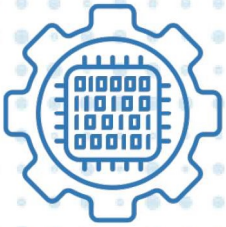


Cyber-Informed Engineering

Cyber-Informed Engineering Workbook: ADMS

CIE Hands-On Training

September 10, 2024

Authors:

Virginia Wright
CIE Program Manager

Benjamin Lampe
CIE Researcher

DISCLAIMER

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

Contents

Acronyms

ADMS	Advanced Distribution Management System
BES	Bulk Energy System
CIE	Cyber-Informed Engineering
DOE	Department of Energy
DMS	Distribution Management System
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
OMS	Outage Management System
PNNL	Pacific Northwest National Laboratory
PUD	Public Utility District
RFP	Request for Proposal
SCADA	Supervisory Control and Data Acquisition

References

1. U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response. *Cyber-Informed Engineering Implementation Guide*. Version 1.0, August 7, 2023. https://www.osti.gov/biblio/1995796.
2. LCEC SCADA System Replacement, Lee Country Electric Cooperative, slides, https://www.lcec.net/trustee/2018/12/SCADA%20System%20Replacement%2012202018%20-%20WEB.pdf
3. “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

4. “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_2 0190930_cos_ADMS_application.pdf

Figures

1. Workbook Purpose

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)[1] offers an opportunity to "engineer out" some cyber risk across the entire system lifecycle, starting from the earliest possible phases of conceptual design and requirements development and system design—the most optimal times 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 uses 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 that engineers design systems for safety, engineers informed by CIE use similar methods to prevent or lessen the impact of a cyber-attack. CIE also allows the engineers to advise the approaches used by specialized Information Technology (IT) and Operational Technology (OT) cybersecurity experts to align cybersecurity mitigations to the most critical consequences identified by the engineers. 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 in Figure 1.

[1] U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response. *Cyber-Informed Engineering Implementation Guide*. Version 1.0, August 7, 2023. https://www.osti.gov/biblio/1995796.

	PRINCIPLE	KEY QUESTION
1	**Consequence-Focused Design**	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?
2	**Engineered Controls**	How do I select and implement controls to reduce avenues for attack or the damage that could result?
3	**Secure Information Architecture**	How do I prevent undesired manipulation of important data?
4	**Design Simplification**	How do I determine what features of my system are not absolutely necessary to achieve the critical functions?
5	**Layered Defenses**	How do I create the best compilation of system defenses?
6	**Active Defense**	How do I proactively prepare to defend my system from any threat?
7	**Interdependency Evaluation**	How do I understand where my system can impact others or be impacted by others?
8	**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?
9	**Cyber-Secure Supply Chain Controls**	How do I ensure my providers deliver the security the system needs?
10	**Planned Resilience**	How do I turn “what ifs” into “even ifs”?
11	**Engineering Information Control**	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
12	**Organizational Culture**	How do I ensure that everyone’s behavior and decisions align with our security goals?

Figure 1 - CIE Principles and Key Questions

PRINCIPLE 1: CONSEQUENCE-FOCUSED DESIGN

Key Question

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

Principle Overview

Consequence-focused design is the first principle 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 identifies the most consequential impacts, sometimes referred to as the high-consequence events (HCEs), 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. The team develops a list of HCE's and prioritizes the most impactful. In the initial review, the team need not evaluate the potential or likelihood of these impacts being induced via digital failure or cyber-attack. Once HCE's are identified, the team can begin to explore how those effects could be realized via adversary attack or digital failure.

PRINCIPLE 2: ENGINEERED CONTROLS

Key Question

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

Principle Overview

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

PRINCIPLE 3: SECURE INFORMATION ARCHITECTURE

Key Question

How do I prevent undesired manipulation of important data?

Principle Overview

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 element or 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.

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 mature and the underlying network and data service architecture is under design, more fine-grained digital controls, and create specific zones and segmentation plans can be created.

PRINCIPLE 4: DESIGN SIMPLIFICATION

Key Question

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

Principle Overview

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 collaborate with cybersecurity specialists to determine how to 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 5: LAYERED DEFENSES

Key Question

How do I create the best compilation of system defenses?

Principle Overview

The best defensive capability for critical consequences is formed by an assemblage of controls, including physics-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 most 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 6: ACTIVE DEFENSE

Key Question

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

Principle Overview

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 actions to be taken upon detection of an identified indicator. Plans should include points of contact for specific roles and responsibilities across the spectrum of functions associated with the system, since **Active Defense** of the system may require support from a broad set of roles, and they may not all be aware of each other. Once plans are in place, systems should be created to ensure that these plans are regularly practiced, and that the overall approach is regularly assessed to identify emerging consequences, indicators, and opportunities for more advanced defensive approaches.

PRINCIPLE 7: INTERDEPENDENCY EVALUATION

Key Question

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

Principle Overview

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 judge 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 8: DIGITAL ASSET AWARENESS

Key Question

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

Principle Overview

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 9: CYBER-SECURE SUPPLY CHAIN CONTROLS

Key Question

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

Principle Overview

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 10: PLANNED RESILIENCE

Key Question

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

Principle Overview

You can imagine 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. Note that a capability may be restored to diminished operation via use of an alternate mechanism or supply source.

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 11: ENGINEERING INFORMATION CONTROL

Key Question

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

Principle Overview

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 12: ORGANIZATIONAL CULTURE

Key Question

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

Principle Overview

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.

3. Workshop Activity Overview

The scenario presented in this workbook is designed to provide a hands-on experience applying CIE principles in a fictional project. It is designed to elicit rich discussion about the principles among workshop participants. There are likely to be key facts about the scenario that 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.

3.1. Workshop Activity Background

You and your team support a utility in the process of performing 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 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.

There are parts of the existing distribution management system (DMS) which are 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.

Provide insights to the project team that is replacing the Utilities' existing DMS system with a more robust and modern ADMS solution. They have identified a solution that promises to offer advanced control and analytical functions on a stable, secure, proven platform. The anticipated benefits of a ADMS Modernization efforts are:

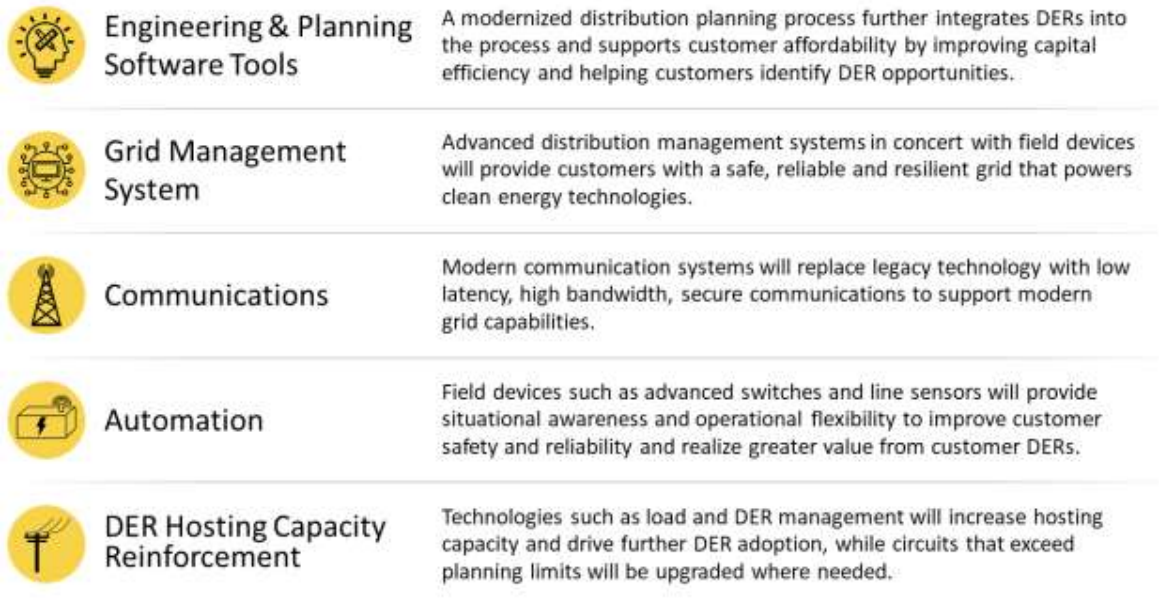


Figure 2 - Grid Modernization Technologies and Customer Benefits[2]

[2] https://gridworks.org/wp-content/uploads/2024/04/SCE-2024-Grid-Modernization-Progress-Report.pdf

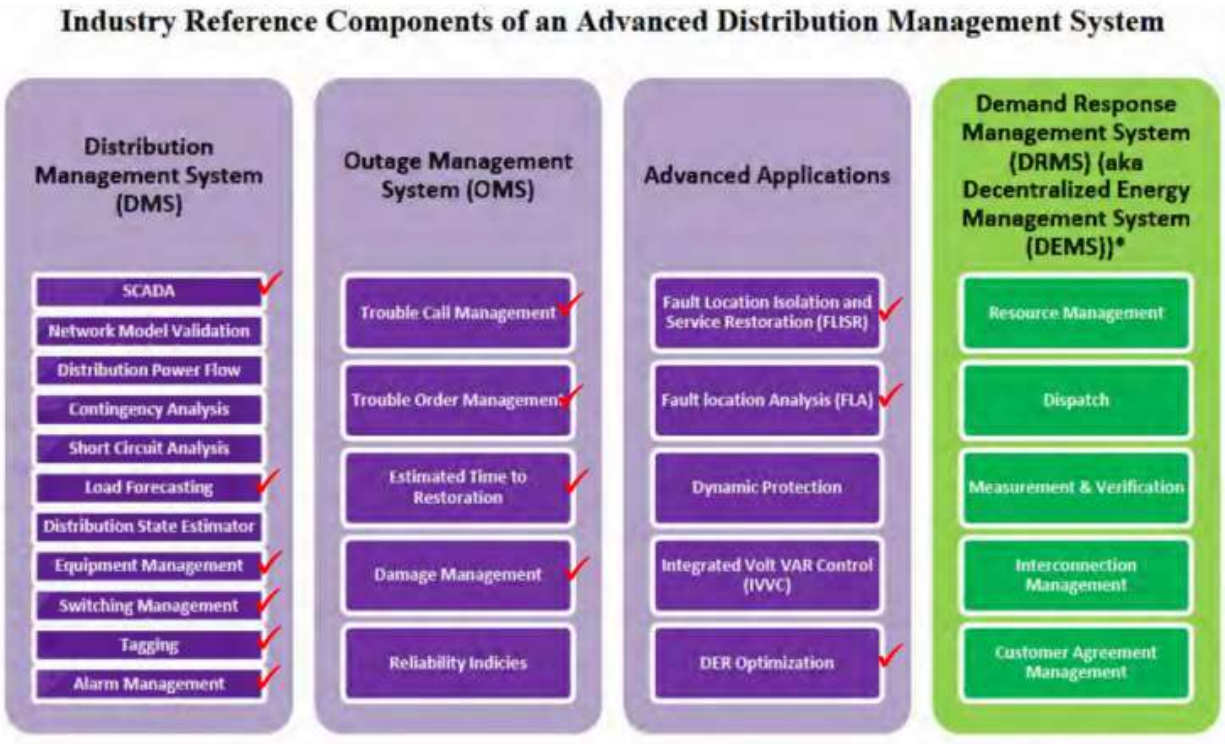


Figure 3 - Desired Features of the ADMS Upgrade (Red Checks)[3]

3.2. Workshop Activity Details

This effort began in 2019. Though it was beset by delays from COVID including both work delays and delays from supply chain shortages, Phase 1 is close to completion, expected in early 2025. Your team will focus on ensuring that the project team for Phases 2 & 3 incorporates the best possible practices for designed-in security.

The first phase of modernizing the ADMS solution is part of a larger project and future phases as described in Figure 5 below.

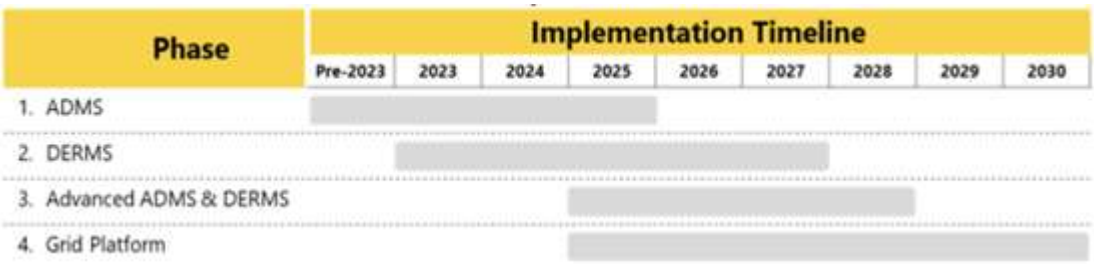


Figure 4 – Distribution Management System (DMS) Phase Implementation Timeline[4]

[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

[4] https://gridworks.org/wp-content/uploads/2024/04/SCE-2024-Grid-Modernization-Progress-Report.pdf

The team prepared an overall work breakdown of critical project elements for the ADMS phases, below:

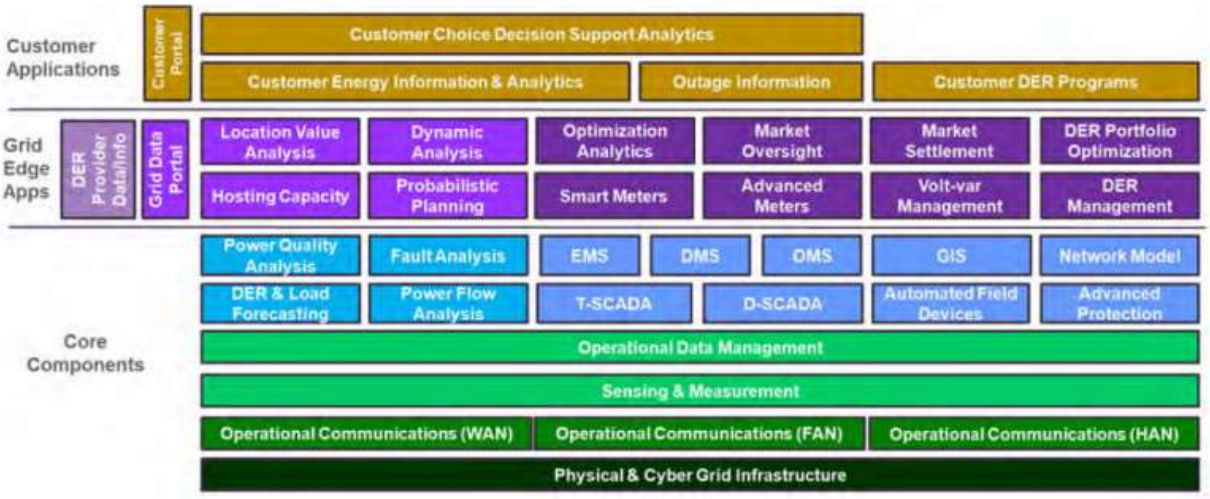


Figure 5 - Core Work Breakdown of Project Elements for ADMS Upgrade

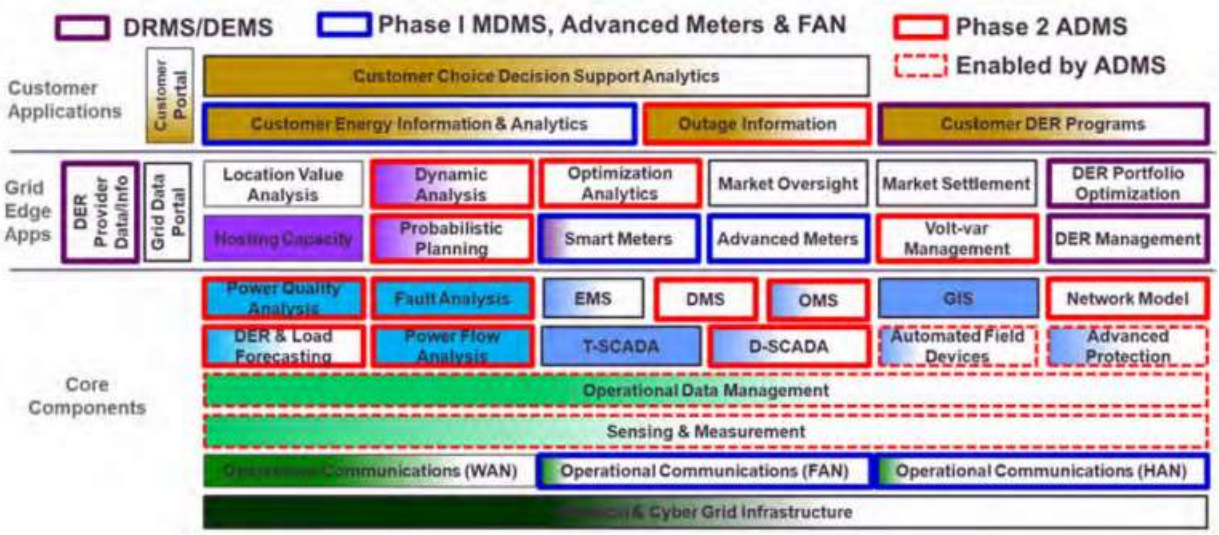


Figure 6 - Project Work Breakdown Showing Work Accomplished, To be Performed, and Interdependencies

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).

3.3. Workshop Activity Scope

In this workshop, our focus is to simulate a collaborative discussion where workshop attendees function as the engineering staff. The instructors assume the role of CIE consultants, guiding the engineering team staff (workshop participants). Together, we aim to assist the utility staff in achieving their goal of ADMS design in response to the upgrade project.

This exercise will guide staff through a series of decision-making processes under the banner of the CIE principles to determine the operational and design practices that align with the utility's modernization goals. The outcome will be a plan confirming top/prioritized consequences, any key design decisions, integration of digital technologies with an appropriate CIE-informed mitigation strategy, and operational protocols for managing the ADMS with planned resilience.

The workshop will delve into CIE Principles, exploring their practical application and effectiveness in the context of the utilities' ADMS system upgrade. Participants will collaborate to further understand the implications of providing a cybersecurity protection scheme on an Operational Technology system that pulls from both traditional cybersecurity characteristics and engineering controls. It is our goal in this exercise to understand how both cybersecurity professionals and engineers can complement each other in a project's outcome.

4. Workshop Activity Analysis using CIE Principles

Work with your assigned team to consider and discuss how each principle applies to this fictional project. As a team, determine your feedback to the Utility engineering team on their implementation of CIE and be prepared to brief your answers out in the room.

The Utility staff team has provided some input for consideration and they are open to your recommendations outside of those inputs.

4.1. CRITICAL FUNCTIONS

4.1.1. What are the mission-critical functions this system is required to perform? (Principle 1)

4.1.2. What areas of the system design are linked to these critical functions? (Principle 1)

NOTES FROM 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.
- 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.

4.2. CONSEQUENCE DEFINITION

4.2.1. What are the consequences that could result from a failure or unexpected operation of the system's critical functions? What impacts could there be to mission delivery, safety, security, the environment, equipment and property, financials, or corporate reputation? (Principle 1)

4.2.2. Are there adverse operating modes that are prone to high-impact consequences? What circumstances require or cause these modes? (Principle 1)

NOTES FROM PROJECT TEAM:

- 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.
- Cybersecurity threats to consider:
    - Ukraine 2015/16,
    - Industroyer2,
    - Colonial Pipeline (attack on an IT-based portion of the system causing operational impacts),
    - Sandworm (misuse and abuse of inherent functionality).
- 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.

4.3. DIGITAL ASSET EVALUATION

4.3.1. What parts of the design contain digital components or subcomponents? How are digital assets used to meet mission-critical functions? (Principle 8)

4.3.2. What network connectivity links each element of the high-level design? How do the various subsystems communicate with each other? (Principle 3)

NOTES FROM 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 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.
- 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 3 - 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.
- The ADMS will reside inside an environment that already has layers of imperfect perimeter protection and detection.
- This system will require communication links with acceptable bandwidth 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.
- 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.
- 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.

4.4. CONSEQUENCE ANALYSIS

4.4.1. Which digital features in a system have the potential to cause critical consequences from unexpected operation or attack, and how can those features be identified during development, procurement, and integration? (Principle 8)

4.4.2. How might loss or instability in a subsystem or the connectivity between system elements lead to high-impact consequences? How would a failure (frailty or attack/exploit) of each component affect the overall system? (Principle 1)

4.4.3. For each of the system's critical consequences, what would a cyber-attack on that consequence require? What systems would an adversary need to access to create the specific effect? How might an adversary need to traverse systems and subsystems in order to get access to the critical systems and components? (Principle 5)

4.4.4. What precursor events could occur leading up to identified high-consequence events? How might adverse consequences manifest within this system, as conceptualized? What deviations from expected system states and anomalies might be initial indicators of one of the identified consequences? (Principle 6)

4.4.5. What potential cascading failures may need to be accounted for? (Principle 7)

4.4.6. What are the limits of acceptable degradation for the system's critical functions? (Principle 10)

NOTES FROM PROJECT TEAM:

- 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 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.
- 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. How might they detect that these consequences have the potential to occur or that an adversary is performing initiating events for the attack.
- What system interdependencies should the team consider? What process, business, technology, etc., interdependencies exist? What risks do you see and what recommendations do you make?
- 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.

- 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?

4.5. MITIGATIONS

4.5.1. Are analog or physical protections engineered into the system (where possible) for each high-consequence event identified? (Principle 2) How dependent are the system's engineered controls on digital technologies? (Principle 2)

4.5.2. What are the minimum functional capabilities needed? In concept, is there anything that is likely to be implemented via digital means that is not explicitly needed? (Principle 4)

4.5.3. What specific controls (digital and otherwise) can ensure that the most critical data is available, valid, and secure? For each key data element, where must monitoring be in place to identify deviations from desired data states or settings? Is active monitoring necessary, or is logging combined with a periodic manual review process sufficient? What data elements should be exposed for external monitoring to reveal potential process anomalies, provide process validation, and to validate security? (Principle 3)

4.5.4. What enterprise IT defensive layers will this system benefit from, e.g., enterprise firewalls, IT network monitoring, etc.? (Principle 5)

4.5.5. What processes are in place to ensure system operators are aware of triggers to temporarily change operations in response to a perceived threat? What stakeholders should be notified if there is an active defensive threat or weakness to this system? (Principle 6)

4.5.6. For services critical to the functionality of the system under design, what additional contract requirements, beyond the normal baseline, should be defined for security, performance, and verification relating to the desired services? What specific quality and security requirements apply to vendors/suppliers/service providers for critical system components and services? (Principle 9)

4.5.7. Do system requirements include a manual operation mode for any system that otherwise is controlled by an automated information system? Does the system's incident response plan contain a specific resilience focus and is there controls to ensure a fail-safe behavior? (Principle 10)

4.5.8. What training, education, and practice will individuals and teams need to operate, maintain, secure, and defend the system throughout its lifecycle? (Principle 12)

NOTES FROM PROJECT TEAM:

- The project team has 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.
- 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.
- 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.
- 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.
- 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.
- 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?

MISCELLANEOUS NOTES:

5. Appendix A: Architectural Drawings

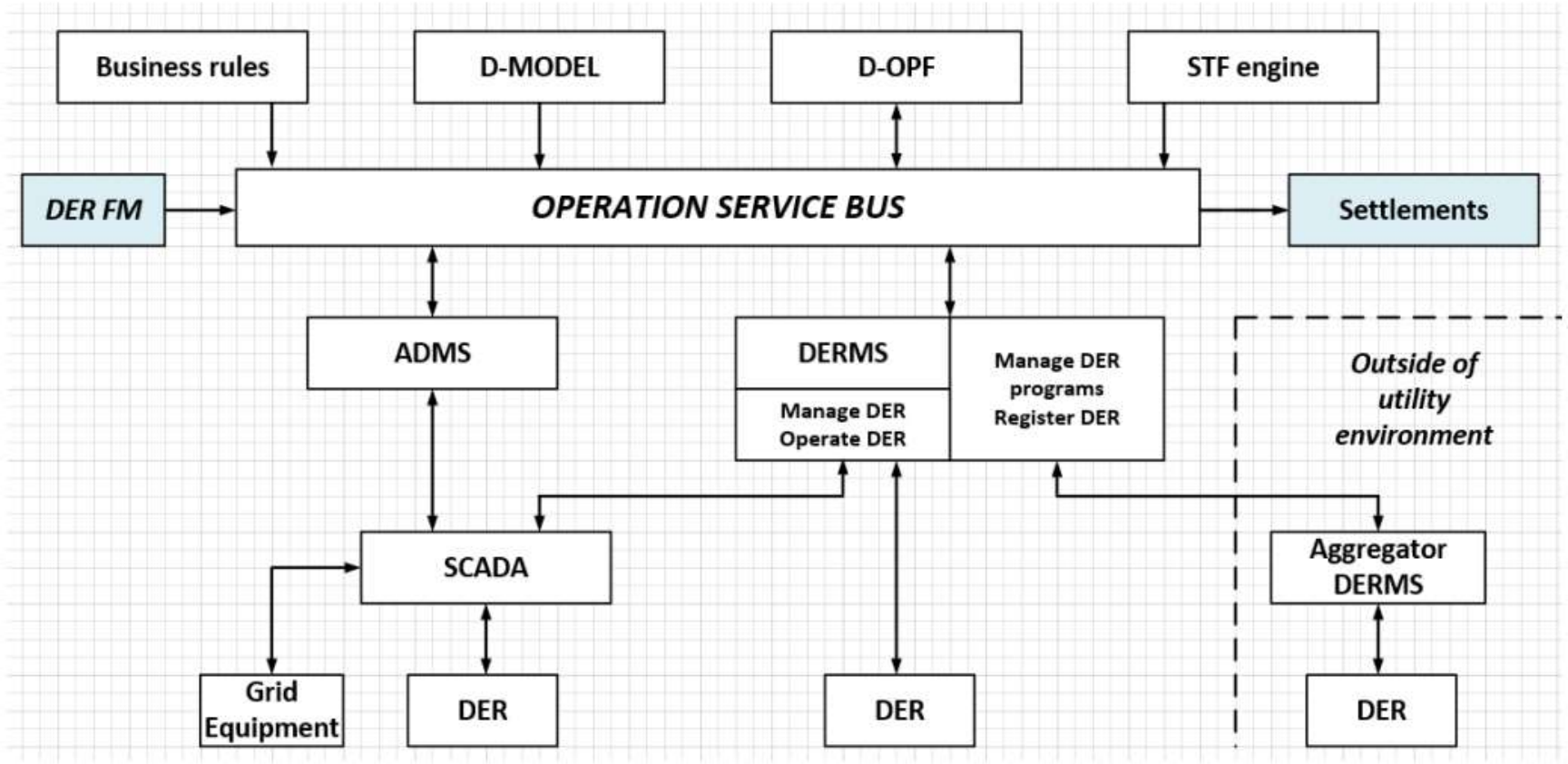


Figure 7 - DERMS deployment and operation example: distribution system application IEEE 2030.11[5]

[5] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9447316

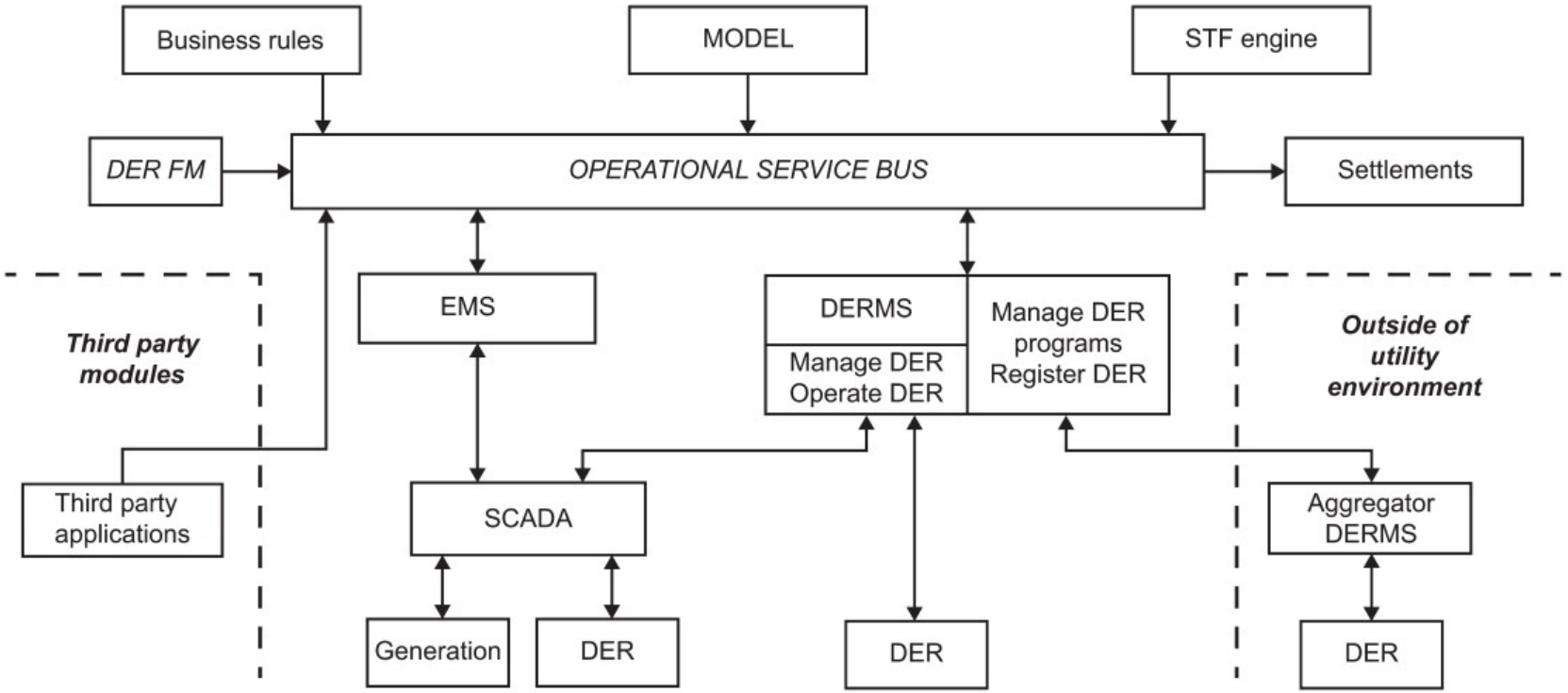


Figure 8 - DERMS deployment and operation example: transmission application IEEE 2030.11[6]

[6] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9447316

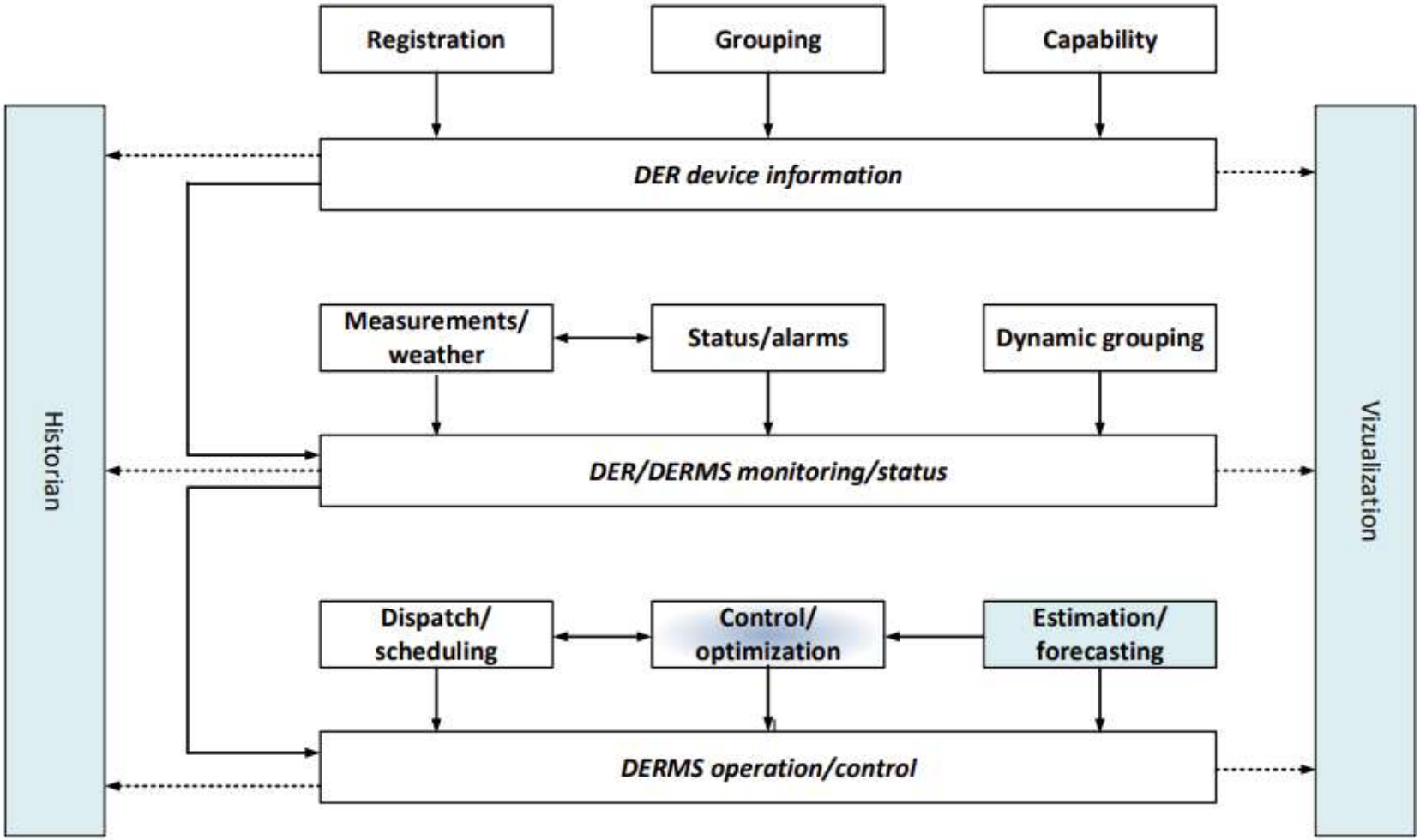


Figure 9 - Examples DERMS functions and their relationships IEEE 2030.11[7]

[7] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9447316

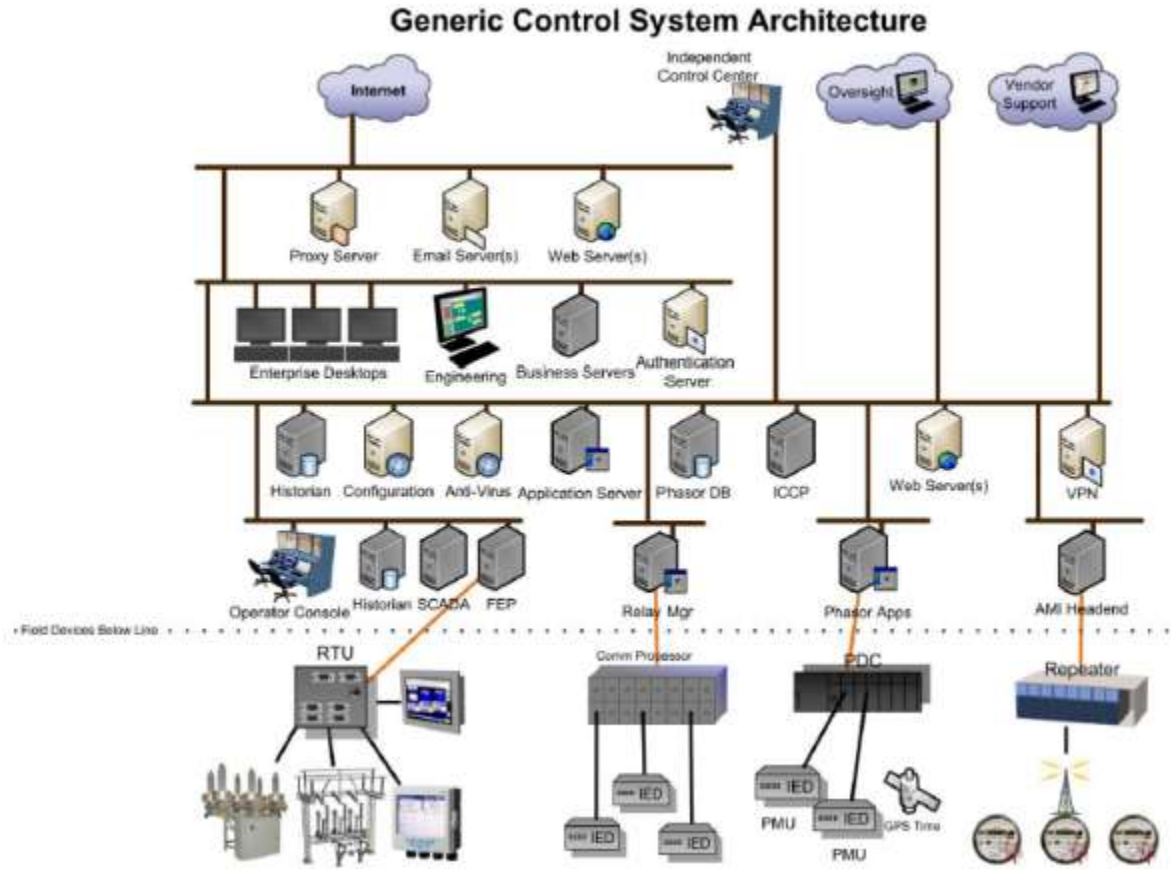


Figure 10 - Generic Information Architecture for a Control System[8]

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.

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

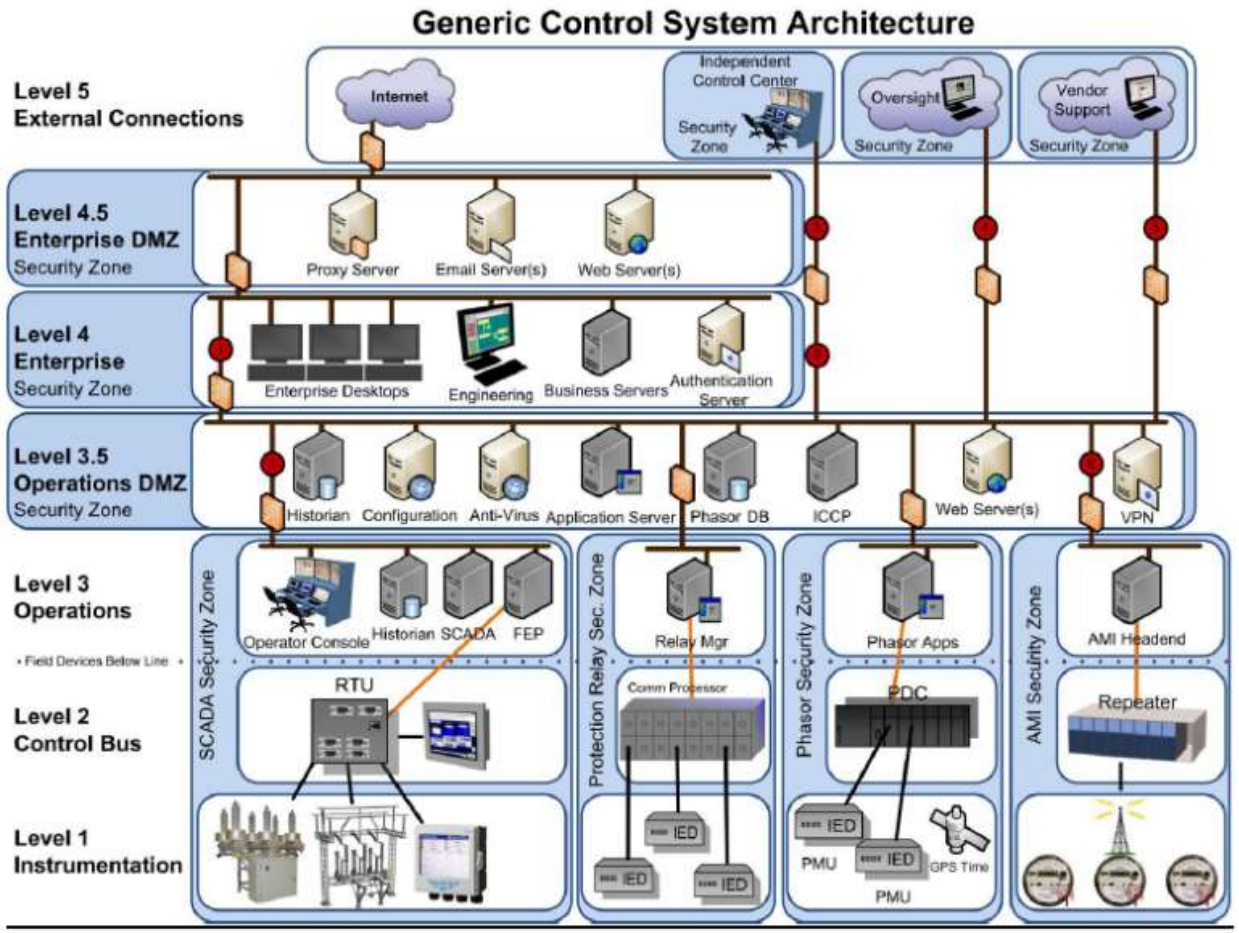


Figure 11 - Generic Control System Architecture, Segmented[9]

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

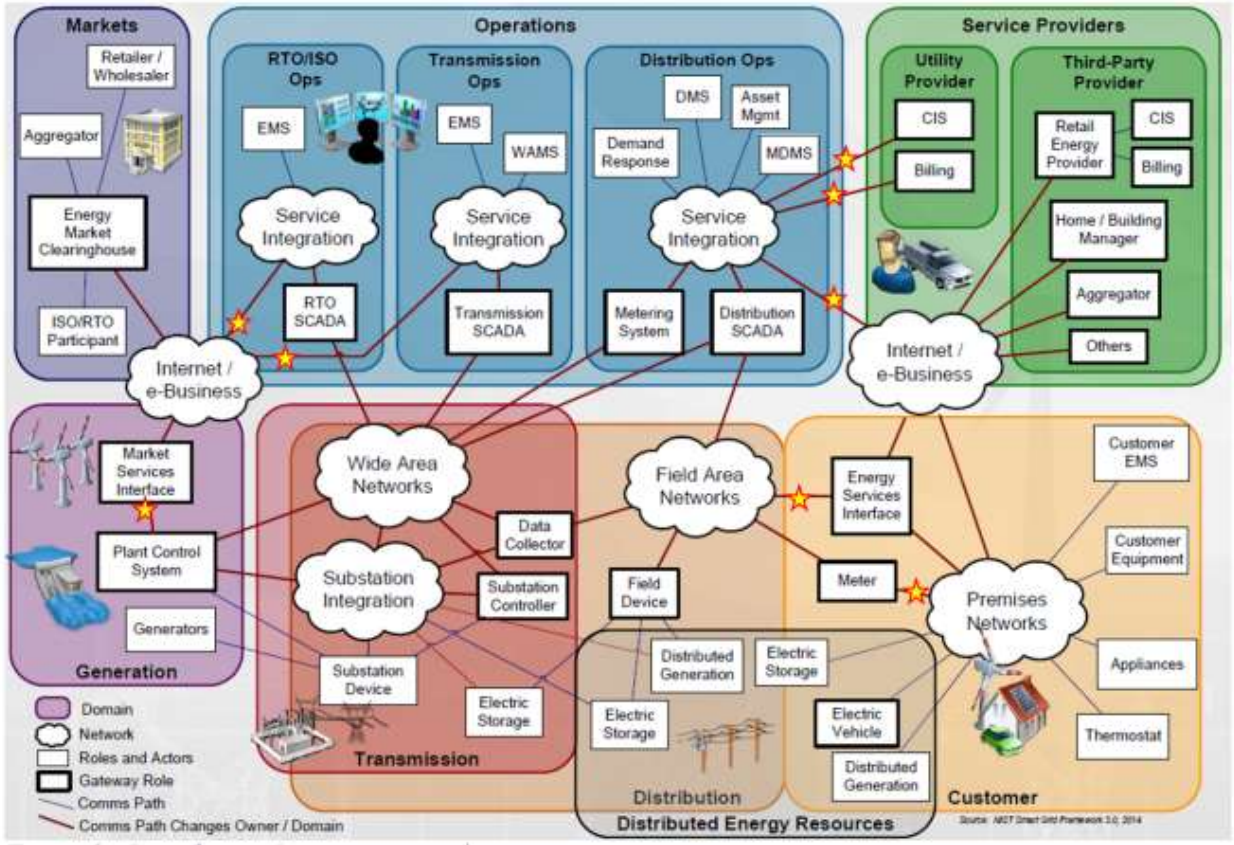
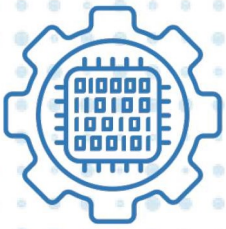


Figure 12 - Distribution Interconnections[10]

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

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



Cyber-Informed Engineering

Idaho National Laboratory