INL/MIS-24-76646-Revision-0

Cyber-Informed Engineering: Cybersecurity for Microgrids Workshop Workbook

February 2024

Virginia L Wright, Benjamin Ruhlig Lampe, Samuel Douglas Chanoski

Changing the World's Energy Future

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

INL/MIS-24-76646-Revision-0

Cyber-Informed Engineering: Cybersecurity for Microgrids Workshop Workbook

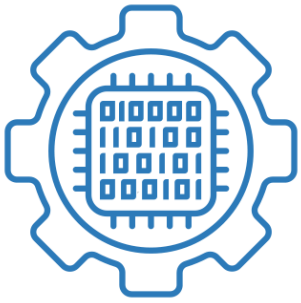
Virginia L Wright, Benjamin Ruhlig Lampe, Samuel Douglas Chanoski

February 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

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



Cyber-Informed Engineering

Cybersecurity for Microgrids Workshop Workbook

January 25, 2024

Virginia Wright
CIE Program Manager, INL

Sam Chanoski
Technical Relationship Manager, INL

Benjamin Lampe
OT/ICS Cybersecurity Education Specialist, INL

Document Number: INL/MIS-24-76646

Document Number: INL/MIS-24-76646

CONTENTS

FIGURES

Page intentionally left blank

ACRONYMS

ADMS	Advanced Distribution Management System
CIE	Cyber-Informed Engineering
CIP	Critical Infrastructure Protection
DMS	Distribution Management System
DMZ	De-militarized Zone
FLISR	Fault Location, Isolation, and Service Restoration
GHG	Greenhouse Gases
HCE	High Consequence Event
HR	Human Resources
ICS	Industrial Control System
INL	Idaho National Laboratory
IT	Information Technology
MW	Mega-Watts
MWh	Mega-Watt-hours
NERC	North American Electric Reliability Corporation
NREL	National Renewable Energy Laboratory
OEM	Original Equipment Manufacturer
OMS	Outage Management System
OT	Operational Technology
PUD	Public Utility District
RFP	Request for Proposal
SCADA	Supervisory Control and Data Acquisition
VAR	Volt-ampere Reactive
VVO	Volt-VAR optimization

Page intentionally left blank

Using Cyber-Informed Engineering for Cyber Defense Workbook

Workbook Background

This case study workbook provides a hypothetical project to support discussion and application of the principles for Cyber-Informed Engineering. Participants in the workshop are encouraged to use the workbook to capture insights and lessons learned. The provided attachment to this workbook contains the visuals for the hypothetical project scope and is used by participants as they capture insights and lessons learned.

Though some elements of this scenario are provided for consideration, there are likely key facts which have been omitted or may be unclear. Participants are encouraged to make any needed assumptions about the project to enable application of the CIE principles.

Though this project is based on real-world case studies, it is fictional.

Cyber-Informed Engineering Summary

Cyber-informed engineering (CIE) offers an opportunity to "engineer out" some cyber risk across the entire device or system lifecycle, starting from the earliest possible phase of conceptual, requirements, and design—the most optimal time to introduce mitigations against cyber risk. CIE is an emerging method to integrate cybersecurity risk considerations into the conception, design, development, and operation of any physical system that has digital connectivity, monitoring, or control. CIE approaches use design decisions and engineering controls to mitigate or even eliminate avenues for cyber-enabled attacks or reduce the consequences when an attack occurs.

In the same way engineers engineer systems for safety, engineers informed by the CIE approach use engineered controls and system design to mitigate or eliminate the effects of cyber-enabled attacks. Likewise, specialized Information Technology (IT) and Operational Technology (OT) cybersecurity experts bring strong cybersecurity capabilities to securing today's energy systems. Working together, both parties actively implement engineered and cybersecurity solutions to address the highest-risk consequences in their systems, ensuring robust protection for their devices and infrastructure.

This workshop summarizes the principles for Cyber-Informed Engineering, provided with the principle's initiating question on the next page.

Principle	Initiating Question
Consequence-Focused Design	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?
Engineered Controls	How do I implement controls to reduce avenues for attack or the damage which could result?
Secure Information Architecture	How do I prevent undesired manipulation of important data?
Design Simplification	How do I determine what features of my system are not absolutely necessary to achieve the critical functions?
Layered Defenses	How do I create the best compilation of system defenses?
Active Defense	How do I proactively prepare to defend my system from any threat?
Interdependency Evaluation	How do I understand where my system can impact others or be impacted by others?
Digital Asset Awareness	How do I understand where digital assets are used, what functions they are capable of, and what our assumptions are about how they work?
Cyber-Secure Supply Chain Controls	How do I ensure my providers deliver the security the system needs?
Planned Resilience	How do I turn “what ifs” into “even ifs”?
Engineering Information Control	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
Organizational Culture	How do I ensure that everyone’s behaviors and decisions align with our security goals?

Exercise Foundation

The exercises below are provided to allow you to have a hands-on experience applying the CIE principles in a fictional project. We'd like to ensure that each of these scenarios invites rich discussion about the CIE principles. Please feel free to ask questions of the moderators or make the necessary assumptions about the project which will help you and your table to engage with, and receive benefit from, the described scenario.

Exercise Background

You and your team support a small utility undertaking a community microgrid project. The utility requests your assistance in identifying security decisions during the design phase that could significantly reduce cyber risk. Ideally, your efforts would focus on creating built-in mitigations for critical system functions. These mitigations should be anticipatory, proactively preventing specific high-consequence attack paths or impacts. Solutions based on physical engineering changes and protections for the system are desired over those which require ongoing monitoring or reaction.

Community Microgrid Project Details

The Community Microgrid Project is planned to serve the heart of the county's population center, a 25-block area of the city's urban core. The overarching goals of the project are to support integrated planning and resource optimization, help the city make the best use of its resources for sustainability and resilience, and attract and retain quality jobs to the area. This project is part of a larger climate-energy-sustainability program from the city and county governments, in partnership with the utility, that is pursuing five objectives:

- Modernize infrastructure and systems to support high-quality job growth and retention and sustain and improve quality of life for customers and the utility.
- Deploy systems to provide resilient and sustainable energy for vital services and facilities.
- Optimize the use of existing renewable and distributed generation and storage to power critical community electric loads (including during regional outages).
- Provide businesses and residents with opportunities to manage energy costs by investing in local renewable generation and storage capacity.
- Plan for future energy needs and return on investment through potential electricity market changes (i.e., demand response, ancillary services, energy and capacity market participation).

Over the past four years, significant infrastructure recapitalization across the utility territory, focusing on the city, has brought the distribution system up to modern standards providing reliable power and with capacity for future growth. Alongside the electrical equipment upgrades the utility has begun adding distribution automation capabilities to certain circuits, including SCADA (supervisory control and data acquisition) control of distribution devices, volt-VAR optimization (VVO) and automated capacitor switching, and fault location, isolation, and restoration (FLISR) schemes. The utility uses a common Distribution Management System (DMS) for SCADA control, with partially integrated Outage Management System (OMS) and crew dispatch functionality; this system was system-integrated to its current state by a variety of vendors and in-house efforts and while its capability does not rise to the level of currently available ADMS there are no plans to replace or significantly change this system.

Community Microgrid Project Scope

Our mission is to provide insights to the design engineering team who has been contracted to perform engineering design for the Community Microgrid Project to be implemented into the utility's existing physical and logical systems in the city area.

Benefits and Features of the Community Microgrid:

- Serve electric demand up to 2.0 MW supplying 10,000 MWh of electric power annually at initial operational capability, with the ability to expand up to 4.5 MW and 23,000 MWh
- Provides real-time monitoring and data of energy usage.
- Manages energy use according to selectable configurations, including optimization for reducing greenhouse gas (GHG) emissions or for economics.
- Provides an incentive for customers within the microgrid footprint to invest in and integrate their own renewable generation capabilities.
- Improves local reliability and resilience against power outages, with the ability to power the city fire and police stations, an emergency warming-cooling shelter building, and residential loads, like vulnerable populations (i.e. senior living, low-income, etc.) housing facility, during a prolonged outage
- Provides the control and communications capabilities for the planned repowering of the utility's 3.5 MW Speer Lake Solar Facility, and the addition of battery energy storage.
- Allows for participation in future energy markets to reduce direct operational costs and improve overall grid reliability (subject to future regulatory approvals).
- Cyber security protections and documentation for NERC CIP compliance, even though not currently required by NERC or the state Public Service Commission

Refer to items, I, II, and III in the Appendix Attachment for visuals about the project scope.

Community Microgrid Project Progress

This effort began in 2021 and has generally followed the design process documented by National Renewable Energy Laboratory (NREL), shown below. Step One was largely completed by City and County officials with some input from Utility leadership, and once the decision was made to proceed, the Utility selected and contracted with a regional design engineering firm to perform Steps Two and Three, with support from Utility engineers and staff as needed. They have produced a final draft conceptual design that promises to offer reliability and resilience, advanced monitoring and control functions, flexibility for future enhancements. Once this conceptual design is approved in Step Four, the project will be solicited for an integrator to carry out final design, procurement, construction, and commissioning. The Utility, before moving to Step Four, wants to take this opportunity to evaluate and improve the security of the design and overall project outcome using CIE.

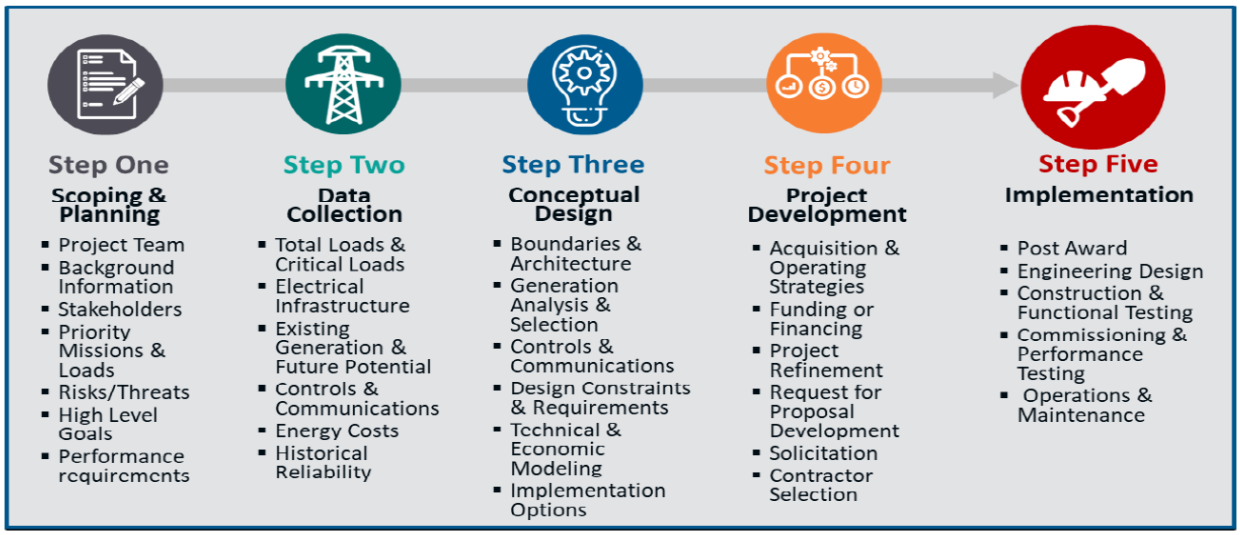


Figure 1 - NREL's Microgrid Design Process[a]

Item IV in the Attachment depicts the Coop/Muni/PUD visual representation of generic critical functions.

Item V in the Attachment illustrates the Distribution System Operators Functions.

Item VI in the Attachment illustrates the generic information architecture for a control system.

Item VII in the Attachment illustrates the generic segmented information architecture for a control system.

Item VIII in the Attachment illustrates the Distribution Interconnections.

[a] https://www.nrel.gov/docs/fy19osti/72586.pdf

Analysis of the Community Microgrid Project using CIE Principles

Please work with the team at your table to consider and discuss how each principle applies to this effort. As a team, determine what your feedback would be to the microgrid design team on their implementation of CIE and be prepared to brief your answers out in the room. The engineering design team (also referred to as the project team) has provided some input (found under each Key Question) but is open to your recommendations outside of those inputs.

Consequence-Focused Design

Consequence-focused design is the first principle that is considered within a Cyber-Informed Engineering project. It results in insights that feed the remainder of the principles. Consequence-focused design begins with an analysis of the business purpose and its primary mission, the critical functions of the business, the interconnection of those functions to the system under consideration, and finally, the critical functions of the system itself. The team is seeking to identify the most consequential impacts, sometimes referred to as the High Consequence Events (HCE's), that could result from disruption of the critical functions, especially those where the disruption of a system function could result in a mission-impacting consequence.

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

From the project team:

- This microgrid will provide power to the county administration offices, city police and fire services, and residential housing, as well as a facility used as a warming and cooling center during extreme weather and a food pantry. Other customers in the footprint are small businesses that are anchor businesses of a revitalized downtown area.
- All customers have an always-on expectation, and secondary expectation of reasonable prices.
- The microgrid will be expected to maintain electric service to customers during power outages in the area.
    - This is a must-work first and every time function, since repeated or significant (e.g., during a severe weather event) failures will likely cause the city and county to withhold support for future microgrid projects.
- Electrical worker physical safety (identified in the team's input in 4.2, Engineering Controls).
- Threats to consider:
    - Supply chain concerns with products from adversary nations,
    - Industroyer2,
    - Sandworm (misuse and abuse of inherent functionality).
- The board and executives are fairly risk-adverse (middle of the road for electric utilities, which are generally on the conservative end of critical infrastructures).
- The board and executives are supportive of applying CIE on this effort and see the value of investing in the process security at the design phase to control costs in operations.
    - We may have to help make the case that our suggestions will do so.

Identify up to FIVE possible high consequence events for the microgrid and document them here.

1.	
2.	
3.	
4.	
5.	

Share the high consequence events with your team and determine which of them should be considered the worst possible case consequence. Document this worst-case consequence event here, provide a justification of why it is considered the worst case, and use it as the basis for the subsequent principles.

Worst Case Consequence Event	**Justification**

Engineered Controls

For the most critical consequences and impacts determined in 4.1 Consequence-Focused design, there is an opportunity to identify specific engineered controls which either limit the possibility of the consequence or mitigate its impact. Taken together, coordinated controls and processes are used to eliminate or significantly reduce the consequences that a cyber attacker could achieve. This requires integrating cyber and engineering experts and expertise into system design, engineering, and operations. An example of an engineered control is a pressure-relief valve in a tank, an analog safety control which safely evacuates material and lowers the pressure. Even if a cyber adversary altered settings to raise the pressure in the tank, the pressure-relief value will provide an engineering control which limits the impact of that attack on the system.

- Think about what kinds of engineered controls that could prevent a worst-case consequence or mitigate its impact.
- Determine which engineered controls are provided as a part of products and services (i.e. Commercial-off-the-shelf) already in the design and which ones need to be designed in.
- Consider both physical controls and digital controls which might mitigate a given consequence and the relative costs and benefits of each.
- Determine whether the controls prevent an attack, lower the impact of the attack, or serve to provide alarms or warnings of adverse situations.

Key Question: How do I implement controls to reduce avenues for attack or the damage which could result?

From the project team:
The team has identified some potential systems and is planning the process to screen prime contractors (integrators) for Request for Proposal (RFP) solicitation (Step Four). They would like this principle to guide any design inputs they need to consider and provide input they'll use to guide vendor selection.

They have identified the following considerations:

- Vendors designed the components used in the microgrid with certain assumptions about existing security controls.
    - The utility is too small to influence these facts but, working with the design engineering team, has choice among a few options of which components to use.
- The operation and maintenance of the electric infrastructure requires many workers to come in close contact with electric hazards with some digital safety controls (e.g., reclosing blocked or instantaneous trips enabled).
    - The team has identified this as a high-impact consequence and would like to consider additional engineered controls to prevent the possibility that a cyber-attack or digital failure could remove the controls and allow injury to line workers.
- If backup local manual controls are used, they will need to be adequately physically secured to prevent access from unauthorized personnel in the vicinity, while not impairing the usefulness of the controls.

Draw or document an engineering control below that mitigates the worst-case consequence identified in Principle 4.1. Describe how it mitigates the worst-case consequence.

Secure Information Architecture

Each system contains data linked to mission-critical consequences and impacts which should be protected from unauthorized viewing and, more importantly, adversary or failure-induced alteration. For each identified data stream, a secure information architecture can be designed, guided by the consequences and impacts identified earlier, to segregate the most important data and the systems which contain it to provide more control, protection, and monitoring of those systems and that data. Some mechanisms used include network segmentation, data segregation, data replication, etc.

We can start early in the system design to identify those data elements most tied to a potential critical consequence, where they originate and are altered through the process, how they should be protected, and whether it is possible to design a data verification mechanism using the process, analog controls, or historic inputs.

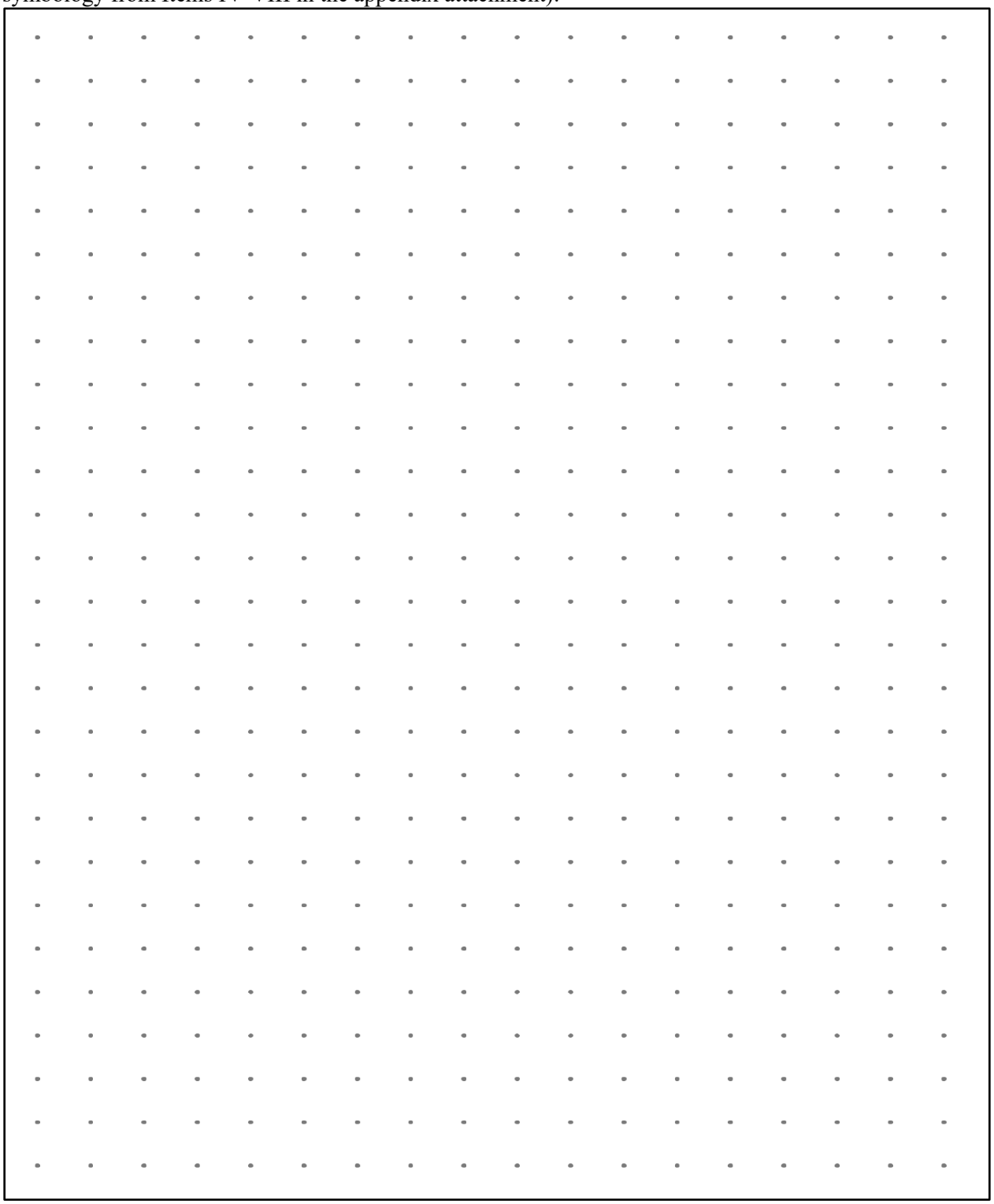
Once our design is more mature and we understand the underlying network and data service architecture, we can add more fine-grained digital controls, and create specific zones and segmentation plans.

Key Question: How do I prevent undesired manipulation of important data?

From the project team:

- The team understands the importance of this principle and would like to ensure that this is considered early before product selection is complete.
- They would like insight into the ingress-egress points to get the necessary data to the right endpoint locations and the accompanying risks.
    - This is for the requirements for the current microgrid project, but also thinking of future requirements from expansion or new value streams.
- Different endpoint functions are taking place in multiple locations, on premise or in private or public clouds.
    - They would appreciate advice on a better way to ensure the best possible security and privacy.
    - They do not think that control actions can be initiated through the manipulation of remote data, however, they would appreciate your consideration of this risk.
- They have identified some desired elements of their architecture, but are open to more ideas:
    - Segmentation from enterprise, control center, and substations – essentially a separate subnet for the microgrid protected by boundary protection devices such as a firewall.
    - Migration or replication of current communication signals to a different/alternate pathway (e.g., include an analog signal to relay information in addition to a local network connection).
    - DMZs to segment from external data exchange with OEMs, customers, and possibly in the future a Balancing Authority and Transmission Operator for new value streams (e.g., frequency regulation or ancillary services).

From the equipment that facilitates the worst-case consequence, identify the data involved in that process and depict the data flow of the information from the equipment to its destination (you are free to use symbology from Items IV-VIII in the appendix attachment):



Design Simplification

Systems formed through acquisition often have more features than are explicitly needed to perform required functions. Though these features can be configured to not be available to authorized system users, they may be available to adversaries who gain access. These features can potentially lead to catastrophic impacts if used by malicious adversaries.

In design simplification, we consider which features of the system are not absolutely necessary and of those which could lead to the worst-case consequences if misused. We consider how to reduce the system to the minimum elements needed to provide mission-critical functions and necessary resilience. For each of the non-essential features, we consider whether we can completely remove them. When that is not possible, we consider how we might implement alarms and alerts when those functions are leveraged, or whether we can capture and prevent undesired commands at a network segmentation boundary before they are executed.

Key Question: How do I determine what features of my system are not absolutely necessary?

From the Project Team:

- The team would appreciate advice on how they can simplify elements of the design.
- Most of the microgrid components we might choose will have a lot of features, not all of which will be used immediately.
    - The team has loosely determined that some features might be phased in over years, and some never used.
    - Features we disable through configuration will still be present in the components we use, just not available via user interfaces.
- The design team's diagrams, items I, II, III, and IV in the Attachment provided, may offer some insights about the most desired features and those which are not prioritized for use.

Consider the worst-case consequence from Principle 4.1, and the equipment used in relation to that consequence, Principle 4.3, identify any functions (digital or engineered) in the available equipment that may not be absolutely necessary.

Layered Defenses

The best defensive capability for critical consequences is formed by an assemblage of diverse controls, from physically based analog mitigations, capabilities to protect key system elements, capabilities to detect adverse operating or security conditions, and capabilities to aid in response and remediation. In resilient layered defenses, engineers, and their operational cybersecurity support team collaborate to prioritize potential consequences, then design and arrange the most effective combination of defenses to mitigate the worst potential impacts. The engineers and operational cybersecurity team work together to ensure that each of the defensive capabilities and services are tuned based on the identified consequences and how the worst impacts of those consequences can be avoided.

Key Question: How do I create the best compilation of system defenses?

From the Project Team:

- The microgrid will reside at the edge of an environment that already has layers of imperfect perimeter protection and detection, with several required interfaces spanning that perimeter.
- Microgrid components are rich in features and configuration options, not all of which the Utility will use. The design team would like your input on how they can ensure that they can detect the use of features that are supposed to be configured out.
- The design team has talked to the Utility's small but knowledgeable operational cybersecurity team in general about the project, but not about specific capabilities and services needed for operational cyber defense.
- The microgrid will reside at the edge of an environment that already has layers of imperfect perimeter protection and detection, with several required interfaces spanning that perimeter.
- The design team would like your ideas to discuss with the operational cybersecurity team about the specific consequences you would recommend they focus on and how they might layer CIE mitigations within their operational cybersecurity.

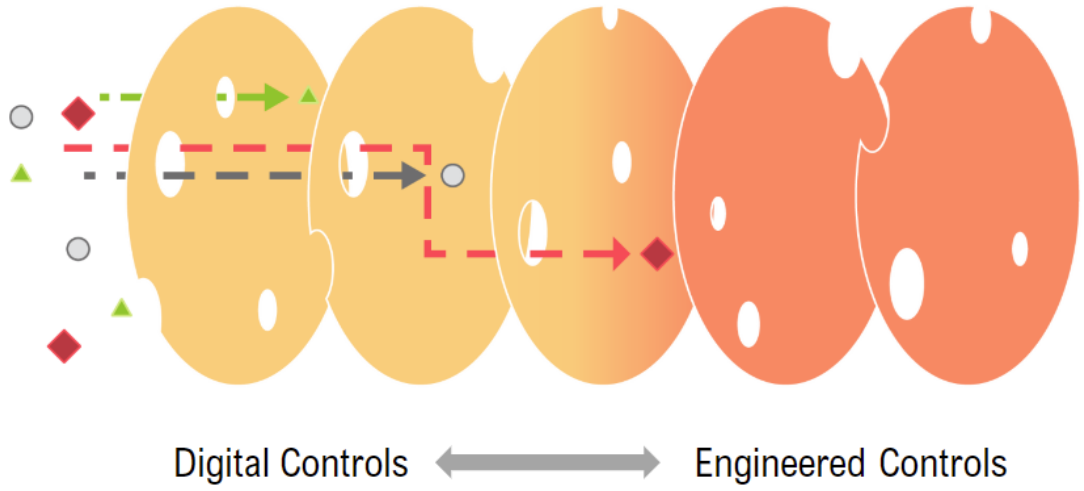


Figure 2 - CIE Defense in Depth[b]

[b] Diagram from Cyber-Informed Engineering Deep Dive Slides.

Consider the equipment used to facilitate the worst-case consequence event identified earlier, identify and document the digital and engineered controls that are used to mitigate the event:

Digital Controls	Engineered Controls

Active Defense

Planning for active defense can begin as soon as a conceptual design for a system exists and it continues through the system's retirement. At the design phase, teams can begin to plan how defensive actions should be carried out for the most consequential events. This activity is aided by ensuring that the system designers, operators, and cybersecurity support team discuss the adverse consequences identified and how such events could occur, especially, at the appropriate level of detail for system maturity, the process, or kill chain of how the adverse consequence would manifest within the system. From this discussion, system states and anomalies which might be initial indicators of one of the identified consequences can be identified.

Next, plans can be developed for the next actions to be taken upon detection of an identified indicator. Plans should include specific roles and responsibilities across the spectrum of roles associated with the system, since active defense of the system may require support from a broad set of roles. Once plans are in place, policies/procedures should be created to ensure that these plans are regularly practiced, and that the overall approach is assessed regularly to identify emerging consequences, indicators, and opportunities for more advanced defensive approaches.

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

From the Project Team:

- The project team is interested in getting insights, for any consequences identified in this analysis, about indicators you can identify which might be part of a failure event or kill chain.
- The team is interested in your insights on roles and responsibilities they may not think to consider who should be incorporated into system defense.
- The team is interested in your suggestions for exercises they could consider which would help to ensure that the team is ready to defend the system.

For each of the layered defenses in the previous principle, document how the layers would work together to control risk, where a human action would be needed to connect the layers, and who would likely need to facilitate that action.

Control	Contingency Action	Role(s)

Interdependency Evaluation

All systems have interdependencies, both direct and indirect. While teams regularly consider the risks posed by physical interdependencies in the normal systems engineering processes, they rarely consider how a cyber-attack or digital failure of an interdependent system may affect the system under design.

When evaluating interdependencies from a cyber-informed perspective, consider existing physical interdependency risks, and assess whether a cyber-attack could amplify their likelihood or severity compared to purely physical events. Are there functions in the interdependent system not normally accessible to operators which might cause adverse effects on our system if activated? Where might interdependent systems activate command logic on the system under design? Where might automation between the two systems causes cascading effects? In the same vein, where might the system under design be able to affect the interdependent systems in unexpected ways.

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

From the Project Team:

- This system will require communication links with acceptable bandwidth and latency to multiple locations.
    - Some of these physical locations are not continuously networked today.
    - Some of these logical resources are external to the Utility and may not be used today but will be necessary to access new value streams in the future.
- Vendor support will be required for nontrivial changes and modifications of the microgrid as a system, and of individual components.
    - Some vendors may require or request a continuous connection to the system for routine troubleshooting and calibration during its initial operation.
    - Many vendors are expected to require interactive remote access as a condition of warranty for their components.
- What other system interdependencies should the team consider? What risks do you see and what recommendations do you make?

Document what 'other' systems this system relies on and what effect a loss of the "other" systems may have on this system. Give special attention to your worst-case consequence.

"Other" System	Effect on this System

Document what effect on the "other" systems, the loss of functionality of this system may have. Give special attention to your worst-case consequence.

Which function of this system is lost	Effect on "Other" System

Digital Asset Awareness

The digitization of our energy infrastructure allows incredible benefits, providing speed and automation of operations not previously possible. However, digital assets and digitized functions have different weaknesses and frailty modes than their analog counterparts. Far beyond simply vulnerabilities to attack, these assets can function or be made to function in ways that their analog counterparts would not, and consideration of these risks is important to ensure that the defensive measures for a system are cyber-informed.

Digital asset awareness begins in design, by considering that any digital device is, at its core, a general-purpose computer with specific command logic for its function layered on top. An attacker, or more rarely, a logic failure can subvert this logic and cause the device to ignore input, change values in command logic or even execute commands or automated logic unexpectedly. The consequences considered earlier in the process can highlight specific impacts we want to mitigate in design, hopefully with controls that are not solely digital in nature.

Secondly, in operations digital devices require different forms of maintenance, including patching and upgrades and the export of logs and commands stored on the system. To ensure that such systems are maintained in accordance with the function of our system, we must track the devices installed by hardware model, software version, patch version, location, last update, last export, system function, etc. We should also export logs and, if possible, retain them for forensic needs, along with a "gold disk" configuration of the latest software and logic, if needed. This ensures that we understand where the systems are within our processes, what is occurring on them, how they are maintained, and any emerging risks which have been identified as vulnerabilities. It also ensures that we can restore or replace them if needed.

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

From the Project Team:

- Some existing systems may need to be changed and upgraded (configuration and physical)
    - Some of these changes will involve trading out analog systems for digital ones.
    - The Utility's operations team is very accustomed to the current systems, and the design team would like input about preparation and training to help the Utility build their understanding and comfort with more functional, digital equipment.
- The microgrid will bring some new functions, and interface with the existing distribution automation module for FLISR (fault location, isolation, and service restoration-automated switching routines in response to faults and associated current and voltage telemetry).
    - This will allow the microgrid to continue to provide uninterrupted service through different outage scenarios.
    - The team notes that it would also allow an adversary to use those same built in capabilities to make a switching sequence that would be undesired, dangerous, or maybe try to damage equipment by repeatedly closing into faults and it could cause larger outages, or worse.
    - The team would appreciate advice on how you advise how they use this function to increase reliability and at the same time, mitigate the risk of misuse, which is a new consideration with the upgrade, not formerly an issue.
- The project team notes that the microgrid project will include new servers, endpoints and supporting networking switchgear.

- Some of the communications between endpoints are new and the team hasn't thought through all the functions (desired and undesired) that communications complexity could cause.

Consider the equipment that could be part of a worst-case consequence identified previously and document the digital functions used in that type of equipment, and the effect if those functions are compromised.

Equipment	Common Digital Functions	Effect of Compromise

Cyber-Secure Supply Chain Controls

Even at the early design phases, engineers can begin to establish the core security features and assumptions which should be implemented by every supplier bringing components or services into the system. These may include guidelines about required features in digital systems, limits on where such systems can be acquired, and how updates must be verified and signed. They may include practices for vendor behavior when providing onsite or remote maintenance. They may include requirements for sharing information about cyber incidents, vulnerabilities, bills of materials and vendor development processes. Each of these controls contributes to the overall supply chain security of the system. These requirements should be discussed with the roles who may have a responsibility for ensuring them, including procurement, cybersecurity, and system operators.

For each control or feature, the team should consider how it will be verified, when it can be verified and how often, and who can perform the verification, (procurement, cybersecurity, operators, etc.). These processes should be built into requirements for development and operations of the system and verification should occur more than once for controls which could change or erode over time. The controls devised by the engineering team should be complimentary to those leveraged by the organization's purchasing and cybersecurity processes, but because they are drawn from potential catastrophic system consequences, they may well exceed the general due diligence performed by the organization.

Key Question: How do I ensure my providers deliver the security we need?

From the Project Team:

- Some of the potential vendors for the microgrid project components system are new to our organization, and it is very likely that most or all the potential vendors for building and integrating the microgrid once design is finalized will be new as well.
    - The project team would appreciate insights about how to begin vetting supply chain practices before a final selection is made.
    - The vendor's products surveyed so far are a mix of in-house-created code and integrated commercially available software and hardware components.
    - We expect the selected vendor to provide both onsite and remote support to the microgrid, once commissioned.
        - We do not yet understand the practices the vendors have for securing remote access.
- We have the ability to influence procurement and can provide insights into the terms of the service contracts but may also have to accept some vendor conditions in order to secure a purchase at a cost we can afford.
- We expect limits to the changes we can make and inspections we can perform on the installed system due to warranty terms and conditions.

Select one of the pieces of equipment from your worst-case consequence and express any insights you would like purchasing agents to know when procuring the equipment from the supplier (i.e. items to watch out for, priorities to enforce), and insights you would like integrators to know when implementing that piece of equipment.

Purchasing

Equipment	**Procurement Insights**

Integrators

Equipment	**Integrator Insights**

Planned Resilience

We must not only imagine a system's normal operation but also proactively plan for its potential failure modes, especially those linked to the most critical undesirable consequences. We must understand them, including how to operate through them, albeit at a lower level of performance or reliability. Ideally, a set of known diminished operating modes can be created which, though not ideal, can be built into expectations for well-understood modes of operation. Within each diminished operating mode, plans can be made for what would cause that mode, how that mode would function, and the changes to staff, systems, safety guidelines, performance, or other system conditions when it is assumed. Once part of our overall set of system operating modes, it is reasonable to train, exercise and assess our performance in each of these diminished modes on a regular basis.

These resilient diminished operating modes should include modes assumed because of a digital failure or cyber-attack. For any critical system, diminished operating modes should include operations during an expected cyber-attack involving one or several of those systems, operating when the team is uncertain of the validity of the data emerging from the system, where critical automation logic is not dependable, or where core network connections or support services are not available. It is likely that exercising these modes will require the operations team to pair with cybersecurity counterparts and understand the roles and responsibilities each will perform. Considering these operating modes may also require that the team consider altering the system design to allow limited manual operations options when digital systems are not operating or trusted.

Considerations for planned resilience should also include how untrusted systems can be restored to full function within the system context, including what operational steps will be required to ensure future trust, or whether that is possible given the function of the system or component.

Key Question: How do I turn my “what ifs” into “even ifs”?

From the Project Team:

- The primary benefit of this microgrid program is to improve service resilience within its footprint, so resilience is one of the most important features of the implemented system. If the microgrid doesn’t improve resilience, we will have failed.
- We recognize that our system must operate 24x7 and forever (or until it is replaced) in whatever environmental and operational conditions exist, even those we have not planned for or imagined.
    - From the prioritized consequence list developed by the team, are there particular adverse environmental or operational conditions for which we should develop diminished operating modes?
- We believe our organization has the knowledge, experience, and resources to operate the individual components of the microgrid manually without the full capabilities of the system.
    - We would appreciate insights about specific diminished operating modes we should consider for the microgrid.

Consider your worst-case consequence, document what an initial dimensioned operating mode may look like, including its effect and how long can that be sustained before it becomes untenable. Then indicate the actions (i.e. action plan) that would lead the system back to normal operating mode.

Initial Dimensioned Operating Mode	**Effects of Dimensioned Mode**
At what point does the dimensioned Operating Mode become untenable for the organization?	
Action Plan to return to Normal Operating Mode	

Engineering Information Control

From the first conception of a system until its retirement, immense amounts of information are created about how the system is designed, the elements and components within it, the skills required to operate it, its performance, procedures for maintenance and operations, and more. This information, in the wrong hands, can aid an adversary to understand system weaknesses, existing component vulnerabilities and even human targets to aid in planning their attack. This information can be released during procurement processes, often shared via public release to ensure an open and fair competitive process. It can be released in job listings, where specific technical criteria are used to find good employment candidates but may also tip an adversary to system features or vulnerabilities. It can be shared in news articles or success stories about the system's entry to operations, where even a system photograph may release information helpful to an adversary.

During the system design process, the engineering team can begin to identify, using the prioritized list of consequences developed earlier, the specific information which would be of most value to an adversary to enact an undesired consequence. They can develop administrative processes for protecting the information, determining who can possess it, how to prevent inadvertent duplication and sharing, how to remove access, how to review and approve information release, how to ensure team members understand the sensitivity of the information they have access to and how to protect it, etc. Because engineering systems are in active use, sometimes for decades, it is crucial that even the earliest information about the system design be protected throughout the lifecycle of the system.

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

From the Project Team:

- We must release a significant amount of our electrical and controls and other sensitive design information to vendors during the procurement process.
    - We recognize that they may involve one or several subcontractors who will be part of their solutions team.
    - We would appreciate insights on how we can build information protection criteria into NDA's signed during the procurement process and how we can ensure that information provided to vendors and their subcontractors remains under our control, to the degree possible, and is not copied or stored by the vendors.
- We believe that there will be significant publicity and media releases about the new microgrid once it is complete.
    - When we select a vendor, they will want to publicize information about their selection and the magnitude of the project they are supporting.
    - When they complete the project, they will want to share information about it, and the beneficial features of the system they installed with future customers.
        - We have seen similar case studies on prospective vendor websites.
    - Our organization will want to alert rate payers to the benefits they will receive from our automation investment and is likely to publish a selection of news articles, both locally and on our website.
    - How can we create plans to ensure that these expected information releases are controlled and do not share more information than we deem appropriate?

- We are likely to hire a small number of temporary employees for the upgrade, some who could transition to permanent status in our operations team.
    - Several will need specific technical skills to be successful in the role we imagine, and we have identified some of the needed skills to be potentially sensitive.
    - Once we release temporary employees hired for the microgrid implementation, we will have to ensure that they do not retain copies of system information.
- What insights do you have about how to best protect our engineering information?

Considering the worst-case consequence and the equipment involved, identify any engineering information deserving of information control protections. For example, make and model of specific equipment involved, software applications used, or material suppliers.

If any of the identified information was given to an adversary through some means such as social media, job posting, etc., how might it be used to compromise the equipment/system and lead to the worst-case consequence?

Organizational Culture

Shared beliefs, perspectives and values about cybersecurity determine how a group will prioritize investments and actions to improve its realization. For a culture which does not value cybersecurity, whether they see it as an unnecessary expense, a low risk or impact, or an impediment to productivity, there will not be a desire to invest in people, processes, and technology to provide cybersecurity. An engineering design team, cognizant of the consequences of digital failure or cyber-attack on a system under design has a core responsibility to aid the entire set of stakeholders who are accountable, responsible, consulted or informed about the system to understand the need for cybersecurity and how each stakeholder's role can affect, both positively and negatively, the overall security of the system.

To build a culture of cybersecurity around the system design process, engineering design teams can emulate best practices for building a safety culture. These include having regular discussions about how and why cybersecurity is incorporated into the system, recognizing, and celebrating good decisions and right actions of team members and treating failures as opportunities for learning and improvement. Because team members external to the design process may not recognize how their job role can contribute to or diminish the cybersecurity of the overall system, it is important for the design team to personalize conversations to the individual. As discussed earlier under supply chain controls, these discussions should extend to everyone involved with the system, even a subcontractor or external service provider. Each person interacting with the system should understand the importance of ensuring its security and how their role contributes to that function.

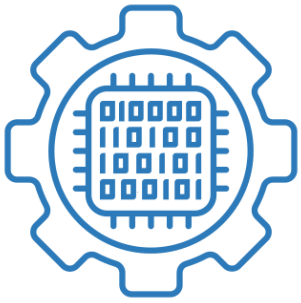
Key Question: How do I ensure that everyone performs their role aligned with our security goals?

From the Project Team:

- Our team is hard-working and values productivity highly. There is a risk, as we institute new processes and procedures, that the team will develop workarounds which allow them to keep their accustomed tools or modes of performance.
    - We seek insights about how to curb this behavior and how to discover it if it is occurring.
    - Also, how we can develop a process, not to blame staff, but to coach and instruct them to more desirable behaviors.
- This upgrade will require different leader, manager, and worker behavior for some existing roles, from procurement to HR, throughout our IT and plant operations team.
    - We expect to conduct an all-hands meeting to inform the team about our overall approach to engineering in security, but we know that won't be enough.
    - We seek advice about how we can identify and nurture good individual behaviors and organizational choices surrounding the microgrid project (actually, all our functions and infrastructure).
    - How can we ensure that new hires get the same acculturation?
- Leadership is accepting of a security by design approach now but may change their minds if the system runs into delays or additional expenses perceived to be caused by the approach.
    - How can we help leadership appreciate the value of cybersecurity over longer time frames?

Consider and document how each of the roles below are involved with defensive controls of this system. Identify how the culture should reinforce their responsibilities.

Operations Team	**Cybersecurity Team**
Safety Team	**Management Team**
Legal/Procurement/HR Teams	**Engineering Team**

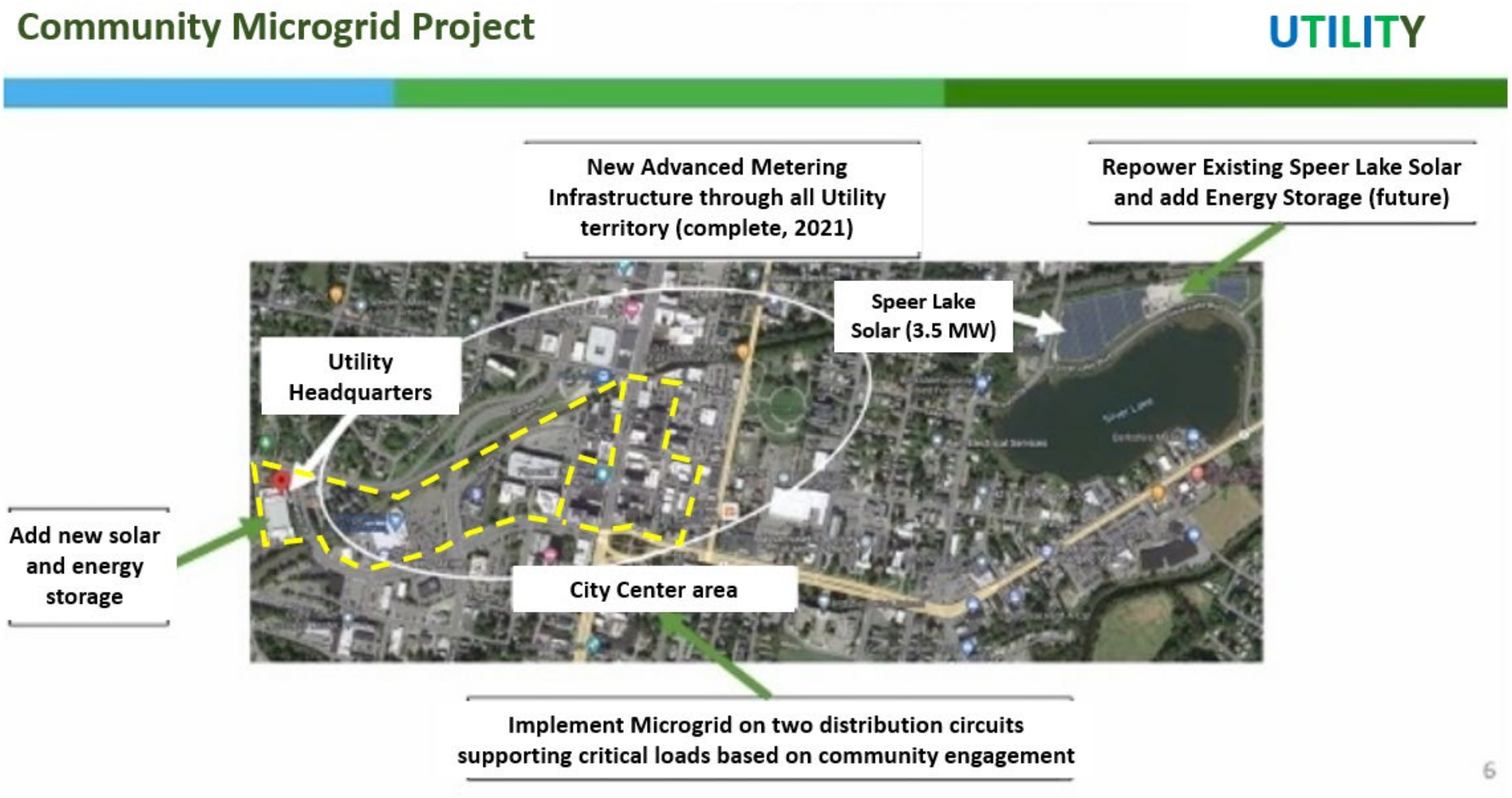


Cyber-Informed Engineering

Cybersecurity for Microgrids Workshop Workbook Attachment

CONTENTS

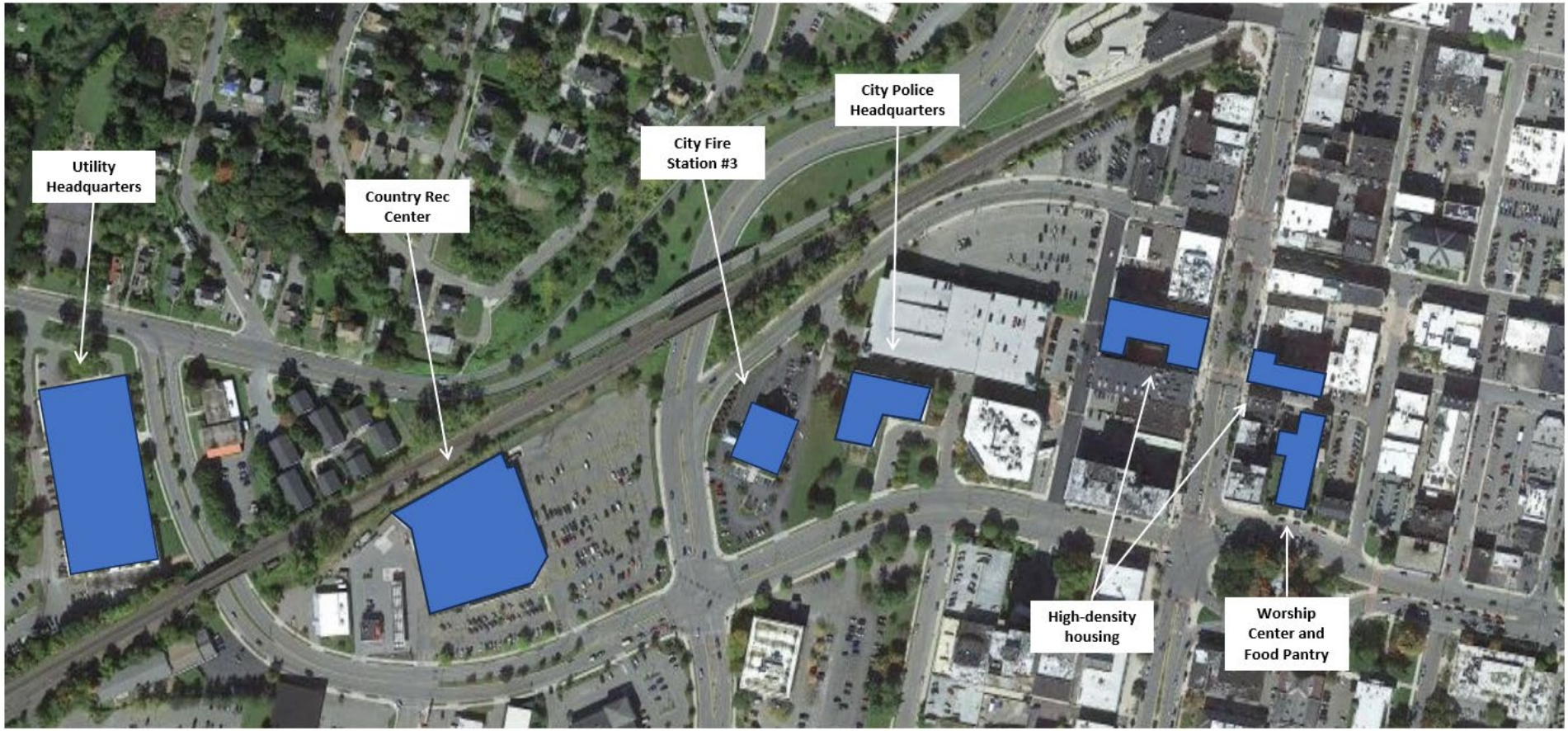
I – Community Microgrid Project Overview



[c]

[c] Slide created by INL from Google Maps imagery

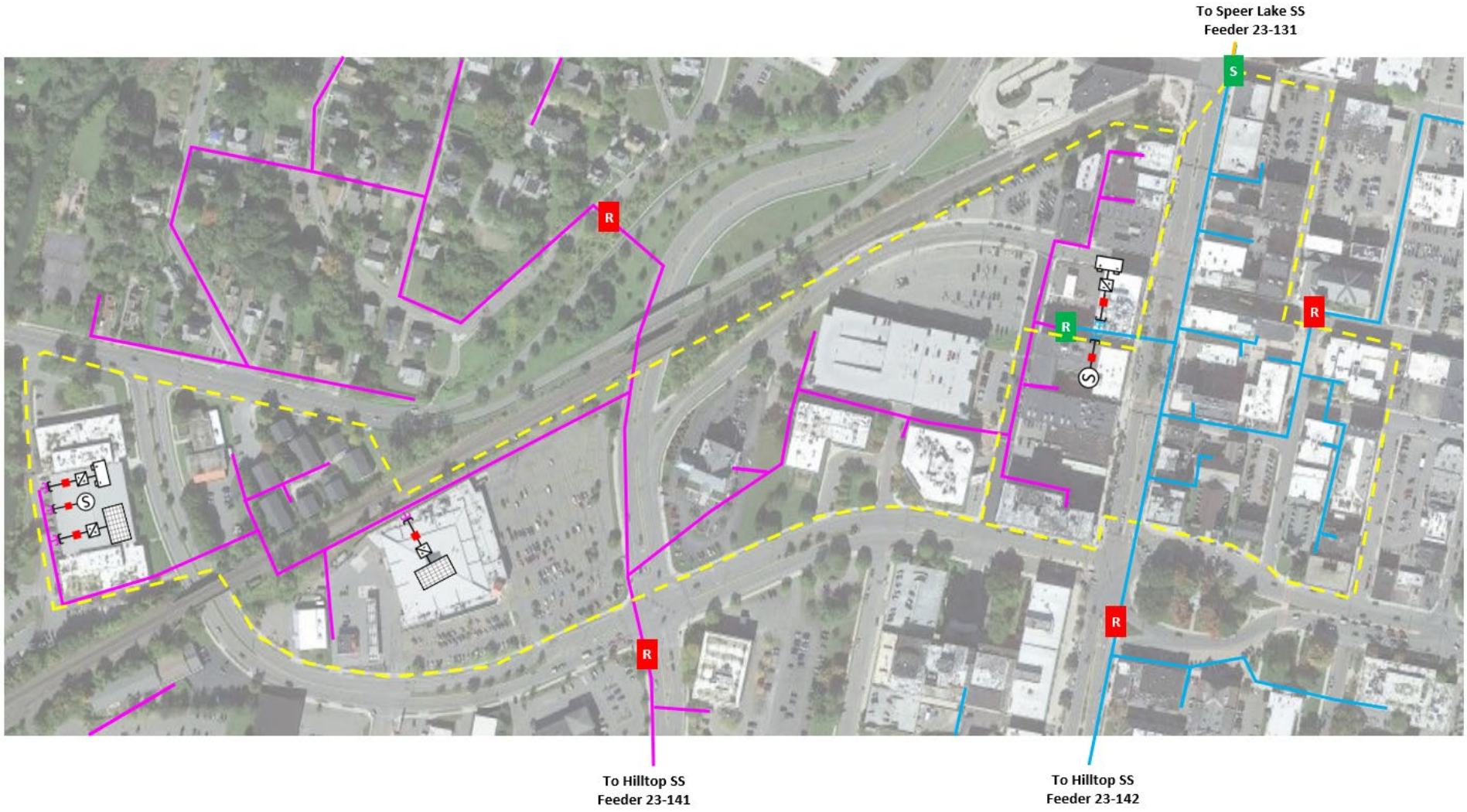
II – Community Microgrid Project Map



d

[d] Slide created by INL from Google Maps imagery

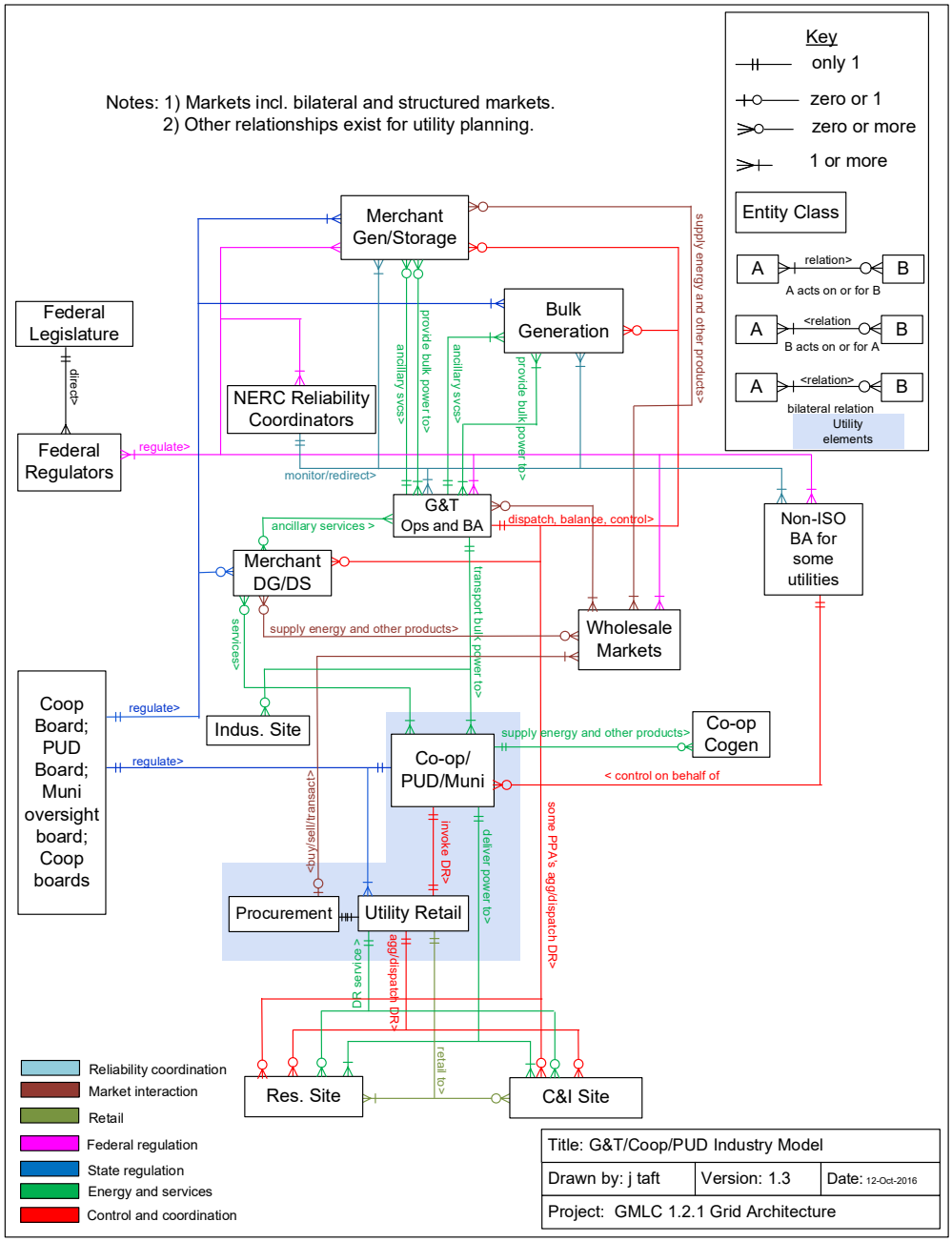
III – Community Microgrid Project Distribution Circuits



e

[e] Slide created by INL from Google Maps imagery

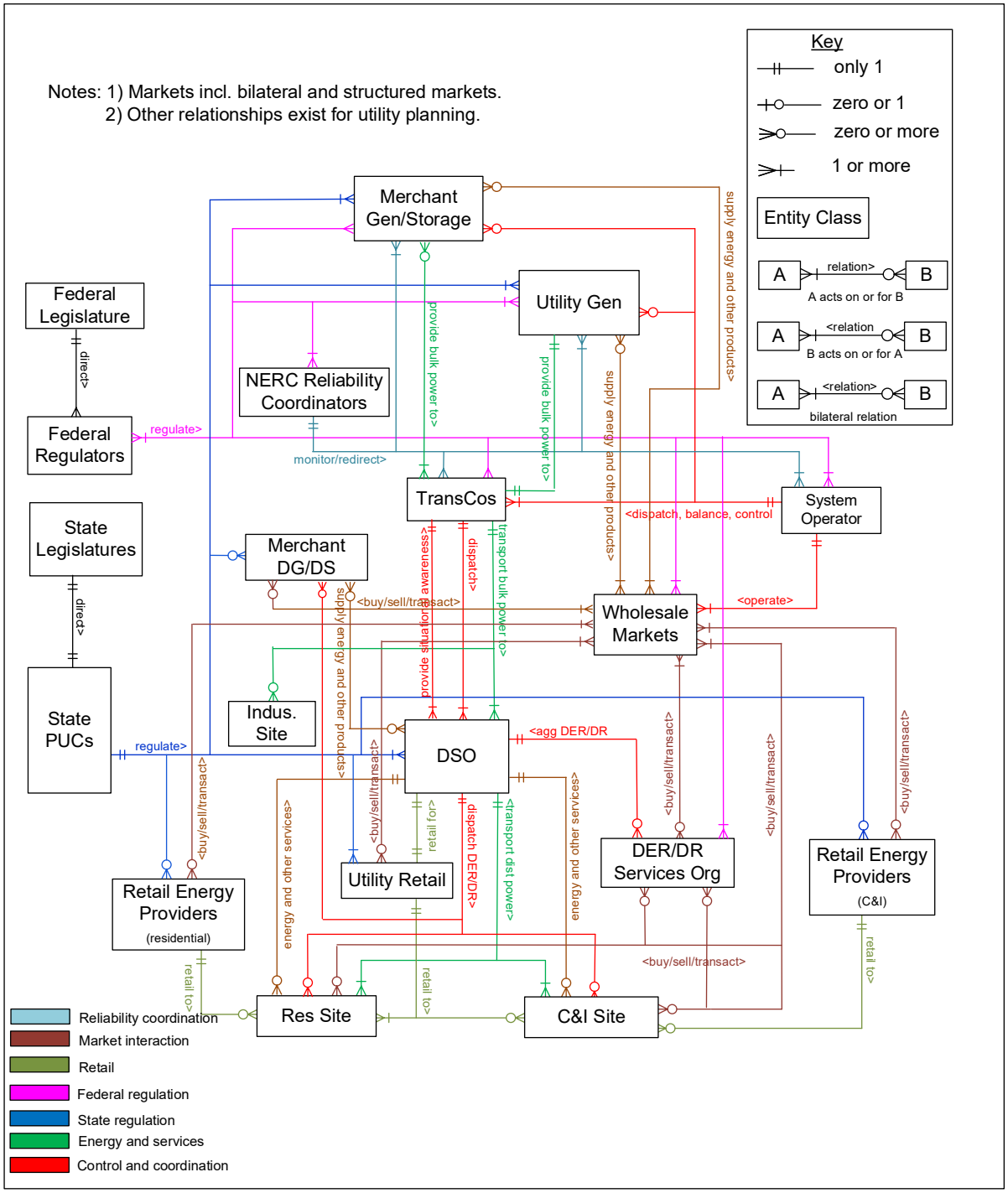
IV - Industry Model (From GMLC Grid Architectural Project)



This image was formed by a DOE Grid Modernization Laboratory Consortium (GMLC) project focused on developing utility reference architectures. The depiction of the Coop/Muni/PUD shows a visual representation of their generic critical functions.[f]

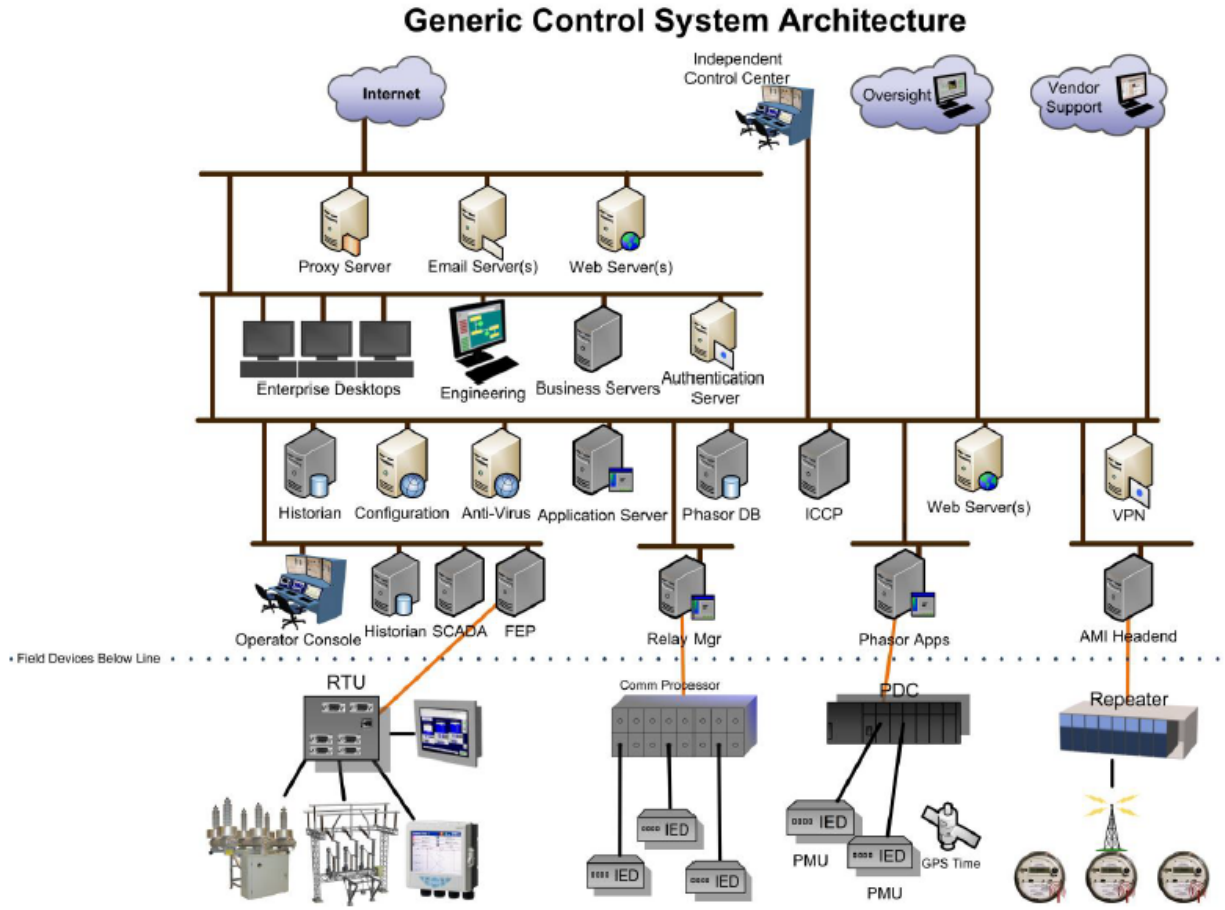
[f] Diagrams are from https://gridarchitecture.pnnl.gov/library.aspx in the "Miscellaneous GMLC Architecture Diagrams and Other Documents" .zip file in the "GMLC 1.2.1 Grid Architectur [sic] Misc Diagrams" .pptx file

V - Potential Distribution System Operator Function Illustration (From GMLC Grid Architectural Project)



This image was formed by the same DOE Grid Modernization Laboratory Consortium project. The DSO role depicted in the drawing shows functions which may emerge for this utility in the future after the microgrid project, and not causally related to it.[g]

VI - Generic Information Architecture for a Control System

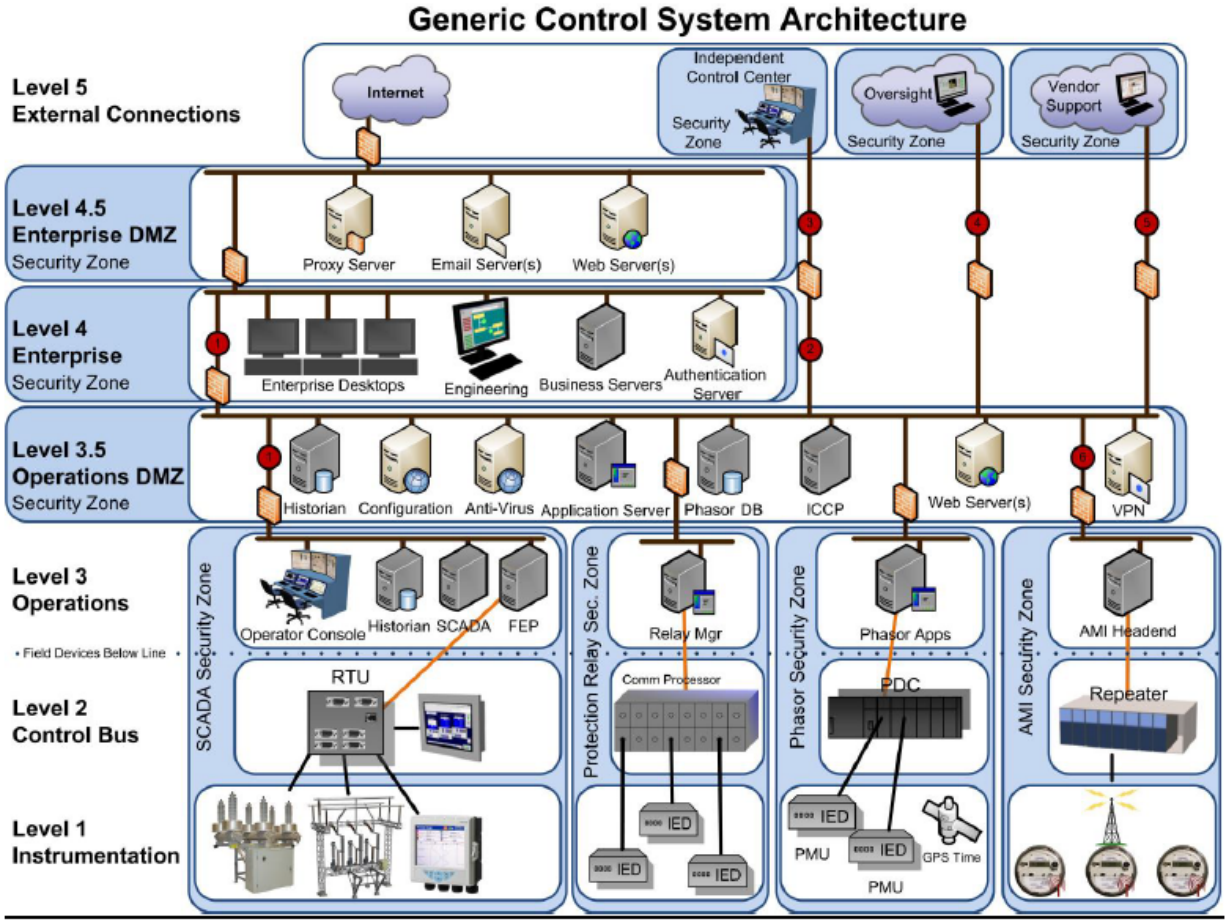


This generic control system architecture and its companion, next page, developed by PNNL in 2011 show a generic control system architecture and then a proposed segmentation plan which may be helpful in considering a **secure information architecture**. The community microgrid will interface with this utility architecture, so think about which elements are present in your organization, and what changes may be needed alongside the microgrid implementation.[h]

[g] Diagrams are at https://gridarchitecture.pnnl.gov/library.aspx in the "Miscellaneous GMLC Architecture Diagrams and Other Documents" .zip file in the "GMLC 1.2.1 Grid Architectur [sic] Misc Diagrams" .pptx file

[h] Diagrams from https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf

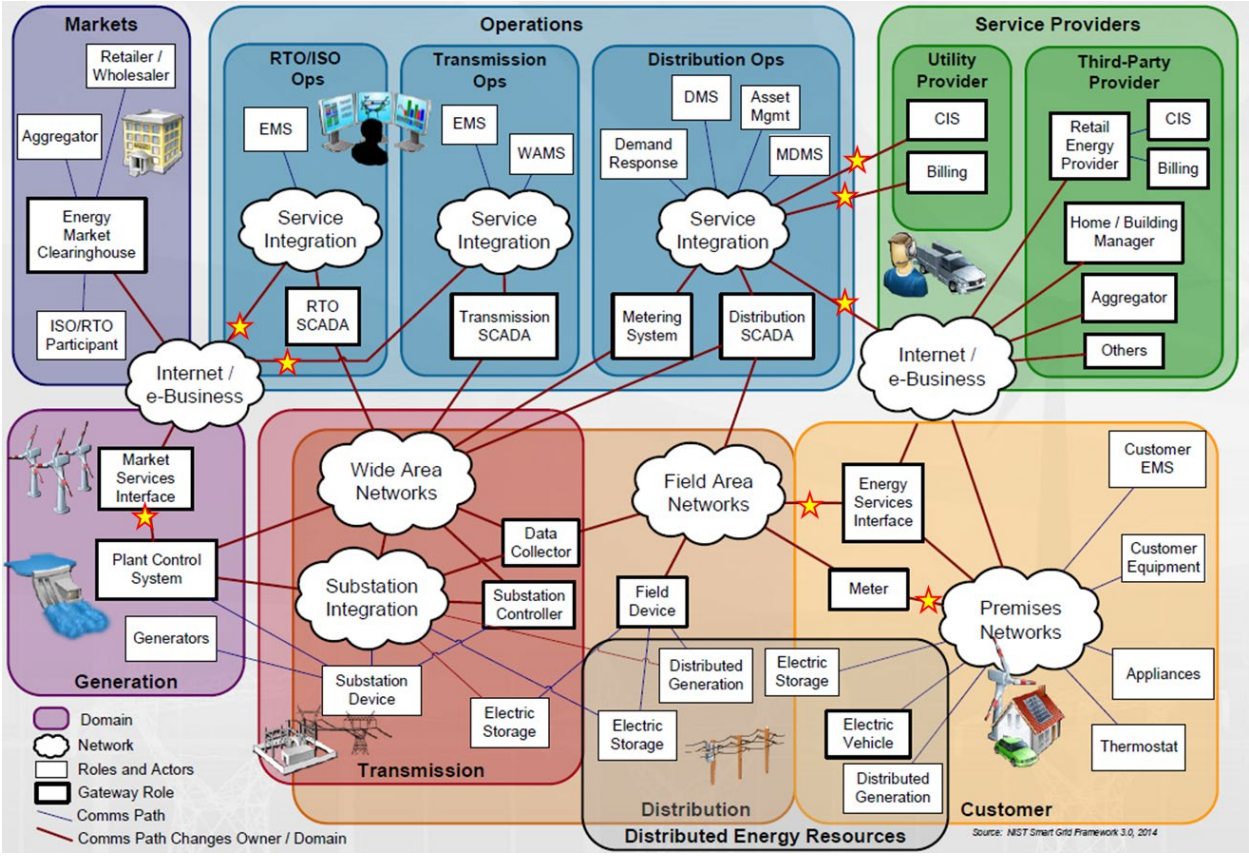
VII – Generic Segmented Information Architecture for a Control System



[i]

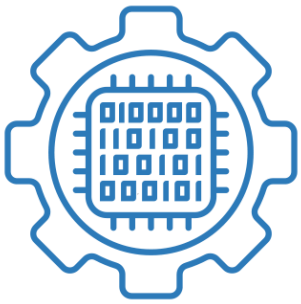
[i] Diagrams from https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf

VIII – Distribution Interconnections



The NIST legacy framework offers some ideas to consider as the team analyzes **interdependencies** and the impact they could have on the project. The stars represent boundaries between a control system owned by a utility (though maybe not your utility) and a lower-trust external IT system.[j]

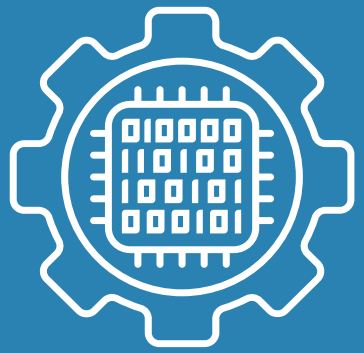
[j] Diagram from https://www.nist.gov/system/files/documents/2019/06/06/presentations-day1.pdf



Cyber-Informed Engineering

Cybersecurity for Microgrids Workshop Slides

Document Number: INL/MIS-24-76646



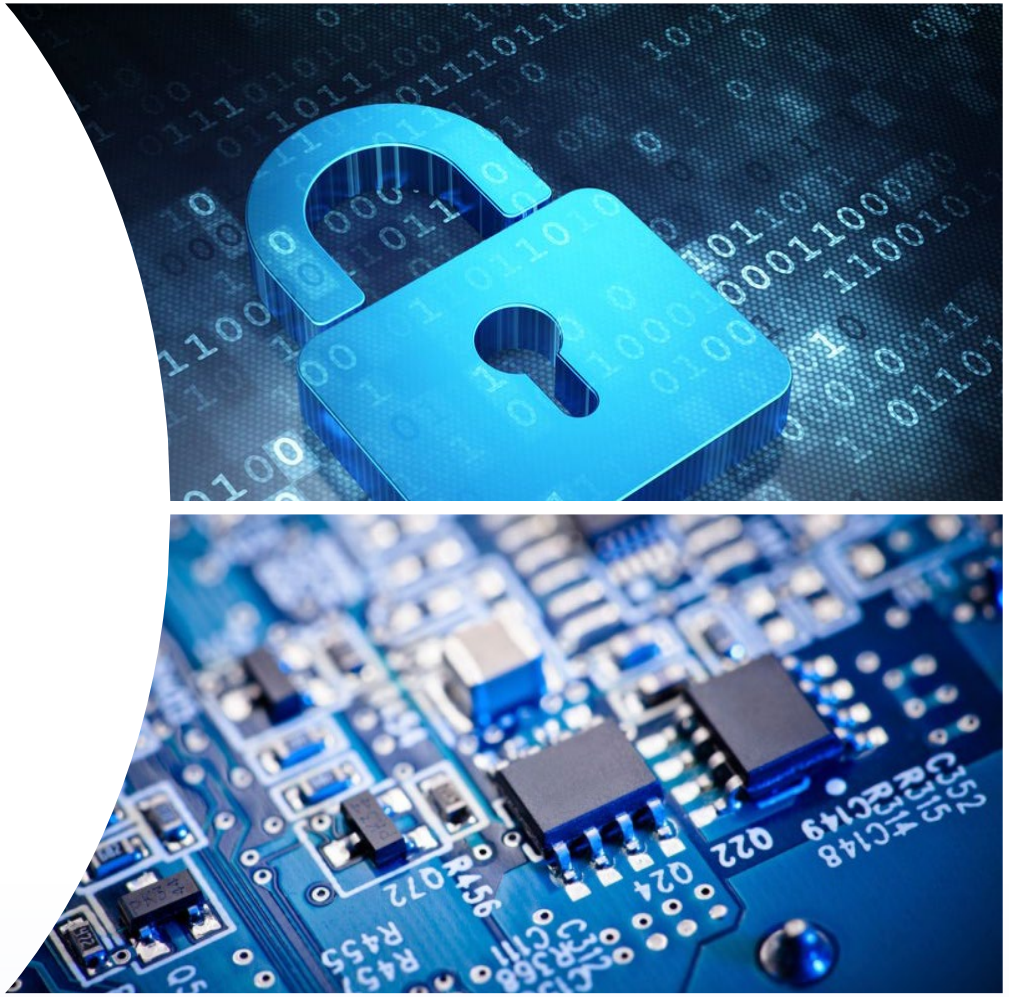
Cyber-Informed Engineering

Principles of CIE

Document Number: INL/MIS-24-76646

Cyber-Informed Engineering (CIE)

- CIE uses **design decisions and engineering controls** to eliminate or mitigate avenues for cyber-enabled attack.
- CIE offers the **opportunity to use engineering to eliminate specific harmful consequences** throughout the design and operation lifecycle in addition to traditional cybersecurity controls.
- Focused on **engineers and technicians**, CIE provides a framework for cyber education, awareness, and accountability.
- CIE aims to build **a culture of cybersecurity** aligned with the existing industry safety culture.



Document Number: INL/MIS-24-76646

Key Premises of the CIE Strategy

Today's risk landscape calls for systems that are engineered to continue operating critical functions while faced with increasingly severe and sophisticated cyber attacks from intelligent, determined adversaries.

While specialized IT and OT cybersecurity experts bring strong skills, **many engineers and technicians who design, operate, and maintain control systems with digital components currently lack sufficient cybersecurity education** and training to adequately address the risk of cyber-enabled sabotage, blended attacks towards the theft of nuclear material, exploitation, failure, and misuse in the design, development, and operational lifecycle.

Accelerating industry's adoption of a culture of cybersecurity by design—complementing industry's strong culture of safety—offers the ability to maintain secure design even as systems evolve and grow in functionality.

CIE offers an opportunity to reduce risk across the entire device or system lifecycle, starting from the earliest possible phase of design.

Early in the design phase is often the most optimal time to achieve low cost and effective cybersecurity, compared to solutions introduced late in the engineering lifecycle.

Document Number: INL/MIS-24-76646

CIE and the Systems Engineering Lifecycle

Document Number: INL/MIS-24-76646

Cyber-Informed Engineering

CIE Principles

PRINCIPLE	KEY QUESTION
Consequence-Focused Design	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?
Engineered Controls	How do I select and implement controls to minimize avenues for attack or the damage that could result?
Secure Information Architecture	How do I prevent undesired manipulation of important data?
Design Simplification	How do I determine what features of my system are not absolutely necessary to achieve the critical functions?
Layered Defenses	How do I create the best compilation of system defenses?
Active Defense	How do I proactively prepare to defend my system from any threat?
Interdependency Evaluation	How do I understand where my system can impact others or be impacted by others?
Digital Asset Awareness	How do I understand where digital assets are used, what functions they are capable of, and what our assumptions are about how they work?
Cyber-Secure Supply Chain Controls	How do I ensure my providers deliver the security the system needs?
Planned Resilience	How do I turn “what ifs” into “even ifs”?
Engineering Information Control	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
Organizational Culture	How do I ensure that everyone’s behaviors and decisions align with our security goals?

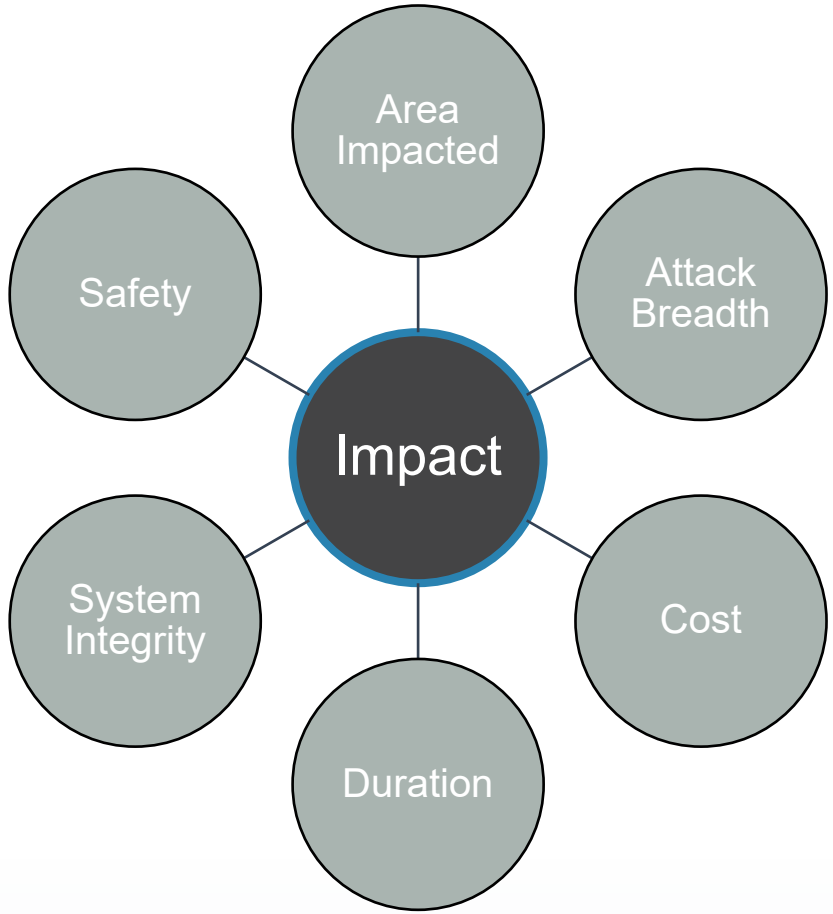
Document Number: INL/MIS-24-76646

Consequence-Focused Design

KEY QUESTION

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

- What is normal operation?
- What is the worst consequence of this operation?
- What are the system's critical functions?
- What is my risk appetite?

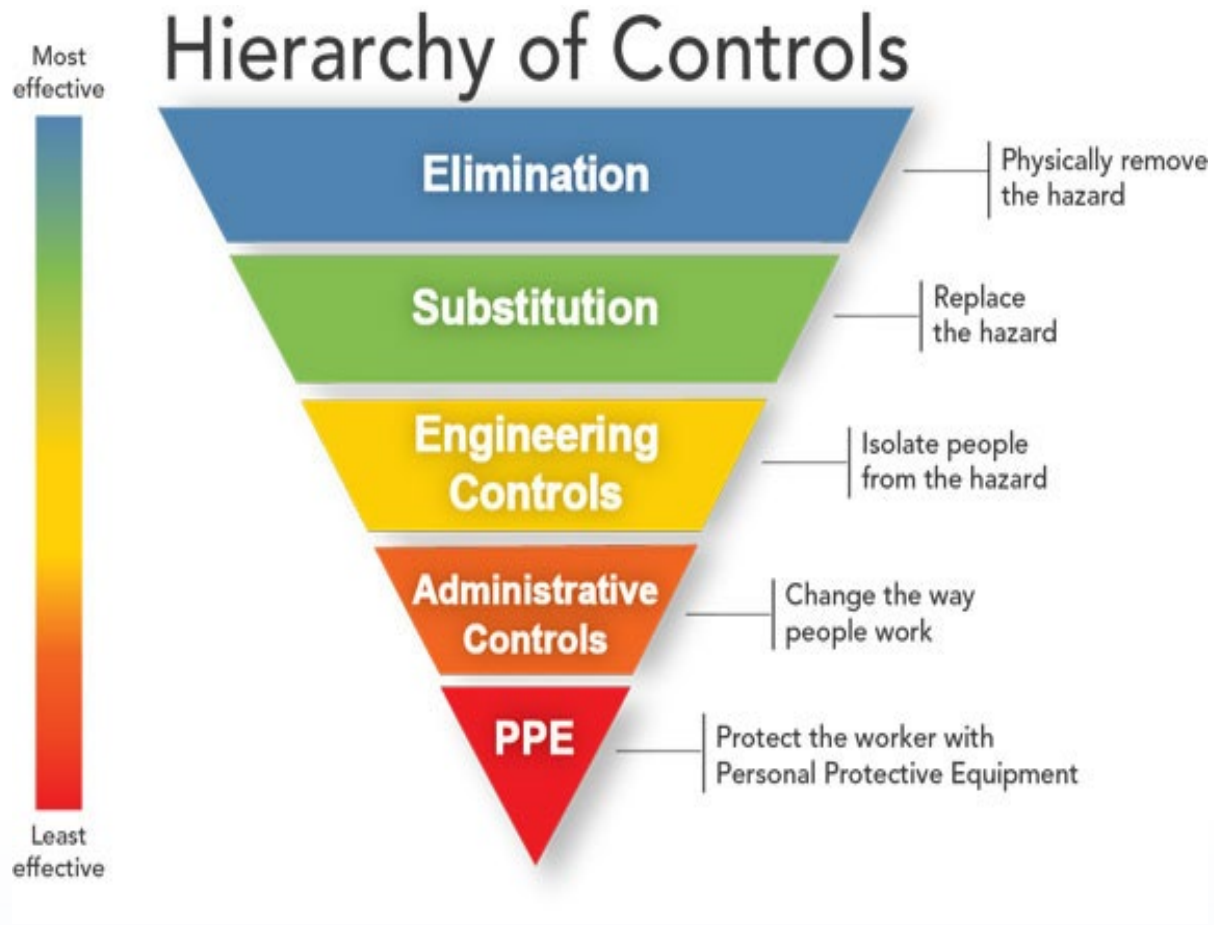


Document Number: INL/MIS-24-76646

Engineered Controls

KEY QUESTION

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



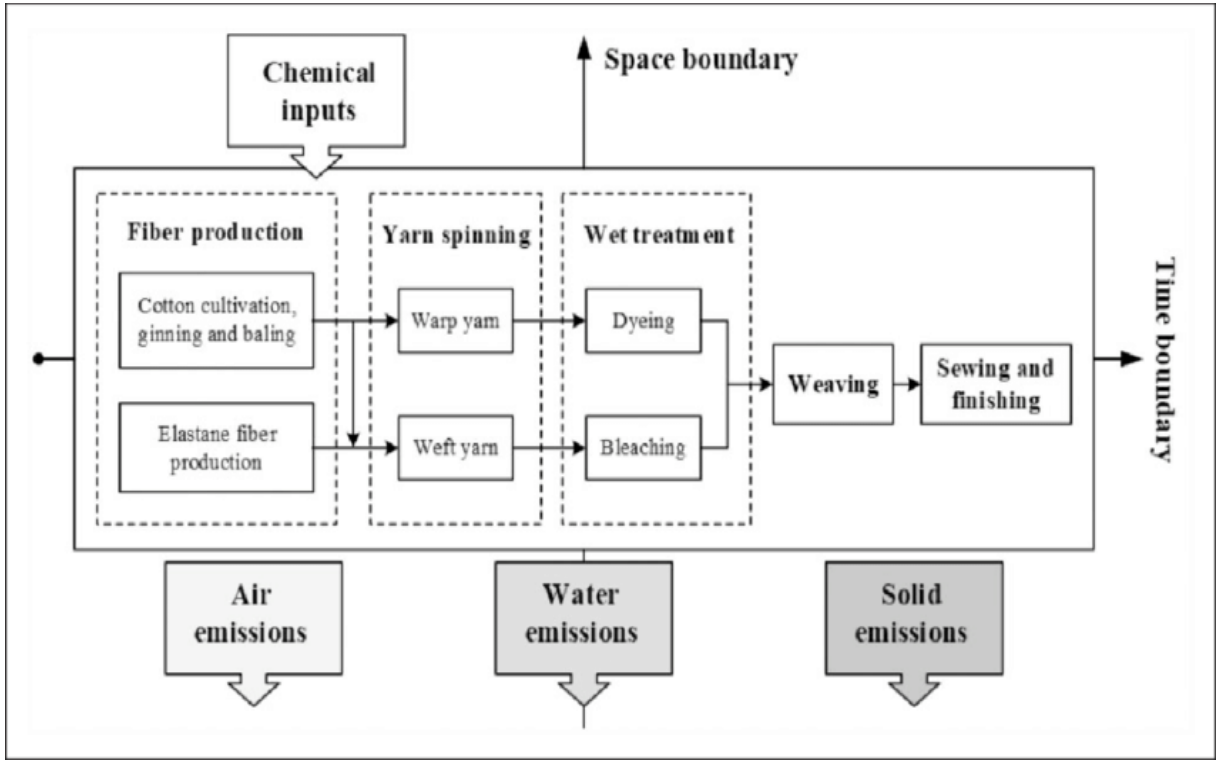
Graphic adapted from: CDC NIOSH - https://www.cdc.gov/niosh/topics/hierarchy/default.html

Document Number: INL/MIS-24-76646

Secure Information Architecture

KEY QUESTION

How do I prevent undesired manipulation of important data?



For our critical functions:

- What is the critical data?
- What systems originate, change, and validate?
- How will data flow?
- How should we group the data flows and data?
- How can we create monitorable boundaries?
- Where are areas of implicit trust?

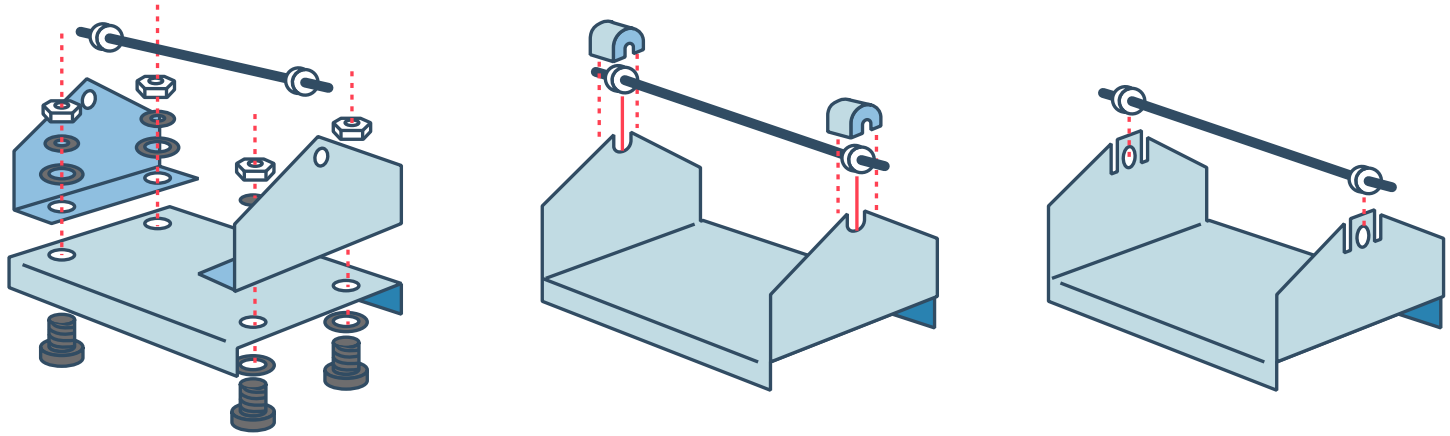
Document Number: INL/MIS-24-76646

Design Simplification

KEY QUESTION

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

- Are all of the elements of my design actually required?
- How do I reduce complication?
- What do I lose by simplifying?



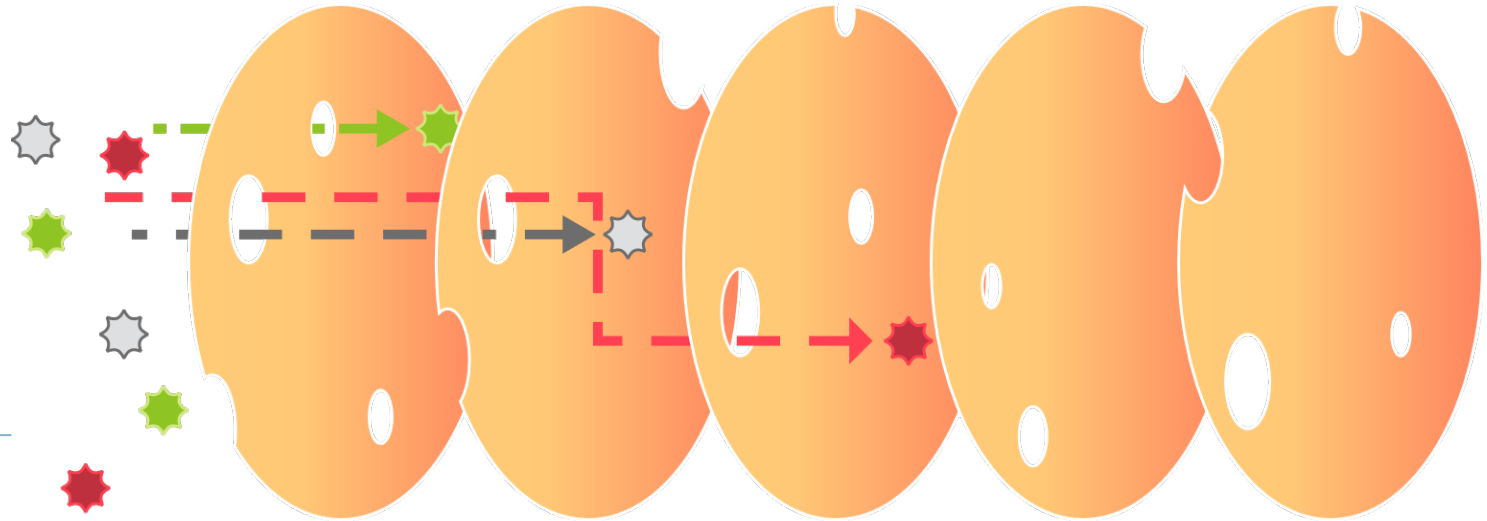
Graphic adapted from: http://www.slideshare.net/BabasabPatil/product-design-ppt-doms

Document Number: INL/MIS-24-76646

Layered Defenses

KEY QUESTION

How do I create the best compilation of system defenses?



Reason's Swiss Cheese Model adapted from: https://skybrary.aero/articles/james-reason-hf-model

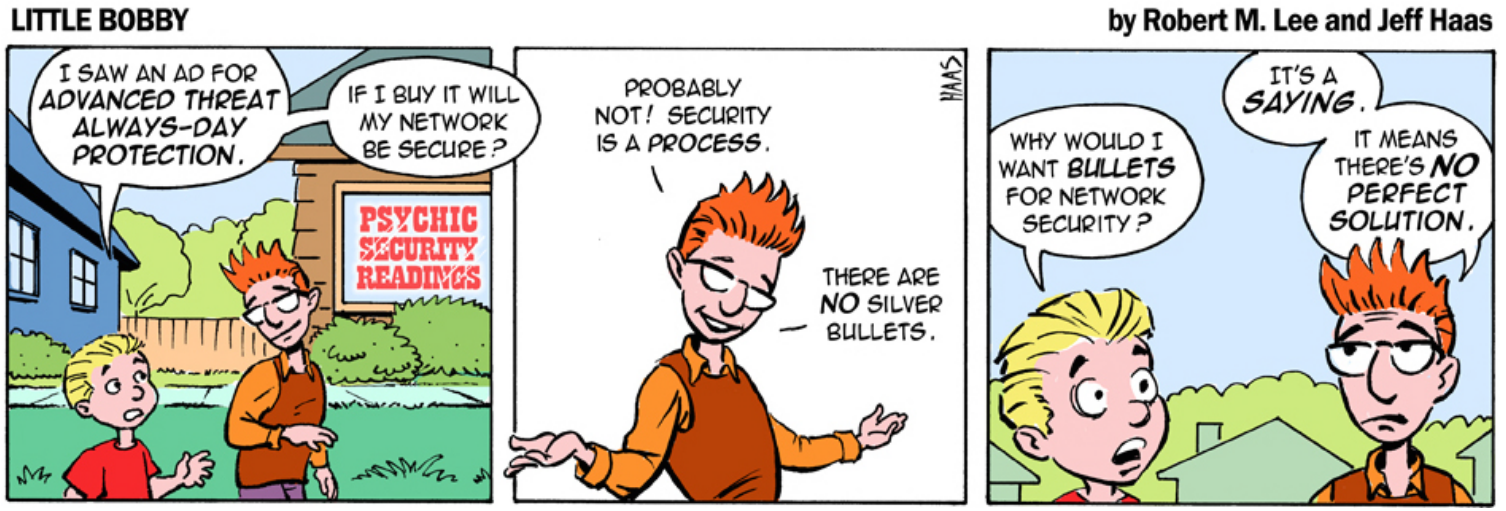
Document Number: INL/MIS-24-76646

Active Defense

KEY QUESTION

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

- How do I protect what I designed?
- How can engineers and IT collaborate in defense?
- How do we exercise/practice defense?
- Have we developed policies and procedures?



Used with permission from: https://www.recordedfuture.com/active-cyber-defense-part-2/

Document Number: INL/MIS-24-76646

Interdependency Evaluation

KEY QUESTION

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

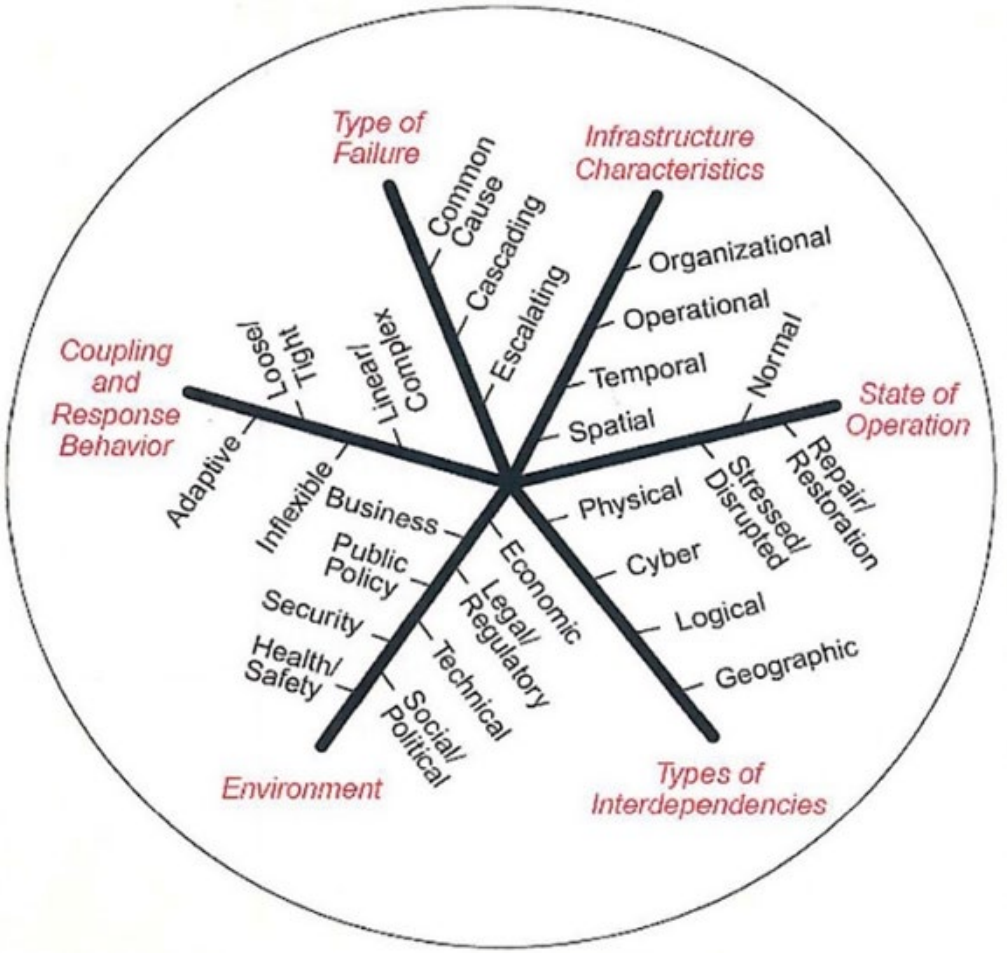


Image adapted from: http://witandwisdomofanengineer.blogspot.com/2010/11/infrastructure-interdependencies.html

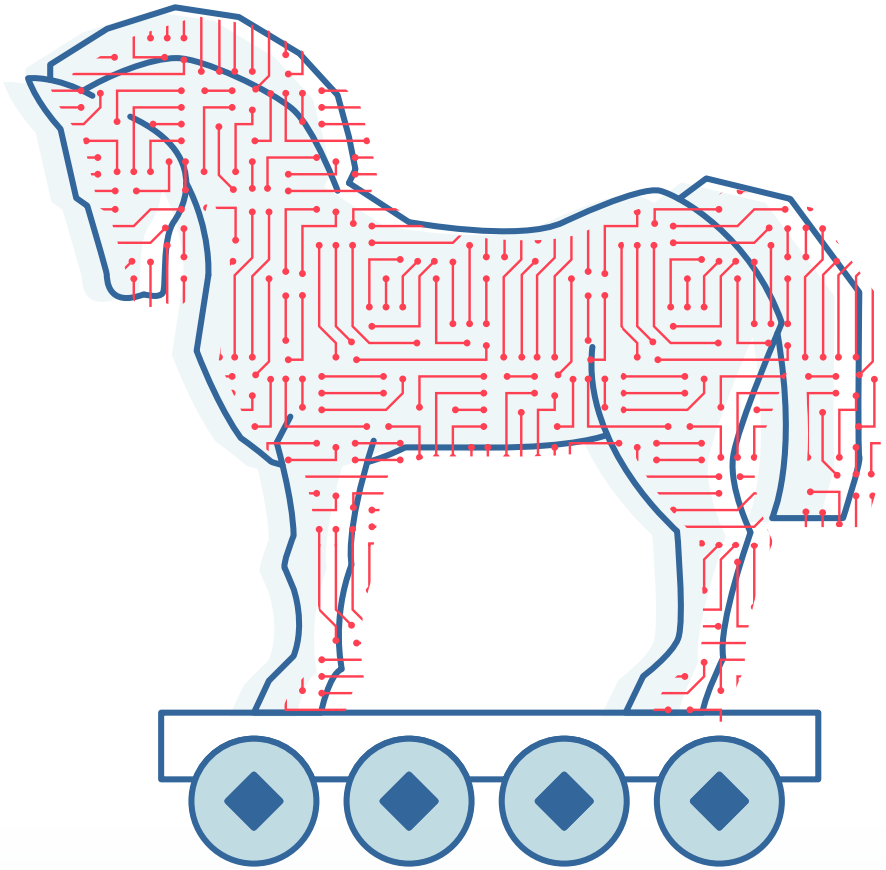
Document Number: INL/MIS-24-76646

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?

- Digital systems are different from their analog counterparts
  - Turning off features doesn't remove them
  - Digital features area a source of different risks
- One way of tracking risk is keeping an inventory of digital assets
  - Simple? Maintaining accuracy is not simple
- How do you protect this information?

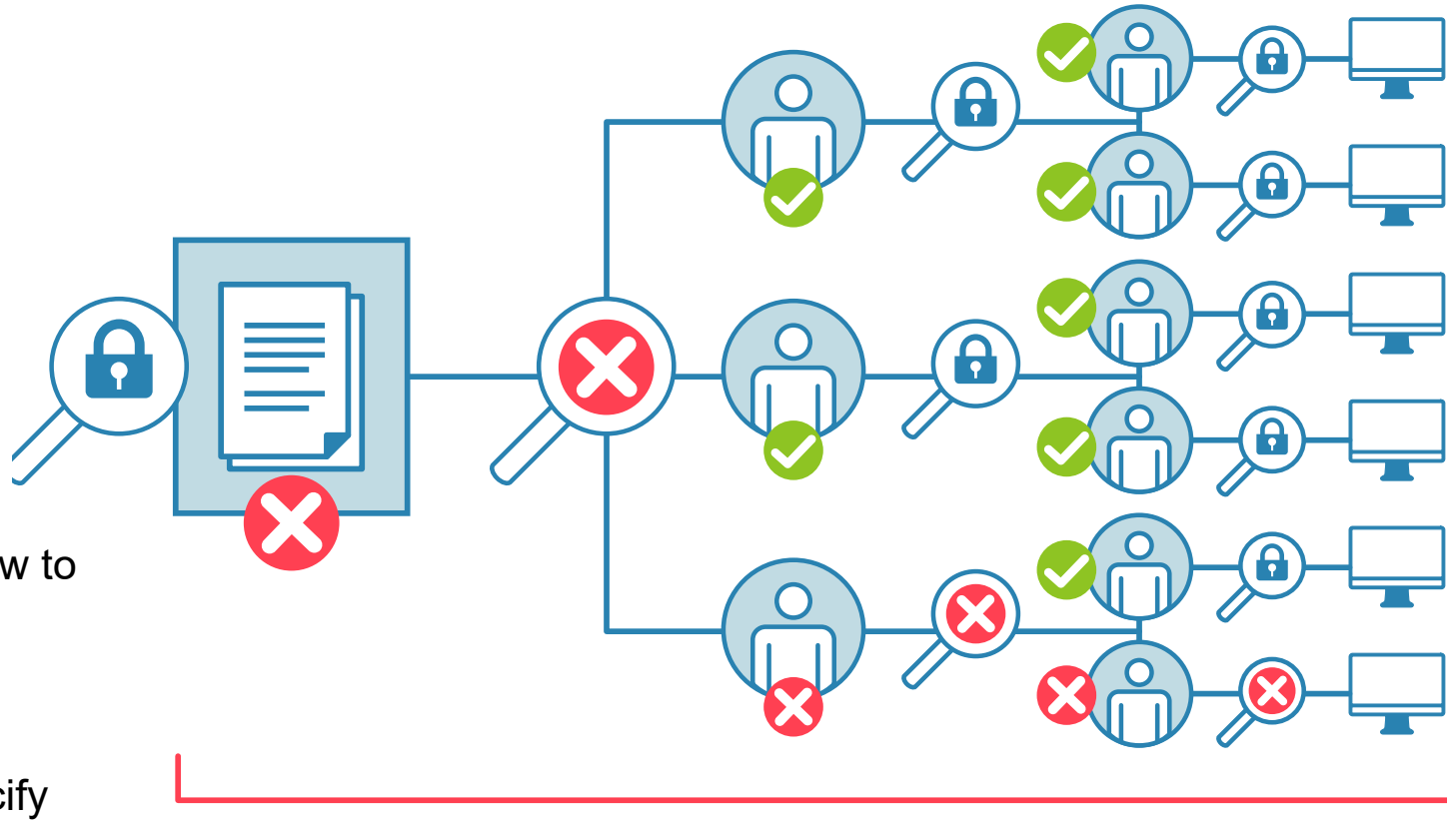


Document Number: INL/MIS-24-76646

Cyber-Secure Supply Chain Controls

KEY QUESTION

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



- How do cyber security requirements flow to vendors, integrators, and third-party contractors?
  - What assumptions are we making?
- Does procurement language must specify the exact requirements a vendor must comply with as part of the system design, build, integration, or support?
- How do we verify compliance?

Document Number: INL/MIS-24-76646

Planned Resilience

KEY QUESTION

How do I turn "what ifs" into "even ifs"?

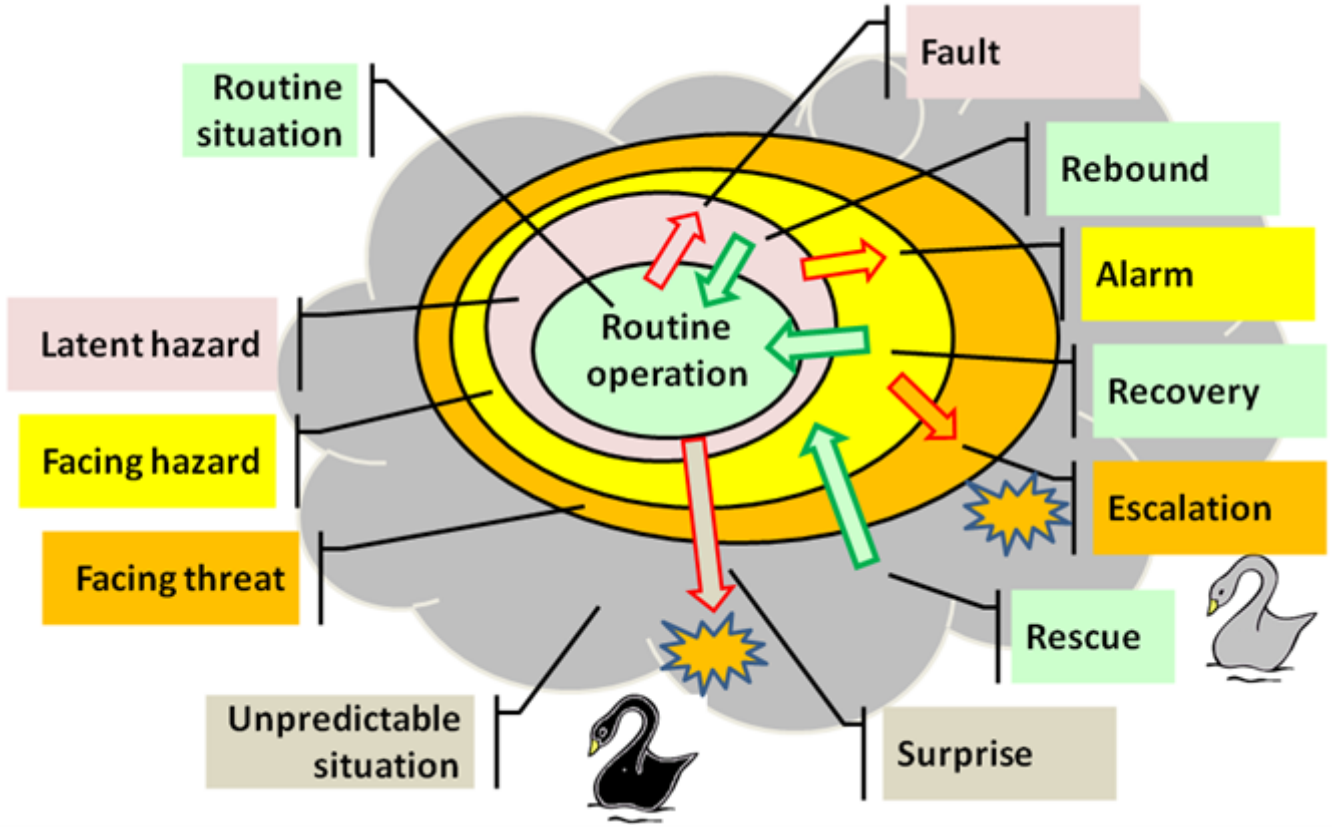


Image from:
https://upload.wikimedia.org/wikipedia/commons/9/9c/Resilience_model.png

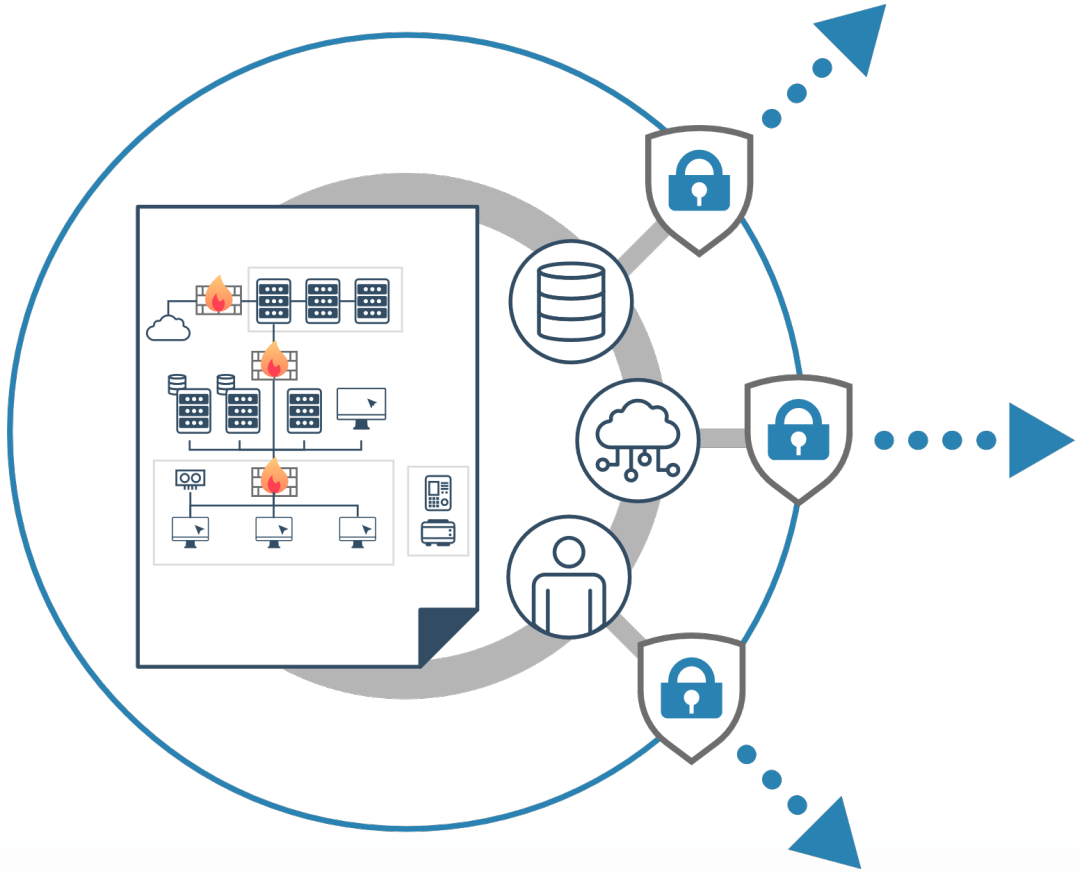
Document Number: INL/MIS-24-76646

Engineering Information Control

KEY QUESTION

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

- **What** information should we protect?
- **Who** has and should have it?
- **How** do we protect it?



Document Number: INL/MIS-24-76646

Organizational Culture

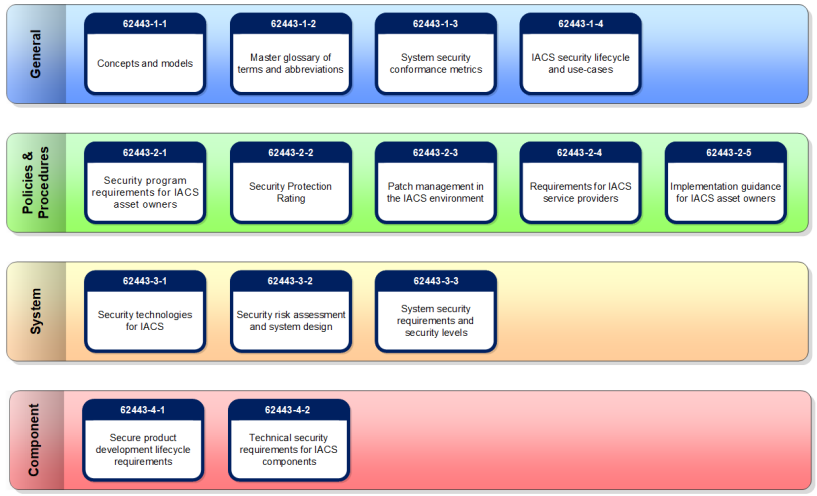
KEY QUESTION

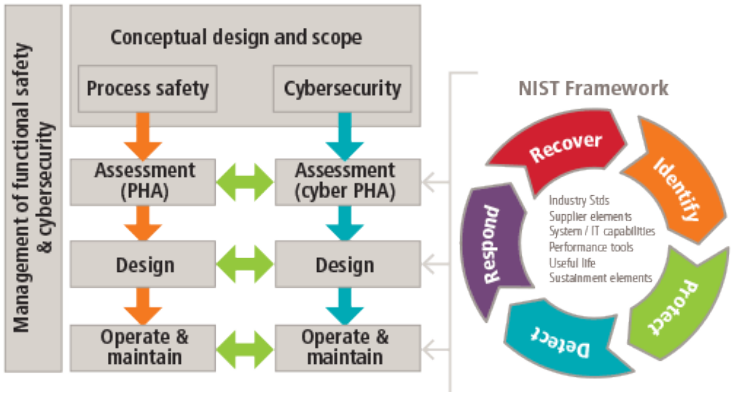
How do I ensure that everyone's behavior and decisions align with our security goals?

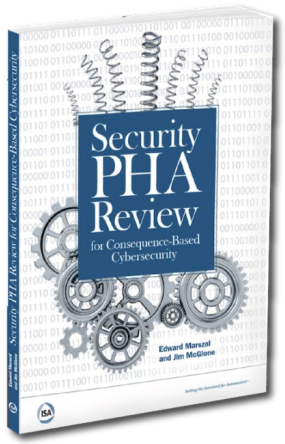
- Include cyber security into engineering and engineering into cyber security
- Ensure entire staff is enlisted and endorses cyber security
- Ensure staff understand and follow processes and procedures
  - All it takes is one user to lower security posture
- How do we encourage a questioning attitude?
- How can we provide the same rigor for cybersecurity as physical protection security and safety?

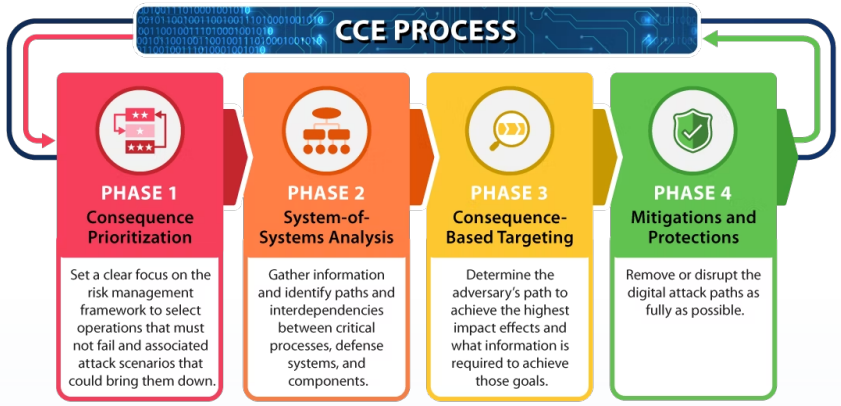
Document Number: INL/MIS-24-76646

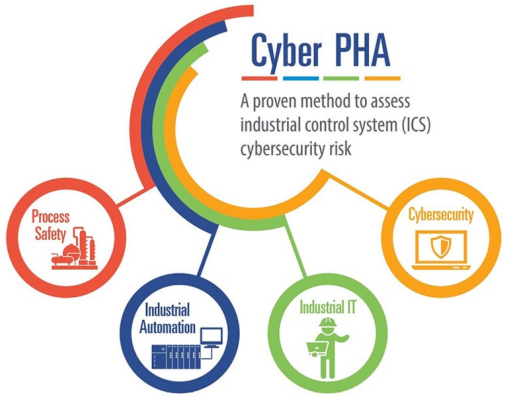
OK, But How Do You CIE?











Document Number: INL/MIS-24-76646

Resources

- Cyber-Informed Engineering Implementation Guide – https://www.osti.gov/biblio/1995796
- National Cyber-Informed Engineering Strategy – https://bit.ly/3z2yI3F
- Cyber-Informed Engineering – www.inl.gov/cie
- Consequence-Driven, Cyber-Informed Engineering – www.inl.gov/cce
- To join the CIE COP, email – CIE@inl.gov

Document Number: INL/MIS-24-76646