Cybersecurity and Infrastructure Sensing

University of Pittsburgh Infrastructure Sensing Collaboration (UPISC)

Workshop 2024

Nov 12 + 13 2024

Emma M Stewart

Chief Power Grid Scientist

Director – Center for Securing Digital Energy Future

National and Homeland Security

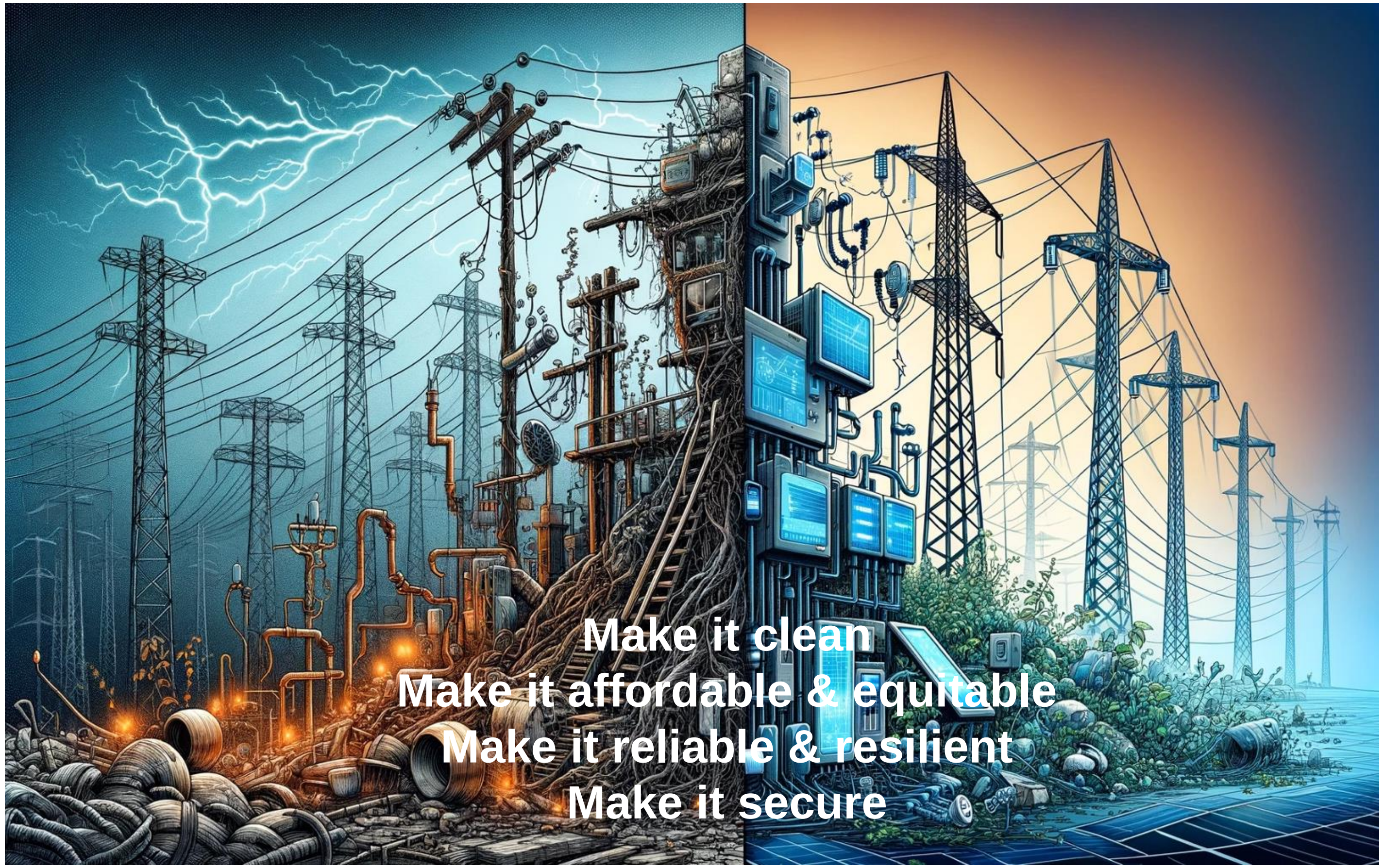
Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory

INL/MIS-24-81986

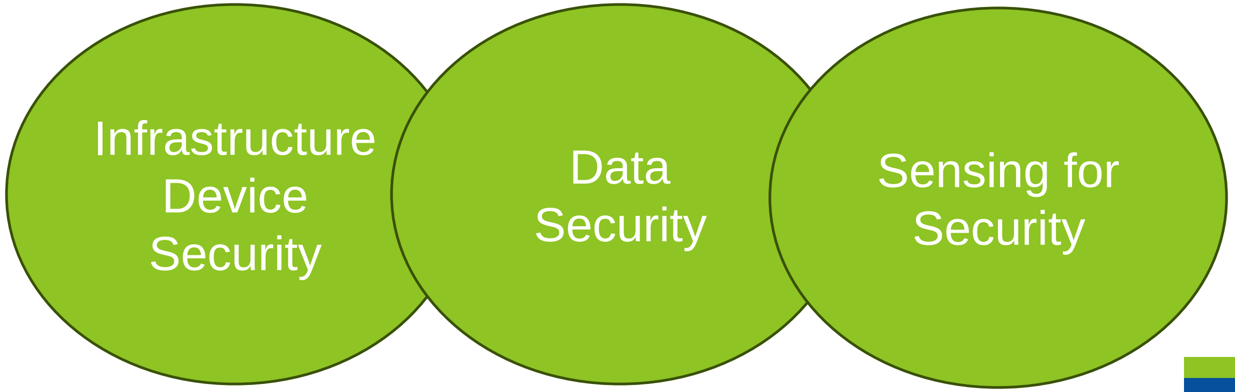
Introduction – Digital Transformation, Cybersecurity and Infrastructure Sensing

- Industry 4.0 = Analog to digital
- More: Power, Reliability, Expectations, Independence, Choice, Complication
- Large Spinning Machines become Solid State Devices, Distributed Controls, Devices, Data and Communications
- Cybersecurity & Infrastructure Sensing
  - Both a need and a risk

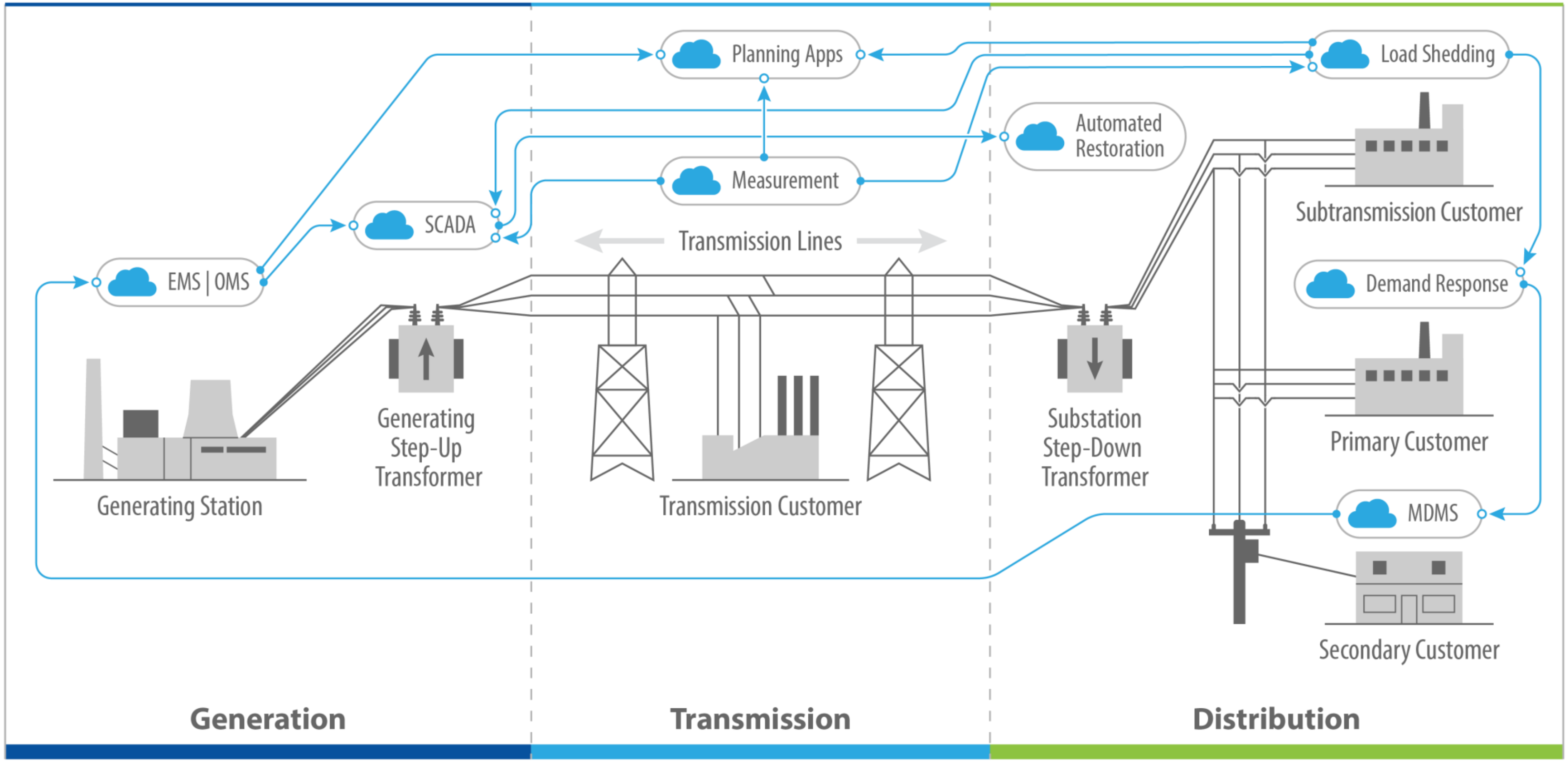


Trends in Digital Energy Ecosystem: Sensing and Cybersecurity

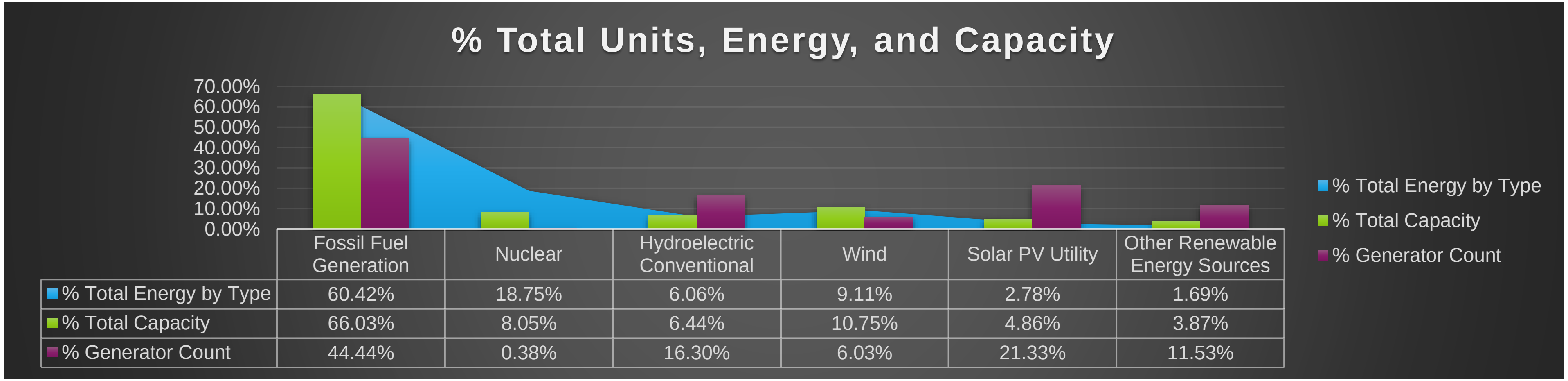
Changes in Digital Energy		Impact to cybersecurity
Growth of stakeholders	→	Increase in attack surface
Growth of endpoints	→	Increase in attack surface, vulnerabilities
Aggregation of data	→	Increase in potential physical risk & impact
Digitization of monitoring	→	Explosion of data to process and store
Digitization of control	→	Need for resilience of critical functionality
Distribution of control	→	Management of roles and privileges
Smarter communications	→	Increase in attack surface



Trends: Interconnected Interdependent Cloud Everywhere

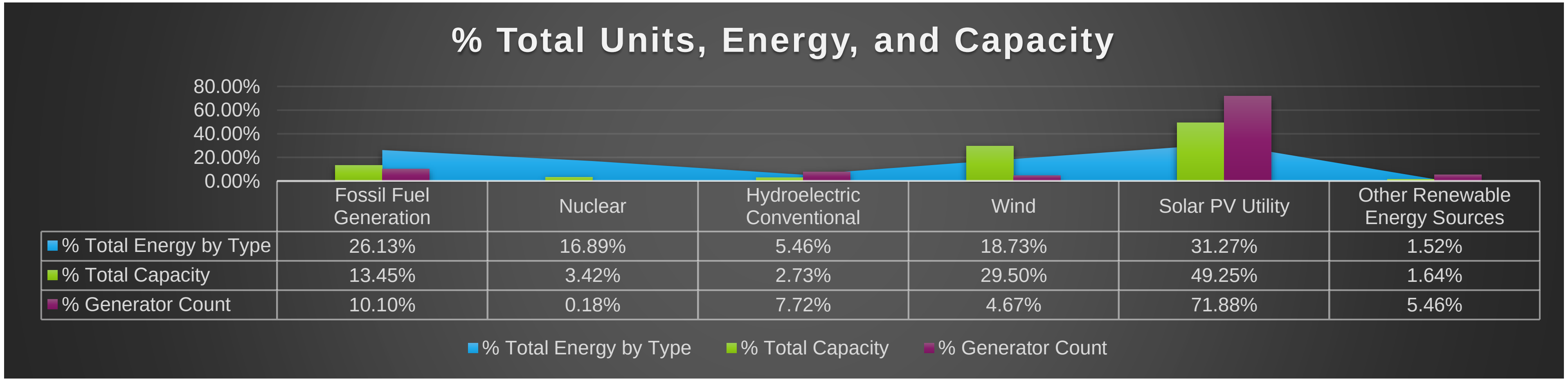


Increase in Capacity and Devices = Increase in sensing and measurement = increase in attack surface



	Fossil Fuel Generation	Nuclear	Hydroelectric Conventional	Wind	Solar PV Utility	Other Renewable Energy Sources
% Total Energy by Type	60.42%	18.75%	6.06%	9.11%	2.78%	1.69%
% Total Capacity	66.03%	8.05%	6.44%	10.75%	4.86%	3.87%
% Generator Count	44.44%	0.38%	16.30%	6.03%	21.33%	11.53%

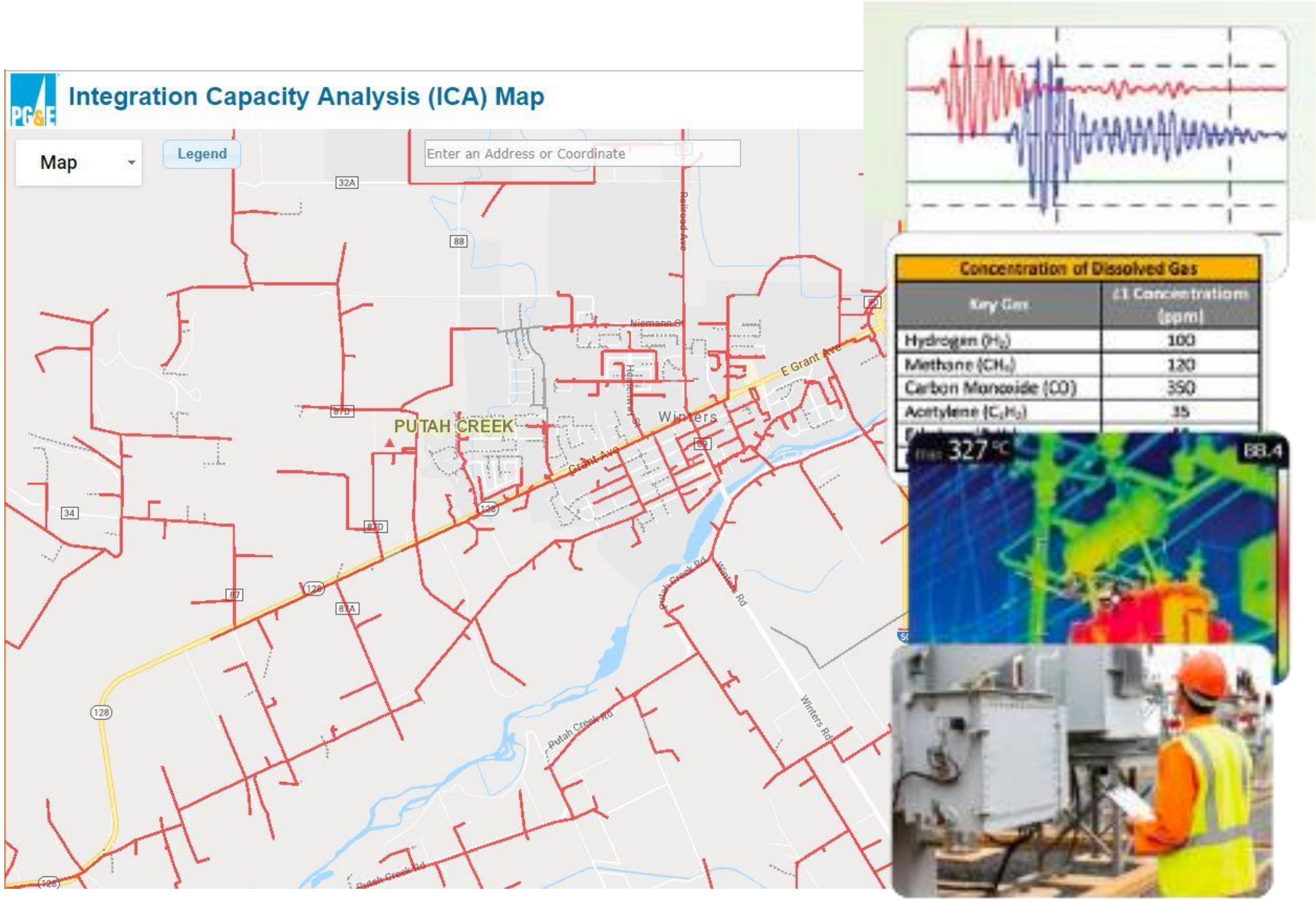
2021



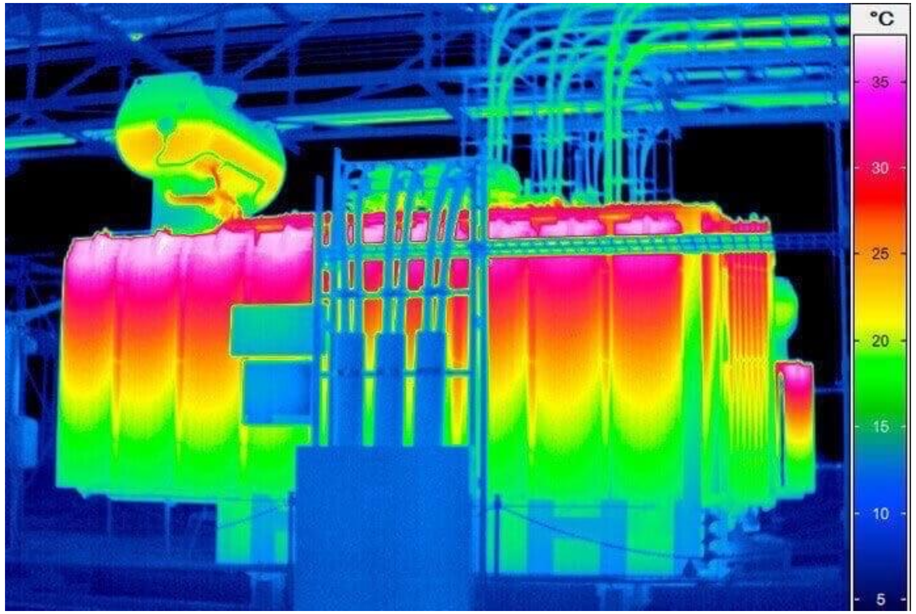
	Fossil Fuel Generation	Nuclear	Hydroelectric Conventional	Wind	Solar PV Utility	Other Renewable Energy Sources
% Total Energy by Type	26.13%	16.89%	5.46%	18.73%	31.27%	1.52%
% Total Capacity	13.45%	3.42%	2.73%	29.50%	49.25%	1.64%
% Generator Count	10.10%	0.18%	7.72%	4.67%	71.88%	5.46%

2030

Sensors and the Electric Grid: Data is Queen… and there is a lot of it available



Concentration of Dissolved Gas	
Key Gas	L1 Concentration (ppm)
Hydrogen (H_2)	100
Methane (CH_4)	120
Carbon Monoxide (CO)	350
Acetylene (C_2H_2)	35



Cybersecurity and Sensing: Introduction

- Electric Grid sensors & IoT
  - Internet of Things (IoT) sensors are smart devices that collect and transmit data in real time. They are used in many fields, including automotive, healthcare, and energy.
- Sensor cybersecurity
  - Early detection: Monitoring sensor behavior can help detect human error and sensor failures early. This can save money and ensure process consistency.
- Network sensors
  - A key tool in cybersecurity, network sensors monitor network traffic and detect threats. They can be physical devices or virtual images, and can monitor both physical and virtual environments. Network sensors can identify applications, monitor response times, and aggregate logs. They can also help with traffic analysis.

Sensing Matters: Example Incidents and Events

- Security of IoT devices: IoT sensors are vulnerable to cyberattacks, and sensor cybersecurity is essential to prevent them.
- Process Sensing and Cyber: incidents
  - IoT sensors failed to turn on a ventilation system, leading to the deaths of nearly 30,000 chickens
  - Blue Cut Fire & Inverter Sensing leading to 1200MW outage
  - FROSTY GOOP – Malware impacting temperature sensing for district heating

CYBERSCOOP Topics Special Reports Events Podcasts Videos

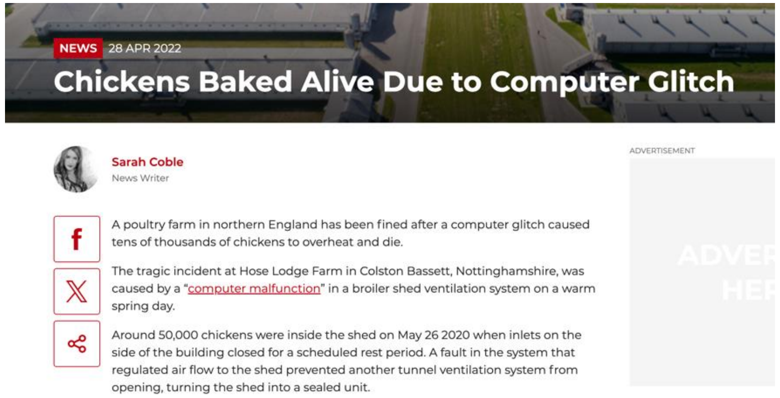
Simple 'FrostyGoop' malware responsible for turning off Ukrainians' heat in January attack

The attack is the latest in a string targeting Ukrainian critical infrastructure and illustrates the growing ease of targeting industrial systems.

BY CHRISTIAN VASQUEZ • JULY 23, 2024

Figure 1.1: Map of the Affected Area and Blue Cut Fire Location

By the end of the day, the SCE transmission system experienced thirteen 500 kV line faults and the LADWP system experienced two 287 kV faults as a result of the fire. Four of these fault events resulted in the loss of a significant amount of solar PV generation.



NEWS 28 APR 2022

Chickens Baked Alive Due to Computer Glitch

Sarah Coble
News Writer

A poultry farm in northern England has been fined after a computer glitch caused tens of thousands of chickens to overheat and die.

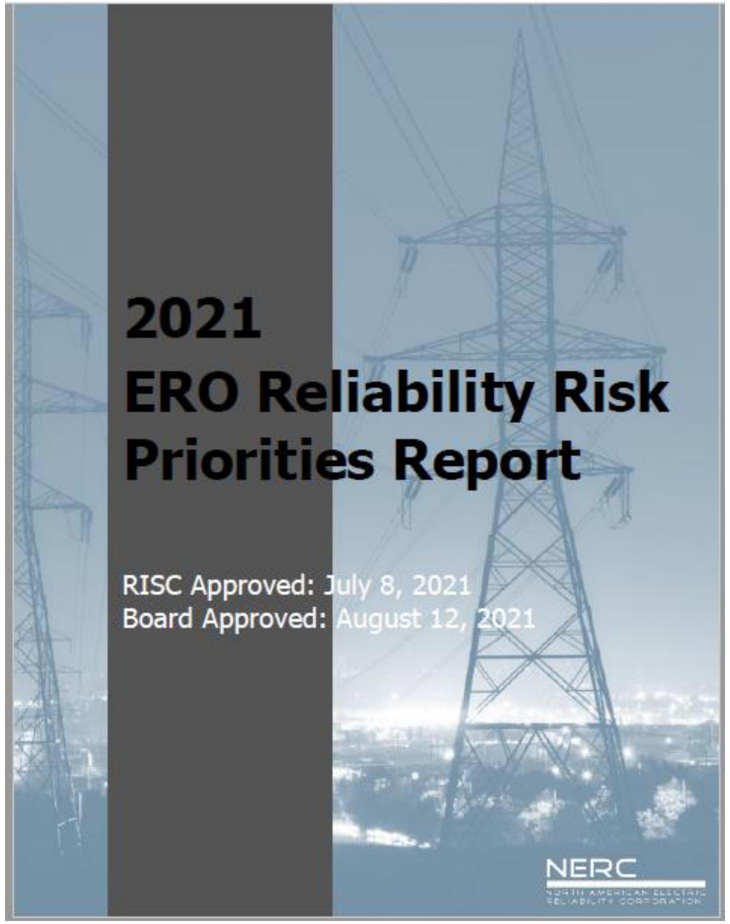
The tragic incident at Hose Lodge Farm in Colston Bassett, Nottinghamshire, was caused by a "computer malfunction" in a broiler shed ventilation system on a warm spring day.

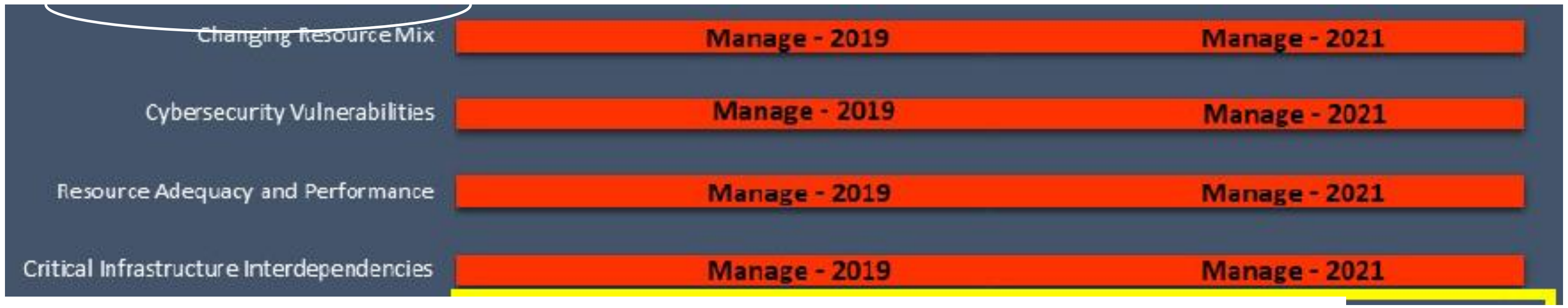
Around 50,000 chickens were inside the shed on May 26 2020 when inlets on the side of the building closed for a scheduled rest period. A fault in the system that regulated air flow to the shed prevented another tunnel ventilation system from opening, turning the shed into a sealed unit.

Risk for the Grid

Changing Resource Mix and Cybersecurity are the highest Ranked Risks

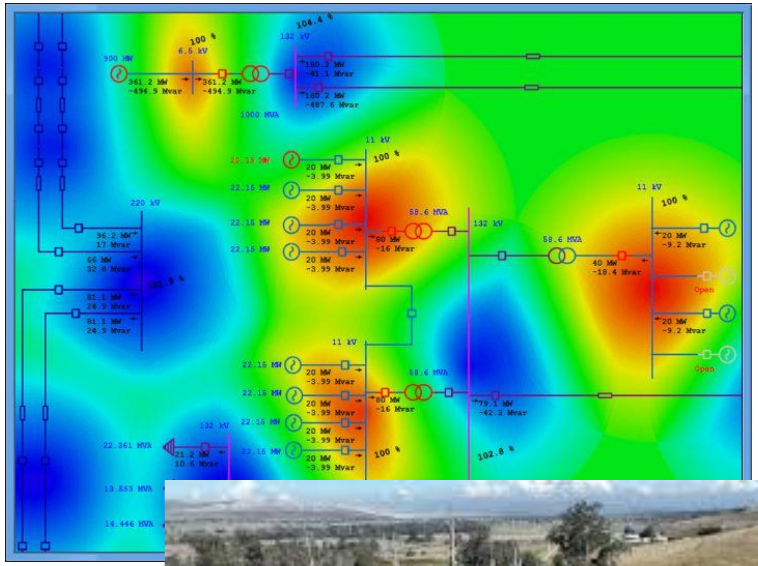
NERC Reliability - Risk

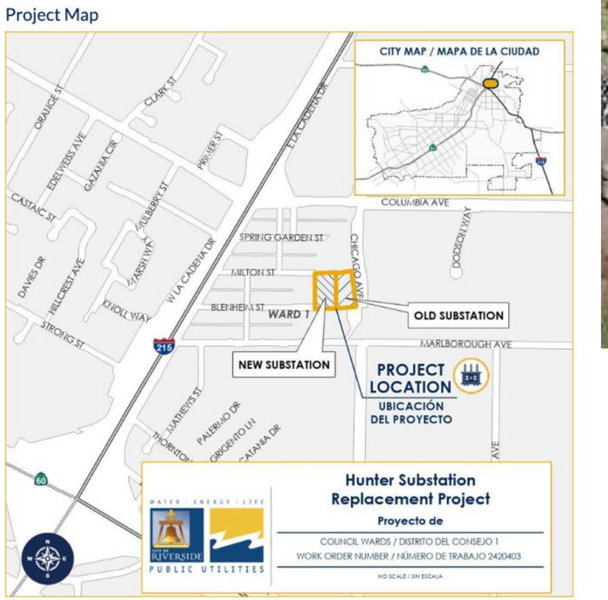




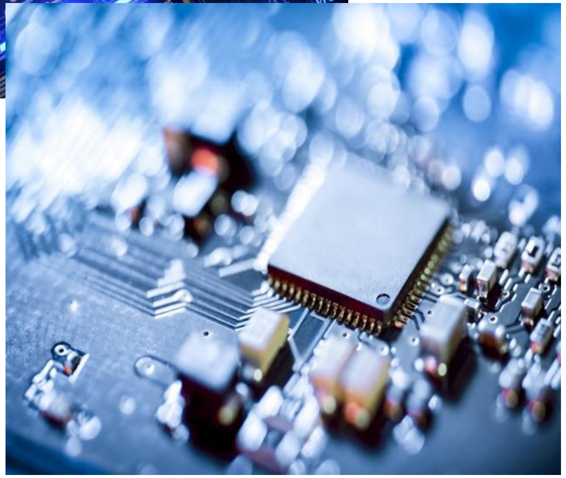
Data Security for infrastructure

- The volume of electric grid infrastructure visible, and available has increased significantly
- In some cases, geographically tied synthetic data, is releasing equivalently impactful data as open infrastructure maps
- Synthetic data is also creating false studies and allocation of resources to defending or not defending the decisions made in regulation and protection
- There are pro's and cons to data releases – remediation of cyber and physical data issues, may limit remediation of climate and weather issues through investment in upgrades



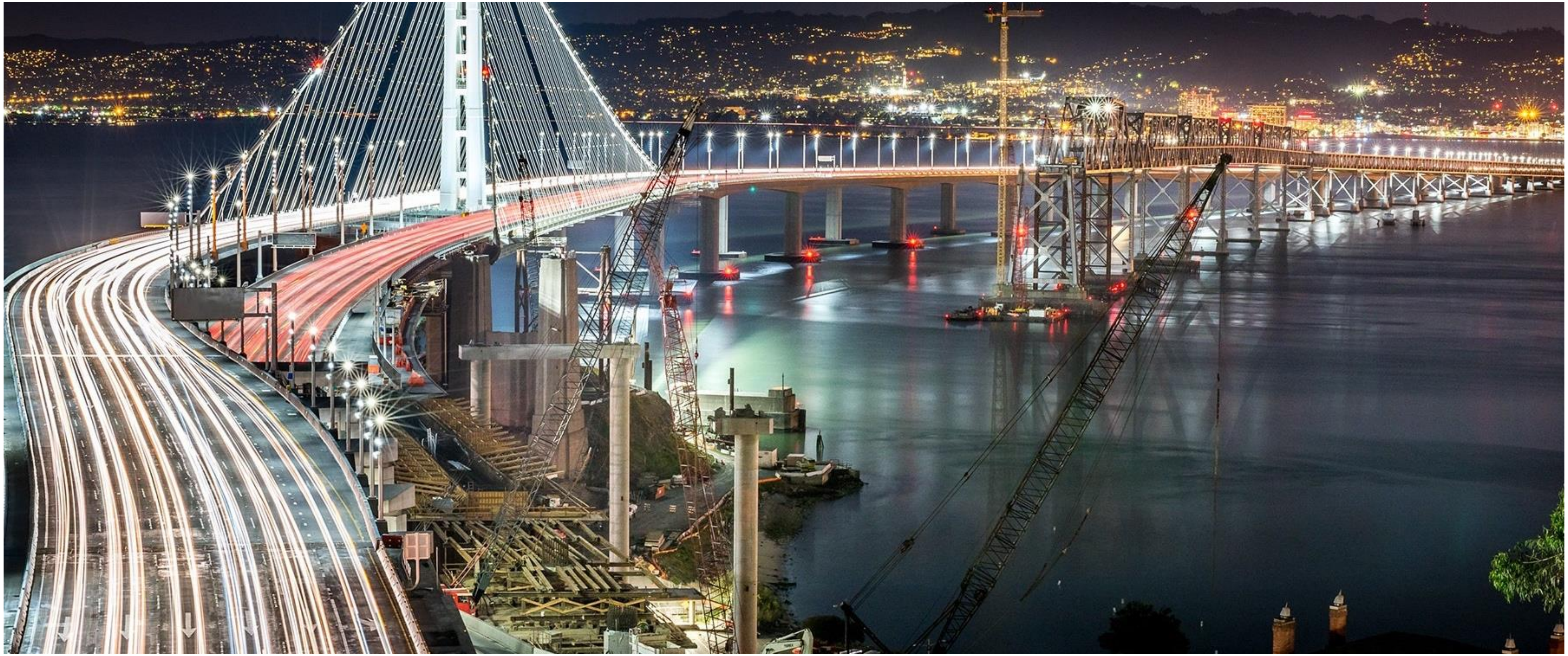


Data Security Trends: Synthesized vs. Real

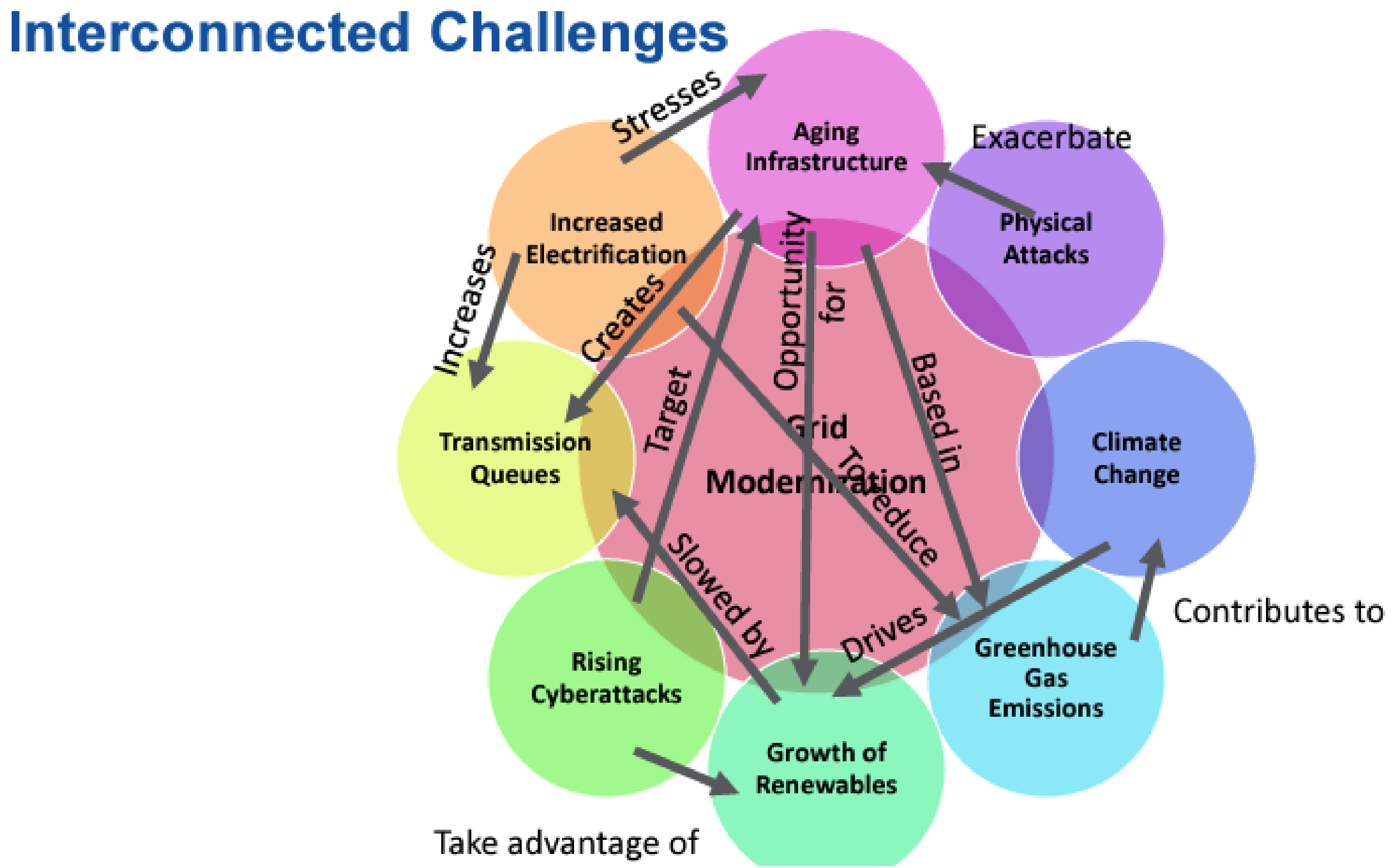


- When data is limited: Grid Models & Simulation of Risk and Consequence use synthetic and overly simplified representations
- Accuracy: Rapidly changing grid, very little realistically we can predict with a synthetic data source
- Too Perfect: Synthetic dataset are often clean when used in development of algorithms for machine learning, which cannot solve for "dirty" or real dataset
- Real World Data: Public distribution grid data and other open-source and commercial data may not be in a standard format, and may present other visibility risks but is far more reliable in assessing risk, making predictions, and informing mitigation strategies

Data Security and Device Dependencies: Customer owned resources and data as operational assets

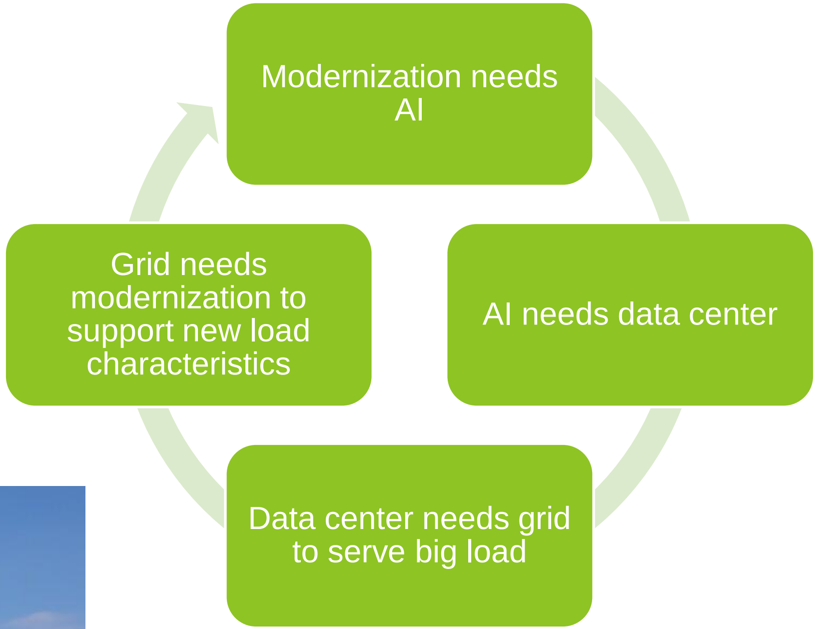


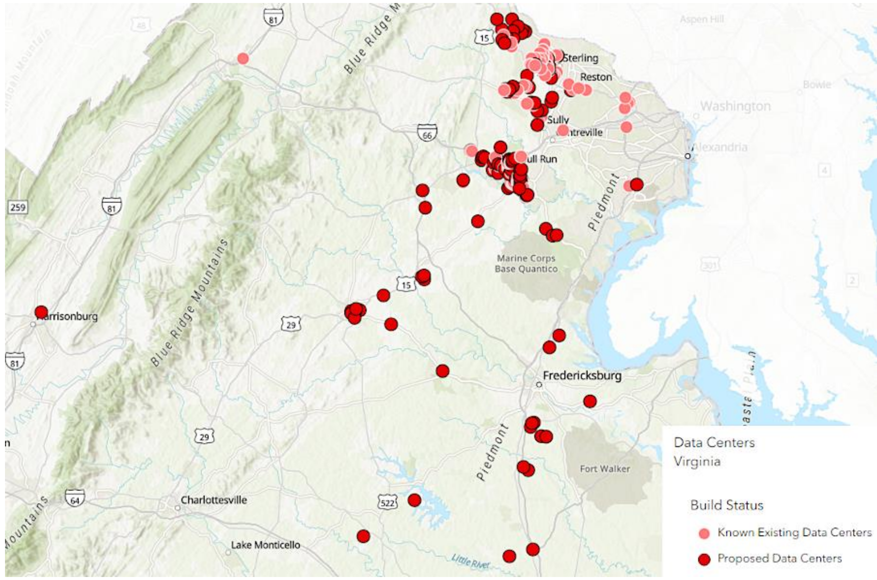
Interdependencies – Data, Resources, Sensors and modernization



Incoming: Massive Load Increases driven by data + AI

- 17GW (2022) to 35GW by 2030
- Entire state of Virginia = 20GW
- Scotland = 6 GW
- Nearly 6 Scotlands, or 1.7 Virginias





Bringing it together – a use case – Blackstart in Industry now

Preparation
- Assess damage – field crew and data
- Define plan, assign roles
- Incident response

System Restoration
- Reconnect big lines, generators
- Major load blocks to stabilize

Load Restoration
- Restore load in each island
- Resynchronize pockets

Bringing it together – a use case – Blackstart in Industry 4.0 – High Data Dependency and Infrastructure Resilience

New Dependencies

Preparation

Assessing Substations for Damage
Cyber Assessment and Root Cause

batteries are charged to last 3+ days

Need data center for processing & damage remediation tools

System Restoration

Determine hyperscale load locational priority

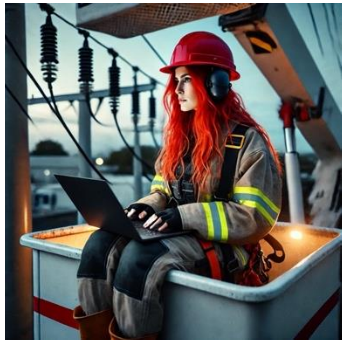
Comms with throughput capability must come up first

Determine distributed crank paths & load pockets




Additional yard for power electronics + technicians

Determine physical equipment needs



Load Restoration

Dispatch Cyber + Physical Teams

Cyber Mutual Assistance

Resynch grid

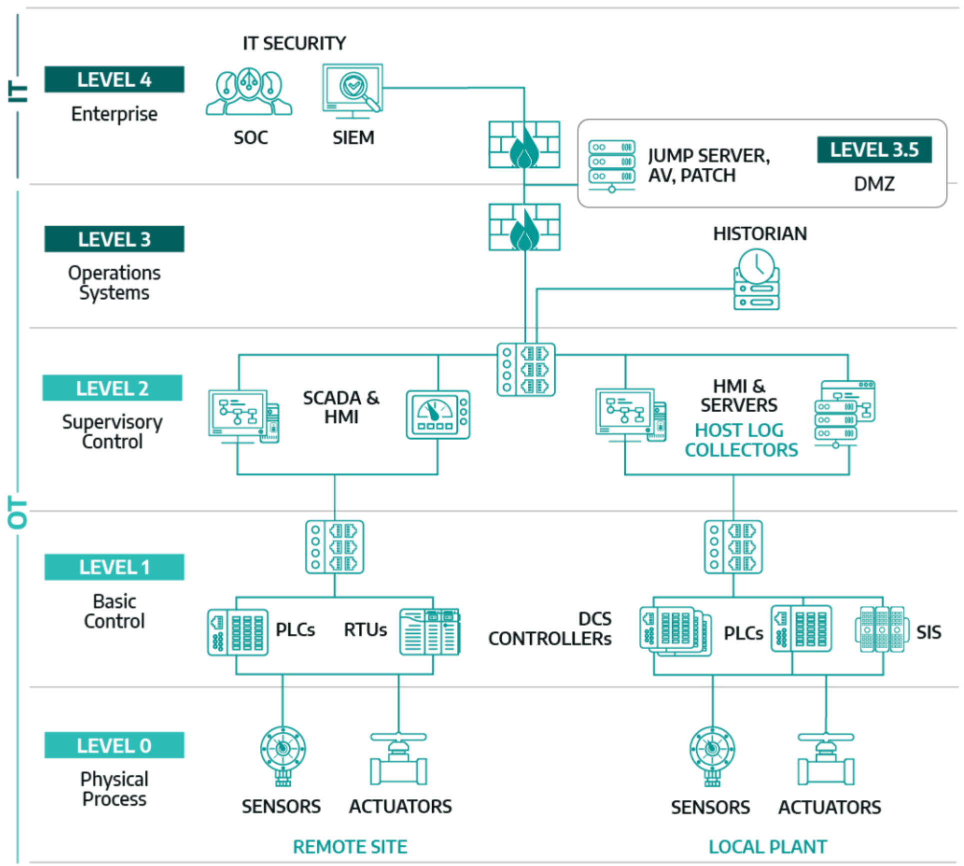
Resynch cloud and data remediation

Sensing for Security: OT Monitoring & INSM (3)

- OT Security Monitoring is continuously collecting data and analyzing the security of operational technology systems to detect and respond to cyber threats in real-time.
- OT systems are designed to manage physical processes, and their security is critical to maintaining operational continuity and safety.
- Key Components of OT Security Monitoring:
  - Real-Time OT Cyberattack Detection: Identifying threats as they occur to prevent disruption.
  - Cyber Resilience in OT: Ensuring systems can quickly recover from attacks. According to a survey by SANS, 67% of OT organizations believe that a cyber attack on their OT systems is likely in the next 24 months
  - Cyberattack Prevention for OT: Implementing measures to thwart attacks before they cause damage.
  - OT Cyberattack Response: Developing strategies to respond effectively to detected threats

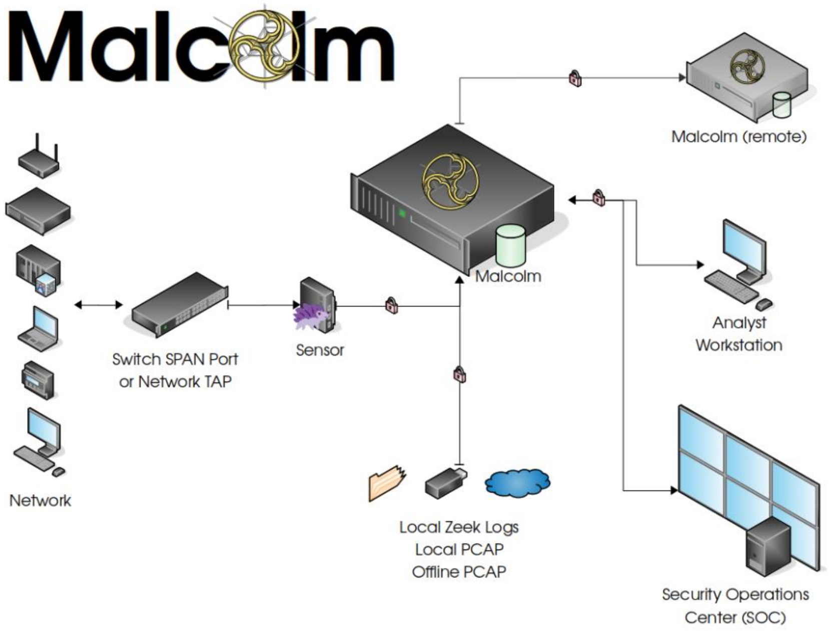
NERC CIP 015-1 – INSM requirements incoming

- The NERC Internal Network Security Monitoring (INSM) is an emerging requirement in the Critical Infrastructure Protection (CIP) Reliability Standards.
- INSM will
  - Detect malicious activity
    - INSM monitors communications within a trusted zone, called an electronic security perimeter (ESP), to detect malicious activity that bypasses perimeter controls.
  - Detect anomalous activity
  - Improve incident response through better data
  - INSM can provide insight into east-west network traffic, which can help provide a more comprehensive picture of an attack.
  - The INSM process consists of three stages: collection, detection, and analysis.
- The Federal Energy Regulatory Commission (FERC) proposed the new INSM requirements in 2023. The standards will apply to all high-impact and medium-impact bulk electric system (BES) cyber systems with external routable connectivity



Threat Hunt on Site for BESS

- **What is it?**
  - Network analysis searching for anomalous behaviors
  - Look for evidence of threat activity
- **What is it for?**
  - Operational systems: look for threat activity in live systems
  - Commissioned systems: verify all is as expected for newly commissioned systems, no unexpected external connectivity
- **Time Commitment**
  - 1-2 site visits from INL SMEs
  - At least 2 weeks of data collected



Outcomes: reconfiguration, identification of intrusion risk, continued assessment

Cyber Physical Resilience – Solutions

Solutions and Discussion

Strategy….

USE THE DATA WE HAVE BETTER

MODEL THE FAILURE & LIMIT THE CONSEQUENCES

MANAGE THE EXTERNAL VARIABLES BETTER

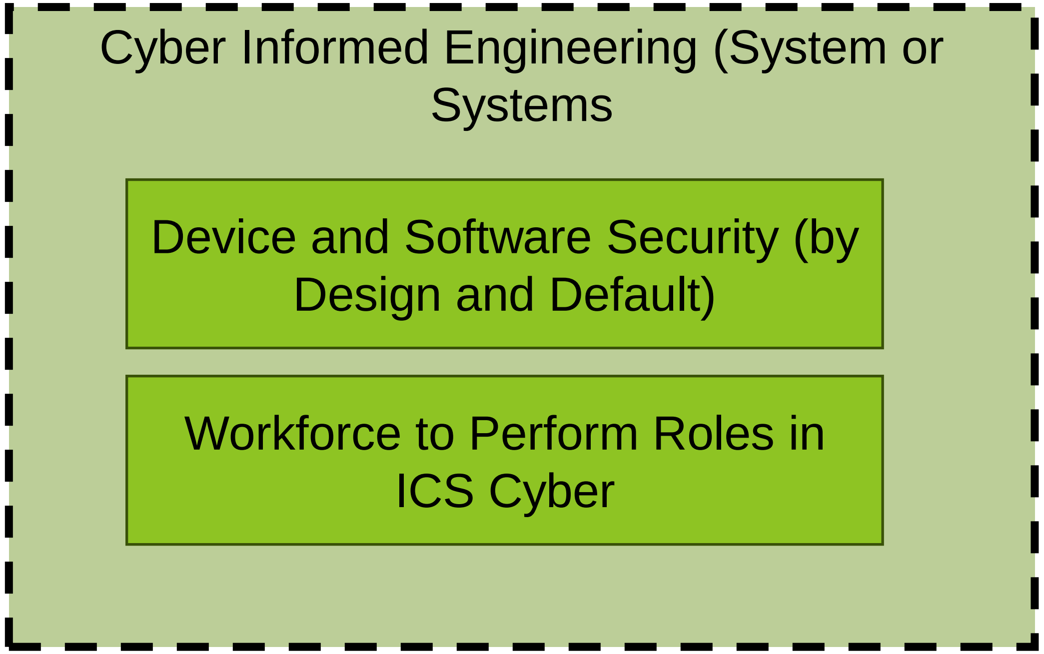
SOFTWARE & COMMS RESPONSE

ASSUME THE PRODUCT IS INSECURE

ENGINEER BETTER THINGS

What do we need to secure, and how can we do it

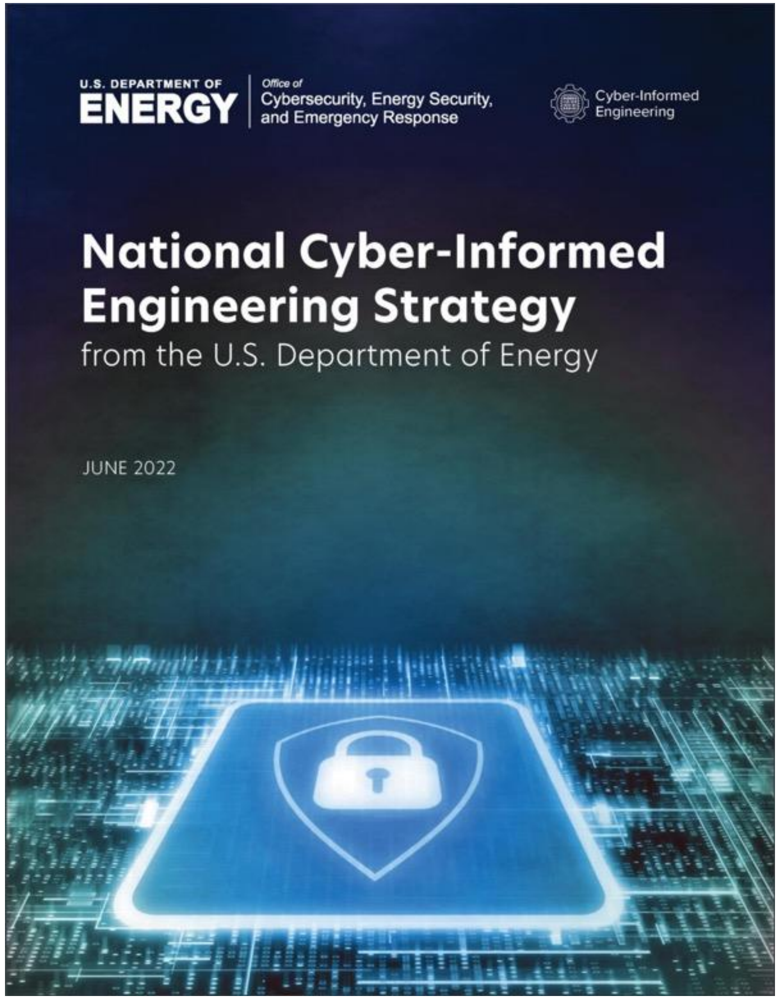
We need the ability to manage and prioritize trusted systems, with redundancy and dependency… all while cleaning up the world



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 engender a culture of security aligned with the existing industry safety culture.



Key Premises of the CIE Strategy

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

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

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

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

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

Designing out the most consequential features, to maximize benefit – pull the plug

What is the purpose of the proposed system

How does it support the org

What sys processes exist for this function

What will happens if it does not perform its purpose

What are the mission critical functions it must perform

What aspects of the CONOPS enable the functions

What needs does it address in the system and how does it do that?

Success Metrics

Net zero targets

Cost reduction

Improve security

What Consequences from unexpected operations

Impact to delivery, safety, security, the environment, property, financials, or corporate reputation

What happens if multiple consequences at once

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

Consequence-Focused Design

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

- What is the normal operation?
- What is the worst it could be?
- What are the system's critical functions?
- What is my risk appetite?

Design Simplification

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

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

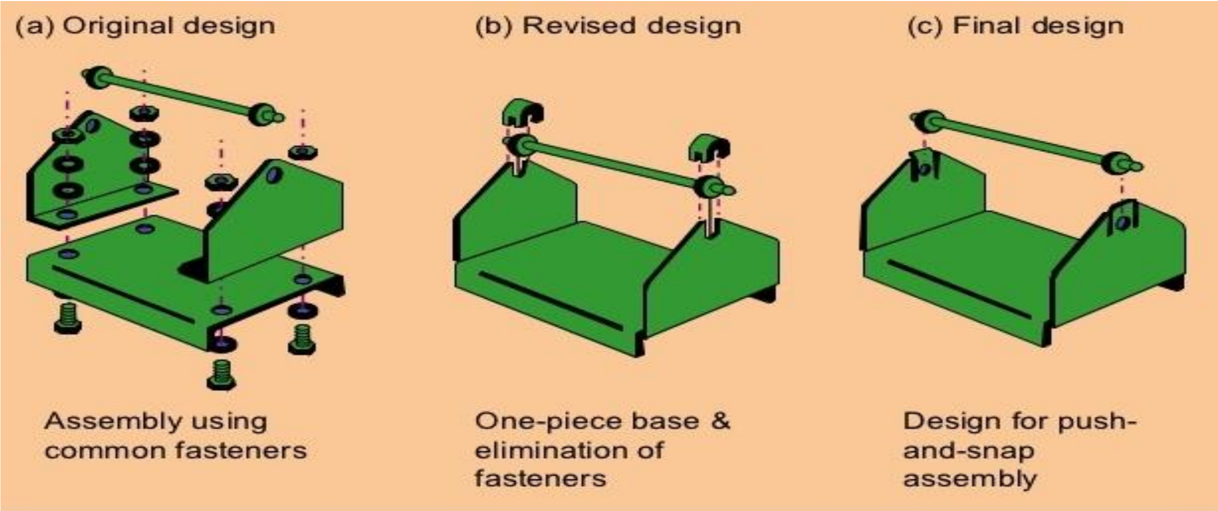
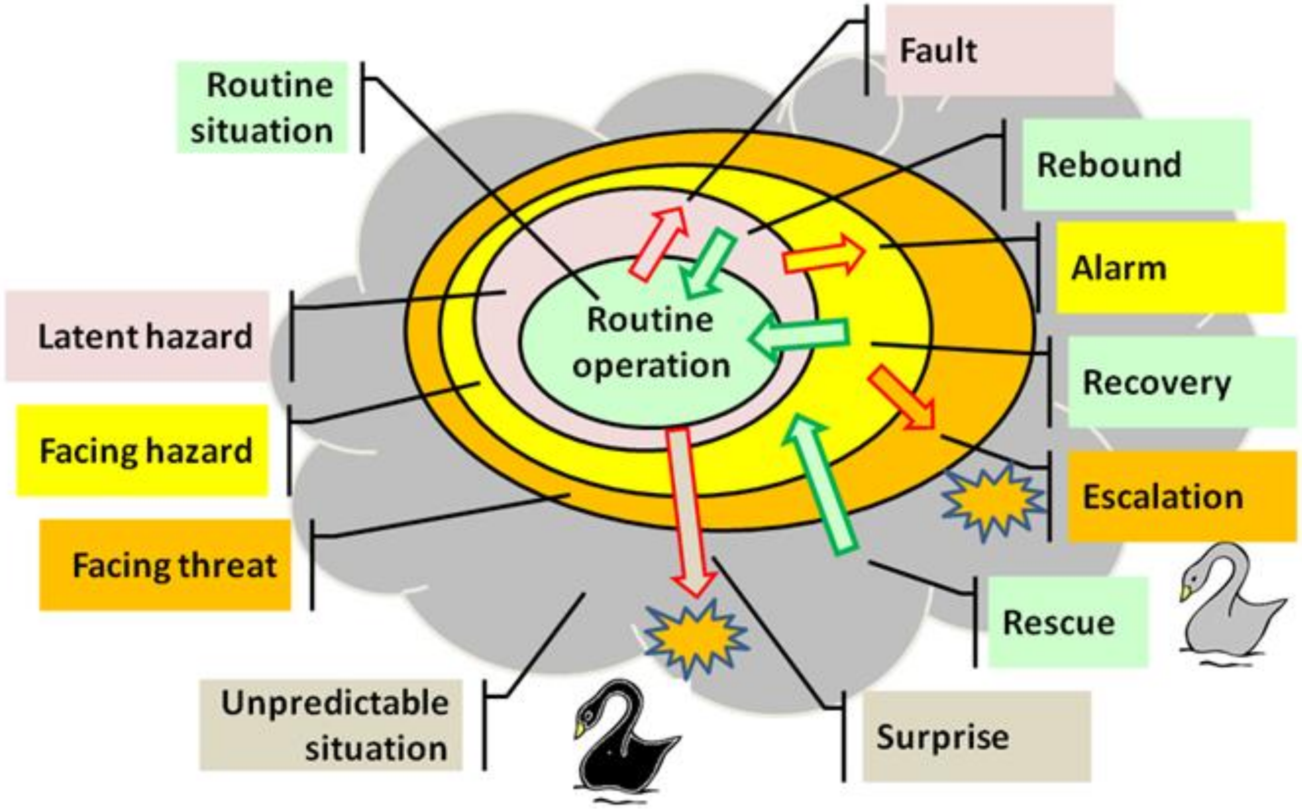


Image from: http://www.slideshare.net/BabasabPatil/product-design-ppt-doms

Resilience Planning

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



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

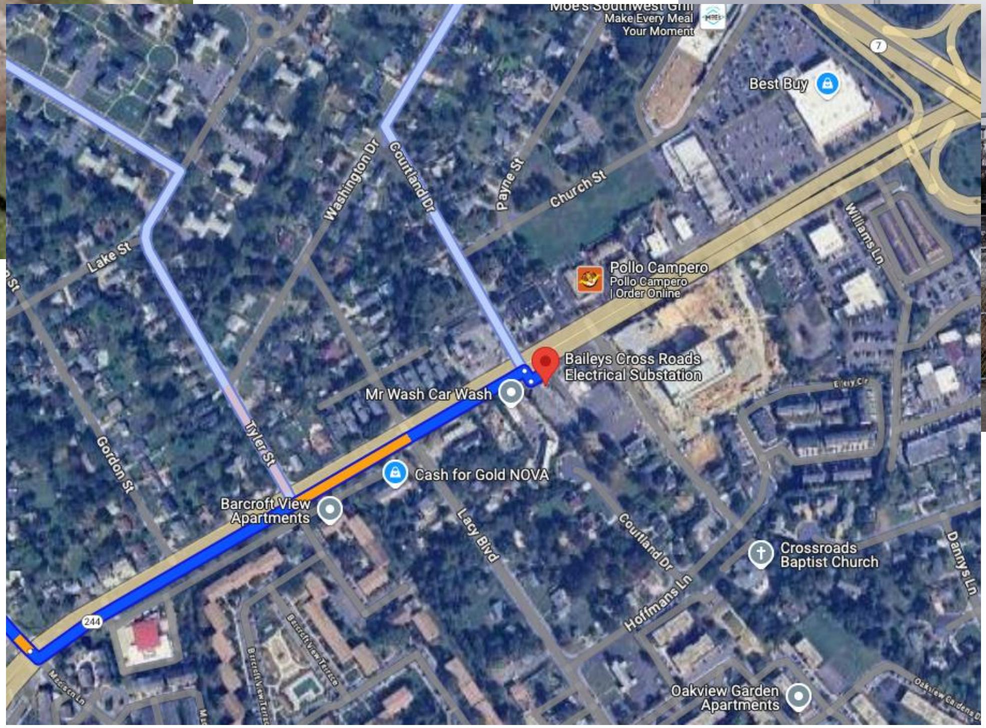
Engineering Information Control

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

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

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

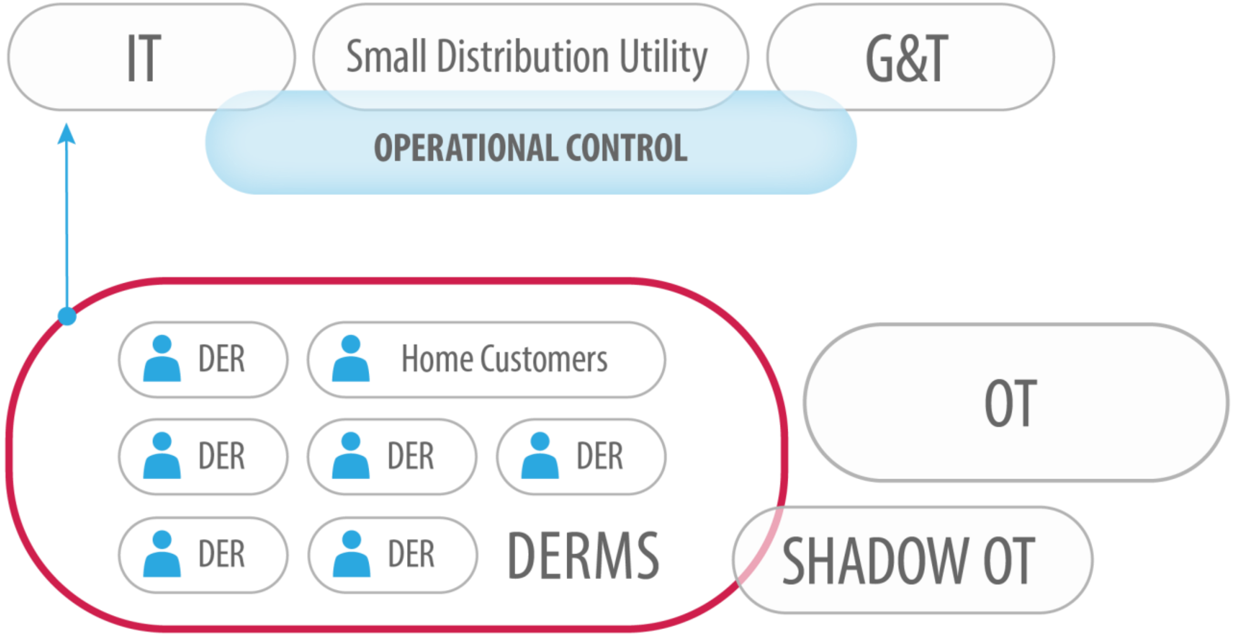
Engineering Controls Example: Transformer Sensing



Solutions 2: Cloud Security
Data Management & Cloud: DERMS + the Cloud

- OT is managed by Transmission provider
  - They have IT but no OT
  - Many customers buying behind the meter resources
- Need a way to manage the data and make decisions on interconnection
- DERMS! - ICSaaS in the Cloud
  - Communicates through FAN
  - Is it OT or IT? Is it Shadow OT?
- Shadow OT?

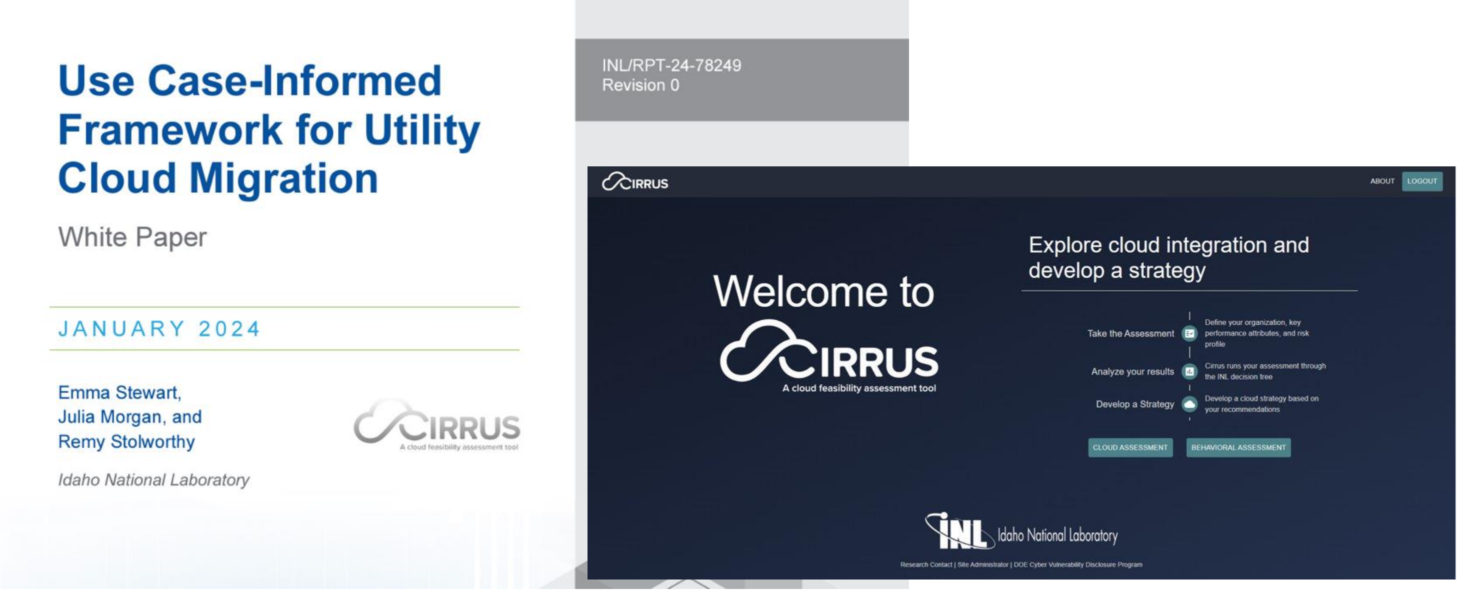
Small utility <50K customers



Solutions for Data Security: Cirrus Tool Rapid Development and Deployment *Responsible use of cloud in Operational Technology*

https://inl.gov/cirrus/

- A **consequence-driven decision support framework** for entities to assess their grid modernization deployment strategy in the cloud
- Test against use cases and partner users **enabling adequate assessment** of deployment plans.
- IAB (30+ attendees) – bimonthly (short)
- COP – bimonthly (15 – 20 attendees)
- Users – 6 demonstration, move to licensing model



EEI Edison Electric Institute · Google Cloud · aws · Schneider Electric · smarter grid solutions · nisc · CLAROTY · United Power · RA · GE VERNOVA · Alabama Power · CAMUS · E-ISAC · NOZOMI NETWORKS

Consequence Driven Cloud Decision Framework for Small/Medium Utilities

Cost/Benefit at every layer of analysis	Tailored to stakeholder user and type – critical functions	Forward looking	Applicable to emerging use cases in grid and digital modernization
Cyber Informed	Explainable	Repeatable	Enable ability to unlock potential modernization paths

Develop & Test a consequence driven decision support framework for entities to assess their grid modernization deployment strategy in the cloud

Solutions 3: Methods for Assessing Appropriate Data Security Parameters

Current Level of Visibility & Vulnerability

- Street
- Basic Internet Search
- Complex Internet Search
- Public Overhead Imagery
- Commercial Imagery

×

Style of Consequence/Impact

- Potential Physical Attack Capability & Impact
- Cyber Attack Capability & Impact

×

Capability of Viewer of Data

- Average Human no expertise in infrastructure
- Qualified Human – basic expertise in infrastructure/degrees in power/EE
- Insider/SME/Utility Worker

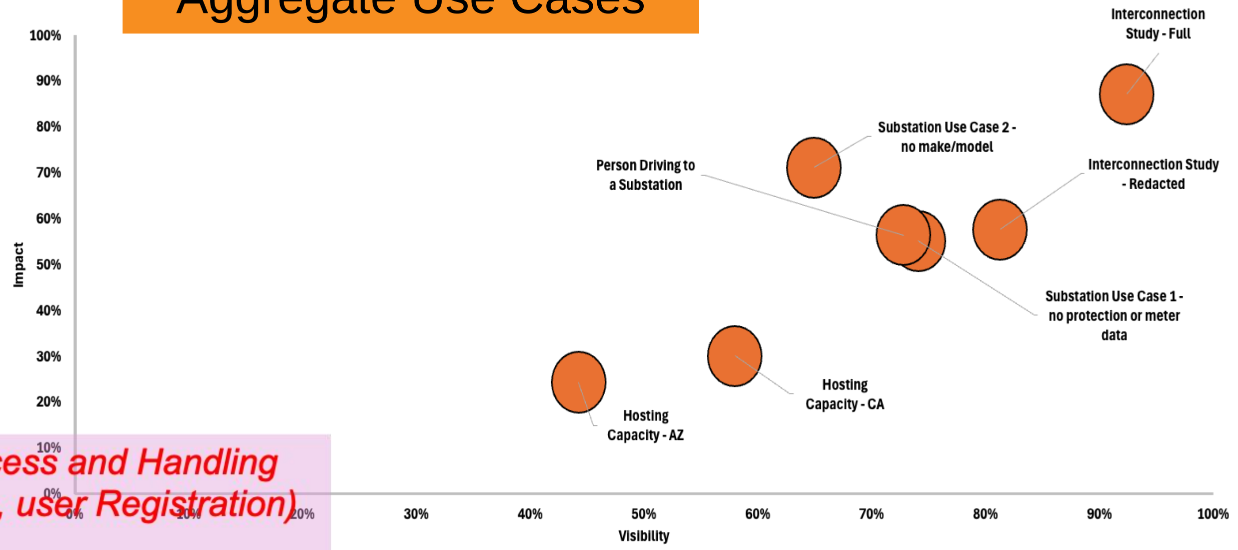
×

Combination of Impact

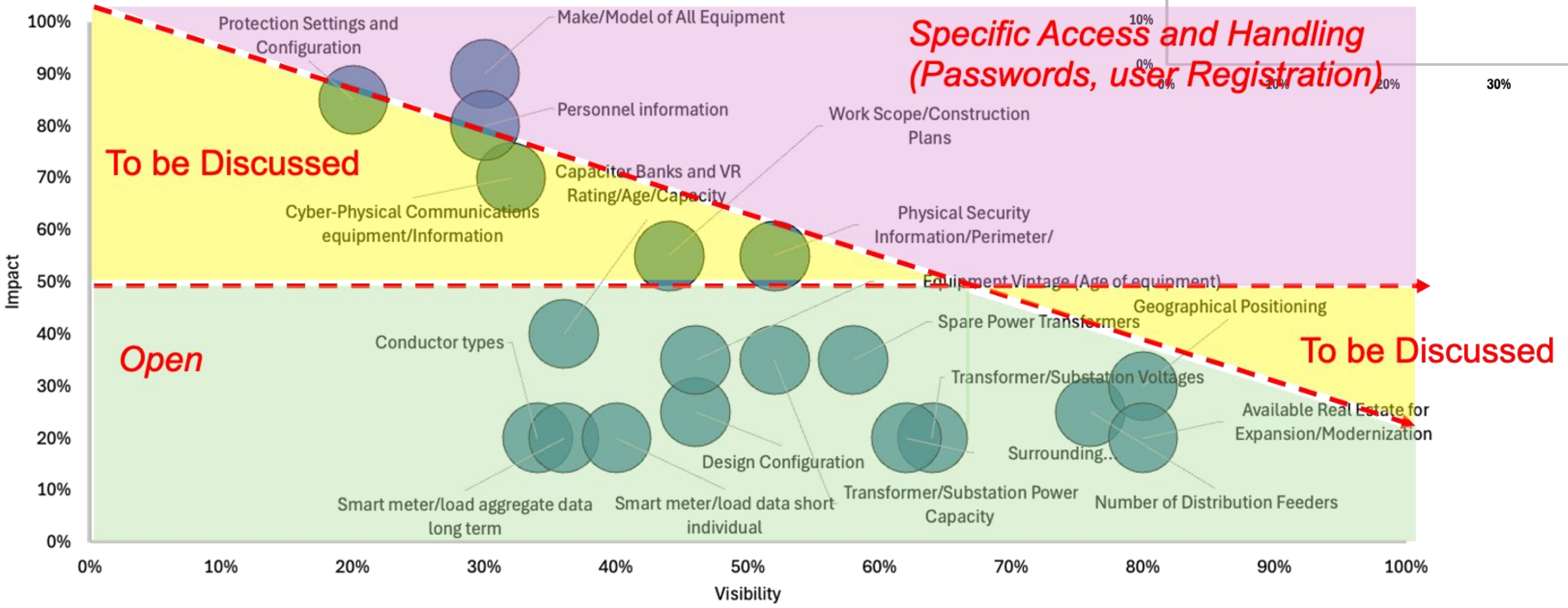
- Aggregate Use Case Data Sets Increasing Risk

Results Visualization: Plotting Data Fields Impact vs Visibility for Comparison – National Baseline set with SME scoring

Aggregate Use Cases

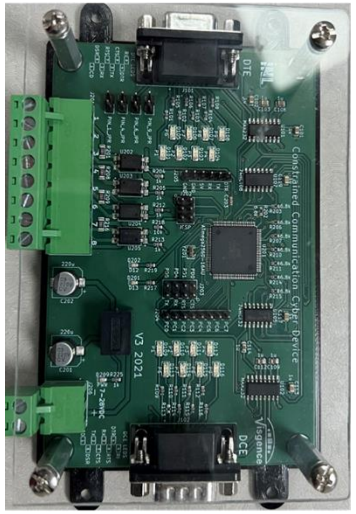


Data Fields



Solutions (4) Secure Sensing and Control for Cyber: Binary Armor

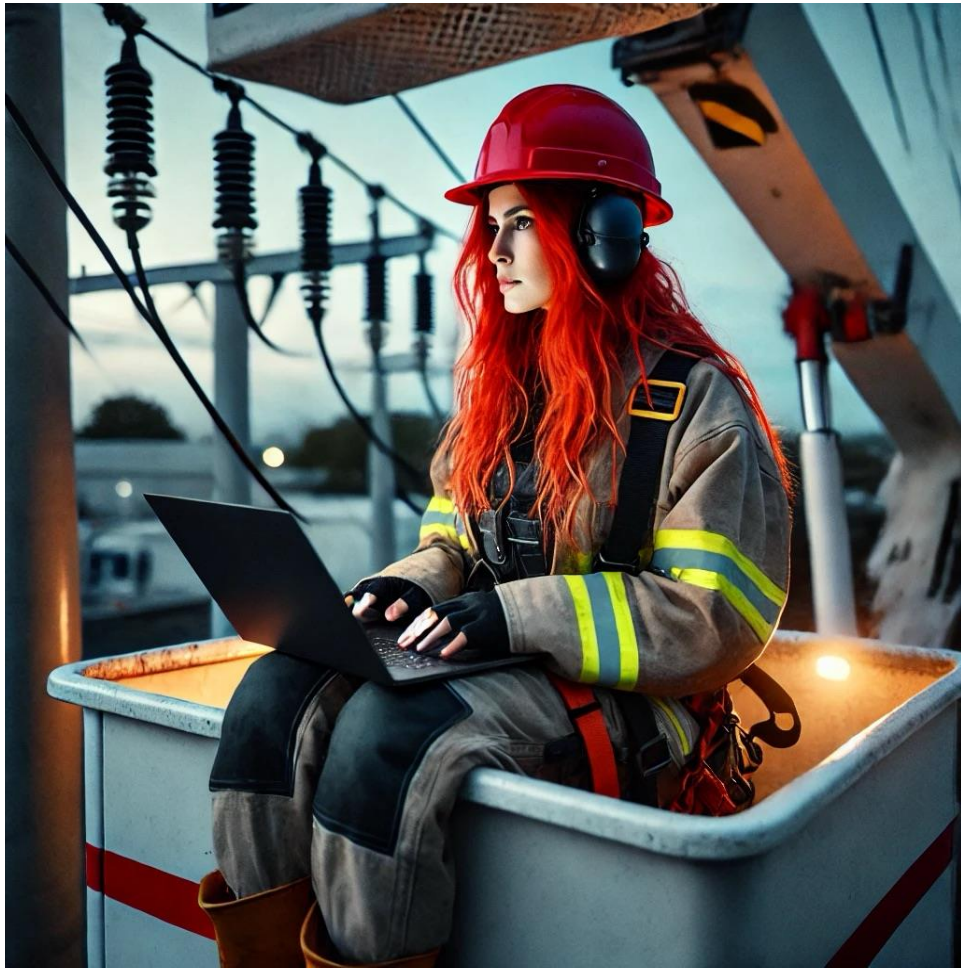
Protective Relay Permissive Communications - Constrained Communications Cyber Device (C3D) is an **impenetrable last line of defense** against **cyberthreats** aimed at **essential electrical grid hardware**



INL's C3D was deployed with a protective relay to CITRC to demonstrate to utilities it's effectiveness at filtering malicious commands

Conclusions

- The industrial change is here
  - But our cybersecurity practices are not
- Really need different disciplines to work together in technical spaces, and translate languages
- Pulling the cyber plug versus the grid plug
- Design it right, secure around the problems



Resources and Contact

- Center for Securing Digital Energy Transformation
- https://inl.gov/national-security/csdet/
- Cyber-Informed Engineering – www.inl.gov/cie
- To Join – CIE@inl.gov
- To find me - Emma.stewart@inl.gov

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.