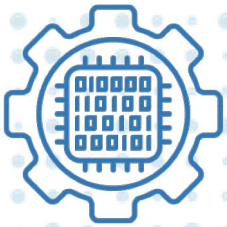
DISCLAIMER

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



Cyber-Informed Engineering

Integrating Cyber-Informed Engineering into Process Automation

September 30, 2025

Authors:

Benjamin Lampe
Idaho National Laboratory

Russell Gold
Idaho National Laboratory

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.

Contents

1. Introduction

Many organizations are increasingly automating their core missions and the delivery of essential functions to address business risks and improve business efficiency. Process automation, which involves running processes with minimal or no manual intervention, can significantly influence an organization's cyber-risk landscape. While process automation produces efficiencies, it also introduces new cyber risks if not properly managed.

Cyber-Informed Engineering (CIE)[1] offers a proactive approach to managing these digital risks. This document aims to support organizations in applying CIE to enhance their cyber-resilience for process automation to ensure these risks are addressed and mitigated. The approach presented can be implemented independently to boost any organization's cyber-resilience, ensuring that the benefits of automation do not lead to unnecessary or unmitigated digital risks. It provides a starting point and considerations for organizations to integrate CIE principles and practices. CIE is an iterative process, enabling continuous improvement and reinforcing the engineering and operations cultures of an organization for digital risk.

This document is organized as follows: Section 1 provides background on CIE, process automation, and their integration. Section 2 examines the twelve CIE principles in the context of process automation, outlining key questions, engineering considerations, and implications for managing digital risk. Section 3 concludes with a synthesis of findings and recommendations to advance resilience by design.

1.1. Background on Cyber-Informed Engineering

The CIE Implementation Guide[2] describes CIE as an extension of "secure-by-design" concepts beyond the digital realm to include the engineering of cyber-physical systems. More importantly, CIE keeps the consequences of cyber-attack from impacting the safety, reliability, and performance of engineered systems. CIE introduces digital risk considerations at the earliest stages of system design, long before the incorporation of software and information security controls or mitigations. It calls on engineers to identify engineered controls and design choices that could eliminate avenues of attack for cyber actors or minimize the damage they could inflict.

CIE expands cybersecurity and cyber-resilience decision making by incorporating the engineering disciplines, not by asking engineers to become cyber experts, but by calling on engineers to apply engineering tools and make decisions that improve cybersecurity outcomes. CIE examines the engineering consequences that a sophisticated cyber attacker could achieve and drives engineering changes that may provide deterministic mitigations to limit or eliminate those consequences.

[1] "Cyber-Informed Engineering (CIE)," Idaho National Laboratory, n.d., https://inl.gov/national-security/cie/.
[2] Wright et al., "Cyber-Informed Engineering Implementation Guide," (Program Document) | OSTI.GOV, September 5, 2023, https://www.osti.gov/biblio/1995796.

1.2. Background on Process Automation

Process automation refers to the use of technology to execute recurring tasks or processes in a business or industrial environment where manual effort can be replaced. At its core, process automation involves the use of control systems, such as programmable logic controllers (PLCs) or robots, and information technologies to handle different processes and machinery in an industry to replace or complement human intervention. One of the fundamental concepts in process automation for control system engineers is the control loop, see Figure 1 below. A control loop is a sub-system of components that continuously monitors and adjusts a process to maintain the desired output. The basic components of a control loop include sensors that collect data from the process which provide a feedback mechanism that continually monitors the output and adjusts as necessary to ensure the process remains within desired parameters, controllers that process the data and make decisions based on pre-set parameters, and final control elements (FCEs) (i.e., actuators) that execute the instructions from the controller to adjust the process. Process automation systems are designed to optimize performance, safety, and reliability.

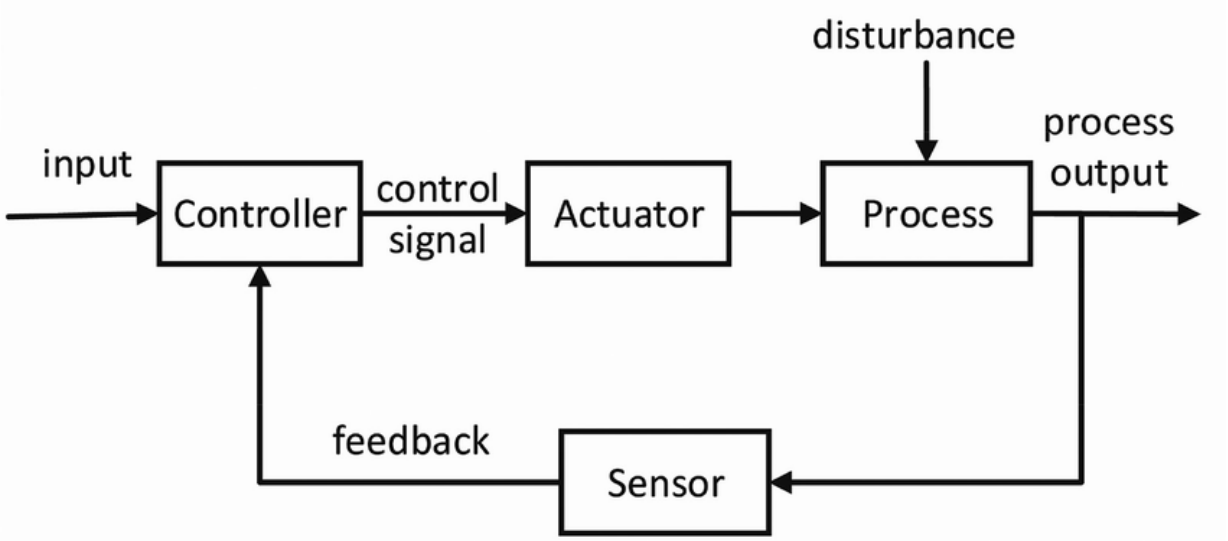


Figure 1 - Control Loop[3]

In the context of safety, process automation plays a crucial role by minimizing human involvement in hazardous environments and ensuring that dangerous processes remain within safety operating limits. Automated systems monitor and control processes with greater efficiency, precision, and consistency than humans, reducing the risk of accidents caused by human error or loss of containment. Examples of such safety mechanisms include safety interlocks and emergency shutdown subsystems, which are designed to prevent or mitigate dangerous situations.

Performance is enhanced through process automation by optimizing the efficiency and accuracy of industrial processes. Automated systems often operate at speeds and with precision that far

[3] Control Loop with Process Model, https://www.researchgate.net/figure/Control-loop-with-process-model-13_fig2_325653843.

exceed human capabilities. This provides increased productivity, higher quality products, and reduced operational costs. Additionally, automation allows for continuous operation, with a stated goal of minimizing downtime and maximizing throughput for business mission and essential functions.

Reliability is another characteristic of process automation. Automated systems are designed to perform repetitive tasks consistently without fatigue or variation, ensuring a high level of reliability in process automation operations. For instance, predictive maintenance, enabled by data analytics and monitoring, allows for the early detection of potential issues before they lead to equipment failure as well as improved work planning and performance over traditional preventative maintenance approaches.

The use of digital technology is integral to modern process automation, providing new tools and infrastructure for increasingly sophisticated control systems. The advent of digital technology has enabled the development of advanced sensors, more powerful and intuitive controllers, and intelligent actuators, all of which have the stated goal to contribute to more effective and efficient automation processes. Digital technology also supports real-time data collection and analysis, empowering organizations to make informed decisions quickly and accurately. However, the increased reliance on digital technology introduces new cyber and digital risks, as automated systems become potential targets for cyberattacks. The resulting impacts on safety, performance, and reliability from adversarial disruptions can threaten a business's mission and essential functions. Therefore, these risks must be analyzed and addressed through CIE.

1.3. Integration of Cyber-Informed Engineering and Process Automation

The integration of CIE and process automation is necessary in navigating the complexities of digital transformation within industrial environments. As components, data elements, and other key areas of the control loop become increasingly digitized, CIE provides a methodology directed at questioning and assessing digital risks. By embedding cyber considerations early in the design phase, CIE enables organizations to identify potential design vulnerabilities and make informed design changes sooner rather than later in the lifecycle. For systems that are already built, CIE offers valuable insights for retrofitting existing infrastructure or establishing new resilient infrastructure to mitigate digital risks brought on by cyber threats. Additionally, CIE equips organizations with the knowledge to understand the trade-offs associated with accepting certain digital risks, ensuring that these decisions are made with an awareness of their potential impact on safety, reliability, and performance. This proactive approach not only enhances the security posture of automated processes but also fosters a culture of continuous improvement and resilience in the face of evolving cyber threats.

2. Principle Analysis

The following section provides descriptions of and considerations for each CIE principle and its relationship to process automation.

2.1. Consequence-Focused Design

Key Question:

How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?

Key Concepts for Engineers to Consider:

When designing a control system, engineers should reflect on the following terms to guide trade-offs and design decisions in the face of digital risks that could lead to unacceptable consequences:

- Purpose / Organization / System / Mission-Critical Functions
- Failure / Unexpected Operation / Impacts
- Loss / Instability / Subsystem

In the context of process automation, identifying critical functions within a control system is linked to understanding the control loops that govern the system's operations. As indicated above, control loops are the set of components and data elements that regulate various process variables, such as temperature, pressure, flow rate, and level, to maintain operating conditions. The relationship between control loops and critical functions is key, as these loops not only influence process performance but also determine how effectively a system can respond to disturbances and maintain safety, performance, and reliability.

As the number of control loops under consideration expands, the complexity of the critical function analysis increases, which often leads to challenges in understanding all potential interactions and dependencies. Therefore, control system engineers must carefully consider assumptions that will help strike the right balance between analytical complexity and the time available for CIE analysis.

To determine an appropriate scope of analysis, understanding the primary objectives (i.e. purpose) of the process is essential. CIE questions centered around the system purpose help draw out primary objectives of the process. This may include understanding the key performance indicators (KPIs) that are critical for the system's operation, such as quality, safety, efficiency, and reliability. By identifying the system’s purpose and associated KPIs, engineers can prioritize essential control loops, allowing them to scope down their analysis to the most impactful areas of the overall process control system.

Another important criterion for validating the scope of analysis is the degree of interaction between control loops. By assessing how various loops interact with each other and whether the functioning of one loop is dependent on another, engineers can identify cascading effects that may arise from disturbances or false actions. This in turn helps prioritize which loops warrant more in-depth investigation when time for analysis is limited.

Once the control loop(s) that represents the critical function for analysis are identified, control system engineers enumerate the key control loop variables to facilitate the discussion within the remaining CIE Principles. The following variables are enumerated:

- The *process variable (PV)* is the specific quantity measured by sensors that indicate the current state of the plant process, such as temperature, pressure, or flow rate. The feedback signal is the physical measurement of the process variable that is fed back to

the controller, essential for maintaining a closed-loop control system by continuously monitoring the process and determining the error.

- The *control variable (CV),* on the other hand, is the controller output that the controller adjusts to influence the process variable, such as the position of a valve or the speed of a motor. The manipulated variable (MV) is often used interchangeably with the control variable but represents the variable that the FCE directly adjusts to influence the process variable. The controller output (CO) is the signal generated by the controller based on the error which signals the FCE, which then adjusts the manipulated variable. This output is typically a continuous signal that drives actuators or other FCEs.
- The *setpoint (SP)* is the desired value that the process variable aims to achieve, serving as the target for the control system. This setpoint is provided by other control loops or by human intervention from the Human-Machine Interface (HMI).

Figure 2 below provides situational awareness for each of these variables in a control loop.

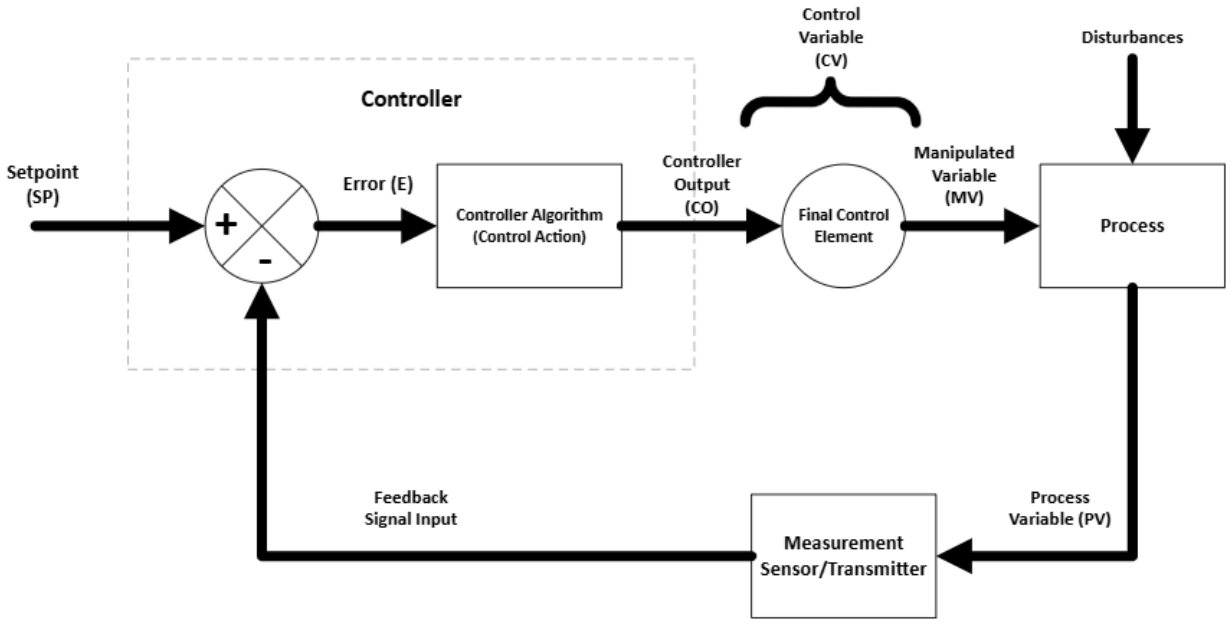


Figure 2. Control Loop Variables

In more advanced control systems, a feedforward signal is often utilized to refine the controller output by anticipating changes in the process before they occur, based on known disturbances or setpoint changes. In a cyber-informed context this is an important concept for consideration when identifying opportunities for engineered controls (i.e., principle 2) because false setpoints or malicious adjustment of control actions or feedback signals represent a new type of disturbance to the process system. Feedforward signals allow the controller or FCE to make proactive adjustments to the manipulated variable, minimizing the impact on the plant process.

The cyber threats that control system engineers face in relation to control loops for modern control systems are illustrated in Figure 3 below.

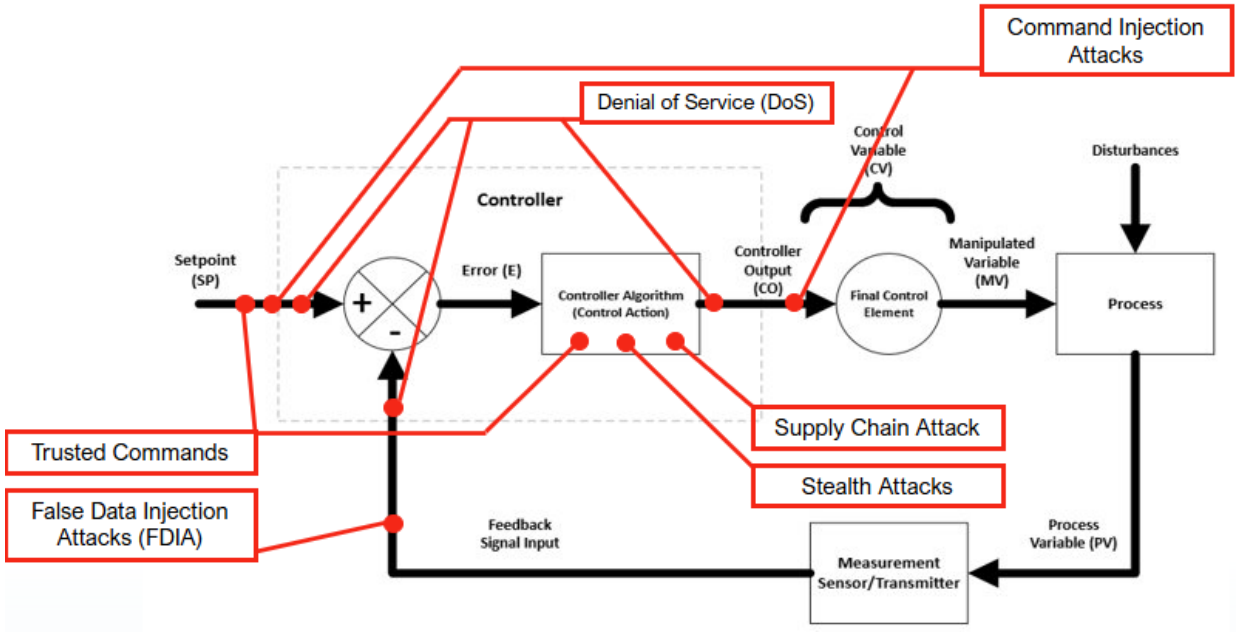


Figure 3. Control Loop Cyber Threats

- Control loop threats often target three main areas of a control loop's input-operation-output dynamic. Threats can: **Alter inputs** in order to change the controller algorithm (operation) response (i.e. FDIA, Trusted commands, DoS, etc.),
- **Fundamentally rewrite the controller algorithm** (operation) response (i.e. supply chain attack, stealth attacks, etc.), or
- **Modify the command** (output) actuation executed by the system (i.e. command injection attacks, DoS, etc.).

Each threat presents a unique opportunity for control system engineers to determine how they might orchestrate the control loop to ensure resilience even if the threat is realized, in order to limit the impact to performance, safety, or reliability. Specifically, in response to these threats, control system engineers must give special attention to control algorithm parameters, such as proportional gain, integral time, and derivative time in a Proportional-Integral-Derivative (PID) controller if utilized, pre-defined rules like interlocks, or more advanced state space models because they define how the controller responds to the error and are crucial for tuning the control system to achieve optimal performance, prevent unsafe actions, or ensure reliability.

This analysis of a control loop often becomes more complex because not all control loops operate within a single-input-single-output (SISO) configuration as indicated above. Many industrial processes rely on multi-input-multi-output (MIMO) control loops, where multiple input variables and output variables interact simultaneously. In such systems, the inputs and outputs are interdependent, meaning a change in one variable can affect several others, making the control and optimization of the process more challenging.

To address undesired consequences, especially those stemming from cyber threats, three key relationships must be rationalized:

- The identification of PVs is necessary to relate to the associated hazards. They are not only indicative of the process's current state to understand performance impacts but also essential to understand safety impacts from potential hazards that could arise if these variables deviate from their desired ranges.
- The effect of the control variable provided by the FCEs, such as actuators, valves, and pumps, and its role in manipulating these process variables. By adjusting the FCEs, engineers can influence the PVs to maintain optimal operating conditions despite cyber risks.
- The strength and integrity of the containment mechanisms that are in place. Containment refers to the physical boundaries that prevent the escape or release of hazardous materials or energies associated with the process. This can include piping systems, storage tanks, walls, wiring, and other structural elements designed to ensure that the process remains safely contained.

Traditionally, understanding the relationship between PVs, FCEs (i.e. the extent of the MV), and containment strength is essential for identifying the types of hazards involved in a process automation system. This relationship is already the basis for existing functional safety analysis methodologies such as Failure Modes and Effects Analysis (FMEA), Hazard and Operability Study (HAZOP), and Process Hazard Analysis (PHA). In a cyber-informed sense, however, the influence of digital threats to this relationship influences the CIE additions to hazard analysis for a process control system. Undesired consequences occur at the intersection of these three variables. Once identified and documented, they form the basis for addressing the remaining CIE principles. For example, if a process variable like pressure exceeds safe limits due to cyber manipulation, the risk of hazardous events, such as a digitally-induced rupture or leak, increases. This risk is significant, especially if containment strength is inadequate or degraded, reducing its lifecycle.

2.2. Engineered Controls

Key Question:

How do I select and implement controls to reduce avenues for attack or the damage that could result?

Key Concepts for Engineers to Consider:

When designing a control system, engineers should reflect on the following terms to guide the use of engineering-based design and control mechanisms (Engineered Controls) that mitigate the consequences of cyber threats on safety, reliability, and performance requirements:

- Hierarchy of Controls
- Physics / Energy Sources
- Dependent on Digital Technologies
- Safety controls / Fail-safe
- Analog / Physical
- Effectiveness

Selecting and implementing engineering controls to reduce avenues for attack or minimize potential damage in process automation systems is the unique opportunity provided to control system engineering beyond the information security protections considered by cybersecurity professionals. These engineering controls introduce a new category of security countermeasures for minimizing the digital risk within the control loop of a control system.

Even if the information protection security controls (i.e. IEC/ISA 62443[4]) are compromised, engineering controls can limit or mitigate the digital risk by controlling the impact. For instance, the extent and methods to which the FCEs can be manipulated and the limits to the containment strength can provide a feedforward signal by Control System Engineers to positively alter how effectively the control loops can respond to the cyber threats against the preceding variables, like setpoints, error, control actions, and controller outputs. Additionally, rethinking the strength of the containment provides a physical barrier against the intelligent consequences.

Incorporating fail-safes and automatic shutdown mechanisms is another example derived from safety engineering (i.e., IEC 61508[5]/61511[6]). Engineers can design systems that automatically initiate safe shutdown procedures or revert to a secure state when anomalous behavior is detected. This approach minimizes potential damage during an incident while preserving system integrity and safety expectations.

Additionally, control system engineers can incorporate new monitoring and diagnostic capabilities as engineering controls to improve the decisions by other CIE principles such as Principle 3 (Secure Information Architecture) and Principle 6 (Active Defense). For example, introducing multiple feedback signals provides visibility into system performance and operational parameters and engineers using a 2oo3 (two out of three) voting mechanism can detect unusual activities or deviations from normal operations early. This allows for prompt intervention before a situation escalates into a more significant issue.

The challenge with engineered controls lies in their scalability, as they are often designed for specific situations. Generally, three archetypes describe engineers' ability to respond to digital risk with engineered controls:

- Direct Replacement – Replaces the current digital logic operations of the control loop or parts of the control loop with physical logic mechanisms, removing them from the adversarial view.
- Redundancy Mechanisms – Integrates a physical logic mechanism with the digital logic operations using logical primitives (i.e. AND, OR, etc.) or some method of switch mode fail-over which is a form of dynamic compensation.
- Boundary Mechanisms – Provides physical threshold checks and responses to reinforce lower boundaries configured in digital logic operations.

[4] "ISA/IEC 62443 Series of Standards - ISA," isa.org, accessed September 8, 2025, https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.
[5] "IEC 61508," Wikipedia, June 2, 2025, https://en.wikipedia.org/wiki/IEC_61508
[6] "IEC 61511," Wikipedia, October 2, 2024, https://en.wikipedia.org/wiki/IEC_61511

2.3. Secure Information Architecture

Key Question:

How do I prevent undesired manipulation of important data?

Key Concepts for Engineers to Consider:

When designing a control system, engineers should reflect on the following terms to guide integration with a larger network architecture that communicates process information:

- Network connectivity
- Key Data elements
- Communicate / Exchanges of Information
- Validate / Verify / Monitor
- Diagnose / Anomalies
- Zones / Boundaries
- Operating Modes – Adverse / Extraordinary

Traditionally, control system engineers aim to prevent communication loss or errors from affecting operations. For example, in a distributed control system (DCS), if a controller receives state information, such as the running status of motors, the input validation logic ensures that if a motor stops, a certain pressure level is present. If not, the system responds to maintain safety. However, this expectation changes with the cyber threat of data manipulation.

In both scenarios, a detailed understanding of network connectivity and the specific communication of control loop data elements between the controller and Human-Machine Interfaces (HMI) or historians is essential. Traditional cybersecurity practices, like IEC/ISA 62443, use data flow diagrams organized in zones and conduits to prevent data manipulation. Including control system engineers in information assurance discussions by adopting CIE questions ensures that data flow sensitivity to manipulation is properly assessed.

In practice, the control system engineer configures the data elements or tags within the controller. This often involves defining the data type, tag name and/or memory address, and specifying whether the data is to be sent or received from other devices as part of the logic operations. Controller Messaging Protocols, like EtherNet/IP (CIP over TCP/IP) or ModbusTCP, are typically used to facilitate these communications. From a CIE perspective, a couple of key practices contribute to securing against the manipulation of data elements.

First, engineers should evaluate the read and write capabilities of each data element. The default may be that the data element is both read-and-write capable, but if the data element is never meant to be written to the network message blocks, then the engineer should enforce a read-only behavior. This protects against a number of network-based cyber threats like FDIA.

Next, engineers should classify data elements based on their importance to the operations and potential impact if manipulated. High-importance elements, such as alarm tags or write-based function codes, should receive the most stringent information security measures.

When engineers convey the sensitivity level of each data element, cybersecurity teams can tailor their monitoring, detection, and response actions as part of the larger secure information architecture response. Given the constraints of time and budget in the organization's cybersecurity program, security measures must focus on protecting the most critical data elements.

From the cybersecurity perspective, this is often achieved through network segmentation (i.e., zones and boundaries) and the configuration of Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) systems. Integrating this perspective from control system engineers allows these tools to be configured to monitor and protect critical data elements, while non-critical data elements receive implied protection from the overarching security architecture.

In addition to configuring data elements accessibility, the cyber-informed control system engineer should include logical mechanisms, like communication status, to validate, verify, and monitor data exchanges within their controller's logic. More specifics on this in Active Defense and Planned Resilience Principles, see Section 2.6 and 2.10 below, respectively.

2.4. Design Simplification

Key Question:

How do I determine what features of my system are not absolutely necessary to achieve the critical functions?

Key Concepts for Engineers to Consider:

When designing a control system, engineers should reflect on the following terms to guide decisions that prioritizes only the minimum features necessary for the robust and successful delivery of the control loop:

- Minimum Capabilities / Implemented Digitally
- Redundant Features
- Regulations / require inclusion
- Features / Certain points in lifecycle
- Simpler device / non-digital / simplify design
- Conflict / trade-offs
- Traceable / Requirements
- Unneeded

Engineers utilize design processes and risk management methods, such as Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), etc., along with requirement traceability, to verify the minimum required components in a design. What changes in this modern age of commercial-off-the-shelf solutions is that components often come with features that exceed what is truly required for the system's operation. For example, a controller often offers multiple communication modes, but only one of those modes is configured and deployed in actual operations of the control loop and larger control system.

Through the design simplification principle, the engineer, aware of digital asset capabilities from Digital Asset Awareness, Section 2.8 below, categorizes the component capabilities into three areas: expected, redundant, and/or unused. Expected capabilities are those required to provide the required ingredients to the control loop. Redundant capabilities are viewed in two ways, one of which is that the capability already exists elsewhere and is not needed or is that the capability already exists and is used to provide fail-over or a voting mechanism in the operation of the control system. Finally, unused capabilities are ones that exist but are not used in the operation of the control system. Engineering out unused or redundant capabilities minimizes the attack surface by reducing the number of features that could potentially be exploited by adversaries. The control system engineer, through Principle 4 (Design Simplification) questioning, can evaluate redundant features and determine if they are necessary for the system's safety, reliability, or performance requirements. If redundant features are not essential, they should be eliminated to simplify the design and reduce potential vulnerabilities. For example, control system engineers often deploy variable frequency drives to provide energy efficiency for pumping and other motor operations. Many newer Variable Frequency Drives (VFDs) require configuration and diagnostics through a software application tool. This introduces cyber susceptibility where the engineer might question, “What if an adversary through a maintenance contract changed the expected settings of this device, am I prepared for the impact of that reconfiguration?”, and “Can I do anything about that?” Considering alternate VFDs, which may be able to reduce the digital risk in that technology may choose to deploy a VFD which allows for configuration through physical DIP switches present on the VFD itself or changing the design to use a motor starter or a Direct-on-Line configuration if the trades off within the safety, reliability, and performance between these possible solutions are tolerable. Access to these configuration elements can be controlled physically, and while not fool-proof, changes the digital risk conversation available to the engineer.

Engineering is based on trade-offs, and ensuring compliance with regulations that mandate the inclusion of specific features is crucial in these types of analyses. Additionally, features that are only needed during specific phases, such as installation or maintenance, should be deactivated or removed during normal operations to enhance security. Whenever possible, the engineer should consider opting for simpler, non-digital devices that fulfill the required functions. Simplifying the design by using non-digital components can significantly reduce the attack vectors available to adversaries. When changes are made to the system, engineers are expected to maintain traceability of requirements throughout the design process and ensure that every feature included is justified and necessary for achieving critical functions. This helps in identifying and removing unneeded features and is co-opted for this CIE Principle.

Engineers should identify non-essential features for the system's critical functions, communicate them to others, and eliminate them. For example, if a controller offers multiple communication modes but only one is used, selecting a component that only includes the required mode reduces the risk of adversaries exploiting unused features. If certain features cannot be removed, understanding their presence helps communicate them to cybersecurity professionals to inform the Secure Information Architecture monitoring approach, see Section 2.3 above. By knowing which features are not actively used, engineers can set up monitoring systems to detect

any unexpected use of these features, which may indicate possible cyber activity in the engineered system.

This principle implemented by control system engineers minimizes potential vulnerabilities, making it harder for adversaries to exploit unused or redundant features. Successful implementation of design simplification requires a thorough understanding of the system's requirements, careful assessment of each feature's necessity, and ongoing communication with cybersecurity professionals to ensure the system remains secure throughout its lifecycle.

2.5. Layered Defenses

Key Question:

How do I create the best compilation of system defenses?

Key Concepts for Engineers to Consider:

When designing a control system, engineers should reflect on the following terms to guide the implementation of cybersecurity and engineering countermeasures:

- Engineered controls / enterprise IT defenses
- Independent / redundant defenses
- Single / common points of failure
- Key elements / interactions
- Component level / system level
- Ensure effectiveness

Creating the compilation of system defenses in process automation systems requires a two scoped approach that integrates multiple layers of security for the control system and system-wide engineering practices. Cyber-informed control system engineers can focus on several key strategies to ensure comprehensive protection against potential threats and vulnerabilities. Figure 4 demonstrates the types of traditional cybersecurity features available at the controller to ensure the configuration file and the operations of the controller are state-fully managed, and the exposure resulting from the use of a computer (i.e., Programmable Logic Controller) to run the control loops maintained within the configuration is minimized.

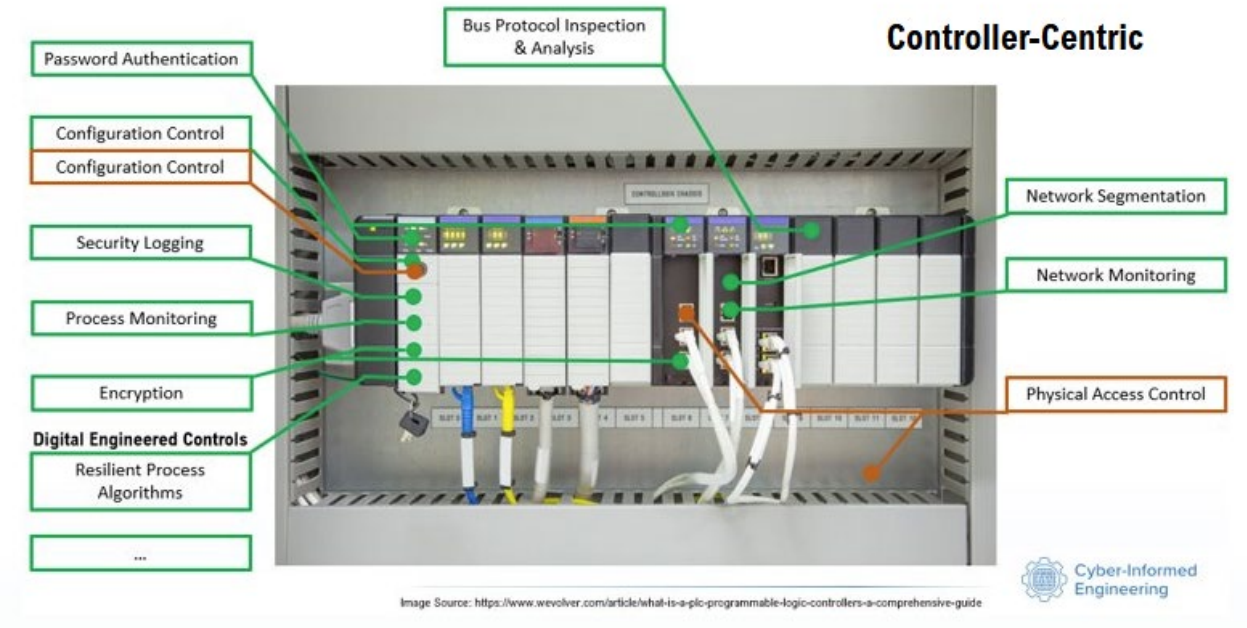


Figure 4. Controller-Centric Layered Defenses[7]

A special type of digital protection is the resilient process algorithm exclusive to the engineer. The control system engineer's design of logical operations can provide resilient characteristics and mitigate certain threat types like input or output manipulation. However, it remains susceptible to attacks against the direct logic operations like supply chain attacks. This is an example of an engineered control for addressing digital risk in modern control systems.

To advance this approach, control system engineers should consider opportunities for layered defenses from a system-wide perspective. Figure 5 depicts using physical mechanisms to limit or control the impacts that may result from adversarial manipulation of the control loop. These types of system-wide protection are the unique result of cyber-informed engineers contributing to the system's protection.

[7] Shreyas Sharma, "What Is a PLC (Programmable Logic Controllers): A Comprehensive Guide," Wevolver, August 29, 2024, https://www.wevolver.com/article/what-is-a-plc-programmable-logic-controllers-a-comprehensive-guide.

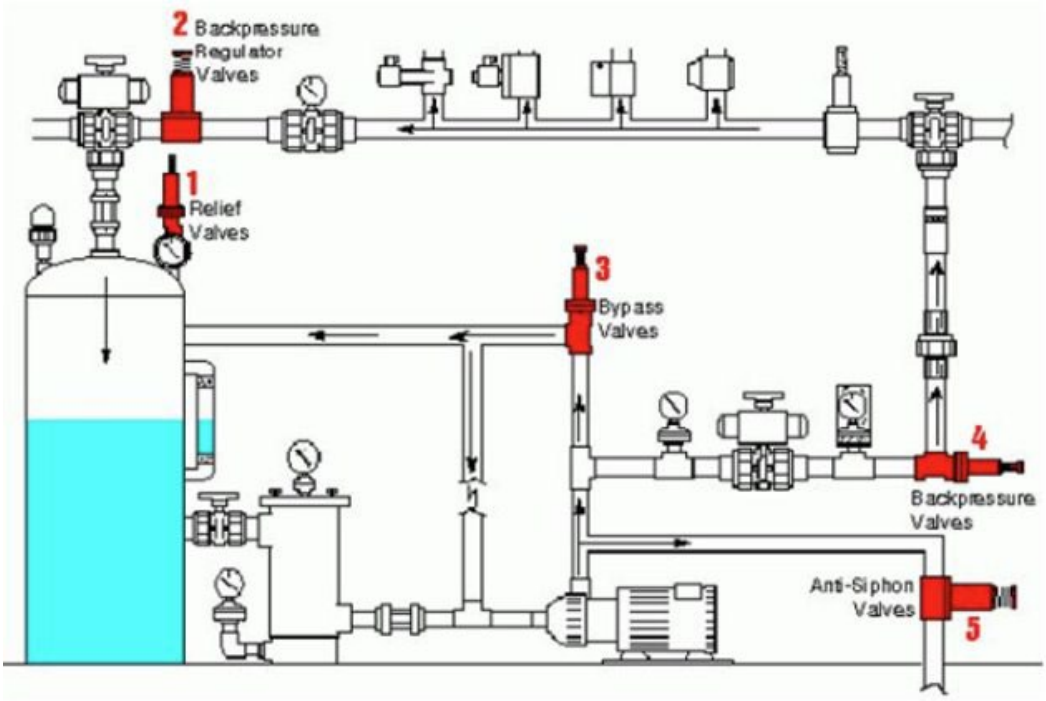


Figure 5. System Wide Protections[8]

Implementing the CIE Principle 5 questioning, control system engineers enable layered defenses against digital threats to be implemented digitally and physically. When thinking about the compliance required by the Risk Management Framework (RMF) through the National Institute of Standards and Technology (NIST) special publication series[9,10,11] with items such as Authorization to Operate (ATO), taking credit for information security and engineered controls in order to authorize the operation of an engineered system demonstrates a higher maturity by an organization in its cybersecurity response to digital risks. Mitigating digital risk through traditional cybersecurity and engineering protections represents the future of cybersecurity. A cyber-informed engineering mindset is essential to coordinate this multi-layered response.

[8] Sachin Thorat, "Pressure Relief Valve - Diagram , Working," Mechanical Engineering blog, February 18, 2020, https://learnmech.com/pressure-relief-valve-diagram-working/.
[9] Joint Task Force, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," CSRC, December 20, 2018, https://csrc.nist.gov/pubs/sp/800/37/r2/final.
[10] Joint Task Force Transformation Initiative, "Managing Information Security Risk: Organization, Mission, and Information System View," CSRC, March 1, 2011, https://csrc.nist.gov/pubs/sp/800/39/final.
[11] Joint Task Force, "Security and Privacy Controls for Information Systems and Organizations," CSRC, December 10, 2020, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

2.6. Active Defense

Key Question:

How do I proactively prepare to defend my system from any threat?

Key Concepts for Engineers to Consider:

When designing a control system, engineers should reflect on the following terms to guide operations that prioritize cyber-conservative approaches:

- Precursor Events / At-risk functions
- Temporary Operational Changes
- Expected system states / deviations
- Troubleshoot / Diagnosis Process Anomalies
- Contingency Plans

Applying the Cyber-Informed Engineering (CIE) principle of active defense, control system design must prioritize proactive measures that mitigate the consequences of cyber threats before they can compromise safety, reliability, or performance. A cyber-informed control system engineer can look at methods such as involving defensive logic directly into the controller's logic (see resilient process algorithms from Layered Defense section above), enabling a cyber-conservative approach to engineering process automation against cyber threats.

At the foundation of this principle is the identification and monitoring of precursor events and at-risk functions—indicators that may signal potential vulnerabilities or early-stage anomalies. Since control system engineers have the responsibility over control logic, and by incorporating these triggers into control logic, the system can autonomously detect deviations and initiate precautionary actions before a threat escalates. Or if supply chain threats are too risky, positioning these precautionary actions are manual mode actions is another response available to control system engineers in facilitating this principle here.

Good engineering ensures systems accommodate temporary operational changes which allows transitions into predefined safe states when threat conditions arise. Threats in traditional engineering have been hazards and other safety conditions as well as reliability conditions like equipment failure. But when considering digital threats, this is even more heightened for control system engineers, even for safety functions which now rely on digital technology for effective operations. Establishing expected system states and acceptable deviations equip control logic and operators alike with a clear baseline, facilitating anomaly detection and contextual understanding during abnormal cyber threat behavior.

In the event of a deviation or anomaly in a process system, integrated diagnostics become essential. For example, these can include streamlined access to system information data such as PLC scan details, controller error codes, and I/O state metrics, which support efficient troubleshooting and process anomaly diagnosis, but for the control engineer, these also represent new logic decisions that can be integrated into the decisions on whether to execute an output or not. By presenting these options within the operational context, engineers and

operators can maintain situational awareness and execute informed decisions with reduced latency which is crucial when heightened threat activity is present.

On the same level as integrating logic and response within the control system are the contingency plans. Cyber-informed engineers have the opportunity to ensure these plans emphasize Hand-Off-Auto (manual mode) capabilities, especially around control system outputs, ensuring operational continuity even when automated systems are degraded. The CIE questions in this principle help to ascertain whether regular practice of local manual operation, supported by detailed procedural documentation is effective and whether these options equip field personnel with the necessary skills and confidence to maintain control in the absence of networked oversight of modern control systems.

To reinforce this cyber-resilient posture, several key engineering active defense practices are integrated by this principle. By embedding these active defense capabilities into control systems as early as the design phase, engineers ensure that operations remain safe and dependable even under cyber threats to the control loops:

- Alarm management with local indications provides immediate feedback on state deviations, enhancing response time.
- Operational logic integration of system information such as scan times, errors, and I/O status ensures deep visibility into system health.
- Communication state awareness, embedded in logic sequences, highlights link integrity and communication disruptions.
- Manual mode operation features enable seamless transitions between automated and manual control.
- Routine manual operation drills and comprehensive documentation foster readiness in isolated or compromised conditions.

2.7. Interdependency Evaluation

Key Question:

How do I understand where my system can impact others or be impacted by others?

Key Concepts for Engineers to Consider:

When designing a control system, engineers should reflect on the following terms to understand how the use of digital technology relates to the dependencies within the and outside of the control system:

- Dependencies / organizations / subsystems / services / infrastructures
- Critical Inputs
- Alternative sources
- Upstream / downstream / external / internal
- Cascading failures
- Third-parties

Understanding where a process automation system can impact others or be impacted by others is not a new concept for control system engineers. Control loop design is inherently interdependent especially for ensuring safety and efficiency while identifying potential risks from interdependencies within the broader system or organizational context. To achieve this understanding, engineers often begin by creating detailed documentation of the process automation system through control narratives or process flow diagrams, which include the conceptual architecture, components, and data flows. These types of documentation map out how different elements of the system interact with one another and with external systems, which allows engineers to visualize relationships and potential points of impact to rationalize the safety and hazard analysis.

What changes from this normal engineering behavior (and is outlined by the CIE questions) is that digital technology used in these interdependency relationships has the ability to be untrustworthy. This characterization is often not included by engineering in an interdependency evaluation. The response to untrustworthy interdependency between systems could include identifying alternative sources or engineering in backup sources like battery energy storage. Identifying all interfaces between their system and other systems—whether upstream or downstream processes, third-party systems, or manual operations—and including the loss of trust allow engineers to rethink their design especially as changes in one system can have cascading effects on others.

Within a system and the various control loops, engineers can utilize their tools like piping & instrumentation diagrams (P&IDs) to provide insights into how their system or control loop fits within the larger operational context, illustrating the flow of materials and energy and clarifying how changes, like the loss of trust, in one area may affect others. This understanding of interdependence is critical to the discussions in many of the other principles, like those often found in Principle 2: Engineered Controls, Section 2.2 above, and Principle 10: Planned Resilience, Section 2.10 below.

2.8. Digital Asset Awareness

Key Question:

How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?

Key Concepts for Engineers to Consider:

When designing a control system, engineers should consider the following terms to guide the use of digital technologies and ensure their capabilities are understood:

- Depend on digital / used to meet system requirements
- Breadth of digital asset
- Implemented Digital means
- Digital Asset Inventory / tracking
- Digital features / known good / expected / disabled
- Interface with digital assets
- Digital maintenance / updates / patching

This principle emphasizes the importance of understanding how digital technologies are deployed, how they function, and what assumptions underpin their integration into control systems, especially their position within the control loop. Especially as systems increasingly rely on digital means to fulfill operational and safety requirements, control system engineers have a role to proactively identify and characterize all digital assets—from basic sensors to complex firmware-enabled devices that are used to deliver the control loop function.

This is important because key transformations continue to occur in modern control environments through the digitalization of the field components (i.e., sensors and actuators). For example, these devices historically operated on fixed physical configurations, relying solely on analog signals and direct hardware inputs or outputs to interact with control systems. Today, many of these sensors and actuators feature embedded processors, configuration software, and digital communication protocols. For example, a pressure transmitter that once simply output a 4–20 mA analog signal may now offer configurable ranges, diagnostic reporting, and digital calibration via a vendor's proprietary software suite. Additionally, these devices also frequently connect through Ethernet cabling or wireless technologies, providing network-based integration into supervisory control systems. This shift means that these digital features—ranging from signal filtering and diagnostics to mode switching and update logging—can actively affect the control loop, especially if those features are misconfigured or maliciously exploited. Therefore, it is essential that control system engineers understand not only how these assets are used in day-to-day operations, but also what optional or latent capabilities exist and how they may influence system behavior in unexpected ways. This CIE principle draws out this understanding for control system engineers.

This awareness in a traditional cybersecurity sense often begins with the creation of an asset inventory. Control system engineers contributing to this inventory are able to expand the information beyond mere device names, addresses, and firmware versions. Engineers tracking what features are available, which ones are intentionally enabled, which are disabled, and how these choices affect control loop performance brings the maturity available through this CIE principle. For instance, a smart valve actuator may include torque limiting, signal smoothing, or position feedback algorithms—each governed by internal software and subject to change through remote updates. Understanding the implications of enabling or disabling these features is essential to system safety and reliability.

Asset awareness often includes interface mapping and data flows, where professionals document how digital assets interact within the network and across system boundaries. These interfaces include control system technologies such as Open Platform Communications (OPC) Unified Architecture (UA) servers, RESTful Application Programming Interfaces (APIs), or hardwired Input/Output (I/O) paths—all of which carry assumptions about protocol integrity and required response latency. Without clarity on these pathways provided by control system engineers, digital features might behave inconsistently or introduce performance anomalies when subjected to cyber threats and go overlooked.

An important element from the CIE questioning includes the routine maintenance practices around patching. It is well understood that updates to firmware or security patches may alter asset behavior, add new functions, or modify command structures. Control system engineers are

key to evaluating whether these changes are against operational and safety requirements before deployment. For example, upgrading the firmware of an ultrasonic sensor used to detect tank levels may shift its default data reporting interval or enable previously inactive diagnostic features, inadvertently overloading the control network, delaying critical tank level alarms, or providing false understanding of current tank levels.

Digital Asset Awareness ensures control system engineers adopt a mindset where software-driven features and networked interactions are treated with the same rigor as physical wiring and instrumentation. Recognizing the digital footprint of every asset used in the delivery of the control loop—from configuration options and data interfaces to patching procedures and firmware dependencies—enables a resilient, cyber-informed control system design. This principle also feeds into the successful execution of other CIE principles like Layered Defense, Section 2.5 above, or Consequence-Focused Design, Section 2.1 above.

2.9. Cyber-Secure Supply Chain Controls

Key Question:

How do I ensure my providers deliver the security the system needs?

Key Concepts for Engineers to Consider:

When designing a control system, engineers should reflect on the following terms to guide strategies that extend their resilience into the supply chain that supports the control system:

- Obtaining products and services
- Availability / Quality / Security
- Interruption in delivery / reoccurring
- Organizations communicate / document / vendor / suppliers / service providers
- Incident / vulnerability / disclosure
- Persistent / long-term connections / contractors
- Support contract / expires / third-party

This CIE principle emphasizes the importance of maintaining security not only within the control system itself but also across the supply chain that supports its development, deployment, and ongoing operation. Control system engineers are expected to be central to shaping how cybersecurity expectations are communicated, upheld, and verified across vendors, integrators, service providers, and support contractors. This is because decisions must be answered in relation to the trade-offs that are present in the safety and reliable operation of the control loop that the supply chain is supporting. Additionally, understanding the vulnerabilities that come from reliance on external parties—and ensuring engineered mitigations (See Principle 2, Section 2.2 above) are in place—is essential to creating a resilient control system architecture.

Modern control system engineering is inherently collaborative. While control system engineers' architect the system and determine technical requirements, it is often third-party integrators who program, commission, and deploy these systems. Later during its operation, long-term operation and support are frequently entrusted to external contractors or service vendors through maintenance contracts. The CIE questioning provided in this principle helps ensure that these

multi-party relationships are understood against the digital risk. Each touchpoint—during procurement, configuration, and support—introduces digital risk if security expectations are not clearly communicated and technically enforced. For example, during the procurement phase, a cyber-informed control system engineer should ensure that products and services being obtained meet security standards aligned with the operational goals of the facility. This would go beyond just selecting devices that meet performance specs; it also includes verifying that firmware is secure or hashed, that patch histories are available, and that the vendor has a transparent process for vulnerability disclosure and update delivery. Even if a cybersecurity professional is the one executing some of those actions, the engineer can validate the success or failure of those actions in a unique way given the uniqueness of this control system technology over traditional information technology (e.g., Windows/Linux operating systems). Selecting a PLC that supports encrypted communications is valuable only if the supplier commits to maintaining encryption standards across firmware revisions and is prepared to notify asset owners promptly in the event of discovered vulnerabilities. Control system engineers can go one step further and provide alternate system architectures (e.g., fail-over, alternate paths) in case the encryption standard is compromised or no longer able to meet system operational objectives.

It is well understood that control system resilience is threatened when availability, quality, or security of supplied products and services degrade—particularly when recurring disruptions occur. For instance, if wireless instrumentation vendors delay patch rollouts following the discovery of a cybersecurity flaw or if integrators fail to document remote access pathways during commissioning, the system remains exposed. Engineers in collaboration with their procurement and cybersecurity counterparts account for these risks by evaluating supplier responsiveness, validating whether supply chain practices allow for timely remediation, and identifying alternate supply sources. Long-term supply chain relationships pose additional risks in modern control systems especially if contractors or vendors maintain persistent access to systems via remote diagnostic channels or update portals. In a traditional cyber-sense, these connections are tightly controlled and regularly audited. For example, if a contractor is granted VPN access to update a motor drive's control parameters, that connection is expected to expire at the end of the contract or be revoked at completion of service. Engineers play a crucial role in validating these relationships by validating settings before and after submission into the control system or provide a fail-safe mode in the event those components or systems are no longer trustworthy.

Finally. If a vendor discloses a vulnerability in a piece of technology used within a plant's control loop, control system engineers are the key personnel to assess whether that vulnerability is exploitable in their specific configuration and what operational consequences might result. Active communication channels with cybersecurity professionals as well as with the suppliers allow for informed decisions—such as implementing compensating controls, new engineered controls, or initiating accelerated updates—before problems materialize in operations.

This CIE principle pushes control system engineers to think of vendors, service providers, and contractors as digital contributors to the control loop. By embedding CIE expectations into procurement documentation, support contracts, and interface standards and by validating

whether these expectations are being met over time, engineers ensure that the supply chain itself is a pillar of cyber resilience—not a blind spot.

2.10. Planned Resilience

Key Question:

How do I turn “what ifs” into “even ifs”?

Key Concepts for Engineers to Consider:

When designing a control system, engineers should reflect on the following terms to ensure that it remains operational even when cyber threats are actively attempting to compromise its safety, performance, or reliability:

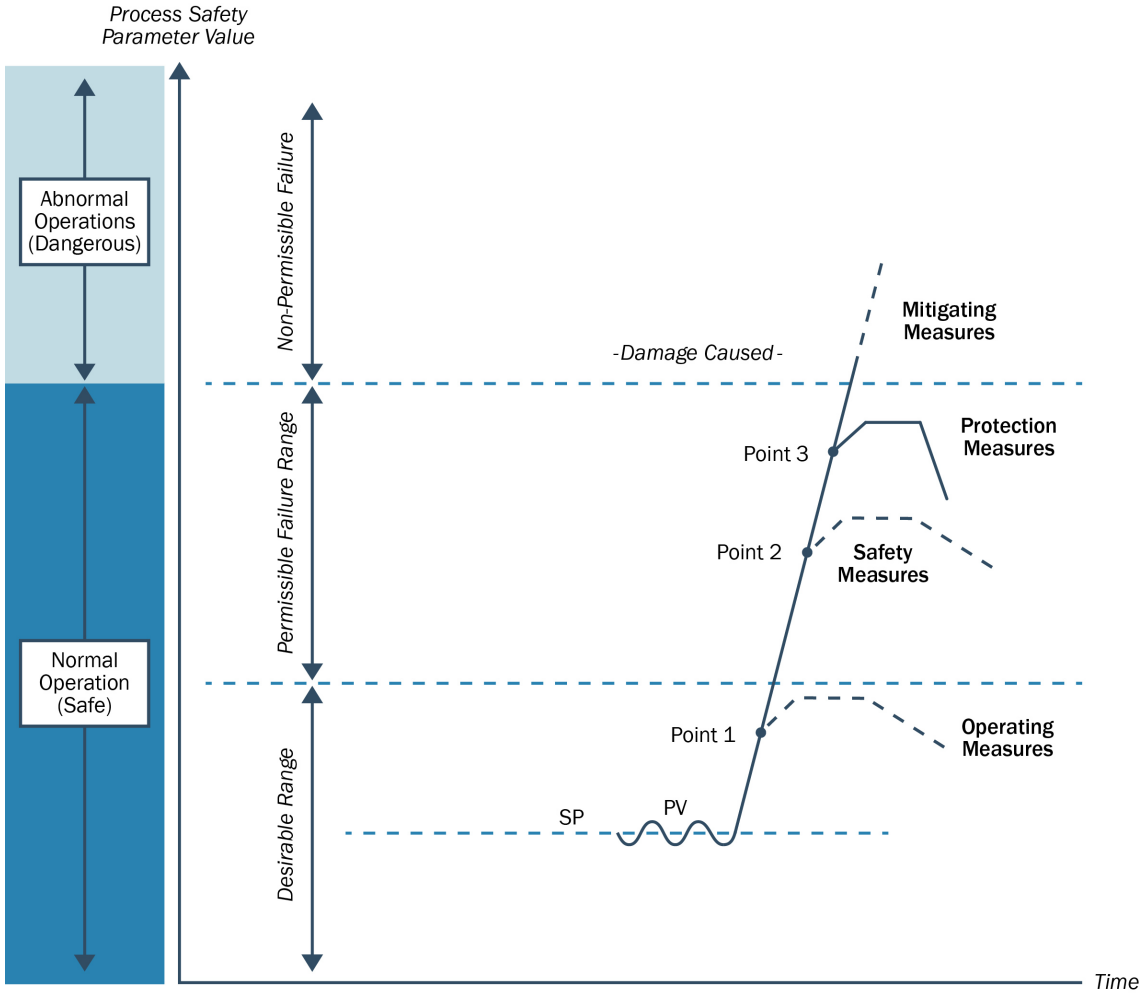
- People / Materials / Equipment
- Withstand / Recover / Catastrophic
- Diminished Operating Mode / Limits of Acceptable Degradation
- Abnormal Operating Conditions / Alternative Sources or Inputs
- Manual Mode of Operation / Bypass / Isolate
- Fail-Secure / Redundancy / Mean Time to Recover

This principle transitions system design from the typical "what if" scenarios, commonly considered by control system engineers, to proactive "even if" strategies, which are standard in safety/hazard contexts but not usually applied to digital risk. Cyber-informed control system engineers architect systems capable of withstanding and recovering from cyber threats—ensuring that both safety and essential performance are preserved even if those threats become active and persistent. This is especially important because many safety functions are actively being digitized.

As suggested, this principle draws heavily from the structured reasoning found in Safety Instrumented Systems (SIS) and associated safety functions, especially the understanding of failure zones, acceptable operating ranges, and protective mechanisms or safety integrity levels (SIL). SIS frameworks guide engineers to define operational states with clarity—normal, permissible failure, and dangerous conditions—and the Planned Resilience principle applies similar logic to cyber disruptions, integrating engineered controls that detect, respond to, and

contain digital threats within the control loop. See Figure 6 for a graphic often used by control system engineers thinking through resilience layers.

Figure 6. Control System Resilience Levels[12]



Effective resilience begins with acknowledging the interconnected reliance on people, materials, and equipment to sustain operations often drawn out of Principle 7 (Interdependency Evaluation, Section 2.7 above). A key practice available to control system engineers is the concept of "A Day Without Automation" and allows them to anticipate how loss or compromise of any one of these elements might impact automation. For example, in a cyber event that disrupts network communications between a supervisory system and field devices (i.e. DoS), the control system should be capable of switching to alternative sources or inputs, such as locally stored process

[12] Chuck Cornell, Control Systems Engineer Technical Reference Handbook (Research Triangle Park, NC: International Society of Automation, 2012), 300.

values or failover instrumentation. These strategies reduce dependence on single points of failure and bolster system durability. This represents good engineering practice even outside of the reality of digital risk.

An essential feature of this CIE principle's questioning is the ability for the system to operate in diminished modes. This involves accepting limits of acceptable degradation, where some performance is forfeited but core safety and function remain intact. The knowledge of acceptable degradation is the role of the control system engineer. For instance, rather than shutting down—which may unintentionally reward adversarial intent—the system can continue in a constrained state that prioritizes protection and survival. These fallback modes might include simplified control logic, alternate routing, or reduced production throughput, each designed with pre-validated tolerances. The requirement for pre-validated tolerances is an expectation for modern process automation systems looking to remain resilient against digital risk, and while it might engineer out network-based threats, supply chain threats require positioning these tolerances into the system-wide context.

Control engineers play the key role in designing controllers with adaptive algorithm parameters. For example, a feedback loop operating under safe conditions may maintain standard PID values, but if the system enters permissible failure ranges, the controller could dynamically increase gain or invoke derivative damping to correct error more aggressively (i.e. dynamic compensation). These digital shifts represent an engineered behavioral change that aligns with safety function strategies—mobilizing more robust control when the system's integrity is threatened. As conditions deteriorate toward abnormal or dangerous operating states, the control system must activate escalation protocols to limit damage. These may include isolating critical pathways, bypassing compromised subsystems, or initiating fail-secure responses. In such cases, redundancy often becomes essential; secondary controllers, redundant communication paths, and parallel safety mechanisms are employed to maintain vital operations. The challenge drawn out by CIE questioning is that these measures also include a level of digital susceptibility and that must also be considered by control system engineers looking to implement traditional safety and reliability responses to the deeper layers of protection.

When considering the loss of automation—either intentional (via manual switchover) or accidental (via cyber attack)—control engineers often provide manual modes to maintain operational continuity under constrained conditions. This is a common CIE response activity. However, control system engineers have the opportunity to constrain these manual modes with minimal personnel, reducing the dependency on full staffing in emergency conditions. A manual mode that is clear, documented, and functionally isolated allows operations to continue without overwhelming staff resources, avoiding full system shutdown and mitigating attack consequences. Overall, CIE's Planned Resilience integrates the protective thinking from SIS with cyber-aware (i.e. digital risk based) automation practices. It enables systems to maintain a functional state—perhaps degraded but still safe—even when targeted by digital adversaries.

2.11. Engineering Information Control

Key Question:

How do I manage knowledge about my system? How do I keep it out of the wrong hands?

Key Concepts for Engineers to Consider:

When designing a control system, engineers should reflect on the following terms to incorporate data protection governance around the key information about the system from falling into unauthorized hands:

- Sensitive Information / Elements of Design
- Shared / Agreements / Contractual Obligations
- Partners / Vendors
- Reporting / Data Retention
- Observe / Infer / Sources

Control system engineers utilize a variety of key documents to effectively describe and manage process systems. These documents provide detailed information on how the systems should operate, the logic behind control sequences, and the physical layout of the system components. Some of the most important documents that covey key process automation understanding and should be integrated into the organization's data protection governance include:

1. **Control Narratives**: Control narratives provide detailed descriptions of the control strategies, sequences of operations, and the logic behind the control systems. They outline how the system should respond under various conditions and are crucial for understanding the intended operation of the control system.
2. **Logic Configuration Files**: These files contain the actual programming code or configuration data for the control systems, such as PLCs or distributed control systems (DCS). They define the control logic, interlocks, alarms, and other control actions that automate the process.
3. **Piping and Instrumentation Diagrams (P&IDs)**: P&IDs are schematic diagrams that show the interconnection of process equipment and instrumentation. They provide a detailed graphical representation of the process flow, including the arrangement of pipelines, valves, sensors, and control devices. P&IDs are essential for understanding the physical and functional relationships within the process system.
4. **Process Flow Diagrams (PFDs)**: PFDs provide a high-level overview of the process flow, showing the major equipment and the flow of materials through the system. They are less detailed than P&IDs but are useful for understanding the overall process and the main components involved.
5. **Functional Specifications**: These documents describe the functional requirements of the control system, including performance criteria, control objectives, and acceptance criteria. They serve as a reference for the design, implementation, and testing of the control system.
6. **Instrument Data Sheets**: These sheets provide detailed information about each instrument used in the control system, including specifications, calibration data, and installation details. They are important for ensuring that the correct instruments are selected and properly configured.

7. **Control System Architecture Diagrams**: These diagrams illustrate the overall structure of the control system, including the network topology, communication protocols, and the arrangement of control hardware and software components. They help in understanding how different parts of the control system interact and communicate with each other.
8. **Alarm and Interlock Schedules**: These documents list all the alarms and interlocks in the control system, along with their setpoints, priorities, and actions to be taken in case of alarm conditions. They are critical for ensuring safe and reliable operation of the process system.
9. **Operator Interface Descriptions**: These descriptions detail the layout and functionality of the HMI screens used by operators to monitor and control the process. They include information on screen navigation, display elements, and control actions available to the operators.
10. **Calibration and Maintenance Procedures**: These documents provide instructions for the calibration, testing, and maintenance of control system components. They ensure that the system operates within specified parameters and remains reliable over time.

This engineering information if captured by an adversary allows the adversary to have a drastically improved ability to craft and design an attack to cripple the process automation system especially if that system only relies on information protection countermeasures and does not also include engineered controls from Principle 2, Section 2.2 above, as part of its Layered Defense (Principle 5, Section 2.5 above) implementation.

2.12. Organizational Culture

Key Question:

How do I ensure that everyone's behavior and decisions align with our security goals?

Key Concepts for Engineers to Consider:

When designing a control system, engineers should reflect on the following terms to ensure alignment between organizational culture and cybersecurity expectations:

- Stated and real priorities / Organization
- Senior Leadership
- Behaviors / Error-likely circumstances
- Training / Education / Practice
- Technical Debt
- Incentivize / Speak-up / Trust

This CIE principle's questioning recognizes that technical cybersecurity cannot succeed in isolation; it must be reinforced by behavioral expectations, shared values, and consistent decision-making across the entire organization. This cultural alignment is especially critical in process automation environments, where engineering decisions directly influence the safety, reliability, and cybersecurity posture of automated operations.

Just as safety culture matured by recognizing that everyone—regardless of role—contributes to the prevention of accidents, cybersecurity culture is actively undergoing a similar evolution. And within that growth, control system engineers occupy a uniquely impactful position. Through their design decisions, maintenance practices, and communication habits, they also help shape how the organization prioritizes cyber risk within industrial operations.

This principle encourages engineers to reflect on both the stated and real priorities of their organization. While cybersecurity goals may be formalized in policy or leadership statements, actual priorities are revealed through how resources are allocated, how mistakes are addressed, and how engineering trade-offs are evaluated. Control system engineers help surface the real risks by identifying where legacy practices—or technical debt—complicate secure system behavior, and they can advocate for changes that balance performance expectations with cyber resilience.

One of the key responsibilities of control system engineers within this principle is to recognize and mitigate error-likely circumstances. For instance, designing a control system that hides diagnostic data behind complex menus, or requiring manual network connections in routine processes, increases the likelihood of unsafe or insecure operator behavior. Engineers using this principle take ownership over usability and clarity in system design—recognizing that human interaction is a cyber factor just as much as digital interfaces are. Control system engineers support this cybersecurity culture by helping others understand the cyber risks embedded in automation platforms. Whether through design documentation, informal knowledge sharing, or participation in cybersecurity drills, they reinforce learning that equips operators, technicians, and support staff with better judgment and faster response times. This also includes practicing and promoting manual fallback operations, as seen in the Planned Resilience principle—making sure the workforce knows how to operate locally when automation is compromised.

As with all cultural movements, it is understood that leadership support is fundamental. Senior leadership sets the tone, but engineers reinforce their vision through their day-to-day decisions. For example, choosing not to bypass alarms during commissioning, or raising concerns about unsupported firmware in vendor-delivered equipment, demonstrates a commitment to resilience over convenience. These actions model behavior that is security-minded, values-driven, and technically sound. A mature cybersecurity culture invites these engineers to speak up. Organizations benefit when engineers feel empowered to question outdated practices, suggest improvements, and report anomalies without fear of backlash. This principle makes clear that control system security is not just about defense mechanisms and software updates. It is about behavior, expectations, and aligned values—every engineer's design, reaction, and recommendation either strengthens or weakens that culture. By embracing this responsibility, control system engineers ensure that organizational decisions consistently reflect the shared goal of operational security, even in the face of evolving cyber threats.

3. Summary

This document discusses the integration of CIE into process automation to enhance cyber-resilience. It emphasizes that while traditional cybersecurity focuses on reducing and mitigating exposure to digital threats, engineers can deploy unique solutions to eliminate classes of digital

threats. It highlights the importance of engineering controls and the execution of CIE principles to reduce and mitigate the impacts of digital risks in modern technologies used in control loops that orchestrate process automation. The outcome of a cyber-informed control system engineer is a system that is resilient by design, capable of withstanding and recovering from cyber threats while maintaining safety, performance, and reliability.

This document also outlines the CIE principles, including consequence-focused design, engineered controls, and layered defenses. All 12 CIE principles guide control system engineers in identifying and mitigating digital risks, ensuring that process automation systems remain secure and resilient.

Cyber-Informed
Engineering