Cyber-Informed Engineering

Cyber-Informed Engineering Requirements Framework Use Cases

Authors:

Sriharsha Etigowni and Richard Macwan

National Laboratory of the Rockies

May 2026
NLR/TP-5T00-97232

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

DISCLAIMER

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

Contents

Executive Summary **2**

Acknowledgments 3

1. Introduction **5**

2. BESS Use Case **8**

2.1. BESS Requirement Specifications From RFP 8

2.2. Cyber-Informed Engineering Requirement Validation 11

2.3. Cyber-Informed Engineering Requirement Elicitation 14

2.4. Cyber-Informed Engineering Requirement Scoping and Deconflicting 17

2.5. Cyber-Informed Engineering Requirement Specification 24

2.6. Cyber-Informed Engineering Requirement Management 29

3. SCADA Improvement Use Case **29**

3.1. SCADA Improvement Program Requirements From Engineering Diagrams 31

3.2. Cyber-Informed Engineering Requirement Validation 34

3.3. Cyber-Informed Engineering Requirement Elicitation 38

3.4. Cyber-Informed Engineering Requirement Scoping and Deconflicting 42

3.5. Cyber-Informed Engineering Requirement Specification 54

3.6. Cyber-Informed Engineering Requirement Management 58

4. Conclusion **59**

References **59**

Executive Summary

The increasing digitalization of critical infrastructure introduces new cyber-physical vulnerabilities that can compromise the safety, reliability, and operational integrity of engineered systems. Traditional cybersecurity approaches often focus on protecting digital assets through software, network, or procedural defenses but frequently overlook how engineering design decisions can inherently reduce or amplify cyber consequences. Cyber-informed engineering (CIE) addresses this gap by embedding cybersecurity awareness directly into the engineering process, emphasizing consequence-focused design and system-level resilience. However, the practical application of CIE principles in real engineering workflows remains underdeveloped, limiting its impact on infrastructure modernization projects.

This paper aims to operationalize the CIE concept through the application of a structured CIE requirements framework with two representative use cases: a battery energy storage system (BESS) and a supervisory control and data acquisition (SCADA) improvement program within a public water utility. The objective is to demonstrate how CIE can be integrated into the requirements development phase of engineering projects to proactively identify, prioritize, and mitigate cyber-physical risks before system deployment. The approach leverages a structured, repeatable framework for classifying and prioritizing functional and nonfunctional requirements based on digital impact, categorized as direct, indirect, or no digital impact. The framework was applied across each system's engineering life cycle, including requirement elicitation, scoping and deconfliction, specification, validation, and management.

The application of the framework yielded several key results. For the BESS use case, CIE principles guided the identification of high-impact digital pathways, enabling the development of engineering requirements that reduce dependency on vulnerable digital controls and enhance system resilience under cyber-compromised conditions. For the SCADA improvement program, the framework facilitated the identification of CIE-driven design enhancements for instrumentation and control subsystems such as disinfectant residual analyzers, chemical dosing pumps, and ultrasonic-level transmitters—focusing on secure control logic, data validation, and consequence isolation. Across both cases, the results demonstrated systematically integrating CIE during the requirements phase leads to improved visibility of cyber-physical dependencies, clearer prioritization of protective design actions, and enhanced alignment between cybersecurity objectives and operational performance goals.

The findings confirm the CIE requirements framework provides a practical pathway for embedding cyber resilience into traditional engineering workflows without introducing complexity or conflicting with performance requirements. By integrating consequence-focused analysis with structured requirement management, this approach ensures cybersecurity becomes an inherent aspect of engineering design rather than an external layer of protection. The paper concludes applying CIE principles early in the system life cycle can materially reduce digital consequence exposure, strengthen system reliability, and inform future modernization efforts across diverse critical infrastructure sectors.

Acknowledgments

This work was authored by the National Laboratory of the Rockies, operated by Alliance for Energy Innovation LLC, for the U.S. Department of Energy under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

List of Tables

Table 1: BESS specifications from RFP 9
Table 2: Classification of existing requirements 18
Table 3: CIE principles alignment scoring 21
Table 4: CIE alignment scoring justification 22
Table 5: Refined and new requirement specification 26
Table 6: SCADA improvement specifications from construction drawings and electrical diagrams 31
Table 7: Classification of existing requirements 44
Table 8: CIE principles alignment scoring 47
Table 9: CIE alignment scoring justification 50
Table 10: Refined and new requirement specification 54

List of Figures

Figure 1: Requirements framework for CIE 7
Figure 2: Requirements framework for CIE 30

1. Introduction

The convergence of operational technology (OT) and information technology (IT) has transformed how modern critical infrastructures are designed, operated, and secured. As these systems become increasingly digitalized, their exposure to cyber-enabled disruptions grows, introducing new vulnerabilities that can lead to real-world physical consequences. Traditional cybersecurity approaches, which often focus on software or network defenses, are insufficient to address these challenges at the engineering level. Cyber-informed engineering (CIE) bridges this gap by embedding cybersecurity awareness and consequence-focused design thinking directly into the engineering life cycle.

CIE integrates cybersecurity considerations directly into the conception, design, development, and operation of cyber-physical systems, particularly critical infrastructure such as energy systems [1]. Its objective is to mitigate or eliminate cyber-enabled attack risks by embedding cybersecurity—a foundational element in engineering decisions and controls—from the earliest stages of a system's life cycle [2]. This approach enables engineers to "engineer out" cyber risks during the initial design phases, achieving greater security and cost efficiency than adding protections later.

CIE expands traditional engineering practices to include defense against digital consequences by equipping engineers to understand and address cyber risks as part of their core responsibilities. It applies engineering tools and controls to protect critical infrastructure prioritizing the most severe threats that could lead to physical damage or operational disruption. CIE is founded on a set of core engineering and cybersecurity principles that promote shared standards, educational initiatives, and collaboration between engineering and cybersecurity disciplines. By integrating these principles, CIE enables the design of critical infrastructure systems that are inherently resilient to cyber threats through holistic and multidisciplinary engineering approaches, moving beyond reliance on traditional IT-based cybersecurity measures.

To introduce CIE at the earlier stages of the system engineering life cycle, a requirements framework for CIE was developed: *Requirements Framework for Cyber-Informed Engineering*.[1] The requirements framework for CIE [3] embeds CIE principles within the traditional engineering requirements life cycle, ensuring security is treated as a foundational element across system design, operations, and maintenance. Specifically, the framework adapts the conventional requirements process to focus on consequence-focused design, the integration of engineering mitigations, and the alignment of cybersecurity measures with critical system functions.

Rather than creating a new requirements methodology, the CIE framework complements existing systems engineering processes by embedding CIE considerations early and continuously. It also emphasizes collaboration among engineers, cybersecurity experts, and other stakeholders to ensure a holistic and resilient security posture. Through this approach, CIE promotes a proactive, security-centric mindset that ensures cybersecurity is systematically addressed not as an afterthought but as an integral component of each phase of system development. Ultimately, this

[1] https://www.osti.gov/servlets/purl/2497726

framework enables organizations to design, specify, and validate resilient systems that maintain operational trustworthiness and mission assurance in the face of evolving cyber threats.

The key components of the CIE requirements framework are shown in Figure 1 and are as follows:

1) **Requirement Elicitation:** Focuses on identifying and documenting cybersecurity-related needs and concerns along with system requirements from all stakeholders through methods such as interviews, document reviews, and operational analysis. This ensures engineering protections, digital safeguards, and defensive design features are recognized early in system development .
2) **Requirement Scoping and Deconfliction:** Assesses, categorizes, and prioritizes requirements, distinguishing between functional (direct system operations) and nonfunctional (e.g., resilience, integrity, culture) cybersecurity requirements. This phase also classifies each requirement based on its digital impact—direct, indirect, or no digital impact—to guide the appropriate application of CIE principles.
    a) **Direct digital** impact refers to systems or components that can be directly influenced by cyber compromise or digital manipulation, such as the battery management system (BMS) in a battery energy storage system (BESS), where digital control directly affects operational safety and performance.
    b) **Indirect digital** impact refers to systems that may be affected through interdependence or secondary cyber effects, where a cyber incident in one subsystem indirectly impacts another. For example, a cyberattack on the cooling system could cause improper thermal regulation, which in turn degrades the overall performance, efficiency, or safety of the BESS—even though the compromised subsystem is not the primary control system.
    c) **No digital** impact includes components or requirements that have no cyber interface or digital dependency, such as the physical dimensions or weight of a BESS enclosure.

    This classification helps engineers focus their attention where it matters most by applying CIE-driven mitigations proportionally to functions with the highest potential for digital consequences while maintaining alignment with system performance, safety, and operational objectives.
3) **Requirement Specification:** Defines requirements with precision, ensuring they are clear, measurable, and verifiable. Requirement modeling is used to represent and validate both system behaviors and cybersecurity interactions, improving traceability and reducing ambiguity in requirement interpretation.
4) **Requirement Validation:** Conducts formal reviews, prototype evaluations, and model checking to confirm all requirements are implementable, testable, and aligned with CIE principles. Each requirement is accompanied by a validation plan specifying how the corresponding security objectives will be evaluated and verified.
5) **Requirement Management:** Provides ongoing governance of requirements throughout the system life cycle. This includes change tracking, threat reassessment, and continuous alignment with cybersecurity and operational resilience goals as system conditions, technologies, and threat environments evolve.

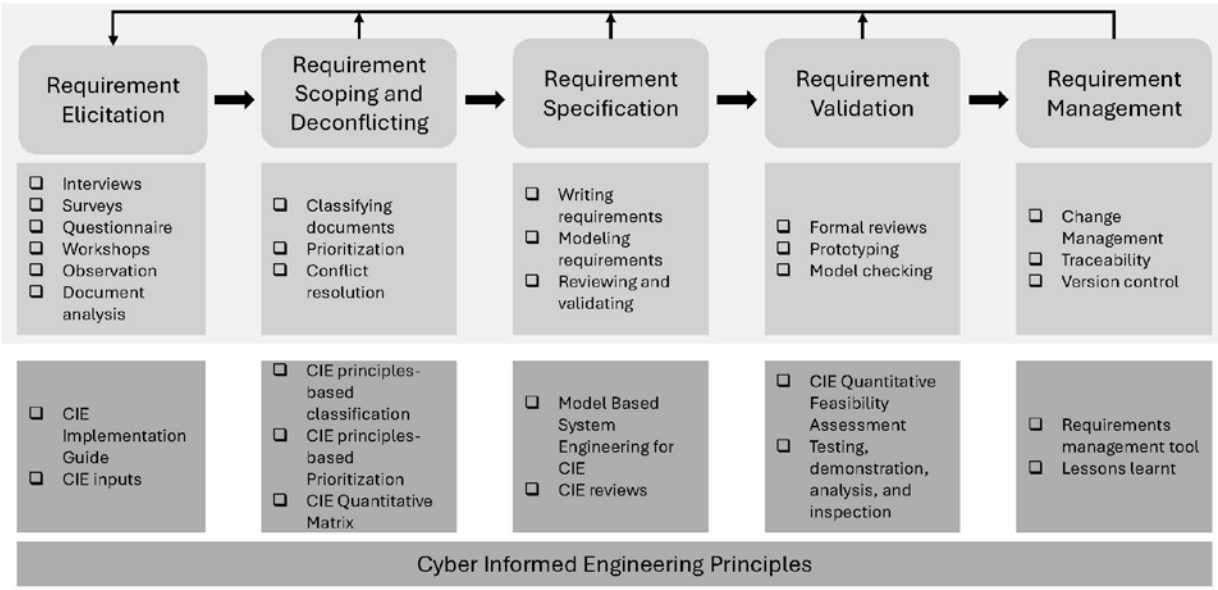

Figure 1: Requirements framework for CIE

Despite significant progress in cybersecurity and industrial control system protection, there remains a fundamental disconnect between cybersecurity strategies and engineering design practices. Many system specifications, procurement documents, and modernization projects fail to account for cyber-physical dependencies and digital consequence pathways during early design stages. The lack of structured methods to integrate CIE principles into requirements development contributes to this gap. This paper addresses this shortfall by applying the CIE Requirements Framework with two distinct yet representative use cases, BESS and a supervisory control and data acquisition (SCADA) improvement program, to demonstrate how CIE can systematically enhance system resilience through consequence-focused engineering decisions.

The methodology adopted in this paper leverages the CIE Requirements Framework developed in prior research, which defines a structured process for eliciting, analyzing, and prioritizing engineering requirements that account for digital consequences. This framework is applied across the system engineering life cycle with two real-world contexts. The framework is used to identify CIE-driven requirements for BESS and SCADA use cases. Each use case follows the steps of requirement validation of the existing requirements, requirement elicitation for the gaps found in the validation, scoping and deconfliction, specification, and management—demonstrating how CIE principles can be operationalized in engineering practice.

The objective of this paper is to demonstrate how the CIE Requirements Framework can be effectively applied to improve the security and resilience of critical infrastructure systems by aligning cybersecurity considerations with core engineering processes. Through the application of CIE to real-world use cases in BESS and SCADA systems, this work illustrates how engineering-based mitigations can minimize or eliminate digital consequences that lead to operational disruptions. Ultimately, this paper seeks to show CIE does not replace existing engineering methodologies but rather enhances them, enabling engineers to systematically integrate security, resilience, and consequence awareness into every phase of design, implementation, and operation.

Chapter 2 is a case study on battery energy storage systems. The requirements for this use case are provided, and the steps in the requirements framework are examined to illustrate how the framework could have helped better define the requirements. Chapter 3 presents another use case on the SCADA improvement program. Chapter 4 concludes this paper.

2. BESS Use Case

The BESS use case examined in this study is based on a real-world deployment initiated through a request for proposals (RFP) process at the National Laboratory of the Rockies (NLR). The RFP serves as a formal solicitation mechanism through which a project owner defines technical specifications, performance criteria, and compliance requirements, inviting qualified vendors or system integrators to submit proposals. The selected vendor is then responsible for the design, engineering, procurement, and commissioning of the BESS in accordance with these specifications.

However, although the RFP process ensures conformance to performance, safety, and interoperability standards, it traditionally lacks structured guidance for embedding CIE principles during requirements development. As a result, cybersecurity often remains a secondary consideration, introduced later in the system life cycle rather than being engineered into the foundational design. This use case provides a representative scenario to evaluate how the CIE Requirements Framework can augment existing RFP-based engineering processes to produce a more secure, resilient, and cyber-aware BESS deployment.

The requirements framework (as shown in Figure 1) starts with requirement elicitation followed by requirement scoping and deconflicting, requirement specifications, requirement validation, and then requirement management. Because the RFP specifies all the requirements for BESS, the following use case will start with a review of these specifications in Section 2.1, corresponding to the middle box in Figure 1. Section 2.2 will then proceed to validation (moving to the right in Figure 1); once the validation shows the RFP is not well aligned with the CIE principles, the use case will jump back to the requirement elicitations in Section 2.3 (the leftmost box in Figure 1), followed by requirement scoping and deconflicting in Section 2.4, followed by requirement specification (again) in Section 2.5. Once the requirement specifications are aligned with CIE principles, Section 2.6 incorporates those into requirement management (the rightmost box in Figure 1).

2.1. BESS Requirement Specifications From RFP

The specifications required for the BESS at NLR were released through an RFP as shown in Table 1. These specifications define the capacity, functioning ability, losses, reliability, fault performance, and digital connection required for the BESS system.

Table 1: BESS specifications from RFP

Item	Specification
General (Note: All ratings for the altitude of 1,800 meters)	
Max continuous active power	±1 megawatts (MW) at 100% state of energy (SoE) ±700 kilowatts (kW) at 10% SoE ±400 kW at 0% SoE
Max continuous reactive power	±1 megavolt ampere reactive (MVAR; 1.25 MVAR for 10 s)
Max peak active power	±1.25 MW for 10 s at 100% SoE ±1.1 MW for 30 s at 100% SoE
Installed energy capacity	1 megawatt-hour (MWh; at 1C discharge rate)
Usable energy capacity	1 MWh
Deep discharge	Deep discharge (0%) capable; ±500 kW at 0% SoE for 10 s with cooling period of no longer than 10 min; max number of deep discharge events: no more than 24 times per year
Round-trip energy efficiency	Above 85%
Power converter efficiency	95% or higher for all power levels above 30%
Energy to power ratio (E2P)	1
Power quality	IEEE 519 compliant; current total demand distortion in grid-connected mode: less than 5% at full load; voltage total harmonic distortion (THD) in grid-forming mode: less than 5% (including 100th harmonic order, measured on line-to-line voltage)
Dynamic Requirements	
Max ramp rate	-1 MW to +1 MW in 1 s (symmetric) or faster -1 MVAR to +1 MVAR in 1 s (symmetric) or faster
Response time in normal operation	No longer than 50 ms
Response time in standby	No longer than 500 ms
Turn-on time	No longer than 1 s
Frequency droop	Operation with symmetric and nonsymmetric frequency droop characteristic (droop can be set in 3%–5% range)
Voltage droop	Operation with voltage droop characteristic
Duty cycle eccentricity (DCE)	2–2.5 (defined as standard deviation divided by the average value of the charging/discharging current)
Response time in grid-forming mode	50 ms or faster to return to nominal voltage (within ±1% accuracy) after 50% load change
Losses	
Self-discharge	No larger than 0.5%/day in standby mode
Standby losses	No larger than 1% of rate power

Reliability and Availability	
Cycle lifetime	At least 40,000 cycles with 80% remaining capacity (for 20%–90% depth of discharge (DOD) range)
Mean time between failures	5 years
Environmental and cooling	
External temperature range	-40 to +40°C
Cooling	Forced air or closed-loop liquid
Enclosure	ISO-type container, durable construction for extended life
Enclosure internal operating temperature	0–40°C
Ambient operating relative humidity	5%–95%
Elevation	1,800 m (6,000 ft)
Contaminants	Dirt, dust, and airborne pollutants typical of an industrial environment
Weight	The existing pads can withstand 400,000 pounds of distributed mass
Physical size	Drawings shall be submitted by subcontractor
Grid connection	
Power converter	Can operate as current and voltage source (capable of grid forming)
Site voltage	13.2 kV nominal, ±10% deviations
Frequency	60 Hz nominal, ±1 Hz deviations
Voltage imbalance	No more than 3% (ratio between negative and positive sequence voltage)
Background harmonics	Should be able to operate on NRL's simulated grid (background simulated grid voltage THD is no higher than 3.5%); regular grid connection normally has THD less than 2%
Grid forming	Voltage regulation: ±1% of nominals, frequency ±0.1% of nominal
Transition from grid-connected to grid-forming mode	Seamless
Transition from grid-forming to grid-connected mode	100 ms or faster
Fault performance	
Frequency excursion ride-through	58–62 Hz for 10 s
Short-circuit current	Programmable short-circuit current contribution for the range from 0 to largest possible current; programmable current vs. voltage depth droop characteristic
Anti-islanding protection	IEEE 1547 (possibility to turn off in voltage fault testing mode)

Automation	
Remote operation requirement	External connection interface to BESS SCADA from NLR control system is required (possible protocols: OPC, EtherCAT, Profibus, Modbus, Scramnet)
Two-way communication	Ability to provide internal state parameters (e.g., state of charge (SoC), state of energy (SoE), state of health (SoH), status flags, alarms, information from converters and battery management systems) to NLR controller and receive setpoints (e.g., start/stop commands, active/reactive power setpoints, operation modes) from NLR controller (1 kilohertz communication bandwidth)
Stand-alone operation	The system should be able to operate in stand-alone mode with no external control using the latest set of parameters entered by NLR
Alarm system	Sensor system for fire alarm, detection sensors for dangerous concentration of flammable and toxic gases, and temperature sensors
Safety and Manuals	
Spill protection	Spill protection for liquid electrochemical batteries
Manuals include	General, system component description including overview one-line for both power and communications connections, operation and control parameter documentation, safety, and maintenance and repair
Marking	Appropriate safety marking and instructions visibly attached on all appropriate components
Hazards	All technology-specific hazards must be identified and documented
Other safety	Door interlocks, touch-safe access to physical communications and programming interfaces as required to set up and maintain unit under normal operation

2.2. Cyber-Informed Engineering Requirement Validation

The validation of requirements in this use case is conducted through a structured review process [4]. The primary objective of this review is to evaluate the completeness, clarity, and relevance of each requirement. Within the context of CIE, the review emphasizes assessing how well the requirements align with key CIE principles ensuring cybersecurity is systematically integrated into the engineering process rather than treated as an external overlay [5]. During this process, each requirement is examined to verify that it accurately reflects security needs and that potential gaps are identified for remediation [6], [7], [8].

The RFP demonstrates strong coverage of electrical, performance, and safety engineering details, including specifications for power, dynamic response, environmental tolerance, and fault ride-through capabilities. However, the RFP is notably weak or silent on many CIE-centric elements—particularly those that connect design requirements to CIE principles. The following principle-by-principle evaluation summarizes the key findings from the review.

CONSEQUENCE-FOCUSED DESIGN

The RFP defines functional performance criteria such as power output, ramp rates, response times, and grid-forming or ride-through capabilities. Although these implicitly address some operational consequences such as loss of capacity or grid instability, there is no explicit mapping from high-consequence outcomes (e.g., uncontrolled deep discharge leading to thermal events

or inadvertent islanding with safety implications) to prioritized requirements that mitigate those risks. Moreover, the RFP does not distinguish or prioritize requirements based on consequence type (e.g., safety, regulatory, or commercial loss), which limits the ability to ensure high-impact events receive the strongest engineering safeguards.

ENGINEERED CONTROLS

The RFP includes numerous physical safety features, such as spill protection, fire detection, door interlocks, and enclosure environmental ratings. Cooling specifications and internal temperature ranges are also defined. However, explicit nondigital fail-safe mechanisms that operate independently of the battery management system or power conversion system (PCS) such as mechanical or analog overcurrent trips, independent thermal cutouts, or mechanical stops for charging are absent. The RFP allows deep discharge conditions but does not prescribe hardware-level constraints to prevent misuse if digital control systems are compromised. This absence weakens physical resilience under degraded digital conditions.

SECURE INFORMATION ARCHITECTURE

The automation section specifies communication protocols (OPC, EtherCAT, Modbus) and two-way data exchange with NLR at 1-kilohertz bandwidth. However, it lacks network zoning or segmentation, authentication, encryption, and protocol hardening measures. There are no constraints on remote vendor access, no requirements for demilitarized zones (DMZs) or jump hosts, and no specifications defining read-only versus write permissions. In addition, there are no requirements for secure time synchronization, replay protection, or secure key management. As written, the RFP defines communication but not communication security.

DESIGN SIMPLIFICATION

The RFP effectively specifies essential energy-to-power and power electronics performance criteria; however, it does not include requirements to minimize unnecessary complexity in control or human-machine interface (HMI) systems. There is also no mention of disabling unused services or interfaces on HMIs and engineering workstations to reduce the attack surface. The omission of such requirements increases the potential for latent vulnerabilities and operational uncertainty.

LAYERED DEFENSE

Although the RFP defines several physical and safety layers such as fire sensors, spill protection, and door interlocks, it does not establish multiple independent defensive layers for critical control functions. For example, there is no explicit requirement for redundant protection across BMS commands, physical breakers, and PCS watchdog functions. Likewise, no provisions exist for overlapping monitoring, such as using an independent analog temperature sensor to cross-check pack overtemperature conditions. The absence of such redundancy creates single points of failure that could allow undetected faults or malicious commands to propagate.

ACTIVE DEFENSE

The RFP includes alarm systems for fire and gas detection but lacks requirements in operator-executable active-defense actions that are physical and independent of networked control. These include a clearly identified manual safe-shutdown pathway that allows operators/technicians to quickly transition critical functions to a predefined safe condition during suspected abnormal control behavior. These include verifiable procedures and interfaces that enable human

intervention to contain consequences in real time (e.g., local isolation of specific subsystems, manual override to conservative setpoints, and confirmation indicators that the system has entered the intended safe state). Without these, the system's ability to detect, contain, and investigate cyber incidents is severely limited.

INTERDEPENDENCY EVALUATION

The RFP provides detailed specifications for subsystems including the converter, BMS, cooling system, and enclosure and outlines their interfaces to the grid and NLR's SCADA environment. However, it does not include explicit mapping of subsystem interdependencies, such as how BMS, TMS (thermal management system), and PCS interactions might influence power-plant-level outcomes. Furthermore, there are no requirements for cross-verification among subsystems (e.g., requiring the PCS to validate the BMS-reported state of charge for consistency). Without such mapping, the potential for cascading or unintended consequences across subsystems remains unaddressed.

DIGITAL ASSET AWARENESS

Although the RFP requests engineering drawings, it does not include a requirement for a digital asset inventory or configuration baseline. There is no mandate for maintaining an asset register (hardware, firmware, software versions, and serial numbers), a software bill of materials (SBOM), or a defined process to track firmware updates and patch states. This gap limits life cycle cybersecurity management and situational awareness for maintenance and response.

CYBER-SECURE SUPPLY CHAIN CONTROLS

Although the RFP implicitly references manufacturer identification and component labeling through technical drawings and specifications, it lacks explicit procurement-level cybersecurity requirements. There are no provisions for firmware signing, vendor vetting, origin assurance, vulnerability disclosure obligations, or update cadence requirements. The absence of these measures weakens supply chain integrity and reduces the traceability of components critical to safe operation.

PLANNED RESILIENCE

The RFP specifies requirements for stand-alone and remote operation, and it defines some degraded behaviors (e.g., stand-alone mode using the latest stored parameters). However, it omits explicit degraded modes for suspected cyber compromise such as safe default setpoints, reduced ramp rates, or limited charge/discharge conditions and lacks a recovery procedure for compromised firmware. As a result, operational resilience under adversarial or uncertain digital conditions remains underdefined.

ENGINEERING INFORMATION CONTROL

Although the RFP mandates the provision of manuals and drawings, it lacks controls governing the distribution of sensitive design information such as network diagrams, firmware, and programmable logic controller (PLC) logic. There is no requirement for controlled access, nondisclosure agreements (NDAs), or data classification for engineering artifacts. Unrestricted information sharing of this nature increases the risk of sensitive design exposure to unauthorized parties.

ORGANIZATIONAL CULTURE

The RFP includes general expectations for operations and maintenance but does not establish requirements for cybersecurity training, incident response planning, vendor support protocols, or defined roles and responsibilities during cyber events. Without clear organizational and procedural integration of cybersecurity, even well-engineered systems may remain operationally vulnerable [9].

2.3. Cyber-Informed Engineering Requirement Elicitation

The CIE requirement validation process identified that the reviewed specifications were not fully aligned with CIE principles. Several requirements could be refined or expanded to better reflect consequence-focused, engineering-driven cybersecurity practices. To address these gaps, a systematic requirement elicitation process was conducted.

The elicitation process extends beyond validation to actively uncover missing or insufficient cybersecurity requirements within the RFP specifications. By applying each principle of cyber-informed engineering, the elicitation identifies gaps, formulates guiding questions, and ensures engineering, operational, and cybersecurity considerations are aligned throughout the system's life cycle. The following subsections describe the principle-by-principle elicitation process used for the BESS deployment.

CONSEQUENCE-FOCUSED DESIGN

The elicitation process begins by identifying the system's most critical outcomes [10], [11], [12]. Engineers and system owners are prompted to define high-consequence events by asking, "*What are the unacceptable end states safety—environmental, regulatory, service continuity, or reputational—if BESS subsystems fail or are manipulated?*" Once these end states are established, each potential failure is mapped to its corresponding consequence through the prompt, "*For each high consequence, what failure modes, both digital and physical, could lead to it?*" To quantify the severity and business impact of these consequences, the discussion extends to, "*What business or mission metrics (e.g., injuries, downtime hours, regulatory fines, lost capacity in MW) best capture the consequence magnitude?*" Supporting data such as incident history, regulatory limits, operational thresholds (e.g., temperature or state-of-charge limits), and emergency response procedures are collected to ensure consequence evaluation is grounded in measurable and operationally relevant terms.

ENGINEERED CONTROLS

The elicitation focuses on reinforcing the physical layer of defense by identifying independent, hardware-based protections. Design engineers are prompted to consider, "*What hardware, analog, or mechanical protections exist that act independently of BMS or PCS control logic (e.g., hardware breakers, thermal cutouts, analog current sensors)?*" In addition, the elicitation explores failure scenarios through questions such as, "*How do these devices behave when the controller is offline or compromised?*" and "*What are the allowable thermal and current envelopes before mechanical trips are required?*" This line of inquiry ensures physical safeguards retain their effectiveness even when digital control functions are degraded or unavailable.

SECURE INFORMATION ARCHITECTURE

This elicitation emphasizes the need for robust and clearly defined communication and data flow architectures. IT and OT architects are asked, "*What is the intended zone-and-conduit architecture, and who will have read/write rights to which data tags?*" Procurement teams are further prompted to clarify, "*What are the access rules for vendor remote maintenance, jump hosts, and external support connections?*" From a cybersecurity standpoint, the discussion centers on "*Which communication protocols are required, and what secure variants are supported (e.g., OPC UA, TLS, or certificate-based authentication)?*" These questions aim to ensure system connectivity is both functional and defensible against unauthorized access or data compromise [13].

DESIGN SIMPLIFICATION

The elicitation under this principle aims to reduce unnecessary complexity that could introduce hidden vulnerabilities. System integrators are prompted to evaluate, "*What optional services, ports, or web interfaces are enabled by default on delivered devices?*" Operational personnel are then asked, "*Which HMI or diagnostic features are essential for operations versus those that serve only as convenience functions?*" From a security perspective, we consider, "*Can any control device be delivered with a pre-hardened image to minimize configuration exposure?*" These prompts help eliminate digital excess, simplify system configurations, and enhance the overall resilience of the deployed BESS system.

LAYERED DEFENSE

This elicitation promotes redundancy and independence across protective mechanisms. Engineering and operations teams are encouraged to document multiple layers of defense by answering, "*For each critical function, what two or more independent controls—physical and digital—are in place to prevent unacceptable outcomes?*" Designers are further asked, "*Are duplicate sensors or relays of different technologies implemented for critical detections?*" Through these structured questions, the process ensures each essential function is protected by multiple, diverse defense mechanisms that prevent single points of failure from escalating into high-consequence events

ACTIVE DEFENSE

The elicitation for active defense focuses on ensuring continuous monitoring, detection, and response readiness. Security and Security Information and Event Management (SIEM) administrators are asked, "*What telemetry and logs must be exported, where are they retained, and who is responsible for responding to detections?*" Vendors are also prompted with, "*Can the BMS or PCS log all setpoint changes, firmware updates, and remote access sessions and export tamper-evident logs?*" This structured inquiry ensures visibility across operational layers and supports the rapid identification of anomalies or unauthorized activities within the system.

INTERDEPENDENCY EVALUATION

Interdependency evaluation seeks to map and understand how failures can propagate across subsystems. System engineers are prompted to create interdependency diagrams through questions such as, "*How do BMS, PCS, TMS, cooling, fire suppression, and grid interfaces interact, and where can a fault propagate between them?*" Operations teams are then asked,

"*What manual overrides or cross-checks exist across subsystems to prevent cascading failures?*" This approach enables engineers to visualize systemic coupling and ensures protective measures account for both direct and indirect digital impacts across interconnected systems.

DIGITAL ASSET AWARENESS

This elicitation emphasizes maintaining a complete and up-to-date inventory of digital assets. Asset managers are prompted with, "*Provide a full inventory including device type, model, serial number, firmware version, network address, and function. Who maintains this inventory, and how often is it updated?*" Procurement teams are asked to supply, "*Software Bills of Materials (SBOMs) and firmware component lists for all digital assets.*" These inquiries promote traceability and visibility across the BESS ecosystem, enabling faster identification of vulnerabilities, version mismatches, and supply-chain risks.

CYBER-SECURE SUPPLY CHAIN CONTROLS

The elicitation for this principle focuses on securing vendor and component provenance. Procurement and security teams are asked, "*What supply-chain attestations are required for components and firmware, and are firmware images digitally signed?*" Vendors are prompted to explain, "*What is your patch cadence, code-signing process, and vulnerability disclosure policy?*" These questions establish accountability and transparency throughout the supply chain, ensuring external dependencies do not introduce hidden cyber risks into the operational environment.

PLANNED RESILIENCE

Planned resilience elicitation ensures the system can maintain essential functions under degraded conditions. Operations personnel are prompted to define, "*What degraded operational modes are acceptable, such as reduced power output or conservative setpoints, and how are they invoked automatically or manually?*" Design engineers are then asked, "*Where are golden images and offline backups stored, and what are the defined recovery time and recovery point objectives?*" These discussions guide the establishment of clear recovery pathways, enabling the system to sustain operation or quickly recover after a disruption.

ENGINEERING INFORMATION CONTROL

The elicitation under this principle focuses on securing sensitive engineering information and documentation. Document owners are asked, "*Where are wiring diagrams, network schematics, PLC logic, and configuration files stored, and who has access permissions?*" Legal and compliance teams are prompted to consider, "*Are nondisclosure agreements and least-privilege controls enforced for all external contractors and vendors?*" These measures ensure critical design information is protected against unauthorized access, tampering, or unintentional exposure, reducing potential attack surfaces.

ORGANIZATIONAL CULTURE

The final elicitation principle addresses the human and procedural aspects of cybersecurity integration. Human resources and operations teams are asked, "*What training programs exist for operators and engineers on OT cybersecurity and incident response, and how frequently are they updated?*" Leadership is then prompted with, "*How are cyber roles, responsibilities, and budgets formally assigned and maintained within the organization?*" By establishing structured governance

and regular training, this principle ensures cybersecurity awareness and accountability become ingrained within the operational culture rather than treated as an afterthought [14].

2.4. Cyber-Informed Engineering Requirement Scoping and Deconflicting

Following the elicitation phase, where foundational system and cybersecurity requirements were gathered through structured interviews and scenario-based questions, the next step in the process is requirement scoping and deconflicting. This phase ensures the elicited requirements are correctly categorized, aligned with digital system impacts, and assessed against the 12 CIE principles to prioritize engineering efforts where they matter most.

The objective of this phase is twofold:

- To distinguish between functional and nonfunctional requirements, clarifying which directly influence system operation and which contribute to resilience, integrity, or organizational culture
- To evaluate each requirement's digital impact—whether direct, indirect, or none—so engineers can proportionally apply CIE mitigations to those system functions that present the highest cyber-physical consequence potential.

By classifying, scoring, and justifying each requirement's relationship to CIE principles, this phase bridges raw elicitation data with actionable specifications. It reveals where traditional cybersecurity measures may be insufficient and where engineered safeguards such as hardware interlocks, control independence, or system segmentation should be emphasized. The scoring also helps identify overlaps and conflicts between requirements, enabling harmonized implementation that supports both safety and secure operability.

To systematically apply this logic, three analytical outputs are presented in this section:

- Table 2 categorizes each specification as functional or nonfunctional and defines its digital impact (direct, indirect, or none), providing a foundational understanding of system exposure.
- Table 3 evaluates each requirement against the 12 CIE principles using a quantitative 1–5 scale, indicating the degree of alignment between the existing specification and CIE objectives.
- Table 4 explains the rationale behind each score, illustrating why certain requirements lack alignment and where engineering or procedural mitigations are needed.

This structured approach transforms the elicited requirements into a traceable, consequence-focused framework that sets the stage for formal specification and refinement in the next phase.

Table 2: Classification of existing requirements

Requirement	Type	Digital Impact	Description
Max continuous active/reactive power, max peak power	Functional	Direct	Defines operational energy delivery controlled by PCS and BMS logic, directly impacted by digital control manipulation
Installed and usable energy capacity	Functional	Direct	Energy storage control relies on BMS digital measurements and management algorithms
Deep discharge capability and limits	Functional	Direct	Controlled digitally through BMS and PCS; manipulation could lead to over-discharge or cell damage
Round-trip and converter efficiency	Functional	Direct	Efficiency governed by PCS control algorithms; cyber manipulation could alter operational efficiency or cause overload
Power quality (IEEE 519 compliance, total demand distortion, total harmonic distortion [THD])	Functional	Direct	Dependent on inverter control firmware and digital regulation loops, cyber tampering could degrade grid quality
Dynamic response parameters (ramp rate, response time, frequency/voltage droop)	Functional	Direct	Directly dependent on PCS and BMS digital control algorithms; manipulation could destabilize grid or equipment
Self-discharge and standby losses	Functional	Indirect	Influenced by control settings but largely governed by physical and chemical properties; minimal direct cyber exposure
Cycle lifetime and mean time between failure	Nonfunctional	Indirect	Reflects design durability and maintenance reliability; can be affected by cyber events altering charge/discharge cycles
Environmental operating conditions (temperature, humidity, elevation)	Nonfunctional	None	Defines physical survivability limits; not influenced by cyber manipulation

Cooling system requirements (forced air or liquid)	Functional	Indirect	Controlled through TMS, which interfaces with BMS; cyber compromise of BMS can cause improper cooling activation
Enclosure (ISO container, internal temperature limits, contaminants)	Nonfunctional	None	Physical property ensuring environmental protection; unaffected by cyber events
Weight and physical size	Nonfunctional	None	Structural attribute; has no cyber interface or dependency
Grid connection parameters (voltage, frequency, imbalance, THD)	Functional	Direct	Controlled through inverter and PCS firmware; direct cyber impact possible through control manipulation
Grid forming and transition (grid connected ↔ grid forming)	Functional	Direct	Managed entirely through PCS control logic; a compromised digital control could disrupt synchronization or stability
Voltage/frequency fault ride-through capabilities (LVRT, HVRT, ZVRT)	Functional	Direct	Implemented through digital protection algorithms in PCS; directly impacted by cyber manipulation
Short-circuit current programmability and droop control	Functional	Direct	Software-defined current limiting behavior in PCS; directly modifiable via cyber compromise
Anti-islanding protection	Functional	Direct	Digital control algorithm feature; disabling or altering could cause unsafe grid operation
Remote operation (e.g., SCADA interface, OPC, EtherCAT, Modbus)	Functional	Direct	Involves network connectivity and remote control; primary cyber exposure point and high-impact digital surface
Two-way communication (state, data and setpoints)	Functional	Direct	Continuous digital exchange between BESS and NLR controller; highly sensitive to cyber manipulation or spoofing
Stand-alone operation (using last parameters)	Functional	Direct	Depends on embedded control firmware logic; cyber compromise could alter default parameters or modes

Alarm system (fire, gas, temperature sensors)	Functional	Indirect	Relies on physical sensors but controlled and logged digitally; can be affected indirectly through communication or BMS failure
Spill protection for electrochemical batteries	Nonfunctional	None	Purely physical containment feature with no cyber interface
Manuals and documentation (operations, maintenance, communication)	Nonfunctional	Indirect	Supports operational integrity and training; cyber compromise could alter or corrupt maintenance instructions
Marking and labeling	Nonfunctional	None	Physical safety indicators; unaffected by cyber activity
Hazard identification and documentation	Nonfunctional	Indirect	Related to operational safety; digital errors or omissions can indirectly affect hazard awareness
Safety interlocks, touch-safe access	Functional	Indirect	Primarily physical controls but can depend on digitally controlled access systems; may be affected indirectly

Requirements that are purely physical such as weight, marking, or enclosure specifications are classified as non-CIE applicable because they lack any digital interface or cyber dependency. These items are retained under conventional engineering quality assurance and verification processes but do not require CIE-driven analysis. For traceability, their no-digital-impact classification should be documented within the requirement management framework to ensure transparency and prevent unnecessary cybersecurity scope expansion.

Scoring scale:
1 = principle absent/not addressed
2 = principle weakly addressed/implicit only
3 = principle partially addressed/some evidence but gaps exist
4 = principle mostly addressed/minor gaps remain
5 = principle fully addressed/clear, testable requirements and validation

CIE principles abbreviations:
CFD Consequence-Focused Design
EC Engineered Controls
SIA Secure Information Architecture
DS Design Simplification
LD Layered Defense
AD Active Defense

IDE Interdependency Evaluation
DAA Digital Asset Awareness
CSSC Cyber-Secure Supply Chain Controls
PR Planned Resilience
EIC Engineering Information Control
OC Organizational Culture

Table 3: CIE principles alignment scoring

Requirement	CFD	EC	SIA	DS	LD	AD	IDE	DAA	CSSC	PR	EIC	OC
Max continuous active/reactive power, max peak power	3	3	1	2	3	1	2	1	1	2	2	1
Installed and usable energy capacity	3	3	1	2	3	1	2	1	1	2	2	1
Deep discharge capability and limits	2	2	1	2	2	1	2	1	1	2	2	1
Round-trip and converter efficiency	3	3	1	2	2	1	2	1	1	2	1	1
Power quality (IEEE 519 compliance, total demand distortion, total harmonic distortion [THD])	3	3	1	2	2	1	2	1	1	2	1	1
Dynamic response parameters (ramp rate, response time, frequency/voltage droop)	3	3	1	2	3	1	2	1	1	2	1	1
Self-discharge and standby losses	2	2	1	2	2	1	1	1	1	1	1	1
Cycle lifetime and mean time between failure	2	2	1	2	2	1	2	1	1	2	1	1
Cooling system requirements (forced air or liquid)	3	3	1	2	2	1	3	1	1	2	1	1
Grid connection parameters (voltage, frequency, imbalance, THD)	3	3	1	2	3	1	2	1	1	2	1	1
Grid forming and transition (grid connected ↔ grid forming)	3	3	1	2	3	1	2	1	1	2	1	1

Voltage/frequency fault ride-through capabilities (LVRT, HVRT, ZVRT)	3	3	1	2	3	1	2	1	1	2	1	1
Short-circuit current programmability and droop control	3	3	1	2	3	1	2	1	1	2	1	1
Anti-islanding protection	3	3	1	2	3	1	2	1	1	2	1	1
Remote operation (e.g., SCADA interface, OPC, EtherCAT, Modbus)	3	2	1	1	2	1	2	1	1	2	1	1
Two-way communication (state, data, and setpoints)	3	2	1	1	2	1	2	1	1	2	1	1
Stand-alone operation (using last parameters)	2	2	1	2	2	1	2	1	1	2	1	1
Alarm system (fire, gas, temperature sensors)	2	2	1	2	2	1	2	1	1	2	1	1
Manuals and documentation (operation, maintenance, communication)	1	2	1	2	1	1	1	1	1	1	1	1
Hazard identification and documentation	2	1	1	2	1	1	1	1	1	1	2	1
Safety interlocks, touch-safe access	1	1	1	1	1	1	1	1	1	1	1	1

Most functional operational requirements (power, dynamics, grid interactions) score moderately on consequence-focused design and engineered controls because the RFP provides strong performance specifications; however, they score very low on information-centric principles (e.g., Secure Information Architecture, Digital Asset Awareness, Supply Chain, Active Defense), pulling overall averages down.

Table 4: CIE alignment scoring justification

Requirement	Description
Max continuous active/reactive power, max peak power	CFD = 3, EC = 3: These performance specifications clearly define operational capability and are therefore consequential from an engineering perspective. SIA = 1, AD = 1, DAA = 1, CSSC = 1, OC = 1: The RFP lacks information security controls, telemetry/logging, asset tracking, supply chain clauses, and organizational elements. LD = 3 and EC = 3 reflect electrical protections implicitly specified; DS = 2 partial; IDE = 2 (some interfaces exist). PR = 2 and EIC = 2: Limited documentation requirements.
Installed and usable energy capacity	Similar rationale to previous requirement: Operationally crucial (CFD = 3) and controlled by BMS/PCS (EC = 3) but missing information/security/supply chain and organizational controls; therefore, low SIA/DAA/CSSC/OC.
Deep discharge capability and limits	CFD = 2, EC = 2: The specification defines limits, but RFP lacks mapped consequences and hardware-level, independent constraints (e.g., mechanical stops), so consequence and engineered-control alignment are weakened. SIA/AD/DAA/CSSC/OC remain absent.
Round-trip and converter efficiency	Performance-focused (CFD = 3, EC = 3). However, efficiency specifications do not include secure telemetry, provenance of firmware, or resilience controls (SIA = 1, DAA = 1), so overall alignment is low.

Power quality (IEEE 519 compliance, total demand distortion, total harmonic distortion [THD])	Operationally important (CFD/EC=3) and informs protective and control behavior. Information security and validation of control logic are not required; therefore, low SIA/AD/DAA/CSSC.
Dynamic response parameters (ramp rate, response time, frequency/voltage droop)	Critical to grid stability and therefore partial alignment with CFD/EC/LD. However, the RFP does not require CIE-style cross-checks, secure architectures, or anomaly detection; SIA/AD/DAA remain low.
Self-discharge and standby losses	Largely physical/chemical (CFD = 2, EC = 2) with minimal cyber exposure (SIA/DAA = 1). The RFP does not integrate these metrics into cyber-aware operational constraints.
Cycle lifetime and mean time between failure	Nonfunctional reliability items; partially affected by operations and therefore indirectly by cyber (CFD/EC/PR moderate), but RFP lacks life cycle tracking, SBOM, and asset register (DAA = 1, CSSC = 1).
Cooling system requirements (forced air or liquid)	Cooling is a cyber-physical dependency: TMS interfaces with BMS so CFD/EC/IDE score higher (3) whereas SIA, AD, DAA, and CSSC remain absent (1). The RFP specifies cooling type but not secure control, independent fail-safes, or cross-checks.
Grid connection parameters (voltage, frequency, imbalance, THD)	Critically dependent on inverter/PCS control (CFD/EC/LD = 3) but lacking secure comms, authenticated control, or detection capabilities (SIA/AD/DAA low), so average is moderate-low.
Grid forming and transition (grid connected ↔ grid forming)	High operational importance (CFD/EC/LD = 3). RFP lacks explicit CIE-validated transition handling (secure validation, cross-checks, anomaly detection); therefore, low across SIA/AD/DAA/CSSC.
Voltage/frequency fault ride-through capabilities (LVRT, HVRT, ZVRT)	Implemented via digital control logic; RFP covers electrical requirements but omits cyber protections and cross-subsystem fail-safe validation.
Short-circuit current programmability and droop control	Good electrical specification but missing controls for secure configuration, tamper detection, and supply-chain assurances.
Anti-islanding protection	A safety-critical digital function: Electrical specification present, but no requirement for validation against malicious manipulation, secure configuration, or audit logging.
Remote operation (e.g., SCADA interface, OPC, EtherCAT, Modbus)	CFD = 3 because remote control is consequential; however, SIA = 1 (no segmentation/authorization/authentication mandated), DS = 1 (no simplification/hardening), AD/DAA/CSSC/OC all low. Remote interface is the primary cyber exposure point and scores poorly on information security principles.
Two-way communication (state, data, and setpoints)	The RFP requires telemetry and setpoint exchange (CFD = 3) but provides no secure architecture, access controls, or logging/forensics (SIA/AD/DAA = 1). Therefore, it is high risk as written.

Stand-alone operation (using last parameters)	The functionality exists (EC/PR moderate), but there is no requirement to secure fallback parameters or to protect golden images and firmware; therefore, low SIA/AD/DAA/CSSC.
Alarm system (fire, gas, temperature sensors)	Physical sensors are specified (EC = 2) but digital logging, secure telemetry, and redundancy are not required (SIA/AD/DAA low), so the alarm chain is only partially aligned with CIE.
Manuals and documentation (operation, maintenance, communication)	Documentation exists but the RFP does not require controlled access, versioning, NDAs, or integrity protections (EIC = 2 only). Without engineering information control, manuals can be a weak link.
Hazard identification and documentation	The RFP asks for hazard documentation, so CFD/DS/IDE gets small credit, but it lacks linkages to digital asset awareness, controlled documentation, or CIE-guided verification (DAA/CSSC low).
Safety interlocks, touch-safe access	Physical interlocks are present according to RFP (EC = 2) and relevant to CFD/PR; however, interlocks that depend on digital controls or remote access lack independent verification and tamper protections (SIA/AD/DAA low), so alignment is partial.

The remediation is first targeted at requirements with the highest direct digital impact and low final scores (e.g., remote operation, two-way communication, grid forming, anti-islanding, dynamic response). Those are operationally critical and currently lack security controls, raising SIA, AD, DAA, and CSSC because these will yield the largest risk reduction per engineering effort. Add explicit CIE deliverables for moderate-score items (e.g., max continuous power, cooling system) such as consequence matrix, interdependency diagrams, independent hardware fail-safes, and acceptance tests (factory acceptance testing [FAT]/site acceptance testing [SAT]) demonstrating hardware-level protections. Institutional fixes such as supply chain clauses, SBOMs, signed firmware, logging/SIEM integration, jump-host remote access and DMZ, and operator training will raise many low-scoring principles simultaneously across many requirements.

2.5. Cyber-Informed Engineering Requirement Specification

The purpose of this stage is to translate the analytical outcomes of the CIE scoping, rating, and elicitation phases into precise, enforceable requirements suitable for direct inclusion in the project's RFP. This specification phase formalizes how previously identified gaps are resolved through integrated engineering mitigations. Several requirements from the earlier analysis showed only partial alignment with CIE principles or lacked explicit design-based mitigations. This section refines those and introduces new specifications to ensure they incorporate CIE-driven design strategies such as engineered physical fail-safes, consequence containment, function isolation, and resilient control behaviors under degraded conditions [15].

Table 5 consolidates these refined and new requirements, embedding CIE mitigations alongside selective traditional cybersecurity controls . This ensures cybersecurity is inherently designed into the system's physical and control architecture rather than applied as a secondary layer. Collectively, these specifications establish the foundation for a safe, resilient, and cyber-informed

BESS deployment [16], [17] ensuring every design decision reinforces both operational reliability and consequence-focused cybersecurity integration.

Table 5: Refined and new requirement specification

Requirement Specification	
Requirement	Refined Requirement
Max continuous active/reactive power, max peak power	The System shall enforce maximum active/reactive power limits through hardware-enforced, controller-independent protective limits that remain effective during loss of supervisory control or controller malfunction. The Vendor shall demonstrate any digital override cannot increase power beyond physical protection thresholds.
Installed and usable energy capacity	The System shall incorporate hardware and firmware interlocks that prevent overcapacity operation and automatically revert to safe-state discharge limits when supervisory control is unavailable. The Vendor should provide configuration baselines and verification of safe-state reversion.
Deep discharge capability and limits	The System shall use an independent analog deep-discharge cutoff circuit that activates even if the BMS is unresponsive. The Vendor should provide evidence during factory acceptance testing that this circuit is functional without any digital signal dependency.
Round-trip and converter efficiency	The System shall detect and correct abnormal efficiency behavior through deterministic power balance validation (input vs. output). The Vendor shall demonstrate that physical metering detects deviation and triggers safe derating independent of digital analytics.
Power quality (IEEE 519 compliance, total demand distortion, total harmonic distortion)	The System shall maintain harmonic compliance through passive filtering and fixed analog damping circuits so digital control loss does not cause noncompliance. The Vendor shall validate the analog fail-safe response curve.
Dynamic response parameters (ramp rate, response time, frequency/voltage droop)	The System shall ensure ramp rate and droop parameters are enforced through hardware governor logic that limits rate of change even if firmware is altered. The Vendor shall demonstrate this enforcement under firmware-disabled conditions.
Self-discharge and standby losses	The System shall use physics-anchored models to validate standby energy loss trends and automatically flag deviations beyond engineering thresholds. The Vendor shall provide calibration data linking measured standby losses to physical cell properties.
Cycle lifetime and mean time between failure	The Vendor should deliver life cycle prediction models linked to measurable electrochemical and mechanical stress indicators and provide evidence that automatic derating occurs when aging thresholds are exceeded.
Environmental operating conditions (temperature, humidity, elevation)	The System shall autonomously transition to a conservative operational envelope upon environmental excursions, using local sensor feedback that cannot be suppressed by remote commands.

Requirement Specification	
Cooling system requirements (forced air or liquid)	The TMS shall operate an independent thermal cutoff path driven by analog sensing to maintain temperature within design bounds. The Vendor shall verify that control loss triggers passive or mechanical fail-safe cooling behavior.
Enclosure (ISO container, internal temperature limits, contaminants)	The Vendor should provide interlocked mechanical barriers and isolation zones designed so maintenance or intrusion automatically disables energy transfer paths. Interlocks shall be designed for safe degradation independent of digital status.
Power converter (current/voltage source)	The PCS shall include physically constrained conversion topology (e.g., hardware-rated choke, current limiter) ensuring grid-forming operation remains within tolerances regardless of control firmware behavior.
Site voltage/frequency tolerance	The System shall include hardware-based under-/overvoltage and frequency trip logic that operates independent of networked control and cannot be suppressed by software.
Voltage imbalance/harmonic handling	The System should maintain stability during voltage imbalance using passive design elements such as LCL filters and hardware synchronizers that continue to function under control degradation.
Grid forming: regulation	The System shall rely on embedded governor logic and inertial response derived from converter physics rather than network timing signals to stabilize voltage and frequency during islanding.
Transition times (grid following ↔ grid forming)	The System shall incorporate deterministic transition sequences stored in nonvolatile control logic; transitions shall execute from validated profiles even if supervisory commands are delayed or missing.
Fault ride-through (LVRT/ZVRT/HVRT)	The System shall integrate hardware-rated protection circuits for LVRT/HVRT and demonstrate through test that trip logic executes with or without network coordination
Frequency excursion ride-through	The System shall apply locally measured frequency validation through phase-locked hardware logic ensuring continued operation or graceful disconnect independent of remote validation.
Short-circuit current programmability and droop control	The System shall use hardware-limited current shaping devices (e.g., saturable reactors or fuses) that enforce safe limits irrespective of software-configured current values.
Anti-islanding protection	The System shall implement passive island detection based on physical parameters (voltage phase drift, current differential) that remain functional without networked SCADA coordination.

Remote operation (e.g., SCADA interface, OPC, EtherCAT, Modbus)	The Vendor should ensure remote commands can influence control logic only within defined consequence boundaries; local fail-safe control shall take precedence over network instructions under abnormal conditions.
Two-way communication (state, data, and setpoints)	The System shall validate all remote setpoints against local physics-based operational envelopes (e.g., power, voltage, temperature). Setpoints exceeding design bounds shall be rejected automatically by local control.
Stand-alone operation (using last parameters)	The System shall enter a predefined conservative operating profile derived from validated engineering limits whenever communications are lost or degraded, maintaining safe containment of stored energy.
Alarm system (fire, gas, temperature sensors)	The System shall operate redundant analog alarm circuits for fire and temperature that generate alarms and trip functions without network dependency; digital alarms serve as supplemental notification.
Manuals and documentation (operations, maintenance, communication)	The Vendor shall provide documentation mapping each requirement to its physical and procedural safeguard, including diagrams showing failure propagation limits and isolation boundaries.
Hazard identification and documentation	The Vendor should 1) produce a hazard analysis showing linkage between digital functions and physical consequences and 2) demonstrate through testing that physical interlocks mitigate those consequences under control compromise.
Requirement	New Requirement
Zone and conduit architecture	The Vendor should design control and monitoring networks to physically separate deterministic control, safety, and monitoring functions using galvanic or fiber isolation, ensuring a breach in one zone cannot alter another.
Hardware fail-safes and mechanical interlocks	The System shall include hardware trips, fuses, and mechanical cutouts designed to default to safe state without controller input. These devices shall be accessible for periodic validation and calibration.
Degraded mode profiles and recovery	The System shall revert to validated conservative profiles derived from consequence modeling whenever primary control logic is unavailable, and restoration shall occur only through authenticated re-enablement by the owner.
Supply chain assurance	The Vendor should provide evidence of provenance for safety-critical components and ensure all replacement or field-service components maintain equivalent physical integrity and security characteristics.
Diverse sensing and cross-checking	The System shall implement measurement diversity (e.g., analog + digital sensors of differing technology) with automatic cross-validation logic that reverts to conservative operation on discrepancy detection.
Training and response procedures	The Vendor should deliver operator training focused on engineering responses to loss of control logic (manual cooling, isolation, safe shutdown) rather than cyber tool response.

Incident and recovery validation	The Vendor shall demonstrate recovery from degraded or isolated state requires explicit physical confirmation of safety conditions (e.g., voltage, thermal equilibrium) before re-energization.
CIE acceptance tests	The Vendor shall perform factory and site acceptance tests that prove hardware protections activate without control software, isolation barriers prevent unintended energy flow, and fallback profiles maintain safety under simulated control compromise.

2.6. Cyber-Informed Engineering Requirement Management

Cyber-informed engineering requirement management will serve as the central mechanism for maintaining alignment between engineering, cybersecurity, and operational safety throughout the project life cycle. Each specification—particularly those refined through the CIE framework—will be managed in a requirement management repository that links every item to the corresponding CIE principle. As operational data and validation results from testing (FAT/SAT) become available, these requirements will be updated to reflect real-world performance and identified gaps.

For example, if validation testing reveals that thermal management interlocks do not adequately respond under degraded network conditions, the associated engineered control requirement will be revised to enforce independent analog fail-safes. Similarly, when communication testing shows latency or protocol weaknesses, secure information architecture requirements will be updated to specify hardened communication pathways and protocol enforcement. The requirement management process will use structured traceability to ensure every change such as updating vendor firmware signing procedures or modifying the BMS-to-PCS data exchange frequency is explicitly linked to both CIE mitigation (e.g., physical consequence containment, function isolation, redundancy) and the supporting cybersecurity mechanism (e.g., authentication, telemetry validation).

This CIE-driven management approach ensures updates are not made solely for compliance or security hardening but to directly reduce digital pathways to high-consequence events identified during consequence mapping. By continuously aligning requirements to field performance, vendor updates, and operational lessons learned, the CIE requirement management process maintains a living specification that evolves to support safe, resilient, and cyber-informed BESS operation throughout its deployment life cycle.

3. SCADA Improvement Use Case

The SCADA improvement use case represents a real-world modernization effort that upgrades operational technology across multiple water system facilities of a public water utility to improve reliability, automation, maintainability, and control of access to critical systems. As part of the SCADA Master Plan, which identified multiple projects over multiple years, this effort focuses on the replacement of aging control infrastructure with new PLC control panels, updated engine control panels, chemical dosing skids, and select field instrumentation and valve assemblies. Deployment occurs across multiple operational sites, where legacy panels are demolished and retrofitted, new conduits and conductors are installed, and networked field devices are reintegrated into the enterprise SCADA architecture. The owner and engineer complete all PLC

programming, SCADA configuration, and network configuration—maintaining configuration ownership for long-term maintainability while ensuring upgraded field assets interface correctly with the supervisory system after wiring and input/output (I/O) baseline are validated.

This use case is intentionally scoped to the contractor-facing technical specifications used to execute field implementation. The design documents and construction drawings referenced in this report are treated as representative examples of contractor deliverables and are not attributed to a specific utility, project, or site. In practice, contractor drawings and specifications are only one component of a broader modernization program. Parallel engineering deliverables define system architecture, SCADA standards, network zoning, control logic, and acceptance criteria that remain the responsibility of the Owner and Engineer. The CIE requirements framework is applied here to strengthen contractor-facing requirements that materially influence cyber-physical exposure while making explicit which decisions and risks cannot be delegated through procurement language. This framing is deliberate—responsibilities should be assigned intentionally, information sharing should be controlled to the minimum necessary for correct installation and verification, and although tasks may be delegated, operational risk ultimately remains with the owner.

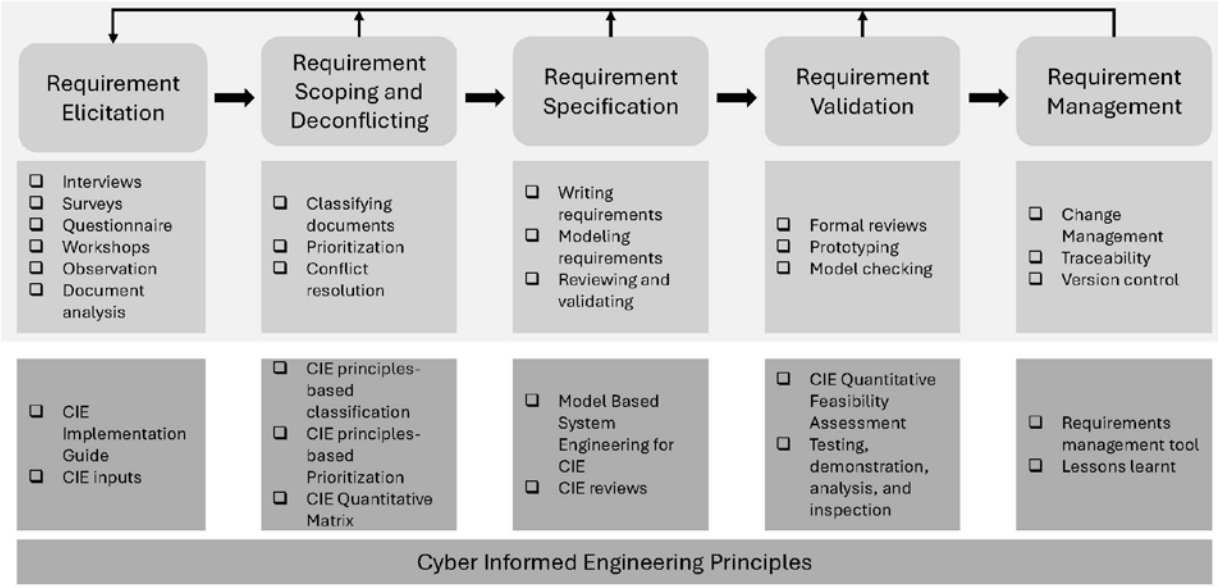

Figure 2: Requirements framework for CIE

The requirements framework (as shown in Figure 2) starts with requirement elicitation followed by requirement scoping and deconflicting, requirement specification, requirement validation, and requirement management. Because the construction drawings and electrical diagrams specify the baseline technical requirements for the SCADA improvement program, the following use case starts with a review of these specifications in Section 3.1, corresponding to the middle box in Figure 2. Section 3.2 proceeds to validation (moving to the right in Figure 2); once the validation shows the requirements are not well aligned with the CIE principles, the use case will jump back to the requirement elicitation in Section 3.3 (the leftmost box in Figure 2), followed by requirement scoping and deconflicting in Section 3.4, followed by requirement specification (again) in Section 3.5. Once the requirement specifications are aligned with CIE principles, Section 3.6 incorporates those into requirement management (the rightmost box in Figure 2).

3.1. SCADA Improvement Program Requirements From Engineering Diagrams

The detailed engineering requirements for the SCADA Improvements Project are defined in the Owner and Engineering design deliverables and associated project specifications. The following requirements summarize contractor-facing technical specifications derived from construction drawings, electrical diagrams, and the scope of work as shown in Table 6. The level of detail provided is sufficient for applying the CIE requirements framework, particularly for identifying digital interfaces, cyber-relevant components, and engineering choices that influence cyber risk.

Because the underlying plan set and associated drawings are controlled and not approved for redistribution, detailed point-to-point wiring schedules, conduit sizes, PLC I/O mappings, exact communication topologies, analyzer wiring diagrams, and equipment specifications cannot be reproduced here. Only information sufficient to apply the CIE requirements framework—specifically the identification of digital interfaces, engineered controls, and cyber-relevant touchpoints—has been included. This use case does not claim the contractor drawings themselves define the engineering requirements or demonstrate the Owner/Engineer's application of consequence-focused design; rather, it evaluates the extent to which contractor-facing specifications preserve, implement, or potentially erode cyber-informed intent during field execution.

Table 6: SCADA improvement specifications from construction drawings and electrical diagrams

Item	Specification
General electrical and wiring	
Conductor material	The Contractor shall use copper conductors for all power and control wiring unless otherwise noted in the contract drawings or approved submittal.
Wiring devices	The Contractor shall furnish heavy-duty, industrial-grade wiring devices and terminations suitable for continuous utility operation.
Conduit type	The Contractor shall install PVC-coated galvanized rigid steel conduit for all new conduit runs unless drawings explicitly specify another material.
Separation of circuits	The Contractor shall route and physically segregate power, instrument (twisted shield pair), and communications (Ethernet/fiber) cabling by separate conduits or divided wire troughs according to the drawings.
Pull cords and spare	The Contractor shall install a 250-lb pull cord in every spare conduit and leave a minimum of one continuous spare conduit per typical multi-bundle route as indicated on the drawings.
Liquid-tight flexible metal conduit (LFMC) limits	The Contractor shall limit LFMC lengths to 12–24 in. at skid/junction box connections as noted on drawings.
Continuous runs	The Contractor shall avoid splices in designated continuous-run instrument cabling paths; all continuous runs shown on the drawings must be preserved during installation.
Grounding, bonding, and compatibility	
National Electrical Code (NEC) compliance	The Contractor shall size all grounding conductors in raceways and perform bonding according to NEC Article 250 and local code.

Panel compatibility	The Contractor shall ensure any new breakers installed into existing panelboards maintain the panel UL listing and are compatible with the panel manufacturer and available ampere interrupting capacity(AIC) values.
Bond continuity	The Contractor shall maintain bonding continuity across any modified metallic raceways, transitions, or expansion fittings (bond jumpers as required).
Panel fabrication and enclosures	
UL 508A assembly	The Contractor shall supply PLC/remote terminal unit cabinet assemblies fabricated and labeled to UL-508A standards
Short-circuit current rating (SCCR)	The Contractor shall design and document assemblies with a minimum SCCR of 10 kA (10,000 A) unless drawings call for higher.
Enclosure ratings	The Contractor shall maintain enclosure NEMA ratings (Type 12 for indoor panels; Type 4X for specified junction boxes) after all modifications and mountings.
Panel internals	The Contractor shall provide door-mounted devices, LED cabinet lighting, fan/thermostat, intrusion switch, two-tier terminal blocks for field transitions, and clearly labeled terminal strips per BOM/elevations.
Nameplate data	The Contractor shall install National Fire Protection Association 70 Article 409.110 compliant nameplates (manufacturer, voltage, phases, full-load current, source, SCCR) on each panel.
PLC/Remote input output (RIO), wiring, and integration (Owner programs PLC)	
I/O terminations	The Contractor shall terminate all field I/O to the PLC I/O terminal blocks according to the I/O wiring schedules and provide wire numbers consistent with drawings.
Field wiring preservation	The Contractor shall label and preserve existing terminal designations prior to any disconnection for demolition; coiled and protected conductors intended for reuse shall be delivered to Owner according to salvage instruction.
Interposing relays and isolators	The Contractor shall install interposing relays, isolators, and redundant DC power modules where shown to preserve signal integrity and provide galvanic separation for field loops.
Panel DIN devices	The Contractor shall install specified I/O power supplies, surge suppression devices, fusing, and terminal block covers according to BOM.
Networking and communications (physical layer and handoff)	
Ethernet cabling	The Contractor shall install and terminate Category-6 (CAT6) shielded or unshielded cables as shown in the drawings; all terminations shall meet CAT6 standards and be tested and documented (wire map and power over ethernet (PoE) where applicable).
Fiber optics	The Contractor shall install, terminate, and test fiber patch panels and jumpers according to drawings; fiber testing results (optical time-domain reflectometer [OTDR]/insertion loss [IL]/return loss) shall be submitted with closeout.
Owner-furnished equipment integration	The Contractor shall mount and wire Owner-furnished network equipment (switches, routers, antennas) according to BOM and

	coordinate power and grounding but shall not commission software/configuration unless specified.
Conduit separation and ports	The Contractor shall provide dedicated conduit and port labeling for each network drop according to port standards in the drawings.
Antenna and cellular	Where cellular backhaul or antenna mounting is indicated, the Contractor shall provide mounting, coax routing, and bulkhead penetrations according to drawing details and coordinate final placement with the Owner.
Field instrumentation and analyzers	
Level instruments	The Contractor shall install ultrasonic-level transmitters and float switches according to the specified models/locations and perform mechanical mounting, conduit, and wiring according to manufacturer instructions.
Disinfectant residual analyzer integration	The Contractor shall install disinfectant residual analyzer mounting and sample tubing, supply 3/8-in. Type 316 stainless steel sample tubing to the analyzer, and provide drain routing and protective routing in motor control center (MCC) areas according to drawing notes.
Instrument cabling	The Contractor shall install continuous TSP instrument cables (no splices where drawings indicate continuous run) and maintain specified drip loops, cord grips, and receptacle connections.
Analyzer power and signals	The Contractor shall provide power, 4- to 20-mA or Modbus signal termination, and LFMC protection according to schematic to each analyzer and verify wiring continuity.
Chemical dosing skids and skid control panels	
Skid installation	The Contractor shall install duplex chemical dosing skids with skid-mounted junction boxes and provide conduit and nipples between skid control panels and skid junction boxes as shown.
Panel feed	The Contractor shall provide 30A/2P breakers and feed conductors to skid control panels as specified and update panel schedules.
Control wiring and LFMC	The Contractor shall wire skid control panels to the skid junction box using LFMC limited to the specified lengths and coil spare conductors according to drawings.
Preservation of hardwired logic	The Contractor shall preserve or reimplement existing hardwired logic paths required for analyzer actuation (e.g., well “running” signal to analyzer solenoid) unless directed otherwise by the Owner.
Engine control panels and pump controls	
Engine control panel replacement	The Contractor shall remove existing duplex engine controllers and install new engine control panels according to panel drawings and BOM, including E-stop circuits and local control stations.
Conductor bundles	The Contractor shall pull the conductor bundles specified in the wiring quantities (e.g., 70 #14 + TSP + grounds) between engine panels, PLC, and junction boxes using the indicated conduits and troughs.
Local E-stop wiring	The Contractor shall provide local E-stop stations wired in redundant pairs to engine panels as noted and install in conduit runs not exceeding 20 ft where specified.
Junction boxes, conduit entries, and mechanical	

Junction box penetrations	The Contractor shall install junction box configuration according to site notes (top entry for PLC/converter cables, bottom entry for field devices) and ensure drip protection and cable management as shown.
Material and rating	The Contractor shall supply junction boxes in 316 stainless Type 4X where specified and label each junction box according to drawing tag (e.g., JB-1, JB-2).
No splices	The Contractor shall not perform splices in designated junction boxes or conduit runs indicated as continuous on the drawings.
Power distribution and breakers	
Breaker compatibility	The Contractor shall install new circuit breakers that match existing panel manufacturer/type to preserve UL listing and meet calculated ampere interrupted capacity (AIC) ratings.
Panel schedules	The Contractor shall update and deliver as-installed panel schedules showing new circuit numbers, breaker sizes, and loads.
Temporary power	The Contractor shall provide temporary power solutions to keep critical monitoring/analyzers operational when existing circuits are touched or during planned outages.
Testing, commissioning handoff and deliverables (owner programs)	
Cabling test deliverables	The Contractor shall provide test reports for CAT6 cable (wire map/results) and fiber (OTDR and insertion loss) as part of closeout.
Panel FAT/SAT support	The Contractor shall perform mechanical/electrical inspections and basic bench validation for fabricated panels and support Owner/Engineer during FAT/SAT activities (Owner conducts PLC programming and final commissioning).
I/O and continuity checks	The Contractor shall verify and submit I/O termination lists and continuity checks to demonstrate correct field-to-panel wiring prior to Owner programming.
As-built documentation	The Contractor shall deliver marked-up record drawings, final panel I/O lists, wiring diagrams, and O&M documentation for Owner turnover.
Safety interlocks, labels, and physical protections	
Interlocks	The Contractor shall install mechanical and electrical safety interlocks, door switches, and enclosure intrusion switches as shown to preserve physical safety functions independent of networked control.
Labeling	The Contractor shall label all junction boxes, conduits, panels, and breakers according to the nameplate and label schedules and provide a final labeling report.
Spill containment	The Contractor shall install skid and secondary containment features as well as floor drains according to chemical skid specifications to prevent spills from entering electrical areas.

3.2. Cyber-Informed Engineering Requirement Validation

The validation of requirements in this use case is conducted through a structured review process. The primary objective of this review is to evaluate the completeness, clarity, and relevance of each requirement. Within the context of CIE, the review emphasizes assessing how well the requirements align with key CIE principles, ensuring cybersecurity is systematically integrated into the engineering process rather than treated as an external overlay. During this process, each

requirement is examined to verify that it accurately reflects security needs and that potential gaps are identified for remediation.

The reviewed contractor-facing technical specifications provide a robust engineering foundation in electrical, mechanical, and installation workmanship that aligns well with conventional SCADA engineering best practices. Most CIE elements that are information centric or systems level (e.g., consequence mapping and prioritization [18], secure information architecture constraints [segmentation, authentication, encryption, DMZ/jump host controls], digital asset registers and SBOM requirements, and contractual supply chain and engineering information controls) are intentionally not expressed in these contractor-facing drawings and specifications because they are controlled by the Owner/Engineer and implemented by utility staff through separate processes and controlled artifacts. One exception visible in this design package is that some critical function assurance features and engineered controls are explicitly specified, which provides a meaningful basis for CIE evaluation at the physical and control-integration layer. The following principle-by-principle evaluation summarizes the key findings from the review.

CONSEQUENCE-FOCUSED DESIGN

The reviewed specifications establish a strong electrical and mechanical baseline such as UL-508A panels, short-circuit current ratings (SSCRs), conduit and grounding practices, and detailed wiring preservation that implicitly support safe operation and equipment survivability. However, the specification set does not require an explicit consequence mapping that ties these engineering items to prioritized, stakeholder-defined unacceptable end states (safety, environmental, service continuity, regulatory). Consequence-focused design analysis and prioritization are typically performed during the Owner/Engineer design process and guided by client risk-management decisions; as a result, the associated consequence documentation is generally not carried in contractor-facing bid drawings and specifications. Accordingly, the drawings and specifications do not provide a consequence matrix or explicit traceability from high-consequence outcomes to specific engineered controls and acceptance tests, which limits the ability of this contractor-facing package (on its own) to demonstrate that protections are prioritized by consequence severity.

ENGINEERED CONTROLS

The reviewed specifications include many important physical and electrical protections such as mechanical spill containment for chemical skids, door interlocks, enclosure NEMA ratings, specified liquid-tight flexible metal conduit limits, and explicit bonding/grounding practices—all of which contribute to baseline robustness. Independent, nondigital fail-safes that remain effective if PLC/remote terminal unit (RTU) logic, panel firmware, or networked control are unavailable or compromised are implemented within the contractor package primarily through the design drawings and associated control details, consistent with the convention that drawings and specifications are interdependent and avoid duplicative statements. Accordingly, interposing relays, redundant DC modules, and other engineered protection elements are treated as “where shown” design features rather than uniformly restated as stand-alone specification clauses. From a CIE validation perspective, the residual gap is less the absence of engineered controls in the design package and more the lack of an explicit, consequence-traceable statement of intent and coverage (e.g., which critical functions are protected by independent nondigital safeguards, under which degraded conditions, and how that coverage will be verified during acceptance testing).

SECURE INFORMATION ARCHITECTURE

Physically, the drawings and port/ducting standards (dedicated conduits, separated power vs. communications, labeled ports) are well-constructed to enable secure zoning. That said, the specification stops at the physical layer and delegates logical network architecture to the Owner and Engineer; it does not require in-scope architectural constraints such as mandatory segmentation, defined zone/conduit mapping, minimum authentication or encryption standards for field protocols, DMZ/jump host controls for remote vendor access, or requirements for secure time synchronization and replay protection. Because PLC programming and network configuration are outside the contractor's deliverables, the specification would benefit from bounding statements that ensure 1) the physical topology does not preclude a secure logical architecture and 2) explicit handoff requirements (e.g., protected port labeling, demarcation points) are enforced.

DESIGN SIMPLIFICATION

The reviewed deliverables emphasize maintainability and correctness (preservation of continuous runs, two-tier terminal blocks for transitions, spare conduits and pull cords), which supports clarity. However, there is no explicit requirement to minimize unnecessary digital services or optional interfaces on delivered HMIs, panel PCs, or engineering workstations. The BOM and Owner-furnished equipment provisions increase functional capability but also risk introducing unneeded attack surface in the absence of controls to disable or harden unused services. A CIE-oriented specification would require delivery of hardened images or a documented minimal feature set for panel PCs and a verification step that nonessential services are disabled.

LAYERED DEFENSES

The reviewed specifications provide multiple defensive elements across physical, electrical, and mechanical domains such as redundant DC supplies, surge suppression, rated enclosures, interlocks, and fire/gas alarm interfaces, forming a credible layered posture. Nonetheless, the specification does not require diverse, overlapping sensing or control technologies that would materially improve resilience, such as independent analog temperature sensing to cross-verify digital measurements or an analog watchdog that can isolate charging if discrepancies occur. The lack of mandated sensing diversity and explicit cross-subsystem veto logic leaves single points of failure where a single compromised control chain could produce unsafe outcomes.

ACTIVE DEFENSE

The technical documents require standard commissioning artifacts (CAT6/fiber test reports, FAT/SAT support, I/O termination lists) and provide space for Owner-installed logging devices, but the contractor-facing requirements do not explicitly define operator-executable response actions (e.g., local safe-shutdown, manual isolation of specific control zones, or switching to predefined conservative local control modes), nor do they require clear indications/feedback that these actions have successfully driven equipment to the intended safe state. Active defense includes physical and operational mechanisms for rapid consequence containment during abnormal or suspicious system behavior, independent of network visibility or cyber tooling. As a result, the installed system may lack the telemetry and auditability needed to detect, investigate, and contain cyber-physical incidents without additional Owner engineering.

INTER-DEPENDENCY EVALUATION

The drawings and wiring schedules clearly document the physical interconnections among PLCs, engine panels, chemical skids, analyzers, and field instruments, which is a necessary foundation for interdependency analysis. However, the specification does not require a formal interdependency deliverable such as a system interaction diagram or fault-propagation analysis, nor does it require cross-verification tests that validate how failure in one subsystem (e.g., engine panel or analyzer) affects downstream logic and safety functions. Without contractual interdependency mapping and acceptance tests that exercise propagation scenarios, cascading failures or unintended emergent behaviors remain a significant residual concern.

DIGITAL ASSET AWARENESS

The specification requires nameplates, as-built drawings, and panel I/O lists, which support manual asset identification and maintenance. However, a requirement for a living, machine-readable digital asset register that records device identities, firmware versions, serial numbers, MAC/IP addresses, and responsible contacts or a software bill of materials for embedded components is missing. The absence of these artifacts reduces the project's ability to rapidly assess exposed assets during maintenance, vulnerability disclosure, or incident response and places additional burden on the Owner to construct asset visibility post-installation.

CYBER-SECURE SUPPLY CHAIN CONTROLS

The BOM and part callouts clarify responsibilities and component origins but stop short of procurement-level cybersecurity clauses. Notably, several key networked components are Owner-furnished specifically to control access, configuration authority, and chain of custody, which partially mitigates supply chain exposure for those elements. There are limited explicit requirements within the contractor-facing package for signed firmware, vendor security attestations, vulnerability disclosure, and patch service-level agreements or provenance documentation for critical networked modules. Given that several delivered panels, embedded modules, and field-connected devices include firmware and embedded components, the lack of supply chain security provisions remains a gap in ensuring the long-term trustworthiness and maintainability of supplied equipment—particularly for contractor-supplied subsystems and any embedded firmware outside the Owner-furnished boundary.

PLANNED RESILIENCE

The specification sensibly requires temporary power, preservation of hardwired logic for critical analyzers, and as-built documentation elements that support recovery and operational continuity. It does not, however, define engineered degraded modes and validated recovery procedures for suspected digital compromise (for example, safe default limits, constrained operational envelopes, or procedures to restore known good firmware images) within the contractor-facing drawing/specification package. These resilience behaviors are typically engineered and governed by the Engineer and Owner and may therefore be deliberately excluded from bid documents and contractor deliverables. In addition, there is no explicit requirement in the contractor package for golden images, offline configuration backups, or contractual recovery time objective/recovery point objective targets. As a result, from the perspective of applying the CIE requirements framework to the contractor-visible specifications, recovery expectations cannot be verified or traced to testable acceptance criteria without supplemental Owner/Engineer requirements.

ENGINEERING INFORMATION CONTROL

The specification mandates delivery of detailed engineering artifacts (drawings, I/O lists, wiring diagrams), but it does not impose controls on their storage, distribution, or integrity within the contractor-facing scope. This absence should not be interpreted as a gap in the overall program; rather, it may reflect engineering information control being applied by the Owner/Engineer through controlled release of design information and by managing sensitive repositories, access approvals, and disclosure constraints outside the contractor's scope of work. There are no requirements in the contractor package for secure document repositories, role-based access control to sensitive schematics, NDAs for external contractors, or integrity protections (e.g., signed deliverables). Consequently, when applying the CIE requirements framework strictly to the contractor-visible specifications, information-control mechanisms are not directly verifiable or traceable to acceptance criteria without supplemental Owner/Engineer governance artifacts.

ORGANIZATIONAL CULTURE

The project documentation specifies turnover, FAT/SAT support, and basic training expectations; however, it does not require cybersecurity-specific curricula for operators or engineering teams, nor does it define roles and responsibilities for incident detection, escalation, or recovery within the contractor-facing technical specification set. This absence should not be interpreted as a lack of organizational requirements overall; rather, these organizational measures are typically developed and governed by the Owner and Engineer and can be embedded in internal operating procedures, training plans, and incident-response playbooks that are intentionally excluded from bid documents. Consistent with that model, the design and construction process may itself function as a continuous improvement mechanism, where lessons learned during design development, installation, and acceptance testing feed back into updated internal processes, requirements, and training. As a result, when the CIE framework is applied strictly to contractor-visible documents, organizational culture controls are not directly auditable without referencing the Owner's internal governance artifacts.

3.3. Cyber-Informed Engineering Requirement Elicitation

The requirement elicitation process builds directly upon the gaps identified during the CIE requirement validation of the SCADA technical specifications. Although the validation revealed that several engineering and control-system elements were not fully aligned with CIE principles—particularly in consequence definition, elimination of high-risk pathways, and integration of cybersecurity into engineering decisions—the elicitation phase expands the analysis by systematically generating the missing requirements. This transition from validation to elicitation ensures the SCADA design evolves from an implicit set of operational assumptions to an explicit set of consequence-focused engineering requirements while recognizing that many intent-level, risk management, and governance artifacts are typically developed and managed by the Owner and Engineer and are intentionally not carried in contract bid documents. By applying each CIE principle to the specific contexts of specifications—including PLC upgrades, communication backhaul, reservoir and pump controls, HMI/SCADA architecture, and integration with the enterprise OT environment—the elicitation provides a structured foundation for embedding cybersecurity into engineering decisions throughout the life cycle of the project. The following

subsections describe the principle-by-principle elicitation process used for the SCADA deployment.

CONSEQUENCE-FOCUSED DESIGN

The elicitation process begins by identifying the SCADA system's most critical outcomes. Engineers, system owners, operators, and safety leads are prompted to define high-consequence events by asking, *"What are the unacceptable end states with respect to safety, environmental release, regulatory noncompliance, service interruption (potable water outage), or severe reputational impact if key SCADA controlled subsystems fail or are manipulated?"* Once these end states are established, each potential failure is mapped to its corresponding consequence through the prompt, *"For each unacceptable end state, what failure modes (both digital [for example, PLC logic tampering, spoofed telemetry, and remote command injection] and physical [for example, valve failure or pump mechanical fault]) could lead to it?"* To quantify consequence magnitude, elicitors ask, *"What operational or business metrics (e.g., interruption hours, volume of untreated water discharged, regulatory exceedance levels, number of affected customers) best capture the impact?"* Supporting artifacts to collect include incident history logs, worst-case scenario calculations, regulatory thresholds for water quality and chemical dosing, and existing standard operating procedures for emergency response. Because this consequence mapping is typically a design and risk management activity rather than a contractor deliverable, the elicitation explicitly captures it as an Owner and Engineer controlled artifact that can be selectively referenced in contractor-facing requirements only where needed to enforce critical function assurance.

ENGINEERED CONTROLS

The elicitation process focuses on identifying hardware and analog protections that operate independently of PLCs and SCADA to prevent or limit unacceptable consequences. Design and maintenance teams are asked, *"What hardware, analog, or mechanical protections exist that act independently of PLC/SCADA control logic (for example, local mechanical pump shutoffs, hardwired disinfectant residual dosing limiters, analog float switches, or independent thermal cutouts)?"* and *"How do these devices behave when PLCs or SCADA are offline, unreachable, or demonstrably compromised?"* To validate these answers, gather the relevant drawings details that specify interlocks, hardwired logic preservation, and field-level protective behaviors, along with equipment datasheets and acceptance test procedures. The elicitation outcome is an explicit inventory of independent engineered controls and the associated acceptance tests demonstrating that critical functions remain bounded even when networked control is degraded.

SECURE INFORMATION ARCHITECTURE

The elicitation identifies how the physical conduit and port topology in drawings must map to a secure logical architecture. Network architects and OT/IT stakeholders are asked, *"What is the intended zone and conduit architecture, and which protocols and encryption/authentication schemes are allowed across each conduit?"* and *"Who will have read versus write privileges to tags and control points, and where are the Owner/Contractor demarcations for network handoff?"* Supporting artifacts to collect include port standards, conduit and port labeling conventions, internal zoning policies, and remote access governance that may be maintained outside contractor documents. The elicitation produces a zoning and protocol baseline that is Owner and Engineer

controlled, plus a constrained set of contractor-facing installation and labeling requirements that preserve the ability to implement that architecture during commissioning.

DESIGN SIMPLIFICATION

The elicitation targets reduction of unnecessary features that would otherwise increase attack surface on panel PCs, radios, and HMIs. Integrators and operations are asked, *"Which services and interfaces are operationally essential versus convenience, and which default services, ports, or accounts can be disabled or removed on delivered devices?"* and *"Can control devices be delivered with a minimal feature baseline that is testable at acceptance?"* Evidence to collect includes vendor default configuration lists, device hardening guidance, and the BOM assignments that distinguish Owner-furnished versus contractor-installed components. The elicitation outcome is a minimal feature baseline and acceptance verification approach that is compatible with the project's division of responsibilities, so the contractor supports physical provisioning while the Owner and Engineer enforce configuration intent where they retain programming and network control.

LAYERED DEFENSE

The elicitation ensures critical SCADA functions have independent, overlapping protections. System engineers and operations staff are prompted, *"For each critical function, such as remote pump start stop, emergency chemical dosing shutdown, or high-level protection, what at least two independent controls from different domains exist, for example, mechanical, analog sensing, or independent cutout, and what still prevents the unacceptable consequence if one control fails?"* To substantiate responses, collect the relevant interlock schematics, hardwired logic paths, and field device specifications referenced by drawings. The elicitation outcome is a layered defense specification with acceptance tests demonstrating that diverse controls remain effective when any single layer is disabled, failed, or bypassed.

ACTIVE DEFENSE

The elicitation establishes what telemetry and logging are required for detection, correlation, and investigation of anomalous events. Security operations, SCADA engineers, and vendor representatives are asked, *"Which events must be logged at the device or system level, such as logic downloads, firmware updates, setpoint changes, and remote sessions, what minimum time stamping and integrity properties are required, and where should log aggregation occur?"* Supporting material includes sample logs from representative devices, historian and alarm tag lists, and the Owner's retention and monitoring policies. The elicitation produces controlled logging and telemetry requirements that are typically implemented by Owner and Engineer configuration activities while specifying any contractor support needs such as panel space, wiring provisions, and demarcation points for secure log export hardware.

INTERDEPENDENCY EVALUATION

The elicitation converts the physical and wiring topology into an operational interdependency model to reveal propagation channels. System engineers and operators are asked, *"Provide an interdependency diagram showing how PLC programs, engine control panels, chemical dosing skids, ultrasonic-level sensors, and communications interact, and identify where faults or malicious actions could propagate across those boundaries."* In practice, this evaluation is typically performed by the Engineer as an intrinsic part of the design process, with the Owner defining

operational requirements and providing feedback on system-level impacts across local and distributed operations. Supporting data include I/O lists, junction box entry rules, and wiring dependencies shown in drawings, supplemented by Owner and Engineer knowledge of control logic and operational modes that may not be present in contractor-facing drawings. The elicitation therefore focuses on making the interdependency evaluation explicit and traceable as a design assurance artifact and on capturing the Owner's operational assumptions and acceptance criteria for managing propagation and cascading effects. The deliverable is an interdependency diagram and fault propagation assessment with test scenarios that can be exercised during acceptance testing to verify containment and safe behavior across subsystem boundaries.

DIGITAL ASSET AWARENESS

The elicitation ensures a machine-readable, operational asset register is produced for the SCADA landscape. Asset managers and procurement are asked to *"Provide a complete inventory (device, model, serial, firmware version, network address or demarcation, physical location, and function) and specify who will maintain and update this registry and at what cadence"* and *"Where feasible, provide an SBOM or firmware provenance statement for embedded software in PLCs, radios, and panel PCs."* Supporting materials include the panel nameplate schedules and Owner-furnished equipment lists. The elicitation outcome is a living asset register and provenance package, recognizing that the contractor may supply identification data whereas the Owner governs the authoritative baseline after turnover.

CYBER-SECURE SUPPLY CHAIN CONTROLS

The elicitation establishes how supply chain risk is managed in a way that matches the project's responsibility split. Procurement, engineering, and vendors are asked, *"Which components are Owner furnished specifically to control chain of custody, and for vendor-supplied components what provenance, secure update practices, and vulnerability disclosure obligations are required?"* Evidence to collect includes vendor security documentation, firmware signing capabilities, and support life cycle commitments. The elicitation outcome is a set of procurement clauses and acceptance criteria focused on consequence containment and maintainable trust while accounting for the fact that key networked elements may already be controlled through Owner furnishing rather than contractor procurement.

PLANNED RESILIENCE

The elicitation defines engineered degraded modes and recovery expectations appropriate for a water utility SCADA environment while acknowledging that these are often developed by the Engineer and Owner staff and excluded from contractor bid documents. Operations and control engineers are prompted, *"What degraded operating envelopes are acceptable and how are they invoked, and what manual local control capabilities must remain available when supervisory control is impaired?"* and *"What restoration process exists for known good configurations, including backups and recovery objectives?"* Supporting evidence includes contingency procedures, acceptance test plans, and configuration management practices maintained by the Owner. The elicitation outcome is a resilience and recovery package that can be selectively translated into contractor-facing provisions where physical installation must support recovery, such as demarcation, labeling, and access to panels and field devices.

ENGINEERING INFORMATION CONTROL

The elicitation clarifies how sensitive engineering artifacts are controlled across the life cycle, recognizing that these controls are typically governed outside the contractor's scope and that the absence of such controls in bid documents can be an intentional application of engineering information control. Document owners, legal teams, and configuration managers are asked, *"Where will wiring/network schematics, PLC logic, and configuration files be stored, who may access them, and what signed-delivery and access-control mechanisms (e.g., role-based access, NDAs) must be enforced?"* The elicitation outcome is an information control plan that references controlled repositories, access governance, and turnover packaging while limiting contractor-facing disclosure only to what is necessary to correctly install and verify the physical system.

ORGANIZATIONAL CULTURE

The elicitation aligns people and processes to the engineered system but treats these measures as Owner and Engineer governance artifacts rather than contractor deliverables. Operations leadership and engineering managers are asked, *"What training, role definitions, and escalation paths are required to operate and maintain the upgraded SCADA assets safely, including how to respond to abnormal control behavior or suspected compromise?"* and *"How are lessons learned from design development and acceptance testing fed back into updated procedures and training?"* The elicitation outcome is a set of internal training and operational readiness artifacts, such as role assignments and exercise objectives, that can be validated through Owner-managed processes without expanding contractor-facing documents beyond their intended scope.

3.4. Cyber-Informed Engineering Requirement Scoping and Deconflicting

Following the elicitation phase, where foundational system and cybersecurity requirements were gathered through structured interviews and scenario-based questions, the next step in the process is requirement scoping and deconflicting. This phase ensures the elicited requirements are correctly categorized, aligned with digital system impacts, and assessed against the 12 CIE principles to prioritize engineering efforts where they matter most.

The objective of this phase is twofold:

- To distinguish between functional and nonfunctional requirements to clarify which directly influence system operation and which contribute to resilience, integrity, or organizational culture.
- To evaluate each requirement's digital impact—whether direct, indirect, or none—so engineers can proportionally apply CIE mitigations to those system functions that present the highest cyber-physical consequence potential.

By classifying, scoring, and justifying each requirement's relationship to CIE principles, this phase bridges raw elicitation data with actionable specifications. It reveals where traditional cybersecurity measures may be insufficient and where engineered safeguards such as hardware interlocks, control independence, or system segmentation should be emphasized. The scoring also helps identify overlaps and conflicts between requirements, enabling harmonized implementation that supports both safety and secure operability.

To systematically apply this logic, three analytical outputs are presented in this section:

- Table 7 categorizes each specification as functional or nonfunctional and defines its digital impact (direct, indirect, or none), providing a foundational understanding of system exposure.
- Table 8 evaluates each requirement against the 12 CIE principles using a quantitative 1–5 scale, indicating the degree of alignment between the existing specification and CIE objectives.
- Table 9 provides the rationale behind each score, illustrating why certain requirements lack alignment and where engineering or procedural mitigations are needed.

This structured approach transforms the elicited requirements into a traceable, consequence-focused framework that sets the stage for formal specification and refinement in the next phase

Table 7: Classification of existing requirements

Requirement	Type	Digital Impact	Description
Conductor material: copper conductors for power and control wiring	Nonfunctional	No	Physical/material specification for electrical reliability and code compliance; no cyber interface
Wiring devices: heavy duty, industrial grade	Nonfunctional	No	Mechanical/electrical durability requirement; not digital
Conduit type: PVC-coated galvanized rigid steel	Nonfunctional	No	Mechanical installation material; no digital dependency
Separation of circuits (power, TSP, communications)	Nonfunctional	Indirect	Physical segregation reduces electromagnetic coupling and supports network segregation; affects signal integrity and security indirectly
Pull cords and spare conduits	Nonfunctional	No	Installation convenience/resilience; not digital
Liquid-tight flexible metal conduit (LFMC) limits at skids/junction boxes	Nonfunctional	No	Mechanical routing constraint; no cyber interface
Continuous runs: avoid splices in instrument cabling	Nonfunctional	Indirect	Preserves signal integrity of instrument/digital measurements; supports reliable digital sensing indirectly
National Electrical Code compliance: grounding and bonding according to Article 250	Nonfunctional	No	Electrical safety/code requirement; not a digital control
Panel compatibility: breakers maintain UL listing and ampere interrupted capacity (AIC)	Nonfunctional	No	Equipment compatibility/safety; not digital
Bond continuity across modified raceways	Nonfunctional	No	Electrical safety/ electromagnetic interference control; no direct digital interface
UL 508A assembly: PLC/RTU cabinets	Nonfunctional	No	Fabrication/labeling standard for panels; physical/administrative requirement
SCCR rating: min 10 kA	Nonfunctional	No	Short-circuit rating for safety; not digital
Enclosure ratings (NEMA Type 12/4X)	Nonfunctional	No	Environmental protection requirement for enclosures; not digital
Panel internals: door devices, fans, intrusion switch, terminal blocks	Nonfunctional	Indirect	Mostly physical; intrusion switches and door sensors interface to control systems and support security/monitoring indirectly

Nameplate data (National Fire Protection Association 70 Article 409.110)	Nonfunctional	No	Identification and compliance marking; administrative
I/O terminations to PLC I/O blocks	Functional	Direct	Directly supports digital control connectivity between field devices and PLCs
Field wiring preservation/labeling for salvage	Nonfunctional	Indirect	Process/documentation that preserves correct digital mapping; supports traceability indirectly
Interposing relays and galvanic isolators	Functional	Indirect	Electrical interface devices protect signal integrity and isolate faults; reduce digital-signal corruption indirectly
Panel DIN devices: I/O power supplies, surge suppression, fusing	Nonfunctional	Indirect	Physical protection for digital I/O; supports digital reliability indirectly
Ethernet cabling (CAT6 install and test)	Functional	Direct	Direct network medium for SCADA/PLC communications (major digital impact)
Fiber optics (install, test, optical time-domain reflectometer [OTDR] deliverable)	Functional	Direct	High-speed network medium carrying SCADA/PLC traffic, which has direct digital impact
Owner-furnished equipment integration (mount/wire)	Functional	Direct	Involves networked devices (switches/routers) and their physical integration, which directly affects digital communications
Conduit separation and port labeling for network drops	Nonfunctional	Indirect	Enables physical support for logical segmentation and later secure zoning, which has indirect digital impact
Antenna and cellular mounting/bulkhead routing	Functional	Direct	Wireless communications are direct digital transport points and attack surfaces
Level instruments: ultrasonic transmitters and float switches	Functional	Direct	Field sensors feed PLCs with process data, which has direct digital dependency
Disinfectant residual analyzer integration	Functional	Direct	Instrument interfaces (4–20 mA/Modbus) provide operational data and control interlocks, which has direct digital impact
Instrument cabling: continuous TSP runs, drip loops	Functional	Direct	Signal wiring for instruments that feed digital controllers; direct impact on digital sensing
Analyzer power and signal termination (4–20 mA/Modbus)	Functional	Direct	Provides digital/analog signals to control systems; direct digital impact

Skid installation: chemical dosing skids and skid junction boxes	Functional	Indirect	Mechanical installation of cyber-physical equipment; the skid control interfaces create indirect digital impact
Panel feed: breakers and feed conductors to skid panels	Functional	Indirect	Power feed for control panels; affects availability of digital control indirectly
Control wiring and LFMC between skid and junction box	Functional	Direct	Control cabling carries signals to/from controllers; has direct digital effect
Preservation of hardwired logic (pump run status to analyzer solenoid)	Functional	Direct	Explicit protection of non-networked, hardwired control paths that affect operation, which has direct digital/functional importance
Engine control panel replacement	Functional	Direct	Replacement panels interface with PLCs and include digital control elements
Conductor bundles (specified quantities routed)	Nonfunctional	Indirect	Installation practice for field signals; supports correct digital connectivity indirectly
Local E-stop wiring (redundant pairs)	Functional	Indirect	Physical safety action but wiring interfaces into control circuits; indirect digital impact because it bypasses or complements digital commands
Junction box penetrations (top entry for PLC, bottom for field devices)	Nonfunctional	Indirect	Mechanical/cable management that supports correct digital routing; indirect
Junction box material and rating (316 SS Type 4X)	Nonfunctional	No	Environmental/material specification; not digital
No splices in designated junction boxes/conduit runs	Nonfunctional	Indirect	Ensures signal integrity and traceability of digital signals; indirect digital support
Breaker compatibility: match manufacturer and ampere interrupted capacity (AIC)	Nonfunctional	No	Electrical compatibility/safety standard; not digital
Panel schedules: update and deliver as-installed schedules	Nonfunctional	Indirect	Documentation that supports later configuration and digital mapping; indirect digital impact
Temporary power for critical monitoring/analyzers	Nonfunctional	Indirect	Operational continuity for digital monitoring assets; indirect digital impact
Cabling test deliverables: CAT6 wire map, fiber OTDR/IL	Nonfunctional	Direct	Verification of digital comms media; directly supports digital functionality and security posture

Panel FAT/SAT support and bench validation	Nonfunctional	Indirect	Testing support that enables correct digital commissioning (Owner programs PLC)—indirect
I/O and continuity checks before Owner programming	Functional	Direct	Ensures correct field-to-PLC wiring for digital control
As-built documentation and O&M deliverables	Nonfunctional	Indirect	Operational documentation enabling maintenance and configuration control that supports digital life cycle management indirectly
Interlocks: mechanical and electrical safety interlocks, door switches	Functional	Indirect	Physical safety features that interact with control logic; they provide indirect digital safety functions (and sometimes direct alarm inputs)
Labeling: junction boxes, conduits, panels, breakers	Nonfunctional	No	Identification for maintenance/operations; administrative, not digital (though aids management)
Spill containment and secondary containment	Nonfunctional	No	Physical environmental protection; no digital link

Requirements that are purely physical such as weight, marking, or enclosure specifications are classified as non-CIE applicable because they lack any digital interface or cyber dependency. These items are retained under conventional engineering quality assurance and verification processes but do not require CIE-driven analysis. For traceability, their no-digital-impact classification should be documented within the requirement management framework to ensure transparency and prevent unnecessary cybersecurity scope expansion.

Table 8: CIE principles alignment scoring

Requirement	CFD	EC	SIA	DS	LD	AD	IDE	DAA	CSSC	PR	EIC	OC
Separation of circuits (power, TSP, communications)	2	4	2	3	3	1	3	1	1	2	1	1
Continuous runs: avoid splices in instrument cabling	2	4	1	3	2	1	2	1	1	2	1	1
Panel internals: door devices, fans, intrusion switch, terminal blocks	2	3	2	2	2	1	2	1	1	2	2	1
I/O terminations to PLC I/O blocks	3	4	2	3	2	1	3	2	1	2	2	1
Field wiring preservation/labeling for salvage	2	3	1	2	1	1	2	2	1	2	3	1
Interposing relays and galvanic isolators	3	4	1	2	3	1	3	1	1	3	1	1

Requirement	CFD	EC	SIA	DS	LD	AD	IDE	DAA	CSSC	PR	EIC	OC
Panel DIN devices: I/O power supplies, surge suppression, fusing	2	4	1	2	2	1	2	1	1	3	1	1
Ethernet cabling (CAT6 install and test)	3	3	2	2	2	1	3	2	1	2	2	1
Fiber optics (install, test, optical time-domain reflectometer [OTDR] deliverable)	3	3	2	2	2	1	3	2	1	2	2	1
Owner-furnished equipment integration (mount/wire)	2	3	1	2	1	1	2	1	1	2	1	1
Conduit separation and port labeling for network drops	2	3	2	3	2	1	2	1	1	2	2	1
Antenna and cellular mounting/bulkhead routing	2	2	1	2	1	1	2	1	1	2	1	1
Level instruments: ultrasonic transmitters and float switches	3	3	1	2	1	1	3	2	1	2	2	1
Disinfectant residual analyzer integration	3	3	1	2	1	1	3	2	1	2	2	1
Instrument cabling: continuous TSP runs, drip loops	3	4	1	3	1	1	3	1	1	2	1	1
Analyzer power and signal termination (4–20 mA/Modbus)	3	3	1	2	1	1	3	2	1	2	2	1
Skid installation: chemical dosing skids and skid junction boxes	2	3	1	2	1	1	3	1	1	2	1	1
Panel feed: breakers and feed conductors to skid panels	2	4	1	2	1	1	2	1	1	3	1	1
Control wiring and liquid-tight flexible metal conduit between skid and junction box	3	3	1	2	1	1	3	1	1	2	1	1
Preservation of hardwired logic (pump run status to analyzer solenoid)	4	4	1	2	2	1	4	1	1	3	2	1
Engine control panel replacement	3	3	1	2	1	1	3	1	1	2	1	1

Requirement	CFD	EC	SIA	DS	LD	AD	IDE	DAA	CSSC	PR	EIC	OC
Conductor bundles (specified quantities routed)	2	3	1	2	1	1	2	1	1	2	1	1
Local E-stop wiring (redundant pairs)	4	4	1	2	3	1	3	1	1	4	1	1
Junction box penetrations (top entry for PLC, bottom for field devices)	2	3	1	3	1	1	2	1	1	2	1	1
No splices in designated junction boxes/conduit runs	2	4	1	3	1	1	2	1	1	2	1	1
Panel schedules: update and deliver as-installed schedules	2	2	1	2	1	1	2	2	1	2	3	1
Temporary power for critical monitoring/analyzers	2	3	1	1	1	1	2	1	1	3	1	1
Cabling test deliverables: CAT6 wire map, fiber OTDR/IL	3	3	2	2	1	1	3	2	1	2	3	1
Panel FAT/SAT support and bench validation	3	3	2	2	1	1	3	2	1	3	3	1
I/O and continuity checks before Owner programming	3	4	2	2	1	1	3	2	1	3	3	1
As-built documentation and O&M deliverables	2	2	1	2	1	1	2	3	1	2	3	1
Interlocks: mechanical and electrical safety interlocks, door switches	4	4	1	2	3	1	3	1	1	4	2	1

Table 9: CIE alignment scoring justification

Requirement	Description
Separation of circuits (power, TSP, communications)	EC = 4 and LD = 3 are driven by explicit physical segregation that reduces cross-coupling and supports robust I/O signal transport. SIA = 2 reflects that the contractor package enables later zoning through conduits and separation, but it does not include Owner and Engineer network security configuration or access control requirements—so AD, DAA, CSSC, and OC remain low in this table.
Continuous runs: avoid splices in instrument cabling	EC = 4 and DS = 3 reflect workmanship requirements that reduce latent faults and preserve measurement fidelity for PLC decision making. The low SIA and AD scores reflect that integrity here is electrical and installation-focused whereas cyber validation, logging, and protocol hardening are handled outside the contractor specification set.
Panel internals: door devices, fans, intrusion switch, terminal blocks	EC = 3 reflects baseline panel robustness and maintainability, and EIC = 2 reflects that intrusion switches provide a physical tamper indication pathway. AD remains low because the contractor requirements do not specify tamper-evident logging, event retention, or monitoring integration, which are Owner and Engineer operational controls rather than contractor deliverables in this use case.
I/O terminations to PLC I/O blocks	CFD = 3, EC = 4, and IDE = 3 reflect that correct I/O termination is essential to safe control outcomes and reliable subsystem interaction. SIA = 2 captures that wiring correctness is a prerequisite to trustworthy data paths, but secure tag authorization, protocol security, and change auditing are outside the contractor scope and therefore score low here.
Field wiring preservation/labeling for salvage	EIC = 3 and DAA = 2 reflect traceability and reduced rework risk through labeling, preservation, and documented handoff. The low SIA and AD scores are retained because information security controls and monitoring are not expressed in contractor-facing drawings and specifications, even though labeling improves maintainability.
Interposing relays and galvanic isolators	These devices provide electrical isolation and redundant signal protection (EC = 4, LD = 3), reducing the propagation of electrical faults into control logic and improving consequence containment (CFD = 3).
Panel DIN devices: I/O power supplies, surge suppression, fusing	EC = 4 and PR = 3 reflect power quality and survivability measures that reduce nuisance failures and improve the availability of control I/O. These are strong engineered protections, but SIA, DAA, CSSC, and OC remain low because life cycle cyber controls are managed through Owner and Engineer processes rather than contractor language.
Ethernet cabling (CAT6 install and test)	CFD = 3 and IDE = 3 reflect that communications transport is operationally consequential and a dependency for supervisory visibility and control. SIA=2 is limited to physical readiness and

Requirement	Description
	test evidence; segmentation rules, authentication, and encryption requirements are not included in the contractor specification set.
Fiber optics (install, test, OTDR deliverable)	CFD = 3 and IDE = 3 reflect operational dependence on reliable transport, and SIA = 2 reflects that physical separation and test deliverables support a secure architecture once configured by the Owner and Engineer. AD remains low because monitoring and breach detection are not specified at the contractor deliverable level.
Owner-furnished equipment integration (mount/wire)	EC = 3 reflects correct physical integration of network gear as part of the overall control system dependency chain. CSSC = 2 is credited because Owner-furnished equipment is an intentional chain-of-custody mitigation in this use case, even though secure configuration, firmware assurance, and monitoring remain outside contractor responsibilities and are not scored high here.
Conduit separation and port labeling for network drops	DS = 3 and SIA = 2 reflect that consistent labeling and dedicated drops enable disciplined zoning and reduce ad hoc attachments later. The low AD and DAA scores reflect that the contractor package stops at physical demarcation and does not include operational telemetry, asset registry governance, or security monitoring requirements.
Antenna and cellular mounting/bulkhead routing	CFD = 2 and IDE = 2 reflect that this supports a consequential communications dependency, but the contractor deliverable is limited to physical mounting and routing. SIA, AD, and CSSC remain low because provisioning, credentialing, and remote access governance are Owner controlled and not expressed in contractor-facing requirements.
Level instruments: ultrasonic transmitters and float switches	CFD = 3 and IDE = 3 reflect that sensor correctness underpins safe operational outcomes and downstream control logic behavior. Low SIA and AD reflect that sensor authentication, redundancy policy, and telemetry integrity monitoring are not contractor deliverables in the reviewed package.
Disinfectant residual analyzer integration	CFD = 3 and IDE = 3 reflect safety and compliance consequences tied to analyzer signals and interlocks. Low SIA, AD, and CSSC reflect that firmware assurance, secure communications configuration, and logging are treated as Owner and Engineer responsibilities and are not specified as contractor deliverables here.
Instrument cabling: continuous TSP runs, drip loops	Continuous instrument cabling is strongly aligned with signal integrity and operational accuracy (EC = 4, CFD = 3) but offers limited information security characteristics.

Analyzer power and signal termination (4–20 mA/Modbus)	CFD = 3 and IDE = 3 reflect that correct termination supports reliable interlocks and process control behavior. SIA stays at 1 because secure protocol selection, access control, and tamper-evident logging are not within the contractor-facing requirement language.
Skid installation: chemical dosing skids and skid junction boxes	EC = 3 and IDE = 3 reflect that skid integration introduces a cyber-physical dependency chain that must be physically correct to avoid unsafe states. Low SIA, DAA, and CSSC reflect that secure electronics configuration, firmware controls, and life cycle governance are not specified in contractor deliverables in this use case.
Panel feed: breakers and feed conductors to skid panels	EC = 4 and PR = 3 reflect that availability and safe power delivery are engineered prerequisites for reliable control and monitoring. SIA, AD, and DAA remain low because this requirement is purely electrical and does not include cyber monitoring or asset management artifacts.
Control wiring and LFMC between skid and junction box	CFD = 3 and IDE = 3 reflect direct dependence of skid control behavior on correct field wiring. SIA and AD remain low because signal spoofing protections, monitoring, and authenticated command pathways are not contractor deliverables in the reviewed package.
Preservation of hardwired logic (pump run status to analyzer solenoid)	Maintaining hardwired actuation preserves out-of-band safety functions and consequence containment (CFD/EC/IDE high), offering a strong CIE control even though it is not a digital control mechanism.
Engine control panel replacement	CFD = 3 and IDE = 3 reflect that panel replacement affects a consequential control function and a key subsystem dependency. Low SIA and CSSC reflect that programming, secure configuration, and firmware governance are not within contractor deliverables in this use case.
Conductor bundles (specified quantities routed)	Conductor bundling supports orderly installation and reduces wiring errors (EC) but offers limited direct cybersecurity value beyond installation discipline.
Local E-stop wiring (redundant pairs)	CFD = 4, EC = 4, LD = 3, and PR = 4 reflect a strong engineered, SCADA-independent protection layer for high-consequence scenarios. SIA and AD remain low because the protection is intentionally physical and local, and cyber monitoring is not specified at the contractor requirement level.
Junction box penetrations (top entry for PLC, bottom for field devices)	Mechanical routing minimizes cable routing issues and protects signal separation (EC/DS) but lacks cyber controls or inventory requirements.
No splices in designated junction boxes/conduit runs	Eliminating splices preserves signal integrity and troubleshooting (EC = 4, DS = 3) and reduces latent fault possibilities, though there is little digital security content.

Panel schedules: update and deliver as-installed schedules	DAA = 2 and EIC = 3 reflect improved traceability and configuration accuracy during turnover through consistent schedules and documentation. SIA and AD remain low because access controls, controlled distribution, and monitoring are managed through Owner information control practices, not contractor deliverables.
Temporary power for critical monitoring/analyzers	Provisioning temporary power supports operational continuity (PR = 3) for safety-critical sensors but does not provide information-security assurances.
Cabling test deliverables: CAT6 wire map, fiber OTDR/IL	Test artifacts substantiate communications integrity (EIC = 3, DAA = 2) and enable commissioning validation, but the specification does not require cryptographic validation or monitoring integration.
Panel FAT/SAT support and bench validation	CFD = 3, EC = 3, and PR = 3 reflect that acceptance activities provide leverage points to verify engineered protections and wiring correctness. Low SIA and AD remain because cyber-focused acceptance criteria, monitoring integration, and operational security processes are Owner and Engineer controlled for this use case.
I/O and continuity checks before Owner programming	Preprogramming checks are essential to ensure correct digital-physical mappings (I/O integrity), strongly aiding consequence-focused validation and commissioning readiness.
As-built documentation and O&M deliverables	DAA = 3 reflects that as-builts materially support life cycle awareness and maintenance readiness. EIC = 3 reflects documentation completeness and turnover traceability while acknowledging that controlled distribution and repository governance are exercised through Owner information control rather than contractor language.
Interlocks: mechanical and electrical safety interlocks, door switches	CFD = 4, EC = 4, LD = 3, and PR = 4 reflect strong engineered protections that remain effective without digital connectivity. Low SIA and AD remain appropriate because the mitigations are primarily physical and local, and monitoring integration is not specified as a contractor deliverable.

The scoring results reflect the contractor-facing nature of the technical specifications. Many requirements strongly support engineered robustness (especially EC, DS, LD, and PR) through installation workmanship, physical segregation, and acceptance evidence, but they score low in SIA, AD, DAA, CSSC, EIC, and OC because those CIE elements are largely exercised through Owner and Engineer design decisions, controlled information practices, and operational governance that are intentionally not expressed in contractor bid documents. The primary CIE strength that does appear directly in the contractor package is the set of critical function assurance features implemented through engineered controls and wiring dependencies (for example, hardwired actuation paths, interlocks, segregation, and acceptance evidence), which provide consequence containment even under degraded digital conditions. Overall, Table 9 indicates the contractor package embeds strong physical and electrical implementation requirements and selectively enables secure architecture through topology constraints. The next section focuses on

how to explicitly carry forward Owner and Engineer CIE outcomes into requirements and acceptance criteria without overexposing controlled design intent.

3.5. Cyber-Informed Engineering Requirement Specification

The purpose of this stage is to translate the analytical outcomes of the CIE scoping, rating, and elicitation phases into precise, enforceable requirements suitable for direct inclusion in the project's contractor-facing specification. This specification phase formalizes how previously identified gaps are resolved through integrated engineering mitigations without requiring disclosure of controlled design intent or Owner internal risk decisions. Several requirements from the earlier analysis showed only partial alignment with CIE principles or lacked explicit design-based mitigations within the contractor deliverable boundary. This section refines those and introduces new specifications to ensure they incorporate CIE-driven design strategies such as engineered physical fail-safes, consequence containment, function isolation, and resilient control behaviors under degraded conditions, and, where appropriate, physical and interface provisions that enable the Owner and Engineer to implement their network and operational security controls.

Table 10 consolidates these refined and new requirements, embedding CIE mitigations alongside selective traditional cybersecurity controls primarily as physical constraints, demarcations, and turnover artifacts rather than configuration directives. This ensures cybersecurity is inherently designed into the system's physical and control architecture rather than applied as a secondary layer. Collectively, these specifications establish the foundation for a safe, resilient, and cyber-informed SCADA deployment while maintaining clear responsibility boundaries: The Contractor implements the physical and installation controls and delivers objective evidence whereas the Owner and Engineer implement configuration, policy, and operational governance.

Table 10: Refined and new requirement specification

Requirement Specification	
Requirement	Refined Requirement
Separation of circuits (power, TSP, communications)	Circuits shall be physically segregated using engineered barriers, independent conduit pathways, and separation distances as defined in the drawings and any Owner-provided consequence classification schedule. FAT/SAT shall verify isolation so faults or induced signals cannot propagate across domains.
Continuous runs: avoid splices in instrument cabling	Instrumentation cabling shall be installed as uninterrupted engineered runs with no in-line joints except at designated termination panels, ensuring consequence isolation and minimizing multipoint failure propagation.
Panel internals: door devices, fans, intrusion switch, terminal blocks	Panel interiors shall include mechanically fail-safe door switches, protected airflow paths, and segregated terminal blocks that prevent shared-fault modes and provide a discrete alarm contact suitable for Owner integration upon intrusion or panel opening.

I/O terminations to PLC I/O blocks	PLC I/O blocks shall use keyed, mechanically differentiated terminations and segregated analog/digital zones to prevent erroneous cross-signaling or unsafe actuator energization under faulted conditions.
Field wiring preservation/labeling for salvage	Wiring shall include engineered strain-relief, moisture barriers, and durable labeling that supports consequence tracing and forensic reconstruction through physical traceability and consistent wire identification without digital tools.
Interposing relays and galvanic isolators	Hardware isolators and relays shall serve as engineered command-limiters, preventing direct PLC-to-actuator energy transfer and constraining unintended operations independent of digital logic.
Panel DIN devices: I/O power supplies, surge suppression, fusing	DIN components shall be arranged to enforce selective isolation, sacrificial surge protection, and fault-blocking layouts that prevent cascading failure across circuits.
Ethernet cabling (CAT6 install and test)	Cabling shall be routed in mechanically isolated paths with engineered strain protection and termination testing confirming isolation, shielding integrity, and minimal susceptibility to cross-domain interference and shall be labeled to preserve the intended zoning demarcations shown in the drawings.
Fiber optics (install, test, optical time-domain reflectometer [OTDR] deliverable)	Fiber runs shall be placed in physically protected conduits with OTDR evidence demonstrating redundancy retention under single-break conditions and isolation from mechanical and thermal stresses and shall document fiber endpoints and patching consistent with the port labeling standard.
Owner-furnished equipment integration (mount/wire)	Owner-furnished equipment integration shall use mechanical isolation couplings, protected mounting, and documented physical demarcation, ensuring no cross-vendor shared-failure modes, and shall record device model and serial identifiers provided with the Owner-furnished equipment for Owner custody tracking.
Conduit separation and port labeling for network drops	Conduits and ports shall be labeled by engineered isolation zones rather than device names, ensuring physical domain separation that prevents accidental bridging of control and administrative paths.
Antenna and cellular mounting/bulkhead routing	Antenna mounting shall include mechanical radio frequency (RF) isolation, protected bulkhead routing, and physical disconnect points to ensure controlled degradation under communication loss.
Level instruments: ultrasonic transmitters and float switches	Level instrumentation shall include mechanically independent verification paths (e.g., float + ultrasonic) so digital or sensor corruption does not drive unsafe water-level control actions.
Disinfectant residual analyzer integration	Disinfectant residual analyzers shall employ redundant sample verification, protected sample lines, and independent

	hardware limits, ensuring safe chemical feed control even under network loss.
Instrument cabling: continuous TSP runs, drip loops	Cable routing shall include engineered moisture diversion, mechanical protection, and routing patterns, preventing multipoint failure through environmental or mechanical intrusion.
Analyzer power and signal termination (4–20 mA/Modbus)	Terminations shall use galvanically isolated paths, independent ground planes, and mechanical interlocks, preventing unintended bridging of signal and power circuits.
Skid installation: chemical dosing skids and skid junction boxes	Skid control wiring shall be physically segregated from chemical dosing paths using engineered barriers that prevent actuator commands from propagating into chemical systems without hardware verification.
Panel feed: breakers and feed conductors to skid panels	Feed wiring shall implement selective isolation breakers and protected conductor routing that localizes faults and prevents loss of multiple control zones.
Control wiring and liquid-tight flexible metal conduit (LFMC) between skid and junction box	LFMC conduits shall incorporate abrasion protection, separated routing by consequence class as indicated by drawings or Owner-provided classification and termination structures, enabling localized isolation without disrupting system stability.
Preservation of hardwired logic (pump run status to analyzer solenoid)	Hardwired safety circuits shall include independent mechanical interlocks, ensuring critical safety behaviors operate correctly even under PLC failure, digital manipulation, or comms loss.
Engine control panel replacement	Engine panels shall enforce safe-state defaults through mechanical override logic, spring-return mechanisms, and independent feedback verification paths.
Conductor bundles (specified quantities routed)	Bundles shall be physically segregated to isolate power, sensing, and control circuits, with mechanical shielding preventing heat, abrasion, or electromagnetic coupling across conductors.
Local E-stop wiring (redundant pairs)	E-stop circuits shall use physically separated redundant paths, engineered to ensure no single mechanical or intentional action can disable both channels simultaneously.
Junction box penetrations (top entry for PLC, bottom for field devices)	Penetrations shall maintain top-entry for PLC/control wiring and bottom-entry for field wiring to create engineered moisture, strain, and cross-circuit contamination barriers.
No splices in designated junction boxes/conduit runs	Conduit and wiring routes shall remain splice-free to maintain engineered isolation, reduce latent failure points, and support straightforward consequence tracing.
Panel schedules: update and deliver as-installed schedules	Schedules shall identify the zoning and isolation identifiers used in the drawings, engineered isolation points, and physical fail-safe paths supporting operational and forensic clarity.
Temporary power for critical monitoring/analyzers	Temporary power shall include engineered bypass limits, reverse-feed protections, and fail-safe disconnects, ensuring analyzers cannot energize unintended loads.

Cabling test deliverables: CAT6 wire map, fiber OTDR/IL	Test documentation shall provide isolation diagrams, engineered protection validation, and proof of physical separation rather than functional testing alone.
Panel FAT/SAT support and bench validation	FAT/SAT shall include consequence-focused hardware tests validating isolation, fail-safe behavior under loss scenarios, and mechanical containment of unsafe conditions, with objective evidence suitable for Owner acceptance.
I/O and continuity checks before Owner programming	Testing shall demonstrate safe default behavior under open-circuit, short-circuit, or noise-induced conditions, proving no unsafe actuation can result from signal corruption.
As-built documentation and O&M deliverables	As-builts shall incorporate mechanical isolation diagrams, consequence-class mapping as provided by the Owner and Engineer, and engineered fail-safe descriptions tied to each circuit.
Interlocks: mechanical and electrical safety interlocks, door switches	Interlocks shall be purely hardware-enforced, independent of digital control paths, ensuring safety functions operate under digital compromise.
Requirement	New Requirement
Consequence-class designation for all circuits	All circuits, panels, and conduits shall be assigned consequence classes by the Owner and Engineer, and the Contractor shall apply the corresponding physical labeling, isolation practices, and protective barriers scaled to the potential impact of failure.
Independent mechanical fail-safes for actuators	Critical actuators shall include mechanical stops, spring-return designs, or other hardware mechanisms forcing safe-default behavior without reliance on PLC logic.
Bidirectional physical verification of sensor data	High-consequence measurements shall be validated using independent physical sensing types (e.g., pressure + ultrasonic + float) to prevent unsafe actuation from corrupted readings
Physical interdependency mapping	The Contractor shall provide as-built dependency inputs (I/O lists, panel to field termination mapping, network drop demarcations, and power dependency annotations) to support the Owner and Engineer interdependency evaluation performed as part of the design and commissioning process.
Degraded-mode operational profiles	Systems shall include engineered operational modes defining safe mechanical behavior during PLC loss, comms disruption, sensor failure, or actuator jamming.
Control containment zones	Control system components shall be grouped into engineered containment zones enabling localized shutdown, fault blocking, and isolation of abnormal behaviors.
Mechanical event-logging points	Panels and enclosures shall include nondigital forensic features such as mechanical counters, tamper markings, and physical stroke indicators that preserve event history without relying on electronic systems.

FAT/SAT fault-injection tests	FAT/SAT shall include mechanical fault-injection (sensor miswiring, cable failure, actuator jam simulation), demonstrating engineered containment and safe-state transitions.
Engineered isolation for Owner-furnished equipment	Owner-furnished equipment devices shall be integrated using mechanical isolation barriers, independent grounding, and protected cabling interfaces, eliminating shared-failure modes, and shall preserve Owner chain of custody through documented handoff records.
Physical documentation control	All documentation shall use controlled distribution markings and transfer procedures, ensuring integrity independent of digital storage consistent with Owner engineering information control practices.

3.6. Cyber-Informed Engineering Requirement Management

Cyber-informed engineering requirement management will serve as the central mechanism for maintaining alignment between engineering, cybersecurity, and operational safety throughout the SCADA modernization life cycle associated with the contractor-facing specification set. Each specification, particularly those refined or added through the CIE framework, will be managed in a structured requirements repository that links every requirement to its associated CIE principle, applicable subsystem (panel wiring, instrumentation, networks, controls), and expected consequence mitigations. As operational evidence accumulates during panel fabrication, field installation, network turn-up, and FAT/SAT validation, these requirements will be iteratively updated to reflect real-world system behavior and newly identified digital-physical interactions while preserving the boundary that configuration, policy, and operational risk decisions remain Owner and Engineer responsibilities.

For example, if SAT testing reveals that pump or well-control interlocks do not maintain safe-state behavior under degraded telemetry or SCADA polling delays, the associated engineered-control requirement will be revised to strengthen hardware independent protections and local defaults that are implementable within the contractor deliverables, rather than relying solely on remote supervisory commands. Similarly, if communication testing identifies issues such as jitter-sensitive protocols, excessive retries on cellular backhaul, or unexpected broadcast traffic across process networks, secure information architecture requirements will be updated to tighten physical demarcations, port labeling, and handoff constraints so the Owner and Engineer can enforce deterministic pathways, protocol whitelisting, and zoning during configuration. The requirement management process will use strict traceability so every update—such as modifying panel intrusion switch logging behavior, adding tamper-evident wiring documentation, refining fiber OTDR deliverables, or adjusting PLC-to-instrument signal validation—is explicitly tied to both a CIE mitigation and the supporting cybersecurity mechanism, with clear attribution of who implements each change (contractor versus Owner and Engineer).

This CIE-driven management approach ensures updates are not introduced merely as generic security hardening but are directly targeted to reduce digital pathways to high-consequence events identified in Owner and Engineer consequence mapping and risk decisions such as loss of chemical dosing control, uncontrolled pump operation, reservoir overfill, or failure of critical instrumentation. By continuously aligning requirements with field performance, vendor component updates, engineering discoveries, and site-specific operational lessons, the CIE requirement

management process maintains a living, technically grounded specification that evolves to support safe, resilient, and cyber-informed SCADA deployment across the entire program life cycle.

4. Conclusion

This report demonstrates the practical application of the CIE Requirements Framework to two representative use cases—a BESS and a SCADA improvement program—to illustrate how engineering processes can be intentionally structured to reduce cyber-physical risks. By integrating cybersecurity considerations directly into the requirements phase, the framework transforms cybersecurity from a reactive layer of protection into a proactive element of system design. The structured classification of requirements by functional type and digital impact (direct, indirect, or no digital impact) enables a disciplined prioritization of engineering controls where digital compromise could have the most severe operational consequences.

The BESS use case highlights how CIE principles can identify high-consequence digital dependencies leading to engineering design decisions that minimize unsafe failure modes and maintain operational integrity under degraded or compromised conditions. Similarly, the SCADA improvement program demonstrates the value of CIE-driven analysis in guiding refinements such as improved isolation of digital pathways, validated signal processing, and engineered fail-safe configurations. These results confirm applying the CIE Requirements Framework produces tangible engineering benefits, including reduced attack surface, improved consequence visibility, and stronger alignment between cyber resilience and operational performance.

Overall, the findings affirm CIE provides a repeatable, scalable methodology for embedding cybersecurity awareness into the engineering life cycle of critical infrastructure. By treating cyber risk as an engineering design parameter, organizations can systematically "engineer out" vulnerabilities before systems are built, tested, and deployed—resulting in more resilient and secure operations. The work further reinforces the importance of multidisciplinary collaboration between engineers, operators, and cybersecurity professionals to ensure CIE principles are not only conceptually understood but practically implemented.

References

[1] "Cyber-Informed Engineering," Energy.gov. Accessed: Oct. 28, 2025. [Online]. Available: https://www.energy.gov/ceser/cyber-informed-engineering

[2] V. L. Wright *et al.*, "Cyber-Informed Engineering Implementation Guide," Idaho National Laboratory (INL), Idaho Falls, ID (United States), INL/RPT-23-74072-Rev000, Sep. 2023. Accessed: Oct. 28, 2025. [Online]. Available: https://www.osti.gov/biblio/1995796

[3] S. Etigowni, R. Macwan, and J. Welsh, "Requirements Framework for Cyber-Informed Engineering," National Renewable Energy Laboratory (NREL), Golden, CO (United States), NREL/TP--5T00-90317, Jan. 2025. doi: 10.2172/2497726.

[4] P. Yockey *et al.*, "Cyber-Informed Engineering Validation Methods and Guidance," INL/MIS--24-81700-Rev000, 2480931, Sep. 2024. doi: 10.2172/2480931.

[5] S. D. Chanoski, "Applying Cyber-Informed Engineering to Power System Operations".

[6] "Engineering Cyber Resilience for the Water Sector Security BSides Las Vegas 2025." Accessed: Apr. 27, 2026. [Online]. Available: https://pretalx.com/security-bsides-las-vegas-2025/talk/EAYEJC/

[7] V. L. Wright and M. Sachs, “Engineering-In Cybersecurity”.
[8] D. Saebeler, D. Emmerich, C. O’Brien, and E. Rogers, “University of Illinois Urbana-Champaign”.
[9] R. G. Cooper, “The S tage- G ate® Product Innovation System: from Idea to Launch,” in *Wiley Encyclopedia of Management*, 1st ed., C. L. Cooper, Ed., Wiley, 2015, pp. 1–13. doi: 10.1002/9781118785317.weom130024.
[10] *idaholab/CIEBAT*. (Mar. 19, 2026). Idaho National Laboratory. Accessed: Apr. 27, 2026. [Online]. Available: https://github.com/idaholab/CIEBAT
[11] *NatLabRockies/CIEPAT*. (Feb. 11, 2026). National Laboratory of the Rockies. Accessed: Apr. 27, 2026. [Online]. Available: https://github.com/NatLabRockies/CIEPAT
[12] *NatLabRockies/CIECAT*. (Feb. 11, 2026). National Laboratory of the Rockies. Accessed: Apr. 27, 2026. [Online]. Available: https://github.com/NatLabRockies/CIECAT
[13] V. Wright and B. Lampe, “Cyber-Informed Engineering Workbook: ADMS,” INL/EXP--24-80782-Rev000, 2453879, Sep. 2024. doi: 10.2172/2453879.
[14] A. Ribeiro *et al.*, “CIE and CCE methodologies can deliver engineered industrial systems for holistic system cybersecurity,” Industrial Cyber. Accessed: Apr. 27, 2026. [Online]. Available: https://industrialcyber.co/features/cie-and-cce-methodologies-can-deliver-engineered-industrial-systems-for-holistic-system-cybersecurity/
[15] *idaholab/CIE_EC_Database*. (Mar. 16, 2026). Idaho National Laboratory. Accessed: Apr. 27, 2026. [Online]. Available: https://github.com/idaholab/CIE_EC_Database
[16 B. Lampe, E. Stewart, R. Stolworthy, and M. Culler, “Cyber-Informed Engineering Approach to Mitigating BESS Supply Chain Concerns,” in *2025 IEEE Power & Energy Society General Meeting (PESGM)*, Jul. 2025, pp. 1–5. doi: 10.1109/PESGM52009.2025.11225654.
[17] “DOE/ID-Number.” Accessed: Apr. 27, 2026. [Online]. Available: https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_150841.pdf
[18] V. Wright and B. Lampe, “Cyber-Informed Engineering Workbook: CIE Hands-On Training,” INL/CON--24-78304-Rev000, 2371031, May 2024. doi: 10.2172/2371031.

Cyber-Informed
Engineering