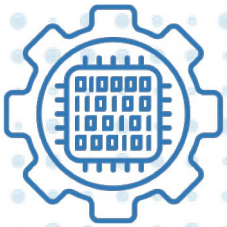
DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof. Reference herein to any social initiative (including but not limited to Diversity, Equity, and Inclusion (DEI); Community Benefits Plans (CBP); Justice 40; etc.) is made by the Author independent of any current requirement by the United States Government and does not constitute or imply endorsement, recommendation, or support by the United States Government or any agency thereof.



Cyber-Informed Engineering

Adapting Traditional Hazards Analysis Methods to Address Cyber Risks

A Cyber-Informed Engineering (CIE) Approach

September 2025

Authors:

Virginia Wright
Idaho National Laboratory

Remy Stolworthy
Idaho National Laboratory

Benjamin Lampe
Idaho National Laboratory

Wesley Yockey
Idaho National Laboratory

Chris Everett
Idaho National Laboratory

Robert Youngblood
Idaho National Laboratory

Sarah Freeman
MITRE

Cyber-Informed Engineering (CIE) Program activities are sponsored by the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (DOE CESER) and performed by Idaho National Laboratory and the National Renewable Energy Laboratory.

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. government or any agency thereof.

INL/RPT-25-88296

Abstract

Traditional hazards analysis (HA) methods, originally developed to address physical and operational risks, often fall short when it comes to identifying and mitigating cyber threats. These cyber threats pose unique and evolving risks to critical infrastructure and industrial control systems (ICS). This report explores the integration of Cyber-Informed Engineering (CIE) principles into existing HA methods to enhance their ability to address cyber-induced risks.

CIE provides organizations with a practical, cost-effective approach to closing the gap between traditional HA methods and the need for cyber risk mitigation. By leveraging existing safety processes and controls, CIE allows users to examine and mitigate cyber vulnerabilities without overhauling existing HA methods. This report identifies areas where HA and CIE naturally align and where their approaches diverge. It emphasizes how CIE principles can be used to adapt HA methods, broadening their scope to include cyber risks and enabling the mitigation of cyber-induced impacts alongside traditional hazards and failure scenarios.

This report examines how CIE can be applied across various HA methods—such as Hazard and Operability Studies (HAZOP), Probabilistic Risk Assessment (PRA), Failure Modes and Effects Analysis (FMEA), Systems-Theoretic Process Analysis (STPA), Hazard and Consequence Analysis for Digital Systems (HAZCADS), and Layers of Protection Analysis (LOPA). It provides strategies for integrating CIE to strengthen the identification, assessment, and mitigation of cyber-induced risks. The findings offer a structured entry point for organizations to embed CIE concepts into hazards and safety analyses, as well as broader engineering processes, ultimately supporting the design and operation of a more resilient infrastructure.

Contents

Figures

Tables

ACRONYMS

CIE	Cyber-Informed Engineering
CIL	Critical Item List
CLOPA	Cybersecurity Layers of Protection Analysis
DCS	Distributed Control System
DOE	U.S. Department of Energy
EC	Engineering Control
EPRI	Electric Power Research Institute
ETA	Event Tree Analysis
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
HA	Hazards Analysis
HAZCADS	Hazards and Consequence Analysis for Digital Systems
HAZOP	Hazards and Operability Study
I&C	Instrumentation and Controls
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
INL	Idaho National Laboratory
IPL	Independent Protection Layer
LOPA	Layers of Protection Analysis
O&M	Operations and Maintenance
OT	Operational Technology
PFD	Probability of Failure on Demand
PRA	Probabilistic Risk Assessment
RPN	Risk Priority Number
SIF	Safety Instrumented Function
SIS	Safety Instrumented Systems
SME	Subject Matter Expert
SNL	Sandia National Laboratories
STPA	System-Theoretic Process Analysis
UCA	Unsafe Control Actions

1. Introduction

The Department of Energy (DOE), Office of Cybersecurity, Energy Security, and Emergency Response (CESER)'s Cyber-informed Engineering (CIE) program, as part of its 2025 scope of work, investigated how engineering-driven mitigations might be integrated into various existing hazards analysis (HA) methods. Hazards analysis is designed to identify risks to safety, reliability, and performance but often overlooks the potential for these risks to be induced via cyber means. By combining a cyber-focused HA with traditional HA and pairing it with established cybersecurity practices for data protection, organizations can more effectively mitigate risks to both data integrity and system functionality.

To advance this effort, researchers at Idaho National Laboratory (INL) undertook a scientific review of multiple HA approaches and engaged subject matter experts (SMEs) to assess their practical application. This work focused on identifying both the strengths and limitations of existing HA methods, as well as pinpointing areas where CIE could augment traditional safety and resiliency practices. The analysis revealed not only where current HA methods are effective but also where they fall short in addressing the realities of cyber-physical threats, evolving adversary capabilities, and the growing interdependence of critical infrastructure and industrial control systems. By highlighting these gaps, INL researchers identified opportunities for CIE's principles to provide additional layers of defense, improve system resilience, and reduce the likelihood of overlooked vulnerabilities.

This report summarizes those findings and offers organizations a structured entry point for integrating CIE concepts into their ongoing hazards analysis, safety analysis, and broader engineering processes. The intent is not to present a finalized, comprehensive CIE-enhanced methodology for every HA approach reviewed. Rather, this report provides a framework for bridging the divide between traditional safety engineering practices and the emerging need for cyber-informed risk mitigation, helping stakeholders chart a path toward more resilient infrastructure design and operation.

2. Traditional Hazards Analysis

Hazards analysis is the process of systematically identifying hazards to support risk management decision-making and the selection of appropriate controls (i.e., measures intended to reduce the risks associated with those hazards). In practice, HA involves examining credible hazard scenarios that could affect a system or process and evaluating the risks associated with each scenario.

The origins of HA are closely linked to safety analysis, particularly in disciplines such as nuclear, aerospace, and chemical engineering, where structured scenario identification has long been used to determine which events or system failures may be safety significant. In most contexts, safety significance is defined along two primary dimensions: the severity of potential consequences and the likelihood of occurrence. Together, these factors provide the basis for prioritizing hazards and identifying which systems, structures, or components require elevated levels of protection, reliability, or oversight.

- **Severity:** This refers to the potential impact of an adverse event related to a specific hazard. Severity is the magnitude of harm, damage, or loss that could result if an adverse event occurs.[1]
- **Likelihood:** This is the probability that an adverse event (associated with a particular hazard) occurs. A high likelihood means that an adverse event is more likely to happen, whereas a low likelihood indicates it is less probable.[2]

In many safety-critical industries, this qualitative assessment is further refined through the use of Safety Integrity Levels (SILs), a framework defined in standards such as IEC 61508 and IEC 61511 (further detailed in Appendix B).[3] SILs provide a quantitative measure of risk reduction required for safety instrumented functions (SIFs), based on the severity and likelihood of hazardous events. By assigning a SIL rating (from SIL 1 to SIL 4), organizations can determine the necessary reliability and performance requirements for safety systems, ensuring that the level of protection is proportionate to the risk. This approach complements traditional HA by introducing a structured, metrics-driven method for specifying and validating safety controls.

For any specific consequence (such as damage or disruption to a system, facility, or process), the level of concern is often based on how likely the scenario is to happen, where "likelihood" is expressed as a probability that accounts for randomness or uncertainty (i.e., stochastic probability). This is calculated as the probability of the determined initiating causes for the hazard, along with the probability that the immediate effects will propagate through the process (and through process deviation) to produce the undesired consequences. This includes the conditional stochastic probability of failure (or unavailability) of the identified controls that might otherwise arrest or mitigate the scenario. Complex scenarios, where the process deviation requires the occurrence of multiple independent events, are often discarded on the grounds of very low stochastic probability of their occurrence. Similarly, scenarios involving the failure of highly dependable controls, particularly passive safeguards, may be eliminated or overlooked as unrealistic.

Broadly speaking, most HA techniques focus on identifying deviations from process control intent. For example, in the case of Hazard and Operability Analysis (HAZOP), deviations may take the form of process parameter deviations such as “no flow,” “high pressure,” etc. In the case of Failure Mode and Effect Analysis (FMEA), deviations take the form of equipment failures such as “fails open,” “leaks,” etc. In both cases, these deviations are starting points for scenario development, which lead from the initial cause, through one or multiple deviations, and ultimately to an undesired consequence, such as a disruption of safety, reliability, or performance or damage to systems or facilities. As part of the HA process, engineers identify potential safeguards that can mitigate these consequences. Significantly, although the development of scenarios is a fundamental aspect of HA, most HA techniques do not specify the process by

[1] FEMA. “Severity.” https://emilms.fema.gov/is_0559/groups/338.html#:~:text=Severity-,Severity

[2] EPA. “Technical Guidance for Hazards Analysis Emergency Planning for Extremely Hazardous Substances.” December 1987. https://www.epa.gov/sites/default/files/2013-08/documents/technical_guidance_for_hazard_analysis.pdf.

[3] IEC. “Safety and Functional Safety: IEC 61508 & Functional Safety.” Government Website. 2022. https://www.iec.ch/functional-safety.

which the scenarios are developed, other than requiring the identification of the potential causes of the deviation, the potential undesired consequences (typically the maximum credible undesired consequences), and any existing controls. Without guidance, it is challenging to ensure comprehensiveness of scenario creation and development in HA.

Traditionally, the set of scenarios developed from the identified process deviations involve stochastic events (i.e., events that occur by chance). These events can be internal, external, man-made, natural, causal, exacerbating, or mitigating; however, currently cyber-induced or actuated events are not considered. Ideally, the HA scenarios comprehensively characterize the credible (probabilistically likely) ways that undesired consequences might be produced.

HA often concludes by making recommendations to improve the safety and/or reliability of the process and/or system under analysis. These recommendations typically focus on the most concerning hazard scenarios and are the result of interdisciplinary discussions that incorporate process knowledge, as well as system safety and risk management expertise. Heuristics such as the Hierarchy of Controls,[4] which identifies a preferred order of approach to control hazardous workplace exposures, may be used to prioritize potential mitigations.[5]

Successful application of HA for risk reduction can be challenging, particularly when hazard identification or reduction requires hazard modeling. To successfully model system abnormalities, an individual must identify the specific behaviors and activities that need to be built into the model, both normal and abnormal. Unfortunately, although minimal harm originates from overlooking *mild* hazards, more devastating results can stem from significant hazards. Because of this danger, many HA approaches emphasize the need for completeness when identifying potential hazards. At the same time, many of these approaches focus primarily on naturally occurring failures rather than those originating from cyber means.

3. Comparing Hazards Analysis and Cyber-Informed Engineering Applications

The CIE research team investigated existing HA methods (i.e., HAZOP, PRA, FMEA, STPA, HAZCADS, and LOPA) to understand if cyber-based disruptions are considered within these processes, as well as how CIE, and its associated 12 Principles outlined in the Cyber-Informed Engineering Implementation Guide,[6] can be used to enhance the mitigation of cyber-induced

[4] National Institute for Occupational Safety and Health (NIOSH)/CDC. “About Hierarchy of Controls.” Government Website. Hierarchy of Controls. Accessed August 6, 2025. https://www.cdc.gov/niosh/hierarchy-of-controls/about/index.html?CDC_AA_refVal=https%3A%2F%2Fwww.cdc.gov%2Fniosh%2Ftopics%2Fhierarchy%2Fdefault.html.

[5] The Hierarchy of Controls has five levels of action, in preferred order based on effectiveness: elimination, substitution, engineering controls, administrative controls, and personal protective equipment (PPE). See Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health, “Hierarchy of Controls,” last updated January 2023.

[6] *Cyber-Informed Engineering Implementation Guide*. INL/RPT-23-74072. Idaho National Laboratory, 2023. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf.

risks. This section begins by outlining the benefits of CIE for safety evaluations, the typical HA process at a high level, then evaluates its ability to account for cyber-induced consequences. It concludes with the INL research team presenting a CIE-modified HA approach, demonstrating how CIE can complement existing methods. As noted in the introduction, these CIE-enhanced approaches represent an initial, high-level integration of CIE with traditional HA practices that can serve as a guide for more formal integration on an individualized (i.e., organizational) basis.

3.1. Benefits of Cyber-Informed Engineering for Safety Critical Operations

Cyber-informed Engineering is an INL-developed approach that emphasizes the use of engineering controls to mitigate digitally induced malicious adverse impacts on safety, reliability, and performance (hazards) to a process or system. [7] Though mitigating information security risks to data (such as loss of confidentiality, availability, and integrity) by instilling specific cybersecurity protections is important, CIE extends this through mitigations that leverage engineering to reduce the potential for undesired impacts to safety, reliability, and performance. Traditional cybersecurity does not address these hazards; instead, it focuses primarily on protecting information flows and data.

Integrating CIE into HA methods ensures a more complete and realistic analysis of potential hazards and broadens the scope of risk assessment to include various loss types by ensuring that deliberate cyber manipulation is considered. Ultimately, this approach contributes to a more secure and reliable infrastructure, capable of withstanding and recovering from cyber-induced disruptions and/or failures.

Including CIE in HA methods can bring several benefits:

1. First, CIE **enhances the comprehensiveness of hazard identification** by incorporating cyber-related scenarios that traditional hazard models may overlook. This helps in reflecting the true adverse potential of cyber deviations, which may not be naturally occurring but are introduced by adversaries with malicious intent.
2. Second, CIE **emphasizes the importance of interdependencies** between cyber and physical systems. Information or data pathways, often underemphasized in traditional safety modeling, are crucial in cyber contexts. By integrating these paths into hazard methods, the analysis becomes more robust and reflective of real-world complexities.
3. Third, CIE considers **resilience, including recovery and restoration** activities, following a cyber-induced failure. This holistic approach ensures that the resources needed for recovery are identified and that the system's ability to bounce back from disruptions is evaluated and enhanced.
4. Additionally, a benefit of integrating CIE into existing HA processes is that **organizations can leverage their current investments in HA**. This integration allows them to extend their hazard assessments to include digitally induced hazards

[7] *Cyber-Informed Engineering.* Idaho National Laboratory, 2025. https://inl.gov/national-security/cie/.

without starting from scratch, maximizing the value of their existing safety infrastructure.

Table 1 illustrates the potential benefits that each CIE principle can bring to traditional HA processes. Table 1 focuses on how each principle enhances or complements the foundational goals of HA, such as identifying, assessing, and mitigating risks, by introducing cybersecurity-aware perspectives and how CIE builds on them. Beginning in Section 3.3, we expand on this foundation with a more detailed analysis that maps these principles to the selected HA methods, highlighting both areas of alignment and critical gaps where traditional approaches fall short of addressing cyber-physical threats.

Table 1. Outlining CIE's principles and the value they bring to traditional HA approaches.

CIE Principle	Relevance to Hazards Analysis (HA)
Principle 1. Consequence-Focused Design	Encourages HA to consider failure modes and consequences brought on by the use of digital technology and the ability for the technology or functions controlled by it to be unintentionally or intentionally manipulated.
Principle 2. Engineering Controls	Aligns with HA's focus on physical and automated safety systems. CIE emphasizes designing out cyber risks using engineering solutions rather than relying solely on software patches.
Principle 3. Secure Information Architecture	Traditional HA often overlooks data flow and communication pathways. This principle introduces the need to analyze how insecure architectures can become vectors for hazards.
Principle 4. Design Simplification	Simplified systems are easier to analyze and secure. This principle supports HA by reducing system complexity, which in turn reduces the number of potential failures or attack paths.
Principle 5. Layered Defenses	While HA considers redundancy and safety barriers, this principle adds a broader cybersecurity lens - ensuring multiple, diverse layers of defense against both physical and digital threats.
Principle 6. Active Defenses	Traditional HA is often passive/reactive. This principle introduces real-time monitoring and response capabilities, which can help detect and mitigate cyber-induced hazards before they escalate.
Principle 7. Interdependency Evaluation	Encourages HA to consider system-of-systems interactions, especially where cyber dependencies (e.g., shared networks or control systems) could propagate failures.
Principle 8. Digital Asset Awareness	Traditional HA may not consider how digital equipment can fail or be made to malfunction by an adversary and thus, the identified hazards are incomplete. This principle ensures that engineers consider how digital systems may be driven to malfunction and the impacts that could result.
Principle 9. Cyber-Secure Supply Chain Controls	A major blind spot in HA. This principle highlights the need to evaluate supply chain risks, such as compromised components or software, which can introduce latent hazards.

Principle 10. Planned Resilience	Supports HA by promoting designs that can recover from disruptions, including cyberattacks - moving beyond prevention to include recovery and continuity.
Principle 11. Engineering Information Control	Traditional HA rarely considers how design and operational data is protected. This principle ensures that sensitive engineering information is not a vector for attacks.
Principle 12. Organizational Culture	HA typically focuses on technical systems. This principle emphasizes the human and cultural factors (e.g., training, awareness, and leadership) that influence both safety and cybersecurity outcomes.

3.2. Deviations between Cyber-Informed Engineering and Traditional Hazards Analysis

Traditional HA methods that focus solely on physical safety without considering cyber factors can systematically overlook scenarios where digital compromises lead to cascading failures. These scenarios include physical harm, outages, or cascading operational failures, which can be devastating to critical infrastructure operations. Failing to address cyber risks during HA can lead to significant operational disruptions, safety hazards, financial losses, theft of operational information, compromised reliability and trust, increased recovery times, and elevated costs. Table 2 includes examples of potential consequences that could result from incomplete HA evaluations.

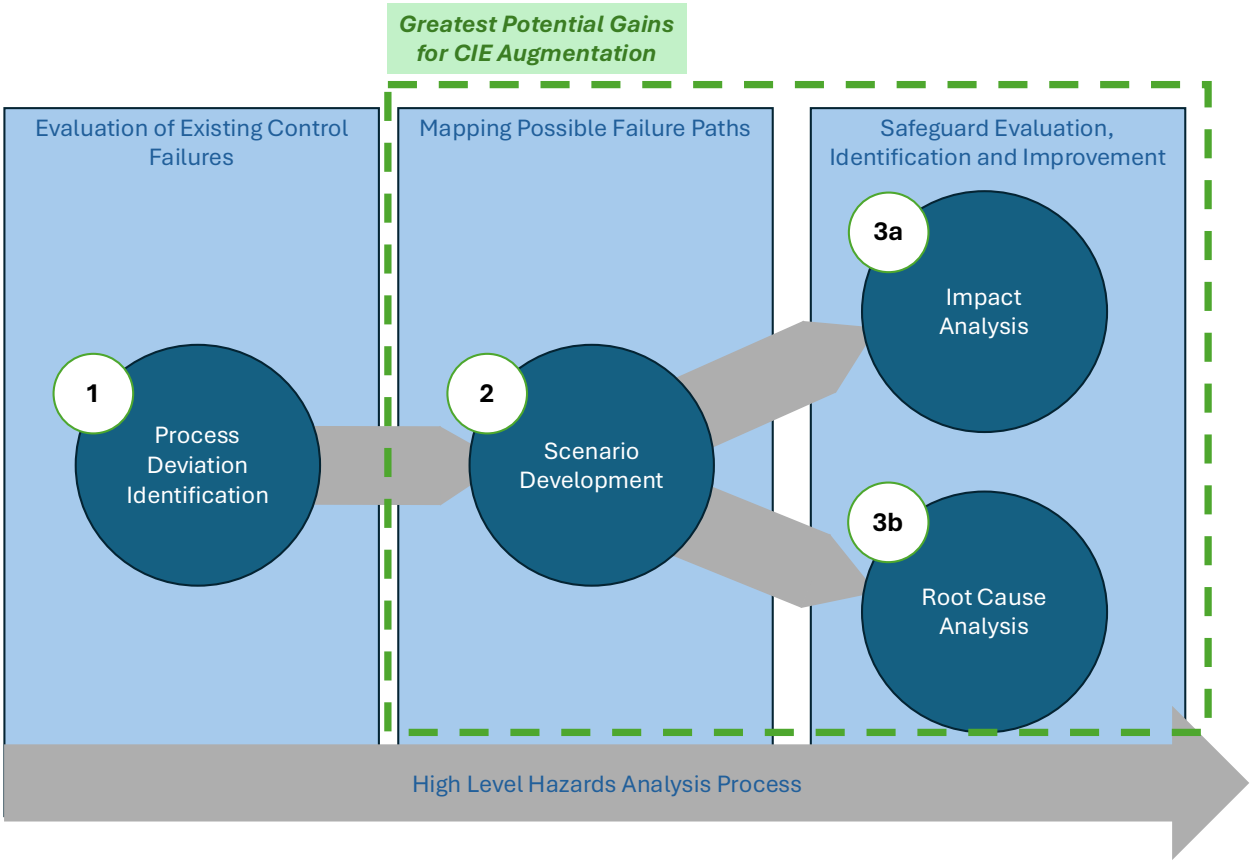
Table 2. Risks and consequences of not including cyber considerations in the HA process.

Risk(s)	Potential Consequence(s)
Incomplete Identification of Failure Modes	Cyber-induced hazards (e.g., operator error based on falsified sensor data or loss of control caused by malicious commands) are not captured, resulting in blind spots within systems.
Hidden Single Points of Failure	Interconnected systems (e.g., cloud services, vendor remote access) could fail simultaneously or result in cascading failures, leading to widespread outages.
Safety Hazards	Cyber incidents can compromise safety-critical systems, leading to dangerous situations such as chemical spills or catastrophic equipment failures, posing serious threats to human life and the environment.
Operational Disruptions and/or Failures	Cyberattacks can disrupt and/or cause failures within operations, resulting in unexpected shutdowns, system malfunctions, and loss of productivity.
Financial Losses	Direct and indirect costs arise from downtime, loss of production, incident response, legal liability, and reputational damage.
Loss of Intellectual Property and/or Theft of Operational Information	Cyberattacks can target sensitive information, leading to the theft of intellectual property or theft of operational information.
Increased Recovery Time and Costs	Reactively addressing cyber incidents can lead to extended recovery times and higher costs to restore normal operations.

Integrating cyber considerations into HA offers key benefits: comprehensive risk visibility, accurate consequence modeling, improved resilience planning, and reduced blind spots. This ensures all potential hazards are accounted for and provides better decision-making.

Although HA methods vary in implementation, many share a common structure and approach. In the context of integrating CIE, the primary enhancements are not centered on the identification of process deviations but rather on the subsequent stages: scenario development, safeguard evaluation, and recommendation formulation (i.e., steps 2, 3a, and 3b in Figure 1). Additionally, because these downstream activities are broadly applicable across HA methods, many CIE modifications and enhancements necessary to incorporate adversary-informed perspectives and cyber-induced failure modes can be implemented across the collective hazard review methods rather than tailored to individual HA techniques.

Figure 1. A generic and high-level process flow for hazards analysis.[8]



Considering the process of identifying the root cause of deviation, CIE greatly expands HA. CIE evaluates deterministic causes stemming from intentional or adversarial behaviors, in addition to stochastic failures, and ensures that digitally-induced hazards are also evaluated. Unfortunately, these events cannot be analyzed probabilistically but instead must be considered based on

[8] It should be noted that the order of impact and root cause analysis can be reversed.

plausibility or feasibility. For example, a cyberattack may involve an orchestrated sequence of discrete events that exploit process knowledge for greatest impact. At the same time, attackers may exploit unknown or unidentified vulnerabilities, a reality that challenges comprehensive identification of potential cyberattack pathways. It should be noted, however, despite these challenges, HA can provide value, particularly to determine if information streams or data pathways are accessible to an attacker. Additionally, HA can illuminate potential safeguard failures, individually or in combination, that could enable a cyberattack.[9]

For instance, when analyzing cyberattack scenarios, traditional stochastic failure probabilities cannot be relied upon for safeguards that are accessible (directly or indirectly) through digital pathways. Such safeguards could be deliberately disabled or manipulated during an attack, meaning their historical reliability data (based on normal operations without malicious interference) does not apply. Instead, stochastic probabilities should only be used for safeguards that are beyond the reach of a digitally-enabled adversary and thus remain immutable. In practice, this means giving 'no or low credit' to any safeguard that an attacker could potentially access.

With respect to understanding *deviations* and undesired consequences (including the identification of mitigative safeguards), traditional HA processes are theoretically adequate, provided that scenarios are fully developed and not dismissed solely on probabilistic grounds. Put another way, traditional hazards analysis methods can work well for identifying problems and safeguards, but only if all scenarios are fully explored and not dismissed just because they seem unlikely. In practice, however, scenario development often depends on probabilistic reasoning to filter out or downplay low-likelihood events. This creates a blind spot for adversary-driven failures, which do not follow traditional probability patterns - a limitation noted by several researchers.[10,11, 12, 13]

Another “blind spot” arises from how HA is typically framed in engineering practice. Although guidance often states that HA applies across a product or system’s lifecycle, many documents

---

[10] Cormier, Addie, and Christopher Ng. “Integrating Cybersecurity in Hazard and Risk Analyses.” *Journal of Loss Prevention in the Process Industries* 64 (March 2020). https://doi.org/10.1016/j.jlp.2020.104044.
[11] Sornette, D., T. Maillart, and W. Kroeger. “Exploring the Limits of Safety Analysis in Complex Technological Systems.” arXiv:1207.5674. Preprint, arXiv, April 3, 2013. https://doi.org/10.48550/arXiv.1207.5674.
[12] Paté-Cornell, Elisabeth. “On ‘Black Swans’ and ‘Perfect Storms’: Risk Analysis and Management When Statistics Are Not Enough.” *Risk Analysis* 32, no. 11 (2012): 1823–33. https://doi.org/10.1111/j.1539-6924.2011.01787.x.
[13] Leveson, Nancy G. *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, 2012. https://direct.mit.edu/books/oa-monograph/2908/Engineering-a-Safer-WorldSystems-Thinking-Applied.

encourage initiating HA early in design to minimize rectification costs.[14, 15, 16, 17] Consequently, most HA methods emphasize early-stage review, whether for new builds (i.e., greenfield) or major retrofits (i.e., brownfield), while offering little guidance on continued analysis for ongoing operations and maintenance (O&M). Yet, O&M is the stage most susceptible to disruption from emerging cyber threats, where evolving adversary capabilities can undermine earlier assumptions. During the review and integration process, the CIE research team observed that some CIE principles align naturally with existing HA practices, but others are absent from formal engineering processes (Figure 2). This gap highlights the need to revisit and validate past HA outputs to ensure they remain comprehensive and accurate.

Figure 2. The 12 CIE Principles.[18]

CIE Principles

1. Consequence-focused Design
2. Engineered Controls
3. Secure Information Architecture
4. Design Simplification
5. Layered Defenses
6. Active Defense
7. Interdependency Evaluation
8. Digital Asset Awareness
9. Cyber-Secure Supply Chain Controls
10. Planned Resilience
11. Engineering Information Control
12. Organizational Culture

CIE encourages that CIE principles be applied throughout the product lifecycle as reflected within the *CIE Implementation Guide*.[19] However, the thoroughness and vigor with which these CIE principles can be applied varies throughout the lifecycle. For example, although organizations may be aware of some of the digital assets that will be procured or used at the

[14] Würtenberger, J, H Kloberdanz, and J Lotz. "APPLICATION OF THE FMEA DURING THE PRODUCT DEVELOPMENT PROCESS – DEPENDENCIES BETWEEN LEVEL OF INFORMATION AND QUALITY OF RESULT." Paper presented at International Design Conference. *DS 77: Proceedings of the DESIGN 2014 13th International Design Conference*, Design Society, 2014. https://www.designsociety.org/publication/35186/application_of_the_fmea_during_the_product_development_process_%E2%80%93_dependencies_between_level_of_information_and_quality_of_result.

[15] Mayer, Lauren, William Shelton, Christian Johnson, et al. *Improving the Technical Requirements Development Process for Weapon Systems: A Systems-Based Approach for Managers*. RAND Corporation, 2022. https://doi.org/10.7249/RRA997-1.

[16] Maher, Steven T, Pe Csp, and Steve Maher. "Preparing for a Successful HAZOP/LOPA (Making or Breaking Quality & Efficiency)." Paper presented at Global Congress on Process Safety, Orlando, FL. *2018 Spring Meeting and 14th Global Congress on Process Safety*, American Institute of Chemical Engineers, April 22, 2018. https://www.rmpcorp.com/wp-content/uploads/2020/11/513595.PreparingForASuccessful.HAZOP_.LOPA_.GCPS-2018.PAPER_.Rev_.2018.04.25.pdf.

[17] Kovesdi, Casey, Paul Hunton, Jeremy Mohon, et al. *Demonstration and Evaluation of the Human-Technology Integration Function Allocation Methodology*. INL/RPT-22-68472-Rev000, 1881859. Idaho National Laboratory, 2022. https://doi.org/10.2172/1881859.

[18] Those highlighted in green are integrated into one of the CIE-enhanced HA approaches introduced later in this section.

[19] *Cyber-Informed Engineering Implementation Guide*. INL/RPT-23-74072. Idaho National Laboratory, 2023. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf.

start of a project, in many cases the level of detail is insufficient for a complete digital asset inventory. The *Digital Asset Awareness* principle in early stages of the engineering lifecycle calls for examination of the consequential functions which are dependent on digital technology generally and where risk due to that dependency can be averted. In later stages, where the specific digital technology has been identified, the analysis can incorporate the specific nature or functions of the assets to be incorporated and even later, in O&M, *Digital Asset Awareness* analyzes changes to the digital asset over time and potential risks introduced by the changes. Table 3 illustrates each of the selected HA methods, evaluated against each of the twelve CIE principles, with alignment marked where our analysis deemed applicable. Among the methods assessed, STPA (System-Theoretic Process Analysis) demonstrated the highest alignment, addressing seven out of the twelve CIE principles. This suggests STPA's broader applicability in integrating cyber considerations into engineering design; however, STPA still lacks five of the CIE principles.

It is worth noting that CIE Principle 9 Cyber-Secure Supply Chain Controls (abbreviated as P9 in the table) and Principle 12 Organizational Culture (abbreviated as P12 in the table) were not addressed by any of the HA methods. This gap is particularly critical for supply chain security, which represents one of the most pressing and underrepresented areas in traditional HA when viewed through a cyber-informed lens. The absence of alignment here highlights a major disconnect between what CIE aims to achieve and what conventional HA methods currently offer.

Table 3. Hazards Analysis methods evaluated against each of the twelve CIE principles.

Cyber-Informed Engineering (CIE) Principle	Hazards Analysis (HA) Methodology						
	HAZOP	PRA	FMEA	STPA	HAZCADS	LOPA	Total CIE Principles Present Over All HA Methods
P1. **Consequence-Focused Design**	✓	✓	✓	✓	✓	✓	6
P2. **Engineering Controls**	✓	✓	✓	✓	✓	✓	6
P3. **Secure Information Architecture**	✓	✓	✓	✓		✓	5
P4. **Design Simplification**				✓	✓		2
P5. **Layered Defenses**		✓		✓		✓	3
P6. **Active Defenses**		✓			✓		2
P7. **Interdependency Evaluation**				✓			1
P8. **Digital Asset Awareness**	✓		✓	✓	✓		4
P9. **Cyber-Secure Supply Chain Controls**							0
P10. **Planned Resilience**	✓		✓				2
P11. **Engineering Information Control**		✓			✓	✓	3
P12. **Organizational Culture**							0

Total CIE Principles in HA Method	5	6	5	7	6	5

By placing primary emphasis on early-stage HA, many organizations unintentionally limit the applicability of certain CIE principle focus areas, particularly when the goal is to *supplement* existing HA processes rather than completely redesign them. In these cases, later lifecycle phases, such as operations and maintenance, may receive less attention, leaving gaps where emerging cyber threats could undermine system safety or reliability. Conversely, a more comprehensive and consistently applied HA and one that explicitly incorporates all relevant CIE principles across every stage of the system lifecycle, can deliver the most effective outcomes. This approach ensures that HA is not a one-time design activity but an ongoing discipline capable of adapting to evolving threats, changing operational conditions, and new engineering insights.

Included in the remaining part of Section 3 are examples of how CIE principles and concepts could be applied to either: 1) improve the quality of the HA or 2) ensure comprehensiveness of these HA approaches. The research team has also included the most relevant questions from the CIE Implementation Guide;[20] however, it should be noted that these questions should not be considered all-inclusive and additional questions within the guide may prove valuable.

3.3. Hazard and Operability Analysis (HAZOP)

HAZOP (Hazard and Operability Analysis) involves a systematic review of a process or operation to identify potential deviations from the design or operational intent that could lead to undesirable consequences. HAZOP is widely used in process industries (e.g., chemical, pharmaceutical, oil) to identify safety and operability issues before they occur.[21] HAZOP is commonly the default HA approach within process engineering and is often used as a starting point for risk analysis to identify high risk scenarios. For example, a HAZOP team could evaluate a chemical manufacturing plant's reactor system. This involves a systematic review of the process parameters, such as temperature and pressure, to identify potential deviations. During the HAZOP study, an operator might provide system-specific expertise to help identify causes, such as a blocked cooling line, and consequences, such as a runaway reaction, when the reactor temperature exceeds the design limit due to a cooling system failure. The team would document existing safeguards, such as automatic shutdown systems, and suggest additional mitigations, like enhancing monitoring of the cooling system. (Figure 3 represents a typical discussion record format for a HAZOP study.)

[20] Ibid.

[21] Shikhaliyev, Ramiz. *Cybersecurity Risks Management of Industrial Control Systems: A Review*. 15, no. 1 (2024): 37–43. http://dx.doi.org/10.25045/jpit.v15.i1.05.

Figure 3. Typical format for a HAZOP Study worksheet.[22,23]

Team: HAZOP Team #3 Meeting Date: ##/##/##				Drawing Number: 70-0BP-57100 (Figure 5.5) Revision Number: 3	
Item	Deviation	Causes	Consequences	Safeguards	Actions
Study node, process section, or operating step description. Definition of design intention.					
1.1					

Completeness in HAZOP is achieved if all deviations and their causes are identified and their consequences understood. The deviations considered are typically specified by standard lists of guide words[24] (e.g., more, less, none, reverse), but identifying deviation causes and consequences involves human creativity, ingenuity, and significant system understanding.

HAZOP WITHIN THE CYBER CONTEXT

HAZOP can be extended to cyber scenarios by treating cyber faults or attacks as potential causes or initiators of hazardous deviations.[25] In some cases, companies have modified traditional HAZOP approaches to consider an intelligent, malicious cyber actor; however, successful application to the cyber domain requires engineers and operators to consider the deliberate modification and manipulation of safeguards, sensors, or data flows. As a start, this means including cyber-related guide words or failure modes (e.g., unauthorized command, data corruption, loss of view) in the HAZOP analysis.[26] Later on, more mature consideration of cyber-risks must evaluate potential deviations not considered in the initial assumptions of the HAZOP analysis. This should be done as a partnership between cyber and engineering organizations.

A summary of HAZOP alignment to and deviation from CIE is included in Table 4 and aggregated comparisons across all HA approaches evaluated are included in Appendix A. The following

---

[22] Rosyidiin, Afrigh Fajar, Agung Nugroho, and Haidar Natsir Amrullah. "Risk Analysis Using the Layer of Protection Analysis Method on Reactor Platforming in the Petrochemical Industry." *Conference of Safety Engineering and Its Application* 2581 (n.d.). https://journal.ppns.ac.id/index.php/seminarK3PPNS/article/download/785/635/.

[23] Notably, this worksheet is also an example of engineering HA that prioritizes prevention and overlooks recovery planning.

[24] A word used to help guide the team into thinking of scenarios which may introduce hazards.

[25] It is worth noting that HAZOP has yielded variants that may have greater applicability to the cyber domain. For example, CHAZOP (Control Hazard and Operability Study) was specifically designed to analyze the safety and reliability of control and computer systems. It focuses on identifying potential failures within control systems, including hardware, software, human factors, cybersecurity, and external factors like power failures. The primary objectives of CHAZOP are to identify possible causes of process upset due to control system failures, assess the consequences of these failures, and recommend design changes or further studies to mitigate identified risks. CHAZOP is typically performed after a traditional HAZOP study and provides critical information needed for Safety Integrity Level (SIL) determination. It is particularly useful for ensuring the reliability and safety of control systems in industrial settings.

[26] This aligns with the IEC 61511 functional safety standard, which now explicitly requires a cybersecurity risk assessment (sometimes called "cyber PHA") of safety instrumented systems (SIS) to identify where all safety barriers could be compromised by an adversary.[26]

table highlights specific features of the reviewed HA method but is not all-inclusive of variations between HAZOP and CIE.

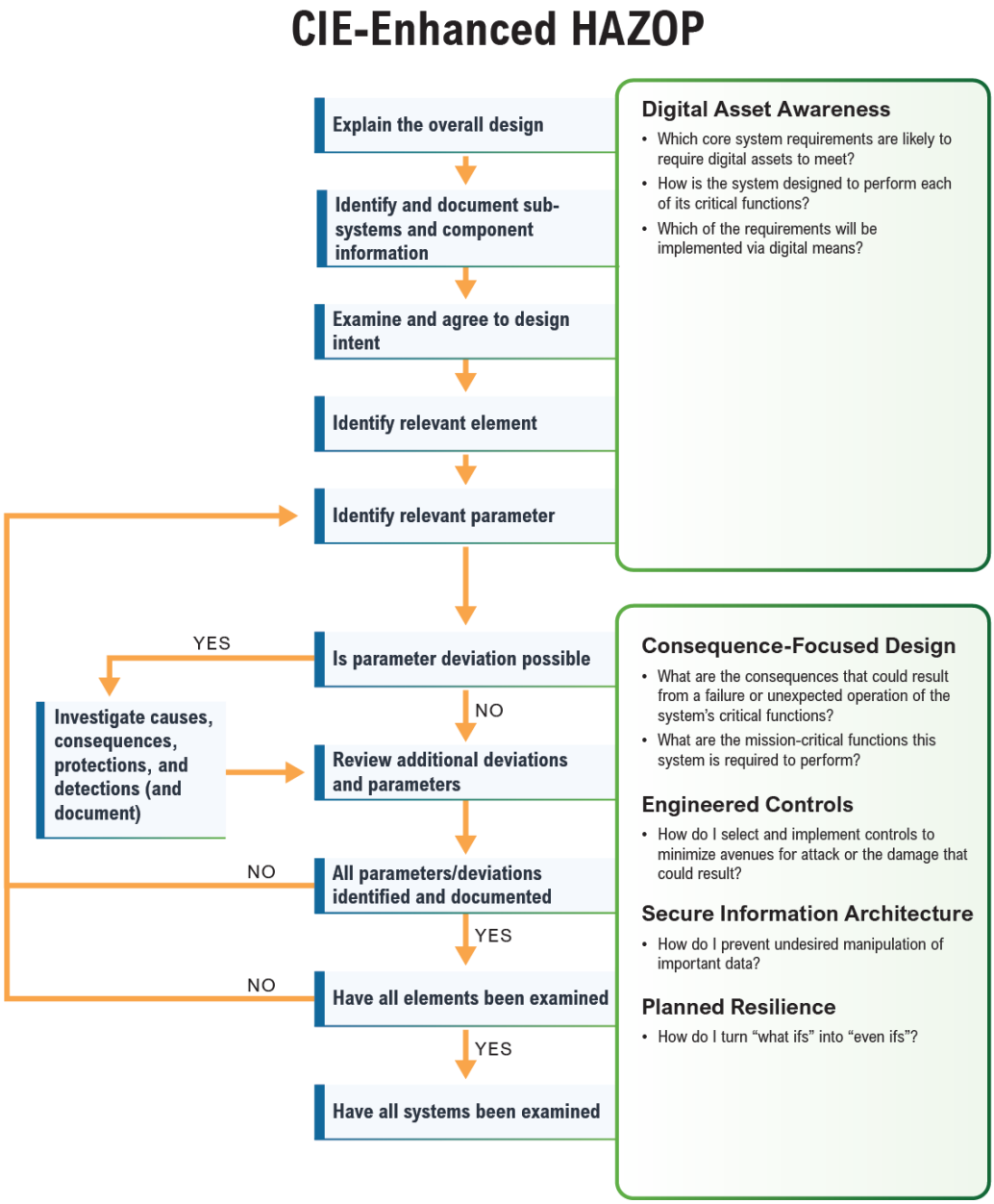
Table 4. A review of HAZOP as compared to CIE.

Gaps and Limitations	Alignment with CIE	Divergence from CIE	CIE Adoption Recommendations
May not account for an intelligent, malicious adversary that manipulates or disrupts safeguards and information flows. May miss cyber-initiated deviations unless the team has cyber expertise.	HAZOP and CIE are both consequence-focused and seek to mitigate the most devastating consequences first. HAZOP is structured around deviations in process flows and/or procedural steps, which is naturally extendible to information flows and digital commands.	HAZOP focuses on independent discrete failure events associated with hazards. In contrast, CIE is very concerned with cascading failures (like those instigated via a cyberattack). Supply chain risks are not accounted for within the HAZOP approach.	HAZOP can be augmented to include the process' information flows in addition to the traditional process flows and procedures. For each information flow, design intent can be defined in terms of the expected information, and deviations can be defined in terms of how that information might be corrupted. This will result in the development of additional scenarios associated with each informational deviation. Alter HAZOP probabilistic prioritization of deviations with consequence – aligning it to CIE. Review the twelve CIE principles and associated questions within the *Implementation Guide*, to improve the completeness of HAZOP review. Studiously evaluate the resilience of safety barriers: how could they be degraded or manipulated. Leverage the CIE framework to identify engineering controls to augment any safety controls.

CIE-ENHANCED HAZOP

Figure 4 demonstrates how a traditional HAZOP process can be enhanced with Cyber-Informed Engineering (CIE) principles. It guides users through examining system design, identifying elements and parameters, and investigating deviations, while incorporating CIE principles such as *Digital Asset Awareness*, *Consequence-focused Design*, *Engineering Controls*, *Secure Information Architecture*, and *Planned Resilience*. (Although there are 12 CIE Principles (Figure 2), this subset is most relevant to HAZOP.) The result is a structured way to analyze causes, consequences, and protections while ensuring cyber and mission resilience are built into system reviews.

Figure 4. A CIE augmentation of traditional HAZOP approaches.[27]



3.4. Probabilistic Risk Assessment (PRA)

Probabilistic Risk Assessment (PRA) is a systematic and comprehensive framework used to evaluate risks associated with complex engineered systems (particularly within nuclear power plants).[28] Due to the complexity of these systems, modeling tools are critical to understand and identify all of the various hazards scenarios. However, the effectiveness of PRA is based partially on the completeness of these modeling tools which can overlook an intelligent adversary. Additionally, PRA focuses on unintentional initiating events, analyzing the likelihood that such events could lead to significant disruptions or failures. It assesses risk by estimating the likelihood and severity of potential adverse outcomes. PRA typically involves the following high-level steps:

- List possible initiating events (equipment failures, operator errors, external hazards) and estimate their frequencies.
- Build fault trees for each undesired "top event" (e.g. core damage, reactor scram failure). The fault tree decomposes the top event into combinations of basic events using logical gates.
- Assign probabilities (or rates) to each basic event (from data or expert judgment). Solve the fault trees to compute the probability of the top event.
- For key initiating events, draw event trees to capture possible success/failure of safety responses, leading to different outcomes and their frequencies.
- Quantify the consequences of each outcome (e.g., release magnitude, damage). Combine with frequencies to evaluate risk (e.g., probability of exceeding a certain release).
- Compare calculated risk against acceptance criteria. Identify dominant risk contributors for mitigation.

Over decades, nuclear power plants and other industries have used PRA to support safety decisions and design improvements. For example, an engineer could conduct a PRA to evaluate the risk of a nuclear plant's core melt due to a loss of coolant accident (LOCA). The engineer would list possible initiating events, such as pipe ruptures or valves failing to reseat, and create fault trees to analyze combinations of failures leading to core damage. The probabilities of these events would be quantified, and the engineer would assess the overall risk. Based on the analysis, they might recommend the addition of mitigations like redundant cooling systems and enhanced inspection protocols.

---

[27] Choi, Jae-Young, and Sang-Hoon Byeon. "HAZOP Methodology Based on the Health, Safety, and Environment Engineering." *International Journal of Environmental Research and Public Health (IJERPH)*, May 2020. http://dx.doi.org/10.3390/ijerph17093236.

[28] U.S. Nuclear Regulatory Commission. "Backgrounder On Probabilistic Risk Assessment." Government Website. Accessed August 29, 2025. https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/probabilistic-risk-asses.html.

PRA WITHIN THE CYBER CONTEXT

In principle, PRA can be applied to cyber risk by treating cyber events (or attack chains) as initiating events in a fault/event tree model. For example, one could assess the probability of a successful cyber intrusion and the failure of physical safety responses, to calculate combined risk. Some early research explores this: for instance, "dynamic PRA" methods consider time-dependent attack sequences in power grids.[29] Adapting PRA faces challenges: cyber threats evolve and do not follow stationary failure rates, and data on attack frequencies is scarce. However, efforts exist to apply PRA concepts to industrial control systems (ICS) cybersecurity. For example, Ralson et al. applied PRA to assess SCADA/DCS cyber risk.;[30] Diao et al. applied it to electric grid operations; and in the nuclear sector, software tools like "Risk Watch" incorporate PRA-like methods for cyber risk in power plants.[31]

In safety-critical ICS applications (e.g., nuclear), cybersecurity might be integrated into existing PRA frameworks. IEC 61511 calls for security risk assessments of safety systems (see HAZOP section), which can be interpreted as adding "cyber-fault trees" to the traditional PRA. For example, the Sandia HAZCADS approach effectively is a form of cyber-PRA (combining hazards tree analysis with logic modeling and cyber risk inputs).[32]

Overall, while PRA is well-established for physical failures, its direct use for cyber risks is still emerging. Its requirement for quantitative probabilities and well-defined consequences makes it harder to apply to the cyber domain, which still operates without the large dataset need to calculate realistic probabilities. However, it is worth noting that despite PRA's inability to address intelligent adversaries, the system-based philosophy aligns with cyber-physical risk philosophy; ICS operators can benefit from treating cyber and safety events under a common probabilistic framework.

A summary of PRA alignment to and deviation from CIE is included in Table 5 and aggregated comparisons across all HA approaches evaluated are included in Appendix A. The following table highlights specific features of the reviewed HA method but is not all-inclusive of variations between PRA and CIE.

Table 5. A review of PRA as compared to CIE.

Gaps and Limitations	Alignment with CIE	Divergence from CIE	CIE Adoption Recommendations

[29]Diao, Xiaoxu, Yunfei Zhao, Carol Smidts, et al. "Dynamic Probabilistic Risk Assessment for Electric Grid Cybersecurity." *Reliability Engineering & System Safety* 241 (January 2024): 109699. https://doi.org/10.1016/j.ress.2023.109699.

[30] Ralston, P. A. S., J. H. Graham, and J. L. Hieb. "Cyber Security Risk Assessment for SCADA and DCS Networks." *ISA Transactions* 46, no. 4 (2007): 583–94. https://doi.org/10.1016/j.isatra.2007.04.003.

[31] Francia, Guillermo A, David Thornton, and Joshua Dawson. *Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems*. n.d.

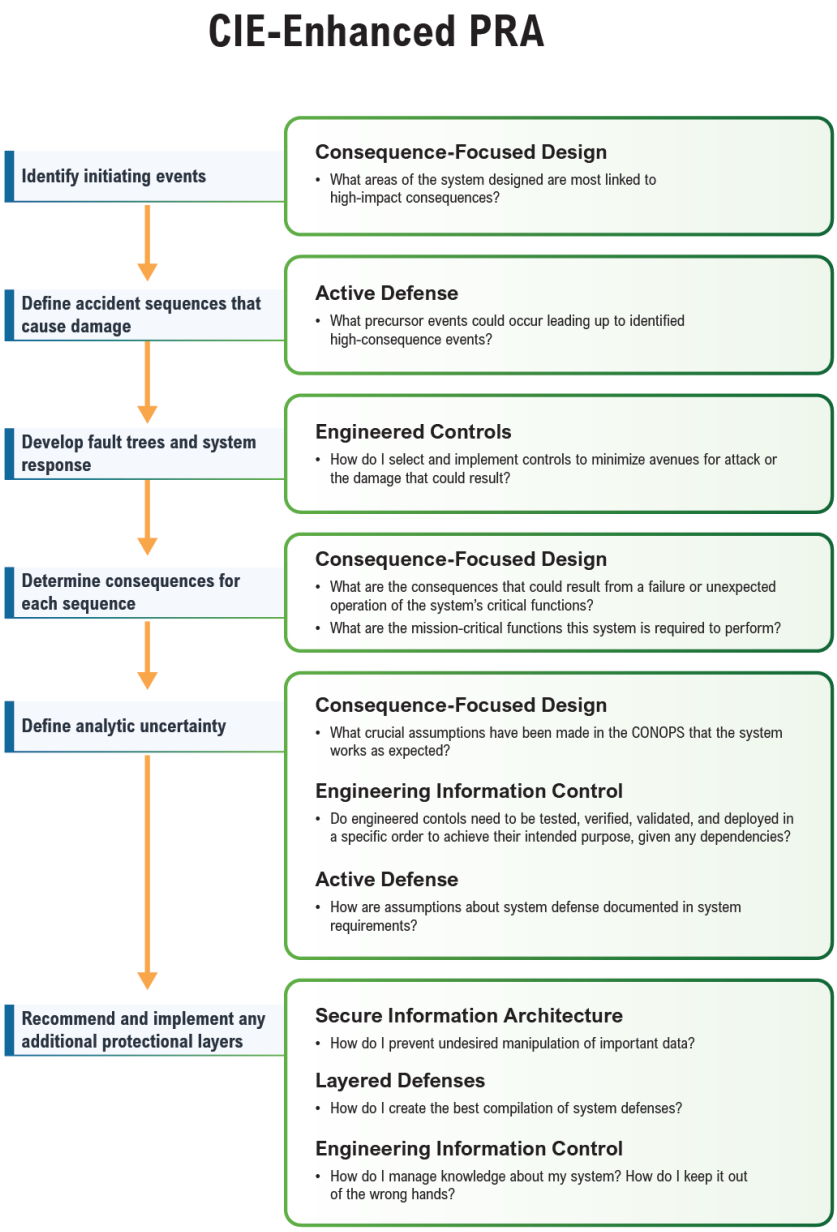
[32] Sandia National Laboratories. "Nuclear Energy Cybersecurity by Design." Government Website. Accessed September 2, 2025. https://energy.sandia.gov/programs/nuclear-energy/nuclear-energy-security/nuclear-energy-cybersecurity-by-design/.

PRA's reliance on expert interpretation to inform probabilities (particularly regarding low-frequency events) may result in some adverse events as being discarded as improbable. PRA treats safeguards as "static" and immutable, which is unrealistic given an intelligent adversary. Additionally, safeguards address initiating events and potential adverse impacts but may ignore defensive or resilience gains from post-event mitigations (e.g., intrusion detection, incident response).	PRA framework already emphasizes the need to define the significant consequence (in alignment to CIE). Provides a structured approach to risk assessment and emphasizes an understanding of the system's data flows.	As a safety-centric method, PRA does not account for deliberate, adaptive adversary behavior (e.g., a threat actor bypassing controls, targeting interdependencies, or disrupting key information exchanges). For example, layered safety controls or safeguards are considered sufficient despite deliberate and targeted manipulation of controls by an adversary. Supply chain risks are not accounted for within the PRA approach.	PRA origins focus on the importance of understanding data and information flows within a system, similar to STPA's emphasis on Unsafe Control Actions (UCAs). Practitioners should be aware that probabilities may be misleading or unknowable, particularly when considering cyberattacks. When considering safeguards, emphasize the importance of diverse and varied safeguards (which could challenge adversary actions). Specifically, the most comprehensive defensive posture stems from a combination of physical and cyber safeguards.

CIE-ENHANCED PRA

Figure 5 outlines how PRA can be enhanced with CIE principles. It follows the PRA workflow (i.e., identifying initiating events, defining accident sequences, building fault trees, determining consequences, and addressing uncertainty), while overlaying CIE considerations such as *Consequence-focused Design*, *Active Defense*, *Engineered Controls*, *Secure Information Architecture*, *Layered Defenses*, and *Engineering Information Control*. (Although there are 12 CIE Principles (Figure 2), this subset is most relevant to PRA.) By integrating these questions and safeguards, the approach ensures both safety and resilience against cyber-induced failures. The outcome is a more robust risk assessment process that anticipates high-consequence events and embeds protective layers into system design and operation.

Figure 5. A CIE-enhanced PRA process flow.[33,34]



[33] Melnyk, Richard. "A Framework for Analyzing Unmanned Aircraft System Integration into the National Airspace System Using a Target Level of Safety Approach." Georgia Institute of Technology, 2013. http://rgdoi.net/10.13140/RG.2.1.2910.1842.

[34] U.S. Nuclear Regulatory Commission. "Probabilistic Risk Assessment (PRA) | NRC.Gov." Accessed August 20, 2025. https://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html.

3.5. Failure Modes and Effects Analysis (FMEA)

Failure Modes and Effects Analysis (FMEA) is a systematic approach to identifying and prioritizing possible failures in a design, manufacturing, or assembly process, product, or service.[35] The method typically involves:[36]

- Defining the system, subsystem, or process under review.
- Breaking down the system into components or functions (e.g., valves, sensors, pumps, microcontrollers).
- Enumerating possible failure modes (e.g., "stuck valve," "controller lost communication").
- Determining each failure mode's effect on the system or safety and assign a severity level.
- Estimate the likelihood of each failure mode and its detection.
    - Often a Risk Priority Number (RPN) is calculated.

      $$RPN = Severity\ (S) \times Occurrence\ (O) \times Detection\ (D)$$
- Rank failure modes by risk and propose actions (e.g., redesign, redundancy, better maintenance and monitoring) to reduce high-risk failure modes.

For example, a design engineer could conduct an FMEA on the aircraft's hydraulic system. The engineer would break down the system into components and identify potential failure modes, such as a hydraulic pump failure. They would determine the effects on flight control and safety, assign severity levels, and estimate the likelihood and detectability of each failure. The engineer would then calculate the RPN and propose actions like installing redundant hydraulic systems and scheduling regular maintenance checks. Hazard analysis should be a structured activity conducted by trained analysts and supported by operations personnel.

FMEA WITHIN THE CYBER CONTEXT

FMEA can be adapted to include failure modes induced by a cyber adversary, as the method already considers failure of digital devices. A typical FMEA worksheet (see Figure 11) records the failure modes, their causes, effects, and the current controls in place, along with recommended actions to mitigate the failures. Within critical infrastructure, FMEA is more often applied to physical faults (e.g., sensor failure, equipment malfunction). Security frameworks, such as NIST SP 800-82, do not explicitly prescribe FMEA for cyber, but engineering teams could use it as one part of a holistic safety/security review. In principle, FMEA's method of examining each component's failure suits inclusion of software and network elements. However,

---

[35] Sharma, Kapil Dev, and Shobhit Srivastava. "Failure Mode and Effect Analysis (FMEA) Implementation: A Literature Review." *Journal of Advance Research in Aeronautics and Space Science* 5, nos. 1 & 2 (2018): 1–17.

[36] Akula, Shravan Kumar, and Hossein Salehfar. "Risk-Based Classical Failure Mode and Effect Analysis (FMEA) of Microgrid Cyber-Physical Energy Systems." *2021 North American Power Symposium (NAPS)*, IEEE, November 14, 2021, 1–6. https://doi.org/10.1109/NAPS52732.2021.9654717.

the method is qualitative and typically designed for random hardware failures; it does not inherently capture *intentional* cyber threats.

Figure 6. Example of an FMEA worksheet.[37]

Failure Modes and Effects Analysis (FMEA)
Failure Modes and Effects Analysis

Steps in the process	Failure Mode	Failure Causes	Failure effects	Likelihood of Occurrence (1-10)	Likelihood of Detection (1-10)	Severity (1-10)	Risk Priority Number (RPN)	Action To Reduce Occurrence of failure
1								
2								
3								
4								
5								
6								
7								
8								
9								
							Total RPN (sum of all PRNs)	

Failure Mode : what could go wrong?
Failure Cause: why would the failure happen?
Failure Effects: what would be the consequences of failure?

likelihood of Occurrence: 1-10 , 10 = very likely to occur
likelihood of Detection : 1-10 , 10 = very unlikely to detect
Severity: 1-10, 10 = most severe effect
Risk priority Number (PRN): likelihood of Occurrence x likelihood of Detection x Severity

For example, a CIE-based, "Cyber-FMEA" (C-FMEA) might list failure modes (Column 1 in Figure 6) like loss of process view (through malicious modification of sensor data) or loss of connectivity (through malware designed to brick controllers). The effects could include both safety impacts and cyber impacts. For example, if a PLC could be reprogrammed by an attacker, that scenario might be treated as a "failure mode" with high safety significance.

A summary of PRA alignment to and deviation from CIE is included in Table 6 and aggregated comparisons across all HA approaches evaluated are included in Appendix A. The following table highlights specific features of the reviewed HA method but is not all-inclusive of variations between FMEA and CIE.

Table 6. A review of FMEA as compared to CIE.

Gaps and Limitations	Alignment with CIE	Divergence from CIE	CIE Adoption Recommendations
FMEA scenarios are often prioritized	FMEA and CIE are both consequence-	FMEA is not well suited to the	FMEA should determine when safeguards are reachable via an information stream

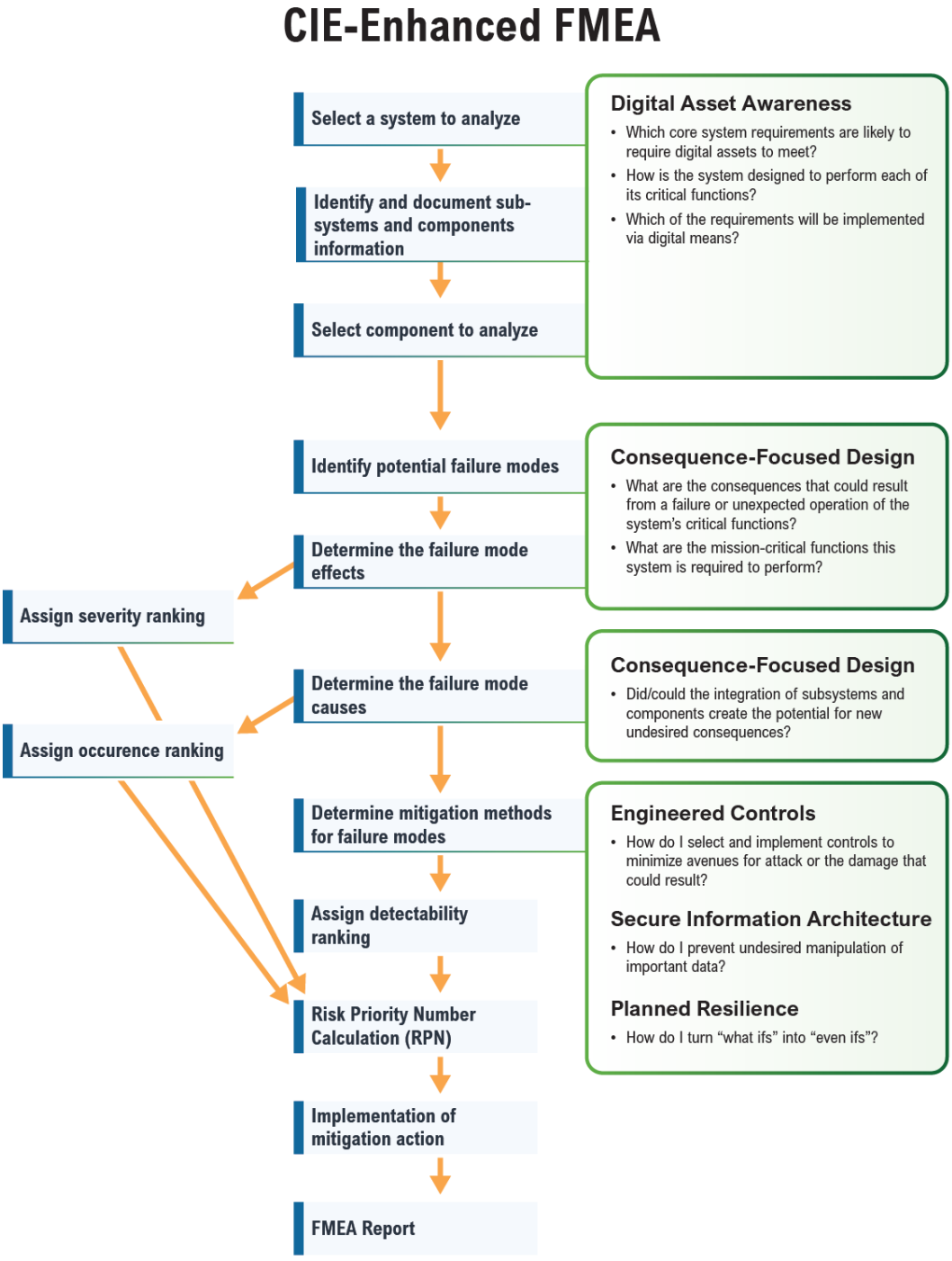
[37] "FMEA Worksheet | Risk Management in Healthcare Workshop." Accessed August 29, 2025. https://riskmngworkshop.wordpress.com/fmea/fmea-worksheet/.

based in part on stochastic probability, whereas cyberattacks are not amenable to stochastic analysis. May overlook complex attack chains and intent-driven scenarios without integration with security methods.	focused and concerned with avoiding the same set of undesired consequences. FMEA can be conducted throughout the systems engineering lifecycle. Systematic, component-level failure analysis can incorporate cyber-based failure modes.	identification of scenarios involving multiple independent failures, whereas CIE is concerned with orchestrated cyberattacks. FMEA-based scenarios are often prioritized based in part on stochastic probability, whereas cyberattacks are not amenable to stochastic analysis. FMEA is concerned with stochastic failures, not intentional adversarial events. Supply chain risks are not accounted for within the FMEA approach.	that is accessible by an adversary. In these instances, the efficacy of the safeguard should be considered. Validate that failure mode lists cover possible cyber events. Create separate/additional scoring for severity, occurrence, detectability within cyber in mind.

CIE-ENHANCED FMEA

Figure 7 illustrates how FMEA can be enhanced with CIE principles. The process follows standard FMEA steps (i.e., selecting a system and components, identifying potential failure modes, determining effects and causes, ranking severity, occurrence, and detectability, and calculating an RPN) but also includes CIE concepts such as *Digital Asset Awareness*, *Consequence-focused Design*, *Engineering Controls*, *Secure Information Architecture*, and *Planned Resilience*. (Although there are 12 CIE Principles (Figure 2), this subset is most relevant to FMEA.) Unlike the HAZOP or PRA enhancements, FMEA emphasizes **component-level analysis and prioritization of risks through scoring**, ensuring that mitigation actions are informed not just by likelihood and impact but also by cyber and mission resilience considerations. The outcome is an FMEA report that integrates both traditional reliability assessment and modern cyber-informed safeguards.

Figure 7. A modified FMEA process flow[38] that includes several CIE principles and associated questions.



3.6. System-Theoretic Process Analysis (STPA)

System-Theoretic Process Analysis (STPA), a newer hazards analysis technique, was designed to address shortcomings in existing HA methods. Specifically, STPA argues that a review of historical accidents indicates that HA methods which focus solely on component behaviors (like FMEA) or local process variable deviations (like HAZOP) would be inadequate to address risks.[39] STPA emphasizes the need for a more comprehensive approach to identify "Unsafe Control Actions (UCAs)" and to evaluate control actions within the broader system context, examining how interdependencies among components can amplify the effects of individual failures and lead to cascading disruptions.[40] The approach promoted by STPA is more comprehensive and provides a deeper understanding of system interactions, though it is often more complex to apply in practice. Additionally, STPA is particularly valuable during early design phases when as-built design documentation is not available.

The main purpose of STPA is to identify UCAs and causal scenarios for each UCA and to understand how system safety constraints may be violated.[41] For example, a systems engineer could use STPA to analyze a railway signaling system. The engineer would identify UCAs that could lead to train collisions, such as incorrect signal commands. They would model the control structure, considering interactions between components, and analyze causal scenarios for the UCAs. The engineer would then develop safety constraints to prevent these hazards, such as implementing fail-safes in the signaling process and communication checks.

STPA WITHIN THE CYBER CONTEXT

Unlike some of the other HA approaches reviewed by the CIE research team (e.g., HAZOP), STPA is more naturally aligned to CIE given that cyber components are included in the base STPA method. In fact, the comprehensive nature of STPA has resulted in other researchers (such as Sandia's HAZCADS team) leveraging STPA to identify UCAs in digital control systems.[42] Additionally, others have extended STPA to address security analysis of cyber and digital systems. STPA-Sec uses the same process but focuses more on cybersecurity losses as

[39] Leveson, Nancy G. "An STPA Primer." 2013. https://psas.scripts.mit.edu/home/wp-content/uploads/2013/10/An-STPA-Primer-version-0-4.pdf.
[40] Leveson, Nancy G. "An STPA Primer." 2013. https://psas.scripts.mit.edu/home/wp-content/uploads/2013/10/An-STPA-Primer-version-0-4.pdf.
[41] Teikari, Ossi. "CORSICA Task 4.1 Hazard Analysis Methods of Digital I&C Systems." VTT, August 2014. https://publications.vtt.fi/julkaisut/muut/2014/VTT-R-03821-14.pdf.
[42] Clark, Andrew, and Adam Williams. "HAZCADS – Hazard and Consequence Analysis for Digital Systems – Publications – Research." Sandia National Laboratories, October 1, 2019. https://www.sandia.gov/research/publications/details/hazcads-hazard-and-consequence-analysis-for-digital-systems-2019-10-01/.

UCAs.[43] For example, one study applies STPA-Sec to analyze how cyberattacks on an HVAC (Chiller) control system could violate safety constraints.[44]

Although STPA may be better suited than other HA methods to address cyber-induced hazards, this approach often overlooks a deliberate, malicious actor – one which seeks to subvert safety constraints. Because of this, STPA, as practiced, can assume the effectiveness of safety controls and that control systems will operate as intended. Unfortunately, past cyberattacks demonstrate the potential risk in this approach, as well as the need to design systems as resilient despite various methods of compromise (e.g., network-based attacks and campaigns, supply chain co-option, human-enabled compromise).[45]

A summary of STPA alignment to and deviation from CIE is included in Table 7 and aggregated comparisons across all HA approaches evaluated are included in Appendix A. The following table highlights specific features of the reviewed HA method but is not all-inclusive of variations between STPA and CIE.

Table 7. A review of STPA as compared to CIE.

Gaps and Limitations	Alignment with CIE	Divergence from CIE	CIE Adoption Recommendations
STPA can be difficult to implement, particularly when evaluating large, complex systems. Because of this, STPA is more sensitive to varying experience levels of users, and the effectiveness of application is highly dependent on user training.	STPA's focus on the importance of system-of-systems analysis aligns it naturally to CIE, which emphasizes the risk that can be introduced through complex system design and system interdependencies. Like CIE, STPA acknowledges the risk that can be	STPA takes into consideration human error, but it does not fully account for an intelligent malicious actor that disrupts the system through complex attacks. Additionally, although UCAs are helpful in illuminating potential safety issues, this emphasis is less effective in	Review questions within the *CIE Implementation Guide* to enhance the identification of UCAs specifically related to cyber threats. Ensure potential adversary actions are encompassed within UCAs (e.g., loss of view resulting from malicious modification of sensor data) so that safety constraints are effective. Assign individuals to specifically investigate the security and sanctity of safety controls: to what degree can these be manipulated or altered?

[43] Silawi, Ehab, Avi Shaked, and Yoram Reich. "TRANSLATING THE STPA-SEC SECURITY METHOD INTO A MODEL-BASED ENGINEERING APPROACH." *INCOSE International Symposium*, September 2024. https://www.researchgate.net/publication/383858664_TRANSLATING_THE_STPA-SEC_SECURITY_METHOD_INTO_A_MODEL-BASED_ENGINEERING_APPROACH.

[44] Khan, Shaharyar, Stuart E. Madnick, and Allen Moulton. "Cyber-Safety Analysis of an Industrial Control System for Chillers Using STPA-Sec." *SSRN Electronic Journal*, ahead of print, 2018. https://doi.org/10.2139/ssrn.3370540.

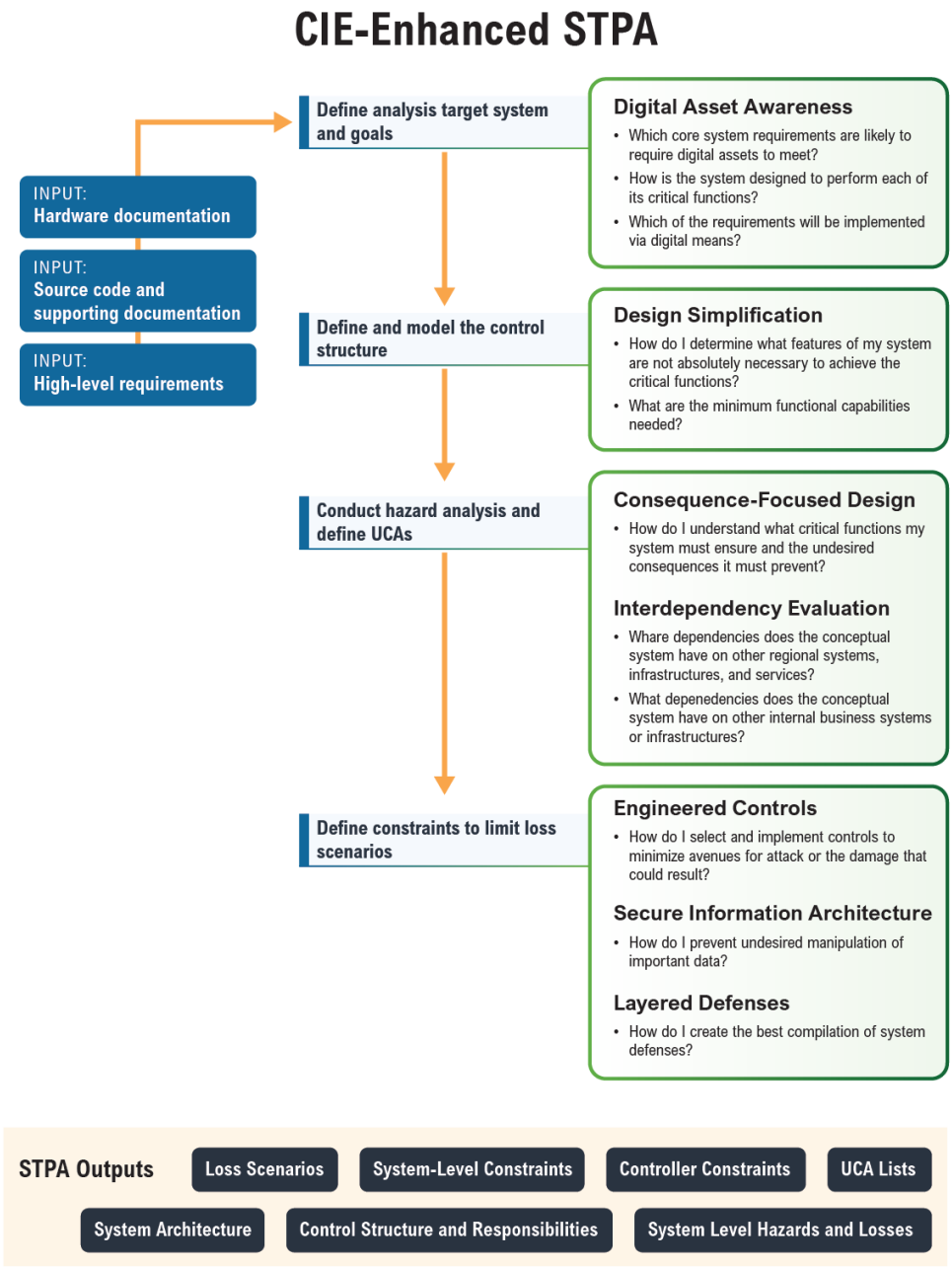
[45] Richard Danzig's "Surviving on a Diet of Poisoned Fruit" argues that modern societies are inevitably dependent on software riddled with vulnerabilities, making complete security unattainable. Instead, rather than pursuing absolute prevention, organizations should anticipate compromise and develop strategies for resilience that focus on limiting damage and ensuring continuity of critical functions. (Available here: Danzig, Richard J. "Surviving on a Diet of Poisoned Fruit." Center for a New American Security, July 2014. https://www.cnas.org/publications/reports/surviving-on-a-diet-of-poisoned-fruit-reducing-the-national-security-risks-of-americas-cyber-dependencies.)

STPA is based on intuitive causal analysis rather than past failure data and probabilities. STPA does not provide explicit guidance on how to consider a malicious adversary, leaving it up to the practitioner.	introduced through digital component failures.	understanding how system performance can be degraded. Supply chain risks are not accounted for within the STPA approach.	

CIE-ENHANCED STPA

Figure 8 displays how STPA can be enhanced with CIE. It begins with defining the system and goals, modeling the control structure, analyzing hazards and UCAs, and then establishing constraints to limit loss scenarios. CIE principles such as *Digital Asset Awareness*, *Design Simplification*, *Consequence-focused Design*, *Interdependency Evaluation, Engineered Controls*, *Secure Information Architecture*, and *Layered Defenses* are integrated throughout to address both safety and cyber resilience. (Although there are 12 CIE Principles (Figure 2), this subset is most relevant to STPA.) The process produces outputs like system architecture, hazards and losses, constraints, controller responsibilities, and UCA lists, ensuring a comprehensive, cyber-informed safety analysis.

Figure 8. A STPA process flow[46, 47] amended with the most relevant CIE principles.



[46] Albertella, Paul. "Using STPA with Software-Intensive Systems." October 19, 2021. https://www.codethink.co.uk/articles/2021/stpa-software-intensive-systems/.

[47] Oginni, Dapo, Fanny Camelia, Mikela Chatzimichailidou, and Timothy Ferris. "Applying System-Theoretic Process Analysis (STPA)-Based Methodology Supported by Systems Engineering Models to a UK Rail Project." *Safety Science* 167 (2023). https://www.sciencedirect.com/science/article/pii/S0925753523002175.

3.7. Hazard and Consequence Analysis for Digital Systems (HAZCADS)

Developed by Sandia National Laboratories (SNL) and EPRI,[48] Hazard and Consequence Analysis for Digital Systems (HAZCADS) integrates PRA with STPA-style analysis ensuring that both digital (software/firmware) and analog components are reviewed. Based on STPA principles, HAZCADS begins with identifying how UCAs in the digital system can lead to traditional safety hazards (e.g., reactor vessel overpressure). Next, organizations identify the potential consequences of the identified hazards using PRA-style methods (e.g., event/fault trees, frequency analysis). Finally, practitioners calculate the associated risk through an evaluation of frequency of occurrence for initiating cyber events and consequence severity.

While the detailed procedures for HAZCADS are proprietary, the method was developed with its roots in nuclear power plant safety design. For example, consider its application to a reactor's emergency shutdown system. A safety analyst could use HAZCADS to identify UCAs in the digital control system that might prevent the reactor from shutting down during an emergency. The analyst would then apply PRA techniques (such as fault trees or event trees) to quantify the potential consequences of such failures and evaluate their associated risk. Based on the findings, the analyst might recommend additional safeguards, such as redundant control channels, diverse shutdown logic, or enhanced testing protocols, to improve overall system reliability.

HAZCADS WITHIN THE CYBER CONTEXT

SNL has described HAZCADS as a fusion of PRA and STPA to "understand security risks at nuclear facilities,"[49] but it could be extended to other industries, sectors, or applications. By design, HAZCADS addresses cyber-induced risks to cyber-physical systems, evaluating scenarios where a cyber compromise could trigger a safety incident. In practice, this involves mapping possible cyber-initiated events (e.g., unauthorized access and modification of a SIS controller, corrupted firmware) into hazard scenarios and then using PRA tools such as event and fault trees to estimate the likelihood and consequences of severe outcomes. The STPA influence within HAZCADS ensures that nontraditional hazards, such as software logic flaws or unsafe control actions, are captured alongside conventional component failure modes.

Although HAZCADS explicitly acknowledges the role of cyber adversaries (placing it ahead of many traditional safety analysis methods), it also inherits limitations from its reliance on PRA techniques. In particular, PRA depends heavily on historical failure data and frequency estimates. This reliance can bias the analysis toward *known* failure modes, making it harder to fully account for **novel or adversary-driven disruptions** that lack precedent in the operational

[48] Program 41.13.01: Operating Plant Initiatives Program | EPRI. "HAZCADS: Hazards and Consequences Analysis for Digital Systems - Revision 1." July 6, 2021. https://www.epri.com/research/programs/111344/results/3002016698.

[49] Sandia National Laboratories. "Nuclear Energy Cybersecurity by Design." Government Website. Accessed September 2, 2025. https://energy.sandia.gov/programs/nuclear-energy/nuclear-energy-security/nuclear-energy-cybersecurity-by-design/.

record. As a result, certain attack scenarios may be overlooked or assigned artificially low priority simply because they are not reflected in past failure statistics.

A summary of HAZCADS alignment to and deviation from CIE is included in Table 8 and aggregated comparisons across all HA approaches evaluated are included in Appendix A. The following table highlights specific features of the reviewed HA method but is not all-inclusive of variations between HAZCADS and CIE.

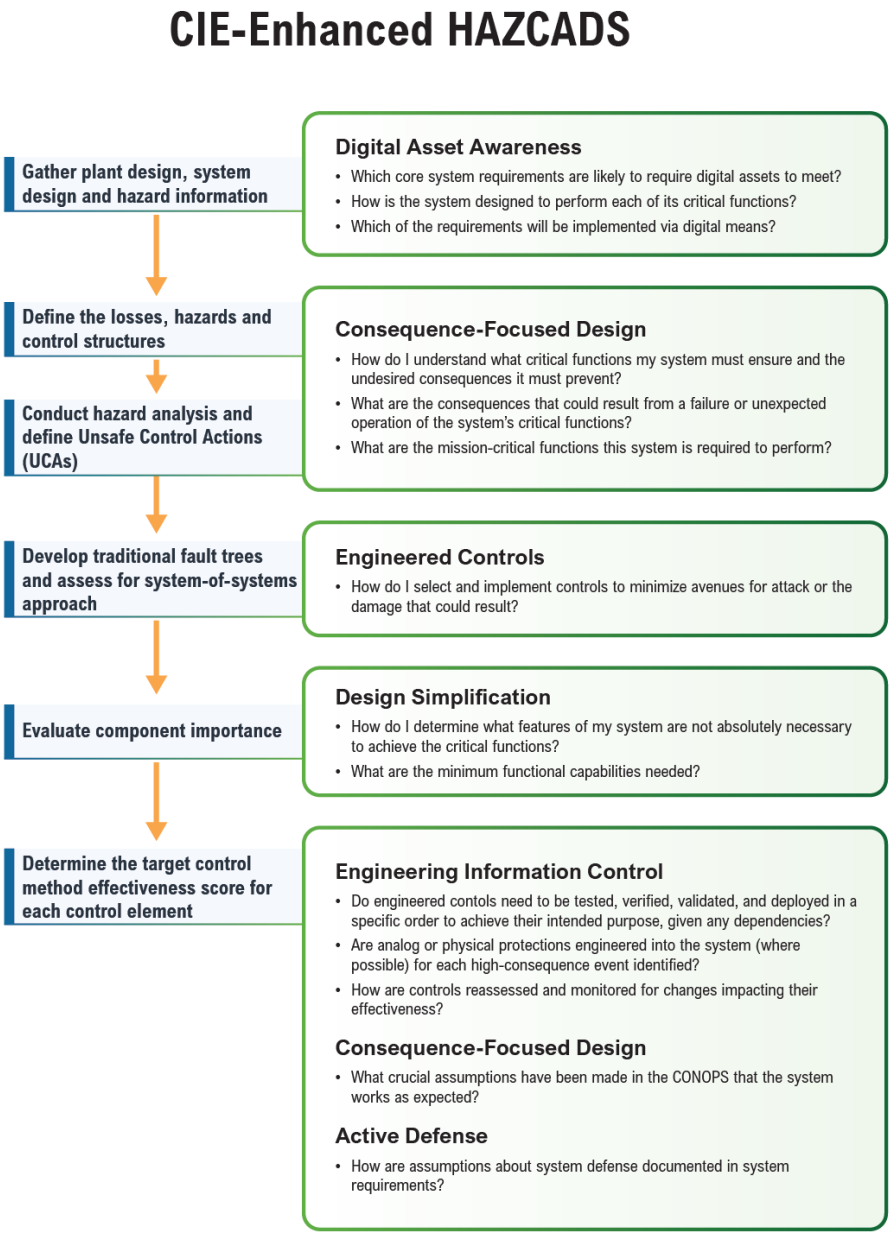
Table 8. A review of HAZCADS as compared to CIE.

Gaps and Limitations	Alignment with CIE	Divergence from CIE	CIE Adoption Recommendations
The proprietary nature of the approach likely challenges widespread adoption. Grounding historical data can yield biases and blinds spots when considering emerging techniques or novel attacks. The focus is on identifying and addressing UCAs through safety controls and does not encourage post event response activities (e.g., incident response and recovery).	Unlike the other HA methods review, HAZCADS emphasizes the risk posed by malicious cyber actors. Can present some alignment with CIE regarding potential to add cyber vulnerabilities and specify engineering mitigations.	Like PRA, HAZCADS relies heavily on historical failure data and frequency estimates when identifying risk. This conflicts with prioritization of severity of consequence emphasized within CIE. Supply chain risks are not accounted for within the HAZCADS approach.	As with STPA, ensure that adversary actions (e.g., loss of control through malicious firmware uploads) are recorded in addition to UCAs. Ensure that any safety controls are properly evaluated for their resilience to cyber-based manipulation or distortion. Closely review any inherent assumptions made with regards to the resiliency of the system or safety design.

CIE-ENHANCED HAZCADS

In Figure 9, the research team modified HAZCADS to include CIE concepts. Typically, HAZCADS begins with gathering plant and system design information before continuing with follow-on steps: defining hazards, analyzing unsafe control actions, building fault trees, evaluating component importance, and assessing control effectiveness. At each step, CIE concepts such as *Digital Asset Awareness*, *Consequence-focused Design*, *Engineered Controls*, *Design Simplification*, *Engineering Information Control*, and *Active Defense* are integrated. (Although there are 12 CIE Principles (Figure 2), this subset is most relevant to HAZCADS.) The result is a structured approach that incorporates cyber resilience and mission assurance into complex system HA.

Figure 9. A CIE-enhanced HAZCADS[50] process flow diagram.



[50] Clark, Andrew J, Mike Rowland, Chris Lamb, Katya Le Blanc, and Robert Youngblood. "Cyber Process Hazard Analysis and Risk Management." August 20, 2025. https://www.osti.gov/servlets/purl/1876592.

3.8. Layers of Protection Analysis (LOPA)

Layers of Protection Analysis (LOPA) is a semi-quantitative risk assessment method that sits between a qualitative review (like HAZOP) and a full quantitative PRA.[51] It focuses on a single initiating event and evaluates whether existing independent protective layers (IPLs) suffice to reduce risk to tolerable levels. Steps of LOPA include:

- **Identify a hazard scenario** (typically flagged by HAZOP or PRA).
- **Define risk targets** by assigning a frequency to the initiating event and a severity to its potential consequence (often based on risk matrices).
- **Estimate initiating event frequency** using historical data or engineering judgment.
- **List existing IPLs** (e.g., alarms, shutdown systems, relief valves, containment, emergency response).
    - Each IPL must be independent of the others.
    - Assign each IPL a probability of failure on demand (PFD), usually from standard tables or databases.
- **Calculate residual risk and compare to tolerable risk threshold.**

$$Risk\ frequency = initial\ frequency\ x\ product\ of\ IPL\ PFDs$$

- **Decide on additional safeguards.** If residual risk is above tolerance, add new IPLs or reduce initiating event likelihood.

LOPA uses order-of-magnitude estimates and simple calculations rather than detailed fault trees. It is commonly used in chemical process safety and SIS design to determine needed SILs for instrumented systems. A process safety engineer evaluating a chemical storage tank might use LOPA to address the risk of overfilling. Existing IPLs could include high-level alarms and automatic shutoff valves. If these do not sufficiently reduce the risk, the engineer might recommend additional safeguards, such as improved operator training or enhanced spill response plans.

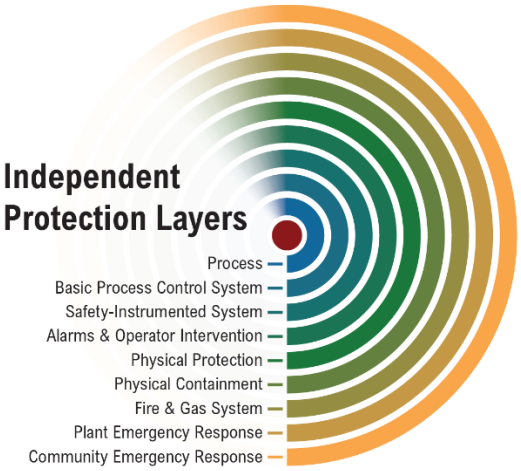
LOPA WITHIN THE CYBER CONTEXT

The philosophy behind LOPA itself (i.e., ensuring multiple independent layers exist) strongly resonates with ICS defense-in-depth practices (e.g., ISA/IEC 62443 and NERC CIP) that call for layered controls. (These controls are often displayed as “bullseye” diagram (shown in Figure 10), with protection layers depicted as concentric barriers around a hazard.) Although LOPA is most commonly used to address safety-associated risks (e.g., IEC 61511 uses it to justify SILs), theoretically, a similar approach could be implemented when addressing cyber-introduced

[51] Eltahan, Fatma M., Monica Toderas, Moustapha S. Mansour, El Sayed Z. El-Ashtoukhy, Mohamed A. Abdou, and F. Shokry. “Applying a Semi-Quantitative Risk Assessment on Petroleum Production Unit.” *Scientific Reports* 14, no. 1 (2024): 7603. https://doi.org/10.1038/s41598-024-57600-2.

hazards, in which various processes, procedures, and technologies come together to strengthen the overall defense of a system.[52]

Figure 10. Typical IPLs against potential incidents.[53]



For example, some researchers have proposed a "cybersecurity LOPA" or CLOPA, which extends the existing LOPA methodology by incorporating security failures into the risk assessment process.[54] The CLOPA approach provides a mathematical technique that quantitatively expresses the trade-offs between reliability and security in cyber-physical system design. CLOPA includes both a safety and security risk assessment (addressing risks from both physical and cyber failures), a mathematical formulation of CLOPA (a model that incorporates security failures into the traditional LOPA framework), and a co-design lifecycle process that integrates safety and security assessments throughout the design and operational phases.[55]

A summary of LOPA alignment to and deviation from CIE is included in Table 9 and aggregated comparisons across all HA approaches evaluated are included in Appendix A. The following table highlights specific features of the reviewed HA method but is not all-inclusive of variations between LOPA and CIE.

---

[52] Baybutt, Paul. "Cyber Security Risk Analysis for Process Control Systems Using Rings of Protection Analysis (ROPA)." *Process Safety Progress* 23, no. 4 (2004): 284–91. https://doi.org/10.1002/prs.10053.
[53] Eltahan, Fatma M., Monica Toderas, Moustapha S. Mansour, El Sayed Z. El-Ashtoukhy, Mohamed A. Abdou, and F. Shokry. "Applying a Semi-Quantitative Risk Assessment on Petroleum Production Unit." *Scientific Reports* 14, no. 1 (2024): 7603. https://doi.org/10.1038/s41598-024-57600-2.
[54] "Cyber LOPA: An Integrated Approach for the Design of Dependable and Secure Cyber-Physical Systems | IEEE Journals & Magazine | IEEE Xplore." Accessed August 26, 2025. https://ieeexplore.ieee.org/document/9761964.
[55] "Cyber LOPA: An Integrated Approach for the Design of Dependable and Secure Cyber-Physical Systems | IEEE Journals & Magazine | IEEE Xplore." Accessed August 26, 2025. https://ieeexplore.ieee.org/document/9761964.

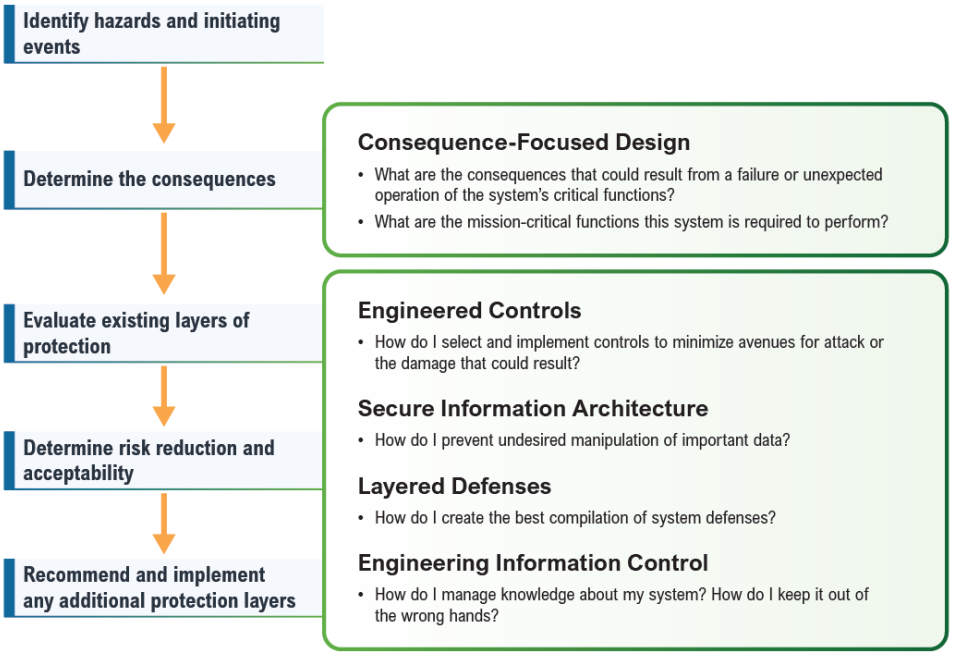
Table 9. A review of LOPA as compared to CIE.

Gaps and Limitations	Alignment with CIE	Divergence from CIE	CIE Adoption Recommendations
LOPA can be less effective than other HA methods when investigating complex system failures and interactions. Requires reliable data on cyber event probabilities, but the analysis is less rigorous than traditional PRA methods. Overlooks failures induced through a deliberate cyberattack.	LOPA naturally aligns to CIE tendencies to promote varied safety controls. Since LOPA is a layered protection method, cybersecurity controls can be treated as a protection layer.	LOPA does not specifically address cyberattacks in its approach, although it is possible that the layered approach for IPLs may provide some natural resilience to cyber-based disruptions (due to diversity of protection methods). Supply chain risks are not accounted for within the LOPA approach.	Leverage CIE principles to identify any overlooked weaknesses or dependencies in the system performance and resiliency. Be wary of assumptions in the efficacy of safety controls and reference CIE principles to identify how cyber threats could degrade safety barriers. Leverage CIE to ensure a thorough dependency analysis is used to define potential consequences from adverse events. Consider potential supply chain risks that could introduce new methods to degrade IPLs. Identify engineering controls through the CIE framework to help mitigate any potential cyber-induced risk.

CIE-ENHANCED LOPA

Figure 11 demonstrates how practitioners can enhance LOPA with CIE, from identifying hazards and initiating events to determining consequences, evaluating protection layers, and assessing risk reduction. Various CIE principles, including *Consequence-Focused Design*, *Engineered Controls*, *Secure Information Architecture*, *Layered Defenses*, and *Engineering Information Control* are integrated throughout the HA process to ensure both safety and cyber resilience. (Although there are 12 CIE Principles (Figure 2), this subset is most relevant to LOPA.) The outcome is a more comprehensive LOPA that accounts for mission-critical functions and protects against both operational and cyber-induced failures.

Figure 11. A typical LOPA process flow[56] amended with CIE concepts.



[56] Caburao, Eunice Arcilla. "Layer of Protection Analysis: A Short Guide." SafetyCulture, October 8, 2024. https://safetyculture.com/topics/risk-assessment/layer-of-protection-analysis/.

4. Conclusion

The INL research team reviewed multiple HA approaches (i.e., HAZOP, PRA, FMEA, STPA, HAZCADS, and LOPA) to evaluate how well they account for cyber-based hazards.[57] The analysis revealed critical gaps that can be mitigated through the integration of CIE. Most HA methods fail to adequately address risks introduced by deliberate cyber manipulation (e.g., HAZOP, PRA, FMEA, LOPA) or to capture the complex, cascading effects that can follow a cyberattack in cyber-physical systems (e.g., HAZOP, FMEA, LOPA). More significantly, all the methods reviewed assume the effectiveness and immutability of safety controls, assumptions increasingly challenged by cyberattacks on supply chains.

Additionally, the findings from Sections 2 and 3 indicate that while some CIE principles naturally align with current HA practices, others are notably absent, particularly in the ongoing operations and maintenance phase. This research identified that existing HA guidance often emphasizes early-stage reviews to minimize costs, leading to less focus on later lifecycle phases. By applying CIE thinking across the entire system lifecycle, from design through decommissioning, organizations can strengthen their ability to anticipate, withstand, and recover from cyber disruptions.

An expansion of this research could involve developing detailed guidebooks tailored to specific sectors and industries. For instance, the CIE team could create a helper guide for a CIE-enhanced HAZOP process specifically for the chemical sector. These HA methods and sector-specific guidebooks would provide step-by-step instructions, practical examples, and best practices to assist organizations with integrating CIE methods into their existing hazard mitigation processes.

Acknowledgements

The authors of this report would like to thank the additional INL SMEs who provided valuable insights, Shannon Eggers, Katya LeBlanc, and Patience Yockey.

[57] It should be noted that this INL review was not all inclusive of existing HA approaches; there are several other HA methods, and their omission from this report should not be considered an indicator of their applicability, efficacy, or effectiveness.

Appendix A: Summary of Alignment between Cyber-Informed Engineering and Hazards Analysis

Table 10 summarizes the research teams' findings investigating various HA methods (i.e., HAZOP, PRA, FMEA, STPA, HAZCADS, LOPA). It evaluates several Hazards Analysis (HA) methods through the lens of Cyber-Informed Engineering (CIE). It highlights where each HA method naturally aligns with CIE, supporting cyber risk considerations, and where gaps or limitations exist, indicating a lack of coverage for cyber-induced threats. Additionally, the table offers CIE adoption recommendations for practitioners, suggesting ways to integrate CIE principles into each framework effectively. Finally, the table outlines gaps and limitations of each methodology, providing a clear understanding of where improvements are needed to enhance their effectiveness in managing cyber risks and consequences.

Table 10: HA methods and their alignment to CIE.

Method	Gaps and Limitations	Alignment with CIE	Divergence from CIE	CIE Adoption Recommendations
HAZOP	May not account for an intelligent, malicious adversary that manipulates or disrupts safeguards and information flows. May miss cyber-initiated deviations unless the team has cyber expertise.	HAZOP and CIE are both consequence-focused and seek to mitigate the most devastating consequences first. HAZOP is structured around deviations in process flows and/or procedural steps, which is naturally extendible to information flows and digital commands.	HAZOP focuses on independent discrete failure events associated with hazards. In contrast, CIE is very concerned with cascading failures (like those instigated via a cyberattack). Supply chain risks are not accounted for within the HAZOP approach.	HAZOP can be augmented to include the process' information flows in addition to the traditional process flows and procedures. For each information flow, design intent can be defined in terms of the expected information, and deviations can be defined in terms of how that information might be corrupted. This will result in the development of additional scenarios associated with each informational deviation. Alter HAZOP probabilistic prioritization of deviations with consequence – aligning it to CIE. Review the twelve CIE principles and associated questions within the *Implementation Guide*, to improve the completeness of HAZOP review. Studiously evaluate the resilience of safety barriers: how could they be degraded or manipulated. Leverage the CIE framework to identify engineering controls to augment any safety controls.

PRA	PRA's reliance on expert interpretation to inform probabilities (particularly regarding low-frequency events) may result in some adverse events as being discarded as improbable. PRA treats safeguards as "static" and immutable, which is unrealistic given an intelligent adversary. Additionally, safeguards address initiating events and potential adverse impacts but may ignore defensive or resilience gains from post-event mitigations (e.g., intrusion detection, incident response).	PRA framework already emphasizes the need to define the significant consequence (in alignment to CIE). Provides a structured approach to risk assessment and emphasizes an understanding of the system's data flows.	As a safety-centric method, PRA does not account for deliberate, adaptive adversary behavior (e.g., a threat actor bypassing controls, targeting interdependencies, or disrupting key information exchanges). For example, layered safety controls or safeguards are considered sufficient despite deliberate and targeted manipulation of controls by an adversary. Supply chain risks are not accounted for within the PRA approach.	PRA origins focus on the importance of understanding data and information flows within a system, similar to STPA's emphasis on UCAs. Practitioners should be aware that probabilities may be misleading or unknowable, particularly when considering cyberattacks. When considering safeguards, emphasize the importance of diverse and varied safeguards (which could challenge adversary actions). Specifically, the most comprehensive defensive posture stems from a combination of physical and cyber safeguards.
FMEA	FMEA scenarios are often prioritized based in part on stochastic probability, whereas cyberattacks are not amenable to stochastic analysis. May overlook complex attack chains and intent-driven scenarios without integration with security methods.	FMEA and CIE are both consequence-focused and concerned with avoiding the same set of undesired consequences. FMEA can be conducted throughout the systems engineering lifecycle. Systematic, component-level failure analysis can incorporate cyber-based failure modes.	FMEA is not well suited to the identification of scenarios involving multiple independent failures, whereas CIE is concerned with orchestrated cyberattacks. FMEA-based scenarios are often prioritized based in part on stochastic probability, whereas cyberattacks are not amenable to stochastic analysis. FMEA is concerned with stochastic failures, not intentional adversarial events. Supply chain risks are not accounted for within the FMEA approach.	FMEA should determine when safeguards are reachable via an information stream that is accessible by an adversary. In these instances, the efficacy of the safeguard should be considered. Validate that failure mode lists cover possible cyber events. Create separate/additional scoring for severity, occurrence, detectability within cyber in mind.

STPA	STPA can be difficult to implement, particularly when evaluating large, complex systems. Because of this, STPA is more sensitive to varying experience levels of users, and the effectiveness of application is highly dependent on user training. STPA is based on intuitive causal analysis rather than past failure data and probabilities. STPA does not provide explicit guidance on how to consider a malicious adversary, leaving it up to the practitioner.	STPA's focus on the importance of system-of-systems analysis aligns it naturally to CIE, which emphasizes the risk that can be introduced through complex system design and system interdependencies. Like CIE, STPA acknowledges the risk that can be introduced through digital component failures.	STPA takes into consideration human error, but it does not fully account for an intelligent malicious actor that disrupts the system through complex attacks. Additionally, although UCAs are helpful in illuminating potential safety issues, this emphasis is less effective in understanding how system performance can be degraded. Supply chain risks are not accounted for within the STPA approach.	Review questions within the *CIE Implementation Guide* to enhance the identification of UCAs specifically related to cyber threats. Ensure potential adversary actions are encompassed within UCAs (e.g., loss of view resulting from malicious modification of sensor data) so that safety constraints are effective. Assign individuals to specifically investigate the security and sanctity of safety controls: to what degree can these be manipulated or altered?
HAZCADS	The proprietary nature of the approach likely challenges widespread adoption. Grounding historical data can yield biases and blinds spots when considering emerging techniques or novel attacks. The focus is on identifying and addressing UCAs through safety controls and does not encourage post event response activities (e.g., incident response and recovery).	Unlike the other HA methods review, HAZCADS emphasizes the risk posed by malicious cyber actors. Can present some alignment with CIE regarding potential to add cyber vulnerabilities and specify engineering mitigations.	Like PRA, HAZCADS relies heavily on historical failure data and frequency estimates when identifying risk. This conflicts with prioritization of severity of consequence emphasized within CIE. Supply chain risks are not accounted for within the HAZCADS approach.	As with STPA, ensure that adversary actions (e.g., loss of control through malicious firmware uploads) are recorded in addition to UCAs. Ensure that any safety controls are properly evaluated for their resilience to cyber-based manipulation or distortion. Closely review any inherent assumptions made with regards to the resiliency of the system or safety design.

LOPA	LOPA can be less effective than other HA methods when investigating complex system failures and interactions. Requires reliable data on cyber event probabilities, but the analysis is less rigorous than traditional PRA methods. Overlooks failures induced through a deliberate cyberattack.	LOPA naturally aligns to CIE tendencies to promote varied safety controls. Since LOPA is a layered protection method, cybersecurity controls can be treated as a protection layer.	LOPA does not specifically address cyberattacks in its approach, although it is possible that the layered approach for IPLs may provide some natural resilience to cyber-based disruptions (due to diversity of protection methods). Supply chain risks are not accounted for within the LOPA approach.	Leverage CIE principles to identify any overlooked weaknesses or dependencies in the system performance and resiliency. Be wary of assumptions in the efficacy of safety controls and reference CIE principles to identify how cyber threats could degrade safety barriers. Leverage CIE to ensure a thorough dependency analysis is used to define potential consequences from adverse events. Consider potential supply chain risks that could introduce new methods to degrade IPLs. Identify engineering controls through the CIE framework to help mitigate any potential cyber-induced risk.

Appendix B: Additional Frameworks, Standards, and Tools

Through the course of INL's research and coordination with subject matter experts (SMEs), several additional frameworks, standards, and tools were identified that, while not included in the primary alignment analysis, offer meaningful contributions to a cyber-aware HA approach. These resources were discussed throughout the research process and are worthy of mention due to their potential to inform, support, or enhance the integration of cybersecurity considerations into traditional HA practices. They provide valuable context and may serve as practical references for organizations seeking to strengthen their HA processes.

IEC 61508 Guidance

IEC 61508 is an international standard for the functional safety of electrical, electronic, and programmable electronic (E/E/PE) systems.[58] It provides a framework for managing risks by defining safety requirements throughout the lifecycle of a product or system. IEC 61508 applies to all industries and focuses on ensuring that safety-related systems function correctly or fail in a predictable (safe) way.

The standard defines a safety lifecycle with 16 phases, divided into three groups:

- Analysis (Phases 1-5): Identifying hazards and assessing risks.
- Realization (Phases 6-13): Designing and implementing safety measures.
- Operation (Phases 14-16): Operating, maintaining, and decommissioning the system.

The standard categorizes safety requirements into four Safety Integrity Levels (SILs), with SIL 4 being the highest. It emphasizes risk assessment to determine the necessary SIL based on the frequency and severity of hazardous events. IEC 61508 is divided into seven parts, covering general requirements, E/E/PE systems, software requirements, definitions, safety integrity levels, guidelines, and examples. It uses a probabilistic approach to account for the safety impact of device failures and is adaptable across various industries, helping demonstrate compliance with regulatory requirements. This comprehensive approach ensures safety is integrated into every phase of a system's lifecycle, from design to decommissioning.

IEC 61511 Standard

IEC 61511 is the international standard that governs the design, implementation, and management of SIS in the process industries, such as chemical, petrochemical, and refining.[59] It is derived from the broader IEC 61508 functional safety framework but is tailored to process operations. At its core, the standard ensures that organizations systematically identify and control hazards using a structured, lifecycle-based approach.

---

[58] "IEC 61508 Standard: A Comprehensive Guide : Electrical Hub." Accessed September 2, 2025. https://azadtechhub.com/iec-61508-standard/.

[59] "IEC 61508-2:2010 | IEC Webstore." Accessed September 2, 2025. https://webstore.iec.ch/en/publication/5516.

Hazards are first identified through Hazard and Risk Assessment (H&RA) techniques such as HAZOP, LOPA, or FMEA. As mentioned above, these analyses highlight scenarios where existing controls and safeguards may not sufficiently reduce risk. For those scenarios, Safety Instrumented Functions (SIFs) are defined (i.e., specific automated protective actions such as high-pressure shutdowns or emergency isolation). Each SIF is then assigned a SIL, ranging from SIL 1 (lowest) to SIL 4 (highest), depending on the required level of risk reduction. The SIL rating sets reliability, performance, and design requirements for the system.

Importantly, IEC 61511 emphasizes a full safety lifecycle. This means hazards are not only considered during design but are continually managed through operation, maintenance, testing, and eventual decommissioning of safety systems. CIE expands this process by emphasizing the reality of the evolving threat actor – although initial designs may account for cyber threats, over time the effectiveness of these controls may erode as new adversary capabilities are developed. Still, by emphasizing the importance of H&RA as an ongoing process, the standard ensures that protective systems remain effective in mitigating risks, even as processes evolve and equipment ages. In doing so, IEC 61511 provides a structured framework for converting hazards analysis results into actionable, reliable protections that keep process facilities safe.

NRC 10 CFR 50.69 Risk Management

NRC 10 CFR 50.69 Risk Management provides a comprehensive framework that incorporates both qualitative and quantitative assessments to understand critical components and functions.[60] This approach is particularly valuable for enabling alternative treatments in lieu of original design considerations. CFR 50.69 allows nuclear facilities to undergo a process of categorizing components within a system into four categories:

- Safety-Related, Safety Significant
- Safety-Related, Low Safety Significant
- Non-safety -Related, Safety Significant
- Non-safety-Related, Low Safety Significant

Within the 10 CFR 50.69 categorization process there are several aspects that include quantitative analysis and several that utilize a more qualitative analysis. Implementation details of 50.69 include a section for categorizing passive components, such as pipes and heat exchangers.[61] This categorization is important for considering the impact of these components on functions that are determined to be critical.

One may consider utilizing the 10 CFR 50.69 framework in addition to CIE to aid in determining what components are relevant to the operation of the system. For the qualitative assessment, CIE's principles include a series of questions designed to evaluate functions. By applying 50.69, these questions can help determine the significance of each function to CIE. Answering these

[60] EPRI. “10 CFR 50.69 Categorization Guidance Document.” https://www.epri.com/research/products/000000003002012984

[61] NRC. “Industry Presentations for 50.69 NRC Knowledge Management-Knowledge Transfer Workshop.” February 2025. https://www.nrc.gov/docs/ML2503/ML25037A126.pdf.

questions can lead to a coarse set of ratings for components performing specific functions. Additionally, where applicable, importance measures can be considered for components within these functions.

Critical Item Lists (CILs)

NASA's Critical Item Lists (CILs) approach can help ensure that hardware and software design, testing, and inspection planning activities are well-informed.[62] During the operational phase of the lifecycle, CILs are utilized to manage failures and ensure mission success. The Failure Mode and Effects Analysis (FMEA) process is integral to this, as it identifies failure modes, including those that could lead to loss of life or failures. These critical failure modes are then documented in a CIL, which undergoes thorough examination for programmatic control. This involves implementing inspection requirements, test requirements, and special design features or changes to minimize the occurrence of these failure modes. Consequently, FMEAs and the resulting CILs not only serve as a reliability check for system designs but also act as primary design drivers for the product or service.

Logic Modeling

Logic modeling, including Fault Tree Analysis (FTA) and Event Tree Analysis (ETA), is used to analyze risk and safety issues by modeling the logical relationships between system components and their potential failures. FTA is a top-down approach that identifies the probability of an unwanted event by analyzing the contributing factors, while ETA is a forward, top-down approach that explores responses to an initiating event and assesses the probabilities of different outcomes.

- **FTA (Fault Tree):** This is a top-down deductive method. You start with a defined top event (an undesired failure or accident) and use logic gates to break it into combinations of lower-level faults. Each basic fault (e.g. "pump fails," "valve stuck") is a leaf node. By calculating the probability of each basic fault, one can compute the probability of the top event. FTA helps identify minimal cut sets (combinations of failures that lead to the top event) and prioritizes components by risk contribution. For example, a fault tree for a reactor trip failure might require "PLC failure OR loss of power supply" under an OR gate, etc. As one explanation notes: "FTA uses a deductive, failure-based approach. While the leaf node represents the triggering event, the root node represents an unwanted event… the events that may lead to the top event are modeled as branches of nodes.[63]

[62] NASA. "Identification, Control, and Management of Critical Items Lists." October 1995. https://extapps.ksc.nasa.gov/Reliability/Documents/Preferred_Practices/1240.pdf.
[63] Francia, Guillermo A., III, David Thornton, and Joshua Dawson. "Security Best Practices and Risk Assessment of SCADA and ICS." Conference Paper. Jacksonville State University. https://icscsi.org/library/Documents/White_Papers/Francia%20et%20al%20-%20Security%20Best%20Practices%20and%20Risk%20Assessment%20of%20SCADA%20and%20ICS.pdf.

- **ETA (Event Tree):** An Event Tree Analysis (ETA) is an inductive method used to illustrate all possible outcomes following an initiating accidental event. It considers the functionality of installed safety barriers and other contributing factors. By examining all relevant accidental events identified through preliminary hazards analysis, HAZOP, or other techniques, ETA helps identify potential accident scenarios and sequences within a complex system. This analysis can reveal design and procedural weaknesses and determine the probabilities of various outcomes from an accidental event.[64] An ETA typically begins with an initiating event (e.g. a reactor loss-of-coolant accident) and follows possible success/failure paths of safety functions. At each stage (barrier), you branch on success or failure. The resulting "tree" enumerates possible end states (e.g., safe shutdown, partial release, core damage) with associated probabilities. ETA is useful for visualizing how combinations of safety system success or failure can lead to different outcomes. Each path through the event tree represents a sequence of events, and probabilities can be assigned by multiplying the probabilities of success/failure at each branch.

[64] Rausand, Marvin. "Chapter 3: Event Tree Analysis." Norwegian University of Science and Technology (NTNU). https://www.ntnu.edu/documents/624876/1277590549/chapt03-eta.pdf/6f3e1b19-4824-4812-adc8-9762d2201c22.

Cyber-Informed
Engineering