INL/CON-24-80907-Revision-0

On the Application of Cyber-Informed Engineering (CIE)

November 2024

Benjamin Ruhlig Lampe

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

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, trade mark, 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/CON-24-80907-Revision-0

On the Application of Cyber-Informed Engineering (CIE)

Benjamin Ruhlig Lampe

November 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

On the Application of Cyber-Informed Engineering (CIE)

Benjamin Lampe
CIE Research Engineer
Idaho National Laboratory
Email: benjamin.lampe@inl.gov

***Abstract*—The 2023 National Cybersecurity Strategy has recommended a transition to secure-by-design methodologies in critical infrastructure. This paper presents the adoption of the National Cyber-Informed Engineering (CIE) Strategy as initiated by the U.S. DOE's CESER office, advocating for the integration of cybersecurity at the earliest stages of system design. The strategy targets design engineers responsible for energy infrastructure to embed CIE principles within the engineering lifecycle, thus enhancing cyber resilience.**

This paper discusses the expansion of secure-by-design concepts to cyber-physical systems, moving beyond traditional IT security to include engineering considerations that can mitigate cyber risks through design choices. The paper introduces Digital Risk Management, balancing traditional cybersecurity with CIE to reduce both likelihood and impact of cyber threats.

A set of CIE starter questions derived from 12 core principles is detailed, aiding engineers to consider cybersecurity in their designs and highlights the importance of CIE in anticipating and reducing the impacts of cyber attacks, suggesting that such integration is essential for national security and infrastructure resilience.

***Keywords*—Cyber-Informed Engineering, National Cybersecurity Strategy, Critical Infrastructure, Secure-by-Design, System Resilience, Digital Risk.**

I. Introduction

The National Cybersecurity Strategy of 2023 [1] called for a large scale shift to secure-by-design approaches for the digital ecosystem that underpins U.S. critical infrastructure systems. For energy infrastructure in particular, it explicitly recommends implementing the congressional-directed National CIE Strategy [2] to proactively build in cybersecurity. This implementation of CIE takes a crucial step in this direction by guiding engineers to incorporate CIE principles throughout the design and engineering process. The National CIE Strategy was developed by an executive task force, assembled by the U.S. Department of Energy (DOE)'s Office of Cybersecurity, Energy Security, and Emergency Response (CESER), that included energy sector asset owners and operators, vendors and manufacturers, standards organizations, research and academic institutions, National Laboratories, and government agencies.

Engineers and technicians who design critical energy infrastructure installations use the practice of CIE to integrate the 12 principles into each phase of the engineering lifecycle, from concept to retirement. Rather than software engineers or operational cybersecurity practitioners, the application of CIE is aimed at system or design engineers because the engineers who design, build, operate, and maintain the physical infrastructure are best positioned to leverage a system's engineering design to diminish the impact of cyber attacks or digital technology failures. At a minimum, CIE expands cybersecurity decisions into the engineering space, not by asking engineers to become cyber experts, but by calling on engineers to apply engineering tools and make engineering decisions that improve cybersecurity outcomes. CIE examines the engineering consequences that a cyber adversary could achieve, and drives engineering changes that may provide deterministic mitigations to limit or eliminate consequences and the impacts of those consequences.

Furthermore, CIE extends "secure-by-design" concepts [3] beyond information technology (IT) and software engineering to include the engineering of cyber-physical systems. Secure-by-design approaches typically describe a shift in focus for software developers from finding and patching vulnerabilities to eliminating the design flaws in the software architecture that enable those vulnerabilities. CIE extends this concept beyond software design, introducing cybersecurity considerations that engineers can address at the earliest stages of system engineering, before the incorporation of software and other digital security controls. Traditionally, engineering design teams have not recognized the opportunity to create cybersecurity improvements in systems through initial design and engineering decisions. These opportunities, if missed, are often costly or even impossible to implement later in the development process, potentially leaving in place cyber risks that security teams must endlessly manage and monitor.

Enabling engineering considerations at the beginning of the system lifecycle not only avoids this outcome, but creates new opportunities to secure the system using physics and mechanics, not just digital monitoring and controls.

II. Digital Risk Management

At its heart, the practice of cybersecurity is the risk management of digital functions, whether those functions are checking your email or controlling when a pump turns on or off. The latter being the focus for cyber-physical systems. As risk, it has traditionally been calculated as the combination of likelihood of occurrence times consequence (Risk = likelihood*consequence). As either the probability of occurrence or the magnitude of consequence goes up, the amount of risk equally goes up. Cybersecurity and its use of controls and countermeasures has expanded the probability-centric measures within the risk calculation into many alternate cybersecurity variables, such as the measure of vulnerability, exposure, or threat. The likelihood that a digital function is compromised is based on the probabilistic quantification of these cybersecurity variables where cybersecurity practices are considered.

Traditional cybersecurity frameworks and practices, such as NIST 800-53 [4], C2M2 [5], IEC 62443 [6] have implemented many practices that focus on the reduction or elimination of the probability-centric variables within these risk calculations. For instance, by implementing access control mitigations like passwords, changing default passwords, adding role-based access control (RBAC), and many others, the system attempts to make it harder for the adversary (lower the likelihood) to compromise the digital function. But in the event those mitigations are bypassed, the adversary is able to realize the full extent of the specific digital function's ability to create a consequence. It is here that traditional cybersecurity uses defense in depth practices and the combination of many independent probabilistic-centric reductions to further challenge the adversary and their probability of realizing a consequence. This overall cybersecurity practice is a necessary element in the overall defensive strategy for a cyber-physical system.

The use of CIE principles and its mitigation seek to amplify the consequence-centric aspects of the risk equation. With CIE, the focus is to control impact independently of likelihood. That way, CIE has the potential to reduce consequence, which is not otherwise controlled by digital mitigations. The next section will describe how CIE uses this basis to effectively walk through an engineering process to promote consequence reduction practices.

When taken together, the implementation of traditional cybersecurity and the practice of CIE, the system is designed to reduce or eliminate both elements of the risk calculation and provide the system owner with a strategy that further promotes the practice of defense in depth so that in event either does not work as envisioned the risk involved in the digital function remains bounded. Ideally the success of both practices produces a new frontier in the understanding and acceptance of risk in cyber-physical systems especially those that manage a nation's critical infrastructure.

III. CIE in System Design

Modern systems are increasing being digitized. More and more of infrastructure functions are the result of measurements read through an analog-to-digital (A/D) circuit providing an abstraction of the physical process, logic and decisions operating on that process state, and any commands being sent through a digital-to-analog circuit (D/A) to actuate the physical process. Engineers often use safety and protection engineering to provide countermeasures outside this digitization paradigm to reduce the impact of digital operations going astray. However, even these safety and protection engineering practices, such as protection relays in power grid operations, are increasingly implemented with digital functionality. Given this, the practice of CIE in system design is paramount to engineer the system to account for this increased digital risk. Where safety and protection engineering focus on operations that malfunction due to changes in the environment or non-malicious failure modes, CIE practice puts focus on operations that malfunction due to malicious failure modes. This lens of consequence is another focus area for engineers designing a system to manage. When applying CIE in system design, using the twelve principles to provide a basis for targeted questions to ensure that failure mode analysis and subsequent design patterns are realized is an effective strategy across any system design. The next section provides a set of CIE starter questions that allows any system engineer to ensure that the design is interpreted through the lens of CIE. Though these questions are similar to those posed in the CIE Implementation Guide [7], these are unique, designed to be relevant at any phase of the system lifecycle.

IV. Minimum Set of Questions To Consider

Principle 1 - Consequence-Focused Design

- What are the systems that perform and support critical facility functions?

- What are the unacceptable high consequence events that impact mission delivery, safety, security, the environment, equipment and property, financials, or corporate reputation?
- What are the critical processes, operations, and/or administrative actions required to protect against unacceptable high consequence events?
- How are identified high consequence events documented, monitored for change, and reassessed?
- Which stakeholders (e.g. operations staff, engineering staff, executive leadership, external parties) would be impacted during or by damage from high consequence events and how are they included in mitigation decisions?

Principle 2 - Engineered Controls

- How are the storage, movement, and use of hazardous quantities of mass or energy (potential and kinetic) controlled by digital technologies?
- How are engineered systems (e.g., IT, operational technology [OT], electrical, mechanical pneumatic, mechanical hydraulic, thermal, chemical) that store, move and use hazardous quantities of product or energy dependent on digital technologies to support critical functions?
- What consequences of failure or maloperation are the engineered controls designed to prevent?
- Where engineered controls depend on digital technologies, where might an analog engineered control add to the protection (or lower the impact) of a high consequence event?
- How do we monitor and ensure the effectiveness of engineering controls through system changes (e.g. expansion) and operational conditions, including those that may weaken their effectiveness (e.g. through undue stress)?
- How do we validate the efficacy of engineered controls, especially those that may be affected or circumvented by administrative workarounds?

Principle 3 - Secure Information Architecture

- What are the key data elements, the critical inputs and outputs, and the mechanisms (people, tools, systems) each process step that the system executes?
- How independent are the key data elements, physically or digitally, to allow diagnosis of the extent or cause of an anomaly?
- Which information exchanges with the system would result in a high consequence event if the data was disrupted or manipulated?
- What engineering and operations-based protection and verification could ensure that key data elements have not been manipulated?
- How could unanticipated adverse or extraordinary operating modes potentially violate security controls or validation mechanisms placed on the data?

Principle 4 - Design Simplification

- Where are opportunities to simplify or eliminate device/system elements or features that are not necessary to meet the minimum functional capabilities and defined system requirements?
- How would a given design simplification introduce tradeoffs (e.g., loss of redundant control, reduced reliability, reduced operator visibility) that conflict with other stakeholder requirements or downstream dependencies?
- How do each of the design elements traceable to a specific project requirement or critical operation/process?
- What non-digital alternative to a digital feature could be applied to satisfy a requirement?
- Which system features used for supporting the operation and maintenance of the system by personnel not necessary (e.g., engineering workstations, remote access for third-party entities, human-machine interfaces [HMIs], operator laptop connections)?

Principle 5 - Layered Defenses

- What layers of digital control defenses (e.g., network segmentation, access control, encryption, etc.) are present in the system?
- What layers of engineered control defenses are present in the system?
- How are multiple defenses independent of each other such that the failure or compromise of one has no effect on others?
- How are critical functions sufficiently protected by layered defenses?
- Where are there single points of failure that could result in undesired exposure of the critical function?
- How can the team assess and adjust layered defenses to maintain the desired level of protection after system upgrades, configuration changes, requirements changes, or changes in critical consequences?

Principle 6 - Active Defense

- What are the indicators, including the earliest precursors, that a high consequence event could be caused, intentionally or unintentionally?
- What temporary operational changes can be made in response to a perceived threat?
- What countermeasures, compensating controls, or alternative operations strategies support active defense while maintaining critical functions?

- How are active defense features/tools/procedures tested, validated, and regularly exercised during systems operations and are those results representative of how they would be expected to perform?
- How are current or new features tested following maintenance, changes, and upgrades?
- Who has the documented responsibility and accountability to initiate and terminate active defense measures, and how are they and others notified of an active threat or aware of triggers to temporarily change operations?

Principle 7 - Interdependency Evaluation

- What supporting utilities (e.g., telecommunications, water, power) provide inputs to the system that are essential for system-level critical function delivery?
- What inputs do the system's critical functions require that are not directly and completely controlled by the system?
- If access to a critical input is lost, can the input be obtained from alternative sources, and/or how will the system continue to execute its critical functions without it?
- What outputs does the system provide that are critical inputs to other business systems or infrastructures?
- If system outputs to dependent system's critical inputs are lost, can the output be produced from alternate sources?
- How are changes in interdependent systems communicated and used to inform the need for additional controls, capabilities, or investments?

Principle 8 - Digital Asset Awareness

- Which digital features in a system have the potential to cause high consequences events from adversarial manipulation or control?
- How are digital feature abuse/misuse scenarios used to identify high consequences events, inform requirements for what the system must be designed to not do, and drive digital and non-digital (i.e., engineered controls) mechanisms to prevent abuse/misuse?
- How do abuse/misuse scenarios inform operators' thinking about systems and affect system requirements?
- What processes ensure that digital assets are tracked and that third-party vendors provide the specifications needed to enable asset tracking?
- What processes ensure that operations and maintenance activities (e.g., changes to software, logic, or configurations) appropriately trigger updates to asset tracking records?
- What is the process to ensure that applied packages from updates/patches are necessary, desired, and make all the changes promised (and only the changes promised; no new unexpected features introduced)?
- Where updates or patching are delayed or not performed, are there alternate defenses that could be implemented to limit impacts of the resulting vulnerability or related exploitations?

Principle 9 - Cyber-Secure Supply Chain Controls

- What assumptions have been made about the availability, quality, and security of the products or services that are critical to system functions or to the mitigation of high consequence events?
- How can the organization reduce supply chain risk by prioritizing familiar technologies, technologies that are expected to be continuously available, and suppliers with a strong history of meeting supply chain constraints?
- How are delivery interruptions of critical components avoided by using alternate methods of delivery or by arranging for multiple alternate sources?
- How does the organization ensure the services and components that are critical to system function are being used in alignment with the vendor's intended purpose to minimize consequences of disruption, the expected security functions and requirements, and the vendor's responsibility and accountability in mitigating and preventing disruptions?
- How will the organization identify and manage the risks of continued use of a component or subcomponent if a vendor support contract expires?

Principle 10 - Planned Resilience

- What are the limits of acceptable degradation for critical system functions and what alternate operating modes would protect and maintain those critical system functions within acceptable limits?
- How reliable are the supporting utilities (e.g., power, communication) and what plans are in place for continued operation if one or more is lost?
- How does the system maintain safety, security, and/or stable operation in the case of partial or complete functional failures (i.e., fail-secure, similar to fail-safe)?
- Do processes controlled by an automated system have a manual operation mode that is practiced and has been verified to have no dependencies on automation?
- How does the organization maintain business continuity and critical function delivery through inci-

dent response and recovery?
- How will resilience measures be validated?
- How do you practice and continually improve response and recovery processes?

Principle 11 - Engineering Information Control
- What information about the system (e.g., requirements, procurement, engineering diagrams, processes and procedures) is sensitive and how is that information protected?
- How are internal stakeholders trained and held accountable to ensure potentially sensitive information is correctly identified and protected?
- How are data sensitivity controls and requirements passed to external stakeholders (e.g., subcontractors, service providers, distributors) and enforced through contracts, procurement, and reporting documents?
- How are internal stakeholder roles and associated access privileges defined and adjudicated to enable necessary access to sensitive system data?
- Do information security policies that overly constrain workflows "encourage" workarounds and bypasses?
- Could an adversary reasonably derive sensitive system information from hiring, recruitment, marketing or other externally facing information sources?

Principle 12 - Organizational Culture
- How do expectations around creating, operating, and maintaining the system transfer from the organization to supporting organizations (e.g., hardware vendors, consulting engineers)?
- How can choices that make the organization less resilient or bring on undue complexity/cost (e.g. delaying hardware and software life-cycle updates) be recognized and documented?
- What assumptions are made about existing skill and experience and what training, education, and practice will be needed for those who will operate, maintain, secure, and defend the system?
- How is interpersonal trust maintained across the entire organization?
- What processes ensure that operators consider the possibility of digital sabotage when responding to and diagnosing process anomalies?
- How can the organization foster a culture of timely reporting of issues in people, process, and technology without fear of reprisal, and with confidence that the issues will be addressed?
- How can the organization positively reinforce behaviors and choices that support security outcomes, while reducing those that harm security outcomes?

V. Applying the Questions

When answering these questions, engineers are guided to key considerations when interpreting the solution to a design problem through the CIE Principles. For each of the twelve principles, the questions guide engineers to the following behaviors and outcomes that provide direct beneficial design patterns throughout the system lifecycle.

Principle 1 - Consequence-Focused Design Engineers map out the system's critical functions and categorize high-consequence events with a cyber-risk focus, similar to their approach for safety risks. This enhances the risk assessment by ensuring that cyber-enabled high consequence events are monitored in system design and regularly reassessed with changing threats. Additionally, engineers and cybersecurity staff ensure that stakeholders are aware of and included in the decision-making for mitigation strategies.

Principle 2 - Engineered Controls Engineers identify how hazardous quantities are controlled by digital technologies and evaluate where analog or alternate controls could enhance resiliency, potentially taking 'dual-credit' for existing safety controls. This also guides continuous monitoring and validation of these engineered controls, especially during system changes and varying operational conditions. Additionally, engineers help validate these controls to ensure they are not circumvented by administrative workarounds.

Principle 3 - Secure Information Architecture Engineers identify the most consequential data elements and ensure their independence to effectively diagnose anomalies. This involves conducting a data exchange impact analysis to determine which information exchanges could result in high consequence events if manipulated. Engineers and informed cyber-professionals, then, implement engineering and operations-based monitoring and verification methods of these key data elements.

Principle 4 - Design Simplification Engineers evaluate opportunities to simplify or eliminate unnecessary device or system elements and features. Not for the sake of simplification, but under the understanding that this reduces threat vectors that may contribute to the realization of a high-consequence event. Furthermore, engineers consider non-digital or simplified alternatives while continuing to satisfy system requirements.

Principle 5 - Layered Defenses Engineers document the layers of digital and engineered controls present in the system. This includes judging the independence of multiple defenses to prevent cascading failures. Engineers also identify single points of failure

to cyber-risk and implement measures to mitigate their impact.

Principle 6 - Active Defense Engineers document indicators and early precursors of high consequence events. This enables the early detection of potential threats useful for cybersecurity professionals. In response to these indicators, engineers also develop and implement temporary operational changes to mitigate perceived threats effectively by operations staff.

Principle 7 - Interdependency Evaluation Engineers identify supporting utilities and critical inputs required by the system. This ensures that all dependencies are clearly understood. Engineers, then, can develop strategies to obtain these critical inputs from alternative sources in case access is lost, thereby maintaining system functionality. Any changes in interdependent systems are communicated effectively in the organization and used to inform possible additional control needs.

Principle 8 - Digital Asset Awareness Engineers hypothesize scenarios where digital functions/variables could be abused or misused, potentially leading to high consequence events. Engineers implement processes to ensure digital functions/variables are tracked in asset inventories. Additionally, engineers participate in the process for validating updates and patches to ensure they are necessary and do not introduce unexpected features.

Principle 9 - Cyber-Secure Supply Chain Controls Engineers document assumptions regarding the availability, quality, and security of critical products or services; which provides a foundation for supply chain risks. Engineers focus on reducing these risks by prioritizing the use of familiar technologies and reliable suppliers. Identified critical services and components are then used in alignment with specifications to minimize the potential for disruption.

Principle 10 - Planned Resilience Engineers define acceptable degradation limits for critical digital functions and develop alternate operating modes to maintain functionality within those limits. One key alternate operating mode for system design could include ensuring that automated processes have manual operation modes. Engineers provide assessment of the reliability of supporting utilities and help develop contingency plans to address potential cyber-enabled losses.

Principle 11 - Engineering Information Control Engineers identify and protect sensitive information about the system. Engineers inform internal stakeholders on how to identify this sensitive information. Access privileges for internal stakeholders are developed to ensure they have the necessary access to perform their roles without encouraging workarounds that could compromise data protection.

Principle 12 - Organizational Culture Engineers ensure expectations are effectively transferred to supporting organizations for a unified approach to system implementation and operation. They document choices impacting resilience to clarify trade-offs in decision-making and assess skills, providing necessary training and education for system operators and service providers.

VI. Conclusions

The minimum set of questions presented in this work provides a scaffolding for incorporating CIE principles into system design. A more comprehensive understanding is available through the CIE Implementation Guide [7] which presents questions across each specific stage of system design. This guide offers consideration for each system lifecycle phase, whether it be at the conceptual, operational, or decommissioning phases. By integrating these specialized questions into their design processes, engineers can proactively design systems with enhanced resilience. Such an approach is critical to ensure that digital functions are resilient to compromise by persistent adversaries, including nation-state actors. Modern systems must be designed to not only withstand attacks but also to continue functioning effectively, diminishing the consequences of any digital function compromise. This is especially true for those systems leveraged for critical infrastructure.

References

[1] The White House, “National cybersecurity strategy,” Online, 2023, accessed: 2024-08-19. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[2] Department of Energy, “National cyber-informed engineering strategy,” Online, 2022, accessed: 2024-08-19. [Online]. Available: https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf

[3] Cybersecurity and Infrastructure Security Agency, “Secure-by-design paper,” Online, 2023, accessed: 2024-08-19. [Online]. Available: https://www.cisa.gov/resources-tools/resources/secure-by-design

[4] National Institute of Standards and Technology, “Security and privacy controls for information systems and organizations,” Online, 2020, accessed: 2024-08-19. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

[5] Office of Cybersecurity, Energy Security, and Emergency Response, “Cybersecurity capability maturity model (c2m2),” Online, 2022, accessed: 2024-08-19. [Online]. Available: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

[6] International Society of Automation, “Isa/iec 62443 series of standards,” Online, 2007-2020, accessed: 2024-08-19. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[7] Department of Energy, “Cyber-informed engineering implementation guide,” Online, 2023, accessed: 2024-08-19. [Online]. Available: https://www.osti.gov/biblio/1995796