INL/CON-23-72563
Revision 000

Using Cyber-Informed Engineering for Cyber Defense Workbook

May 6, 2023

Virginia Wright
CIE Program Manager, INL

Sam Chanoski
Technical Relationship Manager, INL

Tony Turner
CEO, Opswright

Sarah Freeman
Principal Cyber Engagement Operations Engineer, MITRE

Document approved for release as INL/CON-23-72563

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

CONTENTS

FIGURES

Page intentionally left blank

ACRONYMS

ADMS	Advanced Distribution Management System
BES	Bulk Electric System
CIE	Cyber-Informed Engineering
COVID	Coronavirus Disease
DOE	Department of Energy
DSO	Distribution System Operations
FLISR	Fault Location, Isolation, and Service Restoration
GMLC	Grid Modernization Lab Consortium
HR	Human Resources
ICS	Industrial Control System
INL	Idaho National Laboratory
IT	Information Technology
MDMS	Meter Data Management System
NISC	National Information Solutions Cooperative
NIST	National Institute of Standards and Technology
OT	Operational Technology
PNNL	Pacific Northwest National Laboratory
PUD	Public Utility District
RFP	Request for Proposal
SCADA	Supervisory Control and Data Acquisition

References

1. LCEC SCADA System Replacement, Lee Country Electric Cooperative, slides, https://www.lcec.net/trustee/2018/12/SCADA%20System%20Replacement%2012202018%20-%20WEB.pdf

2. “Investing for the Future”, Ngo, Arant, Bilby and Grice, IEEE Power and Energy magazine, https://magazine.ieee-pes.org/wp-content/uploads/sites/50/2020/01/PE_JanFeb2020_Ngo.pdf

3. “APPLICATION OF HAWAIIAN ELECTRIC COMPANY, INC., HAWAI'I ELECTRIC LIGHT COMPANY, INC. AND MAUI ELECTRIC COMPANY, LIMITED”, Hawaiian Electric Company, https://www.hawaiianelectric.com/documents/clean_energy_hawaii/grid_modernization/2019_0327_20190930_cos_ADMS_application.pdf

Page intentionally left blank

Using Cyber-Informed Engineering for Cyber Defense Workbook

1. 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.

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 drawn from a selection of real-world case studies, it is fictional.

2. 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 design—the most optimal time to introduce both low cost and effective cybersecurity approaches. CIE is an emerging method to integrate cybersecurity 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 attack or reduce the consequences when an attack occurs.

While specialized information technology (IT) and operational technology (OT) cybersecurity experts bring strong cybersecurity capabilities to securing today's energy systems, many of the engineers and technicians who design and operate these energy systems currently lack sufficient cybersecurity education and training to engineer systems for cybersecurity from the outset, in the same way they engineer these systems for safety.

This workshop summarized the principles for Cyber-Informed Engineering, provided with the principle's initiating question on the next page. CIE slides are attached in the appendix, along with a collection of CIE references.

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?
Resilient 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 we need?
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?
Cybersecurity Culture	How do I ensure that everyone performs their role aligned with our security goals?

3. Exercise Foundation

The exercises below are provided to allow you to have an 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 principle. Please feel free to ask questions of the moderators or make the necessary assumptions about the project which help you and your table to engage with and receive benefit from the described scenario.

3.1 Introduction

You and your team support a small utility considering an ADMS upgrade. The utility has asked that you help to identify security decisions which, made in design, might heighten the effectiveness of cybersecurity protections on the system and ideally to create designed-in cyber protections for critical system functions which are anticipatory, preventing specific high-consequence attack paths or attack impacts vs. reactive. Solutions which provide passive protection for the system are desired over those which require ongoing monitoring or reaction.

3.2 ADMS Upgrade Project Background

The existing distribution management system is 30+ years old. Although state-of-the-art when deployed, its features and technology are no longer supported by the vendor and do not provide modern capabilities. Additionally, it utilizes a proprietary code, making it difficult to upgrade, interface with other platforms, and enhance.

3.3 ADMS Upgrade Project Scope

Provide insights to the project team who is replacing the Co-op's existing SCADA system with a more robust and modern SCADA/ADMS solution. They have identified a solution that promises to offer advanced control and analytical functions on a stable, secure, proven platform that interfaces with the NISC software suite.

Benefits of a SCADA/ADMS Platform SCADA (Supervisory Control and Data Acquisition)

- Feature-rich, open, scalable and flexible platform
- Provides real-time monitoring and control applications
- Monitoring/managing substation infrastructures, distribution, and transmission networks
- Cyber-security segmentation and hardening
- Mature application and systems architecture ADMS (Advanced Distribution Management System)
- Model and manage the distribution network
- Monitor and control the power system
- Manage planned and unplanned outages
- Analyze and optimize the operation of the network
- Integrate with renewable and distributed generation

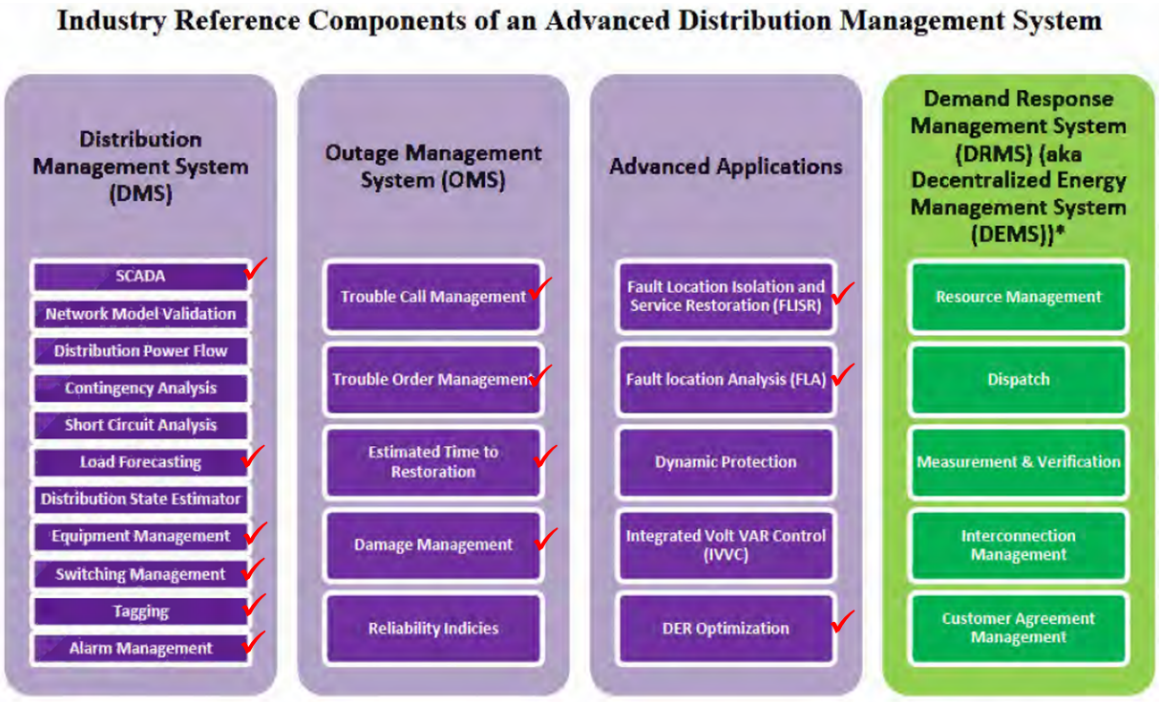


Figure 1 - Desired features of the ADMS upgrade (depicted with red checks)[a]

[a] "APPLICATION OF HAWAIIAN ELECTRIC COMPANY, INC., HAWAI'I ELECTRIC LIGHT COMPANY, INC. AND MAUI ELECTRIC COMPANY, LIMITED**", Hawaiian Electric Company,** https://www.hawaiianelectric.com/documents/clean_energy_hawaii/grid_modernization/2019_0327_20190930_cos_ADMS_application.pdf

3.3.1 ADMS Upgrade Project Progress

This effort began in 2019, and though it was beset by delays from COVID including both work delays and delays from supply chain shortages, Phase 1 has completed. The meters, MDMS, and communications network are in place. Recommendations to improve the security for these items will be considered, however, these items are not of primary interest for the work of your team. Your team will focus on ensuring that the project team for Phase 2 incorporates the best possible practices for designed-in security.

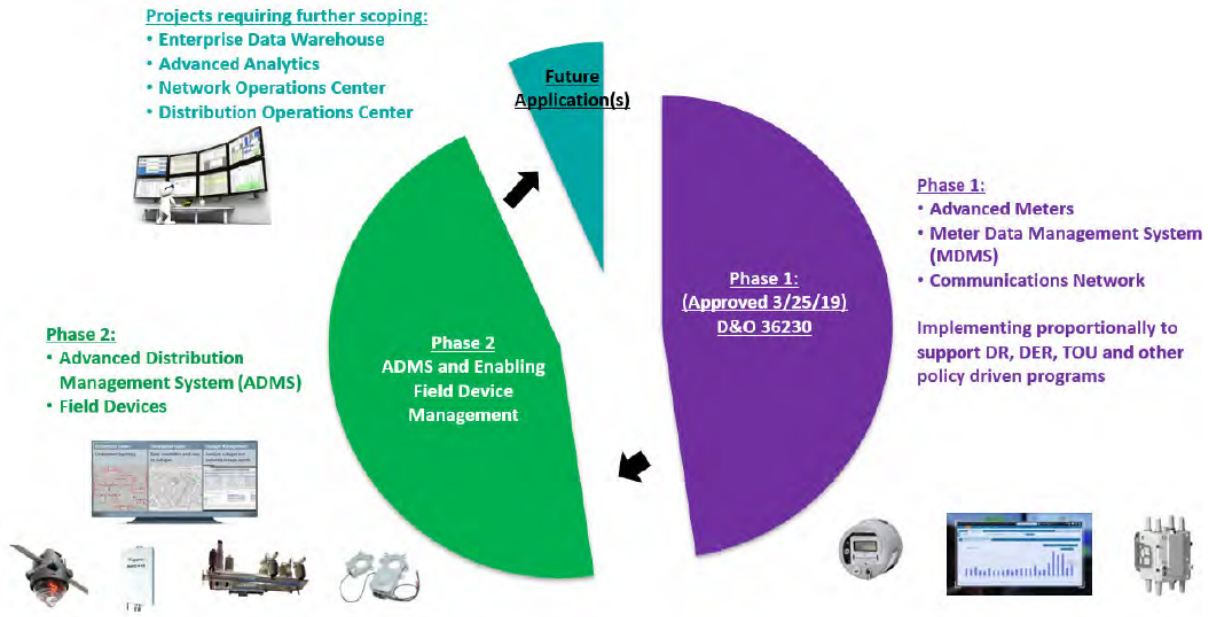


Figure 2 - Project Plan for Phased Deployment[b]

The team prepared an overall work breakdown of critical project elements, below.

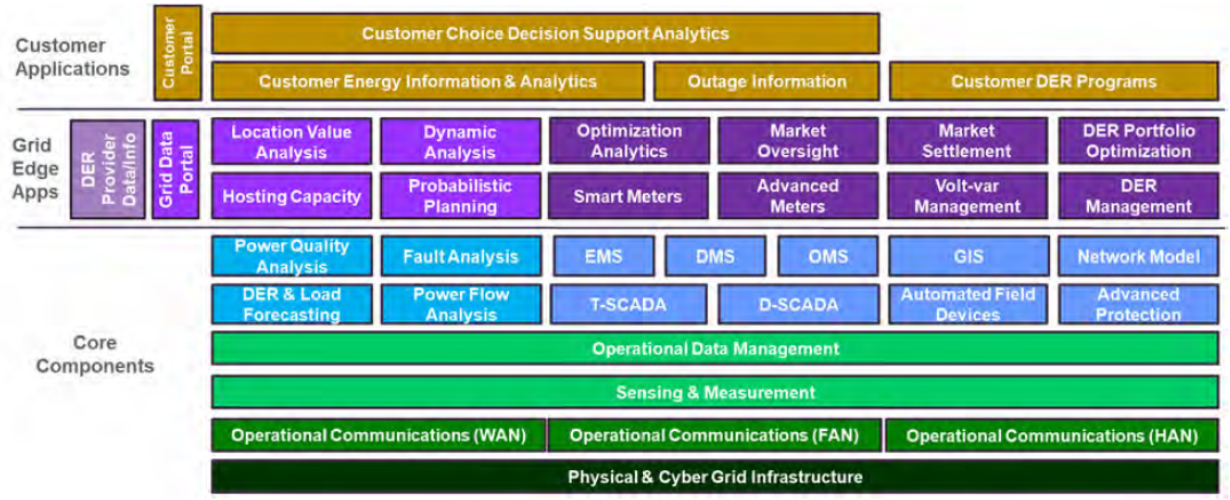


Figure 3 - Core Work Breakdown of Project Elements for ADMS upgrade[c]

[b] IBID

[c] IBID

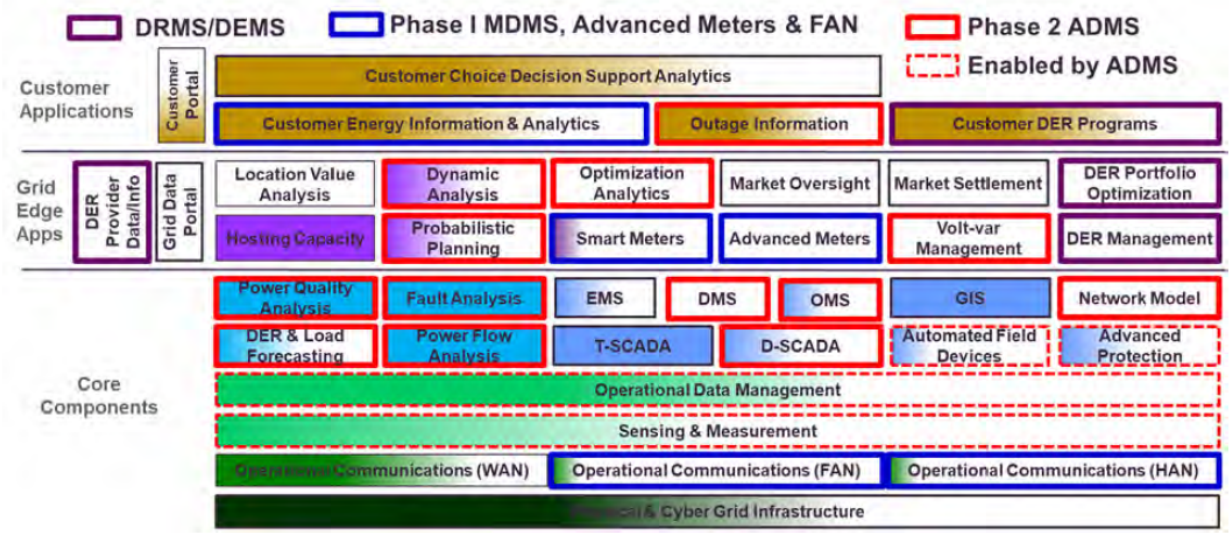


Figure 4 - Project Work Breakdown Showing Work Accomplished, To Be Performed, and Interdependencies[d]

For our team, the project team updated the diagram showing the work performed to-date, (purple and blue outlines), the work they are planning, (solid red outlines), and dependencies they must consider (red dashed outlines).

[d] IBID

3.3.2 Further Architectural Drawings

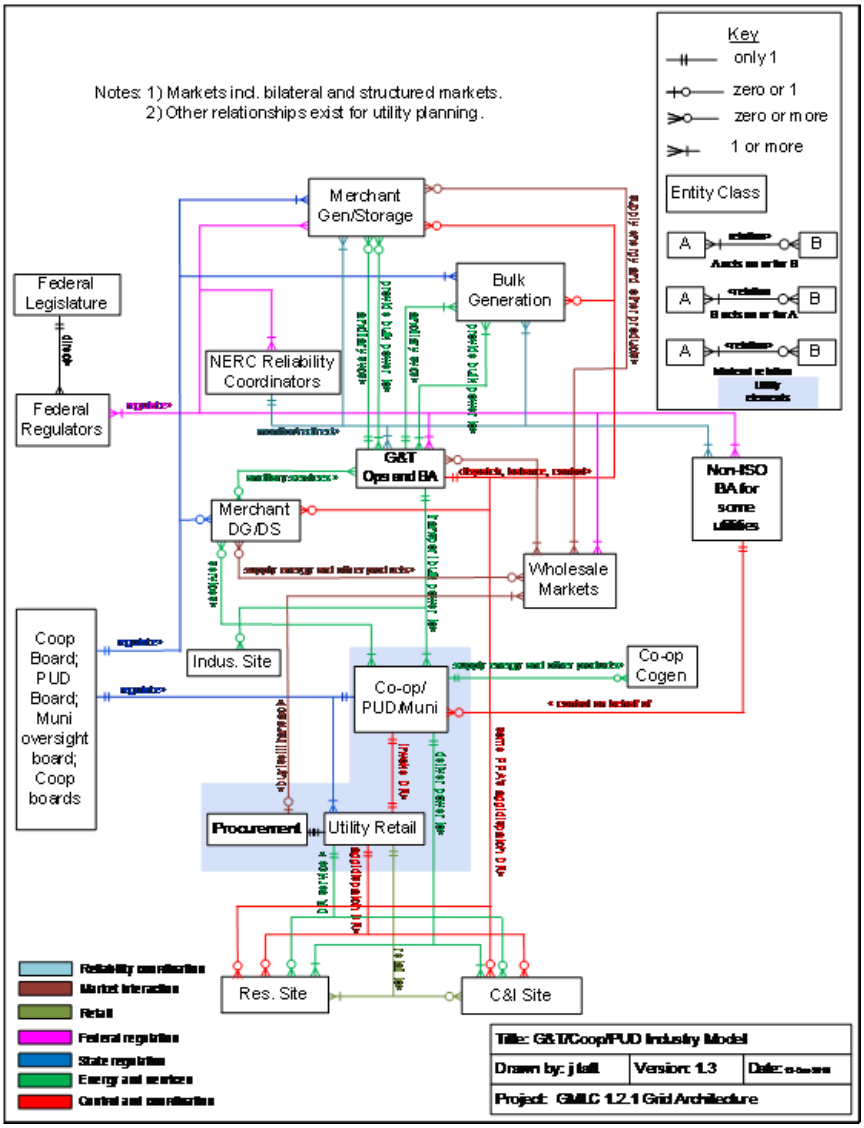


Figure 5 - Industry Model (From GMLC Grid Architectural Project)[e]

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

[e] 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

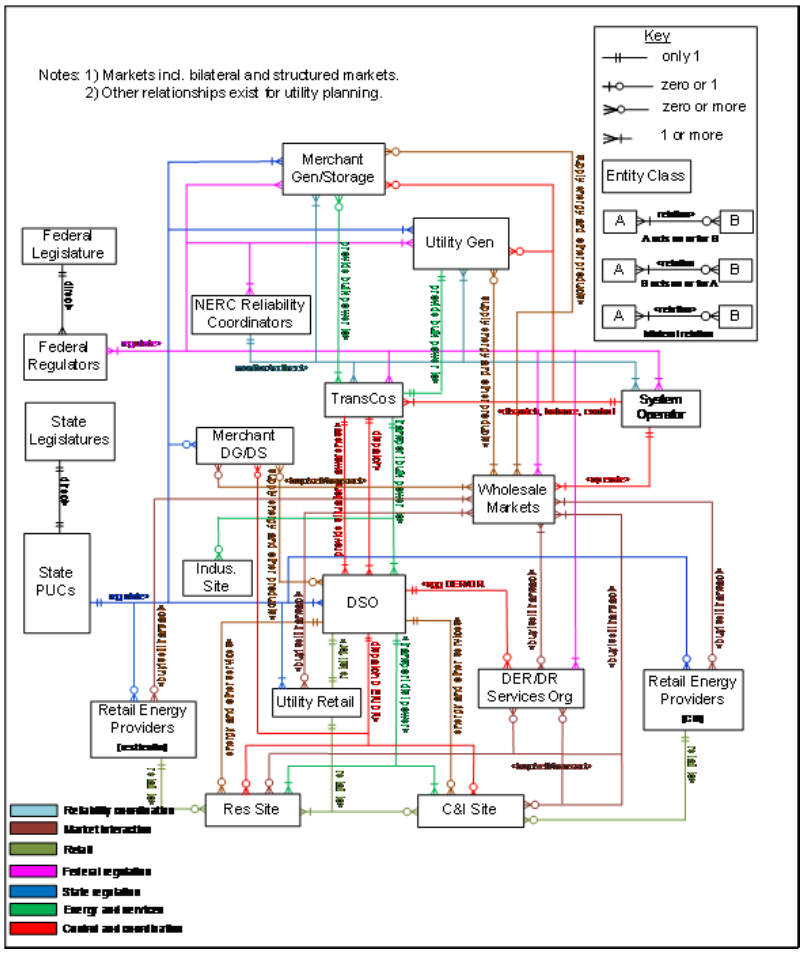


Figure 6 - Potential Distribution System Operator Function Illustration (From GMLC Grid Architectural Project)[f]

This image was formed by the same DOE Grid Modernization Laboratory Consortium project as Figure 5 - Industry Model (From GMLC Grid Architectural Project. The DSO role depicted in the drawing shows functions which may emerge for this utility after the ADMS upgrade.

[f] 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

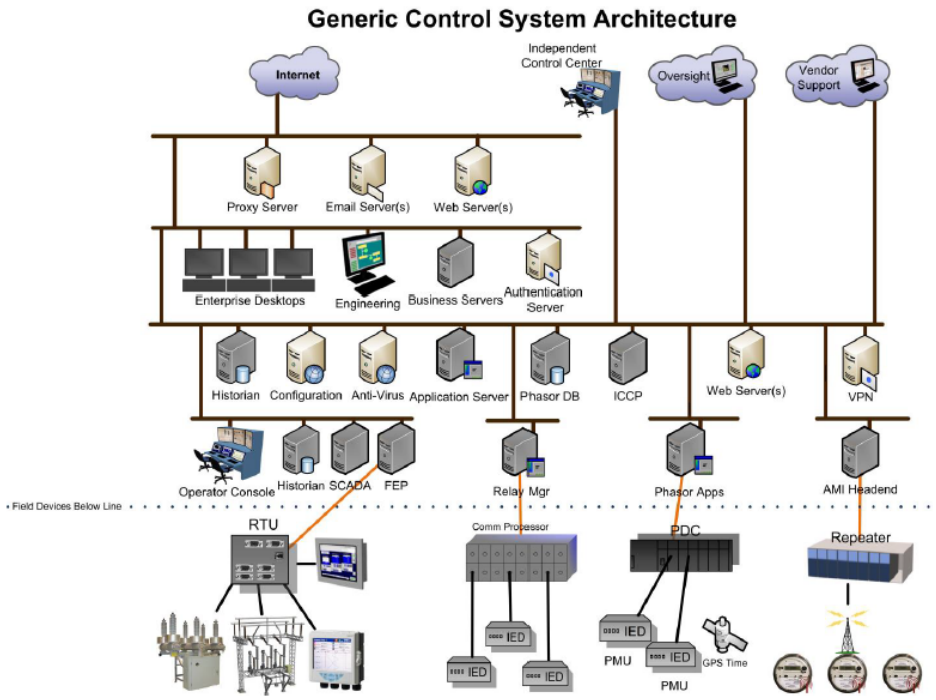


Figure 7 - Generic Information Architecture for a Control System[g]

This generic control system architecture and its companion, next, 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**.

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

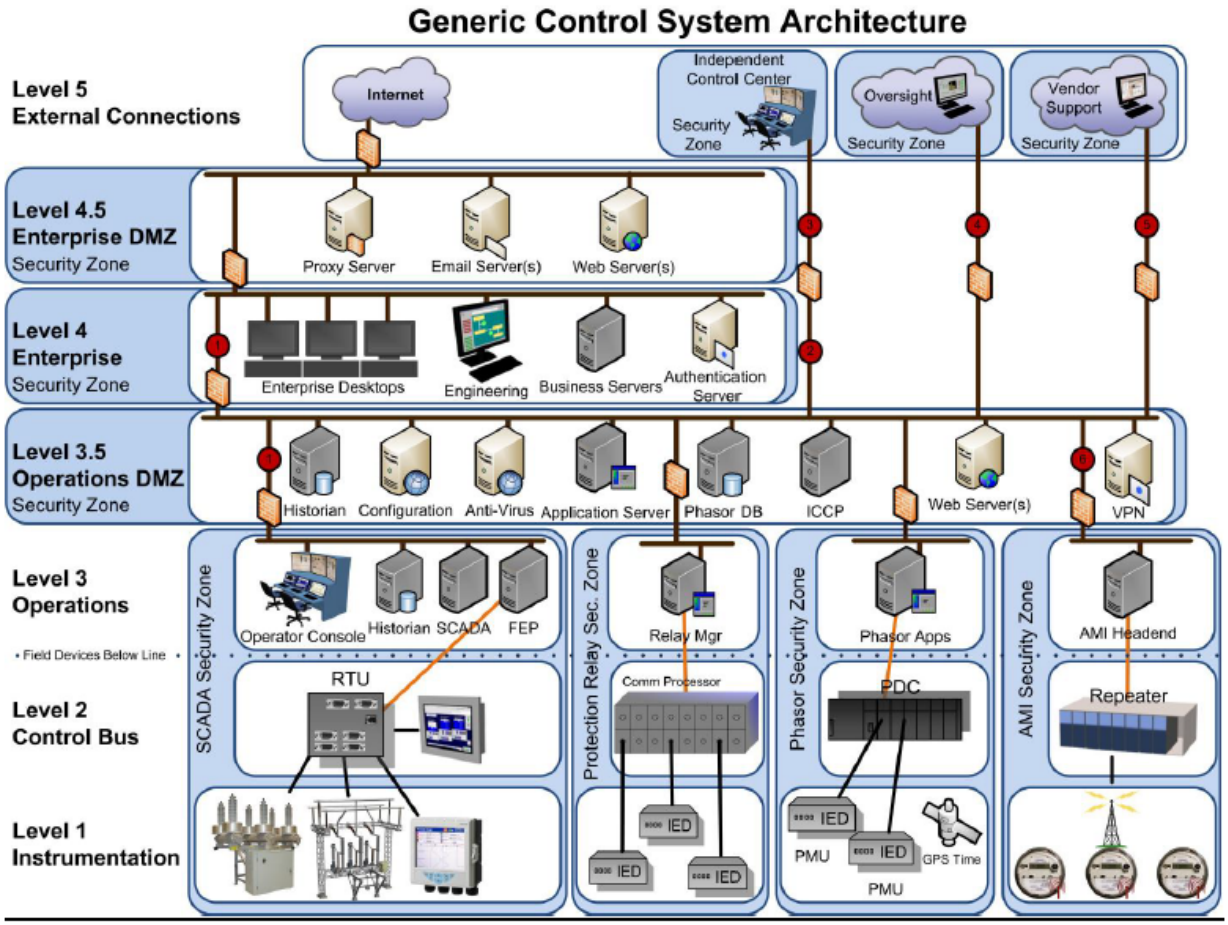


Figure 8 – Generic Control System Architecture, Segmented[h]

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

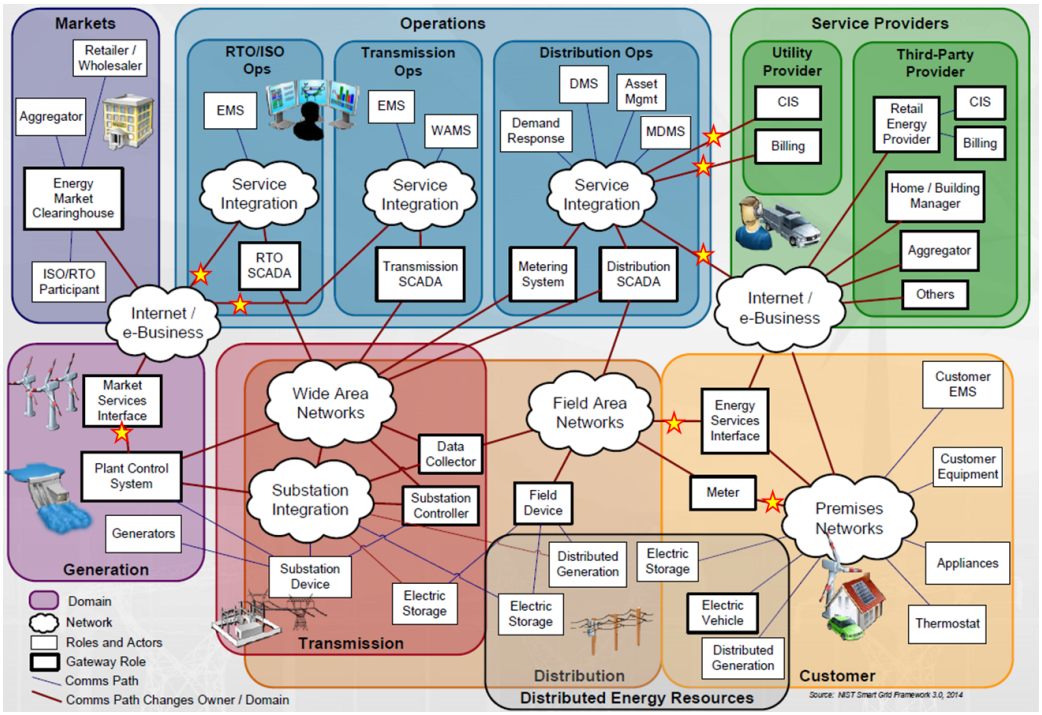


Figure 9 - Distribution Interconnections[i]

The NIST legacy framework offers some ideas to consider as the team analyzes **interdependencies** and the impact they could have on the project.

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

4. Analysis of the ADMS Upgrade 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 ADMS design team on their implementation of CIE and be prepared to brief your answers out in the room. The team has provided some input from their conversations but is open to your recommendations outside of those inputs.

4.1 Consequence-Focused Design

As discussed in the presentation, 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 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 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. (Slide pg. 30)

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

From the project team:

- Our asset owner provides power to hospitals, industrial parks, 911 centers, cell towers, water and wastewater treatment, telecom COs, etc.
- All customers have an always-on expectation, and secondary expectation of reasonable prices.
- The utility may be called upon to shed load to support the BES.
    - This is a must-work first and every time without delay activity.
- See one consequence, identified in the team's input in 4.2, Engineering Controls.
- Threats to consider:
    - Ukraine 2015/16,
    - Industroyer2,
    - Sandworm (misuse and abuse of inherent functionality).
- The board and executives are fairly risk-averse (middle of the road for electric utilities, which are on the conservative end of critical infrastructures generally).
- The board and executives are supportive of applying CIE on this effort and see the value of investing in security at the design phase to control costs in operations.
    - We may have to help make the case that our suggestions will do so.

Notes

4.2 Engineered Controls

For the most critical consequences and impacts determined in Consequence-focused design, we have an opportunity to think about the specific controls we'd like to have in place to prevent them. Eventually, we'll talk about the collection in terms of layered defenses, but at first, we can:

- Think about what kinds of controls we can have in place to prevent a consequence or mitigate its impact.
- We can determine which controls are provided as a part of products and services we are using and which ones we might want to design in.
- We can determine whether we can identify both physical controls and digital controls for a given consequence and the relative costs and benefits of each.
- We can determine whether our controls prevent an attack, lower the impact of the attack, or serve to provide alarms or warnings of adverse situations.

Principle 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 vendors for RFP solicitation. They would like this principle to guide any design inputs they need to consider and also provide input they'll use to guide vendor selection.

They have identified the following considerations:

- ADMS is inherently a digital system, that interfaces with ICS controlling physical systems
- A vendor designed the ADMS with certain assumptions about existing security controls.
    - Our utility is too small to influence these facts but has the choice among a few options of which ADMS to use.
- Operation and maintenance of the electric infrastructure requires my 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.

Notes

4.3 Secure Information Architecture

Each system contains data linked to mission-critical consequences and impacts which should be protected from outsider view 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 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.

Principle 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 have identified some desired elements of their secure architecture, but are open to more ideas:
  - Segmentation for enterprise, control center, substations – with DMZs in between
  - East-west segmentation between substations
- They would like insight into the ingress-egress points to get the necessary data to the right storage and computing locations and the accompanying risks.
  - This will be significantly more than the current system in all ways.
- Different computing and storage functions are taking place in multiple locations, on prem or in private or public clouds.
  - They would appreciate advice on the best way to ensure the best possible security.
  - 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.

Notes

4.4 Design Simplification

Systems formed through acquisition often have more features than are explicitly needed to perform required functions. Though these features can be configured not to be available to authorized system users, they are 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 impactful adverse 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 undesired commands at a network segmentation boundary before they are executed.

Principle 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.
- Any of the ADMS systems 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 configure out will still be present in the tool we receive, just not available via system menus
- The team's diagrams, (Figure 1 - Desired features of the ADMS upgrade (depicted with red checks) above, may provide some insights about the most desired features and those which are not prioritized for use.

Notes

4.5 Resilient Layered Defenses

The best defensive capability for critical consequences is formed by an assemblage of 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 work together to, for the critical consequences identified, arrange the best compilation of those defenses to avert the worst impacts from the prioritized consequences. The engineers and operational cybersecurity team work together to ensure that each of the defensive capabilities and services is tuned based on the identified consequences and how the worst impacts of those consequences can be avoided.

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

From the Project Team:

- The ADMS will reside inside an environment that already has layers of imperfect perimeter protection and detection.
- ADMS has features and configuration options that the old system does not have. The design team would like your input on how they can ensure that they can detect the use of features that are configured out.
- The ADMS design team has talked to the operational cybersecurity team in general about the upgrade, but not about specific capabilities and services needed for operational cyber defense.
    - They 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 with operational cybersecurity.

Notes

4.6 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 killchain 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 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, systems 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.

Principle 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 killchain.
- 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.

Notes

4.7 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, evaluate the physical interdependency risks already considered, but judging whether a cyber-attack might make a given consequence more possible or might have the potential to make it more intense than a physically-driven event. Are there functions in the interdependent system not normally accessible to operators which might cause untoward 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 cause cascading effects? In the same vein, where might the system under design be able to affect the interdependent systems in unexpected ways.

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

From the Project Team:

- The project team notes that the servers needed to support the ADMS system will need more power and cooling than the prior systems.
    - They are building requirements for that upgrade and welcome your thoughts about how to prioritize redundancy in power and cooling requirements.
- This system will require communication links with acceptable band width and latency to multiple locations.
    - Some of these locations are not continuously networked today.
- Vendor support will be required for nontrivial changes and modifications of the ADMS.
    - The vendor may need a continuous connection to the system for routine troubleshooting during its initial operation.
- What other system interdependencies should the team consider? What risks do you see and what recommendations do you make?

Notes

4.8 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 ensuring 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.

Principle 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:

- The project team notes that the ADMS upgrade will include many new servers, endpoints and supporting networking switchgear.
    - Some of the communications between endpoints are new and the team hasn't thought through all of the functions (desired and undesired) that communications complexity could cause.
- Some existing systems will need to be changed and upgraded (configuration and physical)
    - Some of these changes will involve trading out analog systems for digital ones.
    - The operations team is very accustomed to the current systems and the design team would like input about preparation and training to consider to accustom the team to more functional, digital equipment.
- The new ADMS has a 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 team to automatically narrow down the part of the circuit where the fault is, and reconfigure to restore as many customers as possible in tens of seconds
    - 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.

Notes

4.9 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.

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

From the Project Team:

- The potential vendors for the ADMS system are all new to our organization.
    - 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 house-created code and integrated software and hardware components.
    - We expect the selected vendor to provide both onsite and remote support to the ADMS, once installed.
        - We do not yet understand the practices the vendors have for securing remote access.
- We have the ability to create procurement requirements, and can provide input 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.

Notes

4.10 Planned Resilience

Imagining the general operating mode of a system, with all functions available and working as expected, however, resilience requires that we imagine and plan for different kinds of failure modes of a system, ideally including those linked to the set of prioritized undesired consequences created earlier. We must understand these failure modes, including how to operate through them, albeit at a lower level of performance or reliability. Ideally, a set of 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.

Principle Question: *How do I turn my "what ifs" into "even ifs"?*

From the Project Team:

- 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 some fraction of our system for some time without the aid of SCADA.
    - We would appreciate insights about specific diminished operating modes we should consider for the upgraded ADMS system.

Notes

4.11 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.

Principle 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 our electrical and current controls and other digital 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 multiple news releases about our system.
    - 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 their website.
    - 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 new employees for the upgrade, some temporary and some who will be long-term additions to our operating 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 upgrade process, 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?

Notes

4.12 Cybersecurity 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.

Principle 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 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 build a cybersecurity culture.
    - 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 see the value of a culture of cybersecurity?

Notes

Notes

Page intentionally left blank

Appendix A - CIE Slides

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.

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.

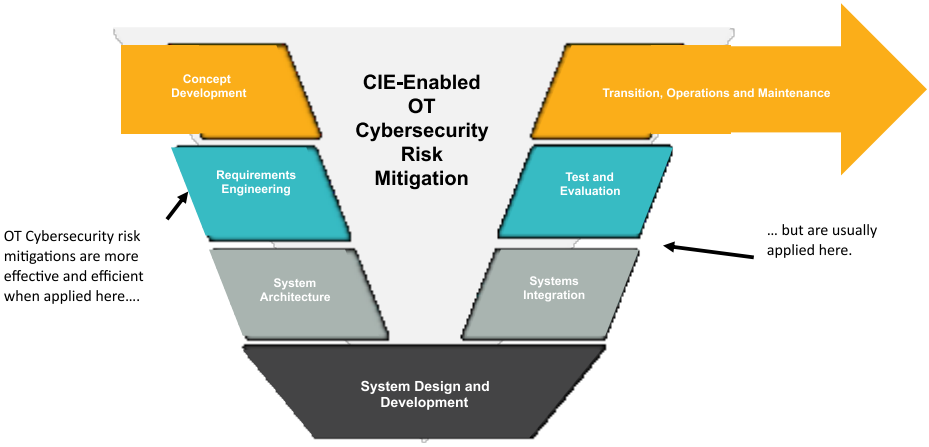
Accelerating industry's adoption of a culture of cybersecurity by design —complementing industry's strong culture of safety—offers the ability to maintain secure design even as systems evolve and grow in functionality.

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.

2023 Co-op Cyber Tech | NRECA

CIE and the Systems Engineering Lifecycle



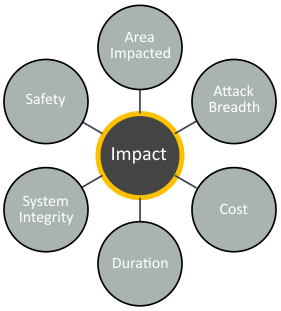
Principles of CIE

DESIGN AND OPERATIONS	ORGANIZATIONAL
Consequence-focused design	Interdependency evaluation
Engineered controls	Digital asset awareness
Secure information architecture	Cyber-secure supply chain controls
Design simplification	Planned resilience
Resilient layered defenses	Engineering information control
Active defense	Cybersecurity culture

Consequence-Focused Design

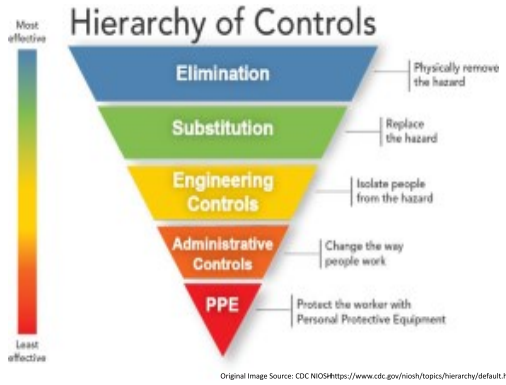
How do I understand what critical functions my system must **ensure** and the undesired consequences it must **prevent**?

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

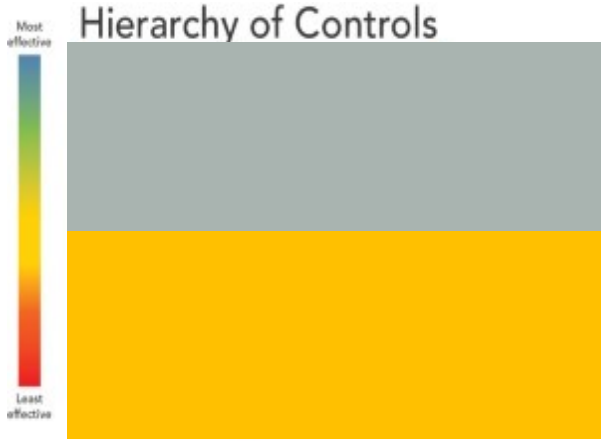


Engineered Controls

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



Engineered Controls



Original Image Source: CDC NIOSH https://www.cdc.gov/niosh/topics/hierarchy/default.html

Design Simplification

How do I determine what features of my system are not **absolutely** necessary?

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

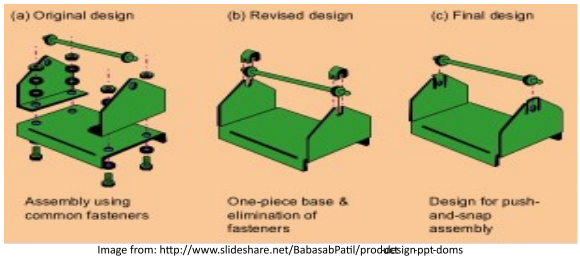
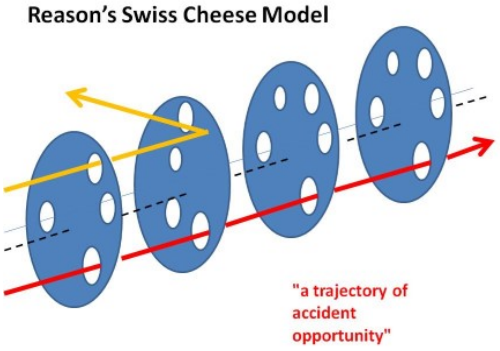


Image from: http://www.slideshare.net/BabasabPatil/product-design-ppt-doms

Layered Defenses

How do I create the best compilation of system defenses?



https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.skybrary.aero%2Farticles%2Fjames-reason-hf-model&psig=AOvVaw0Efrrteg-R_rx5h8hdwbr&ust=1679767123806000&source=images&cd=vfe&ved=0CBEQjhxqFwoTCPCOSb659f0CFQAAAAAdAAAAABAD/

Engineering Information Control

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

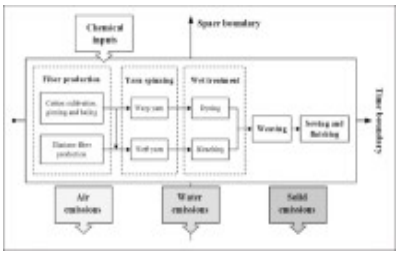
- What information should we protect?
- Who has and should have it?
- How do we protect it?

Image from: https://www.uscomputer.com/2016/02/16/employee-education-thwarts-social-engineering-threat/

Secure Information Architecture

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?



Interdependency Evaluation

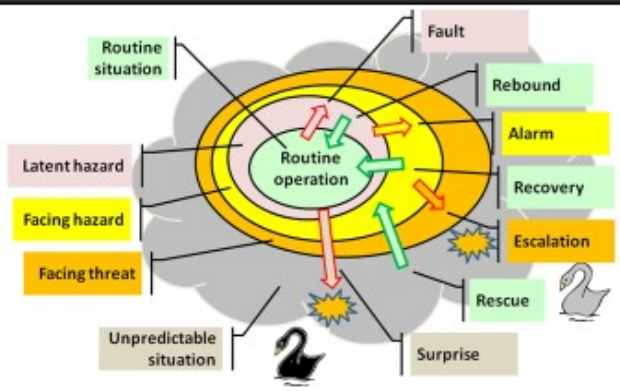
How do I understand where my system can impact others or be impacted by others?

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

2023 Co-op Cyber Tech | NRECA

Resilience Planning

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



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

Active Defense

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

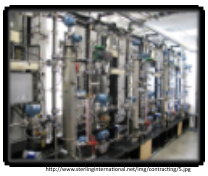
- How do I protect what I designed?
- How can engineers and IT collaborate in defense?
- How do we exercise / practice defense?
- Have we developed policies and procedures?

https://www.recordedfuture.com/activecyberdefense-part-2/ -- Used with permission

Digital Asset Awareness

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 are 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?**

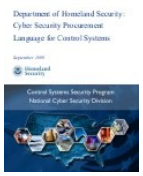


Cyber-Secure Supply Chain

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

- 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?

GLOBAL CYBERSECURITY ALLIANCE



Cybersecurity Culture

How do I ensure that everyone performs their role aligned 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?

Conversations

Explicit Assumptions

Collaboration on Projects

Assessments

Scenarios

Exercises

2023 Co-op Cyber Tech | NRECA

Image from: http://epiphanyinstitute.com/take-time-out-to-get-on-track-and-reach-your-goals/

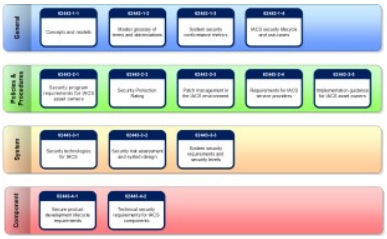
Principles of CIE

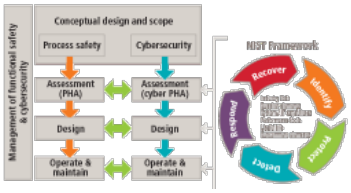
Principle	Key Question
Consequence-Focused Design	How do I understand what critical functions my system must perform and the undesired consequences it must prevent?
Engineered Controls	How do I implement controls to reduce avenues for attack or the damage which could result?
Secure Information Architecture	How do I prevent undesired manipulation of important data?
Design Simplification	How do I determine what features of my system are absolutely necessary?
Resilient 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, what our assumptions are about how they work?
Cyber-Secure Supply Chain Controls	How do I ensure my providers deliver the security we need?
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?
Cybersecurity Culture	How do I ensure that everyone performs their role aligned with our security goals?

2023 Co-op Cyber Tech | NRECA

- 19 -

OK, But How Do You CIE?





Resources

- 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

Page intentionally left blank