Cyber-Informed
Engineering

Technical Assistance for Securing Digital Energy Infrastructure Webinar

Cyber-Informed Engineering and How to Apply It To Your GRIP Project

Navigating Supply Chain Challenges

Building Resilient Systems for Electric Grid Modernization

The main concern revolves around the availability of US-manufactured products for electric grid modernization and navigating the challenges presented by the geopolitical supply chain landscape.

- How do we drive modernization – while appropriately mitigating risk and consequence
- Project design optimization – secure supply chain and criticality of the application to your operation is a primary consideration
- Focus areas:
    - Electric Vehicles (EVs) + EV Supply Infrastructure
    - Battery Energy Storage Systems (BESS) + management systems
    - Inverters
    - Orchestration software (Distributed Energy Resources Management Systems [DERMS]/Advanced Distribution Management Systems [ADMS])
    - Critical-and-Emerging-Technologies-List-2024-Update.pdf (whitehouse.gov)

See the following sections of the FOA for information on disclosure requirements, domestic content, and related information: IV.D.xxi; IV.I; VI.B; Appendix B; Appendix C.

Launch Plan: How to Evaluate and Protect

(Operate large scale storage and other infrastructure with known higher risk items)

Mitigation menu/strategic training and workshops for consequence based/CIE approach, template & training

Key Injects: Procurement, Contracting, Design, Operations & maintenance

Operate through, maintain the investment, resilience and reliability

Grid Deployment Office (GDO) Technical Assistance Program and INL Team

GDO Technical Assistance

INL Securing Digital Energy Infrastructure Program

Digital Assurance TA

Digital Assurance Technical Assistance

- Goals
  - Improve resilience and supply chain sustainability in the grid modernization space with enhanced security programs for digital equipment
  - Secure digital energy infrastructure by guiding organizations through a tailored analysis, design support and mitigation program
  - Respond to rapidly changing regulatory landscape and cutting-edge equipment
  - Evaluate supply chain and protection choices against the consequences
  - Help entities develop a future sustainable assessment and procurement planning system

Center for Securing the Digital Energy Transition

Emma Stewart
Director

Tracy Briggs
Program Manager

Megan Culler
Technical Director for Clean Energy Cybersecurity

Jake Gentle
Staffing Coordination & Cross Division Manager

Virginia Wright
Strategic Advisor & Operations

Wayne Austad
Strategic Advisor

https://inl.gov/national-security/csdet/

Types of Technical Assistance we provide

Short Advisory

- Quick questions
- Consultations with SMEs
- Overview of available resources

Expert Match

- Workshops and webinars
- Personalized discussion of application of available resources

Deep Dive

- Address inquiries with length development processes
- Threat hunting
- Equipment evaluation

Short Advisory Technical Assistance

- **Who is this for?**
  - Organizations with higher cybersecurity maturity
  - Individuals with specific questions
- **What is the time commitment?**
  - <5 hours of SME time
  - Expected to be performed virtually
  - Setup, execution, and follow up can be completed within 1-2 weeks

1. “I have a question”
2. Match questions to an INL subject matter expert (SME)
3. Schedule a call to discuss.
4. After the call, INL will follow up to verify questions have been answered satisfactorily

Virtual SME

- Quick virtual consultations to answer specific questions

Resource Overview

- Call to provide overview of the resources available to support cybersecure BESS deployments

Assessment templates

- Resources provided for do-it-yourself risk mitigation

Expert Match Technical Assistance

- **Who is this for?**
  - Teams looking for training to enhance cyber maturity
  - Projects in design or contracting phase with a need for dedicated cyber support
  - Organizations with inquiries that require increased resources
- **What is the time commitment?**
  - 5-10 hours of SME time
  - Participating organization may want to involve engineering, operations, and cybersecurity personnel
  - Full activity can be completed within 2-6 weeks of initial contact

CIE workshops

- Cyber-informed engineering workshop or webinar

SME Consulting

- Dedicated time from an SME to discuss specific implementation challenges

Design Guidance

- Individual sessions to review BESS design cybersecurity guidance and discuss personalized application

Procurement Guidance

- Individual sessions to review procurement guidance and discuss personalized application

Deep Dive Technical Assistance

- **Who is this for?**
  - Organizations just starting to implement cyber policies, practices, and procedures
  - Inquiries that require substation resources or lengthy development process
  - Applications requiring assistance such as sourcing, assessment of equipment being installed
  - Applicants requesting site visits
- **What is the time commitment?**
  - 15-40 hours expected, could be split across different roles
  - Multiple personnel will be involved (operations, cybersecurity, engineering, networking/IT)
  - Full activity may take 4-8 weeks to plan and execute

Cybersecurity Assessments

- Cyber Security Evaluation Tool
- Measure alignment to standards and best practices

Threat Hunt

- Short-term monitoring for anomalous network behaviors

Equipment Physical/Forensic Assessment

- Assessment of field devices
- Requires devices to be shipped to lab

Site Visit for In-Depth Analysis

- OT equipment, processes, procedures

OT Security Training

- Tailored to participant needs

Malcolm AIA

- Asset Interaction Analysis
- Automated generation of network diagram based on passive monitoring

Cybersecurity and Operational Technology

What is Cybersecurity?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

-- Cybersecurity and Infrastructure Security Agency (CISA)

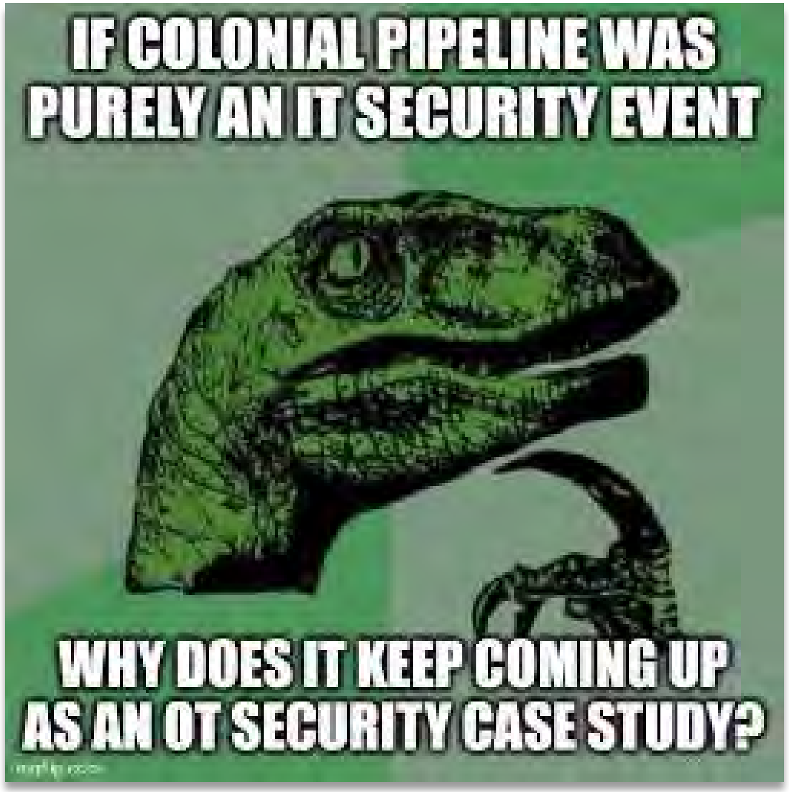
What is Cybersecurity?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

-- Cybersecurity and Infrastructure Security Agency

What's missing in this picture?

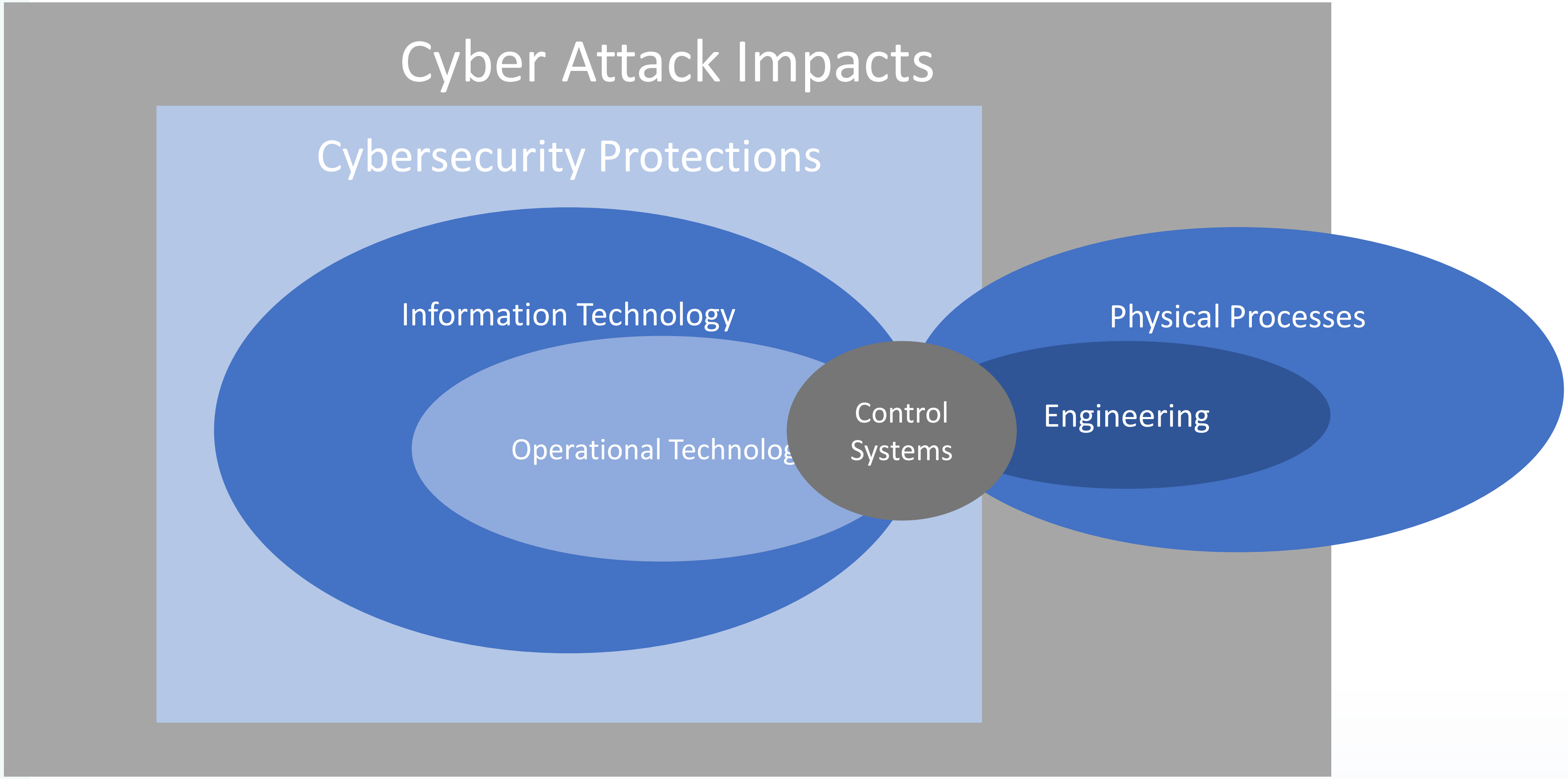
Cybersecurity is not just about data


IF COLONIAL PIPELINE WAS PURELY AN IT SECURITY EVENT
WHY DOES IT KEEP COMING UP AS AN OT SECURITY CASE STUDY?
imgflip.com

Joe Slowick, MITRE

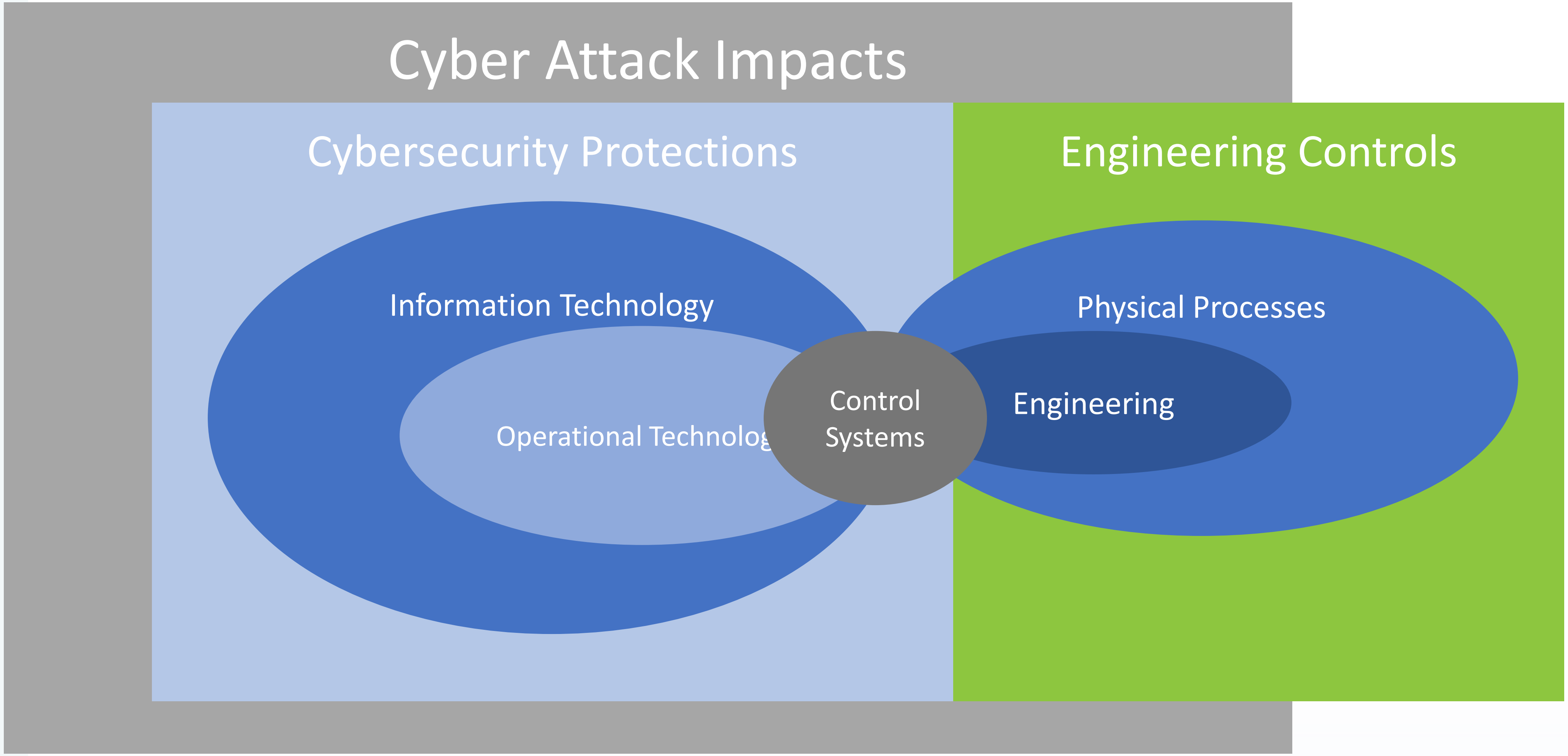
- Ransomware attacked business data on an IT network
- However, pipeline operations were curtailed.
- Why?

Cybersecurity in Operational Technology



Cyber-Informed Engineering

Cyber-Informed Engineering



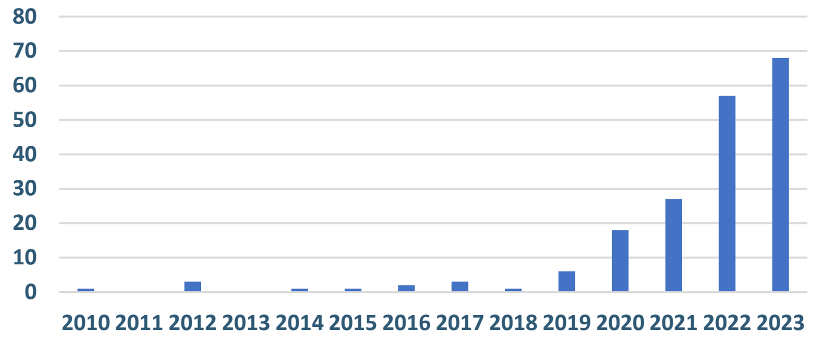
How are Cyber Attacks affecting Physical Infrastructure?

- Ransomware accounts for 80% of attacks where threat actor is known
- Multiple nation-state attacks on OT open to the internet
  - Weak or default passwords
  - Vulnerable system
- Nation States using commodity tools, tactics and techniques
- 50% of identified incidents impacted process and discrete manufacturing
  - Production shutdowns, work stoppages and shipping delays
- Financial impacts are public record:
  - $27-450M
- The largest impacts to operations are indirect, including IT dependencies and “abundance of caution shutdowns”
- OT-related Supply Chain Attacks are increasing

Predictions:

- Ransomware attacks with OT consequences will increase
- Politically motivated attacks will increase in number and impact alongside criminal ransomware
- The success of “indirect” attacks will drive more attempts

OT Cyber Attacks with Physical Consequences



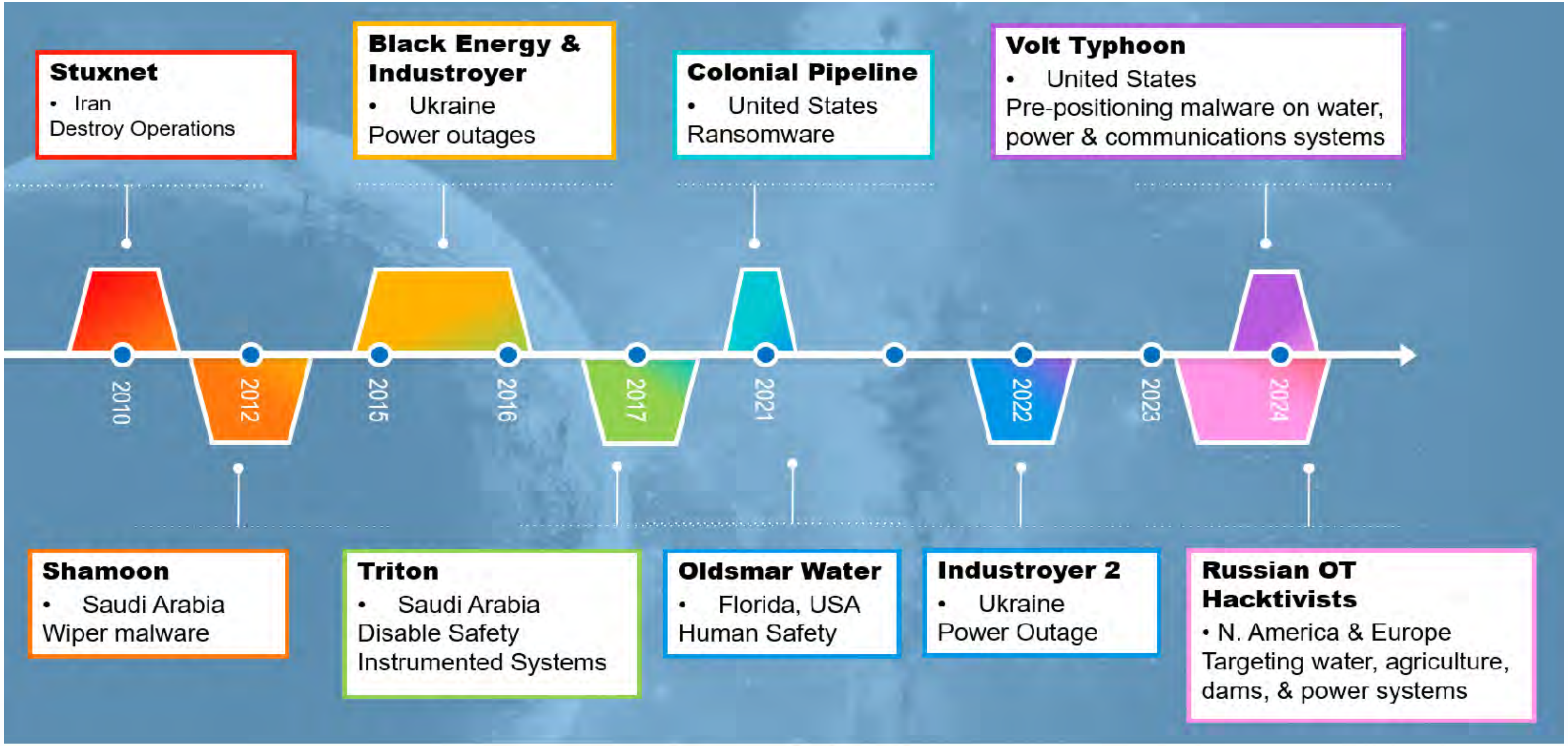
Volt Typhoon

Zyxel Firewalls

Water sector

- Data from Waterfall 2024 Threat Report on OT Cyberattacks with Physical Consequences - https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/2024-threat-report-blog/

Cyber Attacks on Control Systems are Real – and Growing



Stuxnet
- Iran

Destroy Operations

Black Energy & Industroyer
- Ukraine

Power outages

Colonial Pipeline
- United States

Ransomware

Volt Typhoon
- United States

Pre-positioning malware on water, power & communications systems

Shamoon
- Saudi Arabia

Wiper malware

Triton
- Saudi Arabia

Disable Safety Instrumented Systems

Oldsmar Water
- Florida, USA

Human Safety

Industroyer 2
- Ukraine

Power Outage

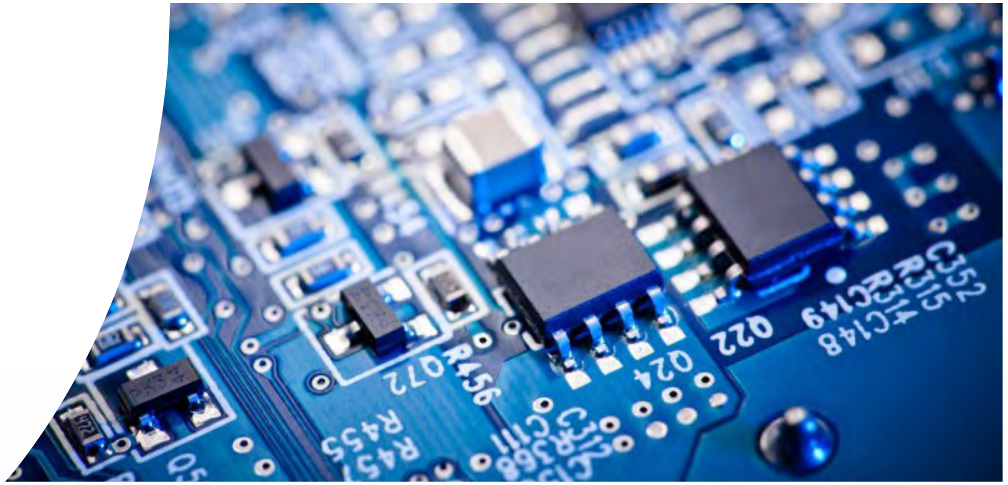
Russian OT Hacktivists
- N. America & Europe

Targeting water, agriculture, dams, & power systems

Cyber-Informed Engineering

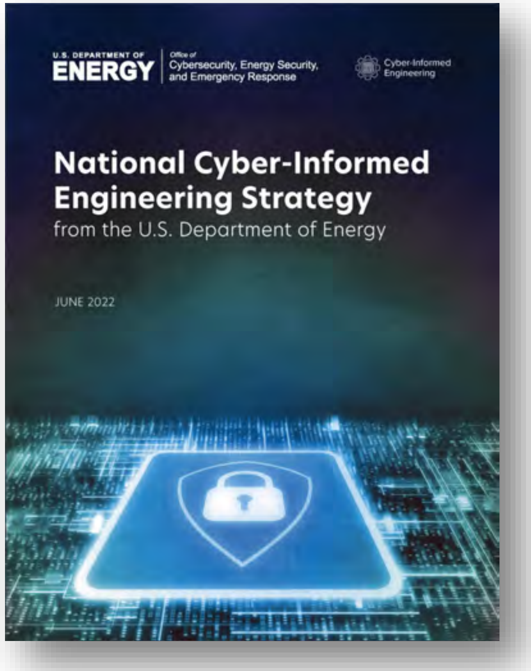
Cyber-Informed Engineering (CIE)

- 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, rather than add cybersecurity controls after the fact.
- Focused on **engineers and technicians**, CIE provides a framework for cyber education, awareness, and accountability.
- CIE aims to create a **culture of security** aligned with the existing industry safety culture.



National CIE Strategy

- Directed by the U.S. Congress in the Fiscal Year 2020 National Defense Authorization Act
- Outlines core CIE concepts
  - Defined by a set of design, operational, and organizational principles
  - Placed cybersecurity considerations at the foundation of control systems design and engineering
- Five integrated pillars offer recommendations to incorporate CIE as a common practice for control systems engineers
  - Intended to drive action across the industrial base stakeholders—government, owners and operators, manufacturers, researchers, academia, and training and standards organizations
- DOE issued the National CIE Strategy June 15, 2022
- CIE has been named in the National Cyber Strategy and the National Cyber Strategy Implementation Plan and in the report on cyber-physical systems by the President’s Council of Advisors on Science and Technology



U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

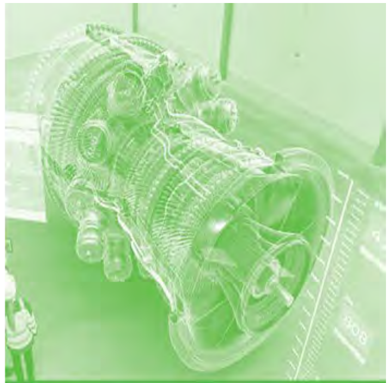
Cyber-Informed Engineering

National Cyber-Informed Engineering Strategy
from the U.S. Department of Energy

JUNE 2022

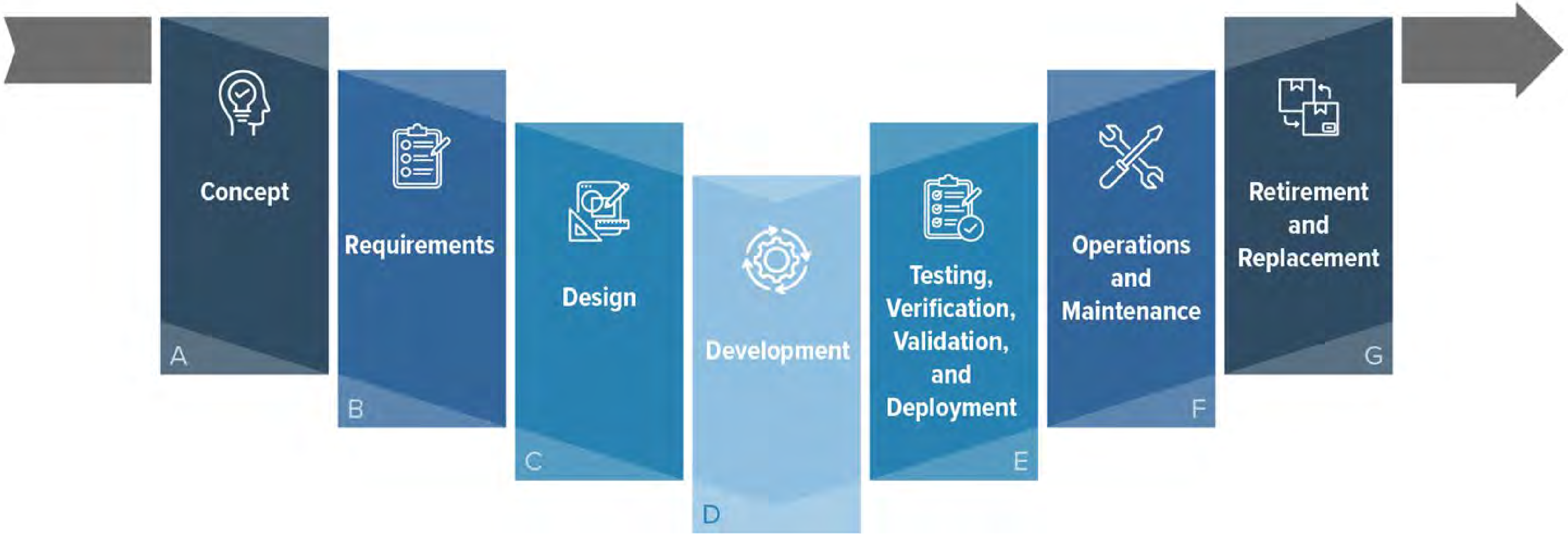
https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf

Pillars of the National CIE Strategy

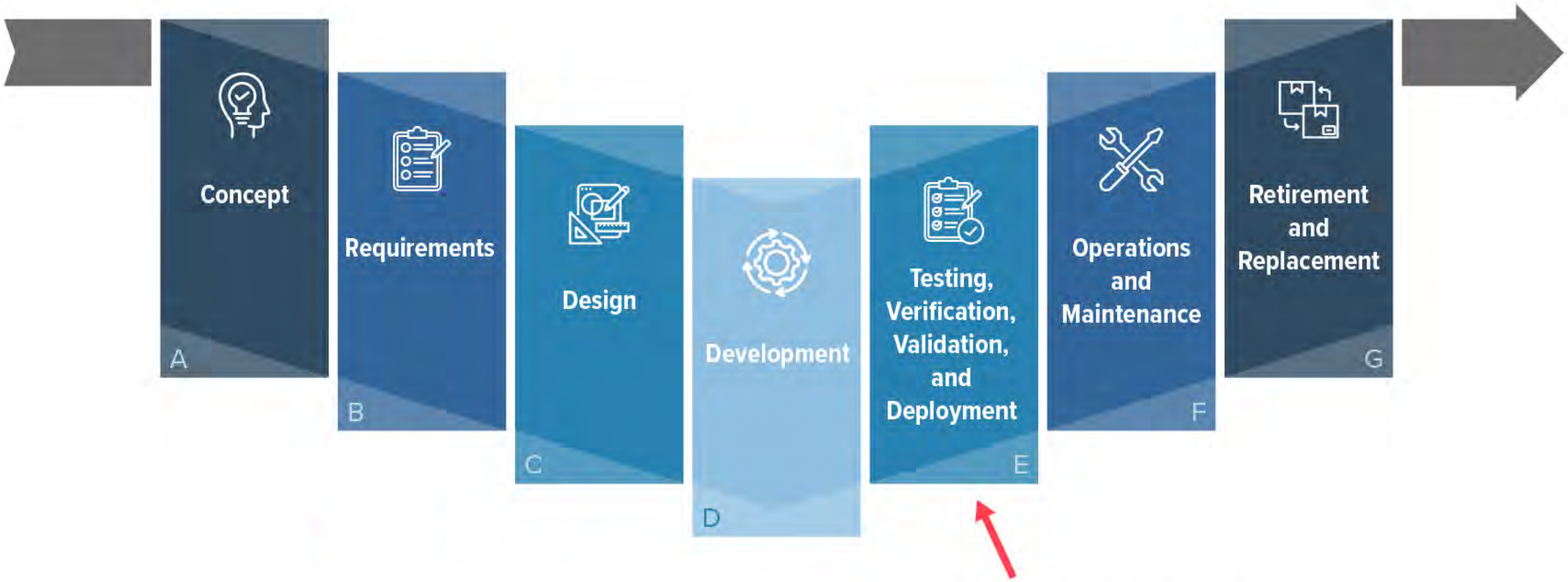


Awareness	Education	Development	Current Infrastructure	Future Infrastructure
Promulgate a universal and shared understanding of CIE	Embed CIE into formal education, training, and credentialing	Build the body of knowledge by which CIE is applied to specific implementations	Apply CIE principles to existing systemically important critical infrastructure	Conduct R&D and develop an industrial base to build CIE into new infrastructure systems and emerging technology

CIE and the Systems Engineering Lifecycle

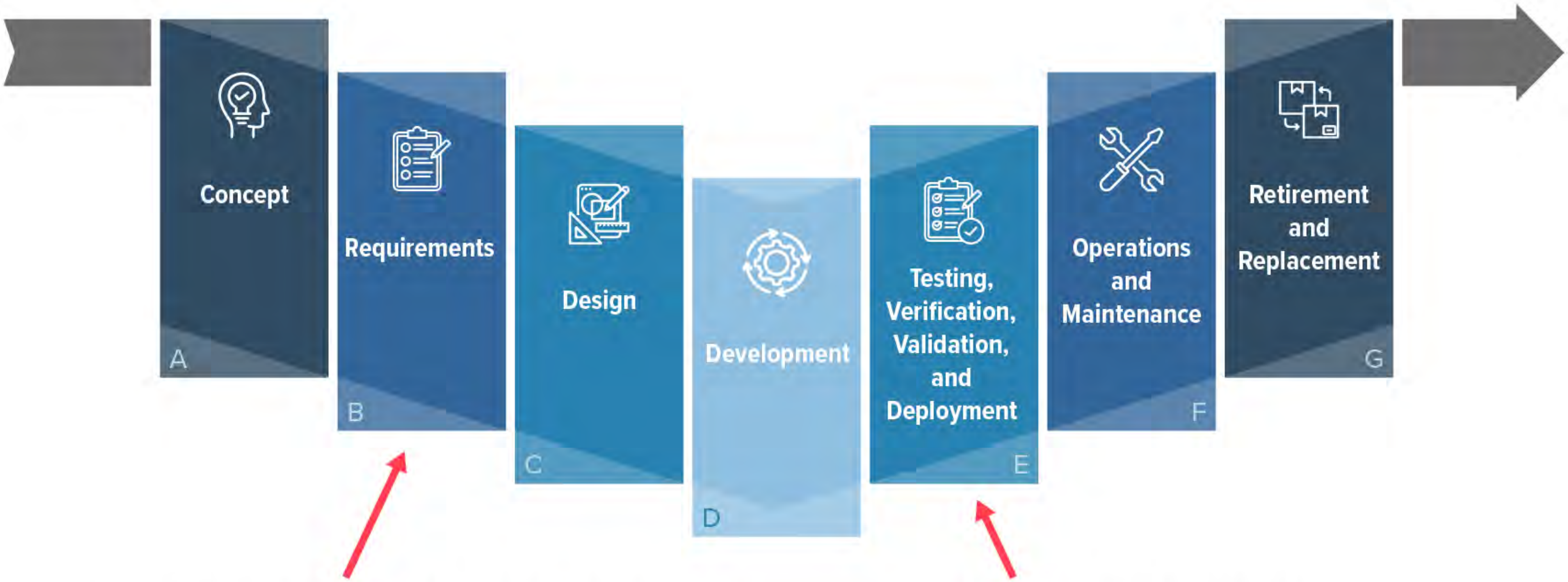

Concept
A
Requirements
B
Design
C
Development
D
Testing, Verification, Validation, and Deployment
E
Operations and Maintenance
F
Retirement and Replacement
G

CIE and the Systems Engineering Lifecycle


Concept
A
Requirements
B
Design
C
Development
D
Testing, Verification, Validation, and Deployment
E
Operations and Maintenance
F
Retirement and Replacement
G

OT Cybersecurity risk mitigations are usually applied here…

CIE and the Systems Engineering Lifecycle


Concept
A
Requirements
B
Design
C
Development
D
Testing, Verification, Validation, and Deployment
E
Operations and Maintenance
F
Retirement and Replacement
G

…but they are more effective and efficient when applied here.

OT Cybersecurity risk mitigations are usually applied here…

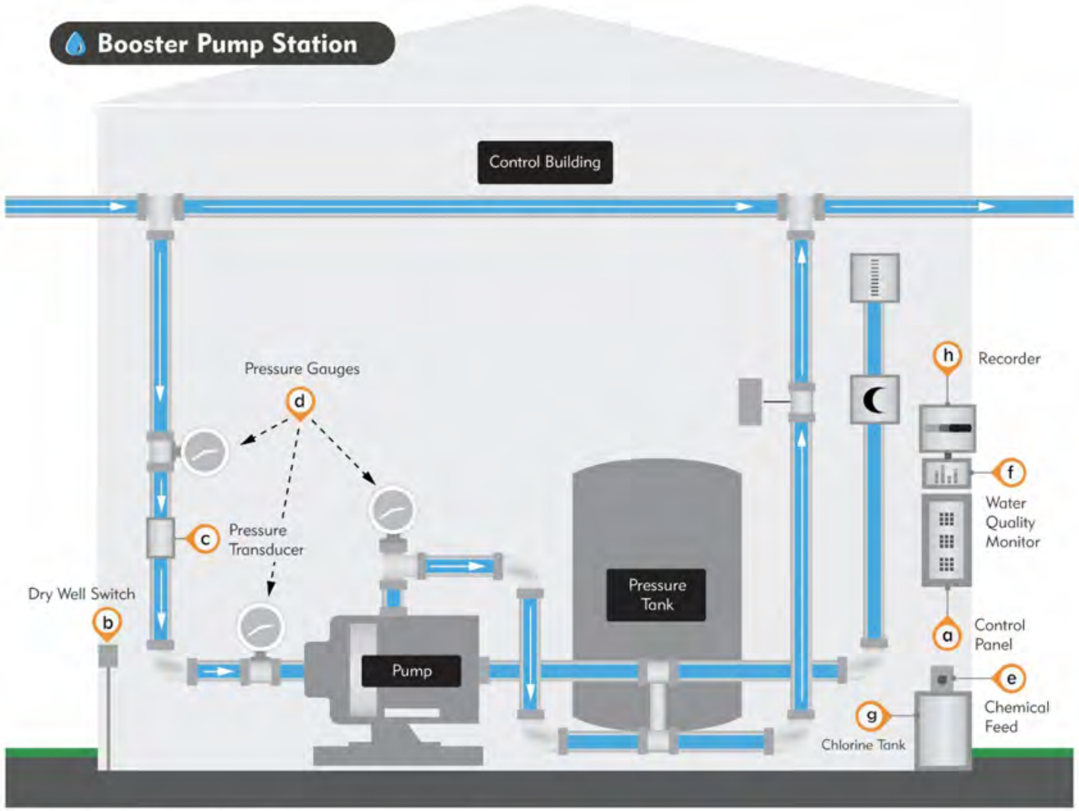
CIE Principles

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

How does this work in practice?

Water Booster Pump Station

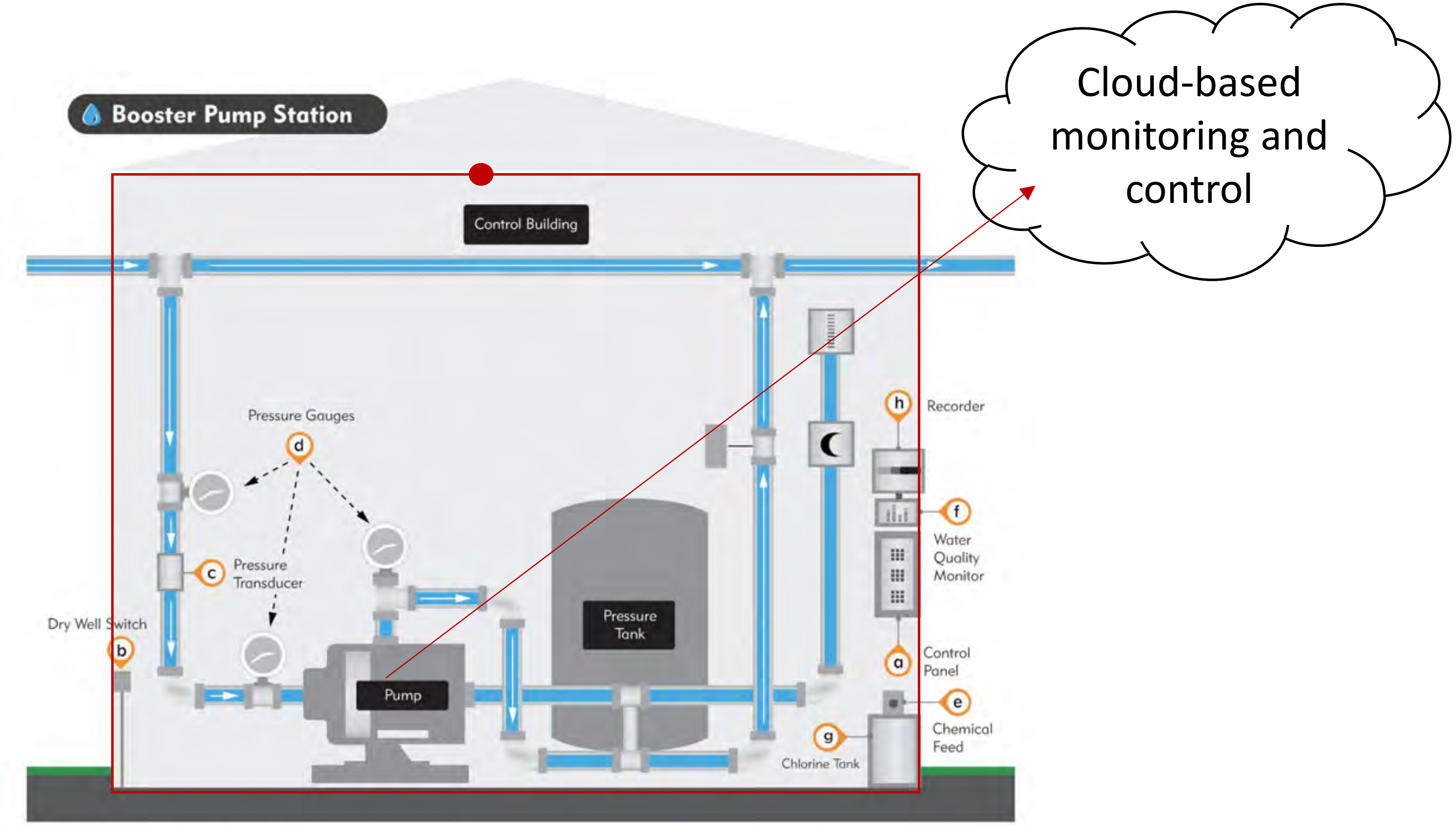
Water Booster Pump Station



Water Booster Pump Station Archives App4Water

https://bmxlovesk.xyz/product_details/13200675.html

Water Booster Pump Station



Cloud-based monitoring and control

Water Booster Pump Station Archives App4Water

https://bmxlovesk.xyz/product_details/13200675.html

Cyber Solution Review

- Control System Software has a qualifying secure development lifecycle.
  - Very mature demonstrated processes
  - Provided SBOM
  - Component infrastructure is up to date
  - Mature vulnerability release process – with regular patches
  - 24/7 Support availability

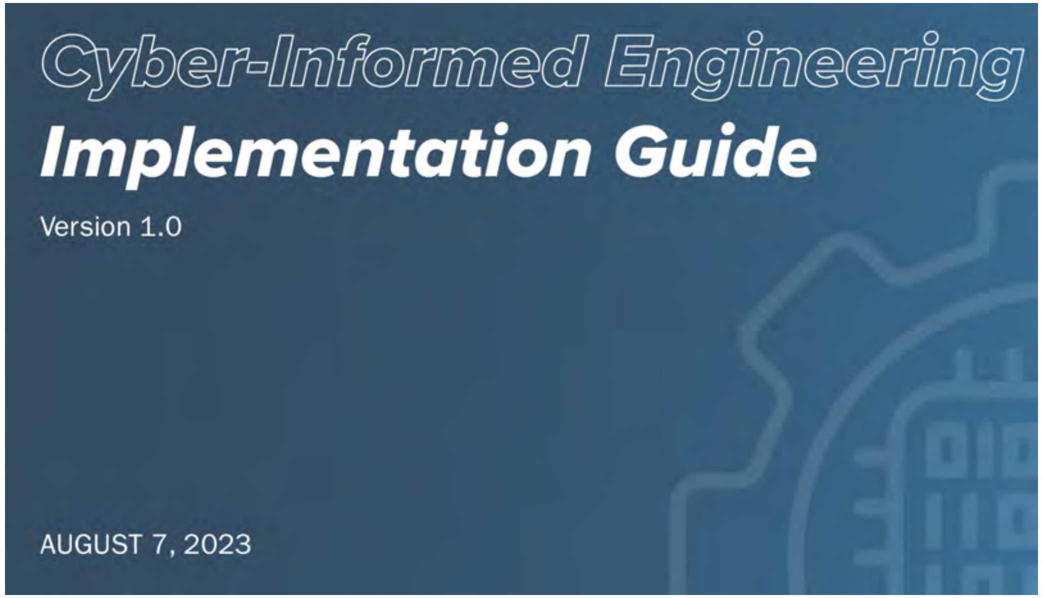
- Cloud provider is reputable and qualified
  - SOC Type 2 and Fedramp (if needed), great physical security
  - Very mature, experienced in hosting critical infrastructure services
  - Demonstrated response and restoration capabilities

IT Installation Review

- Network entry point has standard security package
- Monitoring and logging traffic on this interface according to standard practice
  - Logging interfaces with organizational logging system
- Traffic in and out is encrypted between the cloud provider and the internal network boundary

Organizational Review Board Votes

- Finance / Accounting – ☑
- Information Technology – ☑
- Cybersecurity – ☑
- Engineering Operations – ? ➡



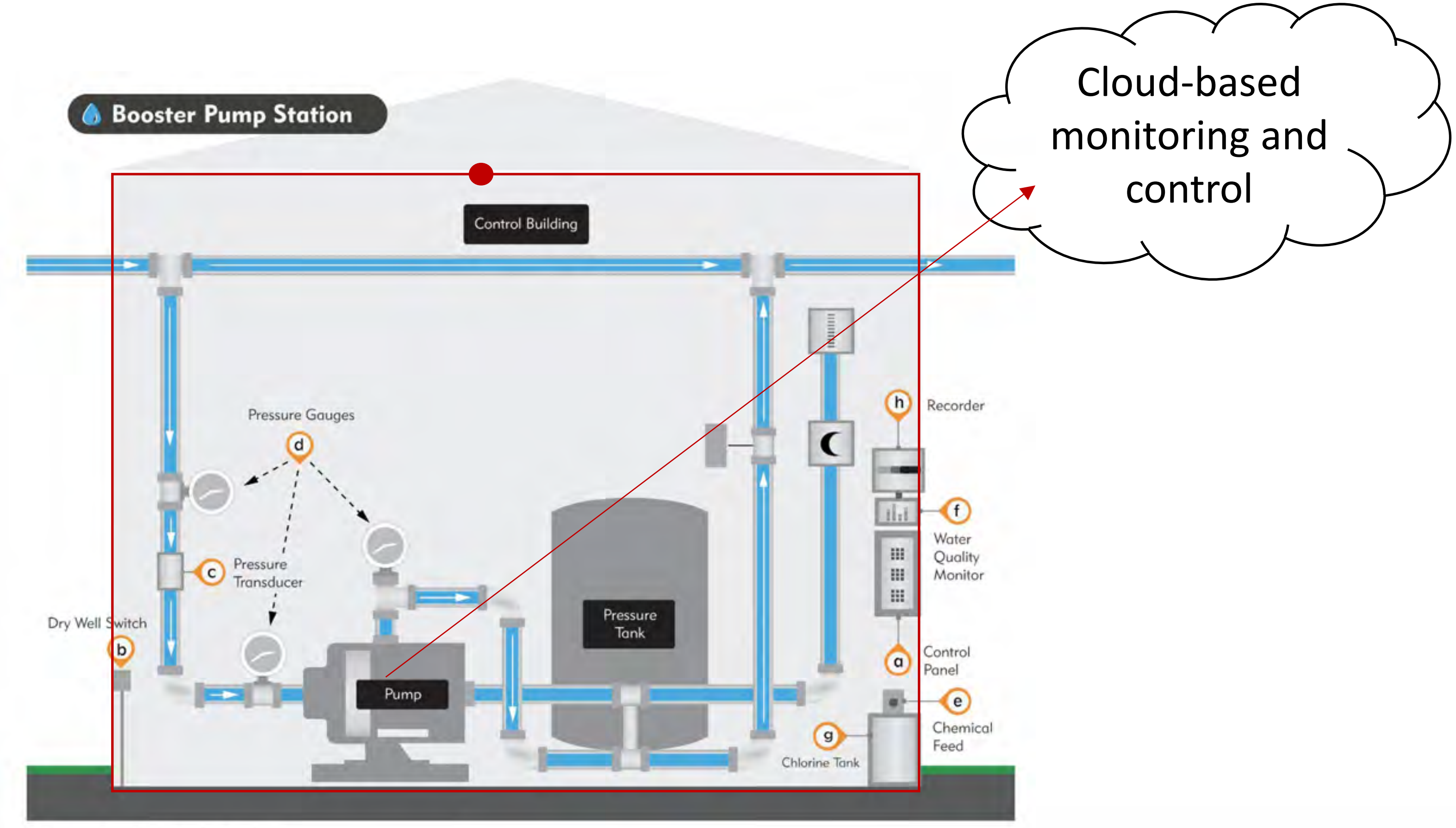
Cyber-Informed Engineering

Implementation Guide

Version 1.0

AUGUST 7, 2023

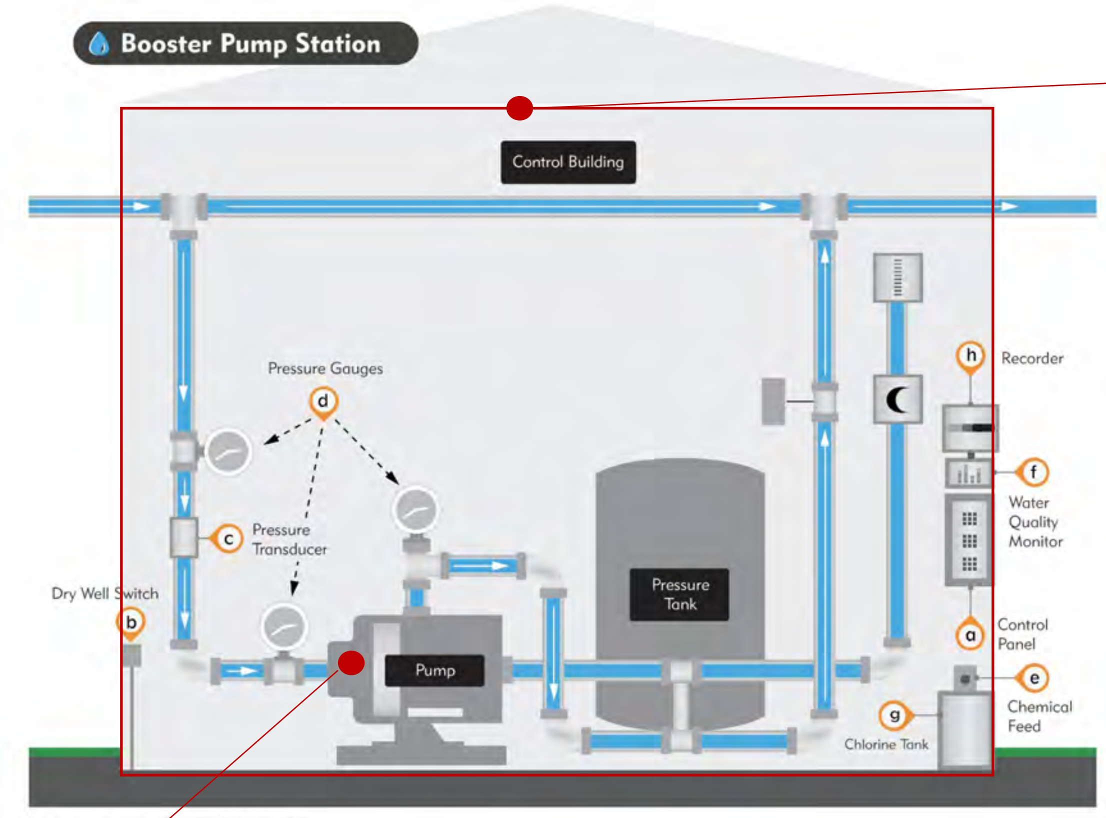
Water Booster Pump Station



Water Booster Pump Station Archives App4Water

https://bmxlovesk.xyz/product_details/13200675.html

Water Booster Pump Station



Water Booster Pump Station Archives App4Water

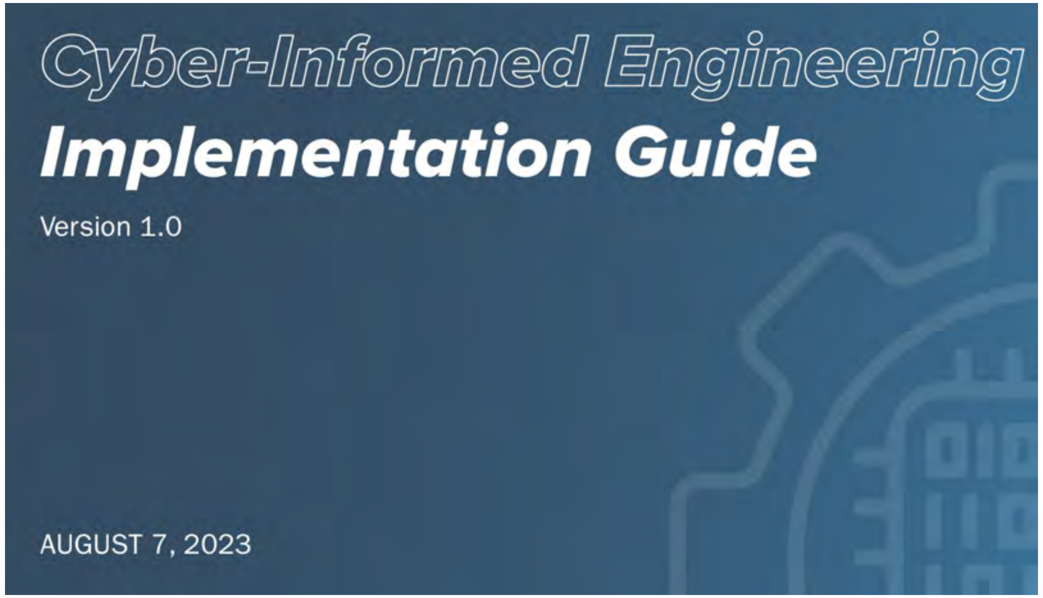
https://bmxlovesk.xyz/product_details/13200675.html

Cloud-based monitoring and control

Mechanical Time Delay Relay

Organizational Review Board Votes

- Finance / Accounting – ☑
- Information Technology – ☑
- Cybersecurity – ☑
- Engineering Operations – ☑ ➡



Cyber-Informed Engineering

Implementation Guide

Version 1.0

AUGUST 7, 2023

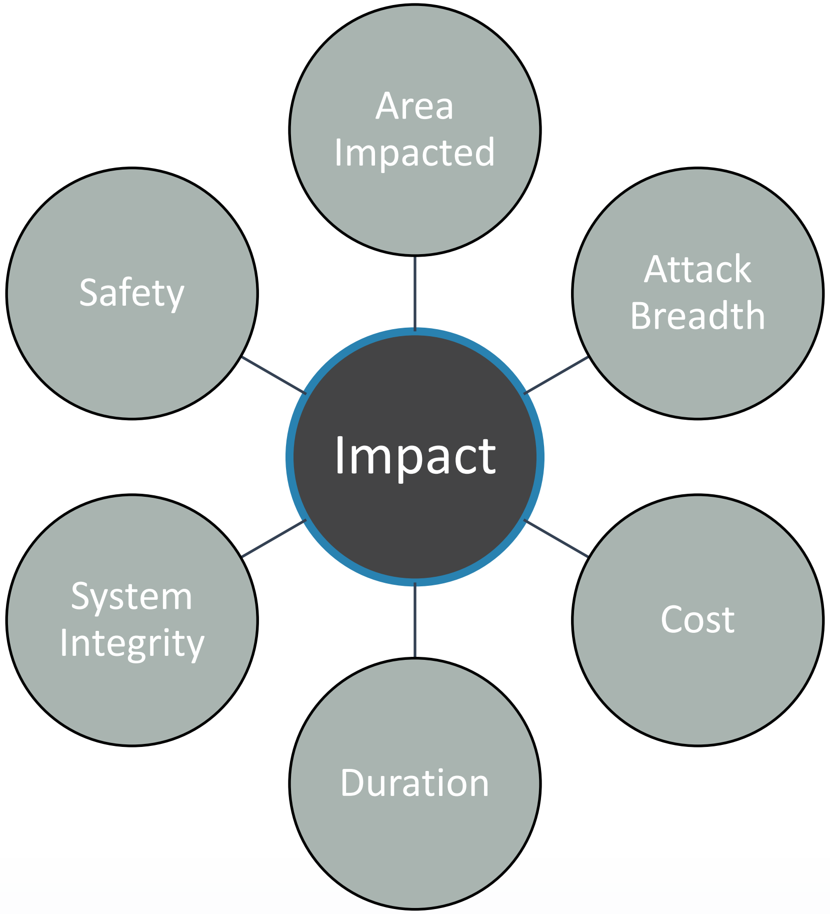
CIE Principles Deeper Dive

Consequence-Focused Design

KEY QUESTION

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

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

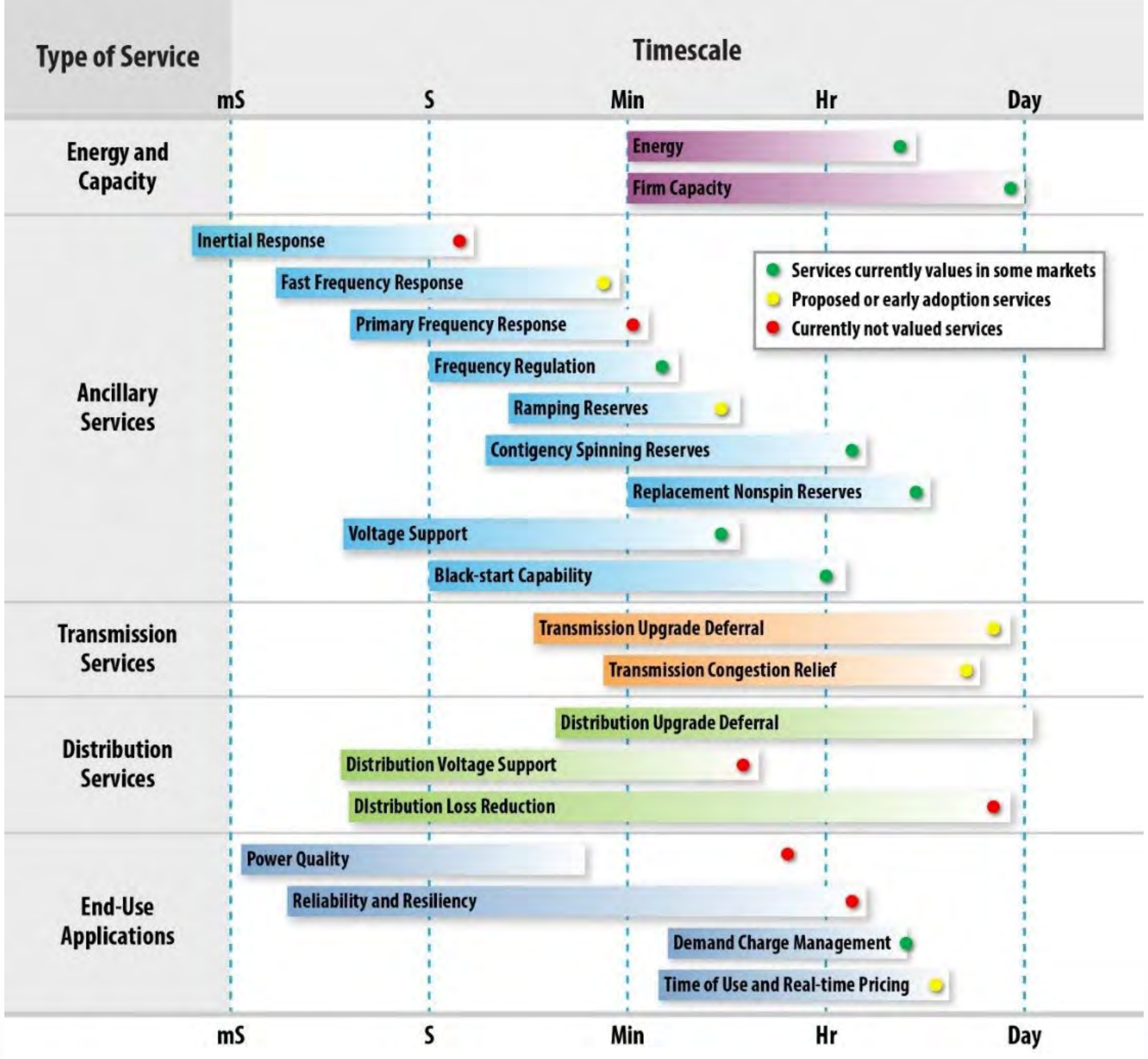


Cyber-Informed Engineering

Consequence-Focused Design in Practice

A critical function could be the grid service(s) that your installation is designed, or contracted, to provide.

Consequence of losing that grid service is determined by each installation and its magnitude.

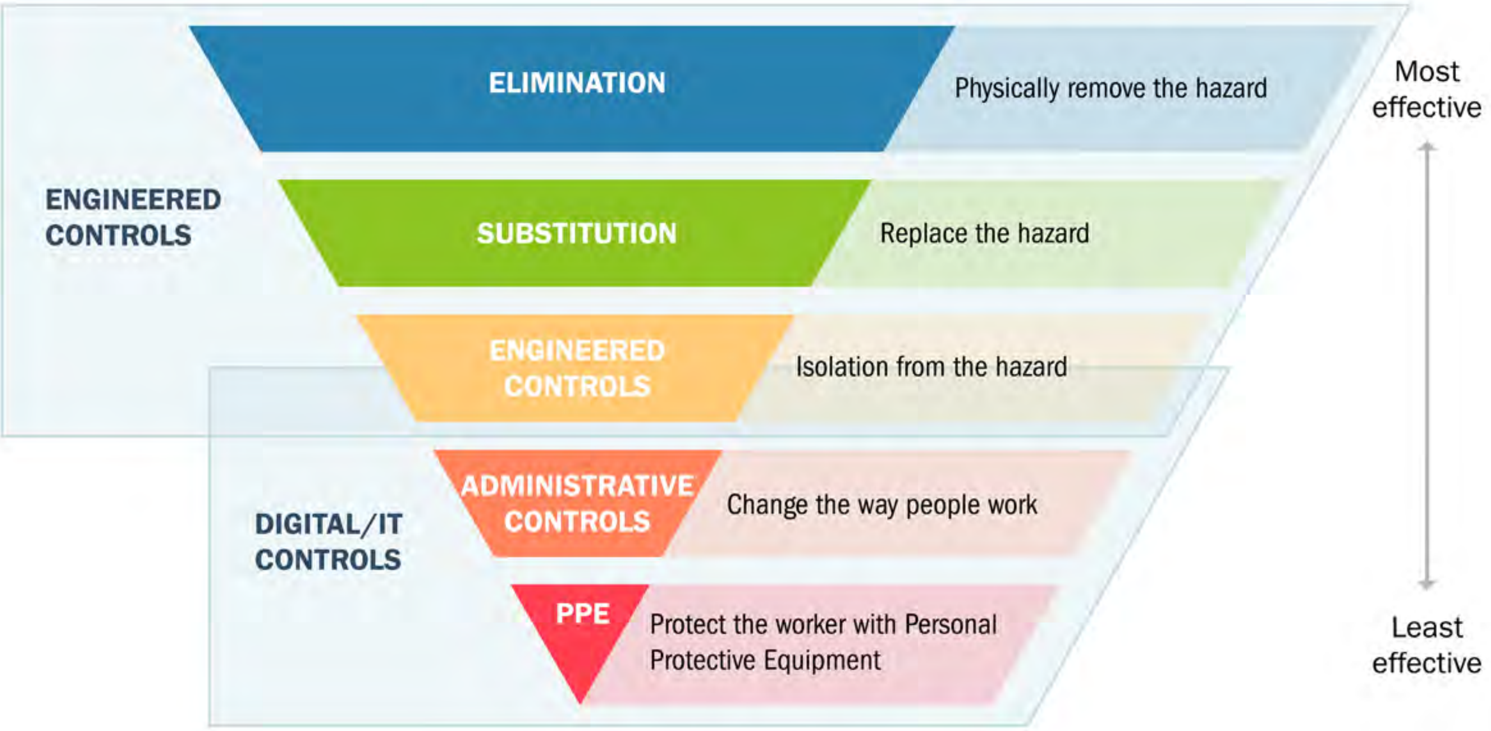


Engineered Controls

KEY QUESTION

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

Hierarchy of Controls



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

Engineered Controls in Practice

Use of a mode key prevents updating of a PLC controller (BESS controller, site controller, etc.) unless you are physically at the unit.

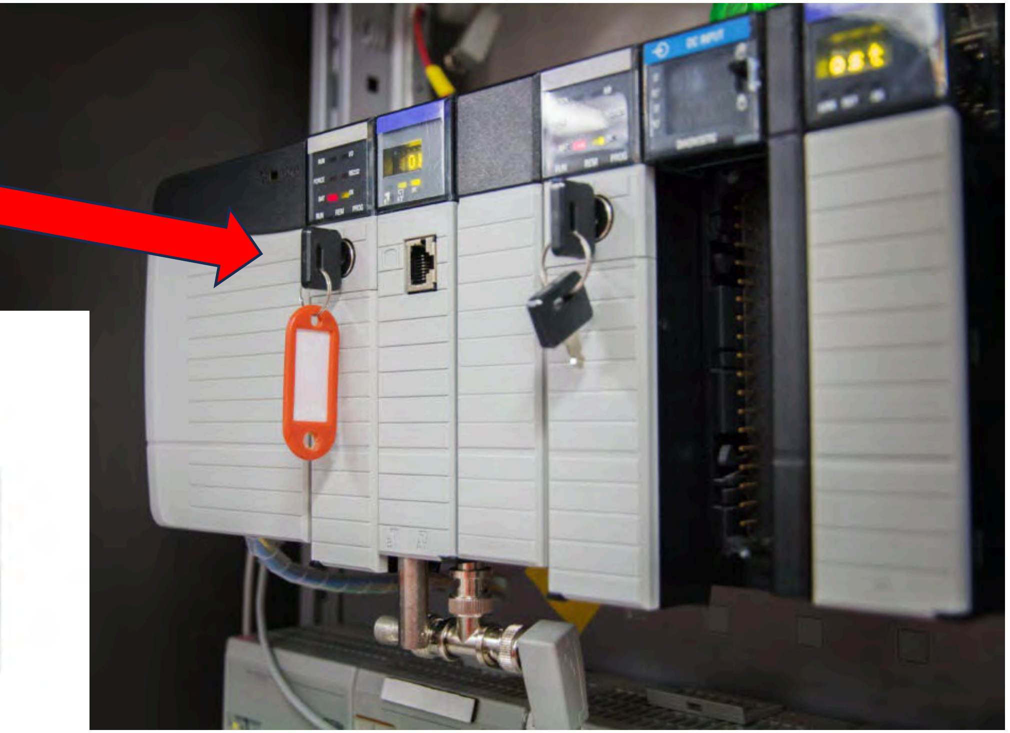


Image Source: https://www.dragos.com/blog/industry-news/value-of-plc-key-switch-monitoring/

Phase monitoring relay can be used to provide a non-digital control decision when a cyber attack creates a phase reversal, phase loss, phase unbalance, overvoltage and undervoltage scenario in 3-phase systems (AC Inverter Side)

Image Source: https://www.automationdirect.com/adc/shopping/catalog/relays_-z-_timers/phase_monitoring_relays

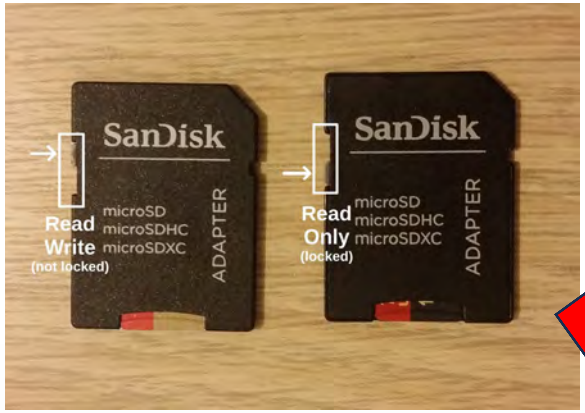


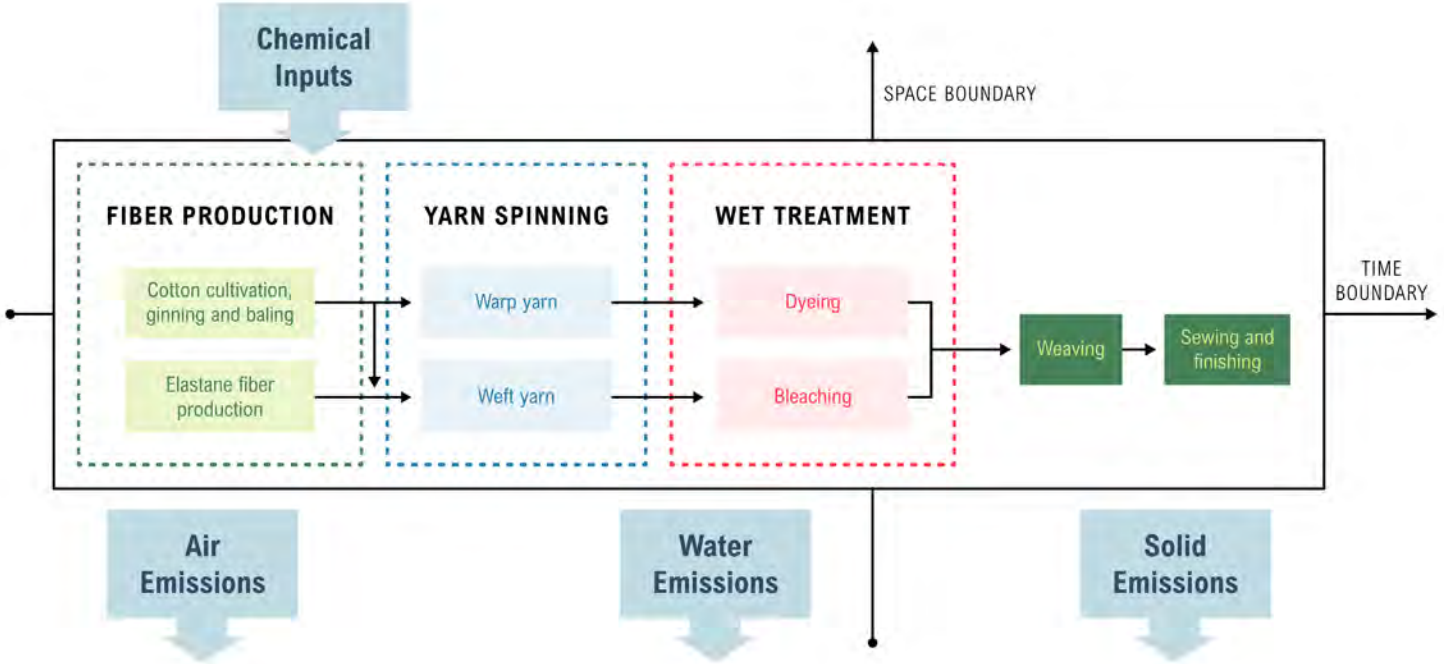
Image Source: https://9to5answer.com/unable-to-open-dev-sdb-read-write-read-only-file-system

SD Card has a toggle switch to change from Read-Write to Read Only to prevent manipulation (firmware updates, code files, etc.)

Secure Information Architecture

KEY QUESTION

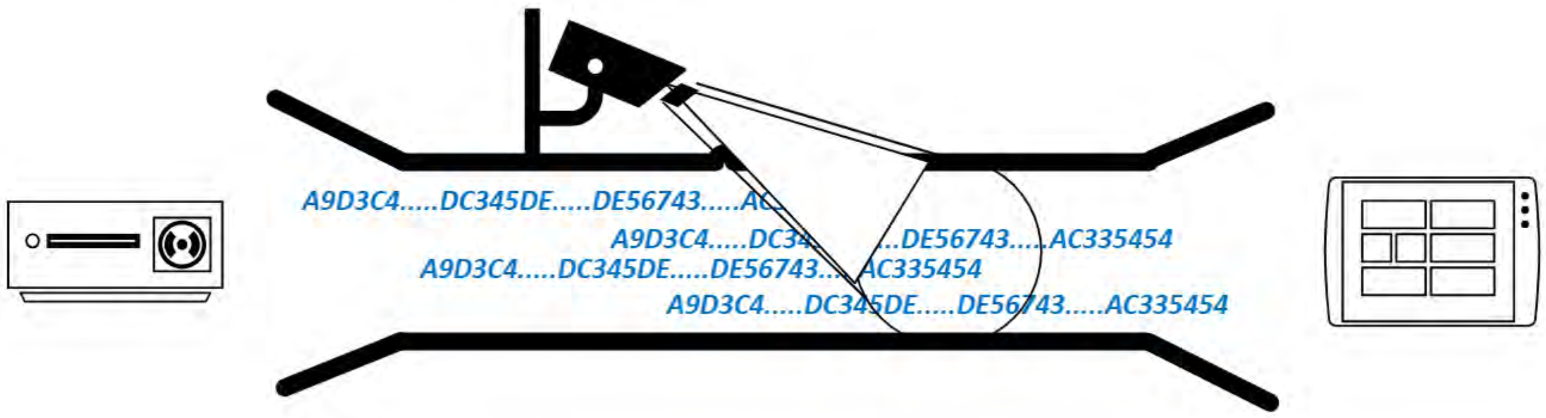
How do I prevent undesired manipulation of important data?



For our critical functions:

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

Secure Information Architecture in Practice


A9D3C4.....DC345DE.....DE56743.....AC
A9D3C4.....DC34
...DE56743.....AC335454
A9D3C4.....DC345DE.....DE56743....
AC335454
A9D3C4.....DC345DE.....DE56743.....AC335454

Key data is used between communicating equipment when sensing and commanding a critical function in the system. This information is best understood by the engineering staff, who should help inform:

- Monitoring Policy and Rules
- Firewall Policy and Rules
- Network Segmentation

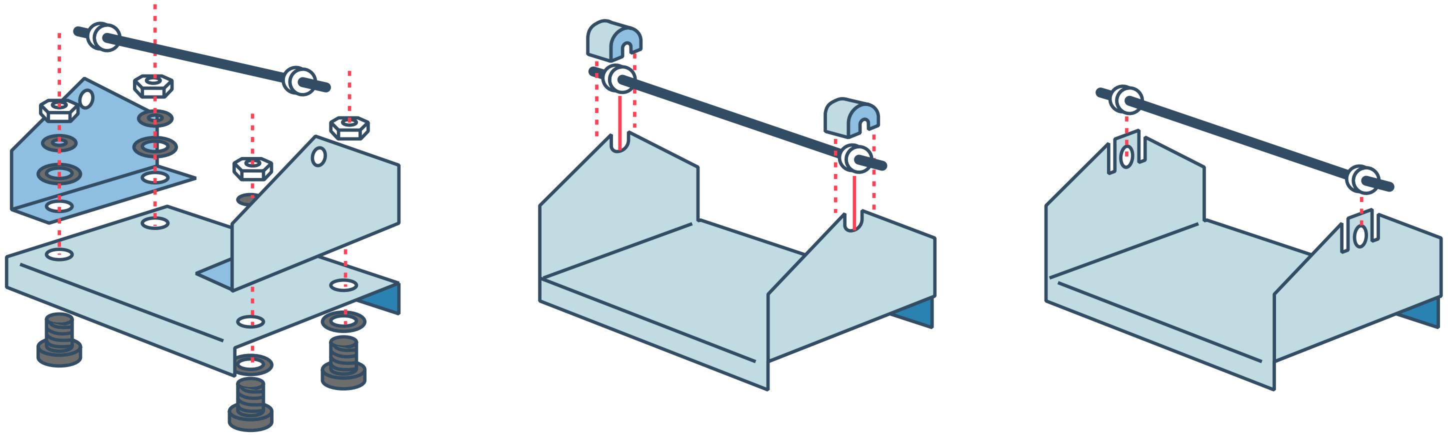
For example, the heartbeat signal that is often used in microgrid installations between the energy management system (EMS) and the BESS Controller to allow for power mode commands to be accepted could be seen as a key piece of data that should be protected and monitored for.

Design Simplification

KEY QUESTION

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

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



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

Design Simplification in Practice

Cell modems are often installed in systems to provide a digital communication between a vendor and their equipment such as a BESS installation.

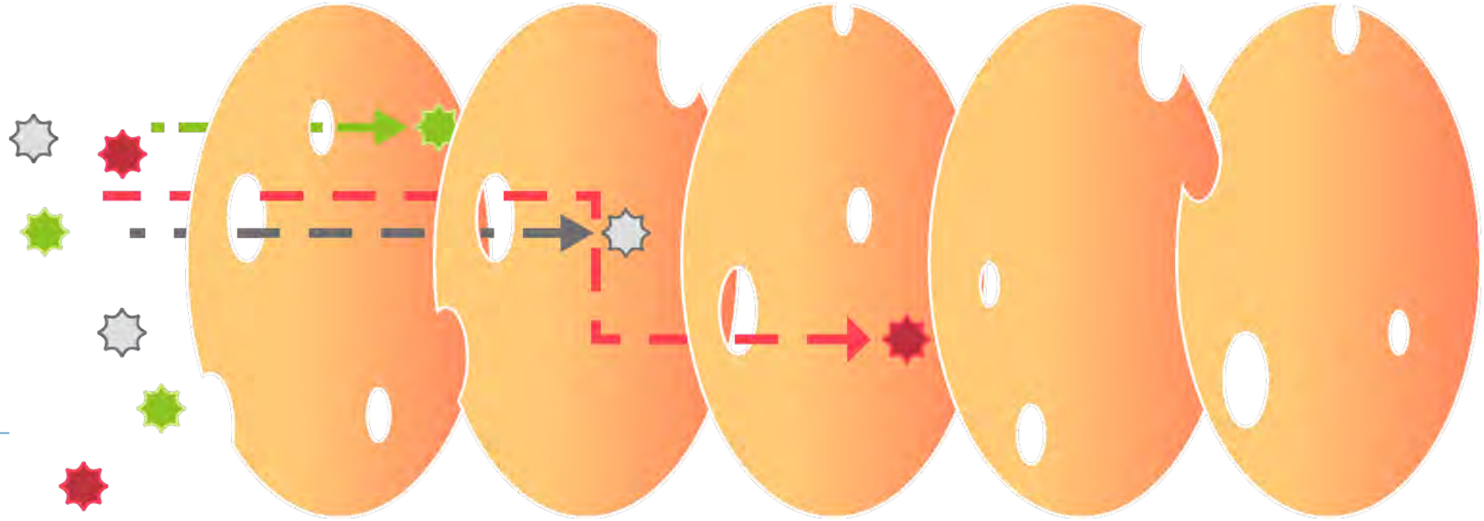
This path is often redundant to a physical communication path through a site firewall and site router to an EMS service. Design Simplification would suggest removing this “alternate” path and require communication only through the firewall.

Image source: https://www.radwell.com/Shop?source=GoogleShopping&IgnoreRedirect=true&ItemSingleId=195062231

Layered Defenses

KEY QUESTION

How do I create the best compilation of system defenses?



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

Layered Defenses in Practice

Cybersecurity Controls

- Network Segmentation
- Access Control (i.e. passwords, RBAC, etc.)
- Monitoring
- Backups
- Updates
- Physical Access Control
- Etc.

Reduce Likelihood

Engineering Controls

- PLC Mode Keys
- Analog Circuitry
- Manual Modes of Operation
- Feasibility Checks in Process Logic
- Etc.

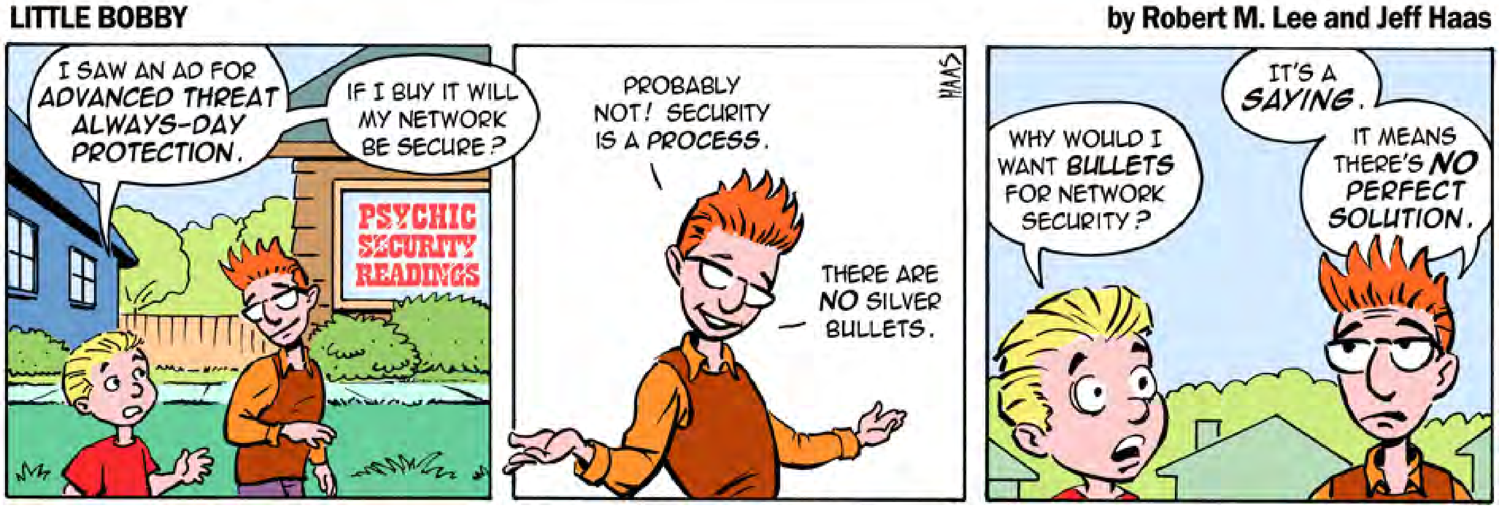
Reduce Impacts

Active Defense

KEY QUESTION

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

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


LITTLE BOBBY
by Robert M. Lee and Jeff Haas
I SAW AN AD FOR ADVANCED THREAT ALWAYS-DAY PROTECTION.
IF I BUY IT WILL MY NETWORK BE SECURE?
PSYCHIC SECURITY READINGS
PROBABLY NOT! SECURITY IS A PROCESS.
THERE ARE NO SILVER BULLETS.
HAAS
WHY WOULD I WANT BULLETS FOR NETWORK SECURITY?
IT'S A SAYING.
IT MEANS THERE'S NO PERFECT SOLUTION.

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

Active Defense in Practice

Operator training includes recognizing indicators, events, or controls available when determining or responding to cyber threats.

When the mouse moves without your control, do you have a procedure to help an operator respond correctly?

At what point does the IT security team call the OT engineering teams when the IT team detects cyber anomalies?

When is the last time we exercised one of our resilience strategies?

Image Source: https://www.saskwind.ca/power-and-renewables/system-operators/

Interdependency Evaluation

KEY QUESTION

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

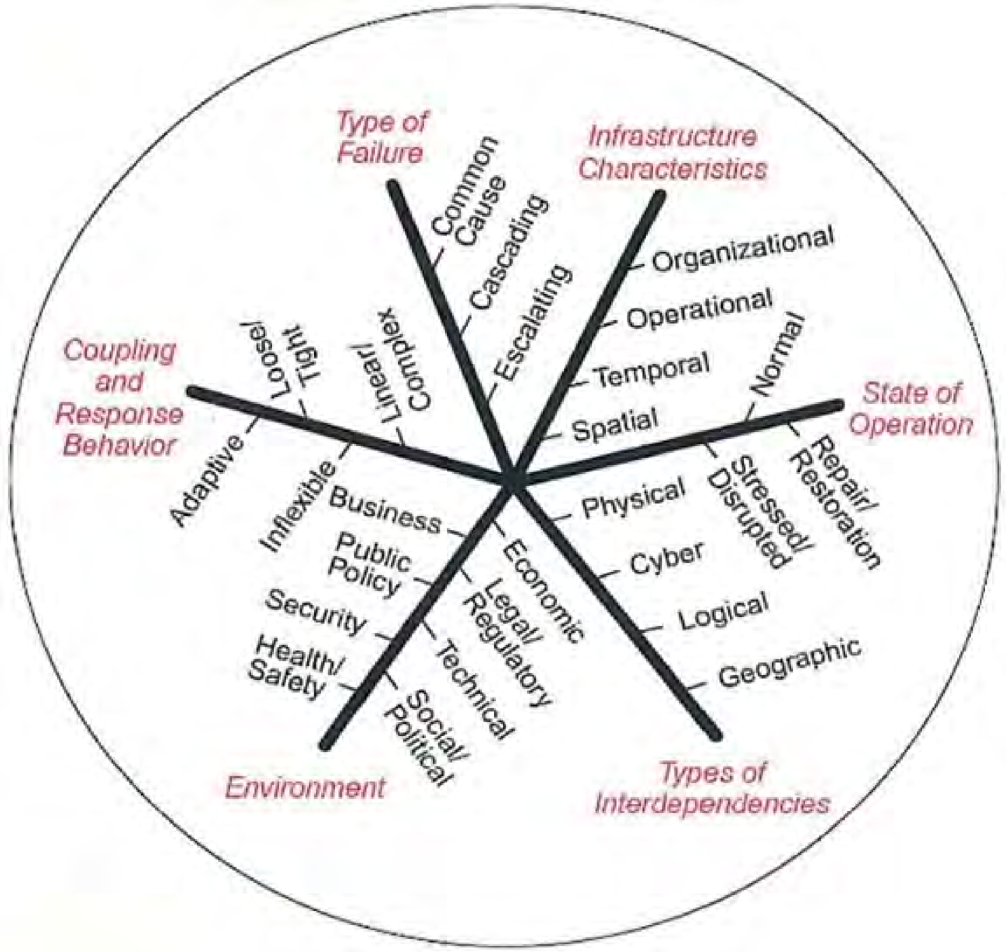


Image adapted from:
http://witandwisdomofanengineer.blogspot.com/2010/11/infrastructure-interdependencies.html

Interdependency Evaluation in Practice

Microgrid installations often have multiple energy sources (BESS, PV, Wind, Synchronous Generators like Propane, etc.).

Given a digital manipulation, could certain energy sources be used against others to create an unacceptable consequence?

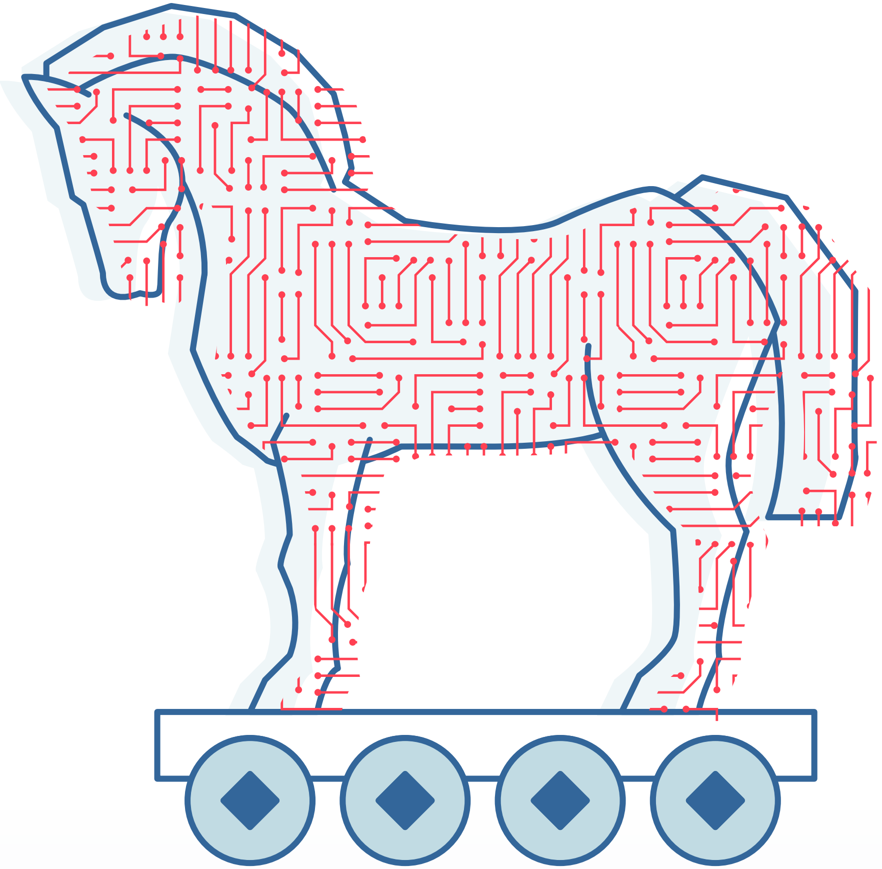
Image Source: https://powersecure.com/customer-solutions/our-solutions/basic-microgrid/

Digital Asset Awareness

KEY QUESTION

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

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



Digital Asset Awareness in Practice

Given the push to modernization, most control and protection devices are providing digitally-delivered functionality.

How could a cyber attack impact critical controls and protections?

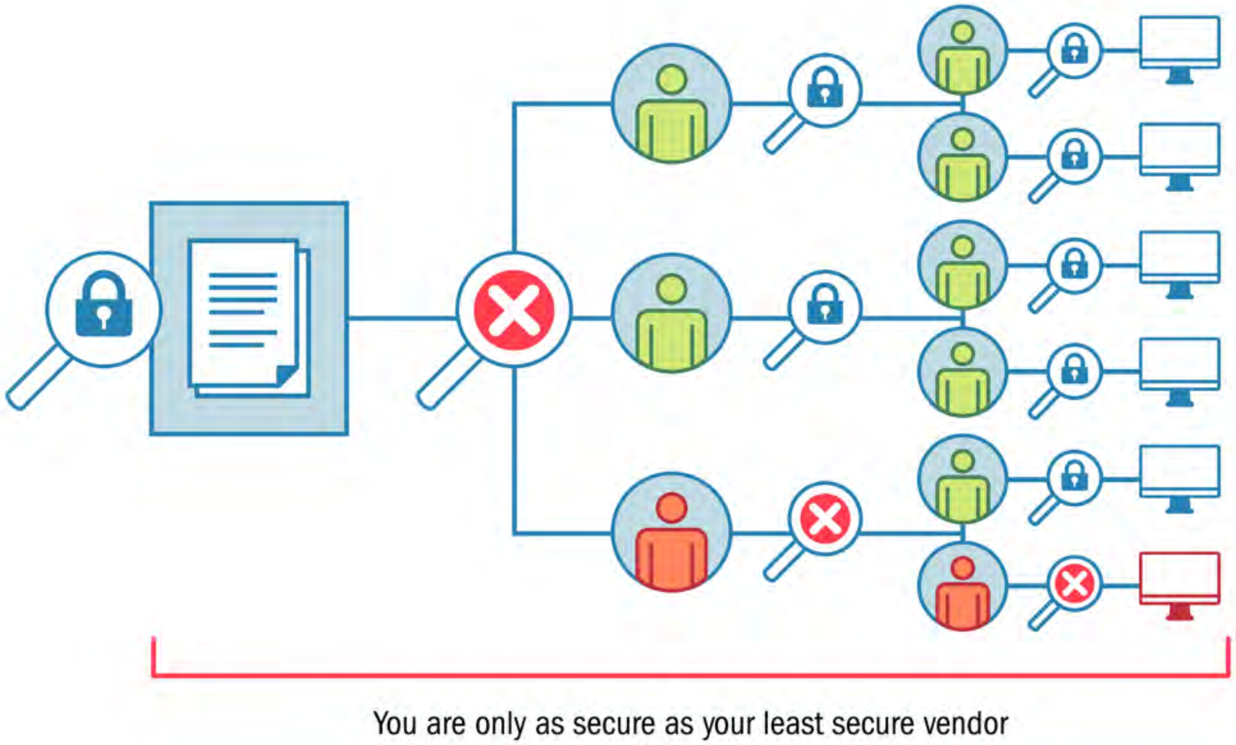
Image Source: https://electrical-engineering-portal.com/download-center/books-and-guides/relays/overcurrent-differential-protection

Cyber-Secure Supply Chain Controls

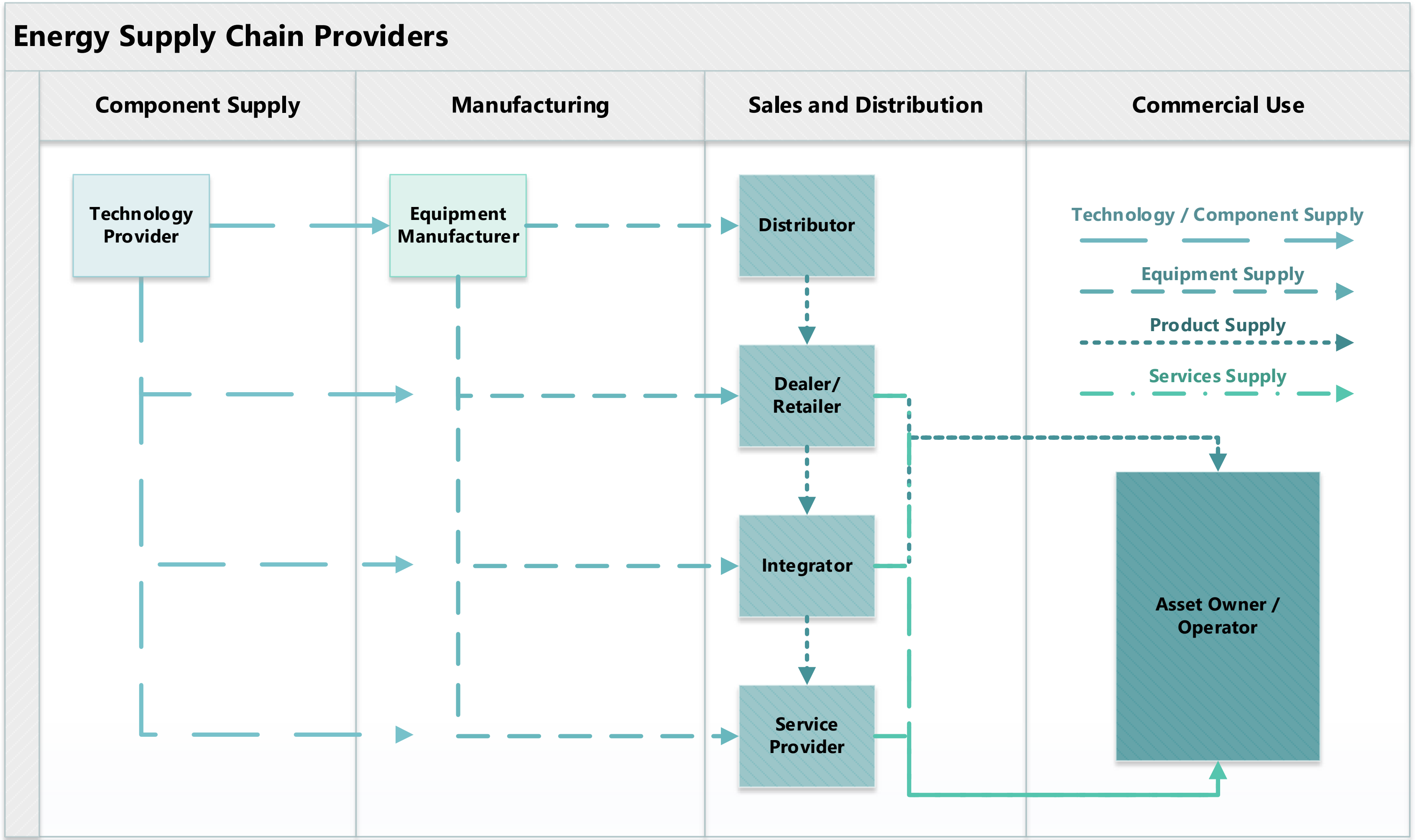
KEY QUESTION

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

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


You are only as secure as your least secure vendor

Cyber-Secure Supply Chain Controls in Practice



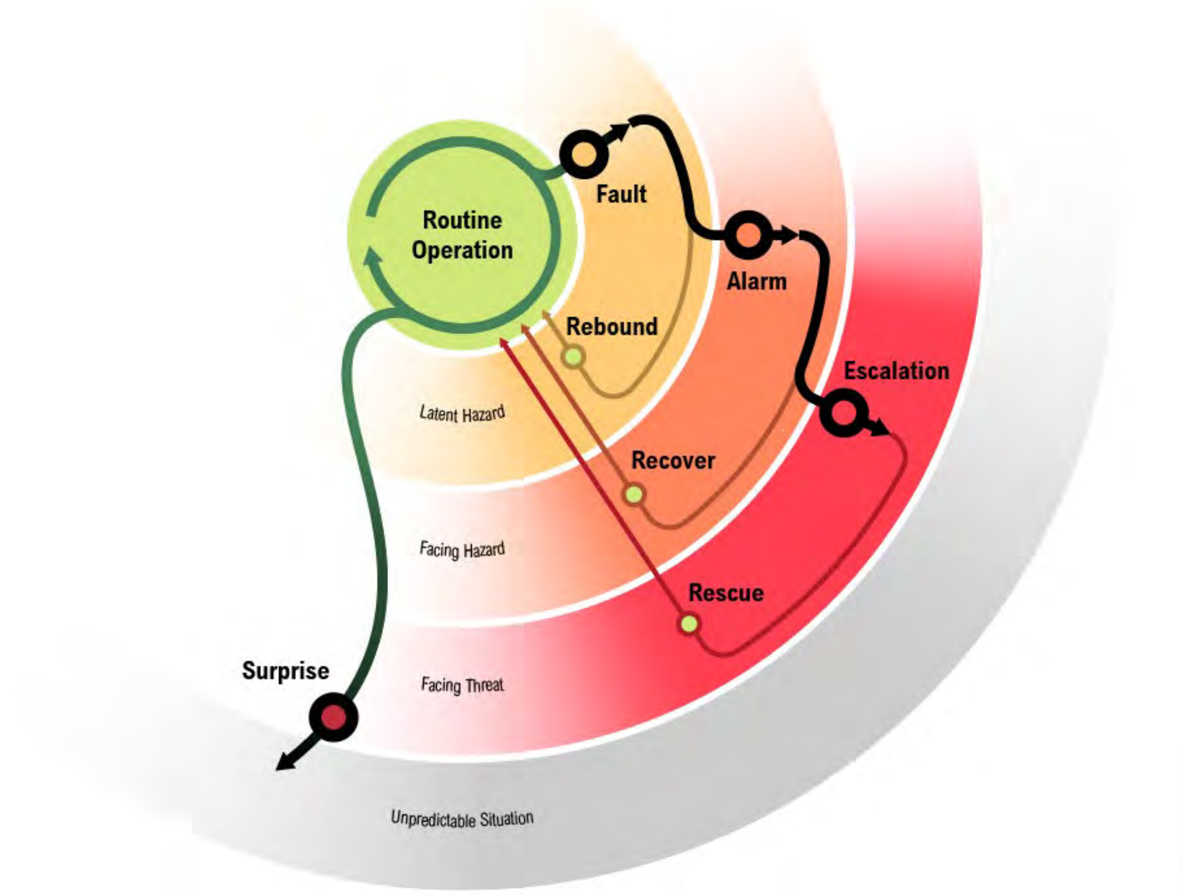
Adapted from https://www.sciencedirect.com/science/article/pii/S1364032117312844#f0010

Planned Resilience

KEY QUESTION

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

- What are the limits of acceptable degradation for critical system functions and what alternate operating modes would protect and maintain those critical system functions within acceptable limits?
- How does the organization maintain business continuity and critical function delivery through incident response and recovery?
- How will resilience measures be validated?



Cyber-Informed Engineering

Planned Resilience in Practice

Day Without Automation (DWOA) Tabletop Exercise & System Design

- ✓People
- ✓Process
- ✓Technology

Image Source: https://www.dreamstime.com/analog-control-room-controlling-machines-working-processes-image221149932

Engineering Information Control

KEY QUESTION

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

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

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

Engineering Information Control in Practice

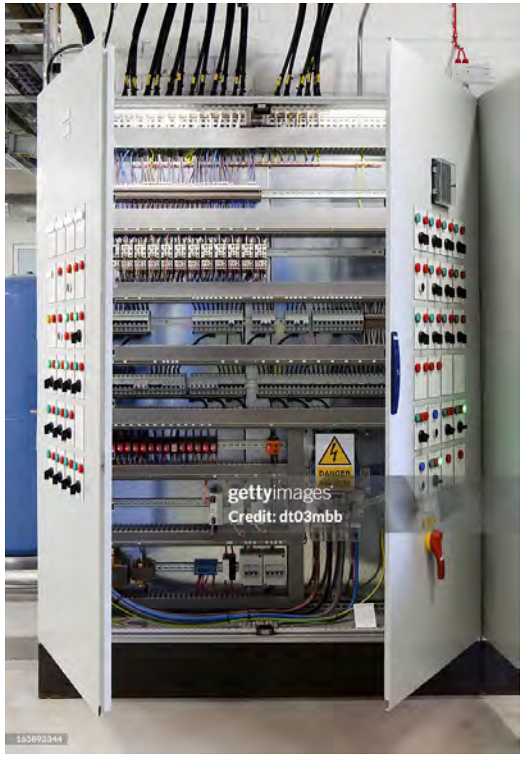
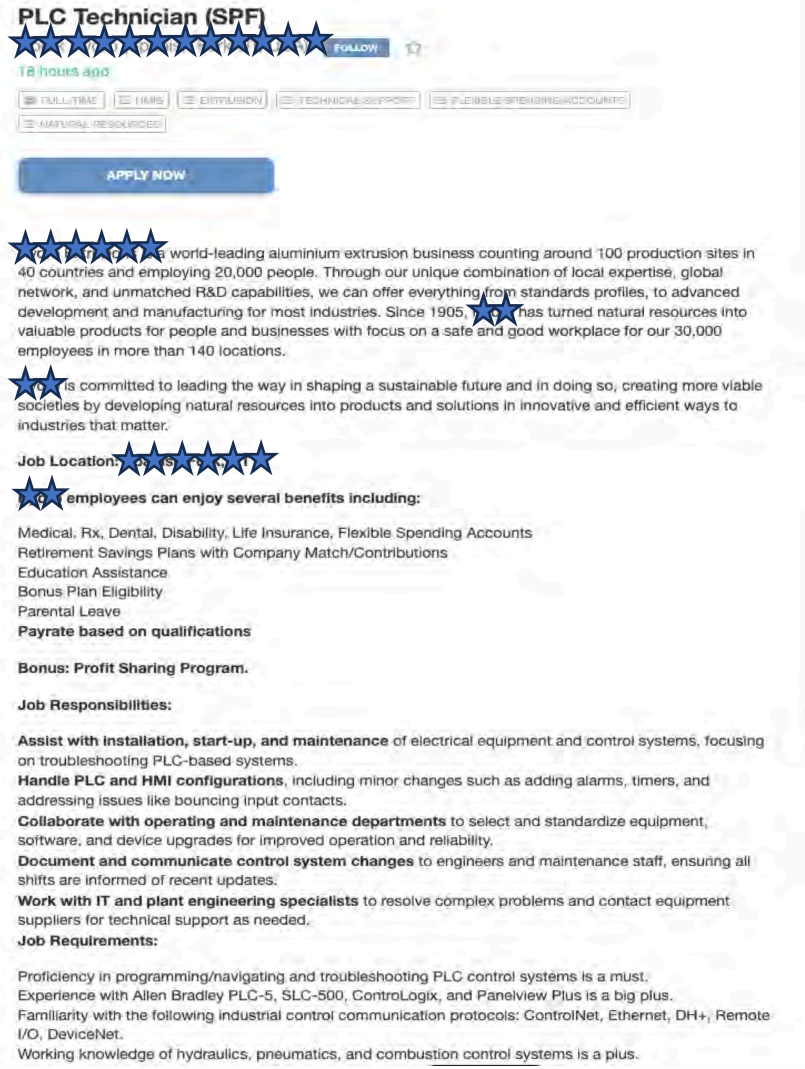


Image Source: https://www.gettyimages.com/detail/photo/systems-control-cabinet-royalty-free-image/165893344



PLC Technician (SPF)

[redacted]

18 hours ago

[redacted] a world-leading aluminium extrusion business counting around 100 production sites in 40 countries and employing 20,000 people. Through our unique combination of local expertise, global network, and unmatched R&D capabilities, we can offer everything from standards profiles, to advanced development and manufacturing for most industries. Since 1905, [redacted] has turned natural resources into valuable products for people and businesses with focus on a safe and good workplace for our 30,000 employees in more than 140 locations.

[redacted] is committed to leading the way in shaping a sustainable future and in doing so, creating more viable societies by developing natural resources into products and solutions in innovative and efficient ways to industries that matter.

Job Location: [redacted]

[redacted] **employees can enjoy several benefits including:**

Medical, Rx, Dental, Disability, Life Insurance, Flexible Spending Accounts
Retirement Savings Plans with Company Match/Contributions
Education Assistance
Bonus Plan Eligibility
Parental Leave
Payrate based on qualifications

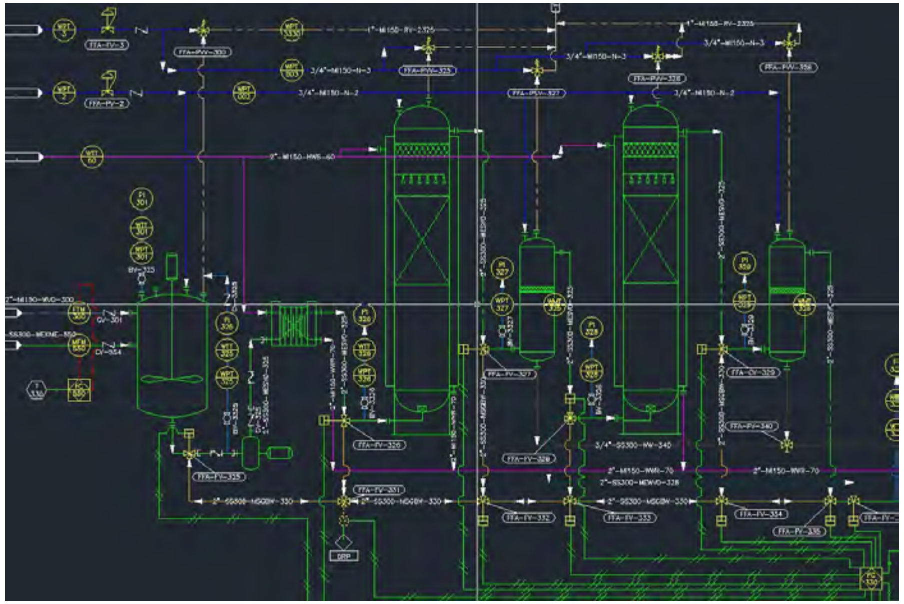
Bonus: Profit Sharing Program.

Job Responsibilities:

Assist with installation, start-up, and maintenance of electrical equipment and control systems, focusing on troubleshooting PLC-based systems.
Handle PLC and HMI configurations, including minor changes such as adding alarms, timers, and addressing issues like bouncing input contacts.
Collaborate with operating and maintenance departments to select and standardize equipment, software, and device upgrades for improved operation and reliability.
Document and communicate control system changes to engineers and maintenance staff, ensuring all shifts are informed of recent updates.
Work with IT and plant engineering specialists to resolve complex problems and contact equipment suppliers for technical support as needed.
Job Requirements:

Proficiency in programming/navigating and troubleshooting PLC control systems is a must.
Experience with Allen Bradley PLC-5, SLC-500, ControLogix, and Panelview Plus is a big plus.
Familiarity with the following industrial control communication protocols: ControlNet, Ethernet, DH+, Remote I/O, DeviceNet.
Working knowledge of hydraulics, pneumatics, and combustion control systems is a plus.

Image Source:
https://www.recruit.net/job/plc-technician-spf--jobs/E193F6688698F576?utm_campaign=google_jobs_apply&utm_source=google_jobs_apply&utm_medium=organic



https://jefersoncosta.com/what-is-pid-piping-and-instrumentation-diagram-or-process-and-instrumentation-diagram/

Organizational Culture

KEY QUESTION

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

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

Conversations

Explicit Assumptions

Collaboration on Projects

Assessments

Scenarios

Exercises

Organizational Culture in Practice

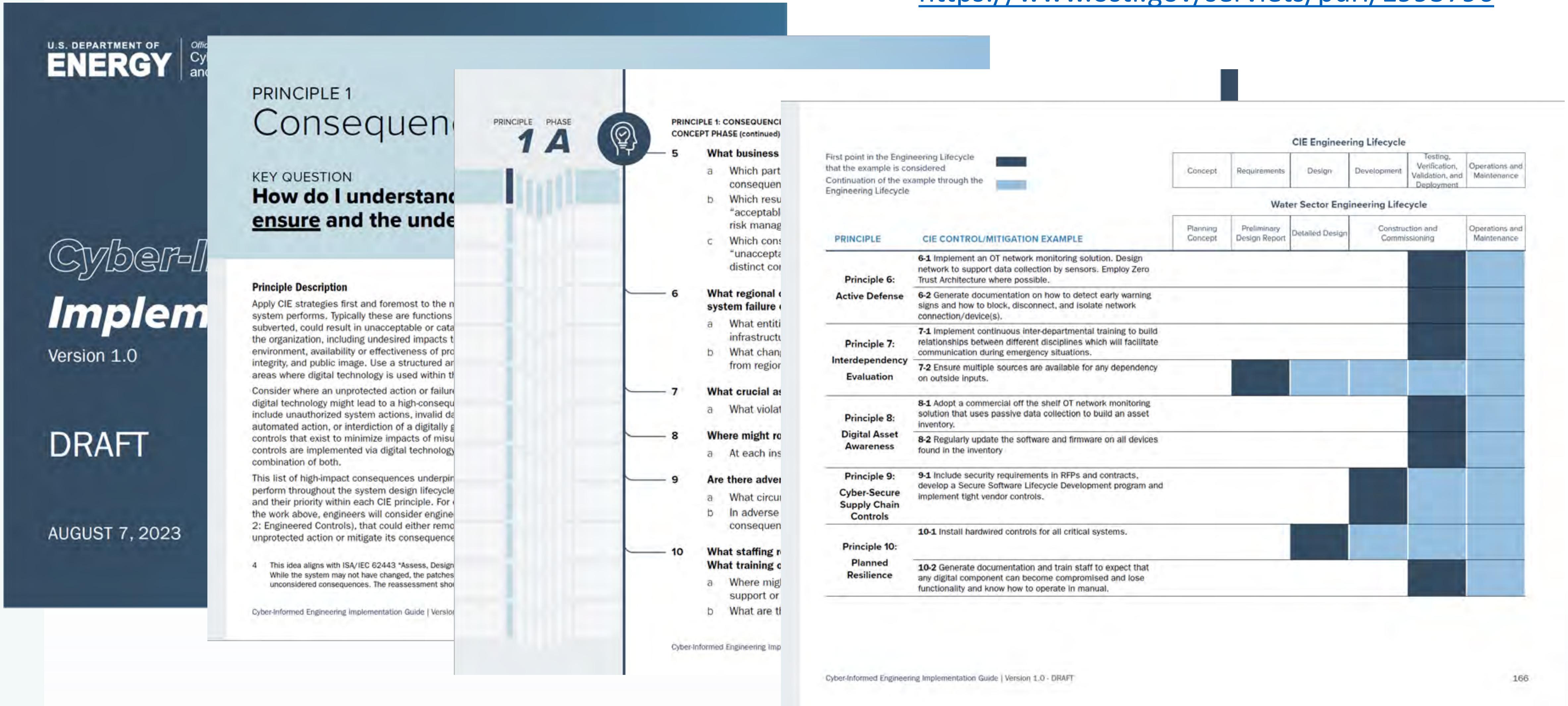
Image Source: https://www.trustntm.com/how-to-create-a-culture-of-cybersecurity-in-your-organization/

- For example, are employees rewarded for speaking up about cybersecurity?
- Do all people and stakeholders involved in the project have the same worldview when it comes to system security?

So Where from here with CIE?

CIE Implementation Guide

https://www.osti.gov/servlets/purl/1995796



U.S. DEPARTMENT OF ENERGY | Offi Cy an

Cyber-I

Implem

Version 1.0

DRAFT

AUGUST 7, 2023

PRINCIPLE 1

Consequen

KEY QUESTION

How do I understand ensure and the unde

Principle Description

Apply CIE strategies first and foremost to the m system performs. Typically these are functions subverted, could result in unacceptable or cata the organization, including undesired impacts t environment, availability or effectiveness of pro integrity, and public image. Use a structured ar areas where digital technology is used within th

Consider where an unprotected action or failure digital technology might lead to a high-consequ include unauthorized system actions, invalid da automated action, or interdiction of a digitally g controls that exist to minimize impacts of misu controls are implemented via digital technology combination of both.

This list of high-impact consequences underpin perform throughout the system design lifecycle and their priority within each CIE principle. For the work above, engineers will consider engine 2: Engineered Controls), that could either remo unprotected action or mitigate its consequence

4 This idea aligns with ISA/IEC 62443 "Assess, Design While the system may not have changed, the patches unconsidered consequences. The reassessment sho

Cyber-Informed Engineering Implementation Guide | Versio

PRINCIPLE 1 A PHASE

PRINCIPLE 1: CONSEQUENC CONCEPT PHASE (continued)

5 **What business**

a Which part consequen

b Which resu "acceptabl risk manag

c Which cons "unaccepta distinct cor

6 **What regional system failure**

a What entiti infrastructu

b What chan from region

7 **What crucial as**

a What violat

8 **Where might ro**

a At each ins

9 **Are there adver**

a What circu

b In adverse consequen

10 **What staffing r What training c**

a Where migh support or

b What are th

Cyber-Informed Engineering Imp

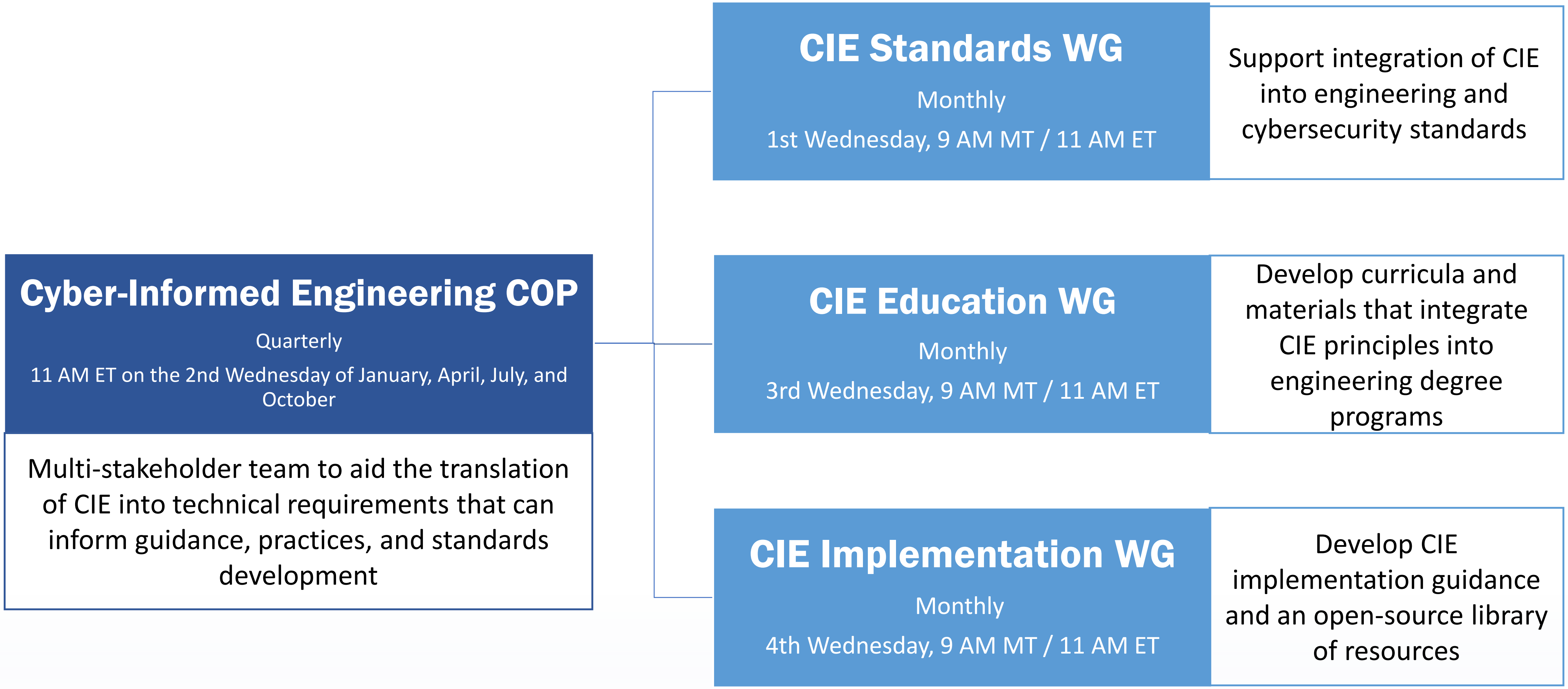
First point in the Engineering Lifecycle that the example is considered ■

Continuation of the example through the Engineering Lifecycle ▨

PRINCIPLE	CIE CONTROL/MITIGATION EXAMPLE	CIE Engineering Lifecycle					
		Concept	Requirements	Design	Development	Testing, Verification, Validation, and Deployment	Operations and Maintenance
		Water Sector Engineering Lifecycle					
		Planning Concept	Preliminary Design Report	Detailed Design	Construction and Commissioning		Operations and Maintenance
Principle 6: Active Defense	**6-1** Implement an OT network monitoring solution. Design network to support data collection by sensors. Employ Zero Trust Architecture where possible.					■	▨
	6-2 Generate documentation on how to detect early warning signs and how to block, disconnect, and isolate network connection/device(s).					■	▨
Principle 7: Interdependency Evaluation	**7-1** Implement continuous inter-departmental training to build relationships between different disciplines which will facilitate communication during emergency situations.					■	▨
	7-2 Ensure multiple sources are available for any dependency on outside inputs.		■	▨	▨	▨	▨
Principle 8: Digital Asset Awareness	**8-1** Adopt a commercial off the shelf OT network monitoring solution that uses passive data collection to build an asset inventory.					■	▨
	8-2 Regularly update the software and firmware on all devices found in the inventory					■	▨
Principle 9: Cyber-Secure Supply Chain Controls	**9-1** Include security requirements in RFPs and contracts, develop a Secure Software Lifecycle Development program and implement tight vendor controls.				■	▨	▨
Principle 10: Planned Resilience	**10-1** Install hardwired controls for all critical systems.			■	▨	▨	▨
	10-2 Generate documentation and train staff to expect that any digital component can become compromised and lose functionality and know how to operate in manual.					■	▨

Cyber-Informed Engineering Implementation Guide | Version 1.0 - DRAFT 166

CIE COP and Working Group Purpose



Cyber-Informed Engineering COP

Quarterly

11 AM ET on the 2nd Wednesday of January, April, July, and October

Multi-stakeholder team to aid the translation of CIE into technical requirements that can inform guidance, practices, and standards development

CIE Standards WG

Monthly

1st Wednesday, 9 AM MT / 11 AM ET

Support integration of CIE into engineering and cybersecurity standards

CIE Education WG

Monthly

3rd Wednesday, 9 AM MT / 11 AM ET

Develop curricula and materials that integrate CIE principles into engineering degree programs

CIE Implementation WG

Monthly

4th Wednesday, 9 AM MT / 11 AM ET

Develop CIE implementation guidance and an open-source library of resources

Recent CIE Publications

Websites

- **DOE CESER CIE Website – https://www.energy.gov/ceser/cyber-informed-engineering**
- **INL CIE Website - https://inl.gov/cie/**
- **NREL CIE Website - https://www.nrel.gov/security-resilience/cyber-informed-engineering.html**

Publications

- **CIE Implementation Guide:** https://www.osti.gov/biblio/1995796
- **CIE Workbook for ADMS:** https://www.osti.gov/biblio/1986517
- **CIE Workbook for Microgrids:** https://www.osti.gov/biblio/2315001
- **CIE Workbook for Water Systems:** https://www.osti.gov/biblio/2371031
- **CIE Assessment Tool: https://github.com/inlguy/CIE/releases/tag/v12.2.4.0** **Just Released!**

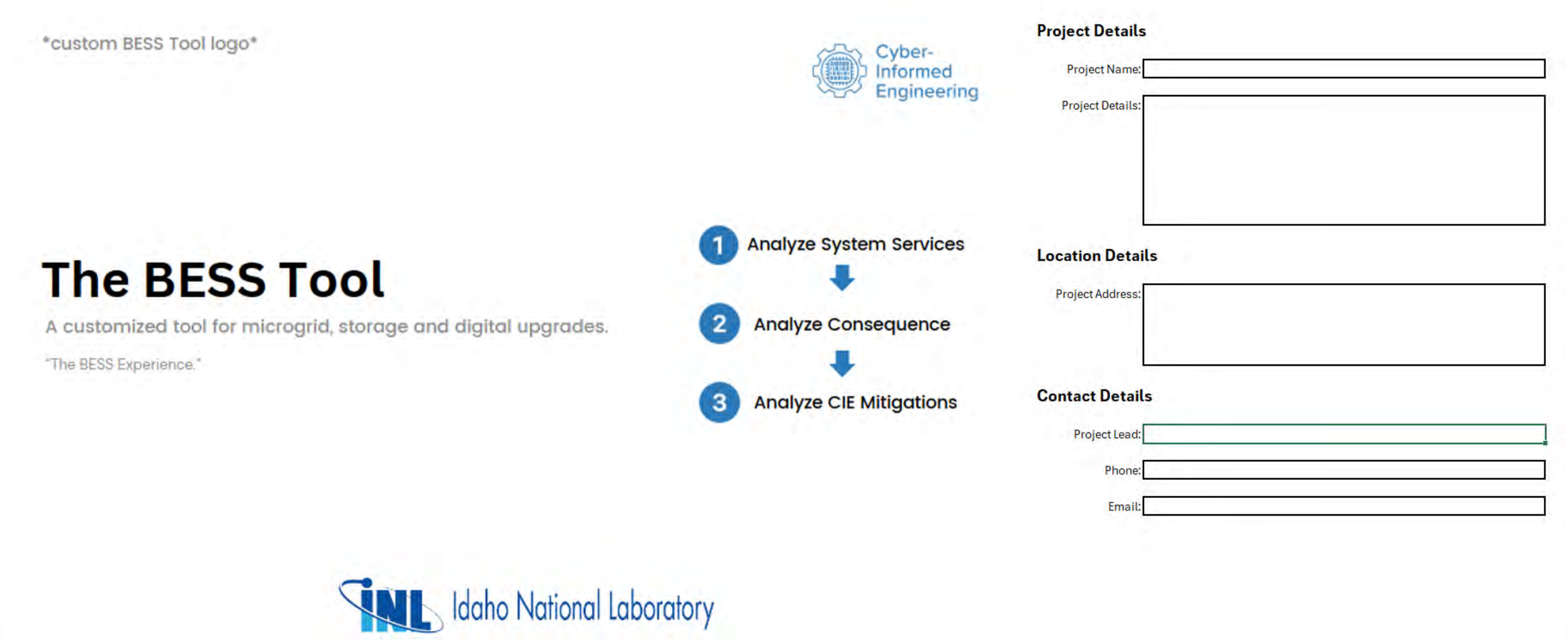
Articles and Briefings

- **SANS ICS Concepts Video:** https://youtu.be/o_vIxW6UTeg
- **Industrial Cyber:** CIE and CCE Methodologies Can Deliver Engineered Industrial Systems for Holistic System Cybersecurity (June 11, 2023) with interviews from INL, 1898, and West Yost
- **Harvard Business Review:** Engineering Cybersecurity into U.S. Critical Infrastructure (April 17, 2023) by Ginger Wright, Andrew Ohrt, and Andy Bochman
- **Shift Left video podcast on GrammaTech blog:** Shifting Left for Energy Security (April 4, 2023) with Ginger Wright, Idaho National Lab and Marc Sachs, Auburn University
- For more CIE articles and publications, visit: inl.gov/cie

Under Development

- **CIRRUS - Tool for leveraging CIE for consideration of OT in the Cloud**
- **CIE Microgrid Tool - Tool for leveraging CIE in the design of microgrids**
- **CIE BESS Tool - Tool for leveraging CIE in the design of BESS installations**
- **Discussions with CISA Secure by Design**

CIE BESS Analysis Tool (CIEBAT)



custom BESS Tool logo

Cyber-Informed Engineering

The BESS Tool

A customized tool for microgrid, storage and digital upgrades.

"The BESS Experience."

1 Analyze System Services

2 Analyze Consequence

3 Analyze CIE Mitigations

Idaho National Laboratory

Project Details

Project Name:

Project Details:

Location Details

Project Address:

Contact Details

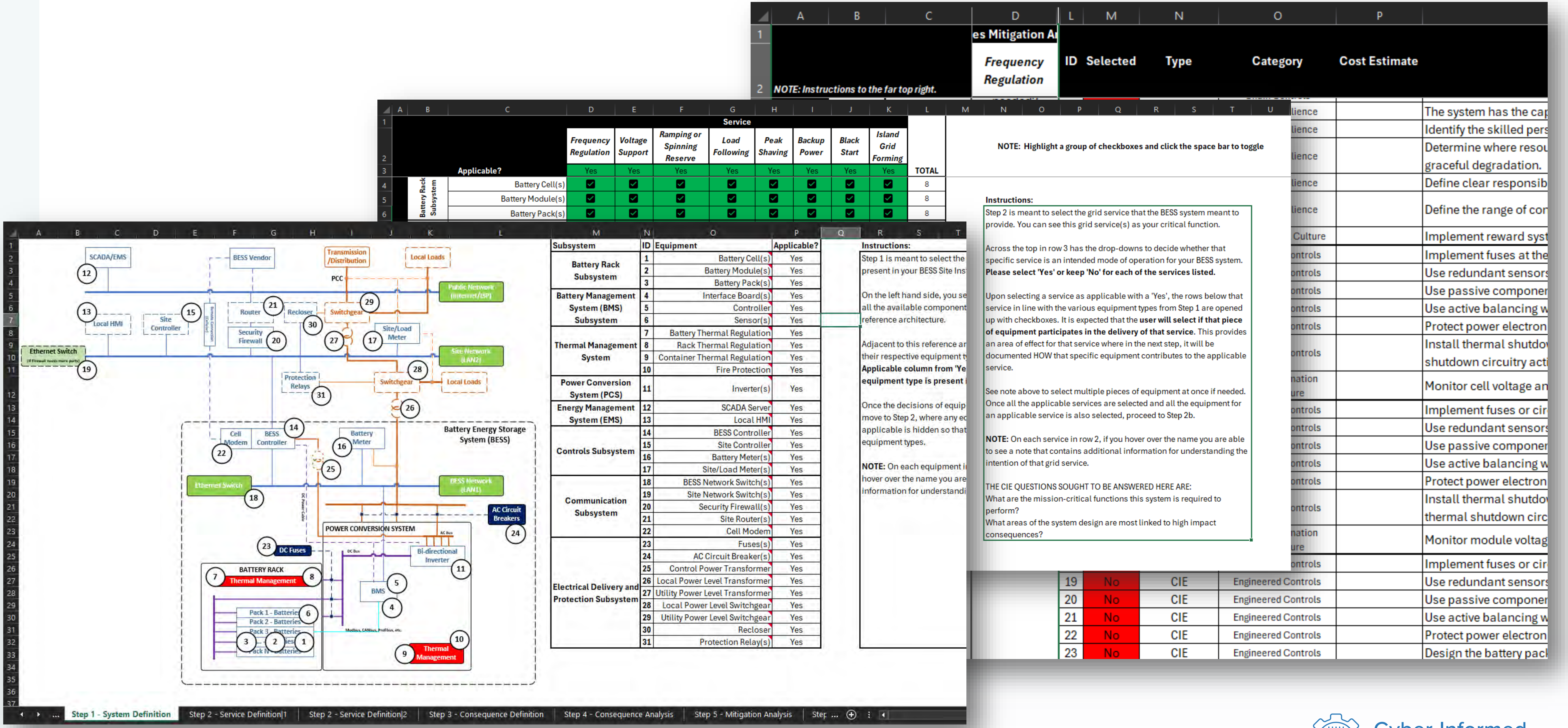
Project Lead:

Phone:

Email:

Cyber-Informed Engineering

CIE BESS Analysis Tool (CIEBAT)



Subsystem	ID	Equipment	Applicable?
Battery Rack Subsystem	1	Battery Cell(s)	Yes
	2	Battery Module(s)	Yes
	3	Battery Pack(s)	Yes
Battery Management System (BMS) Subsystem	4	Interface Board(s)	Yes
	5	Controller	Yes
	6	Sensor(s)	Yes
Thermal Management System	7	Battery Thermal Regulation	Yes
	8	Rack Thermal Regulation	Yes
	9	Container Thermal Regulation	Yes
	10	Fire Protection	Yes
Power Conversion System (PCS)	11	Inverter(s)	Yes
Energy Management System (EMS)	12	SCADA Server	Yes
	13	Local HMI	Yes
Controls Subsystem	14	BESS Controller	Yes
	15	Site Controller	Yes
	16	Battery Meter(s)	Yes
	17	Site/Load Meter(s)	Yes
Communication Subsystem	18	BESS Network Switch(s)	Yes
	19	Site Network Switch(s)	Yes
	20	Security Firewall(s)	Yes
	21	Site Router(s)	Yes
	22	Cell Modem	Yes
Electrical Delivery and Protection Subsystem	23	Fuses(s)	Yes
	24	AC Circuit Breaker(s)	Yes
	25	Control Power Transformer	Yes
	26	Local Power Level Transformer	Yes
	27	Utility Power Level Transformer	Yes
	28	Local Power Level Switchgear	Yes
	29	Utility Power Level Switchgear	Yes
	30	Recloser	Yes
	31	Protection Relay(s)	Yes

Instructions:

Step 1 is meant to select the
present in your BESS Site Ins

On the left hand side, you se
all the available component
reference architecture.

Adjacent to this reference ar
their respective equipment t
Applicable column from 'Ye
equipment type is present i

Once the decisions of equip
move to Step 2, where any ec
applicable is hidden so that
equipment types.

NOTE: On each equipment i
hover over the name you are
information for understandi

		Service								
		Frequency Regulation	*Voltage Support*	*Ramping or Spinning Reserve*	*Load Following*	*Peak Shaving*	*Backup Power*	*Black Start*	*Island Grid Forming*	
	Applicable?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	TOTAL
Battery Rack Subsystem	Battery Cell(s)	☑	☑	☑	☑	☑	☑	☑	☑	8
	Battery Module(s)	☑	☑	☑	☑	☑	☑	☑	☑	8
	Battery Pack(s)	☑	☑	☑	☑	☑	☑	☑	☑	8

NOTE: Highlight a group of checkboxes and click the space bar to toggle

Instructions:

Step 2 is meant to select the grid service that the BESS system meant to provide. You can see this grid service(s) as your critical function.

Across the top in row 3 has the drop-downs to decide whether that specific service is an intended mode of operation for your BESS system. **Please select 'Yes' or keep 'No' for each of the services listed.**

Upon selecting a service as applicable with a 'Yes', the rows below that service in line with the various equipment types from Step 1 are opened up with checkboxes. It is expected that the **user will select if that piece of equipment participates in the delivery of that service.** This provides an area of effect for that service where in the next step, it will be documented HOW that specific equipment contributes to the applicable service.

See note above to select multiple pieces of equipment at once if needed. Once all the applicable services are selected and all the equipment for an applicable service is also selected, proceed to Step 2b.

NOTE: On each service in row 2, if you hover over the name you are able to see a note that contains additional information for understanding the intention of that grid service.

THE CIE QUESTIONS SOUGHT TO BE ANSWERED HERE ARE:
What are the mission-critical functions this system is required to perform?
What areas of the system design are most linked to high impact consequences?

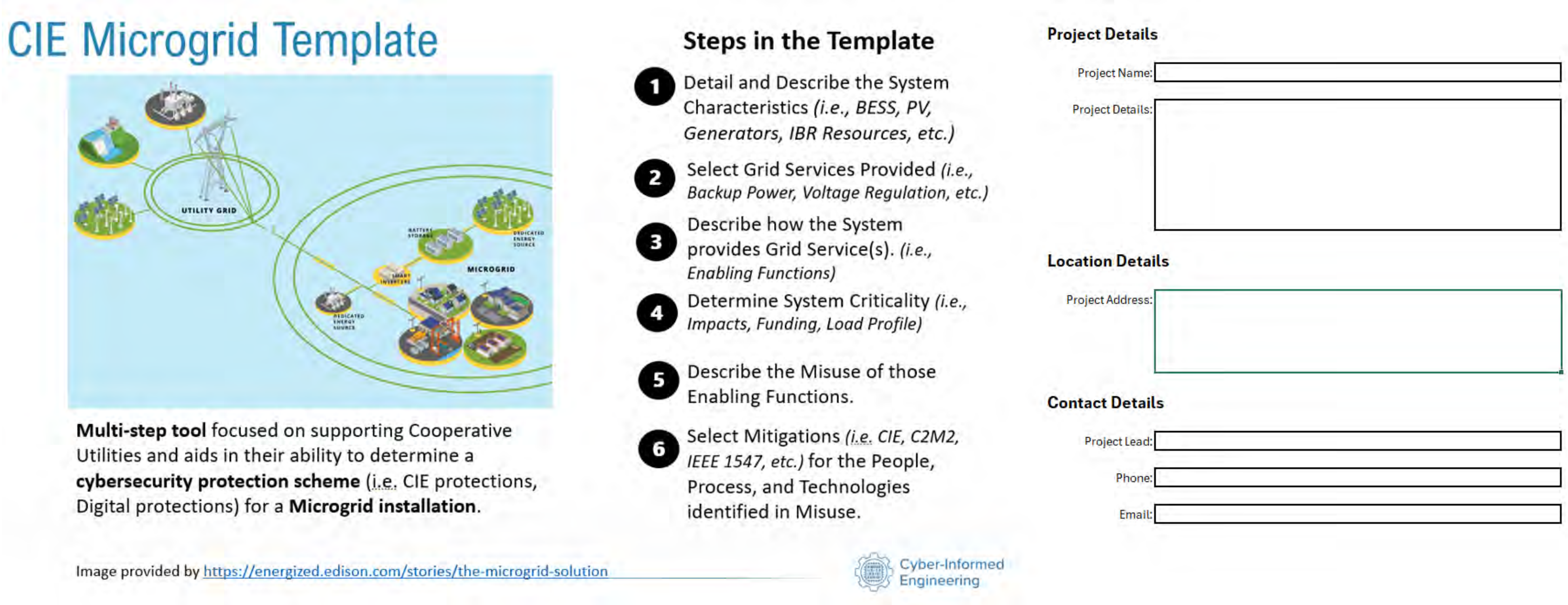
NOTE: Instructions to the far top right.

es Mitigation A

Frequency Regulation

ID	Selected	Type	Category	Cost Estimate	
			lience		The system has the cap
			lience		Identify the skilled pers
			lience		Determine where resou graceful degradation.
			lience		Define clear responsib
			lience		Define the range of cor
			Culture		Implement reward syst
			ontrols		Implement fuses at the
			ontrols		Use redundant sensors
			ontrols		Use passive componer
			ontrols		Use active balancing w
			ontrols		Protect power electron
			ontrols		Install thermal shutdo shutdown circuitry acti
			nation ure		Monitor cell voltage an
			ontrols		Implement fuses or cir
			ontrols		Use redundant sensors
			ontrols		Use passive componer
			ontrols		Use active balancing w
			ontrols		Protect power electron
			ontrols		Install thermal shutdo thermal shutdown circ
			nation ure		Monitor module voltag
			ontrols		Implement fuses or cir
19	No	CIE	Engineered Controls		Use redundant sensors
20	No	CIE	Engineered Controls		Use passive componer
21	No	CIE	Engineered Controls		Use active balancing w
22	No	CIE	Engineered Controls		Protect power electron
23	No	CIE	Engineered Controls		Design the battery pacl

CIE Microgrid Analysis Tool (CIEMAT)



CIE Microgrid Template

Multi-step tool focused on supporting Cooperative Utilities and aids in their ability to determine a **cybersecurity protection scheme** (i.e. CIE protections, Digital protections) for a **Microgrid installation**.

Image provided by https://energized.edison.com/stories/the-microgrid-solution

Steps in the Template

1. Detail and Describe the System Characteristics *(i.e., BESS, PV, Generators, IBR Resources, etc.)*
2. Select Grid Services Provided *(i.e., Backup Power, Voltage Regulation, etc.)*
3. Describe how the System provides Grid Service(s). *(i.e., Enabling Functions)*
4. Determine System Criticality *(i.e., Impacts, Funding, Load Profile)*
5. Describe the Misuse of those Enabling Functions.
6. Select Mitigations *(i.e. CIE, C2M2, IEEE 1547, etc.)* for the People, Process, and Technologies identified in Misuse.

Cyber-Informed Engineering

Project Details

Project Name:

Project Details:

Location Details

Project Address:

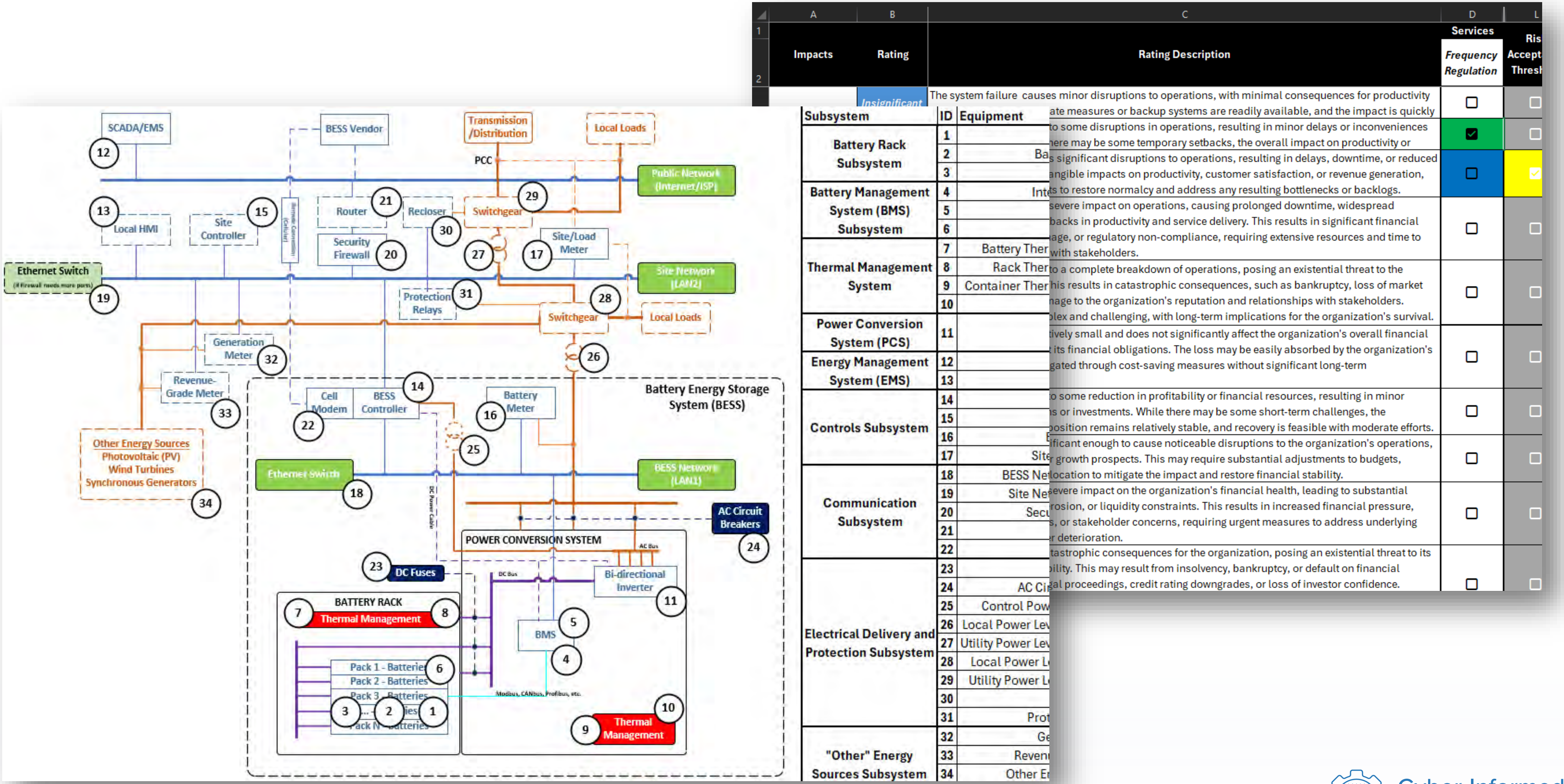
Contact Details

Project Lead:

Phone:

Email:

CIE Microgrid Analysis Tool (CIEMAT)



A Impacts	B Rating	C Rating Description	D Services *Frequency Regulation*	L Ris Accept Thresh
	Insignificant	The system failure causes minor disruptions to operations, with minimal consequences for productivity ate measures or backup systems are readily available, and the impact is quickly	□	□
		to some disruptions in operations, resulting in minor delays or inconveniences here may be some temporary setbacks, the overall impact on productivity or	☑	□
		s significant disruptions to operations, resulting in delays, downtime, or reduced angible impacts on productivity, customer satisfaction, or revenue generation, ts to restore normalcy and address any resulting bottlenecks or backlogs.	□	✓
		severe impact on operations, causing prolonged downtime, widespread backs in productivity and service delivery. This results in significant financial age, or regulatory non-compliance, requiring extensive resources and time to with stakeholders.	□	□
		to a complete breakdown of operations, posing an existential threat to the his results in catastrophic consequences, such as bankruptcy, loss of market nage to the organization's reputation and relationships with stakeholders. plex and challenging, with long-term implications for the organization's survival.	□	□
		tively small and does not significantly affect the organization's overall financial its financial obligations. The loss may be easily absorbed by the organization's gated through cost-saving measures without significant long-term	□	□
		o some reduction in profitability or financial resources, resulting in minor s or investments. While there may be some short-term challenges, the position remains relatively stable, and recovery is feasible with moderate efforts.	□	□
		ificant enough to cause noticeable disruptions to the organization's operations, r growth prospects. This may require substantial adjustments to budgets, location to mitigate the impact and restore financial stability.	□	□
		severe impact on the organization's financial health, leading to substantial rosion, or liquidity constraints. This results in increased financial pressure, s, or stakeholder concerns, requiring urgent measures to address underlying r deterioration.	□	□
		tastrophic consequences for the organization, posing an existential threat to its bility. This may result from insolvency, bankruptcy, or default on financial gal proceedings, credit rating downgrades, or loss of investor confidence.	□	□

Subsystem	ID	Equipment
Battery Rack Subsystem	1	
	2	Ba
	3	
Battery Management System (BMS) Subsystem	4	Inte
	5	
	6	
Thermal Management System	7	Battery Ther
	8	Rack Ther
	9	Container Ther
	10	
Power Conversion System (PCS)	11	
Energy Management System (EMS)	12	
	13	
Controls Subsystem	14	
	15	
	16	E
	17	Site
Communication Subsystem	18	BESS Ne
	19	Site Ne
	20	Secu
	21	
	22	
Electrical Delivery and Protection Subsystem	23	
	24	AC Ci
	25	Control Pow
	26	Local Power Lev
	27	Utility Power Lev
	28	Local Power L
	29	Utility Power L
	30	
	31	Prot
"Other" Energy Sources Subsystem	32	Ge
	33	Reven
	34	Other E

Thank You!

CIE@inl.gov

https://www.energy.gov/ceser/cyber-informed-engineering