INL/EXT-16-40099
Revision 0

Cyber-Informed Engineering

Robert Anderson, Jacob Benjamin,
Virginia Wright, Luis Quinones,
Jonathan Paz

March 2017

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

INL/EXT-16-40099
Revision 0

Cyber-Informed Engineering

**Robert Anderson, Jacob Benjamin, Virginia Wright,
Luis Quinones, Jonathan Paz**

March 2017

**Idaho National Laboratory
Idaho Falls, Idaho 83415**

http://www.inl.gov

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

ABSTRACT

Securing critical digital assets in an ever-changing threat landscape requires more than a dedicated team of cybersecurity professionals. Traditional static defense mechanisms like airgaps and reliance on obscure protocols and access mechanisms may not be sufficient for in-depth defense in an always-connected, information-rich cyber environment. Though technical solutions exist to protect availability, integrity and confidentiality of industrial control systems, these solutions typically secure external system boundaries and not the underlying digital systems themselves. Training engineering personnel in cybersecurity or training information technology specialists in engineering is expensive and often ineffective at addressing systemic vulnerabilities in large and complex digital systems.

INL has developed a framework for bridging the gap between engineering design and cybersecurity to identify cyber vulnerabilities at the earliest stages in the system development life cycle and apply both engineering solutions and information technology to minimize the cyber-attack surface across the entire system engineering process. This methodology focuses on aiding engineering staff who traditionally envision, plan, design, implement, operate, and maintain such systems to understand cyber risk (without becoming cyber experts), and to integrate the subject matter expertise of cybersecurity specialists.

In this document, INL presents the elements of the Cyber-Informed Engineering (CIE) methodology and describes how they can be implemented and integrated. It includes both an application aid and an assessment aid.

CONTENTS

ACRONYMS

CIA	Confidentiality, Integrity, and Availability
CIE	Cyber-Informed Engineering
CSAT	Cyber Security Assessment Team
HART	Highway Addressable Remote Transducer
ICS	Industrial Control System
INL	Idaho National Laboratory
IT	Information Technology
NEI	Nuclear Energy Institute
NIST	National Institute of Science and Technology
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
NRMF	nuclear and radioactive material facilities
PLC	programmable logic controller
PPC	Plant Process Computer
PPS	physical protection system
SPDS	Safety Parameter Display System

Cyber-Informed Engineering

1. OBJECTIVE

Cyber-Informed Engineering (CIE) is a program that provides a framework for deepening the involvement of engineering staff in understanding and mitigating high-consequence and constantly evolving cyber threat within nuclear and radioactive material facilities (NRMF). The cyber threat is aided by the complexities and inter-dependencies of digital components and systems woven into NRMFs, and the engineers involved in the design, procurement, integration, operation, and maintenance of those systems have a unique understanding of and ability to mitigate these factors. The goal of CIE is to inform engineers on cybersecurity as it relates to them, and to strengthen their understanding of cyber risks and mitigations. CIE involves the complete engineering life cycle, and includes stakeholders who have historically limited their input to one subject area, such as safety, quality, physical protection, operations, and maintenance.

2. PURPOSE

Engineers develop solutions to problems encountered in an industrial application. As most engineering designs include safety as one of the highest priorities along with security and quality, the cyber threat brings a unique problem to the engineer. With nearly all instrumentation and control system designers implementing digital solutions, the potential has risen for cyber attacks as a vector to penetrate and move throughout systems, potentially without the user's knowledge. Consequences of this type of attack have not been fully analyzed and represent potentially grave scenarios. CIE makes the cyber threat relevant to the engineering discipline.

3. AUDIENCE

A CIE-defined target audience may extend to any person involved the engineering process, including engineers, operators, maintenance personnel, third-party contractors, and vendors. They all have a role and need to understand the potential cyber risks involved.

3.1 CIE Defined

3.1.1 CIE Definition

"Cyber informed engineering (CIE)[1] is a body of knowledge and a methodology to characterize the risks presented by the introduction of digital computer systems in a traditionally analog environment and offer a strategy to apply engineering risk processes to mitigate these risks. It includes methods to ensure that cyber risks are considered throughout the design life cycle, as well as techniques which allow the elimination of cyber risk via traditional engineering methods." This research focuses on aiding engineering staff who traditionally envision, plan, design, implement, and operate such systems to understand cyber risk (without becoming cyber experts), and to harness the subject matter expertise of cyber-security specialists to aid in minimizing cyber risk throughout the engineering life cycle across all manner of plant systems.

3.1.2 CIE Framework Elements

Cyber-informed engineering is presented as a framework of 11 elements through which an engineer can take an active role in the cyber-security process. Though no element of the framework is completely independent, each may be considered separately of the other.

---

[1] Anderson, R., and J. Price, *Cyber-Informed Engineering: The Need for a New Risk Informed and Design Methodology*, INL/CON-15-34244, https://inldigitallibrary.inl.gov/sti/6618307.pdf, June 2015.

3.1.2.1 Consequence/Impact Analysis. A cyber attack manipulates information confidentiality, integrity, or availability to achieve a desired malicious goal. Impacts may be as simple as exfiltration of sensitive information or may have the effect of physical sabotage. Although cyber-induced consequences or impacts can be recognized in systems throughout an entire organization, limited cybersecurity resources must focus on systems with critical functions that will create the biggest consequence or negative impact to the organization.

Ensuring an operationally safe system is one of the most important responsibilities of an engineer. Security, should closely follow safety as the two can affect each other. The intersection of safety and security sometimes has competing requirements and comes at a price where one requirement may interfere with the other. However, because a cyber attack may bypass original system design, unanalyzed pathways may exist that could render the system unsafe. Therefore, critical functions must be protected against such cyber manipulation at all cost. It is necessary to focus limited resources into the protection of high-consequence functions. A key framework element of the CIE program is the idea of identifying those few critical functions that absolutely must be available when needed. If digital technology is relied upon for these critical functions, then either very strong controls are required or the engineer must remove or minimize known digital vulnerabilities from the design. In domestic nuclear power, Nuclear Energy Institute (NEI) 10-04, Rev. 2,[2] may aid in identifying critical assets and NEI 08-09, Rev. 6, may aid securing the assets.

3.1.2.2 Systems Architecture. The information architecture of a system defines how data flows through the system. With proper architectural controls, access pathways are designed so that data flows through the system only in desired ways and attackers cannot subvert the architecture to use the system or its information in undesired ways. Common tools include data diodes, enclave networked design, network zones, and virtual and local area networks. Some modern engineering system designs include internal controls over the flow of information between subcomponents that intend to provide more robust information architecture within the system. Often, engineering systems are not designed with secure information architecture. In that case, the cyber-informed engineer or technical specialist must consider technology solutions to enforce architectural controls between systems or subsystems. The National Institute of Science and Technology (NIST) created a guide describing key architectural security techniques that can be applied to industrial control systems.[3]

3.1.2.3 Engineered Controls. Controls used to mitigate cyber vulnerabilities must be considered early in the engineering life cycle rather than added or bolted on after the final design. In some cases, the engineering team can design cyber vulnerabilities out of the system or add engineered controls, which mitigate the consequences presented by the vulnerability. Where the need for additive Information Technology (IT) controls for vulnerabilities are either reduced or eliminated, efficiencies in cost and performance can be realized. This idea of introducing engineering controls to mitigate cyber vulnerabilities is not typically considered in modern engineering solutions. However, if implemented, such strategies present a more-robust engineering solution than the alternative with add-on IT equipment. The engineer should consider the cyber specialist as part of the requirements and design team for all digital system design or modification so that vulnerabilities, potential consequences, and applicable engineering controls are considered early and frequently as cyber tactics continually change.

Additive controls include those cyber controls contained in NEI 08-09, Rev. 6, and Nuclear Regulatory Commission (NRC) RG 5.71 appendixes. These controls include intrusion detection systems, insider mitigation programs, and defense in depth.

---

[2] NRC, "Identifying Systems and Assets Subject to the Cyber Security Rule," Nuclear Regulatory Commission, NEI 10-04, Rev. 2, July 2012.

[3] NIST, "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication 800-82 Rev 2, http://dx.doi.org/10.6028/NIST.SP.800-82r2, May 2015.

3.1.2.4 Design Simplification. In modern control system design and operation, the advantages and efficiencies of digital technology have created complex designs and automation that, in many cases, require a team of subject matter experts to understand the full context of process and system functionality. Reliance on complex digital control is common, especially when vendor solutions provide an abundant set of functions and capabilities. While digital system design allows for great efficiencies, its complex nature provides a robust, potentially vulnerable network landscape. The more complex the digital system, the more opportunity it presents for the adversary. Where possible, the engineering team must reduce the complexity of digital design to the bare minimum that is absolutely necessary for critical functions. Implementing the As Low As Reasonably Achievable metaphor can minimize a plethora of vulnerabilities. However, the team must ensure that such functionality reduction does not lead to system frailty. The team must also remember that a procured system may have functionality that is not enabled within the current installation but is latent within the device, such as functionality disabled in software. This functionality must be secured too, as hackers are not bound by software configuration limitations. In some cases, non-digital solutions may provide the safeguards needed to protect against malicious attack. Relying on past practices of security by obscurity, antiquity, or isolation does not work in the modern digital era. NRC RG 5.71,[4] Section B.5.1 (page B-17), "Removal of Unnecessary Services and Programs," offers guidance for domestic nuclear power plants.

3.1.2.5 Resilience Planning. With modern digital systems, vulnerabilities will always exist, whether known or unknown. Because this assertion implies that no digital system is completely secure, it is consequently expected that any given digital component or system may be compromised sometime during its life cycle. Thus, the engineering team must engage in resilience planning for continued operation during and after cyber attacks, even if degraded. Note that simple redundancy in the cyber environment does not introduce resilience as cyber attacks may be levied across multiple systems with the same capabilities and vulnerabilities without a significant increase in the expenditure of effort for the attack. Resilience can imply a hardening of specific components or systems that make an attack more difficult. Contingency planning must also be considered if a compromise has occurred. (How will the compromised system be operated after a detected attack, or how can other systems be used to establish confidence?)

3.1.2.6 Engineering Information Control. As engineering projects commence, it is important to protect specific engineering records that may be considered sensitive information including requirements, specifications, designs, configurations, analysis, testing, and many other activities. Responsibility does not solely rely on the internal engineering team; responsibility should include third-party vendors, analysts, integrators, technical authorities, regulators, or other competent authorities. Sensitive information such as this, if freely distributed outside of protected boundaries, may put these engineered systems at risk. Social media, vendor or corporate websites, conferences, and other public-facing avenues can provide the adversary with plenty of information as they begin their reconnaissance efforts. Even engineers' resumes posted on job-hunting sites can provide a wealth of information for attackers. Such sensitive information must be protected not only during the design and installation process, but as long as the system is operational.

3.1.2.7 Procurement and Contracting. An organization's security requirements, if not transmitted to vendors, integrators, and third-party contractors, will not be adhered to in systems provided by these entities. It is imperative that outside vendors be held responsible for strong cybersecurity and collectively considered as part of the overall organizational cyber defensive posture. One external mobile device connecting to a plant network or isolated remote system can expose an entire organization to cyber attack, including its critical operations. Requiring third parties to deliver hardened components and systems and secure organizational processes, along with hardened perimeter defenses, is absolutely

---

[4] NRC, "Cyber Security Programs for Nuclear Facilities," Nuclear Regulatory Commission, Regulatory Guide 5.71, http://www.nrc.gov/docs/ML0903/ML090340159.pdf, January 2010.

necessary as part of a complete cybersecurity program. Procurement language must include specific requirements that a vendor must comply with as a part of the system design, build, integration, or support. These requirements consider the entire supply chain process from multi-tiered subcontractors, to manufacturer design and fabrication, to final delivery and acceptance. Though such requirements can raise contracting costs, the risk to the organization of a control system breach is minimal in comparison.

An example of procurement language, including requirements for cybersecurity of Control Systems, may be found in the Department of Homeland Security's *Cybersecurity Procurement Language for Control Systems*.

3.1.2.8 Interdependencies. Engineering requires the support of many disciplines, including safety, quality, maintenance, chemical, and others. In a well-orchestrated engineering design, all disciplines share information on how non-desired digital manipulation to a system could affect their area of concern, such as cooling, water, power, communications, etc. The system owner can plan for risks introduced by these interdependencies and understand cybersecurity aspects of the interconnections. For domestic nuclear power plants (NPPs), NEI 08-09, Rev. 6, was used to create a Cyber Security Assessment Team (CSAT). The CSAT consists of individuals with broad knowledge in key disciplines to oversee the cybersecurity assessment process. They rely on their diverse knowledge to ensure interdependencies and impacts are accounted for in the assessments and mitigations.

For NPPs, some interdependencies may fall outside of the "bright line"[5] to include transmission entities that often house equipment on the NPP site, even inside the protected area. Therefore, familiarity with appropriate regulations outside the NRC (e.g., Federal Energy Regulatory Commission and North American Electric Reliability Corporation) may be applicable. NEI 13-10, Rev. 4, provides guidance for securing these "balance of plant" assets that fall outside of the "bright line."

3.1.2.9 Cybersecurity Culture. Safety culture has permeated most industries over the past 50 years as human injury is not acceptable and accidents can cause large financial loss as well as public distrust. Security culture has been reserved primarily for those few personnel and physical systems that protect perimeters, control entry points, and patrol vital areas. In contrast, cybersecurity was initially viewed as an IT problem defending against Internet attacks. Cybersecurity should be treated with the same rigor and attention as physical protection security. Recognizing and implementing cybersecurity is imperative to maintaining a robust safety culture.

Cyber attacks threaten to diminish not only safety controls, but also physical security controls. The ability to intelligently, in real time, affect a digital component or system by overriding its design instructions to perform malicious acts can result in immense consequences for an organization's safety and (physical) security.

As cybersecurity is included into engineering processes, the engineering discipline must be included into cybersecurity. All staff are part of the cyber defense team and must be enlisted to endorse cybersecurity principals that allow them to understand how cyber attacks are utilized for malicious manipulation and perpetuated as more digital technology is brought into everyday activities. The Internet of Things will continue to stress organizational infrastructure while mobile technology will continue to add digital attack pathways. From an engineering perspective, a cybersecurity culture must be institutionalized and include demands that any interaction with digital components or systems receive careful consideration.

---

[5] NRC, "Policy Issue Information," SECY-10-0153, http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2010/secy2010-0153/2010-0153scy-redacted.pdf, November 19, 2010.

Bringing cybersecurity to the same level of acceptance and practice as safety would have an immense effect on the organization's defensive security posture. Much like a safety culture, a cybersecurity culture requires the enlistment and endorsement of the entire staff. Staff that understand the need for security, and their part in the overall security culture helps to ensure that they follow the processes and procedures necessary for strong cybersecurity. Measures, such as establishing controls over removable media, can greatly increase cybersecurity, but only if all users participate in the process.

3.1.2.10 Digital Asset Inventory. Maintaining a complete and accurate digital asset inventory provides a mechanism for organizations to track and analyze not only the hardware and software they possess, but also vulnerabilities residing in them. A complete inventory includes hardware, firmware, and software version levels of all engineering systems within the organization. Engineering and technical personnel must be aware of and understand every digital asset to provide adequate protective measures. Although this element seems fundamental, many complex digital systems undergo numerous upgrades, revisions, and design modifications but the engineers never update their respective asset inventories. A regular "as-built" assessment to verify that the inventory data matches the systems in place is a useful protective mechanism.

Guidance for identification of critical systems and critical digital assets in domestic NPPs may be found in NEI 10-04, Rev. 2, NEI 08-09 Rev. 6, and RG 5.71.[6] The process of asset identification in domestic NPPs requires input from individuals knowledgeable in NPP operations and engineering, information and digital system technology, and physical and emergency preparedness. These individuals typically make up the CSAT and work with system engineers, Instrumentation and Control technicians, security officers, emergency preparedness experts, and the cybersecurity specialist(s).

3.1.2.11 Active Defense. Most cyber defenses to date have been based upon passive protection schemes. These models are primarily reactive to known cyber tactics, techniques, and procedures. Active defense will include dynamic strategies and enhanced technical skill competencies to combat directed persistent attacks utilizing human behavior, supply chain, and state of the art technology. An active defense becomes even more important as part of a resilient strategy. Perimeter defenses and fortress mentalities are ineffective against increasingly advanced cyber attackers. Broad monitoring and detection capabilities must be intrinsic for critical systems. Robert M. Lee from SANS[7] conceptualizes in his whitepaper *The Sliding Scale of Cyber Security* that "The Sliding Scale of Cyber Security is a way to add nuance to the discussion of cyber security by categorizing the actions, competencies, and investments of resources that organizations can make to defend against threats. The model serves as a framework for understanding what actions contribute to cyber security." Defenders must be able to anticipate, detect, and neutralize adversary strategies and tactics while eradicating any artifacts left by the attacker. This also implies the recognition of adversary intelligent co-adaptive behaviors. As was mentioned in Section 3.1.2.1 above (consequence analysis), focus for active defense should concentrate on critical functions. Active defense is more than detection; it is providing the ability to quickly collapse and remove the attacker's presence within the system. Only by having a full, accurate, and complete understanding of all system interactions is the defenders capable of sucha task. The key to active defense is highly skilled personnel resources that can evolve their capabilities to include creative and flexible behaviors.

In addition, and similar to physical protection system (PPS) performance testing, cybersecurity measures should be exercised to verify and validate a strong cyber defense. This would be considered as a subcomponent of a cybersecurity assessment program. Where PPS can test production equipment, cybersecurity measures or controls testing may run the risk of equipment or software damage. It is important that if cybersecurity performance testing is to be executed, a test environment similar to

---

[6] NRC, "Cyber Security Programs for Nuclear Facilities," Nuclear Regulatory Commission, Regulatory Guide 5.71, http://www.nrc.gov/docs/ML0903/ML090340159.pdf, January 2010.

[7] SANS Institute, https://www.sans.org/.

production should be developed. NEI 08-09, Rev. 6, Appendix E, Sections E-7 and E-8 provide guidance on testing and drilling cyber incidents.

4. INDUSTRY VALIDATION

4.1 Next Steps

The framework will be validated through presentation at multiple venues. Industry feedback will be incorporated into future versions of the framework and it will be updated to reflect the priorities a variety of audiences assign to the elements. An updated version of the document will be published in March 2017.

4.1.1 Tools Development

Multiple tools will be developed to aid in the adoption of CIE, including a life cycle-phase grid showing how the elements can be best applied at each phase of the engineering life cycle, talking points guiding conversations, reference lists to supporting documentation, etc. These tools will be published in the CIE update for March 2017.

4.1.2 Cyber-Informed Engineering Assessments

Finally, the team will perform a CIE assessment at a U.S. nuclear reactor, to evaluate the degree to which the team is employing CIE principles and identify proposed improvements. Results will identify opportunities and potential solutions that may also benefit other representative facilities to strengthen the effectiveness of cybersecurity and help put in place processes that can adapt as threats evolve. In addition, this assessment will identify additional tools needed to improve CIE.

APPENDIX A

SOURCE MATERIALS BACKGROUND

APPENDIX A

SOURCE MATERIALS BACKGROUND

A-1. HISTORY OF INSTRUMENTATION AND CONTROL SYSTEMS

Instrumentation and control systems migrated from analog to digital technology throughout the late 1960s and into the 1980s. Where analog devices contain limited remote configuration capabilities or any cyber attributes, digital technology provides increased efficiencies through complex algorithms and automation, the ability to remotely change configuration to meet timely business demands and functionality, provide data to any consumer, and communicate beyond physical borders. Emphasis for the code developers was on functionality, communications, and time to market, not security.

As a result of this history, digital technology has revolutionized the modern era of instrumentation and control for nuclear and radioactive material facilities as well as our personal everyday lives. Because of this fact, the engineering profession must embrace the other fact that with digital technology comes cyber attacks. Mitigations for these cyber threats must be included in every digital design and deployment to minimize potential catastrophic consequences.

A-2. DIGITAL INTEGRATION INTO INSTRUMENTATION AND CONTROL

Most everything in the modern era contains digital devices to monitor, control, store, process, or communicate information. Digital technology has been integrated into every part of society, including social activities. With this continued migration to incorporate nearly every device with digital technology and the ability to communicate (Internet of Things[8]), the engineer must address how the surrounding systems interact and/or may provide for new communication pathways never previously conceived. Some devices can be used as air gap connections, access vectors through trusted relationships never questioned in the past, and information security exfiltration mechanisms never thought possible.

A-3. HISTORY OF CYBER EVENTS AFFECTING INSTRUMENTATION AND CONTROL SYSTEMS

In January 2003, the **Davis-Besse Nuclear Power Station** was infected by the "Slammer" worm virus.[9] Although the virus did not enter the network within the Davis-Besse plant directly, it was able to infect the unsecured network of a Davis-Besse contractor. This contractor had a T1 connection that bridged their unsecured network to the corporate network within the Davis-Besse plant. Investigators later found that there were multiple connections from the Davis-Besse corporate network that bypassed their firewall. According to the April NRC filing by FirstEnergy, this connection essentially created a backdoor from the Internet to the corporate internal network that was not being monitored by any personnel. After gaining access to the corporate network, the worm then infiltrated the plant network. Operators began to notice a decrease in performance within the plant network. Eventually, the worm caused the plants Safety Parameter Display System (SPDS) to crash. This system was responsible for relaying critical information about the reactor core, such as information from coolant systems, temperature sensors, and radiation detectors. These components would be essential for determining a meltdown condition. After the SPDS crashed, another less-critical monitoring system called the Plant Process Computer (PPC) was also taken offline by the worm. It took 4 hours and 50 minutes to restore functionality to the SPDS and 6 hours and

---

8 ITU, "Overview of the Internet of Things," http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060, June 15, 2012.

9 Poulsen, K., "Slammer worm crashed Ohio nuke plant net," The Register, http://www.theregister.co.uk/2003/08/20/slammer_worm_crashed_ohio_nuke/, August 20, 2003.

9 minutes to restore the PPC. Although there were redundant analog components to provide the necessary information to monitor the reactor, this burdened operators since they were required to visit each component to view the necessary information instead of having all of the necessary information available on a single console. This incident perfectly illustrates the simplicity in orchestrating a cyber attack on a control system once the firewall within the network is breached.

- In 2006, the **Browns Ferry Nuclear Power Plant**[10] in Alabama experienced an unusual spike in the data traffic (aka data storm) that reached a programmable logic controller connected to the water recirculation pump actuators causing the actuators to remain in an unresolved status loop. This forced the nuclear plant operators to manually shut down the reactor. The ICS network was not connected to any external network (isolated).
- In March 2008, Unit Two of the **Edwin I. Hatch plant** shut down for 48 hours as a result of an engineer updating a computer on the business network of the plant that was used to collect diagnostic data from the process control network.[11] The update was designed to synchronize the data from the business network with the process control network. After performing the update, the engineer rebooted the computer, which caused the synchronization program to reset the data located on the control network. This caused the control systems to interpret the reset as a sudden drop in the reactor's water reservoir and caused the plant to initiate an automatic shutdown. This example shows the dangers of linking the control network with the business network. Even if there is an increase in availability for the engineers that monitor the reactor, it is still relatively simple to cause a disruption.
- NRC released 10 CFR 73.54,[12] "Protection of Digital Computer and Communication Systems and Networks," on March 27, 2009.

In June 2010, a 500-kB computer worm called Stuxnet[13] was responsible for the attack of the Natanz Enrichment Complex on November 2007 in Iran. Stuxnet is believed to have entered the system via a USB drive, infecting control network computers running Microsoft Windows Operating System. It was able to bypass security checks by presenting a digital certificate allowing it to move freely in the network. Stuxnet then searched for Siemens Step 7,[14] the Windows-based industrial control software used with Siemens S7300[15] programmable logic controllers (PLC) that are used to control the centrifuges at this plant. Stuxnet replicated itself across the network, remaining latent when it was not on a target machine, but activating on machines with Step 7 resident. Stuxnet attempted to obtain access to the Internet to download the most recent version of itself. Once Stuxnet was able to find the correct PLCs, Stuxnet was able to exploit existing "zero-day" software vulnerabilities. Stuxnet eventually gained control of the variable-frequency drives and finally compromised the centrifuge motors making them spin to failure, while at the same time transmitting false information to operators about the state of the PLCs.

---

[10] Lemos, R., "'Data storm' blamed for nuclear plant shutdown," The Register, http://www.theregister.co.uk/2007/05/21/alabama_nuclear_plant_shutdown/?page=1, May 21, 2007.

[11] Krebs, B., "Cyber Incident Blamed for Nuclear Power Plant Shutdown," The Washington Post, http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html, June 5, 2008.

[12] 10 CFR 73.54, "Protection of digital computer and communication systems and networks," Nuclear Regulatory Commission, http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html, December 2, 2015.

[13] Kushner, D., "The real story of Stuxnet," IEEE Spectrum, http://spectrum.ieee.org/telecom/security/the-real-story-of- stuxnet, February 26, 2013.

[14] Siemens, "SIMATIC Step 7 Software," http://w3.siemens.com/mcms/simatic-controller-software/en/step7/Pages/Default.aspx.

[15] Siemens, "SIMATIC S7-300," http://w3.siemens.com/mcms/programmable-logic-controller/en/advanced-controller/s7-300/Pages/Default.aspx.

A-4. CONSEQUENCE – WHY WE CARE

Within the engineering discipline, strict analysis, processes, procedures, and critical thinking are essential. It requires that knowledge of the subject matter be exhaustive and complete so that no unmitigated risk remains that is unacceptable. Traditionally, safety has been the most important aspect of the engineering discipline. However, within the safety envelope, security plays a key role in the protection of those safety mechanisms. Historically, security has been defined as "physical" by nature. However, cyber attacks are now an established threat vector that engineers do not typically consider in their designs or risk analysis. This new, dynamic, and highly successful attack threat vector can potentially manipulate or defeat safety protections. Cyber must be fully understood to alleviate critical consequences.

Organizations must channel limited resources into those digital systems or components that, if left unprotected, could generate very high consequences from a cyber attack. Organizations have performed analysis of severe accident scenarios, but the analysis has been through the lens of equipment or operator failure. There has been next-to-no analysis performed that examines the severe accidents or high-impact consequences an attacker might create by leveraging digital equipment. For some systems, a non-digital solution may be required as either a fail-safe or alternate information source to mitigate the potential for a negative consequence.

APPENDIX B

ENGINEERING FOR CYBERSECURITY

APPENDIX B

ENGINEERING FOR CYBERSECURITY

Cybersecurity has historically concentrated on Information Technology (IT) processes and solutions. These solutions do not take into account the entire engineering process and cannot "engineer" vulnerabilities out of the system. Thinking about cybersecurity requirements and assumptions during the engineering process in the initial life-cycle phases allows for a design that may use a variety of methods to ensure the requirements are met or that may mitigate vulnerabilities. A simple example of this concept would be the addition of logging capability requirements to a small embedded control processor to ensure that data passing into and out of the processor could be reviewed if necessary. This minor change during the design phase would make a huge difference in the security of the final design.

B-1. EXISTING ENGINEERING PROCESSES AND METHODS FAIL TO CONSIDER CYBER RISK

As the typical engineering process considers many factors into the requirements and design phases, one piece is always missing, namely the cyber component. Most engineering projects may only invoke IT-type cybersecurity, which assumes a bolt-on solution already exists that is added to the final design. Engineering system design reviews are held without IT or cyber subject matter expertise. Until recently, the cyber risk was almost never asked about or required to be part of any digital design. The addition of a cyber engineer or specialist can help engineering technical personnel consider cyber risk during all life-cycle phases including risk assessments.

B-2. SECURITY CULTURE

Security culture is prevalent within some industries, including nuclear; however, it is never proportional to the safety culture. Safety has been the highest area of concern for over a half century. The nuclear industry has become very good with safety-based risk analysis and has a lot of data to justify its predictions and analyses. However, security risk assessments have typically been confined to physical protection vulnerabilities shown to be mitigated via guards, gates, and guns. With the addition of digital technology, cybersecurity has been slow to adapt and keep up with an alarming rate of attacks.

B-3. CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY TRIAD – CIA

Professionals working in industrial control systems and IT share a common philosophy as the basis for determining the state of their system's security.

For IT systems, this architecture is referred to as the Confidentiality, Integrity, and Availability (CIA) triad[16] here confidentiality is the concept of making the information held within a system inaccessible to unauthorized users, integrity is the concept of keeping the information on the system unaltered from the original source and availability is the concept of ensuring that all data is accessible to the authorized viewer at all times.

For industrial control systems the triad becomes AIC, emphasizing Availability of data as the most important component for continuous, batch, or hybrid processes, followed by Integrity and Confidentiality.

B-4. DEFENSE-IN-DEPTH

Current ICS security best practices dictate that organizations employ a number of different strategies for the protection of their networks, including defense-in-depth, agile defense, and moving target defenses. The goal of this should be to employ a holistic approach that acknowledges the likelihood of a compromise and takes additional measures to limit the destructive impact of a cyber incident.

16 Albuquerque, R., L. Villalba, A. Orozco, F. Buiati, and T-H. Kim, "A Layered Trust Information Security Architecture," NCBI, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4299037/.

In addition to passive defensive measures, engineers should employ active defenses, such as network intrusion detection combined with baselining of network configurations and communications traffic to support anomaly detection methods that can detect even subtle changes. These proactive defenses should be thought of as a second-line of defense for a well-designed system.

NRC RG 5.71[17] discusses a nuclear defense-in-depth strategy as part of an overall defense mechanism for network/system security. It goes on to state: "Under a defense-in-depth strategy, the failure of a single protective strategy or security control should not result in the compromise of a safety, important-to-safety, security, or emergency preparedness function." While this is true, the engineer is encouraged to recognize within this approach the notion that an unseen/unknown failure is a missed opportunity to identify a potential breach. It is important to recognize that properly designed security controls should be understood to function not only as protection to equipment, but also as warnings and indicators. While the need to reduce complexity is highly valued for its ability to enable safe efficient operations, recognizing where resilience in design can serve to provide indications of issues is a key balance that an engineer must always strive to achieve.

B-5. AIRGAP MYTH/NETWORK ISOLATION

While a strategy of system isolation provides some protection from a cyber event, ensuring isolation over the lifetime of a network is generally considered not to be attainable.

Software licenses will be updated, system software patches will be required, hardware components will be upgraded, and vendors will require access for system maintenance and upgrades.

Software patching is increasingly being shown as a vector to introduce unauthorized code into networks. The typical proposed mitigation to this is a combination of portable media controls with validation of patches, but this methodology is not completely effective as most vendors supply software in black box form, with most end users unable to validate or verify changed functionalities.

To cyber adversaries, the airgap is termed as an "extremely high latency network connection" often because it does not stop information flow. This is aided in part by over reliance on "one-way guards" or "data diodes" without engineering proper controls to characterize the data being transported by these devices. Thus, it is advisable to consider the "airgap" as a barrier instead within a larger network/system design rather than as the primary or "ultimate" control.

B-6. WIRELESS TECHNOLOGY

Industrial sectors with sites located miles or kilometers apart from one to each other utilize wireless technology as their potential intercommunication solution. Advantages of wireless communications include wide-area connectivity, parallel pooling, redundancy, and hot standby. Disadvantages include potential data interception and modification if the data is not encrypted, signal spoofing, and limited bandwidth. Local area network/wide area network,[18] wireless personal area network,[19] and Bluetooth[20] technology have been dominating the industrial application scene.

The Highway Addressable Remote Transducer (HART)[21] protocol is a master/slave protocol for digital communications over the standard 4–20 mA analog communication signal that is commonly used for ICS integration efforts, and it can be used in various modes such as point-to-point or multidrop.

The HART protocol may provide a communication path between networks that have a HART-enabled signal shared between them. If this communication is exploited, an adversary may both bridge the two networks together and enable a covert communication path for staging of malicious software, or implementing tracking of exploitation progress. It is important to note that HART has been shown to be a vector for code injection and other data tampering issues.

---

17 NRC, "Cyber Security Programs for Nuclear Facilities," Regulatory Guide 5.71, Nuclear Regulatory Commission, Cyber security programs for nuclear facilities: https://scp.nrc.gov/slo/regguide571.pdf, January 2010.

18 IEEE, "IEEE 802.11 Wireless Local Area Networks," http://ieee802.org/11/, 2016.

19 IEEE, "IEEE 802.15 WPAN (TG4)," http://ieee802.org/15/pub/TG4.html, September 28, 2016.

20 IEEE, "IEEE 802.15.1 Bluetooth (TG1)," http://www.ieee802.org/15/pub/TG1.html, September 28, 2016.

21 FieldComm Group, "HART Communication Protocol: How HART Works," http://en.hartcomm.org/hcp/tech/aboutprotocol/aboutprotocol_how.html, 2014.

B-7. KEY TECHNOLOGY RISK AREAS

B-7.1 "Over" Functionality/Latent Capabilities

New components that are being manufactured may contain a myriad of features that can be useful for a system and can potentially make it more efficient. However, there may be additional features added to the component to increase the amount of potential customers that may be interested in purchasing it.

These features may not be useful in every system in which the component is installed. While this observation may seem trivial, these extra features can develop into being potential as they become invisible in the system design. Functions that are merely disabled on the software level can be used by an attacker not limited by the designed HMI or software configuration. Because of this, it is important for the cyber-informed engineer to collaborate with the cybersecurity specialist to assess any risks associated with latent capability functions, and what steps should be taken to disable these functions on both the hardware and software level so they cannot be exploited.

B-7.2 The Cybersecurity Specialist, Vendors, Subcontractors, Integrators, and Service Providers

One common weakness that all systems share is their vulnerability to authorized users performing actions that are beneficial to an attacker but detrimental to the system. However, an authorized user may not be an employee at the company where the system is housed; they also come from an external source. Vendor support, subcontract employees, or third-party installers are all potential external authorized users. These users are often a target of choice for an attacker to extract information by means of social engineering. Techniques include ruses to gain physical access to a subcontractor's computer system, or to extract useful information by glancing at the top of employee desks or looking through their trash.[22]

Third-party vendors also pose a risk. Manufacturing components for a system also involves the work of employees, from development to assembly. It is possible for an attacker to infiltrate these facilities and extract information or even implant their own malware into the component before it is shipped out. Because of this, it is important for the cyber-informed engineer to assume that all new components that arrive from a manufacturer are not free of malware or tampering. It is also important that physical controls are in place throughout the facility, which limits the amount of information that third-party authorized users have access to.

B-8. ASSESSMENTS

Cyber-Informed engineering emphasizes the necessity of an "ICS-CS-IT" team following the NRC recommendations written for NEI 13-10 [Rev.0],[23] "Cyber Security Control Assessment," published in December 2013, which describes guidance for licensees to implement cybersecurity controls on critical digital assets consistent with the methodology described in Section 3.1.6 of the Cyber Security Plan.[24]

B-8.1 SANS ICS Kill Chain

The SANS ICS Cyber Kill Chain[25] is a model that has been put forward as the stages of an incident that an adversary must go through to exploit/attack a system. It is divided into two major stages, each with multiple substeps that can serve as disruption points to either detect and respond, or inhibit an adversary's ability to execute a full attack.

---

22 Gragg, D., "A Multi-Level Defense Against Social Engineering," SANS Institute, https://www.sans.org/reading-room/whitepapers/engineering/multi-level-defense-social-engineering-920, December 2002.

23 NEI, "Cyber Security Control Assessments," Nuclear Energy Institute, NEI 13-10, Rev. 0, http://pbadupws.nrc.gov/docs/ML1333/ML13338A622.pdf, December 2013.

24 NEI, "Cyber Security Plan for Nuclear Power Reactors," Nuclear Energy Institute, NEI 08-09, Rev. 6, http://pbadupws.nrc.gov/docs/ML1011/ML101180437.pdf, April 2010.

25 Assante, M. J., and R. M. Lee, "The Industrial Control System Cyber Kill Chain," SANS Institute, https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297, October 2015.

B-8.2 CSET

Cyber Security Evaluation Tool[26] is a Department of Homeland Security software tool that guides users step by step to assess the security of their cyber systems and information technology networks derived from a database of cyber-security standards, guidelines, and practices.

[26] ICS-CERT, "Cyber Security Evaluation Tool (CSET)," Industrial Control System Cyber Emergency Response Team, https://ics-cert.us-cert.gov/Assessments, 2016.

APPENDIX C

ENGINEERING LIFE CYCLE AND POST-BUILT DEFINITIONS

APPENDIX C

ENGINEERING LIFE CYCLE AND POST-BUILT DEFINITIONS

Cyber-informed engineering (CIE) can be used across the entire life cycle from conceptual design to decommissioning (using cyber and engineering controls) on non-digital and digital systems. The life-cycle phases are based on the IEEE 1220-2005 standard.

C-1. CONCEPTUAL DESIGN PHASE

Conceptual design is the first step of any new engineering design. After the find for need, the idea is studied, evaluated, and budgeted to determine if the need is real. It is during this phase that provides the understanding of how the required systems will work, and the how behaviors and performance can be understood.

C-2. REQUIREMENTS/SCHEMATIC PHASE

The requirements/schematic phase is when the development team develops the final product requirements. Information, such as technical and functional requirements and specifications are defined.

C-3. DESIGN DEVELOPMENT PHASE

The design development phase is when the conceptual design ideas and the requirements information turn into documents such as blueprints where the required systems are described in architectural and engineering drawings and if needed, construction documents.

C-4. COMPUTER SIMULATION PHASE

A computer model of the proposed system may be developed and examined to ensure that all system requirements have been accurately determined.

C-5. PROCUREMENT PHASE

If not already determined, vendors, integrators, and other project performers are determined and specific contractual documentation is developed to direct their efforts.

C-6. CONSTRUCTION/IMPLEMENTATION/INTEGRATION PHASE

The operations/construction/implementation phase is when the design and requirements for the system are physically implemented.

C-7. TESTING PHASE AND SIMULATION

The testing phase (software and hardware) ensures the quality, performance, and/or reliability of the developed system.

C-8. POST-CONSTRUCTION

After the engineering project is completed, asset owners and stakeholders are provided with the final set of blue prints and construction documents to ensure the requirements were met.

C-9. OPERATIONS AND MAINTENANCE

During the operations and maintenance phase, the system performs the desired function and as needed, specific alterations or repairs to the system are conducted.

C-10. DECOMMISSIONING

Decommissioning involves the removal of the system from operations and the disposal of both system components and archiving of documentation.

APPENDIX D

APPLICATION AIDS

APPENDIX D

APPLICATION AIDS

Cybersecurity Checklist

Information

Facility: _____ Date: _____

Project: _____ System(s): _____

1. Common Elements for All Phases of the Life Cycle

- ☐ 1.1 Personnel are up-to-date on cybersecurity awareness training and understand their part in the overall security culture.
- ☐ 1.2 Personnel follow cybersecurity processes and procedures that are in place.
- ☐ 1.3 Protect engineering records that may be considered sensitive information.
- ☐ 1.4 Avoid accidently disclosing sensitive information via phone calls, e-mails, or notes left unattended.

2. Conceptual Design

- ☐ 2.1 Contact cyber specialist to join the project design team.
- ☐ 2.2 Consider architecture to minimize digital footprint.
- ☐ 2.3 Document and prioritize identified risks of most importance.
- ☐ 2.4 Consider data flows throughout the system.
- ☐ 2.5 Consider engineering controls while defining design.
- ☐ 2.6 Design goal to minimize complexity to the bare minimum necessary for critical functions.
- ☐ 2.7 Review any lessons learned or operating experience for the system, especially ones involving digital equipment or cybersecurity.

3. Requirements / Schematics

- ☐ 3.1 Cyber specialist identifies any necessary IT controls, including information flow and monitoring controls.
- ☐ 3.2 Consult standards or regulation for additional requirements (ISO 14001-215, NEI 08-09, IAEA NSS 17, NIST 800, RG 5.71, etc.).
- ☐ 3.3 Require diversification to the greatest extent possible.
- ☐ 3.4 Determine vendor considerations or requirements for cybersecurity maintenance (patches, vulnerability disclosures, etc.).

4. Design Development

- ☐ 4.1 Contact the cyber specialist and identify any necessary IT controls, including information flow and monitoring controls.
- ☐ 4.2 Design digital pathways so that information can ONLY flow in desired and analyzed pathways.
- ☐ 4.3 Collaborate with the cyber specialist to map the system against the SANS ICS Kill Chain (an adversary's perspective).
- ☐ 4.4 Develop strategies to detect, anticipate, and neutralize cyber attacks.
- ☐ 4.5 Identify interdependencies by obtaining input from cross-disciplinary representatives.
- ☐ 4.6 Engage in resilience planning for continued operation during a cyber attack.

5. Computer Simulation

- ☐ 5.1 Simulate a cyber attack on the system by controlling the availability and integrity of system resources.
- ☐ 5.2 Simulate operator responses using Standard Operating Procedures (SOPs) and Emergency Operating Procedures (EOPs).
- ☐ 5.3 Document and review the results of the simulation.
- ☐ 5.4 Evaluate the results of the simulation and determine if any corrective actions are necessary before moving forward with the design.

6. Procurement

- ☐ 6.1 Consult DHS Cybersecurity Procurement Language for Control Systems.
- ☐ 6.2 Use cybersecurity procurement language to hold vendors responsible for strong cybersecurity.
- ☐ 6.3 Include disabling or securing latent functionality within the equipment specification.
- ☐ 6.4 Ensure the vendor provides sufficient details on hardware, software, and firmware versions to create and asset inventory.

7. Construction / Implementation / Integration

- ☐ 7.1 Maintain the digital asset inventory by updating it with accurate details on hardware, software, and firmware versions.
- ☐ 7.2 Confirm and identify any new cross-disciplinary interdependencies.

8. Testing & Simulation

- ☐ 8.1 Ensure that complexity reduction did not lead to a lack or resiliency or system frailty.
- ☐ 8.2 Test the defensive protections using a representative test bed as applicable to ensure the protections remain effective.
- ☐ 8.3 Ensure the vendor documents and removes any facility or site acceptance testing artifacts.

9. Post Construction / Operations & Maintenance

- ☐ 9.1 Maintain the digital asset inventory by updating it with accurate details on hardware, software, firmware versions.
- ☐ 9.2 Periodically test the defensive protections using a representative test bed to ensure the protections remain effective.
- ☐ 9.3 Restart the checklist for any additions, modifications, or renovations to the system during its life cycle.

10. Decommissioning.

- ☐ 10. 1 Ensure any digital equipment from the system is sanitized before being discarded or repurposed.

Checklist Step	Framework Element	CIE Document Section
1.1	Cyber Security Culture	3.1.2.9
1.2	Cyber Security Culture	3.1.2.9
1.3	Engineering Information Control	3.1.2.6
1.4	Engineering Information Control	3.1.2.6
2.1	Cyber Security Culture	3.1.2.9
2.2	Systems Architecture	3.1.2.2
2.3	Consequence/Impact Analysis	3.1.2.6
2.4	Systems Architecture	3.1.2.2
2.5	Engineered Controls	3.1.2.3
2.6	Design Simplification	3.1.2.4
2.7	Cyber Security Culture	3.1.2.9
3.1	Engineered Controls	3.1.2.3
3.2	Engineered Controls	3.1.2.3
3.3	Resilience Planning	3.1.2.5
3.4	Procurement and Contracting	3.1.2.7
4.1	Engineered Controls	3.1.2.3
4.2	Systems Architecture	3.1.2.2
4.3	Active Defense	3.1.2.11
4.4	Active Defense	3.1.2.11
4.5	Interdependencies	3.1.2.8
4.6	Resilience Planning	3.1.2.5
5.1	Active Defense	3.1.2.11
5.2	Active Defense	3.1.2.11
5.3	Consequence/impact Analysis	3.1.2.6
5.4	Resilience Planning	3.1.2.5
6.1	Procurement and Contracting	3.1.2.7
6.2	Procurement and Contracting	3.1.2.7
6.3	Procurement and Contracting/Design Simplification	3.1.2.7/3.1.2.4
6.4	Digital Asset Inventory	3.1.2.10
7.1	Digital Asset Inventory	3.1.2.10
7.2	Interdependencies	3.1.2.8
8.1	Design Simplification/Resilience Planning	3.1.2.4/3.1.2.5
8.2	Active Defense	3.1.2.11
8.3	Procurement and Contracting	3.1.2.7
9.1	Digital Asset Inventory	3.1.2.10
9.2	Active Defense	3.1.2.11
9.3	Cyber Security Culture	3.1.2.9
10.1	Engineering Information Control	3.1.2.6

Assessment Methodology

Purpose

The purpose of this methodology is to assess the level of integration of CIE framework elements, determine strengths and weaknesses of the framework elements, ascertain any high-value changes to the engineering design process, and identify any new elements that should be added to the framework.

Facility Data Gathering

Complete the Data Gathering Questionnaire. This document is used to familiarize the assessor with the programs and processes in place within the facility.

CIE Framework Integration

Complete the Framework Integration Assessment using information obtain in the Facility Data Gathering Questionnaire. Compare and contrast the information obtained with the Cybersecurity Checklist and determine the level of integration of the framework elements.

CIE Assessment Report

Complete the CIE Assessment Report. Document any strengths, weaknesses, high-value changes, or new elements. Determine the assessment score by tabulating the sum of the points in the Framework Integration Assessment.

Data Gathering Questionnaire

Name _____ Date _____

Complete the following 13 questions. Be sure to include as much detail as possible and sources where applicable.

1. Describe how is information such as data network, and/or ICS network, and/or DMZ schematic connection diagrams are protected, include at point in the design process does this information become protected.

2. Describe how resiliency is achieved for network segmentation devices. Include the level of diversity of the network and or boundary devices.

3. Describe the collaboration of team members involved in the network segmentation design (i.e., IT, ICS, CSAT, Engineering, and Cyber Security).

4. Describe the aspects of the cyber security training for employees and contractors? Include whether it covers social engineering, phishing, dumpster diving, portable media usage and whether they have job or organizational specific cyber training.

5. Describe how software is deemed "trustworthy." Include processes and/or programs in place that ensure software integrity.

6. Describe how the computers, test/simulation equipment, and portable media and mobile devices protected from undesired malware.

7. Document whether simulations or testing being done behind a properly protected environment.

8. Describe how threats from malicious insiders or accidental insiders mitigated.

9. Describe the asset inventory program. Include whether it documents the including hardware, software, and firmware versions of assets.

10. Describe how updates distributed to isolated or critical systems.

11. Document the frequency at which passwords are changed. Include whether it is consistent with NEI 08-09 D-4.3. If alternate frequencies are used include the justification.

12. Describe how rogue wireless detection as described in NEI 08-09 D-1.17 is performed. Include the frequency. If alternate frequencies are used, include the justification.

13. Describe what happens to digital equipment when it is decommissioned. Include whether equipment is sanitized by cybersecurity personnel to remove sensitive information.

Framework Integration Assessment

Review Information

Your Name: [Your Name]

Date: _____ Review Period: [Date] to [Date]

Guidelines

Complete this review, using the following scale:

1 = Not Applicable
2 = Principle not integrated in life-cycle phase.
3 = Principle partially present, but no plans to further integrate
4 = Principle partially present, documented plans for further integration
5 = Principle integrated in life cycle

Conceptual Design

	5	4	3	2	1 (N/A)
Consequence and Impact Analysis	☐	☐	☐	☐	☐
Systems Architecture	☐	☐	☐	☐	☐
Design Simplification	☐	☐	☐	☐	☐
Engineering Information Control	☐	☐	☐	☐	☐
Cyber Culture	☐	☐	☐	☐	☐
Interdependencies	☐	☐	☐	☐	☐
Resilience Planning	☐	☐	☐	☐	☐
Procurement and Contracting	☐	☐	☐	☐	☐
Digital Asset Inventory	☐	☐	☐	☐	☐
Engineered Controls	☐	☐	☐	☐	☐
Active Defense	☐	☐	☐	☐	☐

Requirements / Schematics

	5	4	3	2	1 (N/A)
Consequence and Impact Analysis	☐	☐	☐	☐	☐
Systems Architecture	☐	☐	☐	☐	☐
Design Simplification	☐	☐	☐	☐	☐
Engineering Information Control	☐	☐	☐	☐	☐
Cyber Culture	☐	☐	☐	☐	☐
Interdependencies	☐	☐	☐	☐	☐
Resilience Planning	☐	☐	☐	☐	☐
Procurement and Contracting	☐	☐	☐	☐	☐
Digital Asset Inventory	☐	☐	☐	☐	☐
Engineered Controls	☐	☐	☐	☐	☐
Active Defense	☐	☐	☐	☐	☐

Design Development	5	4	3	2	1 (N/A)
Consequence and Impact Analysis	☐	☐	☐	☐	☐
Systems Architecture	☐	☐	☐	☐	☐
Design Simplification	☐	☐	☐	☐	☐
Engineering Information Control	☐	☐	☐	☐	☐
Cyber Culture	☐	☐	☐	☐	☐
Interdependencies	☐	☐	☐	☐	☐
Resilience Planning	☐	☐	☐	☐	☐
Procurement and Contracting	☐	☐	☐	☐	☐
Digital Asset Inventory	☐	☐	☐	☐	☐
Engineered Controls	☐	☐	☐	☐	☐
Active Defense	☐	☐	☐	☐	☐

Computer Simulation	5	4	3	2	1 (N/A)
Consequence and Impact Analysis	☐	☐	☐	☐	☐
Systems Architecture	☐	☐	☐	☐	☐
Design Simplification	☐	☐	☐	☐	☐
Engineering Information Control	☐	☐	☐	☐	☐
Cyber Culture	☐	☐	☐	☐	☐
Interdependencies	☐	☐	☐	☐	☐
Resilience Planning	☐	☐	☐	☐	☐
Procurement and Contracting	☐	☐	☐	☐	☐
Digital Asset Inventory	☐	☐	☐	☐	☐
Engineered Controls	☐	☐	☐	☐	☐
Active Defense	☐	☐	☐	☐	☐

Procurement	5	4	3	2	1 (N/A)
Consequence and Impact Analysis	☐	☐	☐	☐	☐
Systems Architecture	☐	☐	☐	☐	☐
Design Simplification	☐	☐	☐	☐	☐
Engineering Information Control	☐	☐	☐	☐	☐
Cyber Culture	☐	☐	☐	☐	☐
Interdependencies	☐	☐	☐	☐	☐
Resilience Planning	☐	☐	☐	☐	☐
Procurement and Contracting	☐	☐	☐	☐	☐
Digital Asset Inventory	☐	☐	☐	☐	☐
Engineered Controls	☐	☐	☐	☐	☐
Active Defense	☐	☐	☐	☐	☐

Construction / Implementation / Integration	5	4	3	2	1 (N/A)
Consequence and Impact Analysis	☐	☐	☐	☐	☐
Systems Architecture	☐	☐	☐	☐	☐
Design Simplification	☐	☐	☐	☐	☐
Engineering Information Control	☐	☐	☐	☐	☐
Cyber Culture	☐	☐	☐	☐	☐
Interdependencies	☐	☐	☐	☐	☐
Resilience Planning	☐	☐	☐	☐	☐
Procurement and Contracting	☐	☐	☐	☐	☐
Digital Asset Inventory	☐	☐	☐	☐	☐
Engineered Controls	☐	☐	☐	☐	☐
Active Defense	☐	☐	☐	☐	☐

Testing	5	4	3	2	1 (N/A)
Consequence and Impact Analysis	☐	☐	☐	☐	☐
Systems Architecture	☐	☐	☐	☐	☐
Design Simplification	☐	☐	☐	☐	☐
Engineering Information Control	☐	☐	☐	☐	☐
Cyber Culture	☐	☐	☐	☐	☐
Interdependencies	☐	☐	☐	☐	☐
Resilience Planning	☐	☐	☐	☐	☐
Procurement and Contracting	☐	☐	☐	☐	☐
Digital Asset Inventory	☐	☐	☐	☐	☐
Engineered Controls	☐	☐	☐	☐	☐
Active Defense	☐	☐	☐	☐	☐

Post Construction	5	4	3	2	1 (N/A)
Consequence and Impact Analysis	☐	☐	☐	☐	☐
Systems Architecture	☐	☐	☐	☐	☐
Design Simplification	☐	☐	☐	☐	☐
Engineering Information Control	☐	☐	☐	☐	☐
Cyber Culture	☐	☐	☐	☐	☐
Interdependencies	☐	☐	☐	☐	☐
Resilience Planning	☐	☐	☐	☐	☐
Procurement and Contracting	☐	☐	☐	☐	☐
Digital Asset Inventory	☐	☐	☐	☐	☐
Engineered Controls	☐	☐	☐	☐	☐
Active Defense	☐	☐	☐	☐	☐

Operations & Maintenance					
	5	4	3	2	1 (N/A)
Consequence and Impact Analysis	☐	☐	☐	☐	☐
Systems Architecture	☐	☐	☐	☐	☐
Design Simplification	☐	☐	☐	☐	☐
Engineering Information Control	☐	☐	☐	☐	☐
Cyber Culture	☐	☐	☐	☐	☐
Interdependencies	☐	☐	☐	☐	☐
Resilience Planning	☐	☐	☐	☐	☐
Procurement and Contracting	☐	☐	☐	☐	☐
Digital Asset Inventory	☐	☐	☐	☐	☐
Engineered Controls	☐	☐	☐	☐	☐
Active Defense	☐	☐	☐	☐	☐

Decommissioning					
	5	4	3	2	1 (N/A)
Consequence and Impact Analysis	☐	☐	☐	☐	☐
Systems Architecture	☐	☐	☐	☐	☐
Design Simplification	☐	☐	☐	☐	☐
Engineering Information Control	☐	☐	☐	☐	☐
Cyber Culture	☐	☐	☐	☐	☐
Interdependencies	☐	☐	☐	☐	☐
Resilience Planning	☐	☐	☐	☐	☐
Procurement and Contracting	☐	☐	☐	☐	☐
Digital Asset Inventory	☐	☐	☐	☐	☐
Engineered Controls	☐	☐	☐	☐	☐
Active Defense	☐	☐	☐	☐	☐

CIE Assessment Report

Report Information

Facility _____ Assessor _____

Start Date _____ Assessment Score _____

Strengths

Notes	Framework Element	Life-cycle Phase(s)

Weaknesses

Notes	Framework Element	Life-cycle Phase(s)

High-Value Changes Identified

New Framework Elements