traditionally performed well, it may take some time for the overall scores to reveal recent decreases in quality or reliability. Given sufficient numbers of user reviews, this can be addressed by showing a time history of reviews to identify recent trends.

Reputational/historical analysis is different from SME elicitation as the analysis is retrospective, while SME elicitation is prospective.

Strengths:

- Social rating systems leverage real-world experiences with a given resource, sometimes spanning an extended period of "in the field" usage and often capturing a wide range of use cases.
- Expert reviewers may be able to identify security vulnerabilities or other shortcomings that an ordinary user might not recognize.
- For both social rating systems and expert reviews, results are intuitive and concrete (i.e., they do not depend on models, future projections, scenarios, etc.).
- Negative results can be shared rapidly across a large community, and a review site can provide a centralized location for archiving such knowledge.

Weaknesses:

- For social rating systems, there is a time lag between the first availability of a resource and the time at which the sample set of reviews has grown large enough to support meaningful conclusions.
- Social rating systems can be negatively impacted by uninformed reviewers, and the entities being rated may be capable of influencing their scores.
- Expert reviews are often based on a small sample set, so rare defects are likely to be missed. If the vendor or manufacturer knows the product is being provided to an expert reviewer, it might even provide a hand-picked unit that has undergone stricter testing or has been modified to hide defects.

- Assessments are necessarily retrospective; unless the review system is structured to identify trends, recent changes in quality or reliability may not be recognized.

Case study: eBay feedback system

eBay's review system focuses on rating the site's members (the buyers and sellers who participate in the online auctions). Since most of the products are used, or "one of a kind," buying from a reputable seller is of great importance. Selling to a reputable buyer is similarly important to ensure that bids will be honored and paid promptly. eBay's feedback score is based on the number of positive ratings the user has received from the other party in prior transactions. After the first ten positive reviews the user receives a yellow star. As the feedback score increases, the star changes color, with a silver shooting star representing one million or more positive responses. In addition to the feedback score, there are four additional scores on the feedback profile for each eBay member:

1. **Positive feedback rating:** The percentage of positive ratings left by members in the last 12 months. This is calculated by dividing the number of positive ratings by the total number of ratings (positive + negative).
2. **Recent Feedback Ratings:** The total number of positive, neutral and negative feedback ratings the member has received in the last one, six, and twelve months.
3. **Detailed seller ratings:** Detailed seller ratings provide more details about this member's performance as a seller. Five stars is the highest rating, and one star is the lowest. These ratings do not count toward the overall feedback score and they are anonymous so that sellers cannot trace detailed seller ratings back to the buyer who left them.
4. **Bid retractions:** The number of times the member has retracted a bid in the last twelve months.

Adapted from [9].

Figure 5: Case study of reputational or historical analysis, based on the eBay feedback system

2.3 Expert Judgment

Many of the techniques discussed in the previous sections rely on input from SMEs. Typically the SMEs provide critical inputs; however, there is still a framework that operates on those inputs to perform the risk assessment. In contrast, the techniques described in this section ask the SMEs to directly assess relative or absolute levels of risk.

Table 4: Report Card for Expert Judgment

Expert Judgment	
NAS Category	Expert elicitation
Input	SME
Aggregation	Optional
Weighting	Subjective or None
Output	Any
Scenario Based	Optional
T, V, C	Optional
Tools	• Four square risk maps • Delphi method
Implementation Challenges in Cyber	• Difficult to find experts with appropriate expertise • Assessments are subjective, so different set of SMEs can generate very different results • Difficult to assess/account for SME bias and cognitive bias
Examples	• Direct ranking of risk scores and/or relative risk • Red teaming and penetration testing
Illustration	Figure 6: Master Yoda

Figure 6: Master Yoda

2.3.1 Direct ranking of risk scores and/or relative risk

NAS Category: Relative risk scores/ranking

Risk ranking through SME elicitation may involve various techniques where the evaluation occurs at the "risk" level, rather than at the input level for subsequently determining risk. A seminal risk ranking study conducted by EPA in 1987 titled "Unfinished Business" compared the risks associated with major environmental problems [21]. In this paper, their risk ranking method is described as follows:

> The method we used to compare environmental problem areas can best be described as systematically generating informed judgments among Agency experts…The participants assembled and analyzed masses of existing data on pollutants, exposures, and effects, but ultimately had to fill substantial gaps in available data by using their collective judgment. In this sense, the project represents expert opinion rather than objective and quantitative analysis. But despite the difficulties caused by lack of data and lack of accepted risk assessment methods in some areas, the participants feel relatively confident in their final relative rankings. [21]

Challenges involved in risk ranking include the many different ways to define risk and differences among stakeholders as to which consequences are most important. Risks can be defined and grouped in various ways, which can impact the results of risk-ranking exercises [22].

One method for deriving risk rankings is to use a matrix that maps varying degrees of consequence against varying degrees of likelihood: the combination of consequence and likelihood scores gives the risk ranking (Figure 7) [23]. The highest risk entries are those that rank highly on both the likelihood and the consequence scales. Scoring scenarios along these two axes represents a simplified form of probabilistic risk assessment[1].

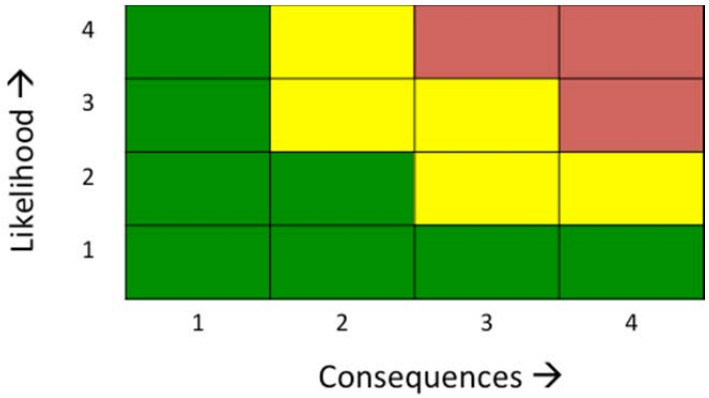


Figure 7: Example of a risk matrix used for risk ranking

Examples of likelihood and consequence scales include the Department of Defense *Standard Practice for System Safety* (MIL-STD-882D) for mishap risk classification, which ranks four severity categories (from catastrophic to negligible) against five "mishap probability levels" (from frequent, or $<10^{-1}$ during lifetime, to improbable, or $<10^{-6}$ during lifetime). Different hazards can be prioritized by mishap risk classification [24, 25]. Although a popular method for US government applications, analysis by Cox

[1] Probabilistic risk assessment is described in Section 2.8.

suggests “risk matrices should be used with caution for risk management decisions, and only with careful explanations of embedded judgments” [23].

2.3.2 Four-square risk maps

NAS Category: 4-square risk-maps

Although mentioned in the NAS report, Internet searches did not reveal a commonly used risk technique by this name. The closest match appears to be a technique that uses a two-by-two risk matrix [26].

2.3.3 Delphi Method

NAS category: Delphi Method

The Delphi method (also Delphi technique) was developed by the RAND Corporation in the 1950s as a forecasting method that relies on a panel of experts. As described by the 1969 RAND paper by Dalkey, the technique possesses three key features [27]:

> (1) Anonymous response—formal questionnaire is filled out by group members;
>
> (2) Iteration and controlled feedback—interaction is effected by a systematic exercise conducted in several iterations, with carefully controlled feedback between rounds;
>
> (3) Statistical group response—the group opinion is defined as an appropriate aggregate of individual opinions on the final round. This can reduce the bias introduced by dominant individuals, and groups tendency towards conformity.

Although Delphi method was initially designed to predict what impact new technologies will have in warfare, [28], it has also found uses in many other areas and spun off several variant forms [29, 30]. A review paper of the Delphi method suggests “there is no consistent evidence that the technique outperforms other structured group procedures,” but the authors acknowledge the “sheer variety of technique formats that have been used as representative of Delphi” makes the assessment difficult [31]. Discussion in [32] summarizes how the design of elicitation techniques for the Delphi method and other closely related techniques (such as nominal group theory) can impact the results.

One identified problem with the Delphi method is accounting for possible correlation among future events. Cross impact analysis is a technique that can help capture the interactions between different possible events [29].

2.3.4 Red Teaming and Penetration Testing

NAS Category: N/A

In red-teaming and penetration testing, SMEs are authorized by the owners of a facility or system to attempt to overcome its security systems, similar to what an adversary would do during an attack. The SMEs are trained to think like an adversary and may even adapt the goals and capabilities of a particular adversary. This method is best suited to challenging assumptions and/or identifying vulnerabilities. Although typically not intended as a risk assessment, the adversary perspective may be very important in understanding risk [33-35]. For instance, an assessment of the robustness of the overall security posture might be informed by the ease with which a red team could identify potential issues and/or the number and severity of vulnerabilities that they identified.

2.4 Risk Factors

This approach relies on the identification of factors that are indicative of the presence of risk. These factors do not necessarily indicate how much risk is present, nor are they necessarily tied to particular negative outcomes; therefore, additional interpretation of the risk factors may be needed. In many cases, the linkage between a factor and the corresponding risk is one of correlation, rather than causation [36, 37]. Historical data as well as expert's reviews/opinions can be used to feed the risk factor model and determine the risk associated with the event of interest.

The first step is to identify relevant risk factors for the given problem. Once the risk factors are identified, a risk ranking scale/score is identified for each risk factor. Each activity/transaction/event being evaluated is scored for each risk factor and the associated risk is determined using historical data and/or expert reviews. The scores are then combined in applicable way (e.g., summation across all risk factors or weighted summation) (e.g., [37]).

Advantages of this approach are its concreteness and clarity, and the fact that it is not scenario based, which makes it easier to implement and more scalable than the scenario based methods. It also works well for complex systems where multiple factors may contribute to risk in unknown ways.

The lack of scenarios is also a disadvantage of this method, as it may be difficult to interpret what the risk factors mean. It is also difficult to assess which risk factors are most important in determining risk, particularly in cases where there is not a large data set of risk factors and associated outcomes. It may be difficult to determine the optimum technique for combining multiple risk factors into a single risk score. Finally, in criminology, it has been argued that oversimplifying complex problem by converting it to simple quantities can be limiting and lead to inaccurate assessments [38].

Table 5: Report Card for Risk Factors

Risk Factors	
NAS Category	N/A
Input	Both
Aggregation	No
Weighting	Subjective or None
Output	Qualitative
Scenario Based	No
T, V, C	No
Tools	N/A
Implementation Challenges in Cyber	• Correlational, so method does not assess how much risk is present
Examples	• Qualitative medical risk factors
Illustration	Figure 8: Surgeon General's warning

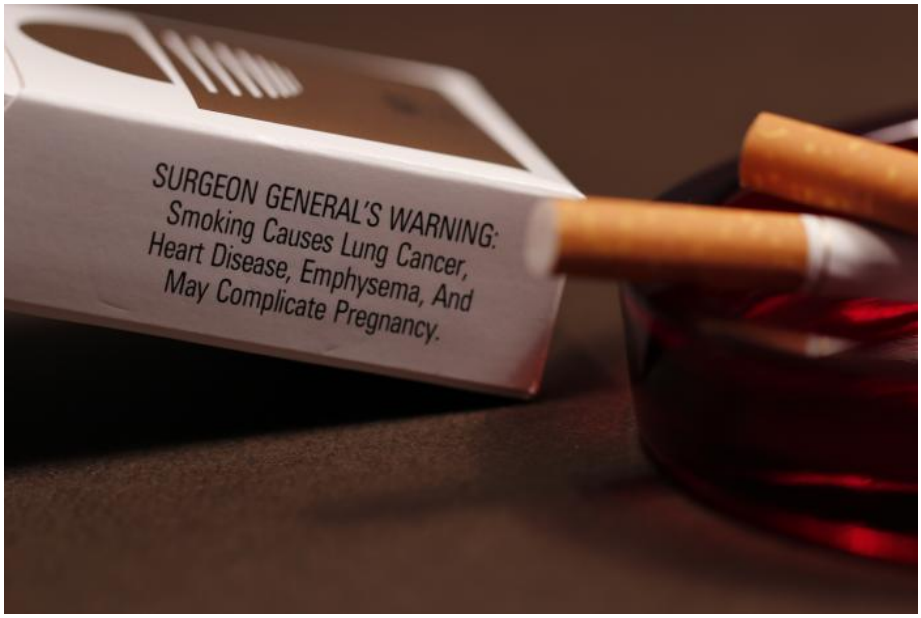


Figure 8: Surgeon General's warning on a pack of cigarettes

Photo Credit: Debora Cartagena [2]

As an example, risk factors are often used as a way of describing behavioral and environmental factors that can lead to certain medical conditions. For instance, the Centers for Disease Control and Prevention (CDC), provides the following information on lung cancer [39]:

> Research has found several risk factors for lung cancer. A risk factor is anything that increases the chance of getting a disease. Examples of risk factors for lung cancer include—
>
> - Smoking tobacco and being around others' smoke.
> - Exposures at home or work (such as radon gas or asbestos).
> - Personal history (such as having radiation therapy or a family history of lung cancer).

Strengths:

- Concrete and clear.
- Good for complex problems where multiple factors are contributing to risk.
- Can be implemented.

Weaknesses:

- Not tied to particular scenarios, so it is difficult to interpret what risk factors mean in terms of risk.
- Not clear which risk factors have more weight than others and how to incorporate that into the model.
- Does not measure risk; this method only suggests that the risk could be present but does not assess the degree of risk.
- May oversimplify complex problem by converting it to simple quantities, which could limit the value of the risk assessment.

2.5 Risk Factors with Regression Analysis

This method is similar to the risk factors approach, except that statistical methods are used to establish the degree of correlation between risk factors and particular outcomes. This approach can be used to quantify risk present in a particular situation and, in some cases, can provide evidence that supports the identification of causal relationships [40, 41]. This approach originated in epidemiology, where a risk factor can be associated with a particular medical condition through a statistical analysis of large data sets. This technique has also found applications in finance and criminology [36, 38, 42].

Table 6: Report Card for Risk Factors with Regression Analysis

Risk Factors with Regression Analysis	
NAS Category	Generalized regression models
Input	Both
Aggregation	Yes
Weighting	Data-based
Output	Quantitative or Semi-quantitative
Scenario Based	No
T, V, C	No
Tools	N/A
Implementation Challenges in Cyber	• Large data sets of potential risk factors and resulting outcomes may not be available in cyber.
Examples	• Epidemiological studies
Illustration	N/A

2.6 Multi Criteria Risk Analysis

Multi-criteria decision making (MCDM) or decision analysis is a sub-discipline of operations research that explicitly considers multiple criteria in decision making environments [43]. It is used to simplify the decision making process in complex problems that involve multiple, often conflicting criteria.

In risk analysis, the most frequently used MCDM methods are multi-attribute risk analysis (MARA), and multi-objective risk analysis (MORA) [43]. In this section we will focus on MARA and then point the main differences between MARA and MORA.

When implementing MARA the following steps are necessary [44]:

1. Identify attributes: Identifying the correct set of attributes that contribute to risk is crucial for successful MARA implementation. The attributes are identified by decomposing the problem into smaller, less complex components. This typically yields a hierarchical structure. The main branches can, but do not have to be, organized by threat, vulnerability, and consequence. The set of attributes should be non-conflicting, non-redundant, coherent, and logical.
2. Develop scoring methodology: Each attribute in the tree structure is assigned a score usually through SME elicitation. The scoring scale should be carefully structured and the rules for scoring must be well defined and consistent. Only the lowest level of the hierarchy structure is scored.
3. Assign weight factors: Often some attributes are more important than others, and therefore

Table 7: Report Card for Multi Criteria Risk Analysis

Multi Criteria Risk Analysis	
NAS Category	N/A
Input	Both
Aggregation	Yes
Weighting	Subjective
Output	Semi-quantitative
Scenario Based	Optional
T, V, C	Optional
Tools	• Analytic hierarchy process • Swing weights • Fuzzy logic • Expert elicitation tools
Implementation Challenges in Cyber	• Selection of attributes, weights and scores is subjective. • Complex problems can have a large number of attributes
Examples	• BTRA 2006 • Nuclear Terrorism Initiative (NTI) • Global Threat Reduction Initiative (GTRI) • Global Nuclear Threat Program (GNTP)
Illustration	See Figure 3.8

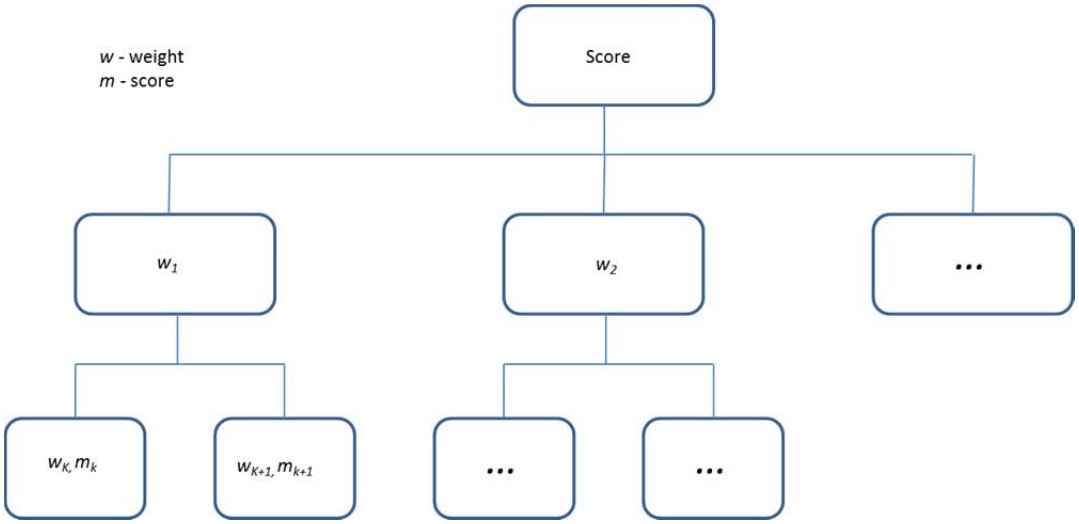


Figure 9: Notional MARA hierarchy tree

should have more contribution to the final risk score. Each attribute and level in the hierarchy structure is assigned a weight factor through SME elicitation. There are several tools that can be used for weight assignment to help remove bias and make the process more consistent, such as analytical hierarchy process and swing weights. Since importance of an attribute can significantly vary by different scenarios, multiple sets of weights, tied to specific scenarios, can be developed.

4. Aggregation: The final risk score is calculated by rolling up all the attributes scores and weights into a single score using an aggregation scheme. The aggregation scheme should account for orthogonality of the attributes, their inter-dependency and redundancy. Typically, the aggregation scheme is some combination of multiplication and addition. The general rule of thumb is that orthogonal attributes should be multiplied, while parallel and independent attributes should be added.

MARA is useful when there are many risk factors because it provides a means for consolidating many factors into a few scores or even a single score. A general MARA tree structure is shown in Figure 9.

The main difference between MARA and MORA is that in MARA, the number of alternative solutions for this type of problem is finite and discrete. In MORA, which is also known as Multiple-Criteria Design problem, the alternatives are not necessarily known, and the number of possible alternatives is infinite, and comes from a continuous set of solutions [43].

Strengths:

- MARA is easy to compute and can be done with simple spreadsheets.
- MARA can deal with more complex risk analysis problems where multiple attributes of opposite directionality contribute to risk.
- MARA combines both objective data and SME judgment.

Weakness:

- In MARA, the selection of measures, weights and aggregation schemes is subjective.

- If wrong attributes are chosen, or weights and scores are not assigned accurately, MARA can give very poor results.

2.7 Risk-Informed Management of Enterprise Security

Risk-Informed Management of Enterprise Security (RIMES) is a Sandia-developed method that provides a structured framework for eliciting and organizing SME feedback to support risk-informed security analysis (e.g., [5], [12], and [45]). It is designed for situations in which few models exist, but there is nonetheless substantial knowledge spread across one or more communities of SMEs. Although this technique has not been used widely, it has been tested and refined through high-consequence security analysis performed at Sandia [5, 12].

RIMES begins with the same basic questions as probabilistic risk analysis (PRA)[2], but it uses difficulty as a proxy for the likelihood of a given adversary attack scenario. This is based on observations suggesting that there is a large class of adversaries who would only launch an attack when success seems reasonably likely. Given a choice between two attacks that generate similar consequences but have different difficulties, these adversaries would choose the less difficult option, making it a more likely attack route. Similarly, as attack scenarios rise in difficulty, there are fewer adversaries capable of succeeding at such attacks, making them less likely. For the presumably large group of adversaries who follow this planning process, the difficulty of an attack serves as a reasonable proxy for its likelihood. By focusing on potential targets and their defenses, this approach also avoids difficulties with generating probabilities that correspond to highly uncertain or rapidly changing properties, such as adversary intent. As shown in Figure 10, the highest risk is associated with easy (low difficulty) attacks capable of generating high consequences. While this method does adopt much of the framework of PRA and has many advantages

Table 8: Report Card for RIMES

RIMES	
NAS Category	N/A
Input	Both
Aggregation	Optional
Weighting	Optional
Output	Quantitative or Semi-quantitative
Scenario Based	Yes
T, V, C	Yes
Tools	• Expert elicitation
Implementation Challenges in Cyber	• May be difficult to develop credible/spanning scenarios • Lack of existing framework and models for cyber security may make it difficult to analyze scenarios
Examples	• Risk-Informed Management of Enterprise Security (RIMES) • Integrated Infrastructure Security (I^2S) • Sandia study on airport security
Illustration	Figure 10: Difficulty/Consequence Plot as used in I2S

[2] As discussed in Section 2.8, PRA is based on three questions: (1) What can happen? (2) How likely is that to happen? and (3) If that does happen, what are the consequences?

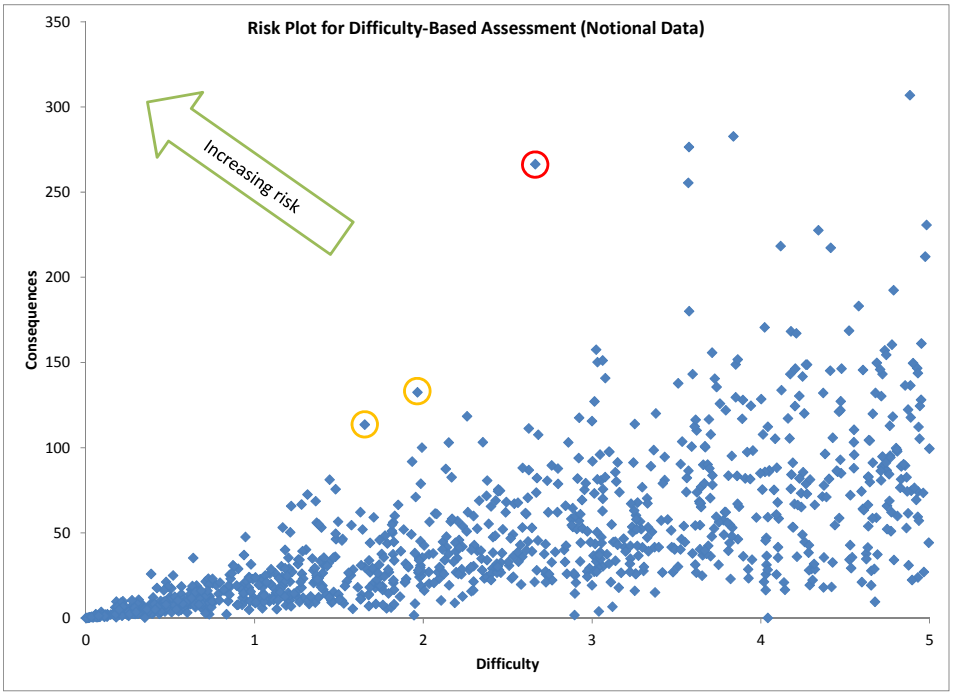


Figure 10: Difficulty/Consequence Plot as used in I²S

Source: Figure 2 from [5]

for security analysis, some security risk analysts remain skeptical that difficulty can or should be used as a proxy for probability [12].

When implementing the RIMES methodology the following steps are necessary [5, 12]:

1. Identify the consequences that are of greatest concern for the given enterprise
2. Generate multiple attack scenarios that can lead to the consequences identified in the first step using SME elicitation. By design, each scenario is assumed to produce a certain consequence, so separate determination of consequences is not needed. Further, only the scenarios that produce the consequences of concern are included, limiting the scenario space and simplifying the analysis.
3. Identify the attributes of a scenario that contribute to the difficulty of successfully executing an attack, such as the following: the number of attackers used in the scenario, the level of training required for attackers, the degree to which the attack must be performed stealthily, etc.
4. Develop scoring guidelines that describe how each of the attributes developed in the previous step should be associated with particular levels of difficulty. For instance, the number of attackers corresponding to a "Level 1" difficulty would be defined. This supports objective and consistent scoring of all of the scenarios. This process is somewhat similar to MARA scoring: important attributes are identified, and a scoring table is assigned for each of those attributes. As in MARA, identifying the right attributes, as well as developing consistent scoring tables is critical for successful implementation.
5. Analysts and SMEs evaluate the relative difficulty of each attack scenario using the scoring tables to promote consistent and reproducible scoring. The scenarios are scored along for individual attribute, and the scores are combined to yield an overall difficulty score. In some

implementations the weighting is not formally defined, and is derived from SME discussion (RIMES, I^2S), while in others it is formally defined (e.g., through a system of weights). The evaluation of difficulty can loosely be interpreted as a scenario-based MARA.

6. Results can be presented as triplets of data, in a scatter plot of difficulty vs. consequences, or as summary statistics.

Although heavily SME-dependent, initial work suggests that this process could be automated by incorporating SME feedback into an expert model [46].

Strengths

- In complex problems, where it is impossible to account for all scenarios and all possible consequences, RIMES offers a compromise by focusing only on scenarios that lead to the consequences of greatest concern.
- Using difficulty as a measure of likelihood reflects observed adversary planning behavior.
- The difficulty of successfully executing a scenario can be judged without requiring detailed knowledge of an adversary's intent, providing a more stable basis for strategic decision-making. Nonetheless, the result is consistent with the traditional threat, vulnerability, and consequence framework for assessing risk.
- The underlying techniques are relatively mature and have been demonstrated successfully in high-consequence security analysis.
- This method is well suited to heavily cross-disciplinary problems and those in which the majority of the available knowledge is scattered across communities of SMEs rather than captured in a model.
- Interim results (such as the set of consequences of concern, the attributes of difficulty, and the scoring tables) provide valuable insights, even before the risk assessment is complete.
- The methodology can be adapted to support automated analysis.
- RIMES represents a modified form of PRA, offering linkage to a widely accepted method of risk assessment, but with adaptations tailored to security analysis. In particular, using difficulty as a proxy for probability may be more intuitive for analysts and decision makers who would be unlikely to trust a PRA based on Bayesian methods.
- The threat component of risk is optional. This can be useful when little or no information is available in the threat domain.

Weaknesses

- This method does not build on the mathematical underpinnings of probability and statistics, as “difficulty” is not a well-defined mathematical concept. This limits its ability to produce meaningful summary statistics and risk metrics, and this may limit its acceptance.
- Some analysts trained in the formal methods of PRA may be suspicious of using difficulty in lieu of probability, potentially leading to claims that this technique does not actually measure “risk.”
- As with PRA, this technique requires a sufficiently complete scenario set to identify the key drivers of risk. If those scenarios are overlooked, the results will underestimate the risk.
- Although RIMES includes techniques for focusing on the most important scenarios, the initial round of assessment is likely to require significant resources.

2.8 Probabilistic Risk Assessment

Probabilistic risk assessment (PRA) seeks to answer three questions ([47]):

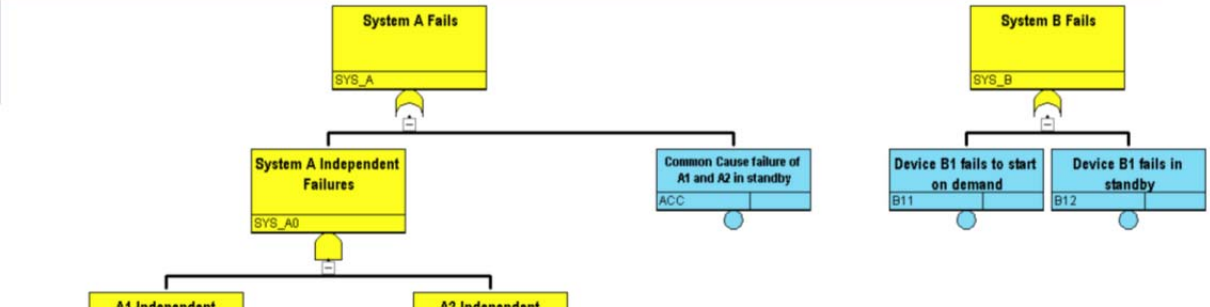
1. What can happen? What can go wrong?
2. How likely is that to happen?
3. If that does happen, what are the consequences?

The answers to these three questions can be framed into the following triplet ([47]):

1. A scenario describing a sequence of events leading to a negative outcome;
2. The probability of that scenario occurring (or a probability distribution function); and
3. The consequences of that scenario playing out to its completion, measured in units that are appropriate to the problem (e.g., lives lost, financial damage, interruption of critical functions, etc.).

The results of PRA can be most fully described by capturing all of the data in these triplets. For instance, a table might be constructed that describes each scenario, along with its probability and consequences (e.g., [47]). Alternately, the data could be captured in a scatter plot in which each point represents a single scenario and the axes are measured in terms of probability and consequences (e.g., [48]). In addition, it is

Table 9: Report Card for Probabilistic Risk Assessment

babilistic Risk Assessment	
Category	Probabilistic/Quantitative risk analysis including fault trees/event trees
t	Both
egation	Yes
ghting	Data-based
but	Quantitative
ario Based	Yes
, C	Yes
s	• Event trees • Fault trees • Monte Carlo simulation • Bayesian probabilities
lementation lenges in er	• Lack of consensus on interpretation of probabilities • Little basis for determining reasonable estimates of probabilities in high-consequence security analyses • Developing credible/spanning set of scenarios may be difficult • For complex problems the number of possible scenarios and corresponding probabilities ca overwhelmingly large
nples	• NRC safety studies of nuclear power plants • Planning studies of NASA missions • Bayesian networks
tration	

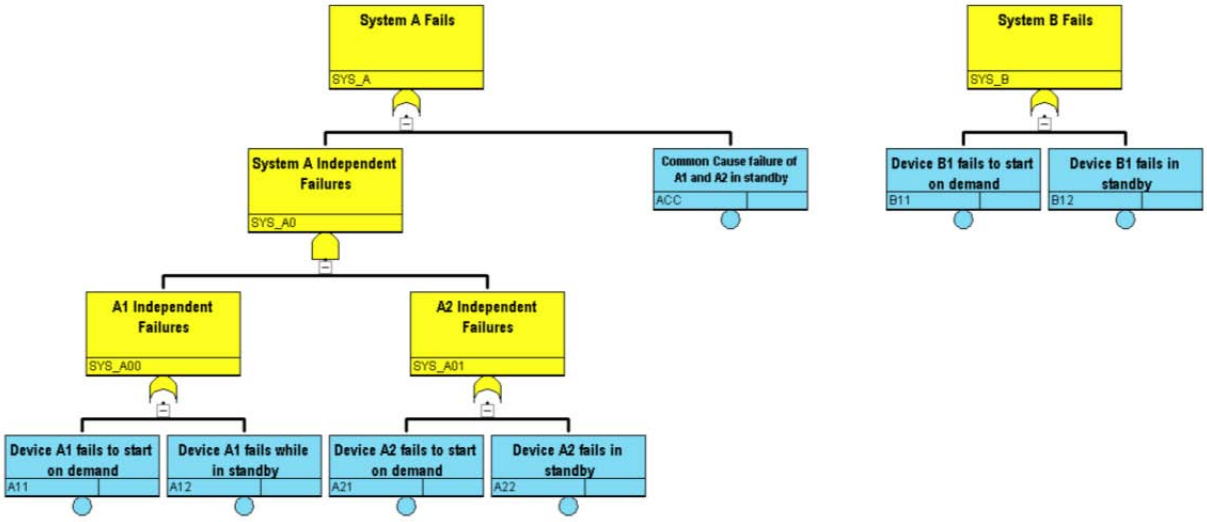


Figure 11: Fault tree used for PRA

Source: Figure 12-4 from [6]

often useful to further analyze these results to produce a variety of summary scores or risk metrics. For instance, the expected loss associated with a set of scenarios can be calculated using a weighted average:

$$\langle C \rangle = \sum_i p_i \, C_i$$

where p_i is the probability of each scenario, and C_i represents the associated consequences (e.g., [12]). Other risk metrics can also be calculated that more closely align with the outcomes of concern. For example, any of the following might be relevant to a particular problem ([6]):

- The probability of an event of a certain magnitude occurring;
- The reasonable "worst case" outcome (e.g., the 95% percentile range of outcomes); or
- A probability distribution function of certain classes of outcomes.

Often these risk metrics represent systems level concerns. Therefore, instead of looking at the probability of failure of a certain component of the system, they might be calculated to determine the probability of having any accident that could lead to the loss of one or more human lives. PRA also offers techniques through which a sensitivity analysis can be used to find "importance measures" that describe the degree to which the output metrics change as a function of the input parameters [6].

PRA grew out of efforts to study the safety of nuclear power plants in the 1970s. Prior to that time, safety analyses tended to focus on reliability by ensuring that there was no single-point failure in critical systems that could lead to a catastrophic outcome. The initiating events leading to these failures were typically viewed as "low probability, high consequence" events. PRA was able to address a broader range of failure scenarios, revealing that multi-point failures consisting of several "high probability, low consequence" initiating events could still trigger catastrophic outcomes. Having a methodology that could capture these events was therefore important [6].

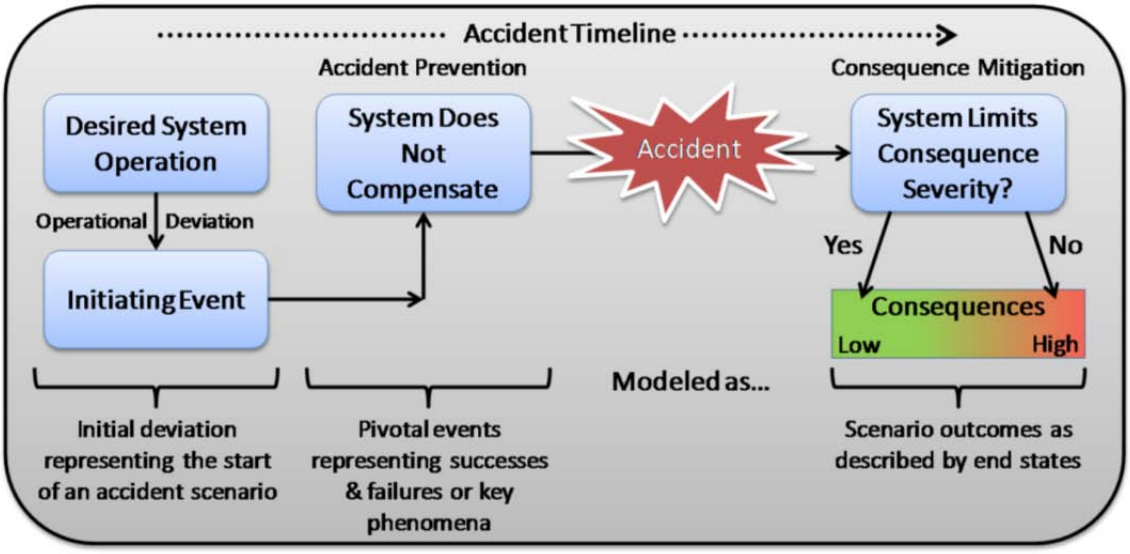


Figure 12: Framework for a PRA scenario

Source: Figure 3-2 from [6]

At the time, the results of PRA were considered controversial, and many of the same concerns survive today. In particular, it can be difficult to identify a complete scenario set, and if the dominant drivers of risk are absent from the scenarios that have been identified, the risk analysis will underestimate the true risk. There have also been long-standing concerns about the ability to quantify input parameters and the uncertainties in those parameters [6].

Within the PRA community, techniques have been developed to address some of these concerns. For instance, a hierarchical approach can support the development of a more complete scenario set by listing all of the critical functions and breaking those down into progressively finer elements until individual failure modes can be identified. Several tools can assist in this process [6]:

- A **master logic diagram** is a hierarchical breakdown describing all of the initiating events that could occur. Implicit in this diagram is a definition of "normal" operations, so that initiating events can be defined as triggers that cause non-normal operating conditions to occur [6].
- An **event tree** provides a mechanism for following through all of the possible cascades of events that could occur after a given initiating event. This helps to model whether the initiating event causes other failures and also provides an opportunity to study potential responses by operating personnel, safety systems, etc. [6].
- A **fault tree** helps to break down high-level descriptions of failure modes (e.g., one of the failures that might occur in an event tree) into the basic events that could contribute to that failure. A basic event might consist of the failure of a particular component or a particular decision by operators. The probability of a basic event occurring should be directly quantifiable from data, preferably described as a probability distribution function to reflect uncertainties in those values. The overall fault tree can then be built up through a series of AND and OR operators that describe how the different basic events can combine to cause higher-level failures [6].

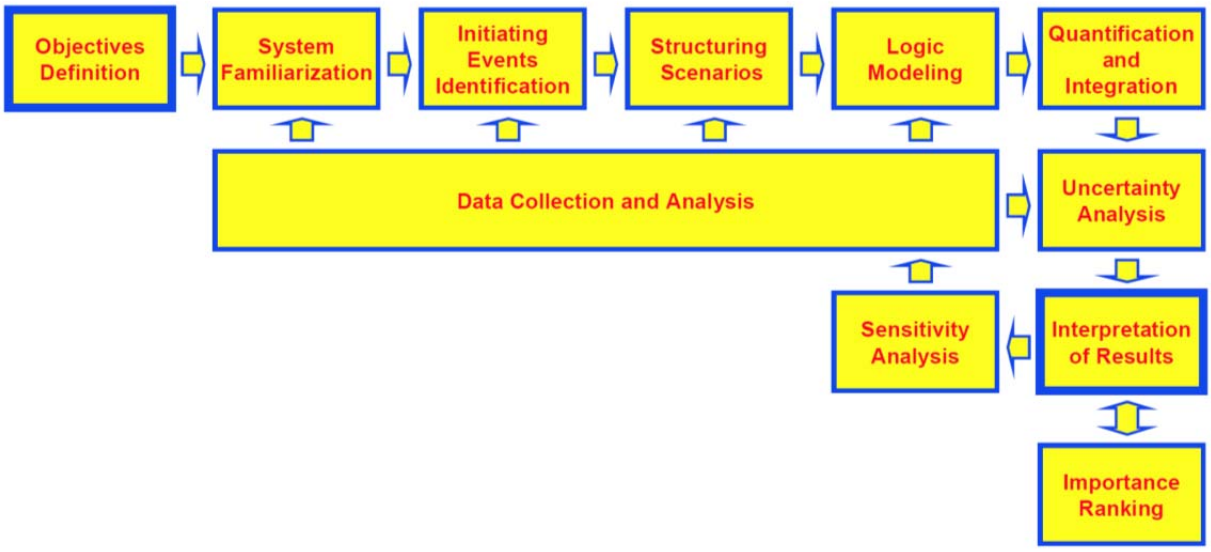


Figure 13: Typical PRA flow

Source: Figure 3-13 from [6]

While each of these logic diagrams can be relatively simple, they must be backed by a larger body of analysis to provide the necessary data. Consequently, it can require substantial effort to collect and research the data needed to perform a PRA [6].

In general, scenario development should be considered a key component of successful PRA. The need for completeness in the scenario set (or at a minimum, the identification of the scenarios that dominate the risk calculation) is sufficiently important that it justifies a substantial effort during the PRA process. Because the set of scenarios can be rather large, computerized analysis of the logic-based hierarchies is likely to be required; one guide to practicing PRA suggests that manual enumeration of all relevant scenarios is “completely impractical” [6].

The determination and propagation of uncertainty also plays a key role in PRA, both at the input and the output, and techniques have been developed to allow uncertainties to be properly reflected in the analysis. For instance, there are two fundamentally different sources of uncertainty that could contribute to the probability of a given scenario. Aleatory (or stochastic) uncertainty represents the natural variability in physical processes while epistemic uncertainty corresponds to uncertainties in the state of knowledge about a certain event. It is important to capture both forms of uncertainty in the PRA [6].

By using probability distribution functions to capture these uncertainties, the outcomes can also be described in terms of a probability distribution function, which may be important in understanding the likelihood of severe outcomes that occur in the tails of the distribution. Additionally, understanding where the largest uncertainties lie provides an opportunity for the decision-maker to decide to “buy down” the uncertain by funding additional research and modeling [6].

Overall, PRA has demonstrated substantial success in a variety of high-consequence safety analyses. Over several decades of practice, a large body of knowledge, supported by many tools and techniques, has developed around the practice of PRA. Moreover, although there does not seem to be a universally accepted quantification of risk, the framework used in PRA – in which risk is assessed as the set of

probabilities and consequences associated with a range of scenarios – is viewed by many as representing the "formal" mathematical definition of risk.

Despite these successes and widespread acceptance, challenges remain in developing a complete set of scenarios and in quantifying the parameters needed for PRA. While there are methods for addressing these challenges, some risk practitioners remain uncomfortable using PRA for certain types of analysis, often for these reasons [6, 12].

Some risk assessments incorporate the threat, vulnerability, and consequence framework (described in Section 1.2) by defining risk as "threat times vulnerability times consequence" (see, e.g., [49]). Typically, this is achieved by mathematically defining "threat" as the probability that an adversary will attempt an attack, with "vulnerability" defined as the probability that an attack would succeed, given that it is attempted (e.g., [11]). Consequences are estimated by determining the outcome that would be caused by a successful attack. This formulation of risk is consistent with probabilistic risk assessment, although it does require that "threat" and "vulnerability" carry dual definitions representing both their standard English meanings, as well as their mathematical definitions.

Strengths:

- PRA benefits from a large body of practitioners who have built up substantial experience, tools, and techniques over decades of use.
- PRA has a proven track record in safety analysis.
- The PRA formulation has widespread acceptance as the *de facto* definition of risk.
- PRA builds on well understood mathematical principles of probability and statistics.
- Given appropriate inputs, PRA allows high-level questions to be answered in a way that is likely to be meaningful to decision-makers.

Weaknesses:

- PRA requires a complete set of scenarios (or at least a set of scenarios that includes the dominant risk drivers); if the dominant contributors to risk are not identified, the risk analysis could significantly underestimate the risk.
- PRA requires quantification of probabilities, which works well in safety analysis but has proven difficult in security analyses. Although Bayesian probabilities can be used in such cases, many analysts and decision-makers remain uncomfortable with the seeming subjectivity of Bayesian techniques.

3 RISK ASSESSMENT TOOLS

3.1 Causal Loop Diagrams (Systems Dynamics)

NAS Category: Influence Diagrams

A causal loop diagram aids in visualizing how interrelated variables affect one another. The diagram consists of a set of nodes representing variables connected together. The relationship between these variables can be positive (nodes are changing in the same direction) or negative (nodes are changing in the opposite direction). To determine whether a causal loop diagram is reinforcing or balancing, one can start with an assumption (e.g. “Node 1 is increasing”) and follow the loop around. The loop is reinforcing if after going around the loop, one ends up with the same result as the initial assumption. The loop is balancing if the result contradicts the initial assumption [50].

Causal loop diagrams can be used in risk assessment to see how different attributes contribute to risk and relate to each other, and it can indicate the directionality of risk (i.e., risk increases or risk decreases) as some of the variables change. Causal loop diagrams have been used by the DHS office of policy to illustrate cyber risk, terrorism risk, natural disaster risk and epidemic risk.

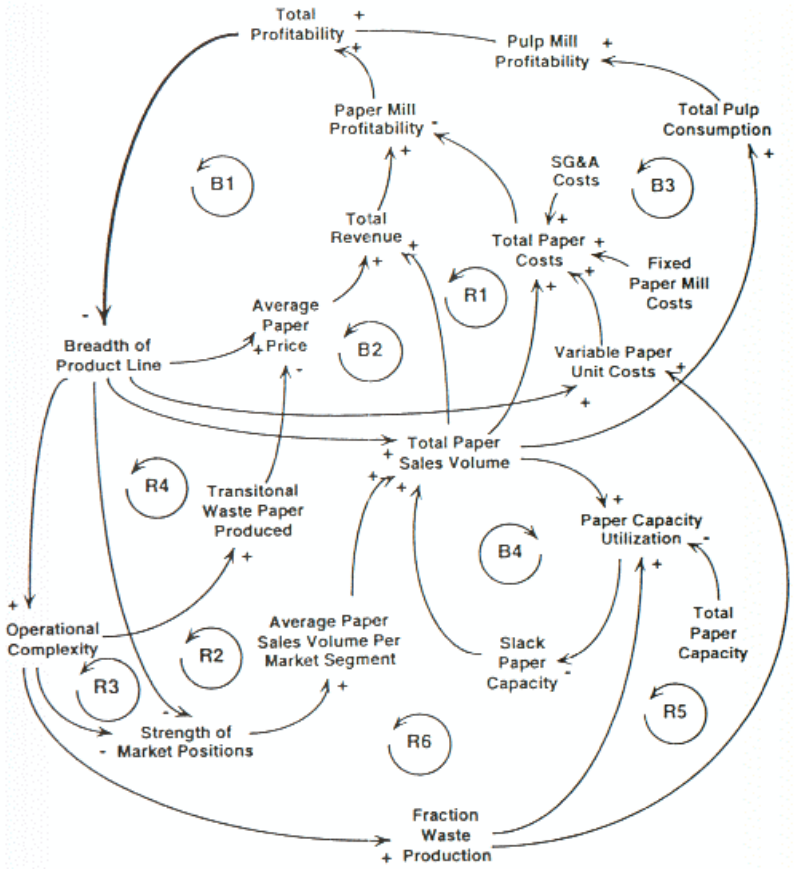


Figure 14: Example of a causal loop diagram

Source: Figure 3 from [8], reproduced as Figure 18 in [10]

3.2 Expert Elicitation

See Section 2.3.

3.3 Fuzzy Logic

NAS Category: N/A

Fuzzy logic is a form of logic where variables can have degrees of truthfulness between zero and one. In contrast to the standard logic, fuzzy logic measures the degree of membership of the set [51].

Frequently in risk assessment obtaining data is a crucial step and quantitative data is often not available. While qualitative data is more easily obtainable, it is often subjective, inaccurate, or subject to uncertainty. Fuzzy logic can provide a framework for handling such subjectivity and uncertainty [52].

3.4 Game Theory

NAS Category: Economic game theory models

Game theory provides a mathematical tool for modeling the strategic interactions of rational decision makers [53]. It can be useful for supporting a risk assessment when outcomes depend on strategic interactions between attacker and defender (e.g., [54]).

3.5 Bayesian Statistics

NAS Category: Bayesian techniques

There are several well-understood schools of thought regarding the interpretation of probabilities. In the "frequentist" interpretation, probabilities can be estimated from historical data. For instance, the probability of rolling a certain value on a die might be based on experiments in which the die was rolled many times and the results were recorded. The "classical" interpretation allows probabilities to be based on the identification of equivalent outcomes. In this view, the probability of rolling a certain value on a die might be based on a physical argument that the die is symmetrically constructed such that all of the faces are equally probable. These approaches to statistics are commonly used in the physical sciences, as they implicitly assume that probabilities can be objectively represented, independent of the experimenter [3, 55, 56].

In contrast, the "Bayesian" (or "subjective") interpretation argues that probabilities reflect the subjective beliefs of the experimenter, in which case the methods and mathematics of statistics can be used to propagate those beliefs in a rational manner. Under the Bayesian approach, an experimenter might believe that a six-sided die is a fair die and will therefore define a "prior probability" that there is a one-sixth probability of rolling a six. This estimate of probability could be based on experiment or analysis of the die, but it could also be based solely upon the experimenter's belief that the person providing the die is honest. If the experimenter then rolled the die 100 times, never producing a six, Bayesian statistics could be used to calculate an updated value for the probability of rolling a six (known as the "posterior probability"). In this way, Bayesian statistics tells the experimenter how to update his or her assumptions about the world as new information is acquired [3, 6, 56].

Because it allows the formalism of statistics to be used with subjective inputs, the Bayesian interpretation of probabilities can provide important means of executing quantitative assessments, such as PRA, even when historical data is lacking. However, this subjectivity may expose the results to significant criticism,

although rigorous methods of expert elicitation may improve acceptance [3, 57, 58]. Sensitivity analyses can be particularly important when using Bayesian statistics, as they reveal the degree to which the input assumptions affect the results (e.g, [59]).

3.6 Fault Trees

NAS category: Probabilistic/Quantitative risk analysis including fault trees/event trees

See Section 2.8.

3.7 Event Trees

NAS category: Probabilistic/Quantitative risk analysis including fault trees/event trees

For event trees, also see Section 2.8.

Event trees are used to identify possible sequences of events and the associated outcomes. Typically, each node in the event tree corresponds to an implied question (“does X happen?”), and the two branches leading out of that node represent the states corresponding to “yes” and “no” answers to that question. If appropriate to the situation, more than two output branches can be defined, as long as they are mutually exclusive [6].

3.8 Attack Graphs

NAS Category: N/A

Attack graphs can help to visualize and generate attack scenarios. By systematically describing the prerequisites and effects of individual steps in a possible attack, attack graphs describe potential adversary actions. Automated algorithms can then be used to develop and prioritize potential attack scenarios. Attack graphs can be used to support red teaming and to support scenario development for a scenario-based risk assessment [60-63].

3.9 Prediction Markets

NAS Category: Lotteries/bet preferences

Prediction markets rely on the collective results of individuals making rational economic choices to predict the probability of a particular outcome or the value of a parameter. For instance, participants might be asked to trade shares in a virtual stock market or to place bets on certain results. The pricing of different shares (or the odds being given on certain bets) can be used as a basis for estimating the desired values. This technique has been applied in a variety of contexts, and is often considered to provide useful results, particularly when certain assumptions are satisfied. However, attempts to use this technique in national security decisions have faced sufficient political backlash [64, 65].

The Wikipedia article on prediction markets provides the following comparison of expert elicitation techniques:

> A series of laboratory experiments to compare the accuracy of prediction markets, traditional meetings, the Delphi method, and the nominal group technique on a quantitative judgment task, found only small differences between these four methods. Delphi was most accurate, followed by NGT [nominal group technique] and prediction markets. Meetings performed worst. The study also looked at participants' perceptions of the methods. Prediction markets were rated least

favourable: prediction market participants were least satisfied with the group process and perceived their method as the most difficult. [65]

3.10 Scenario Planning

NAS Category: Scenario Envisioning

One method of making decisions in the face of uncertainty is to identify two or three "axes" that capture the major dimensions of uncertainty. Potential futures can then be envisioned by considering different outcomes along each of those axes [66, 67].

As an example, someone planning for retirement might face uncertainty regarding the value of investments. Potential futures could then be represented by the following table:

	Stock market goes up	Stock market goes down
Housing market goes up	Scenario A	Scenario B
Housing market goes down	Scenario C	Scenario D

Each of the four potential outcomes (labeled A through D) could then be used as a source of discussion to identify potential strategies, risks, etc. The conditions of each scenario could be considered in an abstract sense (as shown in the table), or they could be used as the basis for more detailed scenarios.

This technique can provide a framework for identification of relevant scenarios, enumeration of risks, and elicitation of SME feedback.

3.11 Sensitivity Analysis

NAS Category: N/A

In many assessments, the inputs are highly uncertain. A sensitivity analysis helps clarify the impact that this uncertainty has on the results. As an example, the assessment could be repeated using different input values that span the range of uncertainties. If the results are found to be robust against changes in the inputs, the results of the assessment can be accepted with a high degree of confidence. The sensitivity analysis can also reveal which uncertainties have the greatest impact on the results, providing a basis for identifying where it would be worthwhile to invest in reducing uncertainties on input parameters. In a quantitative risk assessment (such as PRA), the sensitivity analysis can produce probability distributions over the likely outcomes, which are often quite valuable [6, 68].

3.12 Reliability Analysis

NAS Category: Stochastic processes (reliability, system availability, extreme value theory)

Reliability analysis is used to calculate the probability that a component will function as specified past a certain time. It can be used to prioritize improvements in the design and to focus resources and maintenance efforts on components that are most likely to fail or malfunction. It can also be used to estimate the rate at which components are expected to malfunction and what impact the overall system will experience due to these failures [69].

4 CONCLUSIONS

The choice of an appropriate risk assessment methodology depends heavily on the given problem, and the implementation or a risk assessment will vary significantly as practitioners adapt the technique to the system being studied. As a starting point for selecting a methodology, Table 10 summarizes basic characteristics of the methodologies discussed in this document. This table can be used to quickly identify viable methodologies for a particular problem (or quickly rule out methodologies that are not applicable).

Table 10: Methodology Comparison

	Input	Aggregation	Weighting	Output	Scenario Based	T, V, C
Adherence to Best Practices	Both (SME and/or Data)	No	None	Qualitative	No	No
Reputational or Historical Analysis	Both (SME and/or Data)	Optional	Optional	Any (Quantitative, Semi-quantitative, or Qualitative	No	No
Expert Judgment	SME	Optional	Subjective or None	Any (Quantitative, Semi-quantitative, or Qualitative)	Optional	Optional
Risk Factors	Both (SME and/or Data)	No	Subjective or None	Qualitative	No	No
Risk Factors with Regression Analysis	Both (SME and/or Data)	Yes	Data-based	Quantitative or Semi-quantitative	No	No
Multi Criteria Risk Analysis	Both (SME and/or Data)	Yes	Subjective	Semi-quantitative	Optional	Optional
Risk-Informed Management of Enterprise Security (RIMES)	Both (SME and/or Data)	Optional	Optional	Quantitative or Semi-quantitative	Yes	Yes
Probabilistic risk assessment (PRA)	Both (SME and/or data)	Yes	Data-based	Quantitative	Yes	Yes

Another critical factor in choosing a particular methodology is the availability and quality of relevant input data. Although difficult to systematically quantify, some methodologies seem better suited to initial assessments of systems that are poorly understood, while others are better able to fully use a high-quality data set describing a well-understood system. Figure 15 gives a qualitative impression of these trade-offs by notionally illustrating the level of data and system understanding that is required by each methodology to achieve a certain level of fidelity in the risk assessment. The two dotted lines correspond to the fidelity that could reasonably be achieved by a particular deadline (the “August target”) as well as the fidelity that seems likely to be achievable with further study (the “reasonable limit”).

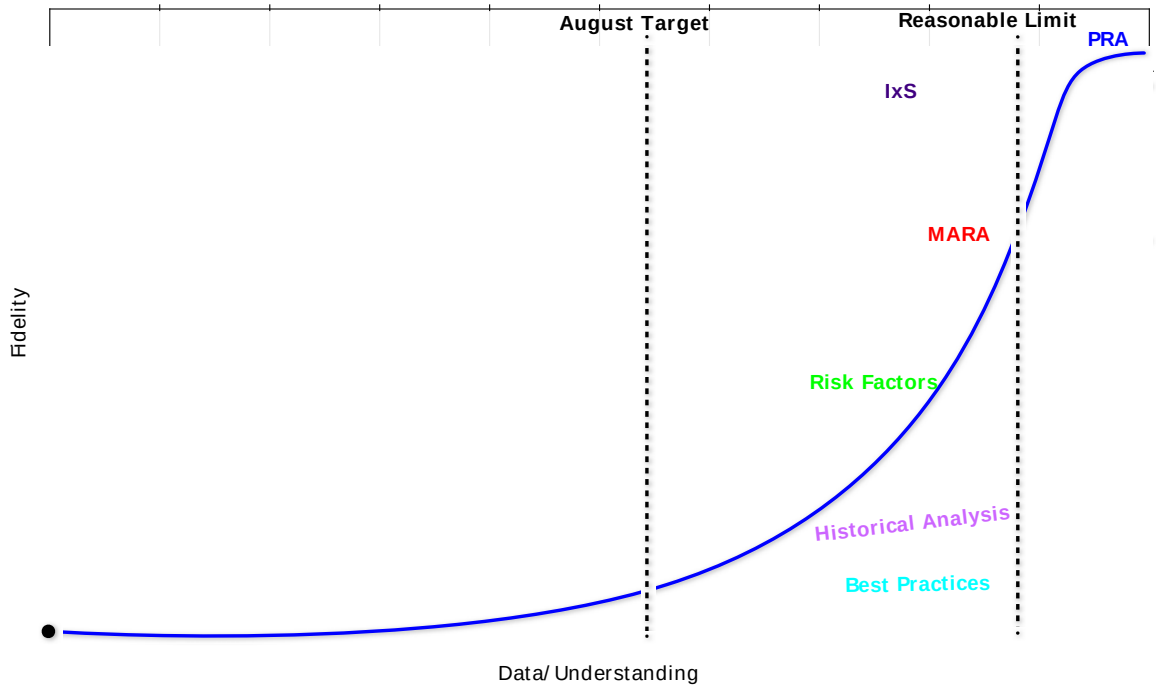


Figure 15: Qualitative comparison of methodologies' fidelity as a function of input data and/or understanding of system

5 REFERENCES

1. U.S. Department of Agriculture (USDA). http://www.nal.usda.gov/fnic/Fpyr/pyramid.gif.
2. Cartagena, D., *14542*, 2012, Centers for Disease Control and Prevention (CDC), Public Health Image Library (PHIL). http://phil.cdc.gov/phil/home.asp.
3. U.S. Department of Homeland Security. *DHS Risk Lexicon: 2010 Edition* 2010; http://www.dhs.gov/dhs-risk-lexicon (direct link: http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf).
4. National Research Council Committee to Review the Department of Homeland Security's Approach to Risk Analysis, *Review of the Department of Homeland Security's Approach to Risk Analysis*2010: The National Academies Press. http://www.nap.edu/openbook.php?record_id=12972.
5. Sumner, M. and S.P. Gordon, *Integrated Infrastructure Security (I^2S): A Risk-Based Approach to Prioritization of Cybersecurity Allocations for Critical Infrastructure*, 2013, Sandia National Laboratories: Albuquerque NM, SAND2013-3987.
6. Stamatelatos, M., H. Dezfuli, G. Apostolakis, C. Everline, S. Guarro, D. Mathias, A. Mosleh, T. Paulos, D. Riha, C. Smith, W. Vesely, and R. Youngblood, *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners (Second Edition)*, 2011, NASA (U.S. National Aeronautics and Space Administration). http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20120001369_2012001000.pdf.
7. *USDA Food Pyramid.gif*. 2006; http://en.wikipedia.org/wiki/File:USDA_Food_Pyramid.gif [accessed 2013 Oct. 2].
8. Risch, J.D., L. Troyano-Bermúdez, and J.D. Sterman, *Designing corporate strategy with system dynamics: a case study in the pulp and paper industry.* System Dynamics Review (Wiley), 1995. **11**(4): p. 249-274.
9. Ebay, Inc. *Feedback scores, stars, and your reputation*. http://pages.ebay.com/help/feedback/scores-reputation.html [accessed 2013 Sept. 6].
10. Radzicki, M.J. and R.A. Taylor. *U.S. Department of Energy's Introduction to System Dynamics: A Systems Approach to Understanding Complex Policy Issues ("Feedback" page)*. 1997; http://www.systemdynamics.org/DL-IntroSysDyn/feed.htm [accessed 2013 Sept. 27].
11. U.S. Department of Homeland Security. *National Infrastructure Protection Plan*. 2009; http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.
12. Wyss, G.D., J.P. Hinton, K. Guzman, J.F. Clem, J.L. Darby, C.J. Silva, K.W. Mitchiner, J.H. Gauthier, and J.P. Eddy, *Risk-Based Cost-Benefit Analysis for Security Assessment and Investment Prioritization*, 2011, Sandia National Laboratories. p. 138, SAND2011-0003.
13. Wyss, G.D., D.J. Pless, R.E. Rhea, C.J. Silva, P.G. Kaplan, R. Aguilar, and S.H. Conrad, *Total risk assessment methodology*, 2009, Sandia National Laboratories: Albuquerque, NM, SAND2009-0178.
14. SANS Institute. *The Critical Security Controls: Twenty Critical Security Controls for Effective Cyber Defense*. http://www.sans.org/critical-security-controls/ [accessed 2013 Sept. 6].
15. SANS Institute. *A Brief History Of The 20 Critical Security Controls*. http://www.sans.org/critical-security-controls/history.php [accessed 2013 Sept. 6].
16. Teaching and Learning with Technology at Penn State University and the University of Calgary, *7 Things You Need to Know about Social Rating Systems*. http://ets.tlt.psu.edu/wp-content/uploads/socialratings1.pdf.
17. Mills, E., *Study: eBay sellers gaming the reputation system?*, in *CNET*2007. http://news.cnet.com/8301-10784_3-6149491-7.html.
18. Streitfeld, D., *The Best Book Reviews Money Can Buy*, in *The New York Times*2012. http://www.nytimes.com/2012/08/26/business/book-reviewers-for-hire-meet-a-demand-for-online-raves.html.

19. Enterprise Risk Management Initiative Faculty and B. Taylor. *Reputation Risk Management*. http://www.poole.ncsu.edu/erm/index.php/articles/entry/reputation-manage-risk/ [accessed Oct. 2 2013].
20. Milestone Internet Marketing, Inc. *eBuzz Connect*. 2011; http://www.ebuzzconnect.com/ [accessed 2013 Oct 1].
21. United States Environmental Protection Agency, *Unfinished Business: A Comparative Assessment Of Environmental Problems (Overview Report)*, 1987, 000R87901. http://nepis.epa.gov/Exe/ZyPURL.cgi?Dockey=2001635G.txt.
22. Florig, H.K., M.G. Morgan, K.M. Morgan, K.E. Jenni, B. Fischhoff, P.S. Fischbeck, and M.L. DeKay, *A Deliberative Method for Ranking Risks (I): Overview and Test Bed Development.* Risk Analysis: An International Journal, 2001. **21**(5): p. 913-913.
23. Cox, L.A., *What's wrong with risk matrices?* Risk Analysis, 2008. **28**(2): p. 497-512.
24. U.S. Department of Defense, *Standard Practice for System Safety*, 2000. https://acc.dau.mil/adl/en-US/255833/file/40632/MIL-STD-882D.pdf.
25. Smith, R.E., *Update on Revisions to MIL-STD-882*, in *NDIA 11th Annual Systems Engineering Conference*2008: San Diego, CA. http://www.dtic.mil/ndia/2008systems/RobertSmith.pdf.
26. Rochester Institute of Technology, Department of Outreach Education and Training *Cost Benefit Analysis*. https://www.rit.edu/~w-outrea/training/Module5/M5_CostBenefitAnalysis.pdf [accessed 2013 Sept. 6].
27. Dalkey, N.C., *The Delphi Method: An Experimental Study of Group Opinion*, 1969, RAND Corporation: Santa Monica, CA. http://www.rand.org/pubs/research_memoranda/RM5888.
28. RAND Corporation. *Delphi Method*. 2011; http://www.rand.org/topics/delphi-method.html [accessed 2013 Sept. 9].
29. Linstone, H.A. and M. Turoff, eds. *The Delphi Method: Techniques and Applications*. 2002. http://is.njit.edu/pubs/delphibook/delphibook.pdf.
30. *Delphi Method*. 2013; http://en.wikipedia.org/wiki/Delphi_method [accessed 2013 Sept. 9].
31. Rowe, G. and G. Wright, *The Delphi technique as a forecasting tool: issues and analysis.* International Journal of Forecasting, 1999. **15**(4): p. 353-375.
32. Herrmann, A., *The Quantitative Estimation of IT-Related Risk Probabilities.* Risk Analysis, 2013. **33**(8): p. 1510-1531.
33. *Red team*. 2013; http://en.wikipedia.org/wiki/Red_team [accessed 2013 Sept. 27].
34. *Red Teaming and Alternative Analysis*. http://redteamjournal.com/about/red-teaming-and-alternative-analysis/ [accessed 2013 Sept. 27].
35. *Penetration test*. 2013; http://en.wikipedia.org/wiki/Penetration_test [accessed 2013 Sept. 27].
36. *Risk factor*. 2013; http://en.wikipedia.org/wiki/Risk_factor [accessed 2013 Sept. 26].
37. Kindinger, J.P. and J.L. Darby, *Risk Factor Analysis—A New Qualitative Risk Management Tool*, in *Project Management Institute Annual Seminars & Symposium*2000, Project Management Institute: Houston. http://marketplace.pmi.org/Pages/ProductDetail.aspx?GMProduct=00100297600 and https://www.lanl.gov/orgs/d/d5/documents/risk-fact.pdf.
38. *Risk factor (criminology)*. 2012; http://en.wikipedia.org/wiki/Risk_factor_(criminology) [accessed 2013 Oct. 2].
39. Centers for Disease Control and Prevention (CDC). *Lung Cancer*. 2013; http://www.cdc.gov/cancer/lung/basic_info/risk_factors.htm [accessed 2013 Sept 6].
40. *Epidemiology*. 2013; http://en.wikipedia.org/wiki/Epidemiological [accessed 2013 Sept. 26].
41. Kleinberg, S. and G. Hripcsak, *A review of causal inference for biomedical informatics*. Journal of Biomedical Informatics, 2011. **44**(6): p. 1102-1112.
42. *Risk factor (finance)*. 2013; http://en.wikipedia.org/wiki/Risk_factor_(finance) [accessed 2013 Oct. 2].
43. *Multi-criteria decision analysis*. 2013; http://en.wikipedia.org/wiki/Multi-criteria_decision_analysis [accessed 2013 Sept. 6].

44. U.S. Department of Homeland Security, Biological Threat Characterization Center of the National Biodefense Analysis and Countermeasures Center, *Bioterrorism Risk Assessment*, 2006: Fort Detrick, MD. http://www.dhs.gov/dhs-risk-lexicon (direct link: http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf).
45. Wyss, G.D., J.F. Clem, J.L. Darby, K. Dunphy-Guzman, J.P. Hinton, and K.W. Mitchiner. *Risk-based cost-benefit analysis for security assessment problems*. in *2010 IEEE International Carnahan Conference on Security Technology (ICCST)*. 2010.
46. Sumner, M., *Unpublished work*, 2013.
47. Kaplan, S. and B.J. Garrick, *On The Quantitative Definition of Risk.* Risk Analysis, 1981. **1**(1): p. 11-27.
48. World Economic Forum, *Global Risks 2012 (Seventh Edition)*, 2012. http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf.
49. Cox, L.A., *Some Limitations of "Risk = Threat x Vulnerability x Consequence" for Risk Analysis of Terrorist Attacks.* Risk Anal. **28**(6): p. 1749-1761.
50. *Causal loop diagram*. 2013; http://en.wikipedia.org/wiki/Causal_loop_diagram.
51. Pokorádi, L., *Fuzzy logic-based risk assessment.* Academic and Applied Research in Military Science, 2002. **1**(1): p. 63-73.
52. Bajpai, S., A. Sachdeva, and J.P. Gupta, *Security risk assessment: Applying the concepts of fuzzy logic*. Journal of Hazardous Materials, 2010. **173**(1-3): p. 258-264.
53. *Game Theory*. 2013; http://en.wikipedia.org/wiki/Game_theory [accessed 2013 Sept. 27].
54. Nochenson, A. and C.F.L. Heimann *Simulation and Game-Theoretic Analysis of an Attacker-Defender Game*.
55. Hájek, A., *Interpretations of Probability*, in *The Stanford Encyclopedia of Philosophy*, E.N. Zalta, Editor 2012. http://plato.stanford.edu/entries/probability-interpret/.
56. *Probability interpretations*. 2013; http://en.wikipedia.org/wiki/Philosophy_of_probability [accessed 2013 Sept. 27].
57. Keeney, R.L. and D. Vonwinterfeldt, *Eliciting Probabilities from Experts in Complex Technical Problems.* IEEE Transactions on Engineering Management, 1991. **38**(3): p. 191-201.
58. Kaplan, S., *'Expert information' versus 'expert opinions'. Another approach to the problem of eliciting/ combining/using expert knowledge in PRA.* Reliability Engineering & System Safety, 1992. **35**(1): p. 61-72.
59. *Robust Bayesian analysis*. 2013; http://en.wikipedia.org/wiki/Robust_Bayesian_analysis [accessed 2013 Sept. 27].
60. Swiler, L.P., C. Phillips, D. Ellis, and S. Chakerian. *Computer-attack graph generation tool*. in *DARPA Information Survivability Conference & Exposition II (DISCEX '01)*. 2001.
61. Swiler, L.P., C.A. Phillips, and T.R.M. Gaylor, *A graph-based network-vulnerability analysis system*, in *Graph based network vulnerability analysis system*1997, Sandia National Laboratories: Albuquerque NM, SAND97-3010C.
62. *Scenario and Attack Graphs*. http://www.cs.cmu.edu/~scenariograph/ [accessed 2013 Sept. 27].
63. Heath, Z., J. Letchford, A. Smith, and Y. Vorobeychik, *SANDMAN (Attack Planner) Brief*, 2013, Sandia National Laboratories.
64. *Policy Analysis Market*. 2013; http://en.wikipedia.org/wiki/Policy_Analysis_Market [accessed 2013 Sept. 27].
65. *Prediction market*. 2013; http://en.wikipedia.org/wiki/Prediction_market [accessed 2013 Sept. 27].
66. *Scenario Planning*. 2013; http://en.wikipedia.org/wiki/Scenario_planning [accessed 2013 Sept. 27].
67. *Futurology: Scenario*. http://future.wikia.com/wiki/Scenario [accessed 2013 Sept. 27].
68. *Sensitivity analysis*. 2013; http://en.wikipedia.org/wiki/Sensitivity_analysis [accessed 2013 Sept. 27].

69. *Reliability engineering*. 2013; http://en.wikipedia.org/wiki/Reliability_engineering [accessed 2013 Sept. 27].

6 DISTRIBUTION

1	MS0899	Technical Library	9536 (electronic copy)


Sandia National Laboratories