Survey of Cyber Risk Analysis Techniques for Use in the Nuclear Industry

Shannon Eggers[a] and Katya Le Blanc[b]

Idaho National Laboratory, P.O. Box 1625, Idaho Falls, ID 83415,
[a]Shannon.Eggers@inl.gov (corresponding author), [b]Katya.LeBlanc@inl.gov

Abstract*: Using traditional probabilistic risk analysis methods for severe accident safety risk management on non-digital systems, structures, and components at nuclear power plants is well-established. In contrast, cyber risk analysis of digital assets is still an immature field with unproven techniques due, in part, to the continuously changing threat environment and the challenge of digital assets failing in unexpected ways. As the nuclear fleet continues to adopt digital instrumentation and control systems, it is increasingly important to have effective and efficient cyber risk analysis techniques to support risk management decisions, such as risk elimination by system redesign or risk mitigation by implementation of prioritized security controls. To understand the state of the art in cyber risk analysis for future research, we surveyed 36 publications across ten application domains. We describe our survey methodology and rate each technique based upon scope, adoptability, and repeatability. We examine the unique constraints of the nuclear industry and outline the strengths and weaknesses of using the cyber risk analysis techniques in the industry, highlighting gaps with current techniques. We also discuss challenges and potential research directions for advancing the science for both existing and new advanced reactors.*

Keywords: Cyber Risk Analysis, Nuclear Cybersecurity, Digital I&C

1 INTRODUCTION

Globally, 78% of the 442 operational nuclear power reactors began commercial operation prior to 2001 (IAEA, 2021). In the U.S., all but one of the 95 operating nuclear power reactors began commercial operation prior to 1997. Fleet modernization efforts, including replacement of analog with digital technology, are underway to reduce operation and maintenance costs, improve efficiencies, and replace aging equipment. In addition, it is anticipated that advanced nuclear plants, such as generation III+ and IV reactors with large, small modular, and micro reactor designs, will primarily use digital instrumentation and control (I&C) systems. While the installation of digital technology improves the reliability of nuclear power plants (NPPs), this technology introduces new risks due to cyber vulnerabilities.

Risk is inherent in all aspects of an organization, regardless of industry or sector. Risk management is the standard practice of analyzing, evaluating, and treating risk to minimize the negative effects of loss from adverse financial, operational, environmental, political, organizational, cyber, or other similar events. However, despite the fact there are over 200 risk management methods and guidelines throughout the world (Paul and Vignon-Davillier, 2014), there are still limitations in nuclear I&C cyber risk analysis approaches.

U.S. NPPs are required to provide high assurance that critical digital assets (CDAs) are adequately protected against cyber-attacks (NRC, 2009). In addition to providing protection against radiological sabotage, adequate identification of risks from both inadvertent and deliberate cyber incidents will enable plants to implement a risk-informed approach to establishing countermeasures.

This literature survey was performed to provide the current state of the art on cyber risk analysis techniques for I&C systems, specifically as they relate to NPPs. However, to ensure techniques were not arbitrarily excluded, cyber risk analysis research related to information and communications technology (ICT) was included.

Our goal in this literature survey was to evaluate cyber risk analysis techniques based on three primary criteria:

1. Scope. Is the entire cyber risk issue space covered? Does the technique consider all consequences, beyond just safety or security? Are all hazards considered, including both deliberate and inadvertent actions?
2. Adoptability. Can the technique be readily implemented at an NPP? If so, what is the level of rigor or ease of implementation while maintaining appropriate coverage of the issue space? And, what is the technology readiness level (TRL)?
3. Repeatability. How repeatable is the process? Is the technique easily repeated to provide ongoing evaluation of relative risk upon changes to threats, vulnerabilities, or risk treatments? If the technique is repeated by different analysts, are the same or similar results obtained? Likewise, if the technique uses expert elicitation or specific source data, how repeatable is the process?

Similar to the value tree for defining degrees of risk-informed by Szilard *et al.* (Szilard et al., 2015), we rate each technique based on these criteria to provide an overall score, with the intent to highlight gaps in current state-of-the-art cyber risk analysis (Figure 1).

The remainder of this paper is organized as follows: Section 2 steps through a background on traditional risk analysis and severe accident risk analysis prior to providing an overview of cyber risk analysis and its mapping to traditional risk analysis. Section 3 provides an overview of current standards and guidelines for industrial control systems (ICS) generically and the nuclear industry specifically. Section 4 describes the survey methodology, while Section 5 provides further detail on each criterion along with an analysis of the results. Section 6 identifies gaps in the techniques and Section 7 provides a discussion on their adoption in the nuclear industry. Section 8 provides conclusions and a brief discussion of future work.

2 BACKGROUND

2.1 Traditional Risk Management

As shown in Figure 2, risk management is the process by which organizations (1) identify possible risks to assets, (2) evaluate these risks against their risk tolerance, and (3) respond to the risk based upon their tolerance. Risk management is a mature field that has existed for almost 40 years. While definitions of risk vary, Kaplan and Garrick define risk as the “possibility of loss or injury” and the “degree of probability of such a loss” (Kaplan, 1997).

Step 1, risk analysis, traditionally uses a methodology that answers three questions posed by Kaplan and Garrick (Kaplan and Garrick, 1981):

- What can go wrong?
- What is the likelihood it will go wrong?
- What are the consequences if it goes wrong?

Thus, as indicated by Equation 1, risk is the complete set of triplets including the scenario (or undesired event), likelihood (or probability of the scenario), and consequences (or impact of the scenario).

$$Risk = f(scenario, likelihood, consequence) \quad (1)$$

In step 2, risk evaluation, an organization rates its risk exposure against its risk tolerance to determine the risk significance of an event or events. Although risk evaluation includes prioritizing the risks based on likelihood and consequence, it is important to recognize the risk is not simply the product of probability and consequence, but rather a function of probability and consequence. For example, a low-probability, high-consequence event resulting in fatalities will have a much different risk significance to an organization than a high-probability, low-consequence event despite potentially having the same result when multiplying consequence ratings by probability. Moreover, the 'scenario' portion of the triplet definition explicitly specifies what must be prevented via risk management.

Step 3 of the risk management process includes determination of the risk response or risk treatment. After identifying and evaluating risks, an organization typically has four choices for responding to the risk—risk acceptance, risk avoidance or elimination, risk transfer, or risk mitigation. Risk mitigation involves reducing the likelihood and/or severity of the consequence by implementing changes or controls in the organization or process. An organization balances many factors when determining risk treatments, such as risk tolerance, regulatory requirements, and cost.

2.2 Traditional Severe Accident/Safety Risk Analysis

Historically, safety concerns in the aerospace, chemical, and nuclear industries drove the development and application of risk analysis techniques. In 1975, the first plant-scale model that attempted to fully quantify severe accident risk was published in WASH-1400 (NUREG 75/014), the Reactor Safety Study, sponsored by the U.S. Atomic Energy Commission (NRC, 1975). The probabilistic risk assessment (PRA) technique in WASH-1400 attempted to estimate public risks posed by NPPs by examining the potential paths by which nuclear fuel could melt and release radiation to the environment. Since the initial publication of WASH-1400, PRAs in the nuclear industry evolved into a logical framework for identifying the likelihood and consequences of severe accidents, which could lead to radiation release impacting the health and safety of the public. In light-water reactors, there are three levels to a PRA as shown in Figure 3. A level 1 PRA evaluates the frequency of core damage, level 2 evaluates the probability of specific release of radioactive material, and level 3 evaluates the frequency of adverse public health or environmental impacts.

PRAs are model-based graphical techniques that use plant assets and design along with historical data (i.e., vendor, plant, and industry data on equipment and events) to determine the likelihood of an event and the frequency of potential consequences. In the nuclear industry, a PRA using event tree analysis (ETA) and fault tree analysis (FTA) results in the development of 'minimal cut sets' and estimation of core damage frequency. Minimal cut sets are the sequences of events or failures that must happen for a top event to occur in an FTA model.

2.3 Cyber Risk

Quantitative safety risk analysis relies heavily on known historical data for functional failure and accident analysis. Safety PRAs address incidents with adverse consequences that are random, unexpected, and unintentional, yet can still be modeled. Nuclear safety PRAs may consider failure of an operator to perform an action, but they are ineffective with modeling deliberate or malicious actions

intended to cause damage. Moreover, it is difficult to model digital systems, structures, and components (SSCs) and their related functions in safety PRAs since, in contrast to analog devices, they often fail in unexpected ways, resulting in an incomplete set of failure modes.

2.3.1 Scenario development

When answering the question 'what can go wrong?' in cyber risk analysis, researchers typically define the digital device, system, and/or function, the vulnerabilities associated with these devices or systems, and the possible threats against them to create scenarios or sets of scenarios that result in adverse impact. In fact, the following equation is commonly seen in literature:

$$Cyber\ Risk = \ Threat\ x\ Vulnerability\ x\ Consequence \tag{2}$$

where

threat is the potential for unintentional incidents OR hostile actions,

vulnerabilities are unknown or exploitable weaknesses, and

consequence is the impact of the action.

Since the full set of threats and vulnerabilities is often unknown and constantly changing, the set of scenarios or possible undesired events is difficult, if not impossible, to fully define. Factors that influence the evaluation of deliberate threats include adversarial knowledge, motivation, intent, characteristics, and capabilities—including those tactics, techniques, and procedures (TTPs) used to compromise an asset.

2.3.2 Likelihood determination

Determining the likelihood, or probability, in cyber risk is similarly problematic since it is not only impossible to determine likelihood if the complete set of scenarios is unknown, but also difficult to accurately model the probability of intentional attacks by intelligent and adaptive adversaries. And, unlike quantitative safety risk analyses, historical data on cyber incidents and attacks in nuclear plants is limited. Indeed, some researchers neglect likelihood and determine a conditional risk based upon the scenario occurring (Clark et al., 2018; Clark et al., 2017; EPRI, 2018b). Alternative approaches may consider likelihood of an attack occurring, likelihood of an attack succeeding, and/or likelihood of adverse impact occurring.

Factors influencing the probabilities are often a function of threats, vulnerabilities, and any mitigations that may be in place. For example, an adversary may attempt to attack a control system from a plant's outward-facing internet—this attack may have a high probability of occurring based upon accessibility to the internet, but a low probability of succeeding based upon security controls used to implement secure architecture, such as network segregation, firewalls, and data diodes. Likelihood of the attack occurring is also dependent on the 'attractiveness' of the compromise to an adversary. The attractiveness of a compromise, however, is different for each adversary as it depends on the adversary's motives, intent, and skill.

2.3.3 Consequence determination

As shown in Figure 4, the consequence of a cyber incident is typically discussed in terms of the C-I-A triad (confidentiality—integrity—availability). Loss of confidentiality, usually considered the least

important consequence in ICS, may result in loss of sensitive information that may be used to plan future, more damaging attacks. Additionally, loss of company or facility data may financially damage or otherwise harm the company.

Loss of integrity and availability may result in safety-related (e.g., radiological sabotage, loss of life, injury), financial-related (e.g., lost generation, equipment damage), or reputation-related consequences. Loss of integrity includes modification of data, logic, or commands; it may impact the truthfulness of a system, resulting in adverse system operation. Loss of availability (e.g., denial of service attack) may impact data and communication flow in a system, which also may result in adverse system operation.

2.3.4 Cyber risk analysis

Equation 2 fails to recognize that risk is not multiplicative but a function of attributes where vulnerability is conditional on threat and consequence is conditional on both threat and vulnerability. Therefore, the following equation is more accurate:

$$Cyber\ Risk = f(threat, vulnerability, consequence) \quad (3)$$

where cyber risk is a function of threats, vulnerabilities, and consequences, including likelihood of scenario success given these threats and vulnerabilities. Unfortunately, since historical data is limited and determination of likelihood and impact is often subjective and based on expert opinion, cyber risk is more complex than simply solving an equation. Cyber risk analysis is further complicated by the fact that threats and vulnerabilities continuously change as adversaries become smarter, threat vectors change, and technology advances. Therefore, it is not only difficult to determine the current risk state, but also nearly impossible to predict the future state. As described by Tweneboah-Koduah and Buchanan, security risk assessments are “more an art than science” (Tweneboah-Koduah and Buchanan, 2018). And, as Oppliger succinctly writes regarding quantification of cyber risk, “we must admit that we’ve reached a dead end and that our nice mathematical formula for quantifying risks hardly works in practice and is therefore useless” (Oppliger, 2015). In fact, the same issue with likelihood uncertainty exists in assessing physical security. To overcome this obstacle, the Risk-Informed Management of Enterprise Security (RIMES) methodology uses degree of attack difficulty rather than attack likelihood for physical security risk analysis of nuclear facilities (Duran et al., 2013). Despite the challenges, significant efforts are underway to develop methodologies for assessing cyber risks. These techniques are reviewed in Section 5.

3 CYBER RISK STANDARDS AND GUIDELINES

Voronca surveyed worldwide standards used for risk assessment at energy companies (Voronca, 2012). While this review was not specific to cyber risk, the report concluded that many of the standards and guidelines provide generalist approaches that do not capture the specificities of critical energy infrastructures. European risk assessment methods are further behind U.S. standards, in part due to the fragmented infrastructure and differences in security culture (Giannopoulos et al., 2012). Knowles *et al.* also performed a detailed review of standards and guidelines for ICS. They concluded that guidance for managing cyber risks in control-system-specific publications is both too high-level and scarce (Knowles et al., 2015).

The problem of inadequate risk assessment standards in critical infrastructure is magnified when addressing cyber risk analysis in ICS environments, including the nuclear industry. Table 1 lists cyber risk

standards and guidance within information security, ICS security, and nuclear security domains. As shown, several cyber risk assessment standards exist for ICT environments; however, the cyber challenges in ICT are much different than those in ICS. An inventory of methods and tools available for network and information security risk management is provided by ENISA (ENISA, 2021). It must also be noted that many of the standards and guidelines cover the entirety of the risk management process (i.e., analysis, evaluation, response) rather than focusing on risk analysis as reflected in Equation 3.

Focus	Publication	Accessibility
Information security	NIST SP 800-30 Rev. 1, Guide for conducting risk assessment	Free
	NIST SP 800-39, Managing information security risk	Free
	DHS Cyber security evaluation tool (CSET)	Free
	ISO/IEC 27005, Information security risk management	Paid
ICS cybersecurity	NIST SP 800-82 Rev 2, Guide to industrial control system security	Free
	IEC 62443-3-2, Security risk assessment and system design	Paid
	NERC CIP-002-5.1a, Cyber security-BES cyber system categorization	Free
	ANSI/API Standard 780, Security risk assessment methodology for the petroleum and petrochemical industries	Paid
Nuclear cybersecurity	NRC Regulatory Guide 5.71, Cyber security programs for nuclear facilities	Free
	NEI 08-09 Rev 6, Cyber security plan for nuclear power reactors	Free
	EPRI Cyber Security Technical Assessment Methodology: Risk Informed Exploit Sequence Identification and Mitigation	Paid
	EPRI HAZCADS: Hazards and consequences analysis for digital systems	Paid
	IAEA NSS 17, Computer security at nuclear facilities	Free

Table 1. Relevant cyber risk standards and guidelines.

Standards incorporating information security risk management include NIST SP 800-30 Rev 1 (NIST, 2012), NIST SP 800-39 (NIST, 2011), and ISO/IEC 27005:2018 (ISO/IEC, 2018). Additionally, the Department of Homeland Security (DHS) released a Cyber Security Evaluation Tool (CSET) to provide a systematic approach to evaluating an organization's security posture (DHS, 2021). This tool, however, is only a series of questions based upon the NIST standards and does not provide a true cyber risk analysis.

Standards incorporating ICS security risk management include NIST SP 800-82 Rev 2 (Stouffer et al., 2015) and IEC 62443-3-2 (IEC, 2020). While these standards provide high-level information on cyber risk assessments, they lack the implementation details necessary to appropriately evaluate and capture risk to a facility due to a cyber threat. The chemical industry, on the other hand, provides a systematic approach for qualitative or quantitative security risk assessment in ANSI/American Petroleum Institute (API) standard 780 (ANSI/API, 2013) and a white paper titled "Security Vulnerability Assessment Methodology" (API/NPRA, 2003). The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standard CIP-002-5.1a evaluates conditional risk to categorize critical bulk electric system (BES) assets solely based upon impact of a compromise (vulnerability and likelihood are negated in Equation 3) (NERC, 2015).

In early 2011, the U.S. Nuclear Regulatory Commission (NRC) established a task force to develop more comprehensive and holistic risk-informed, performance-based regulatory approaches to ensure the safe and secure use of nuclear material (NRC, 2021). The NRC's risk-informed approach to regulatory decision making considers insights from PRAs in conjunction with other engineering insights to complement the agency's deterministic approach and defense-in-depth philosophy. In 2011, the International Nuclear Safety Group at the International Atomic Energy Agency (IAEA) also developed a framework for an integrated risk-informed decision process to provide guidance on incorporating deterministic considerations with probabilistic analyses (IAEA, 2011a).

Although the NRC is transitioning to risk-informed approaches, the transition to risk-informed cybersecurity regulations and guidance is incomplete. Additionally, there are no actionable cyber risk analysis tools from the NRC or Nuclear Energy Institute (NEI) for NPP use at this time. Currently, the U.S. nuclear industry follows Regulatory Guide (RG) 5.71 (NRC, 2020e), NEI 10-04 (NEI, 2012) and NEI 08-09 (NEI, 2010) for implementation of an NPP's cyber security plan. Similar to NERC-CIP standards, NRC and NEI cyber risk guidance is focused on consequence, specifically on adverse impacts to the health and safety of the public.

As seen in Figure 5, digital assets are classified as CDAs if they are associated with safety-related, important-to-safety, security, or emergency preparedness functions, or if they are supporting equipment which, if compromised, adversely impacts those functions (NRC, 2020e). While this CDA classification and the subsequent CDA consequence assessments outlined in NEI 13-10 (NEI, 2017) narrow the scope of the program, it falls short of a risk-informed process. Furthermore, even though section C.13 in RG 5.71 (and corresponding section E-12 in NEI 08-09) is titled 'Evaluate and Manage Cyber Risk,' the section is primarily focused on vulnerability scanning tools and does not provide specific risk analysis guidance. NEI is currently revising NEI 10-04 and NEI 08-09 to reduce the scope of CDAs, but the changes, as currently written, will not incorporate a formal analysis of cyber risk as defined by Equation 3 (NEI, 2020a, b, c; NRC, 2020a, b, c).

Internationally, the IAEA Nuclear Security Series No. 17 (NSS-17) recommends the use of a risk assessment and management process, but it does not prescribe a specific methodology and refers readers to ISO/IEC 27005 (IAEA, 2011b). Additionally, risk-informed nuclear regulatory approaches are typically concerned with scenarios that affect the health and safety of the public or loss of special nuclear material, whereas holistic risk-informed approaches consider broader impacts, such as lost generation, equipment damage, or personnel injury.

The Electric Power Research Institute (EPRI) released the "Cyber Security Technical Assessment Methodology (TAM)" report to use in the characterization of a digital asset's attack surface and determination of the most appropriate security controls (EPRI, 2018a). While the TAM steps a user through creation of a cyber security data sheet, shared control method library, and relationship set data sheet, it directs users to its Hazard Analysis and Consequences Analysis of Digital Systems (HAZCADS) process for determination of potential hazards and consequences associated with the compromise of a digital asset (EPRI, 2015, 2018b). HAZCADS is reviewed in this survey.

4 SURVEY METHODOLOGY

With over 200 risk management methods and guidelines around the world (Paul and Vignon-Davillier, 2014), there have been many attempts by researchers to accurately assess cyber risk. However, since none of these tools meet all criteria for establishing the level of cyber risk for ICT and ICS environments (Baybutt, 2017), research and development into improved methods is ongoing. We undertook this survey to better understand cyber risk analysis techniques for use in the nuclear industry.

Reviews of cyber risk standards and cyber risk assessment methods for ICS are provided in a number of sources (Cherdantseva et al., 2016; Chockalingam et al., 2017; Giannopoulos et al., 2012; Knowles et al., 2015; Kriaa et al., 2015; Tweneboah-Koduah and Buchanan, 2018; Voronca and Voronca, 2015). We performed a search for cyber risk analysis techniques using IEEE Explore, Web of Science, and Google Scholar. Contrary to the other cyber risk literature reviews, we specifically focused our search on

risk analysis techniques rather than the broader risk assessment or risk management search terms as we were interested in the first step, risk analysis, rather than the latter steps of the risk management process. We also ignored publications that concentrated on only individual aspects of the cyber risk equation (e.g., vulnerability analysis, threat analysis, scenario development). Additionally, while we are primarily interested in cyber risk for the nuclear industry, we included publications from many application domains outside of nuclear power to determine their applicability in our research.

We selected 36 publications for review. We rated the risk analysis techniques based on three criteria—scope, adoptability, and repeatability—considering the technique, end goal, and starting basis as part of the scope, TRL and level of rigor as part of adoptability, and source data as part of repeatability. The number of citations for an article was excluded as a metric for this survey as a measure of industry adoption or acceptance since this number will be under-represented for newly developed or low TRL techniques.

5 ANALYSIS OF CYBER RISK ANALYSIS PUBLICATIONS

5.1 Scope Criteria

As cyber risk researchers, we are interested in risk analysis tools that provide the industry a holistic, graded approach for identifying cyber risk that moves beyond the traditional safety focus to include other concerns, such as financial or operational impacts. The ability to provide a relative risk score that an organization can use to prioritize risk treatment decisions, to include both regulatory and business impacts in one analysis, will help drive smart, efficient cyber risk reduction practices. While the Consequence-driven, Cyber-informed Engineering (CCE) approach is primarily concerned with high consequence events (HCE) for an overall business entity, its process of calculating an HCE severity score based upon criteria weights and criteria severity is an example of such a graded approach (Bochman and Freeman, 2021).

We evaluated the techniques based on if, and how, consequence is considered as well as whether its purpose is applicable for use at an NPP. The scope criteria was determined for each technique on a scale from 0 to 4 as defined in Table 2:

Index	Description
0	No applicability for NPP (consequence not considered)
1	Very low applicability for NPP (single impact considered, economic focus, strategy-based, incomplete analysis scope)
2	Low applicability for NPP (multiple impacts considered, limited scope, requires modifying plant PRA)
3	Medium applicability for NPP (all impacts considered, limited scope)
4	High applicability for NPP (all impacts considered, deliberate and inadvertent cyber risk considered, sufficient scope)

Table 2. Scope criteria rating.

Since the scope of the risk analysis technique is often dependent on the type of technique and the analysis starting point, we also surveyed each publication based on these topics. We noted two themes from this assessment. First, the cyber risk analysis methods vary between formula-based and model-based techniques as well as qualitative, semi-quantitative, and quantitative techniques. Second, the technique often depends on the end goal and the domain in which it is intended for use. Formula-based, quantitative techniques intended for use in ICT-based domains often have a financial goal, while model-

based, semi-quantitative techniques intended for use in an ICS-based domain often have a safety goal. Results of this analysis is provided in the following sections. The overall criteria ratings for each technique are provided in Section 5.5.

5.1.1 Technique

Risk analyses either use quantitative, semi-quantitative, or qualitative techniques to derive the level of risk for a plant, system, or component. Although many authors describe their method as quantitative, we believe that due to limited data and challenges with modeling the dynamic aspects of threat and vulnerability, these quantitative methods for determining cyber risk are inherently flawed. In safety risk analysis, historical data on equipment failure, adverse events, and environmental factors are available to calculate probabilities and uncertainties in quantitative methods, such as PRA. Even if complete histories on cyber-attacks or compromises were available (they are not), the continuous changes associated with threat vectors, adversarial skills, and technological advances would make this data irrelevant and the alleged quantitative analysis inaccurate.

Many of the self-described quantitative methods are, in fact, semi-quantitative methods that use numerical values based on expert opinion, which can be subjective and unrepeatable. For instance, an author may describe a technique that applies numerical rankings to qualitative values or ranges (e.g., 1, 2, 3 for High, Medium, Low impact) as quantitative. Since no true numerical probabilities or uncertainties are applied to these qualitative observations, methods that use these devices are more properly classified as semi-quantitative. As indicated in Table 3, the only techniques classified as quantitative in this survey were those using econometric data.

Table 3 also categorizes the techniques based on whether they use formulas or models. Formula-based techniques are deterministic approaches using straightforward mathematical equations for risk calculation. Model-based techniques determine risk using a logical method represented either graphically or non-graphically. Most of the techniques reviewed in this survey used graphical models. The methods also primarily used deterministic, rather than stochastic, approaches.

Category	Method	Type*
Formula-Based	Mean Failure Cost (MFC) (Abercrombie et al., 2013; Chen et al., 2015; Jillepalli et al., 2017)	QT/SQ
	Return on Security Investment (ROSI) (Bojanc and Jerman-Blažič, 2008)	QT
	Equation-based Risk Score (RS) (Caralli et al., 2007; Kure et al., 2018; Papa et al., 2011; Wu et al., 2015)	SQ
Model-Based, Non-Graphical	Risk Matrix (RM) (2013; Braband, 2017; Hutle et al., 2015; Mohr, 2016; Moore, 2013; NIST, 2012)	SQ
	Game Theory (GT) (Gouglidis et al., 2017; Schauer et al., 2017)	SQ
	RM + GT (Zhang et al., 2018)	SQ
	Intrusion Modes + Criticality Analysis (IMECA) (Zelinko et al., 2017)	SQ
Model-Based, Graphical	Security Argument Graph (SAG) (Jauhar et al., 2015)	SQ
	Petri-Net (PN) (Zhou et al., 2017)	SQ
	Attack Trees (AT) + Vulnerability Tree (VT) (Patel et al., 2008; Ralston et al., 2007)	SQ
	AT + Chain Diagrams (CD) (Paul and Vignon-Davillier, 2014)	QL
	AT + Analytical Hierarchy Process (AHP) (Argyropoulos et al., 2018)	SQ
	Failure Modes & Effects Analysis (FMEA) + AT (Birr et al., 2016)	QL
	FMEA + Hierarchical Holographic Modeling (HHM) ATs (Henry and Haimes, 2009)	SQ
	Failure Modes, Vulnerabilities, & Effects Analysis (FMVEA) + Systems Theoretic Process Analysis (STPA) (Kivelä et al., 2018)	SQ
	Fault Tree Analysis (FTA) + Event Tree Analysis (ETA) + Attack Trees (AT) (Abdo et al., 2018)	SQ
	Boolean logic Driven Markov Processes (BDMP) (Piètre-Cambacédès and Bouissou, 2010)	QT
	FTA + STPA (HAZCADS) (Clark et al., 2018)	QL
	FTA + STPA + Attack Graphs (AtG) (EPRI, 2015)	SQ
	Unified Markup Language (UML) + Hazards and Operability (HAZOP) (Raspotnig et al., 2018; Schmittner et al., 2015)	QL
	ETA + Bayesian Networks (BN) (Shin et al., 2017)	SQ
	BN (Landucci et al., 2017)	SQ
	3D Risk Profiling (3DR) (Tam and Jones, 2019)	SQ

*QT=Quantitative, SQ=Semi-Quantitative, QL=Qualitative

Table 3. Classification of cyber risk analysis methods.

Formula-based techniques

Formula-based techniques were typically seen in non-safety environments such as enterprise ICT. Econometric methods calculate mean failure cost, cost-benefit of risk mitigation, or return on security investment using quantitative data on asset values and security control implementation costs (Abercrombie et al., 2013; Bojanc and Jerman-Blažič, 2008; Chen et al., 2015; Jillepalli et al., 2017). These calculations are often used to prioritize control implementations to align with an organization's risk tolerance.

Other formula-based methods calculate risk values using semi-quantitative and quantitative data. Various formulas have been studied to 'quantify' risk to determine both relative risk and security control prioritization (Caralli et al., 2007; Kure et al., 2018; Papa et al., 2011; Wu et al., 2015). As mentioned, the challenge with these approaches is that they are typically subjective, with source data identified and/or ranked based on expert opinion, rather than truly quantitative.

Non-graphical model-Based

Model-based, non-graphical risk analysis methods may use game-theoretic frameworks or matrix-based tools, such as failure modes and effects analysis (FMEA), failure modes, vulnerabilities, and effects analysis (FMVEA), and intrusion modes and effects criticality analysis (IMECA), to identify risk. These tools were generally developed for analyzing cyber risk independent of plant safety or performance.

Risk analysis methods integrating game theory (GT) model intelligent interactions between adversaries and defenders (Gouglidis et al., 2017; Zhang et al., 2018). Certain GT techniques model the adversary's strategy to cause as much damage as possible to evaluate security control implementations to optimize cyber security spending. While GT may improve protections from cyber events, the models require quantitative data based on inexact assumptions (Zhang et al., 2018). In addition, full games for large systems are thought to be too complex (Fielder et al., 2016).

FMEA is a systematic, non-sequential bottom-up method that identifies known or potential failures, problems, or errors based on historical or inferential data at the component level. In cyber security risk analysis, FMVEA is often used since it incorporates a systematic review of component level vulnerabilities and how these vulnerabilities are susceptible or can be targeted during a cyber event. As digital assets can fail in unexpected ways, an FMVEA model will be incomplete due to omission of unknown failures. FMVEA is also a resource-intensive process if performed on every digital SSC in a plant.

IMECA is a further modification of FMEA that examines the effects of intrusions during system operation (Zelinko et al., 2017). IMECA is a bottom-up approach that identifies the vulnerabilities for each component and its criticality to system operation. Similar to FMVEA, IMECA is also a resource-intensive process resulting in an incomplete model.

Other non-graphical model techniques use traditional heat-map risk matrices to determine a risk score or value based upon parameters such as likelihood and impact. The parameters may be calculated via a formula or applied using a ranking (e.g., High, Medium, Low). The two parameters are then combined on a matrix to identify the resulting risk score. The risk matrix itself is arguably not an analysis method, rather it is simply a visualization tool. That said, although often considered subjective and/or ambiguous, the risk matrix technique is often used to determine a risk score with and without security controls to evaluate and prioritize control implementations (ANSI/API, 2013; Braband, 2017; Mohr, 2016; NIST, 2012).

Graphical, model-based techniques

Model-based, graphical methods use visual techniques, such as FTA, ETA, attack tree analysis, vulnerability tree analysis, and system-theoretic process analysis (STPA) to represent systems. Graphical models are logic techniques that systematically describe pathways within a system to identify and categorize deviations. These graphical risk models are very effective on smaller scales. For large systems such as plant-wide industrial control systems, however, there are often cognitive scalability issues as the systems are too complex to render and comprehend.

FTA is a graphical model developed in the 1960's that represents, in symbolic logic model, the cause-and-effect relationships between combinations of events leading to an identified top undesired event (Figure 6a). FTA contains only those activities that contribute to the top event and may be created using quantitative or qualitative techniques. Quantitative FTA, as used in PRA, identifies event probability at each step—the probability is propagated up to the top event to calculate an overall probability of occurrence. A combination of conditions that, if all occur and cause a top event, is termed a cut set. Although a somewhat resource-intensive process, FTA is useful for identifying single points of failure as well as vulnerabilities and potential mitigations.

Attack trees (AT) are a variation of FTA in which an attack is the top event instead of an overall system fault or design basis accident (DBA). In an attack tree, analysts identify paths that adversaries could follow based on known TTPs and evaluate scenario likelihood instead of failure rate or probability. Attack trees are useful for identifying weaknesses; however, they are difficult to use on large systems or plants because of their complexity. Attack graphs are similar to attack trees but use a different visual format to indicate entry points, exit points, nodes, and attack pathways.

Like FTA, vulnerability trees (VT) are top-down approaches that decompose the relationship between a top vulnerability and the sequence of vulnerabilities an adversary must exploit in order to reach the top. Vulnerability trees help inform attack scenarios that an adversary may follow in order to exploit an SSC. Like attack trees, however, vulnerability trees are complex and difficult to use on large systems.

While FTA is a top-down approach, ETA is a bottom-up approach (Figure 6b). ETA is also a symbolic logic model which, starting with an initiating event, identifies the sequence of propagating events leading to a final undesired event or loss. ETA may use qualitative or quantitative techniques, has a clear order from beginning to end, and can account for mitigations. ETA, however, is complex, resource intensive, and requires a new tree for each initiating event.

STPA models systems into hierarchical control structures which are then used to identify unsafe control actions for which mitigation measures can be used (Leveson, 2011). STPA first identifies top level accidents or hazards to avoid, then identifies the control actions leading to the top event. STPA-Sec modifies STPA to incorporate both safety and security (Young and Leveson, 2013). While STPA moves beyond identifying system failures to find complex causal chains of events in control structures, analyzing all interactions between controllers and system level components, including human interactions, it is very resource intensive in a complex environment.

Security Argument Graph (SAG) is tool developed for the smart grid using failure scenarios defined by the U.S. National Electric Sector Organization Resource (NESCOR) (Jauhar et al., 2015). The SAG tool provides a graphical representation that connects mal-activity processes with system components and threat agents to evaluate the probability of a failure scenario occurring. Currently, the tool only applies to the NESCOR scenarios (Jauhar et al., 2015). In addition, a semi-quantitative method using weighted fuzzy petri-nets (PN) was developed by Zhou *et al.* to evaluate an overall risk value for a facility (Zhou et al., 2017). While this PN method may provide valuable information for overall facility risk, it does not provide enough detail for use in ICS.

Hybrid techniques

With hybrid methods, techniques are combined to present a more complete representation of the risk from cyber events. Hybrid methods in safety PRA combine top-down FTA with bottom-up ETA. Some researchers combine bow-tie analysis with attack tree or threat analysis to cyber-inform a safety PRA (Abdo et al., 2018). Still others integrate safety and cybersecurity by combining FTA with STPA (Clark et al., 2018) and attack graphs (AG) (EPRI, 2015), or using FTA-based Boolean logic Driven Markov Processes (BDMP) (Piètre-Cambacédès and Bouissou, 2010). Many researchers also combine FMEA/FMVEA with attack trees (Birr et al., 2016), Hierarchical Holographic Modeling (HHM) attack trees (Henry and Haimes, 2009), or STPA (Kivelä et al., 2018).

HAZCADS is one such hybrid technique combining FTA and STPA investigated for use in the nuclear industry (Figure 7). In this technique, unsafe control actions from digital SSCs are identified through STPA. Minimal cut sets are then developed by integrating unsafe control actions, assuming conditional risk (i.e., likelihood=1), into an established FTA (Clark et al., 2018).

Attack trees have been combined with vulnerability trees to evaluate threat-impact (TI) and cyber-vulnerability (CV) indices in supervisory control and data acquisition (SCADA) applications (Patel et al., 2008; Ralston et al., 2007). While a risk value is not determined, the TI and CV values are evaluated with and without controls applied to determine if the impact from a cyber event is reduced. Attack trees were also combined with chain diagrams (CD) to improve cognitive scalability of large systems, such as found in air traffic control systems. Argyropoulos *et al.* recently evaluated combining attack trees in the Secure Tropos security-by-design model with likelihood metrics determined by the Analytic Hierarchy Process (AHP) used in software engineering (Argyropoulos et al., 2018). This AT-AHP approach expresses the level of threat mitigation as a linear cost function for cost-benefit analysis in applying security controls.

ETA was combined with Bayesian Networks (BN) by Shin *et al.* to numerically evaluate a cyber PRA for an NPP reactor protection system (RPS) (Shin et al., 2017). The method relies on experts to determine and rank threats and mitigations as input into a BN model which informs a cybersecurity risk index (CSRI) calculation. The CSRI value is then used as an input into the ETA of a safety PRA to cyber-inform the PRA.

Unified Modeling Language (UML) using misuse sequence diagrams and failure sequence diagrams were combined with hazard and operability (HAZOP) guidewords to provide a combined safety and security analysis in the Combined Harm Assessment of Safety and Security for Information Systems (CHASSIS) tool (Schmittner et al., 2015).

IMECA and Support Vector Machine (SVM) tools were combined by Zelinko *et al.* (Zelinko et al., 2017). SVM was used to develop a vulnerability classifier tool derived from common vulnerabilities and exposures (CVE) and national vulnerability database (NVD) data to define vulnerability probabilities and severities. This data was used in an IMECA model to calculate system risk based on probability and damage related to the vulnerabilities in each software and hardware component within the system.

5.1.2 Goal

While the holistic end goal of risk analysis is to identify and inform a company of potential risks so that risk management decisions can be prioritized, variations in technique goals were identified. We categorized these cyber risk analysis goals into five areas as shown in Figure 8. They are further broken down by technique in Table 4.

Most of the techniques surveyed were focused on identifying components, functions, or pathways requiring security controls based on the assessed risk level (Birr et al., 2016; Caralli et al., 2007; Henry and Haimes, 2009; Kure et al., 2018; Landucci et al., 2017; Papa et al., 2011; Paul and Vignon-Davillier, 2014; Tam and Jones, 2019; Wu et al., 2015; Zelinko et al., 2017; Zhou et al., 2017). Wu was also concerned with dynamic risk and how it changed over time during an attack (Wu et al., 2015).

As many critical ICS processes must ensure continuous, safe operation, several of the techniques focused on cyber-informing safety analyses (Abdo et al., 2018; Clark et al., 2018; 2015; Kivelä et al.,

2018; Mohr, 2016; Pièrre-Cambacédès and Bouissou, 2010; Schmittner et al., 2015; Shin et al., 2017). The goal of these models is to integrate cyber risk into safety analyses to capture overall system or device interactions.

Other techniques were primarily developed to prioritize the implementation of security controls to determine those that would be most effective in eliminating or reducing the impact of a cyber compromise (Braband, 2017; Hutle et al., 2015; Moore, 2013; NIST, 2012; Patel et al., 2008; Ralston et al., 2007; Zelinko et al., 2017). Most commonly with these techniques, risk is evaluated with and without use of a security control to determine if the control effectively reduces risk.

For some techniques, the goal is financial analysis to decide where best to allocate cybersecurity mitigation funds (Bojanc and Jerman-Blažič, 2008). These techniques include mean failure cost (Abercrombie et al., 2013; Chen et al., 2015; Jillepalli et al., 2017), ROSI, or prioritized linear cost functions using attack trees with AHP (Argyropoulos et al., 2018). And finally, the typical goal of GT-based techniques is to identify optimal attack strategies and the resultant optimal defense strategies (Gouglidis et al., 2017; Schauer et al., 2017; Zhang et al., 2018).

End Goal	References
Identify need for controls	AT+CD (Paul and Vignon-Davillier, 2014) RS (Caralli et al., 2007; Kure et al., 2018; Papa et al., 2011; Wu et al., 2015) SAG (Jauhar et al., 2015) PN (Zhou et al., 2017) FMEA+AT (Birr et al., 2016) FMEA+HHM AT (Henry and Haimes, 2009) BN (Landucci et al., 2017) 3DR (Tam and Jones, 2019)
Cyber-inform safety analysis	RM (Mohr, 2016) FMVEA+STPA (Kivelä et al., 2018) FTA+ETA+AT (Abdo et al., 2018) BDMP (Pièrre-Cambacédès and Bouissou, 2010) HAZCADS (Clark et al., 2018) FTA+STPA+AtG (EPRI, 2015) UML+HAZOP (Raspotnig et al., 2018; Schmittner et al., 2015) ETA+BN (Shin et al., 2017)
Prioritize controls	RM (2013; Braband, 2017; Hutle et al., 2015; Moore, 2013; NIST, 2012) IMECA (Zelinko et al., 2017) AT+VT (Patel et al., 2008; Ralston et al., 2007)
Financial analysis	MFC (Abercrombie et al., 2013; Chen et al., 2015; Jillepalli et al., 2017) ROSI (Bojanc and Jerman-Blažič, 2008) AT+AHP (Argyropoulos et al., 2018)
Identify optimal strategy	GT (Gouglidis et al., 2017; Schauer et al., 2017) RM+GT (Zhang et al., 2018)

Table 4. Goal of risk analysis by technique.

5.1.3 Starting basis

During our survey, we recognized that the techniques had different origins from which to start the analysis, such as asset, impact, threat, and vulnerability. The distribution of origins used within the techniques is illustrated in Figure 9.

Most of the techniques we surveyed used threat determination as the starting basis for risk analysis. These threat-originated techniques often evaluate the adversaries' TTPs and determined the likelihood of attack based upon a given component or attack tree. The asset-originated techniques were classified as those starting with an asset inventory prior to applying risk analysis to the assets. Many financially driven, quantitative risk analysis techniques, such as those calculating mean failure cost, also started with the asset.

Techniques were classified as impact-originated if they first considered consequences and losses as the basis for risk analyses. In general, we identified that game-theoretic techniques, combined security and safety techniques, and top event analysis techniques (i.e., FTA) started with impact analysis. The vulnerability-originated techniques were classified as those starting with vulnerability assessment as the basis for risk analysis. These techniques were typically focused on vulnerability mitigation as an end goal. We also classified 25% of the techniques as using a hybrid approach, combining two of the origins.

5.2 Adoptability Criteria

A key criterion for a cyber risk analysis method is that it must be implementable at an NPP. Existing plants have thousands of digital assets; advanced reactors will likely have more. Does the technique maintain sufficient coverage of the issue space while still enabling efficient analysis? As such, we evaluated the tools based on adoptability, rating them on a scale from 0 to 3, as defined in Table 5. Level of rigor and TRL are discussed in the following sections.

Index	Description
0	No possibility for adoption; level of rigor too high; Unlikely to move higher than TRL 3
1	Low capability for adoption; high level of rigor; TRL < 4
2	Medium capability for adoption; medium level of rigor; TRL 4, 5, 6
3	High capability for adoption; low level of rigor; TRL > 6

Table 5. Adoptability criteria rating.

5.2.1 Level of rigor

A challenge with some cyber risk analysis techniques is the extensive time and resources required to model every digital component or function in a plant. Since the U.S. nuclear industry is currently focused on streamlining processes to improve NPP efficiencies for enhanced economic competitiveness, expensive analysis may prove counterproductive for the existing fleet. However, while techniques requiring high levels of rigor may not be readily adopted in the current fleet, they may still be applicable for use with new advanced and autonomous reactors throughout design, licensing, construction, and operations.

We classified rigor into high and medium groupings as none of the techniques reviewed in this survey were considered easy to implement for every SSC in an NPP. The results of this classification are listed in Table 6. Methods that incorporate an implementation tool or database to assist with the process were scored with a lower level of rigor.

Rigor	Category	Technique
High	Formula-based	MFC (Abercrombie et al., 2013; Chen et al., 2015; Jillepalli et al., 2017) ROSI (Bojanc and Jerman-Blažič, 2008) RS (Kure et al., 2018; Wu et al., 2015)
	Model-based, Non-graphical	RM (Braband, 2017; Hutle et al., 2015; Mohr, 2016; Moore, 2013) GT (Gouglidis et al., 2017; Schauer et al., 2017) RM+GT (Zhang et al., 2018)
	Model-based, graphical	SAG (Jauhar et al., 2015) PN (Zhou et al., 2017) AT+VT (Patel et al., 2008; Ralston et al., 2007) AT+CD (Paul and Vignon-Davillier, 2014) AT+AHP (Argyropoulos et al., 2018) FMEA+HHM AT (Henry and Haimes, 2009) FMVEA+STPA (Kivelä et al., 2018) FTA+ETA+AT (Abdo et al., 2018) BDMP (Piètre-Cambacédès and Bouissou, 2010) HAZCADS (Clark et al., 2018) FTA+STPA+AtG (EPRI, 2015) ETA+BN (Shin et al., 2017) BN (Landucci et al., 2017) 3DR (Tam and Jones, 2019)
Medium	Formula-based	RS (Caralli et al., 2007; Papa et al., 2011)
	Model-based, Non-graphical	RM (2013; NIST, 2012)
	Model-based, graphical	IMECA (Zelinko et al., 2017) FMEA+AT (Birr et al., 2016) UML+HAZOP (Raspotnig et al., 2018; Schmittner et al., 2015)

Table 6. Level of rigor by technique.

5.2.2 TRL

In addition to rigor, we considered the TRL of the technique. In keeping with standard TRL nomenclature, we categorized the techniques into levels as illustrated in Figure 10. As shown in Table 7, most techniques were classified at or below TRL 4. This indicates the technique is still in early research stages; while the technique may include a risk analysis framework or theoretical discussion, it lacks sufficient steps or methodology for current adoption in the nuclear industry. We also classified techniques still in R&D yet not easily adaptable to the nuclear industry, with a lower TRL.

Several techniques that built onto an industry standard framework, such as an IEC or API standard, were ranked at TRL 6. HAZCADS, a technique piloted and marketed by EPRI, was rated at TRL 7-8. Additionally, while the NIST SP 800-30 (NIST, 2012) and ANSI/API Standard 780 (ANSI/API, 2013) risk frameworks are not directly transferrable for use in the nuclear industry, we classified them as TRL 8-9 due to inclusion of detailed steps for risk analysis and their widespread use.

TRL	Reference	Notes
3	(Birr et al., 2016; Braband, 2017; Patel et al., 2008; Ralston et al., 2007; Raspotnig et al., 2018; Schmittner et al., 2015; Shin et al., 2017; Zelinko et al., 2017; Zhang et al., 2018)	No case study provided.
3-4	(Argyropoulos et al., 2018; Henry and Haimes, 2009; Kivelä et al., 2018; Paul and Vignon-Davillier, 2014; Piètre-Cambacédès and Bouissou, 2010; Zhou et al., 2017)	Case study provided.

TRL	Reference	Notes
4	(Caralli et al., 2007; Kure et al., 2018; Landucci et al., 2017; Moore, 2013; Papa et al., 2011; Tam and Jones, 2019; Wu et al., 2015)	Case study provided.
4-5	(Abdo et al., 2018; Abercrombie et al., 2013; Bojanc and Jerman-Blažič, 2008; Chen et al., 2015; EPRI, 2015; Jauhar et al., 2015; Jillepalli et al., 2017; Mohr, 2016)	Case study provided.
5-6	(Gouglidis et al., 2017; Schauer et al., 2017)	Tool developed.
6	(Hutle et al., 2015)	Technique based IEC standards.
7-8	(Clark et al., 2018)	HAZCADS has been adopted and piloted by EPRI.
8-9	(ANSI/API, 2013; NIST, 2012)	NIST and API SRA Standards are in use.

Table 7. TRL by technique.

5.3 Repeatability Criteria

Cyber risk is not static—adversaries learn new skills and develop more sophisticated attacks using different TTPs; new technology is installed, or existing technology is updated, resulting in different vulnerabilities and attack surfaces; and organizations implement new risk treatments or modify existing ones. This constantly changing environment requires ongoing cyber risk analysis to ensure the organization's risk level and security posture are maintained as desired. This necessitates a repeatable risk analysis methodology to address ongoing changes in relative risk. If different people perform an analysis on the same data, will the result be the same? How is repeatability affected if expert judgement or expert elicitation is required? What happens with different experts? Is there potential for a software tool or automated process to streamline the analysis?

We evaluated each of the techniques on repeatability, rating them on a scale from 0 to 3, as defined in Table 8. Sources of input data, which may impact repeatability, are discussed in the following section.

Index	Description
0	No capability for repeatability
1	Low capability for repeatability, reliance on qualitative data and/or experts
2	Medium capability for repeatability; combination of sources
3	High capability for repeatability; trusted data sources

Table 8. Repeatability criteria rating.

5.3.1 Source and input data

An ideal ICS cyber risk analysis incorporates a repeatable process which results in the same risk determination regardless of who performs the analysis. Unfortunately, much of the analysis with cyber risk relies upon expert opinion on threats and adversaries, asset vulnerabilities, and impacts or consequences. While there are well-established approaches for expert elicitation, these processes are time intensive and may not result in repeatable outcomes.

To provide insight into potentially useful data sources that may improve repeatability, we documented the source and input data, if any, for each method. We included any data used as input

into the technique, such as expert opinion/elicitation, historical data, threat databases, vulnerability databases, scenario databases, and established attack classification tools. As shown in Table 9, we determined that sources varied widely. However, 89% of the techniques still used some form of expert elicitation or opinion.

Source Data or Inputs	Usage	Reference
Expert opinion/elicitation	2	(Abdo et al., 2018; Abercrombie et al., 2013; 2013; Bojanc and Jerman-Blažič, 2008; Braband, 2017; Caralli et al., 2007; Chen et al., 2015; Clark et al., 2018; EPRI, 2015; Gouglidis et al., 2017; Henry and Haimes, 2009; Hutle et al., 2015; Jauhar et al., 2015; Jillepalli et al., 2017; Kivelä et al., 2018; Kure et al., 2018; Landucci et al., 2017; Mohr, 2016; Moore, 2013; NIST, 2012; Papa et al., 2011; Patel et al., 2008; Piètre-Cambacédès and Bouissou, 2010; Ralston et al., 2007; Raspotnig et al., 2018; Schauer et al., 2017; Schmittner et al., 2015; Shin et al., 2017; Tam and Jones, 2019; Wu et al., 2015; Zelinko et al., 2017; Zhou et al., 2017)
Equipment costs	1	(Bojanc and Jerman-Blažič, 2008)
Historical threat data	2	(ANSI/API, 2013; Hutle et al., 2015)
API SRA results (as input)	1	(Zhang et al., 2018)
CAPEC	2	(Argyropoulos et al., 2018; Birr et al., 2016)
CVSS	2	(EPRI, 2015; Wu et al., 2015)
NVD	2	(EPRI, 2015; Zelinko et al., 2017)
CVE	6	(Argyropoulos et al., 2018; 2015; Gouglidis et al., 2017; Schauer et al., 2017; Wu et al., 2015; Zelinko et al., 2017)
CWE	1	(Birr et al., 2016)
MAGERIT categories	2	(Gouglidis et al., 2017; Schauer et al., 2017)
ENISA threat landscape (2015)	2	(Gouglidis et al., 2017; Schauer et al., 2017)
SECCRIT cloud-related threats	2	(Gouglidis et al., 2017; Schauer et al., 2017)
NISTIR threat interface categories	1	(Abercrombie et al., 2013)
NESCOR failure scenarios	2	(Abercrombie et al., 2013; Jauhar et al., 2015)
EBIOS database-threats (obsolete)	1	(Paul and Vignon-Davillier, 2014)
STRIDE framework	2	(Kivelä et al., 2018; Schmittner et al., 2015)

Table 9. Source data by technique.

Vulnerability data and scores based upon CVE, common weakness enumeration (CWE), common vulnerability scoring system (CVSS), and the NVD are used by some researchers (Argyropoulos et al., 2018; Birr et al., 2016; EPRI, 2015; Gouglidis et al., 2017; Wu et al., 2015; Zelinko et al., 2017). Threat databases from ENISA, MAGERIT, and SECCRIT are integrated into the tool developed by Gouglidis *et al*. (Gouglidis et al., 2017). Failure scenarios from NESCOR are used by Abercrombie *et al.* and Jauhar *et al.* (Abercrombie et al., 2013; Jauhar et al., 2015). Jillepalli *et al*. use threat categories from NIST SP 800-82 (Jillepalli et al., 2017), Hutle *et al*. use threat level tables from the HMG IS1 UK standard (now withdrawn) (Hutle et al., 2015), and Paul and Vignon-Davillier use the threat database from EBIOS (Paul and Vignon-Davillier, 2014). The API standard 780 and Ralston *et al*. suggest using threat data based on

facility, national, and global histories (ANSI/API, 2013; Ralston et al., 2007), which is, arguably, incomplete and difficult to acquire.

Aside from threat and vulnerability databases, the common attack pattern enumeration and classification (CAPEC) tool from Mitre is used by Argyropoulos *et al.* and Birr *et al.* to identify common attack patterns and applicable countermeasures (Argyropoulos et al., 2018; Birr et al., 2016). Researchers use costs associated with current equipment and countermeasures for cost-based analyses. And, while not indicated in Table 9, facility information, such as system drawings, digital asset lists, and system function documents, are generally required for any cyber risk analysis.

5.4 Application Domain

We launched a wide search of cyber risk analysis techniques, including both ICT and ICS environments. Figure 11 shows the distribution of domains for the publications reviewed. Four of the publications developed techniques for ICT while the remaining developed them for ICS. Only four of the 32 ICS techniques were developed specifically for the nuclear industry.

Table 10 further breaks down the domains by technique. As expected, the formula-based, econometric risk analysis methods were developed solely for ICT environments, which are primarily concerned with protecting against confidentiality attacks. These methods provide IT managers the knowledge required to determine financially optimized cyber risk treatments. While the survey discovered three publications in the utility domain that used mean free cost for risk analysis, most techniques in the ICS domains used model or hybrid techniques.

Domain	Technique
Air Traffic Control	AT+CD (Paul and Vignon-Davillier, 2014)
Automotive	UML+HAZOP (Raspotnig et al., 2018; Schmittner et al., 2015)
ICT	ROSI (Bojanc and Jerman-Blažič, 2008), AT+AHP (Argyropoulos et al., 2018), RM (NIST, 2012), RS (Caralli et al., 2007)
Machinery	FMVEA+STPA (Kivelä et al., 2018)
Maritime	3DR (Tam and Jones, 2019)
NPP	HAZCADS (Clark et al., 2018), FTA+STPA+AtG (EPRI, 2015), BN (Shin et al., 2017), IMECA (Zelinko et al., 2017)
Petroleum/Chemical	RM (ANSI/API, 2013; Moore, 2013), FT+ETA+AT (Abdo et al., 2018), BN (Landucci et al., 2017), PN (Zhou et al., 2017), RM +GT (Zhang et al., 2018)
Railway	RM (Braband, 2017), FMEA+AT (Birr et al., 2016)
Generic SCADA/ICS	RS (Kure et al., 2018; Papa et al., 2011; Wu et al., 2015), AT+VT (Patel et al., 2008; Ralston et al., 2007), FMEA+HHM AT (Henry and Haimes, 2009), BDMP (Piètre-Cambacédès and Bouissou, 2010), RM (Mohr, 2016)
Utility/Smart Grid	MFC (Abercrombie et al., 2013; Chen et al., 2015; Jillepalli et al., 2017), GT (Gouglidis et al., 2017; Schauer et al., 2017), SAG (Jauhar et al., 2015), RM (Hutle et al., 2015)

Table 10. Domain by cyber risk technique.

5.5 Technique Ratings

The scope, adoptability, and repeatability criteria ratings are summarized in Table 11. A total score as well as any comments on the ratings are also provided for each technique.

Technique	Ref	Scope	Adoptability	Repeatability	Total	Comments
Formula-Based						
MFC	(Abercrombie et al., 2013; Chen et al., 2015; Jillepalli et al., 2017)	1	1	2	4	Economic focus.
ROSI	(Bojanc and Jerman-Blažič, 2008)	1	1	2	4	Economic focus.
RS	(Kure et al., 2018)	2	2	2	6	Somewhat arbitrary selection of scores; end goal is a risk level for attack scenario.
RS	(Papa et al., 2011)	1	1	1	3	Formula based only on likelihood and impact with weighting factors.
RS	(Caralli et al., 2007)	3	1	1	6	Simplistic.
RS	(Wu et al., 2015)	2	2	1	5	Calculates dynamic risk during an attack.
Model-Based, Non-Graphical						
RM	(NIST, 2012)	3	2	1	6	Generic risk model.
RM	(ANSI/API, 2013)	3	2	1	6	Deliberate attacks by non-strategic actors.
RM	(Braband, 2017)	2	1	1	4	Theoretical approach applying all IEC 62443-3-2 security levels to 7 foundational requirements on each asset.
RM	(Hutle et al., 2015)	3	2	1	6	Technique uses many different tools which may cause implementation challenges.
RM	(Moore, 2013)	3	1	1	5	Uses Eq. 2 where threat is based on likelihood of act and vulnerability is based on likelihood of success.
RM	(Mohr, 2016)	2	1	1	4	Use of adversarial risk assessment matrix.
GT	(Gouglidis et al., 2017; Schauer et al., 2017)	2	1	2	5	Optimization based on economics.
RM + GT	(Zhang et al., 2018)	3	2	1	6	Based on API SRA methodology, adding strategic adversaries.
IMECA	(Zelinko et al., 2017)	1	1	2	4	Vulnerability focus.
Model-Based, Graphical						
SAG	(Jauhar et al., 2015)	1	1	2	4	Evaluates probability of success for NESCOR failure scenarios.
PN	(Zhou et al., 2017)	1	1	1	3	Evaluation of entire facility.
AT + VT	(Patel et al., 2008; Ralston et al., 2007)	1	1	1	3	Economic focus; uses historical probabilities of defined scenarios.
AT + CD	(Paul and Vignon-Davillier, 2014)	2	2	2	6	Focused on deliberate attacks, attack likelihoods, and feared consequences.
AT + AHP	(Argyropoulos et al., 2018)	1	1	2	4	Goal-oriented security approach incorporating AHP-estimated likelihood and impact values.
FMEA + AT	(Birr et al., 2016)	1	1	1	3	Limited details on approach.
FMEA + HHM ATs	(Henry and Haimes, 2009)	2	1	1	4	Calculates probability of attack success.

FMVEA + STPA	(Kivelä et al., 2018)	2	1	1	4	Risk is calculated by multiplying estimate attack probability by estimated threat severity.
FTA + ETA + AT	(Abdo et al., 2018)	2	2	2	6	Develop cut sets related to security and/or safety. Likelihood based on vulnerability and difficulty levels.
BDMP	(Piètre-Cambacédès and Bouissou, 2010)	3	2	1	6	Combines safety and security modeling using BDMP with Markov process associated with each leaf.
HAZCADS	(Clark et al., 2018)	2	2	2	6	Conditional probability of cyber incident in combined PRA FTA and STPA model.
FTA + STPA + AtG	(EPRI, 2015)	2	2	1	5	Adds attack graphs to cut sets identified by HAZCADS.
UML + HAZOP	(Raspotnig et al., 2018; Schmittner et al., 2015)	2	1	1	4	Misuse sequence diagrams and failure sequence diagrams combined with HAZOP to identify safety and security risk.
ETA + BN	(Shin et al., 2017)	3	1	1	5	Risk score based on attack likelihood and mitigations.
BN	(Landucci et al., 2017)	1	1	1	3	Evaluates likelihood of attack occurring and attack success on a facility, using threat level determined from API/SRA.
3DR	(Tam and Jones, 2019)	1	1	1	3	Analysis of attacker and target attributes to identify vulnerability, ease of attack, and attacker reward.

Table 11. Scope, adoptability, and repeatability criteria ratings for each technique.

6 GAPS IDENTIFIED

In theory, cyber risk management frameworks and risk analysis methods should be straightforward to implement. Likewise, it seems straightforward to simply add "cyber" considerations to mature methods like PRA. In practice, however, cyber risk analysis is very difficult, especially in ICS environments. And, as indicated by the amount of ongoing research in this field, there is not yet an industry-accepted risk analysis methodology. Cyber risk analysis is difficult because human adversaries are intelligent, unpredictable, persistent, and adaptable. It is impossible to map all possible attack scenarios that might lead to core damage at an NPP. It is also impossible to remove or fully mitigate all cyber risk unless a facility is built completely without digital components.

We were interested in discovering repeatable cyber risk analysis techniques that can be implemented in NPPs with sufficient scope to enable prioritization of both operational and regulatory-based security decisions. As shown in Table 11, we did not find a technique that satisfices all three criteria. We further categorized a subset of these gaps in Table 12.

Gaps for Nuclear	References
No focus on safety-related consequence	(Abercrombie et al., 2013; Argyropoulos et al., 2018; Bojanc and Jerman-Blažič, 2008; Chen et al., 2015; Gouglidis et al., 2017; Jillepalli et al., 2017; Patel et al., 2008; Ralston et al., 2007; Schauer et al., 2017)
No final risk determination (either quantitative, semi-quantitative, or qualitative)	(Patel et al., 2008; Ralston et al., 2007; Raspotnig et al., 2018; Schmittner et al., 2015)
Focused on overall facility security	(Zhou et al., 2017)
Requires analysis of every asset or intensive process	(Abdo et al., 2018; ANSI/API, 2013; Braband, 2017; Clark et al., 2018; EPRI, 2015; Henry and Haimes, 2009; Hutle et al., 2015; Kivelä et al., 2018; Mohr, 2016; NIST, 2012)

Gaps for Nuclear	References
Requires modification to current PRA	(Clark et al., 2018; EPRI, 2015)
Lacks detail or poor usage guidance	(Birr et al., 2016; Raspotnig et al., 2018; Schmittner et al., 2015; Zhang et al., 2018)
Limited or subjective/arbitrary data (i.e., system relationships, threat, vulnerability, attack vectors, failure times)	(Caralli et al., 2007; Jauhar et al., 2015; Kure et al., 2018; Landucci et al., 2017; Moore, 2013; Papa et al., 2011; Paul and Vignon-Davillier, 2014; Pièvre-Cambacédès and Bouissou, 2010; Shin et al., 2017; Tam and Jones, 2019; Zelinko et al., 2017)

Table 12. Classification of gaps for adoption in the nuclear industry.

Considering the scope criteria, many of the techniques do not incorporate safety-related consequences in the analysis (Abercrombie et al., 2013; Argyropoulos et al., 2018; Bojanc and Jerman-Blažič, 2008; Chen et al., 2015; Gouglidis et al., 2017; Jillepalli et al., 2017; Patel et al., 2008; Ralston et al., 2007; Schauer et al., 2017). We determined that the lack of safety focus was primarily due to the technique's end goal. Additionally, several techniques did not derive an actual final risk determination regardless of whether that analysis was quantitative, semi-quantitative, or qualitative (Patel et al., 2008; Ralston et al., 2007; Raspotnig et al., 2018; Schmittner et al., 2015) and one technique was focused primarily on overall facility security instead of ICS security (Zhou et al., 2017).

Considering the adoptability criteria and level of rigor, techniques that rely on analyzing the pathway or control logic for every digital asset in an NPP may be untenable as NPPs have thousands of digital assets (Abdo et al., 2018; ANSI/API, 2013; Braband, 2017; Clark et al., 2018; EPRI, 2015; Henry and Haimes, 2009; Hutle et al., 2015; Kivelä et al., 2018; Mohr, 2016; NIST, 2012). There were also several techniques that had insufficient or poor guidance by which to perform the analysis (Birr et al., 2016; Raspotnig et al., 2018; Schmittner et al., 2015; Zhang et al., 2018). Furthermore, while there is ongoing research to integrate safety and security into a cyber-informed PRA, we believe this approach may be undesirable for the existing fleet as it potentially adds unnecessary complexity to PRAs. While seemingly a logical progression towards developing a holistic risk analysis, incorporating CDAs or their control logic, connections, and/or pathways into an existing plant PRA is problematic. For instance, incorporating cyber aspects into a safety risk analysis greatly increases the scope of a PRA, which increases rather than decreases the burden of the existing cybersecurity and PRA programs. However, while the resources required to perform such analyses are potentially prohibitive for the existing fleet, these techniques may be more useful on new advanced reactors throughout their design and construction lifecycle.

Considering the repeatability criteria, it is preferred to use repeatable methods to help identify when risks exceed an NPP's risk tolerance such that mitigation strategies or security controls can be implemented to reduce the risk to an acceptable level. This does not imply that an explicitly quantified risk technique is necessary; it simply means that a repeatable technique for assessing relative cyber risk is necessary to effectively establish and prioritize risk management decisions. Expert elicitation or judgement can be subjective and/or ambiguous. Since 89% of the techniques surveyed in this paper rely on some form of expert judgement, repeatability is a challenge.

PRAs are quantitative techniques that use historical equipment data and known events to evaluate probabilities of unexpected, unintentional safety incidents—this type of data is largely absent for cybersecurity events. In addition, digital SSCs not only fail in unexpected ways, but modeling

deliberate, intentional attacks is challenging in a PRA. It is for these reasons that HAZCADS evaluates conditional cyber risk by neglecting the probability of unsafe control actions (UCA). While it may seem unreasonable to assume a UCA will definitively occur, this analysis provides valuable risk insight into how a UCA could affect the probability of a top event.

7 DISCUSSION

As discussed in Section 3, the power reactor cybersecurity program in the U.S. is largely programmatic and compliance-based without the inclusion of risk analysis techniques to risk-inform the processes. And, while the NEI and NRC are potentially reducing the scope of CDAs in the cyber security program, the process still will not include formal cyber risk analysis techniques (NEI, 2020a, b, c; NRC, 2020a, b, c). Furthermore, although the reduced scoping will lower the costs associated with implementing the cyber security program, the programmatic requirements to address the controls will still be cumbersome, expensive, and often may not provide the desired cyber-protections against radiological sabotage.

Risk-informing processes or programs in the nuclear industry is often defined as using an NPP's PRA in combination with deterministic evaluations (e.g., engineering analysis, expert judgement, experience) to guide decision making. While PRA is one technique for identifying risk, it is better suited to safety analysis. As discussed, the quantitative requirements of PRA are not currently satisfiable for cyber risk analysis. Several of the risk analysis approaches surveyed combine a safety PRA with cyber risk analysis to cyber-inform a safety analysis. Since the U.S. nuclear industry has indicated a desire to streamline processes in the cybersecurity plan to improve efficiencies while maintaining or improving cyber-protection against radiological sabotage, adding greater complexity via cyber-informed PRAs or safety risk analyses may be in direct opposition to this improvement pathway. These techniques, however, may be more amenable for use in advanced reactors that do not yet have an established cybersecurity program.

Cost-based cyber risk analyses that ignore safety or ICS concerns are also inappropriate solutions for the nuclear industry. These risk analysis techniques provide useful cost-benefit analysis information for ICT environments; however, pure financial analyses that ignore system interactions and production or safety impacts are unsuitable for ICS environments. In addition, pure quantitative cyber risk analysis is unattainable as threats and vulnerabilities are constantly changing and data is unavailable for quantifying current or future scenario likelihoods.

Returning to the traditional set of triplets in cyber risk analysis—threat, vulnerability, and consequence—a plant's current licensing basis can be used to identify high-consequence design basis events (DBE) or DBAs that can lead to radiological release, including those safety-related SSCs that are relied upon to remain functional during DBAs to protect the health and safety of the public. Often, if compromise of a digital SSC can lead to a DBA, then that SSC is classified as a CDA and is included in the facility's design basis threat (DBT) signifying that it must be protected by the licensee to minimize radiological sabotage. From a regulatory perspective, the licensee is not required to protect the facility from beyond-DBT events.

Therefore, it is possible that consequence-informing cyber risk analyses may offer more insight into protecting a nuclear facility against a DBT than cyber-informing safety risk analyses. Consequence or safety-informed cyber risk analysis may also be simpler to implement and maintain than a cyber-

informed PRA. Independent of method, effective risk-informed processes can help prioritize protection and mitigation efforts, even if the analysis results in a determination of relative risk rather than absolute risk. The ability to analyze how relative risk changes as other factors change (e.g., equipment, security control, procedural/administrative modifications) provides valuable insights to help provide high assurance of protection against cyber-attacks that could result in radiological sabotage.

While protecting a nuclear facility against a DBT is regulated by the cybersecurity rule, owners also want to protect their plants from non-DBT cyber incidents that might cause economic losses from plant shutdown, equipment damage, or intangible effects, such as reputation. The risk evaluation and risk treatment for those digital assets that cannot impact radiological release, or the health and safety of the public, could fall outside of the NRC regulatory guidance and, therefore, be subject primarily to the facility's decision-making process. Then again, a facility may still be subject to regulatory guidance under the NERC-CIP standards. If an NPP generates less than 1500 MWe, however, it may be designated as low impact with limited NERC-CIP requirements, such as cybersecurity awareness, physical access control, electronic access control, and incident response. Consequence-informing cyber risk analysis, with inclusion of both radiological, safety impacts and non-radiological, plant impacts, may enable the industry to 'right size' their cyber security program by using regulatory guidance to apply the highest security controls to those CDAs impacting safety and more business-driven, cost-effective processes to prioritize security control implementation to the remaining digital assets.

Although determining likelihood is challenging, cyber risk analysis techniques that develop qualitative or semi-quantitative risk scores to identify those SSCs that must be protected to prevent a DBA may have the most promise for nuclear industry adoption. The ability to evaluate an SSC's cyber risk before and after security control implementation is also a highly important feature for the tool. Several techniques reviewed expand upon the traditional cyber risk analysis set of triplets to include more detailed analysis of threats and vulnerabilities. The API SRA methodology defines the likelihood of attack based upon attractiveness of an asset to a given threat and likelihood of the success based upon the vulnerability and attack attempt (ANSI/API, 2013). Extensions of the API SRA method have also been studied (Landucci et al., 2017; Zhang et al., 2018; Zhou et al., 2017).

Tam and Jones developed a visual risk value using system vulnerability, ease of exploit, and attacker reward as axes (Tam and Jones, 2019). Vulnerability is a function of attack vector, asset vulnerability, and consequence. Ease of exploit is a function of attacker profile, asset type, attacker resources, and implemented security controls. Attacker reward is a function of attacker profile, asset type, attacker's goal, and consequence. Although this system was designed as a visual identification for maritime cyber risk, the technique could potentially be adapted for the nuclear industry to develop a relative risk score.

Risk values are also calculated by Kure *et al.* and Wu *et al.* (Kure et al., 2018; Wu et al., 2015). The technique developed by Kure *et al*. derives semi-qualitative scores for asset criticality, vulnerability, impact, and likelihood but it uses an arbitrary weighting factor for each asset that would potentially be challenging to define for all digital assets in an NPP (Kure et al., 2018). Wu *et al*. calculate risk as a function of attack severity, attack success probability, and attack consequence where attack severity is a function of frequency, intensity, and stealth of attack; success probability is a function of a vulnerability's ease of exploit, number of authentication times required, and exploitation level location;

and consequence is a function of economic loss, casualties, environmental damage, and repair cost (Wu et al., 2015).

These semi-quantitative risk calculations show promise for determining consequence-informed cyber risk in the nuclear domain, especially if an NPP's DBA is used to inform the consequence, impact, or severity values. The DBA could also be used to inform the asset type, asset criticality, or asset attractiveness values. That said, we argue that the technique should be a "cyber" risk analysis, not a "cybersecurity" risk analysis. An all hazards approach to cyber risk analysis that considers both deliberate and inadvertent acts will more adequately determine risk due to use of digital assets. Thus, those techniques that focus only on adversarial attacks do not provide a complete risk profile. Facilities must develop strategies for mitigating the effects from human errors and component failures as well as cyber-attacks. Further research is necessary to determine if these techniques, or variations of these techniques incorporating DBA-informed data, provide a useful methodology for risk-informing the CDA determination and security control assessment processes in an NPP's cybersecurity program.

8 CONCLUSIONS AND FUTURE WORK

As shown in Figure 12, vulnerabilities disclosed in ICS environments increase annually (Claroty, 2021). As the number of vulnerabilities increase and threat sophistication continues to evolve, the need to adequately understand relative cyber risk is important for effective prioritization of risk reduction measures to ensure a strong security posture. Therefore, we surveyed 36 publications to better understand the state of the art in cyber risk analysis and to evaluate their strengths and weaknesses for use in the nuclear industry.

While many techniques may provide valuable insight into cyber risk at a facility, this survey found that there is not yet a tool that provides repeatable, actionable risk analysis with the appropriate scope, level of rigor, and TRL for use in an NPP. All techniques fell short of achieving high ratings on the value tree of scope, adoptability, and repeatability.

We did, however, identify that most techniques used graphical, model-based approaches that were either semi-quantitative or qualitative. Additionally, we determined the goal for 53% of the techniques was to either identify the need for security controls or to prioritize the use of security controls. We also identified that most techniques have a low TRL and have not yet been validated in real environments. Furthermore, all but two of the techniques relied on some form of expert elicitation, a challenge for repeatable analyses.

We found that cyber risk analysis remains a challenge in all application domains and industries. The inherent unknown unknowns associated with current and future cyber threats, vulnerabilities, and adversaries limit the use of meaningful quantitative risk assessments. Thus, we are forced to evaluate cyber risk qualitatively or semi-quantitatively. While it is important to use meaningful and repeatable analyses to ensure accurate and maintainable risk-informed security control implementation decisions, we determined these cyber risk analysis solutions do not yet exist.

Methodologies that increase the complexity and cost of the cybersecurity program without providing an upgraded benefit over current NRC or NEI guidance (e.g., cyber-informed safety risk analysis) will be challenging to implement in the existing nuclear fleet. Conversely, cost-based approaches do not include the requisite level of safety focus for industry adoption. Safety-informed or consequence-informed cyber risk analysis methods that qualitatively or semi-qualitatively determine a

relative risk value show promise for use in the nuclear industry. Future research will be performed to determine if these methods, or variations of these methods as informed by an NPP's DBA, DBT, and current licensing basis, will benefit the industry to drive cyber-informed decision making to minimize cyber risks from all hazards, including radiological sabotage as well as unintentional actions or failures. Additional research is also necessary to evaluate if the same technique(s) can be used effectively for existing reactors as well as future advanced reactors.

9 ACKNOWLEDGEMENTS

The authors wish to acknowledge the contributions of Dr. Robert Youngblood, who provided critical reviews and suggestions.

10 FUNDING

This work was supported by the U.S. Department of Energy Office of Nuclear Energy Cybersecurity Crosscutting Technology Development program under DOE Idaho Operations Office, Contract DE-AC07-05ID14517.

11 REFERENCES

Abdo H., Kaouk M., Flaus J.M., Masse F., 2018. A safety/security risk analysis approach of industrial control systems: A cyber bowtie – combining new version of attack tree with bowtie analysis. Computers & Security. 72, 175-195. https://doi.org/10.1016/j.cose.2017.09.004.

Abercrombie R.K., Sheldon F.T., Hauser K.R., Lantz M.W., Mili A., 2013. Risk assessment methodology based on the NISTIR 7628 guidelines, 2013 46th Hawaii International Conference on System Sciences. IEEE, Hawaii. https://doi.org/10.1109/HICSS.2013.466.

American National Standards Institute/American Petroleum Institute (ANSI/API), 2013. ANSI/API STD 780: Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries. https://standards.globalspec.com/std/1603209/ansi-api-std-780.

American Petroleum Institute/National Petrochemical & Refiners Association (API/NPRA), 2003. Security vulnerability assessment methodology for the petroleum and petrochemical industries. https://www.nrc.gov/docs/ML0502/ML050260624.pdf.

Argyropoulos N., Angelopoulos K., Mouratidis H., Fish A., 2018. Risk-aware decision support with constrained goal models. Information & Computer Security. 26, 472-490. https://doi.org/10.1108/ICS-01-2018-0010.

Baybutt P., 2017. Issues for security risk assessment in the process industries. Journal of Loss Prevention in the Process Industries. 49, 509-518. https://doi.org/10.1016/j.jlp.2017.05.023.

Birr P., Hetzer M., Petretti S., 2016. IT security risk analysis and threat mitigation for railway applications, Fast abstracts at International Conference on Computer Safety, Reliability, and Security (SAFECOMP), Trondheim, Norway. https://hal.archives-ouvertes.fr/hal-01370249.

Bochman A.A., Freeman S., 2021. Countering Cyber Sabotage: Introducing Consequence-driven, Cyber-informed Engineering (CCE). CRC Press. https://doi.org/10.4324/9780367491161.

Bojanc R., Jerman-Blažič B., 2008. An economic modelling approach to information security risk management. International Journal of Information Management. 28, 413-422. https://doi.org/10.1016/j.ijinfomgt.2008.02.002.

Braband J., 2017. Towards an IT security risk assessment framework for railway automation, arXiv.org. https://arxiv.org/abs/1704.01175.

Caralli R.A., Stevens J.F., Young L.R., Wilson W.R., 2007. Introducing Octave Allegro: Improving the information security risk assessment process, Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst. https://apps.dtic.mil/sti/citations/ADA470450.

Chen Q., Abercrombie R.K., Sheldon F.T., 2015. Risk assessment for industrial control systems quantifying availability using mean failure cost (MFC). Journal of Artificial Intelligence and Soft Computing Research. 5, 205-220. https://doi.org/10.1515/jaiscr-2015-0029.

Cherdantseva Y., Burnap P., Blyth A., Eden P., Jones K., Soulsby H., Stoddart K., 2016. A review of cyber security risk assessment methods for SCADA systems. Computers & Security. 56, 1-27. https://doi.org/10.1016/j.cose.2015.09.009.

Chockalingam S., Hadžiosmanović D., Pieters W., Teixeira A., van Gelder P., 2017. Integrated safety and security risk assessment methods: a survey of key characteristics and applications, in: Havarneanu G., Setola R., Nassopoulos H., Wolthusen S. (Eds.), Critical Information Infrastructures Security. CRITIS 2016. Lecture Notes in Computer Science. Springer, pp. 50-62. https://doi.org/10.1007/978-3-319-71368-7_5.

Clark A., Williams A., Muna A., Gibson M., 2018. Hazard and consequence analysis for digital systems–a new approach to risk analysis in the digital era for nuclear power plants. Transactions of the American Nuclear Society. 119, 888-891. https://epubs.ans.org/download/?a=44369.

Clark A., Williams A., Wheeler T., 2017. Addressing cyber hazards in nuclear power plants with STPA-informed fault tree analysis, 5th European STAMP/STPA Workshop and Conference 2017, Reykjavik, Iceland. https://www.osti.gov/servlets/purl/1471168.

Claroty, 2021. Claroty biannual ICS risk & vulnerability report: 2H 2020, Claroty Resarch Group. https://security.claroty.com/biannual-ics-risk-vulnerability-report-2H-2020.

Department of Homeland Security (DHS), Cyber Security Evaluation Tool (CSET) https://github.com/cisagov/cset (accessed June 25, 2021).

Duran F.A., Wyss G.D., Jordan S.E., Cipiti B.B., 2013. Risk-Informed Management of Enterprise Security: Methodology and applications for nuclear facilities, Institute of Nuclear Materials Management 54th Annual Meeting, Palm Desert, CA. https://www.osti.gov/servlets/purl/1107550.

Electric Power Research Institute (EPRI), 2015. Program on technology innovation: Cyber hazards analysis risk methodology phase II: A risk informed approach. https://www.epri.com/research/products/3002004997.

EPRI, 2018a. Cyber security technical assessment methodology, risk Informed exploit sequence identification and mitigation, Revision 1. https://www.epri.com/research/products/000000003002012752.

EPRI, 2018b. HAZCADS: Hazards and consequences analysis for digital systems. https://www.epri.com/research/products/000000003002012755.

European Union Agency for Network and Information Security (ENISA), Inventory of risk management / risk assessment methods and tools. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory (accessed June 25, 2021).

Fielder A., Panaousis E., Malacaria P., Hankin C., Smeraldi F., 2016. Decision support approaches for cyber security investment. Decision Support Systems. 86, 13-23. https://doi.org/10.1016/j.dss.2016.02.012.

Giannopoulos G., Filippini R., Schimmer M., 2012. Risk assessment methodologies for critical infrastructure protection. Part I: A state of the art. JRC Technical Notes. https://core.ac.uk/download/pdf/38624408.pdf.

Gouglidis A., Busby J., Hutchison D., Shirazi S.N., König S., Galbis A.Z., 2017. HYRIM: Deliverable 2.3. Software tools for hybrid risk management in SCADA networks, in Hybrid risk management for utility networks, ETRA Investigación y Desarrollo S.A. https://hyrim.net/wp-content/uploads/2017/12/HyRiM-D2.3-Software-Tools-for-Hybrid-Risk-Management-in-SCADA-Networks.pdf.

Henry M.H., Haimes Y.Y., 2009. A comprehensive network security risk model for process control networks. Risk Analysis: An International Journal. 29, 223-248. https://doi.org/10.1111/j.1539-6924.2008.01151.x.

Hutle M., Hansch G., Fitzgerald W., 2015. SPARKS: D2. 2 Threat and risk assessment methodology, SPARKS Consortium. https://project-sparks.eu/wp-content/uploads/2014/04/D2_2_Threat_and_Risk_Assessment_Methodology.pdf.

International Atomic Energy Agency (IAEA), 2011a. INSAG Series No. 25, A framework for an integrated risk informed decision making process, Vienna. https://www.iaea.org/publications/8577/a-framework-for-an-integrated-risk-informed-decision-making-process.

IAEA, 2011b. Nuclear Security Series No. 17, Computer security at nuclear facilities, Vienna. https://www.iaea.org/publications/8691/computer-security-at-nuclear-facilities.

IAEA, 2021. Power Reactor Information System (PRIS), Vienna. https://www.iaea.org/resources/databases/power-reactor-information-system-pris (accessed June 25, 2021).

International Electrotechnical Commission (IEC), 2020. IEC 62443-3-2, Security risk assessment and system design. https://webstore.iec.ch/publication/30727.

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), 2018. ISO/IEC 27005:2018, Information technology - security techniques - information security management systems - Information security risk management. https://webstore.iec.ch/publication/63500.

Jauhar S., Chen B., Temple W.G., Dong X., Kalbarczyk Z., Sanders W.H., Nicol D.M., 2015. Model-based cybersecurity assessment with NESCOR smart grid failure scenarios, 2015 IEEE 21st Pacific Rim

International Symposium on Dependable Computing (PRDC), pp. 319-324. https://doi.org/10.1109/PRDC.2015.37.

Jillepalli A.A., Sheldon F.T., de Leon D.C., Haney M., Abercrombie R.K., 2017. Security management of cyber physical control systems using NIST SP 800-82r2, 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 1864-1870. https://doi.org/10.1109/IWCMC.2017.7986568.

Kaplan S., 1997. The words of risk analysis. Risk Analysis. 17, 407-417. https://doi.org/10.1111/j.1539-6924.1997.tb00881.x.

Kaplan S., Garrick B.J., 1981. On the quantitative definition of risk. Risk Analysis. 1, 11-27. https://doi.org/10.1111/j.1539-6924.1981.tb01350.x.

Kivelä T., Golder M., Furmans K., 2018. Towards an approach for assuring machinery safety in the IIoT-age. Logistics Journal: Proceedings. 2018. https://doi.org/10.2195/lj_Proc_kivelae_en_201811_01.

Knowles W., Prince D., Hutchison D., Disso J.F.P., Jones K., 2015. A survey of cyber security management in industrial control systems. International Journal of Critical Infrastructure Protection. 9, 52-80. https://doi.org/10.1016/j.ijcip.2015.02.002.

Kriaa S., Pietre-Cambacedes L., Bouissou M., Halgand Y., 2015. A survey of approaches combining safety and security for industrial control systems. Reliability Engineering & System Safety. 139, 156-178. https://doi.org/10.1016/j.ress.2015.02.008.

Kure H., Islam S., Razzaque M., 2018. An integrated cyber security risk management approach for a cyber-physical system. Applied Sciences. 8, 898. https://doi.org/10.3390/app8060898.

Landucci G., Argenti F., Cozzani V., Reniers G., 2017. Assessment of attack likelihood to support security risk assessment studies for chemical facilities. Process Safety and Environmental Protection. 110, 102-114. https://doi.org/10.1016/j.psep.2017.06.019.

Leveson N., 2011. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press. http://library.oapen.org/handle/20.500.12657/26043.

Mohr R., 2016. Evaluating cyber risk in engineering environments: A proposed framework and methodology, in Information Security Reading Room, SANS Institute. https://www.sans.org/reading-room/whitepapers/ICS/evaluating-cyber-risk-engineering-environments-proposed-framework-methodology-37017.

Moore D.A., 2013. Security risk assessment methodology for the petroleum and petrochemical industries. Journal of Loss Prevention in the Process Industries. 26, 1685-1689. https://doi.org/10.1016/j.jlp.2013.10.012.

National Institute of Standards and Technology (NIST), 2011. SP 800-39: Managing information security risk: Organization, mission, and information system view. https://doi.org/10.6028/NIST.SP.800-39.

NIST, 2012. SP 800-30, Revision 1: Guide for conducting risk assessments. https://doi.org/10.6028/NIST.SP.800-30r1.

North American Electric Reliability Council (NERC), 2015. CIP-002-5.1a-cyber security-BES cyber system categorization. https://www.nerc.com/pa/Stand/Pages/CIP0025.1aRI.aspx.

Nuclear Energy Institute (NEI), 2010. NEI 08-09: Cyber security plan for nuclear power reactors, Revision 6. https://www.nrc.gov/docs/ML1011/ML101180437.pdf.

NEI, 2012. NEI 10-04: Identifying systems and assets subject to the cyber security rule, Revision 2. https://www.nrc.gov/docs/ML1218/ML12180A081.pdf.

NEI, 2017. NEI 13-10: Cyber security control assessments, Revision 6. https://www.nrc.gov/docs/ML1723/ML17234A615.pdf.

NEI, 2020a. ML20126G492, Endorsement of NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Emergency Preparedness Functions," Dated March 2020. https://www.nrc.gov/docs/ML2012/ML20126G492.pdf.

NEI, 2020b. ML20199M368, NRC Review of NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Safety-Related and Important-to-Safety Functions," Dated July 2020. https://www.nrc.gov/docs/ML2019/ML20199M368.pdf.

NEI, 2020c. ML20205L604, Endorsement of NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with the Balance of Plant," dated July 2020, by August 30, 2020. https://www.nrc.gov/docs/ML2020/ML20205L604.pdf.

Nuclear Regulatory Commission (NRC), 1975. WASH-1400, NUREG-75/014, Reactor safety study: An assessment of accident risks in US commercial nuclear power plants, Washington D. C. https://www.osti.gov/biblio/7134131.

NRC, 2009. 10 C.F.R. § 73.54, Protection of Digital Computer and Communication Systems and Networks.

NRC, 2020a. ML20129J981, Response to NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Emergency Preparedness Functions," dated March 2020. https://www.nrc.gov/docs/ML2012/ML20129J981.pdf.

NRC, 2020b. ML20209A442, Response to NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with the Balance of Plant," dated July 2020. https://www.nrc.gov/docs/ML2020/ML20209A442.pdf.

NRC, 2020c. ML20223A256, Response to NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Safety-Related and Important-to-Safety Functions," dated July 2020. https://www.nrc.gov/docs/ML2022/ML20223A256.pdf.

NRC, 2020d. Probabilistic Risk Assessment (PRA). https://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html (accessed December 1, 2020).

NRC, 2020e. Regulatory Guide 5.71, Cyber security programs for nuclear facilities. http://pbadupws.nrc.gov/docs/ML0903/ML090340159.pdf.

NRC, 2021. Risk-informed activities. https://www.nrc.gov/about-nrc/regulatory/risk-informed/rpp.html (accessed June 25, 2021).

Oppliger R., 2015. Quantitative risk analysis in information security management: A modern fairy tale. IEEE Security & Privacy. 13, 18-21. https://doi.org/10.1109/MSP.2015.118.

Papa S.M., Casper W.D., Nair S., 2011. Availability based risk analysis for SCADA embedded computer systems, Proceedings of the 2011 International Conference on Security and Management (SAM). CSREA Press, Las Vegas, NV, pp. 541-547. http://world-comp.org/p2011/SAM5110.pdf.

Patel S.C., Graham J.H., Ralston P.A., 2008. Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements. International Journal of Information Management. 28, 483-491. https://doi.org/10.1016/j.ijinfomgt.2008.01.009.

Paul S., Vignon-Davillier R., 2014. Unifying traditional risk assessment approaches with attack trees. Journal of Information Security and Applications. 19, 165-181. https://doi.org/10.1016/j.jisa.2014.03.006.

Pièvre-Cambacédès L., Bouissou M., 2010. Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes), 2010 IEEE International Conference on Systems, Man and Cybernetics. IEEE, pp. 2852-2861. https://doi.org/10.1109/ICSMC.2010.5641922.

Ralston P.A.S., Graham J.H., Hieb J.L., 2007. Cyber security risk assessment for SCADA and DCS networks. ISA Transactions. 46, 583-594. https://doi.org/10.1016/j.isatra.2007.04.003.

Raspotnig C., Karpati P., Opdahl A.L., 2018. Combined assessment of software safety and security requirements: An industrial evaluation of the CHASSIS method. Journal of Cases on Information Technology (JCIT). 20, 46-69. https://doi.org/10.4018/JCIT.2018010104.

Schauer S., König S., Latzenhofer M., Rass S., 2017. Identifying and managing risks in interconnected utility networks: The HYRIM risk management process, in: IARIA (Ed.), SECURWARE 2017: The Eleventh International Conference on Emerging Security Information, Systems and Technologies, Rome, Italy. http://www.thinkmind.org/index.php?view=article&articleid=securware_2017_5_20_30042.

Schmittner C., Ma Z., Schoitsch E., Gruber T., 2015. A case study of FMVEA and CHASSIS as safety and security co-analysis method for automotive cyber-physical systems, CPSS '15: Proceedings of the 1st ACM Workshop on Cyber-Physical System Security. Association for Computing Machinery (ACM), pp. 69-80. https://doi.org/10.1145/2732198.2732204.

Shin J., Son H., Heo G., 2017. Cyber security risk evaluation of a nuclear I&C using BN and ET. Nuclear Engineering and Technology. 49, 517-524. https://doi.org/10.1016/j.net.2016.11.004.

Stouffer K., Pillitteri V., Lightman S., Abrams M., Hahn A., 2015. SP 800-82, Revision 2: Guide to industrial control systems (ICS) security, National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r2.

Szilard R.H., Youngblood R., Frepoli C., Yurko J.P., Swindlehurst G., Zhang H., Zhao H., Bayless P.D., Rabiti C., Alfonsi A., 2015. Risk-Informed Margin Management (RIMM) Industry Applications IA1-Integrated

Cladding ECCS/LOCA Performance Analysis-Problem Statement, Idaho National Laboratory (INL). https://doi.org/10.2172/1369619.

Tam K., Jones K., 2019. MaCRA: A model-based framework for maritime cyber-risk assessment. WMU Journal of Maritime Affairs. 18, 129-163. https://doi.org/10.1007/s13437-019-00162-2.

Tweneboah-Koduah S., Buchanan W.J., 2018. Security risk assessment of critical infrastructure systems: A comparative study. The Computer Journal. 61, 1389-1406. https://doi.org/10.1093/comjnl/bxy002.

Voronca S., 2012. Analising some of the existing risk assessment and management standards applied worldwide, for energy companies. Journal of Sustainable Energy. III, 77-84. https://doi.org/10.1093/comjnl/bxy002.

Voronca S., Voronca S., 2015. Survey of existing risk assessment and management standards applied worldwide, for power companies, 6th International Conference on Modern Power Systems, Cluj-Napoca, Romania, pp. 369-373. https://ie.utcluj.ro/files/acta/2015/Number3/MPS2015_Voronca.pdf.

Wu W., Kang R., Li Z., 2015. Risk assessment method for cyber security of cyber physical systems, 2015 First International Conference on Reliability Systems Engineering (ICRSE). IEEE, pp. 1-5. https://doi.org/10.1109/ICRSE.2015.7366430.

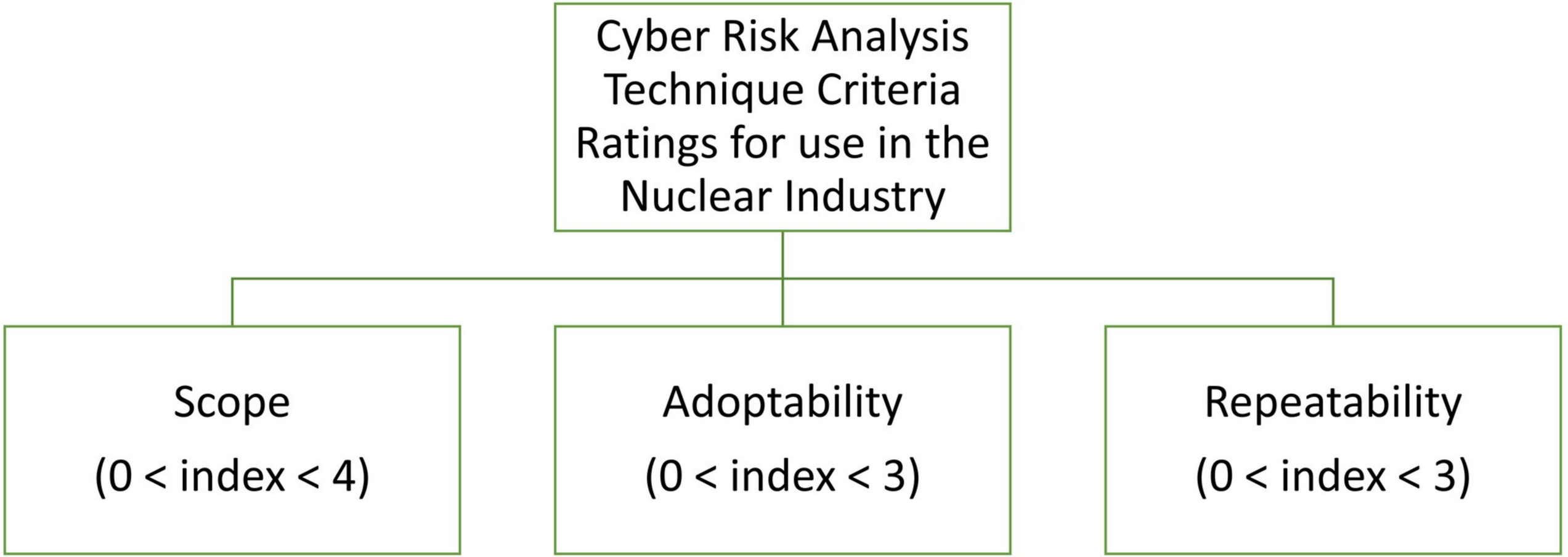
Young W., Leveson N., 2013. Systems thinking for safety and security, ACSAC '13: Proceedings of the 29th Annual Computer Security Applications Conference, pp. 1-8. https://doi.org/10.1145/2523649.2530277.

Zelinko I., Kharchenko V., Leontiev K., 2017. Cyber security assessment of component off-the-shelf Based NPP I&C System using IMECA technique, Proceedings of the 2017 25th International Conference on Nuclear Engineering. Volume 9: Student Paper Competition. American Society of Mechanical Engineers (ASME), Shanghai, China. https://doi.org/10.1115/ICONE25-67120.

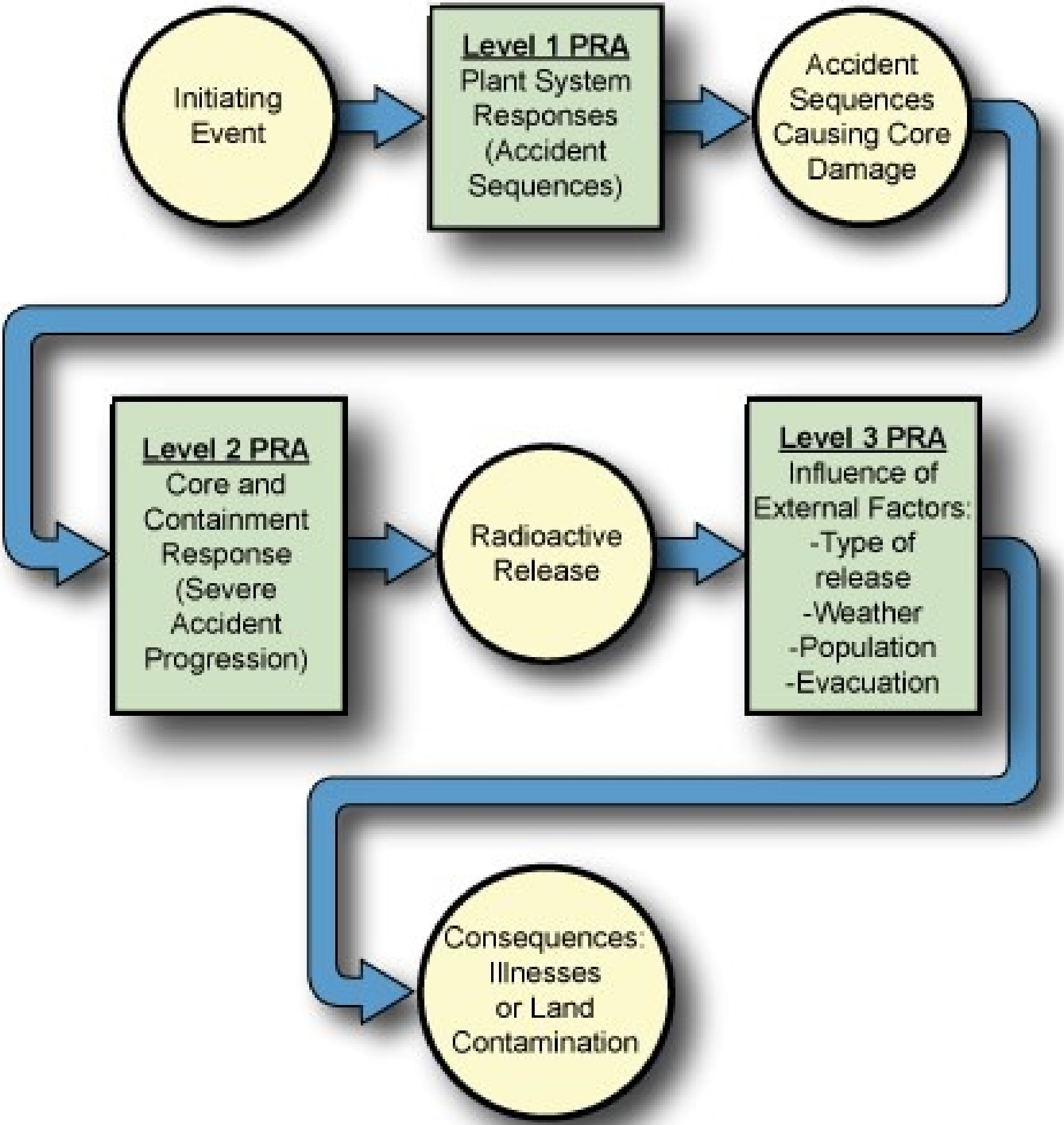
Zhang L., Reniers G., Chen B., Qiu X., 2018. Integrating the API SRA methodology and game theory for improving chemical plant protection. Journal of Loss Prevention in the Process Industries. 51, 8-16. https://doi.org/10.1016/j.jlp.2017.11.002.

Zhou J., Reniers G., Zhang L., 2017. A weighted fuzzy Petri-net based approach for security risk assessment in the chemical industry. Chemical Engineering Science. 174, 136-145. https://doi.org/10.1016/j.ces.2017.09.002.

Figure Captions:


Cyber Risk Analysis Technique Criteria Ratings for use in the Nuclear Industry
Scope
(0 < index < 4)
Adoptability
(0 < index < 3)
Repeatability
(0 < index < 3)


1
Risk Analysis
• Scenario
• Likelihood
• Consequence
2
Risk Evaluation
Prioritization based on risk tolerance
3
Risk Treatment
• Acceptance
• Avoidance
• Transfer
• Mitigation


Initiating Event
Level 1 PRA
Plant System Responses (Accident Sequences)
Accident Sequences Causing Core Damage
Level 2 PRA
Core and Containment Response (Severe Accident Progression)
Radioactive Release
Level 3 PRA
Influence of External Factors:
-Type of release
-Weather
-Population
-Evacuation
Consequences: Illnesses or Land Contamination

No
disruption
in systems
or functions

Availability

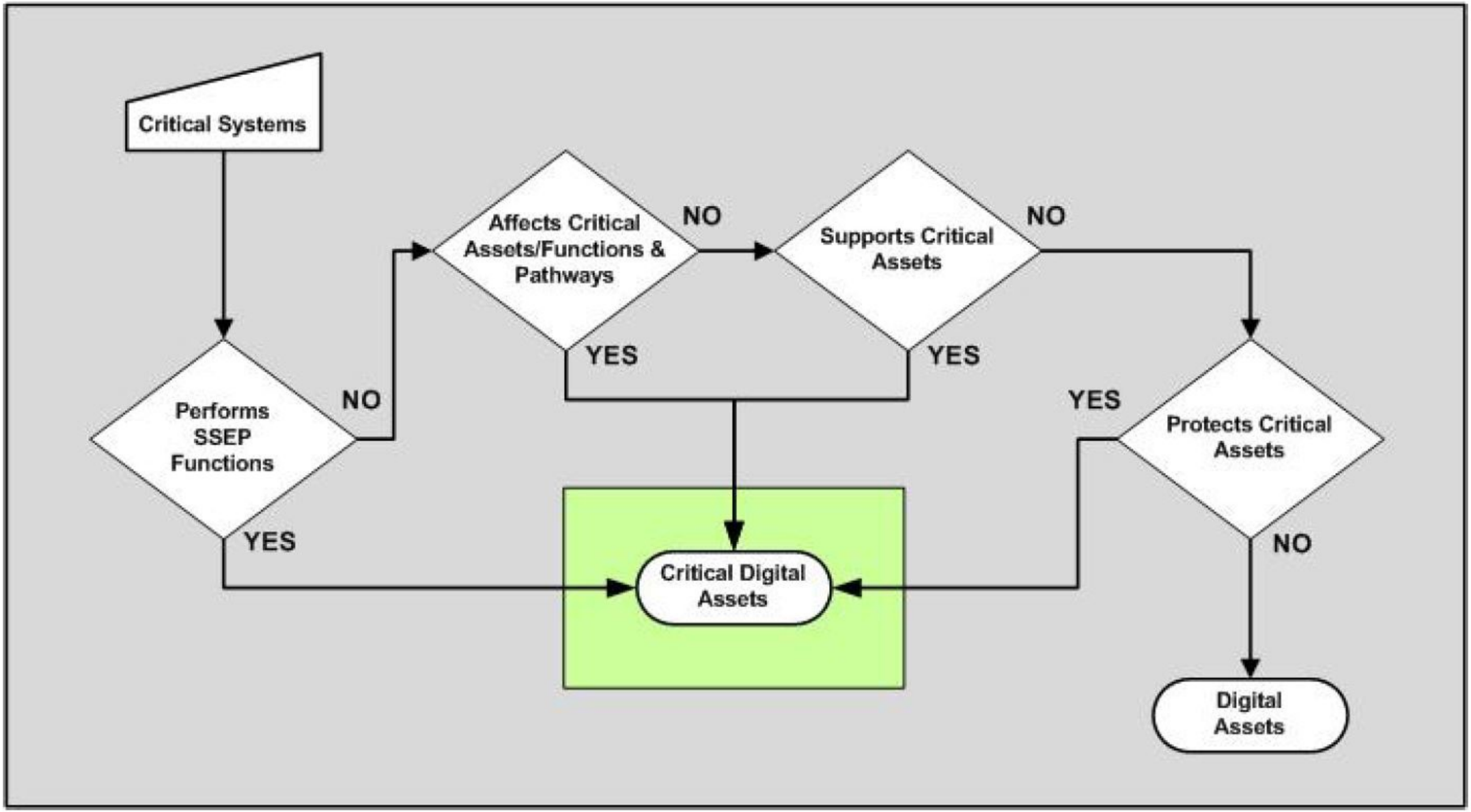
ICS Cybersecurity Objectives

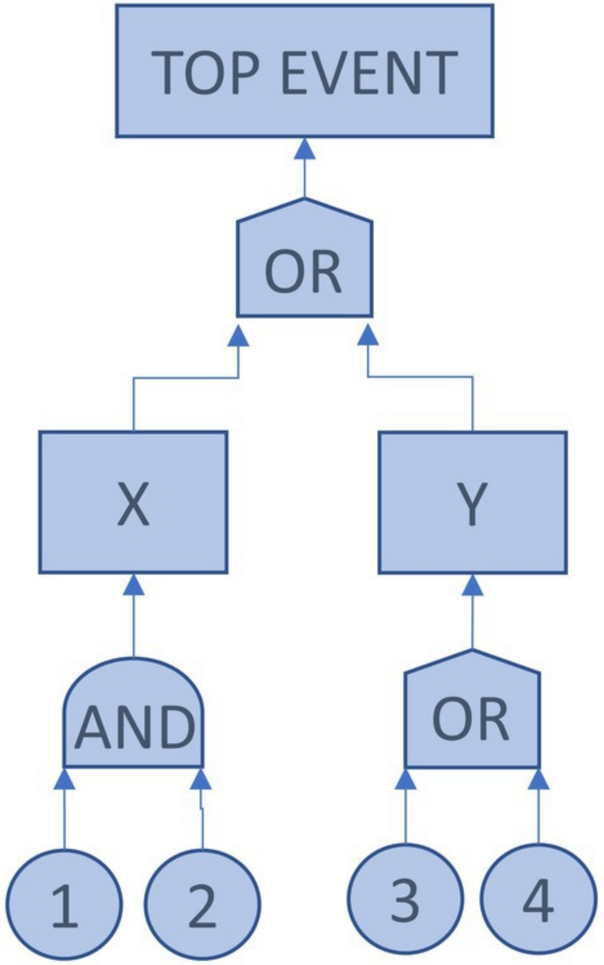
Privacy of
sensitive
information

Confidentiality

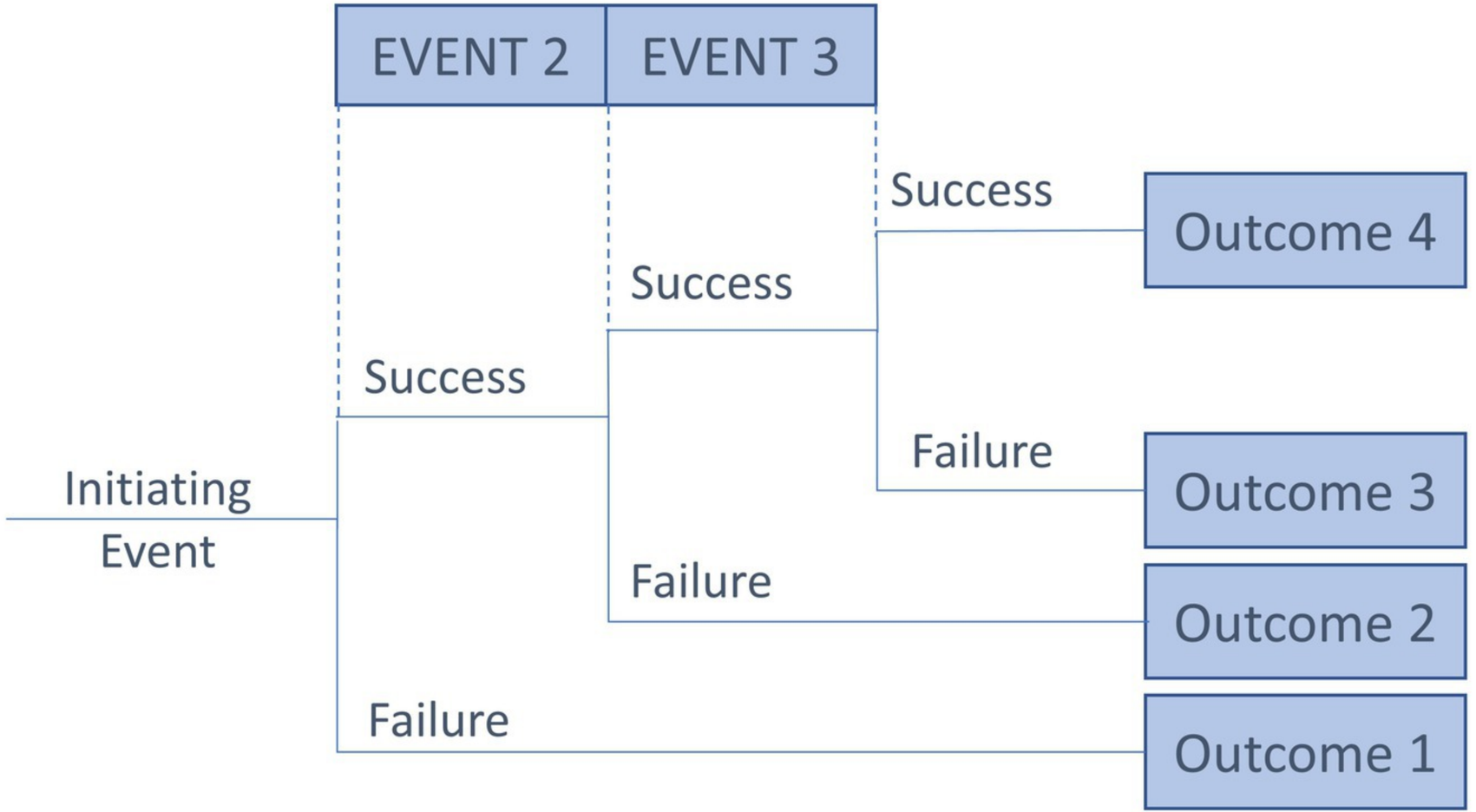
Accurate &
complete
data

Integrity

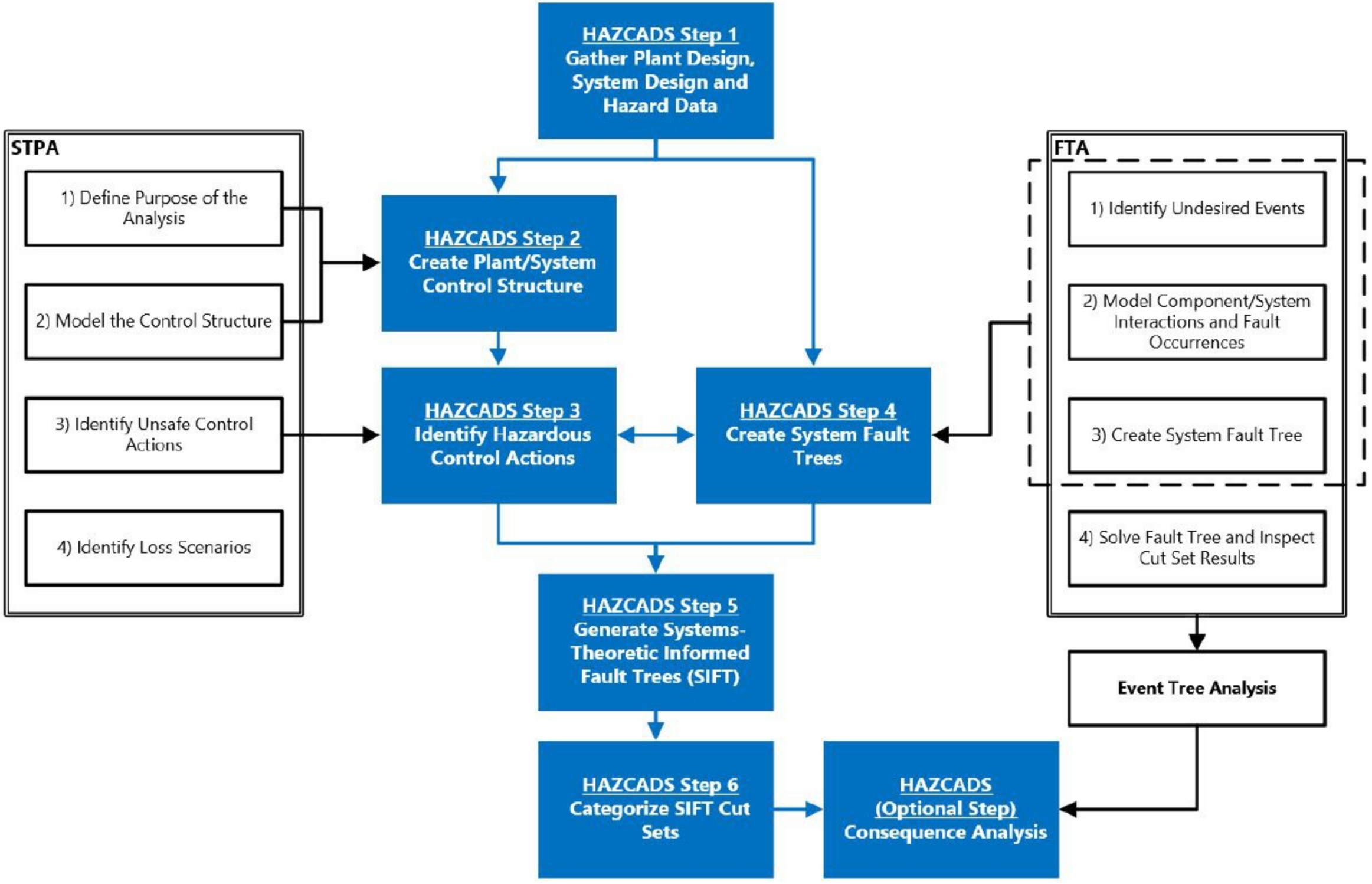

Critical Systems
Performs SSEP Functions
NO
YES
Affects Critical Assets/Functions & Pathways
NO
YES
Supports Critical Assets
NO
YES
Protects Critical Assets
YES
NO
Critical Digital Assets
Digital Assets

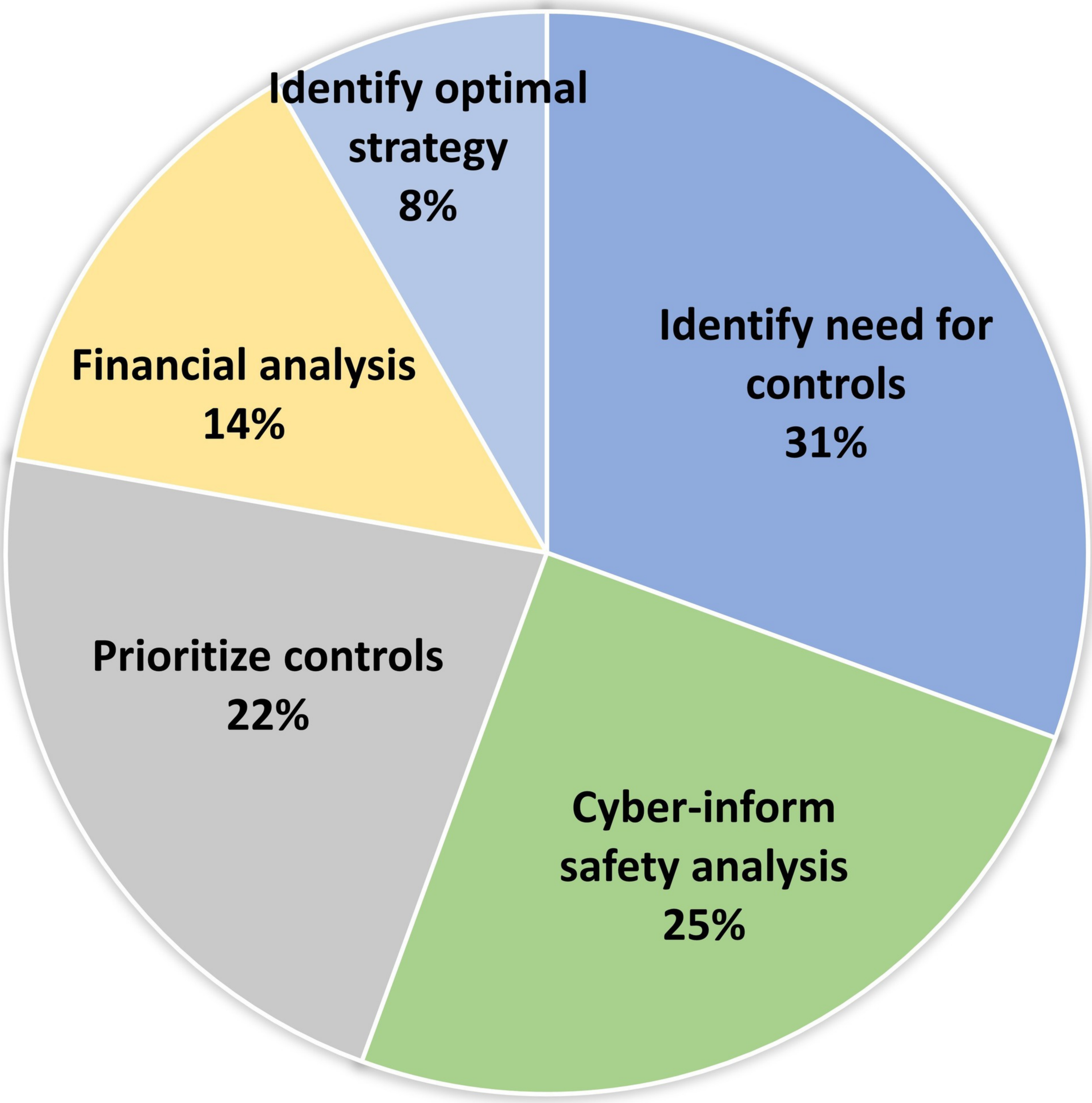


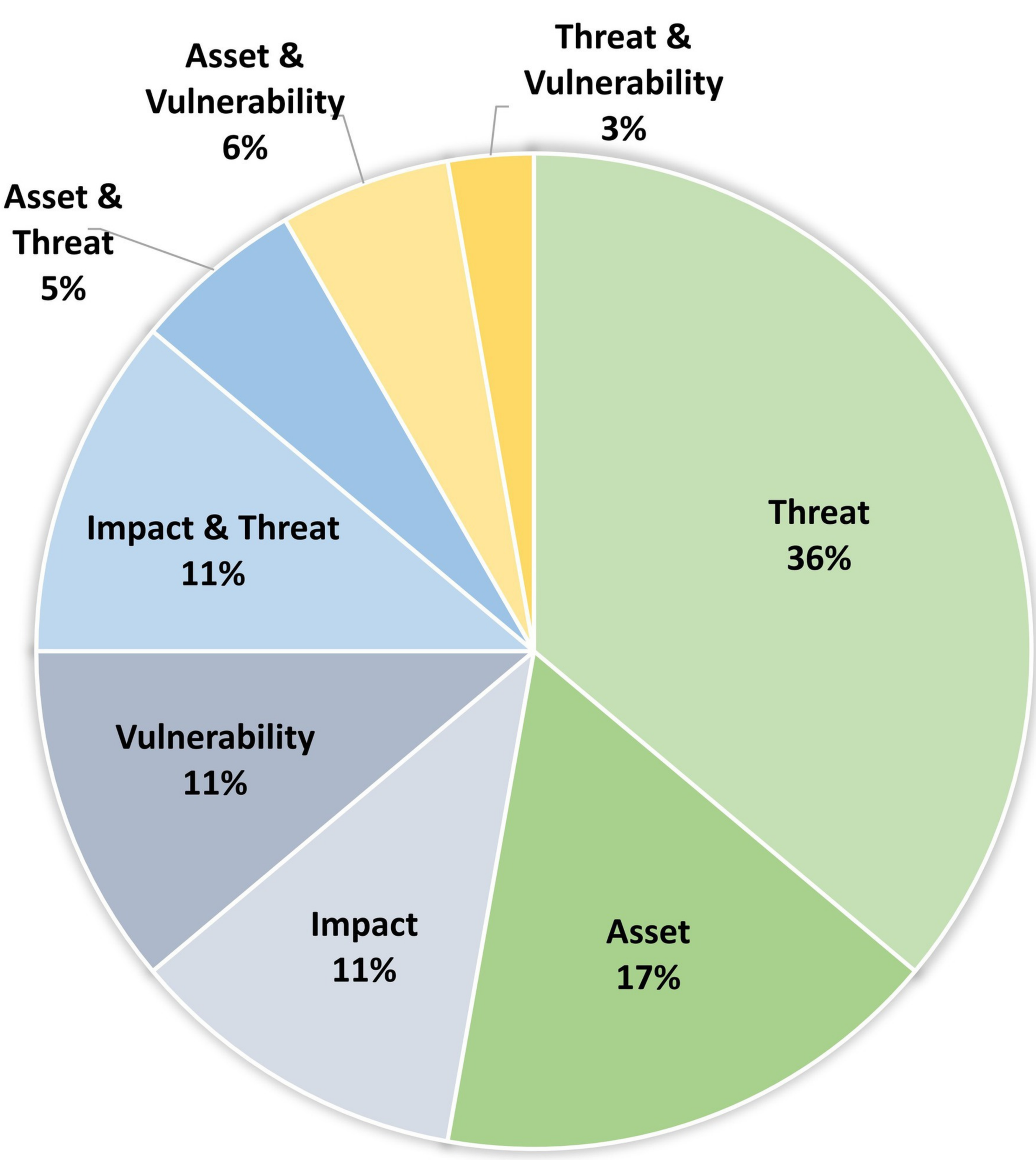
(a) FAULT TREE ANALYSIS



(b) EVENT TREE ANALYSIS


HAZCADS Step 1
Gather Plant Design, System Design and Hazard Data
STPA
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios
HAZCADS Step 2
Create Plant/System Control Structure
HAZCADS Step 3
Identify Hazardous Control Actions
HAZCADS Step 4
Create System Fault Trees
FTA
1) Identify Undesired Events
2) Model Component/System Interactions and Fault Occurrences
3) Create System Fault Tree
4) Solve Fault Tree and Inspect Cut Set Results
HAZCADS Step 5
Generate Systems-Theoretic Informed Fault Trees (SIFT)
Event Tree Analysis
HAZCADS Step 6
Categorize SIFT Cut Sets
HAZCADS
(Optional Step)
Consequence Analysis


Identify optimal strategy 8%
Identify need for controls 31%
Financial analysis 14%
Prioritize controls 22%
Cyber-inform safety analysis 25%


Threat & Vulnerability 3%
Asset & Vulnerability 6%
Asset & Threat 5%
Impact & Threat 11%
Vulnerability 11%
Impact 11%
Asset 17%
Threat 36%

Deployment

TRL 9: Technique proven through successive use

TRL 8: Technique completed and qualified

TRL 7: Technique prototyped at facility

Development

TRL 6: Technique demonstrated on actual system

TRL 5: Technique validated on actual system

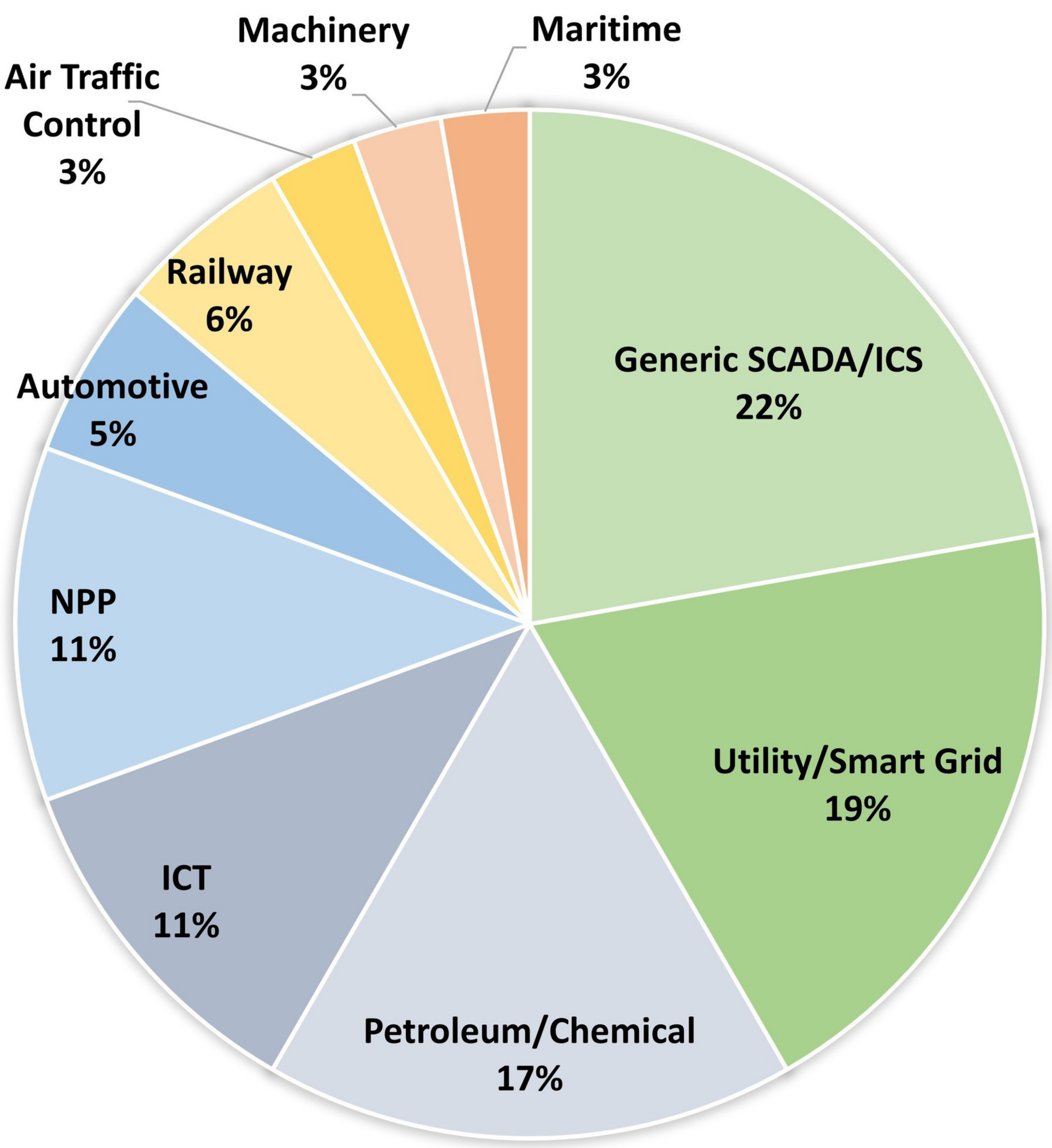
TRL 4: Experimental pilot of technique

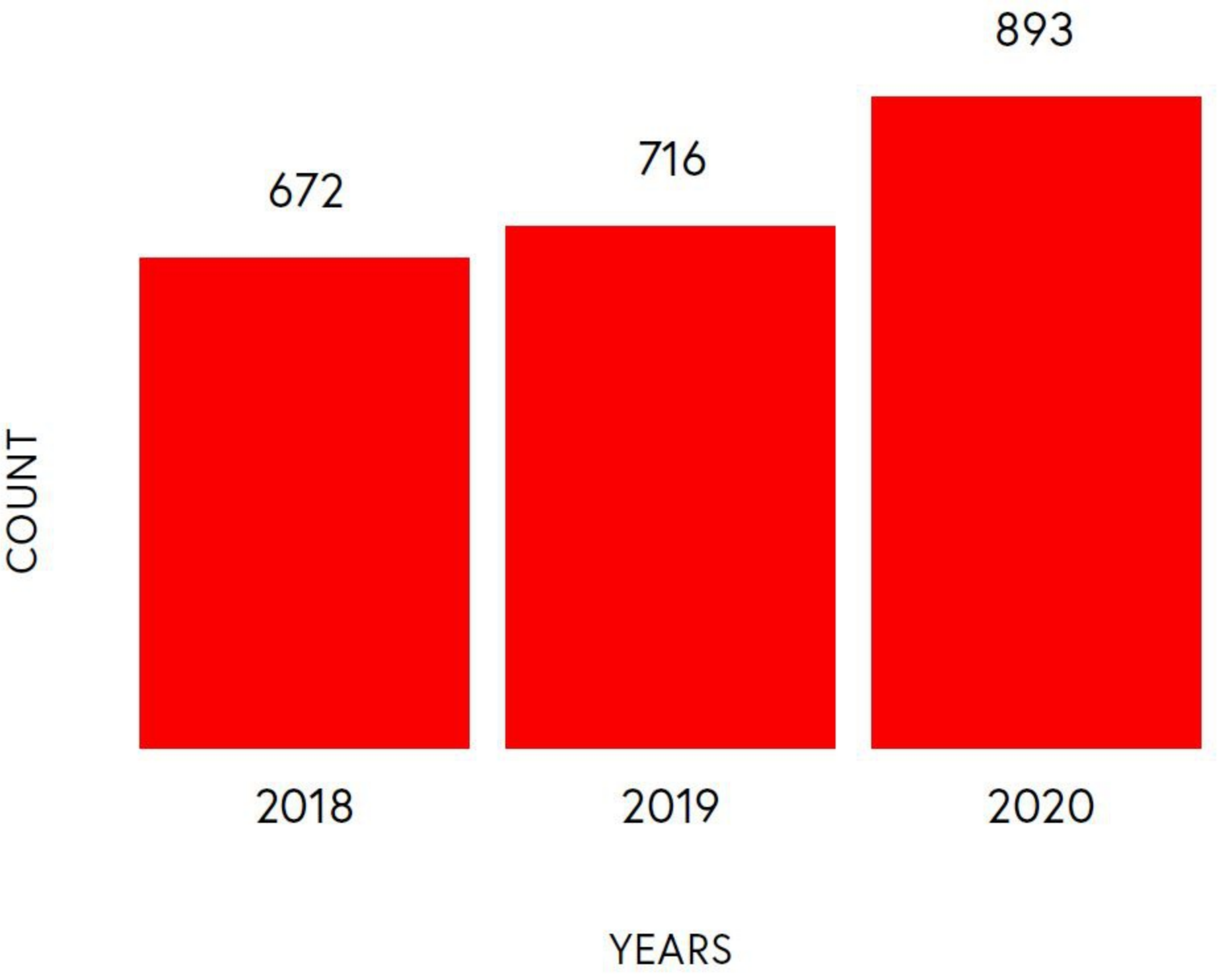
Research

TRL 3: Technique proof-of-concept

TRL 2: Technique conceptually formulated

TRL 1: Basic principles observed


Machinery
3%
Maritime
3%
Air Traffic
Control
3%
Railway
6%
Automotive
5%
Generic SCADA/ICS
22%
NPP
11%
Utility/Smart Grid
19%
ICT
11%
Petroleum/Chemical
17%


893
716
672
COUNT
2018
2019
2020
YEARS