RSAConference™2024

San Francisco | May 6 – 9 | Moscone Center

THE ART OF POSSIBLE

SESSION ID: CID-M05

Cloud-Enabling the Electric Grid with Consequence-driven Approaches

#RSAC

Dr Emma M Stewart

Chief Power Grid Scientist
Idaho National Laboratory
@turbo81

James Briones

Reliability Risk and Assurance Program Manager
DOE Grid Deployment Office

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

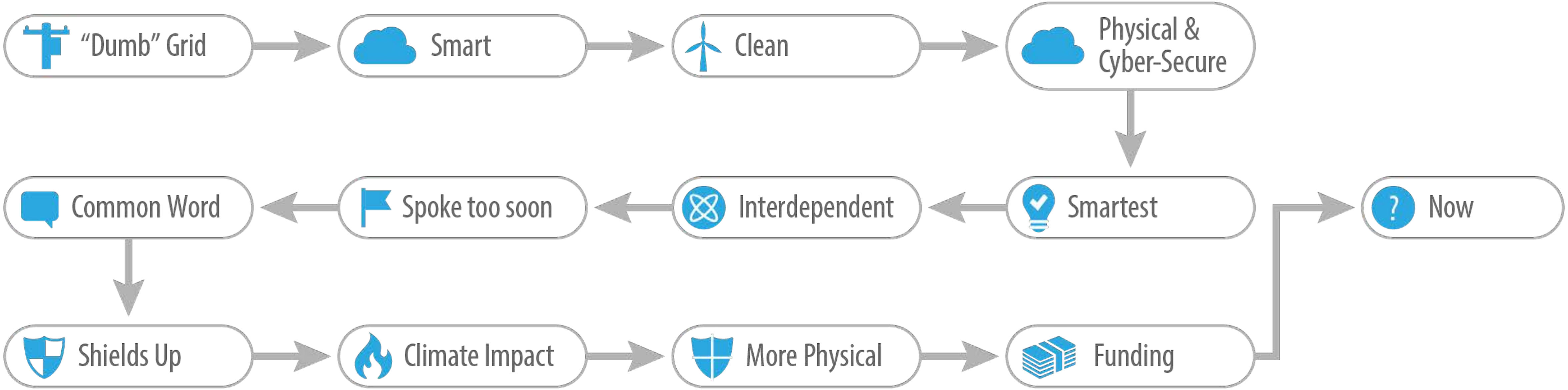
Introduction

- The way we deliver power is changing
- Analog to digital
- More: Power, Reliability, Expectations, Independence, Choice, Complication
- Cloud is everywhere and challenging
- How do we get **all the benefits and minimize the risk?**

What Would you Buy?

Energy Delivery Digital Transformation:

Where are we Going?



"Dumb" Grid

Smart

Clean

Physical & Cyber-Secure

Smartest

Interdependent

Spoke too soon

Common Word

Shields Up

Climate Impact

More Physical

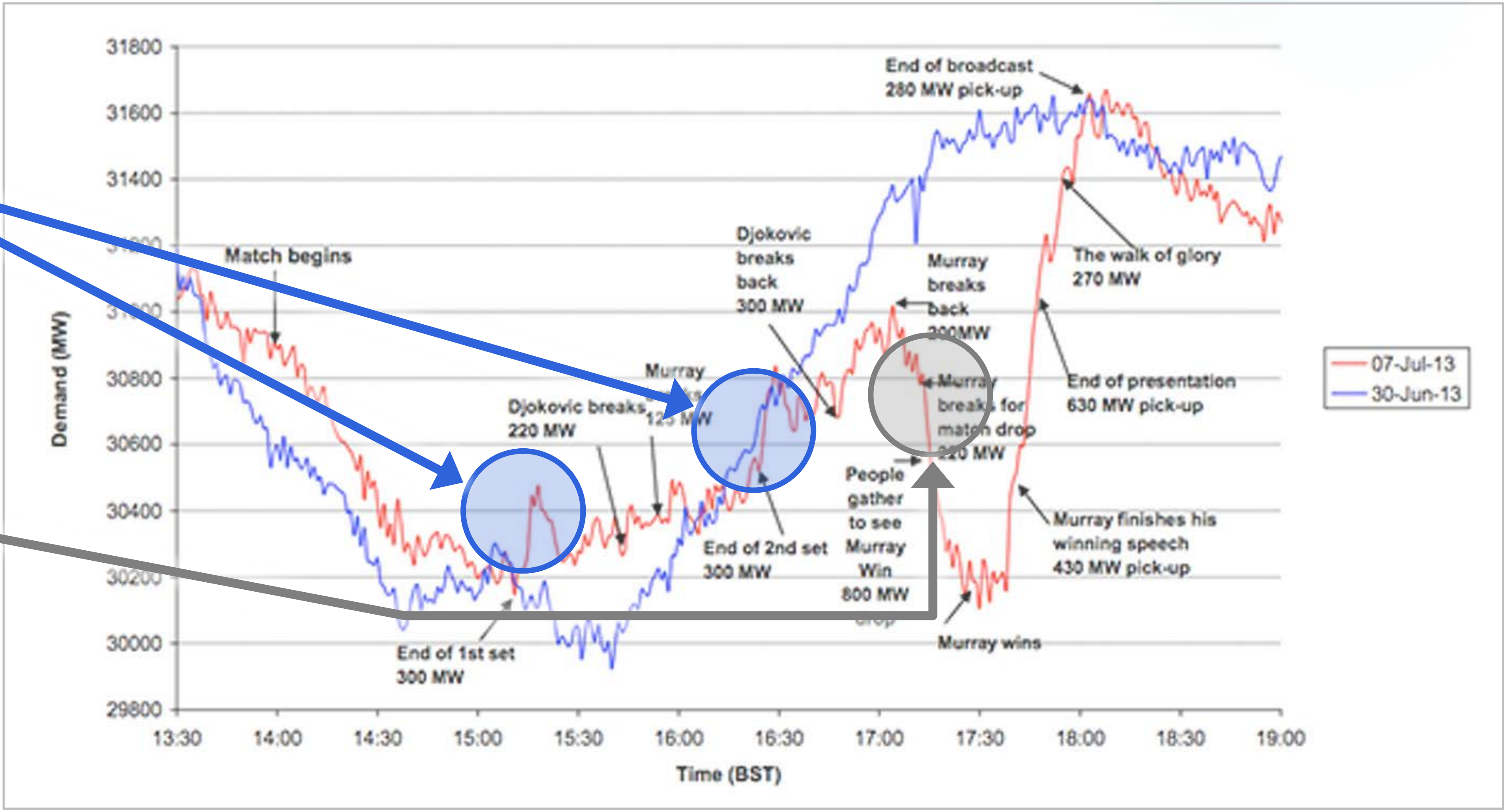
Funding

? Now

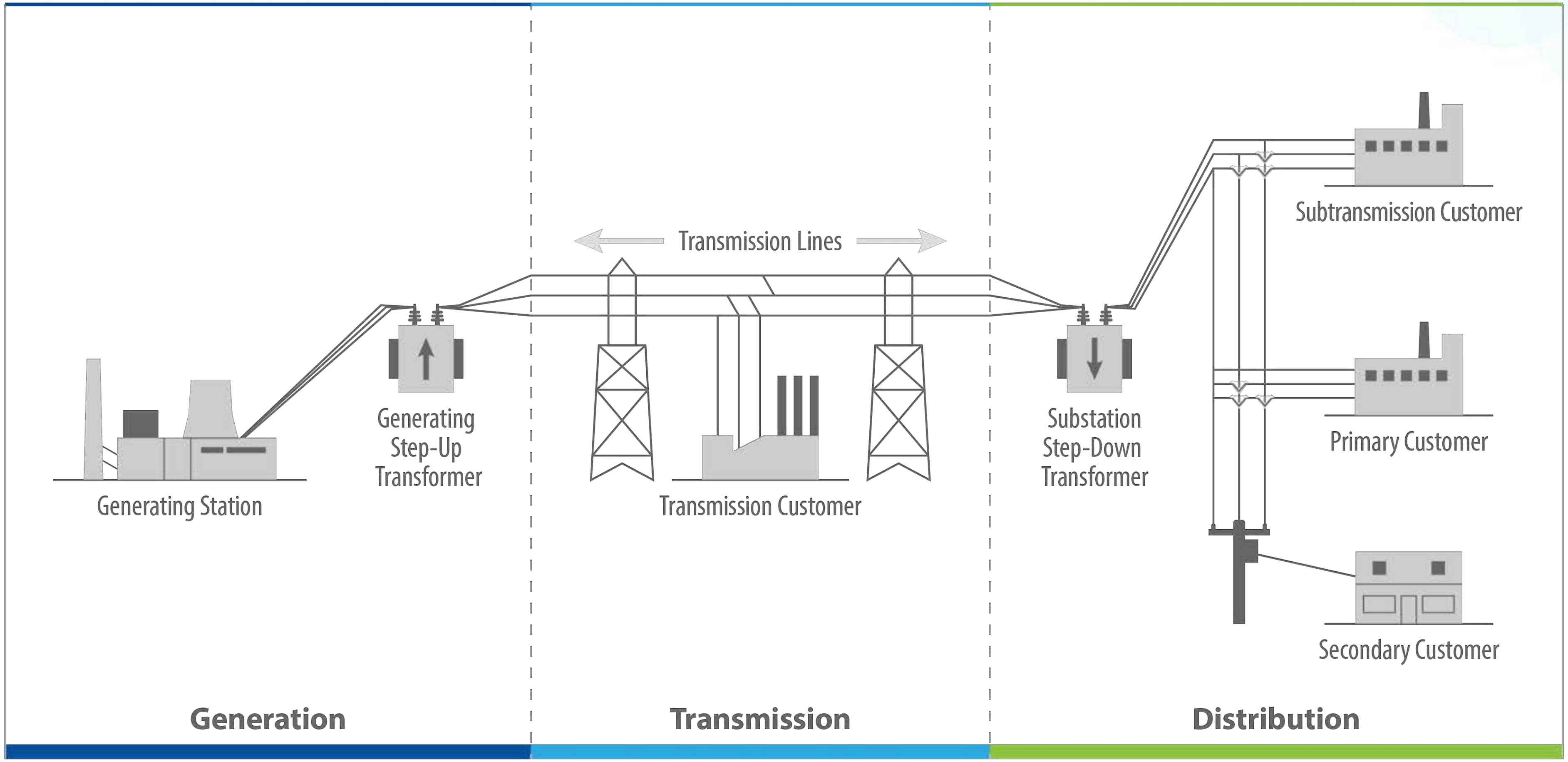
If a cup of tea can swing the grid….

Everyone in Scotland **turned on their tea kettle**

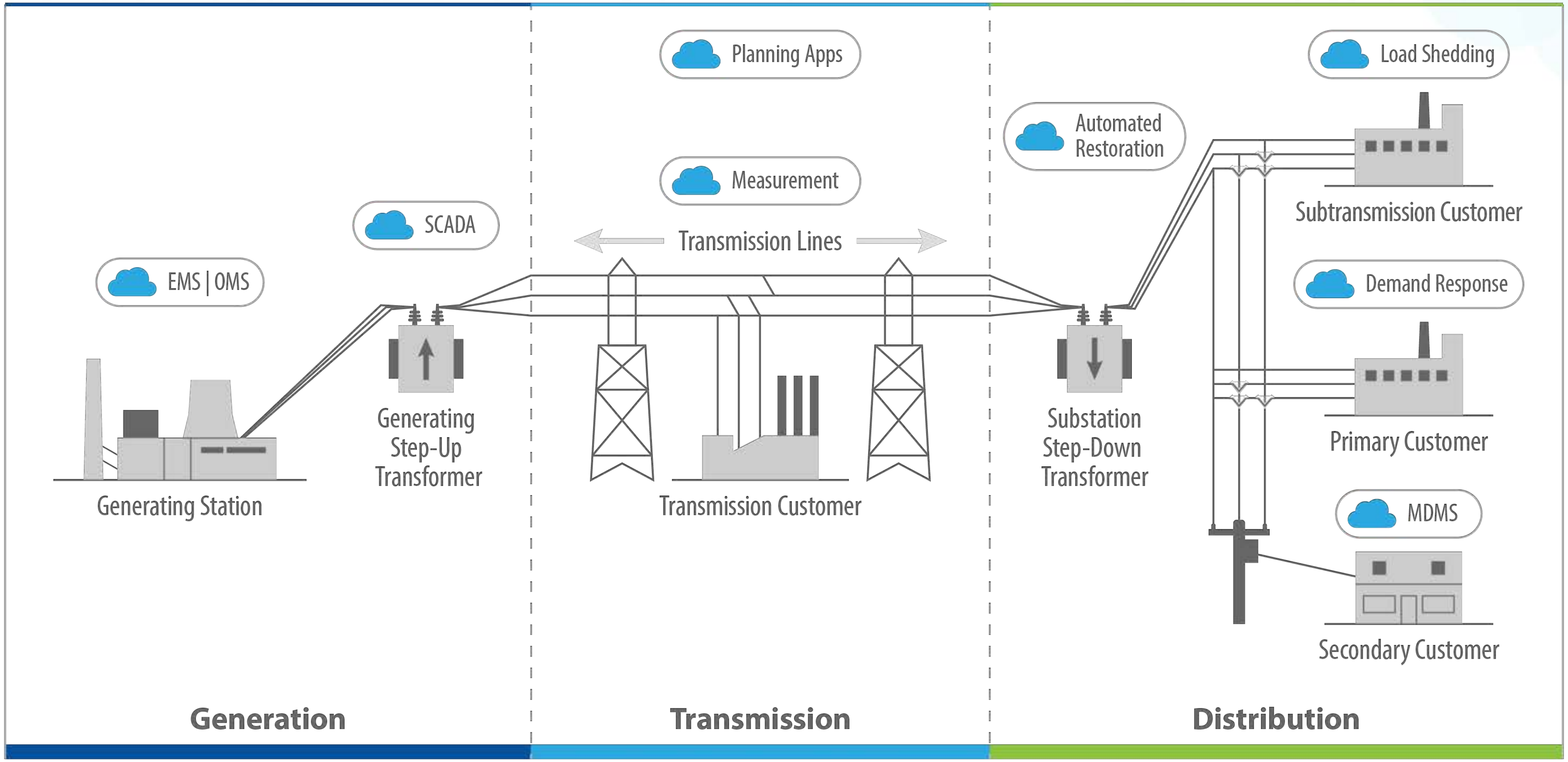
Everyone in Scotland **stopped**



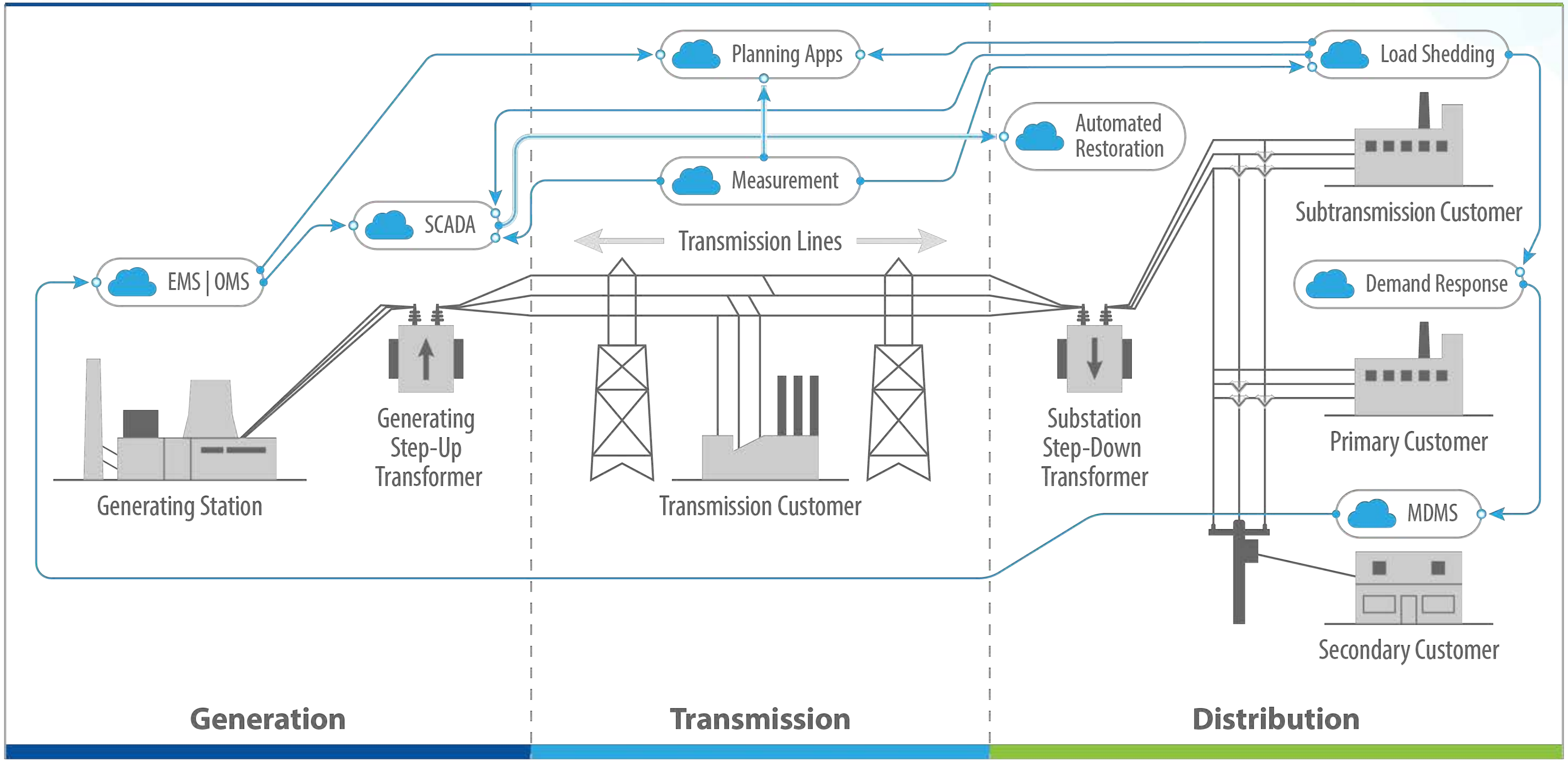
Cloud Everywhere



Cloud Everywhere

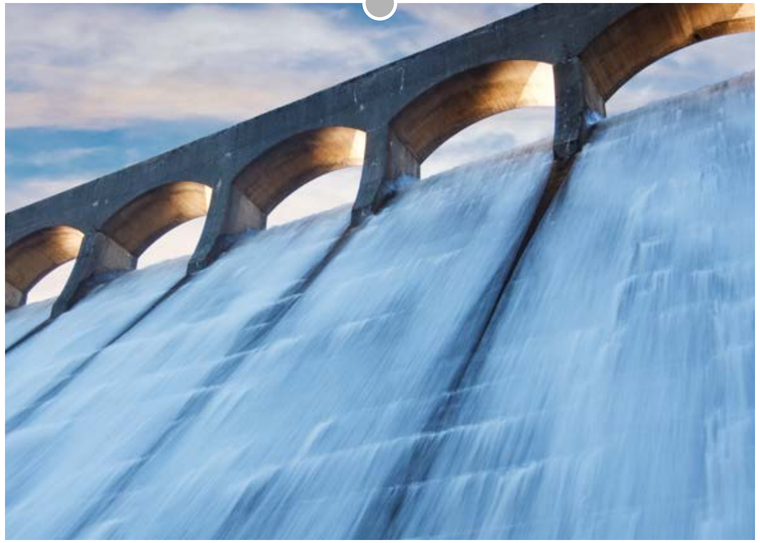


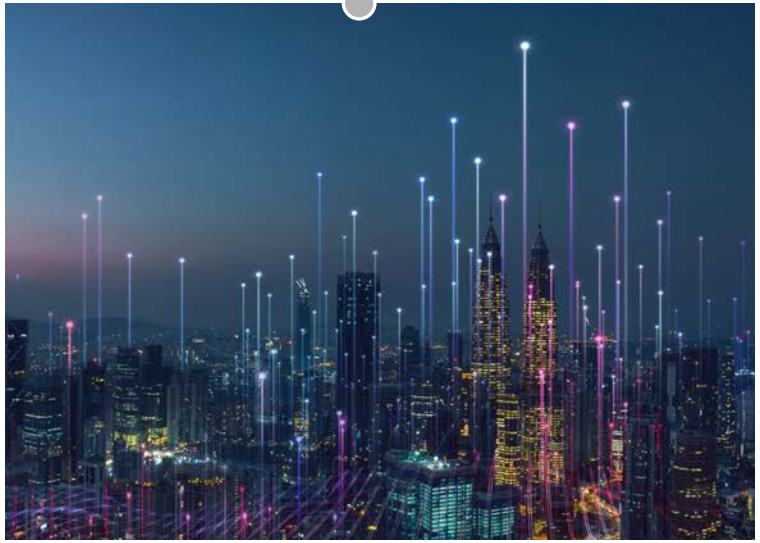
Interconnected Interdependent Cloud Everywhere



Not Just Electric

Industrial Control moving to the cloud affects **other sectors**

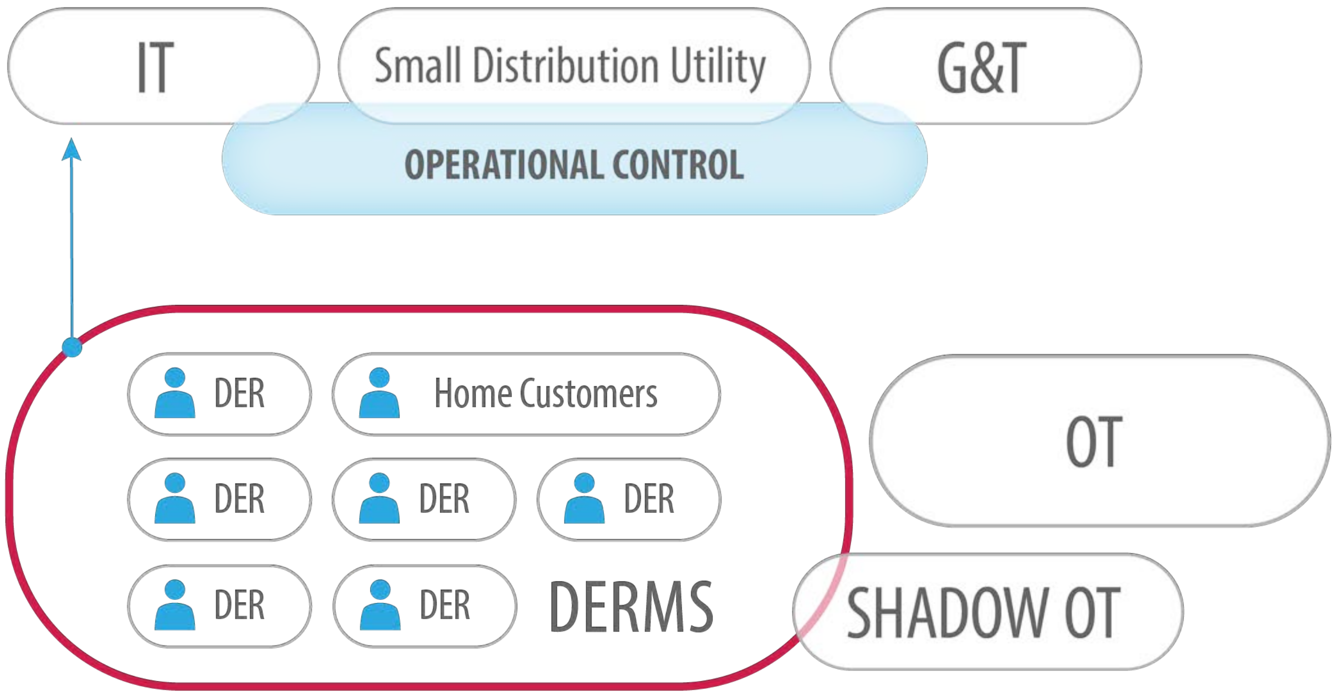




Investment in the Grid and Cloud Infrastructure Security Trends

- **$1.2T** in infrastructure investments
- Industrial Control Systems as a Service (ICSaaS)
- AI as a Service
- Hybrid and Multi-Cloud
- Edge computing everywhere

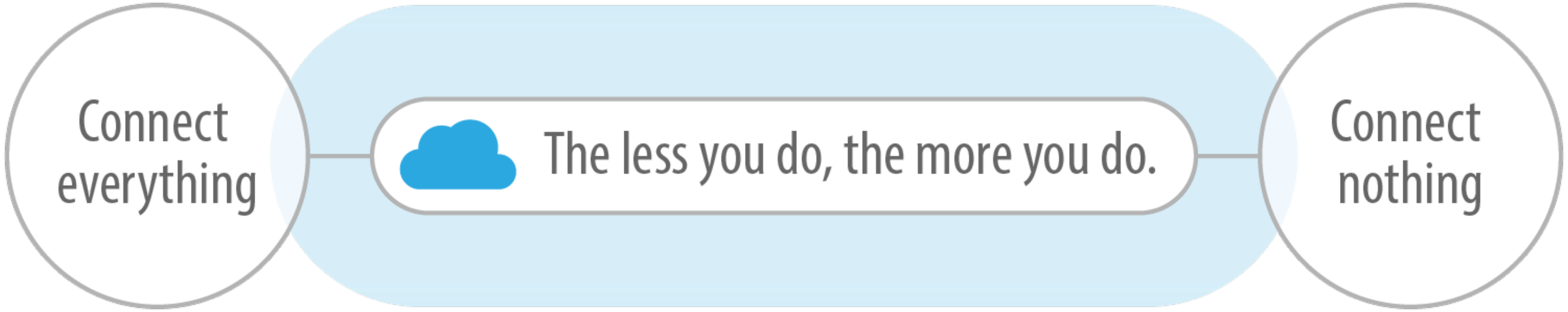
A Story: *DERMS + the Cloud – Shadow OT?*



- Small utility <50K customers
- OT is managed thought the G&T
- They have IT but no OT
- A lot of customers buying behind the meter resources
- Need a way to manage the data, make decisions on interconnection
- DERMS! - ICSaaS in the Cloud
- Communicates through FAN
- Is it OT or IT? Is it Shadow OT?

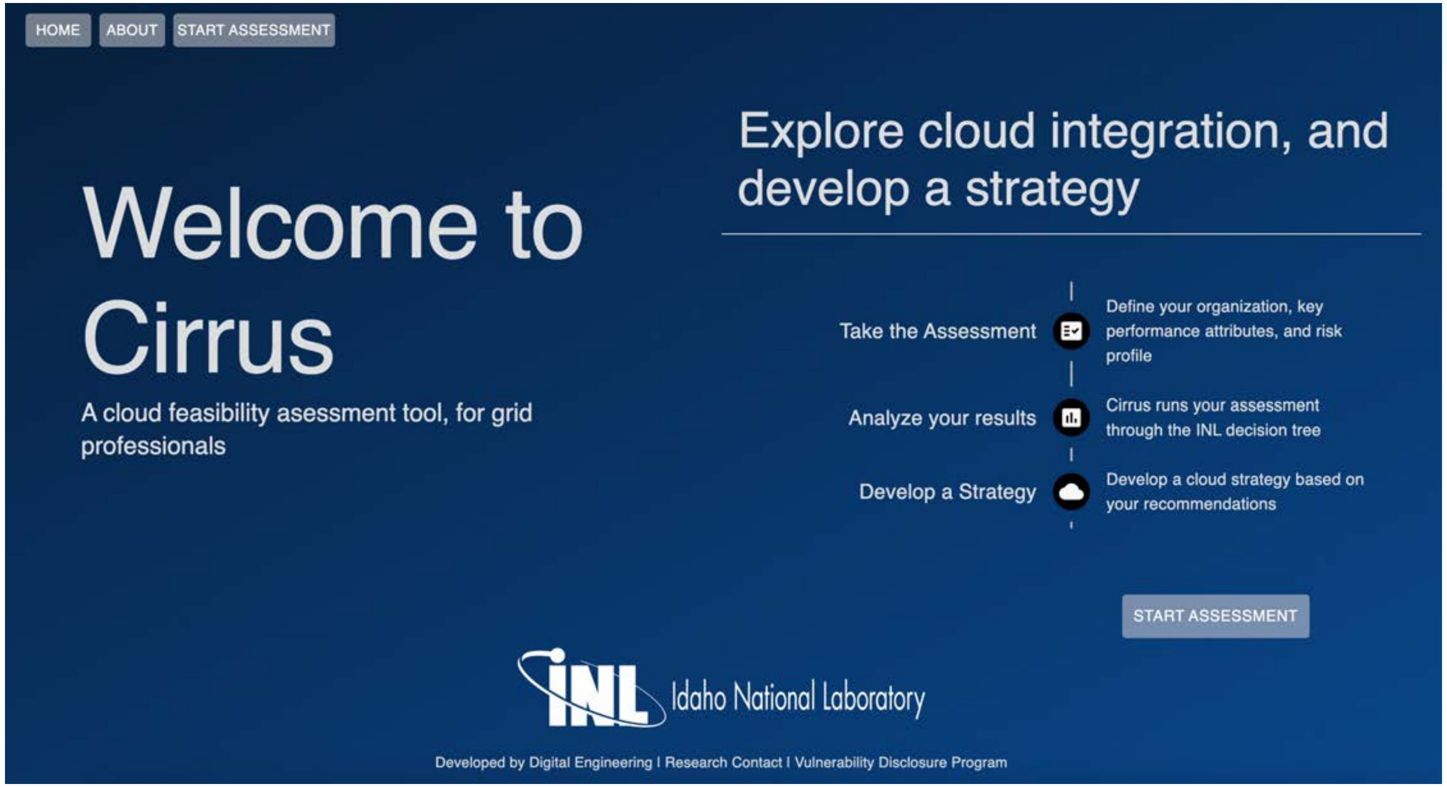
Securing Digital Infrastructure: competing objectives

- **Define** a decision support process and operationalize it
- **Incorporate** basic design principles for interconnection – lose the heterogeneity
- **Reduce** the attack surface in the first place with secure and right-sized design



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.



Welcome to Cirrus

A cloud feasibility asessment tool, for grid professionals

Explore cloud integration, and develop a strategy

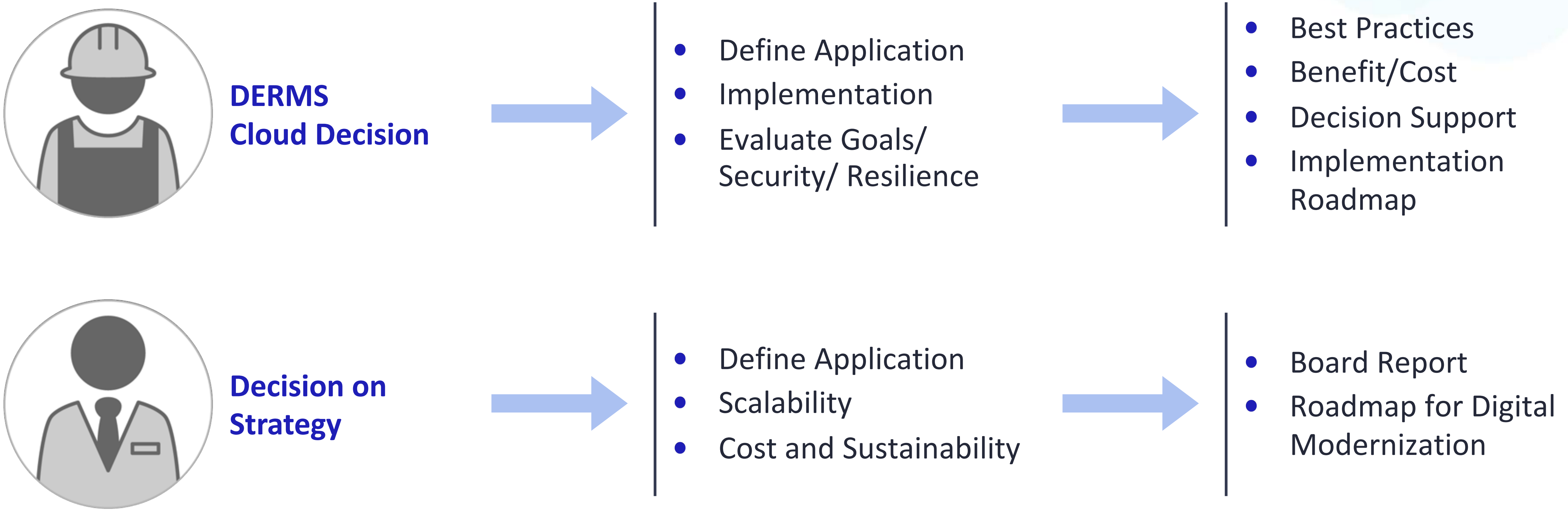
Take the Assessment — Define your organization, key performance attributes, and risk profile

Analyze your results — Cirrus runs your assessment through the INL decision tree

Develop a Strategy — Develop a cloud strategy based on your recommendations

Developed by Digital Engineering I Research Contact I Vulnerability Disclosure Program

The Users at a Utility: *Who Are You Talking To?*



DERMS Cloud Decision

- Define Application
- Implementation
- Evaluate Goals/ Security/ Resilience

- Best Practices
- Benefit/Cost
- Decision Support
- Implementation Roadmap

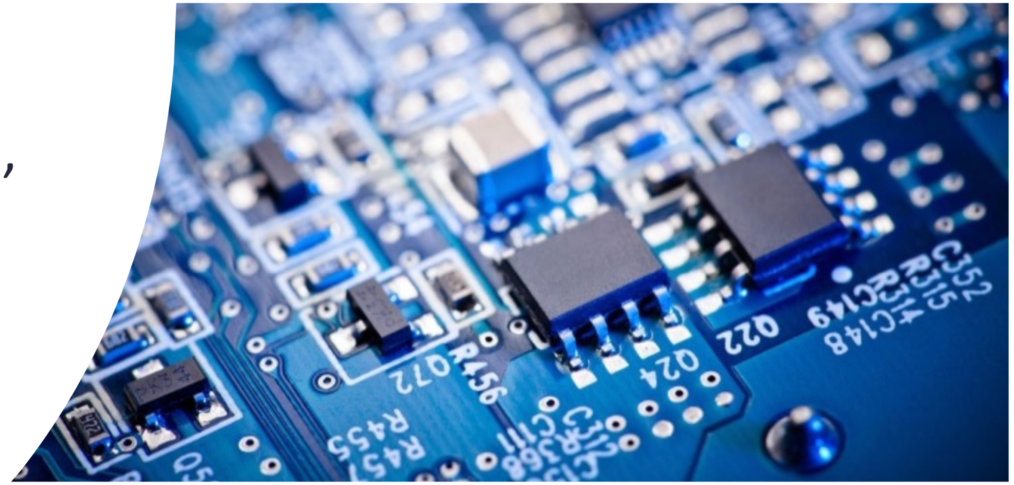
Decision on Strategy

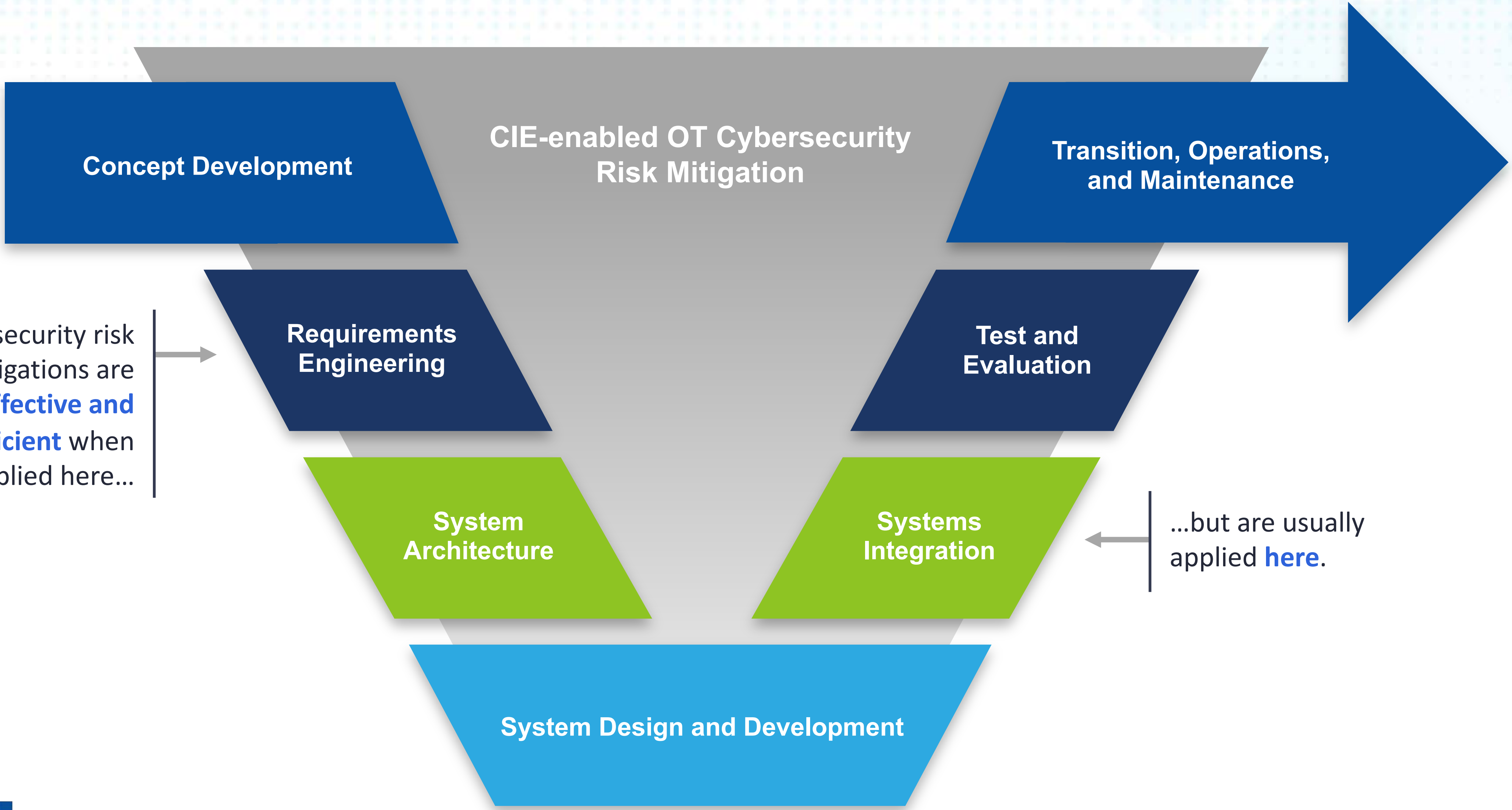
- Define Application
- Scalability
- Cost and Sustainability

- Board Report
- Roadmap for Digital Modernization

Cyber-Informed Engineering (CIE)

- Uses **design decisions and engineering controls** to eliminate or mitigate avenues for cyber-enabled attack.
- 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.
- Focuses on **engineers and technicians**, and provides a framework for cybersecurity education, awareness, and accountability.
- Aims to engender a **culture of security** aligned with the existing industry safety culture.




Concept Development
CIE-enabled OT Cybersecurity Risk Mitigation
Transition, Operations, and Maintenance
Requirements Engineering
Test and Evaluation
System Architecture
Systems Integration
System Design and Development

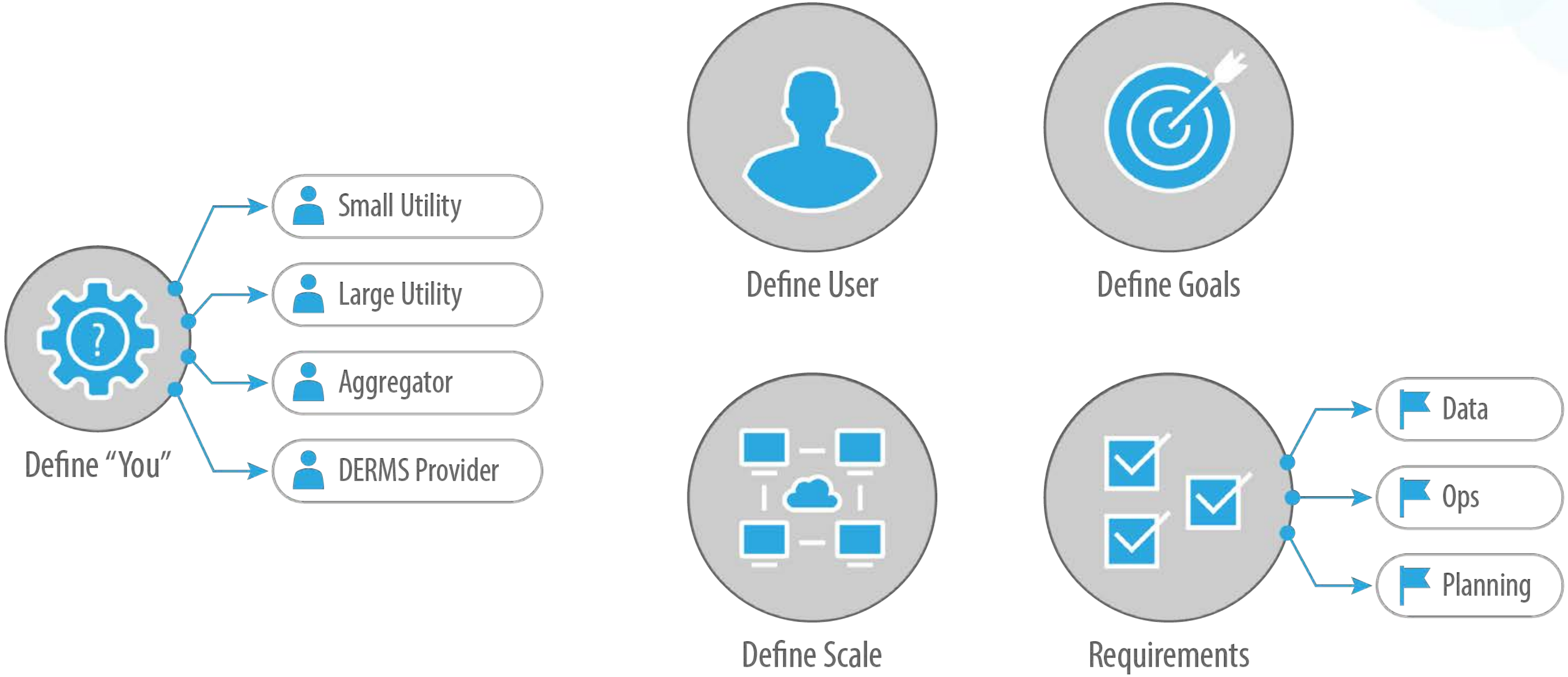
Cybersecurity risk mitigations are **more effective and efficient** when applied here…

…but are usually applied **here**.

Framework Design Principles: *Getting to Yes*

- Consequence-driven
- 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

Step 1: *Readiness Assessment*



Define "You"

- Small Utility
- Large Utility
- Aggregator
- DERMS Provider

Define User

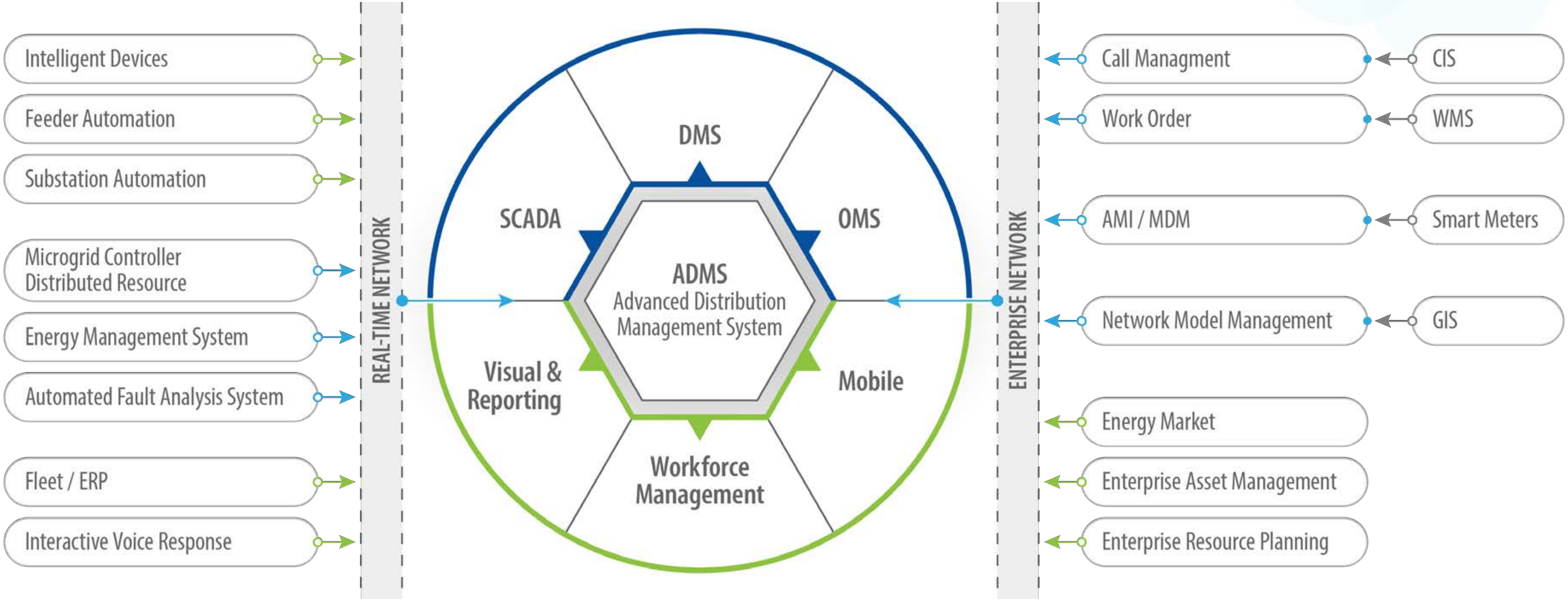
Define Goals

Define Scale

Requirements

- Data
- Ops
- Planning

Test Case 1: *ADMS*



Idaho National Laboratory

Step 2: Assess Consequence *(Good and Bad)*

What is the purpose of the proposed system?

How does it support the org?

What system processes exist for this function?

What system processes if they fail or operate incorrectly, will cause the purpose to fail?

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?

What short-term outcome is needed from this application (metrics for success)?

Net zero targets

Cost reduction

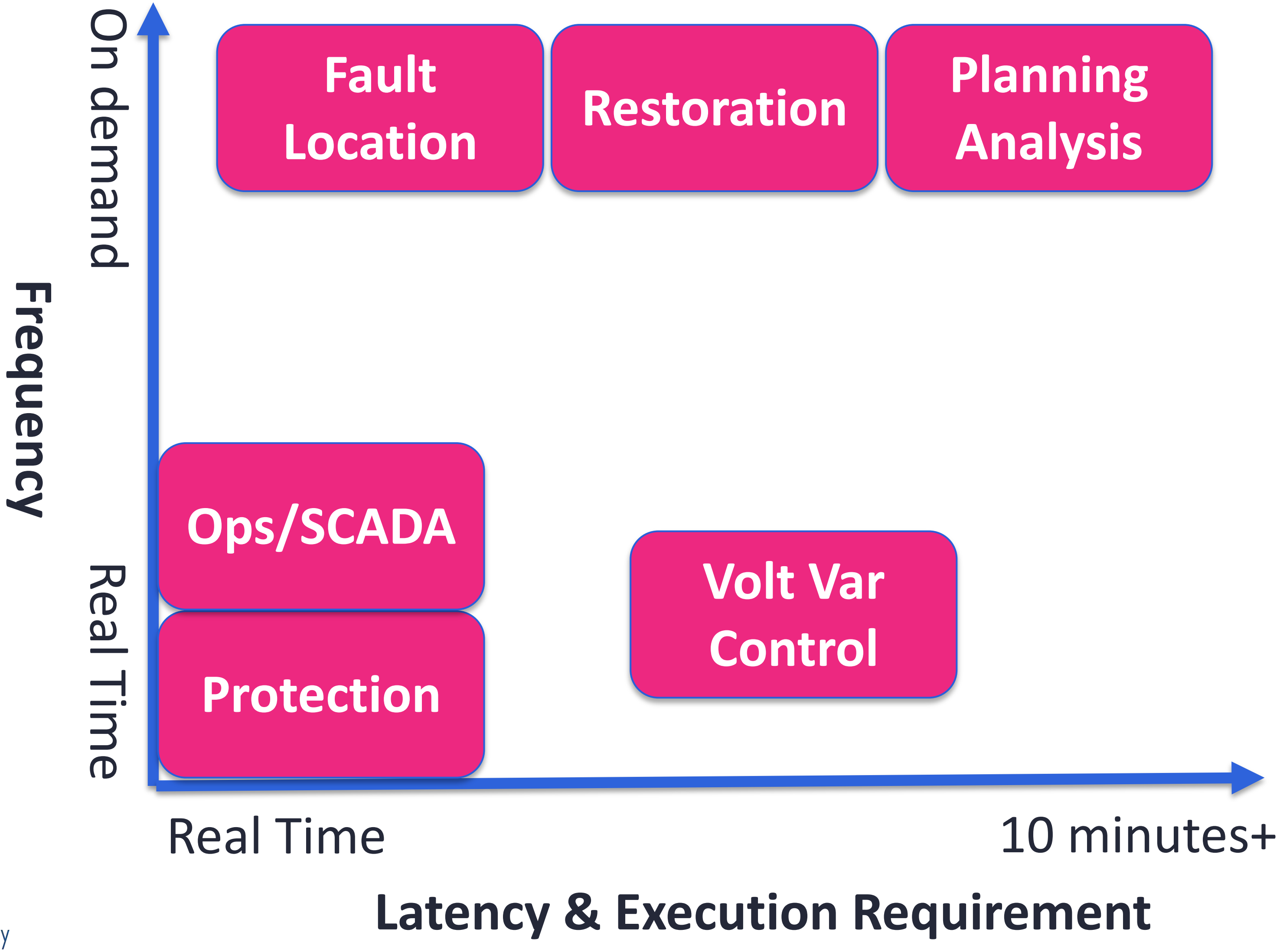
Improve security.

What consequences are from failure or unexpected operations?

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

What happens if multiple consequences at once?

Consequence and Benefit Assessment: Application Requirements



Industrial
Controls
Timing Matters

How do we rank application frequency and execution time for potential engineering controls?

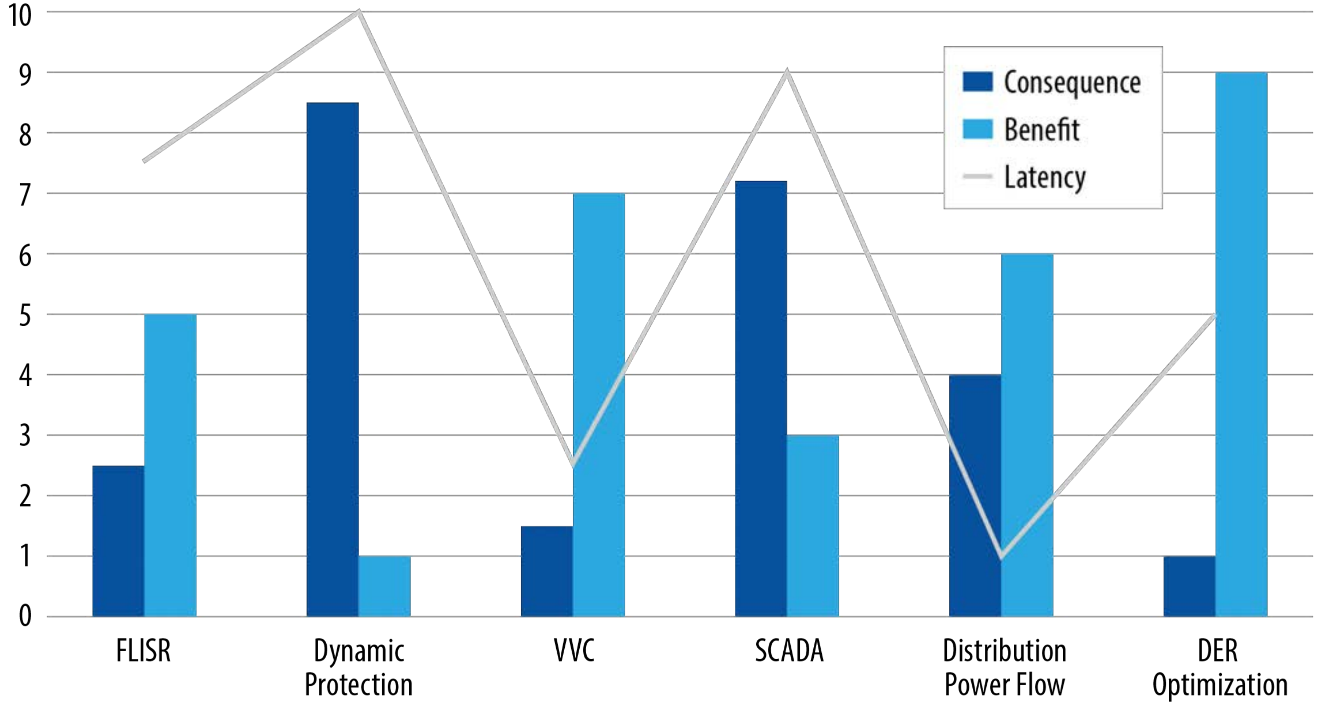
Score and Rank Consequences

What criteria and priority?

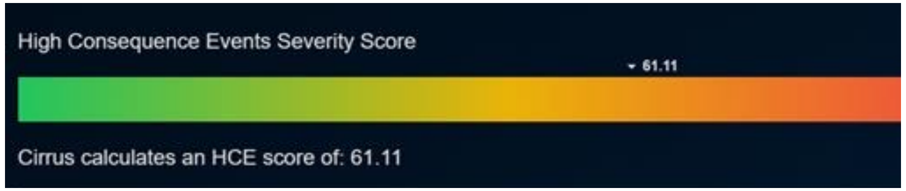
- Scale of Low, Medium, or High based on input to the *Who am I* section.

Criteria	None	Low (1)	Medium (3)	High (5)
Area/Load Impact (3)		Loss of failure to service firm load of less than XMW	Loss of failure to service firm load between X+1 and Y MW	Loss of failure to service firm load greater than Y + 1 MW
Duration (3)		Return of all service in less than 1 day (inability to serve firm load) (or) supply outage for less than 1 week	Return of all service 1–5 days (inability to serve firm load) (or) supply outage for 1 wk – 1 month	Return of all service >5 days (inability to serve firm load) (or) supply outage >1 month
Safety (4)		Risk onsite	Definite safety risk offsite	LOL Potential
Cost (1)		Significant but can recover	Multiple years to financially recover	Trigger of liquidity crisis/potential bankruptcy

Evaluation and Ranking

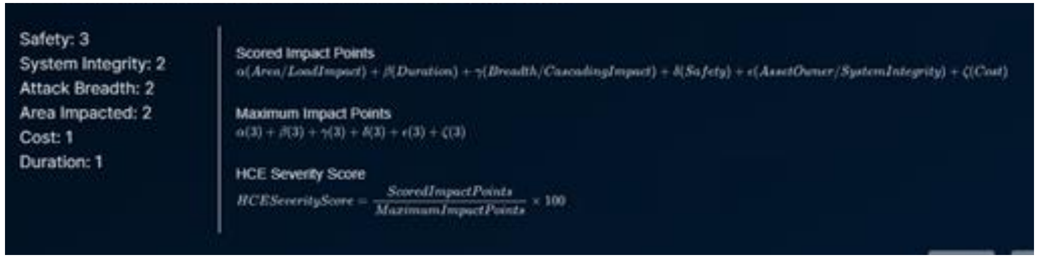


1. Highest priority applications
2. Pros and cons
3. Understanding of technical need initially
4. Framing thoughts for solutions.



High Consequence Events Severity Score

Cirrus calculates an HCE score of: 61.11



Safety: 3
System Integrity: 2
Attack Breadth: 2
Area Impacted: 2
Cost: 1
Duration: 1

Scored Impact Points

$\alpha(Area/LoadImpact) + \beta(Duration) + \gamma(Breadth/CascadingImpact) + \delta(Safety) + \epsilon(AssetOwner/SystemIntegrity) + \zeta(Cost)$

Maximum Impact Points

$\alpha(3) + \beta(3) + \gamma(3) + \delta(3) + \epsilon(3) + \zeta(3)$

HCE Severity Score

$$HCESeverityScore = \frac{ScoredImpactPoints}{MaximumImpactPoints} \times 100$$

Step 3 – 8: Solutions Assessment

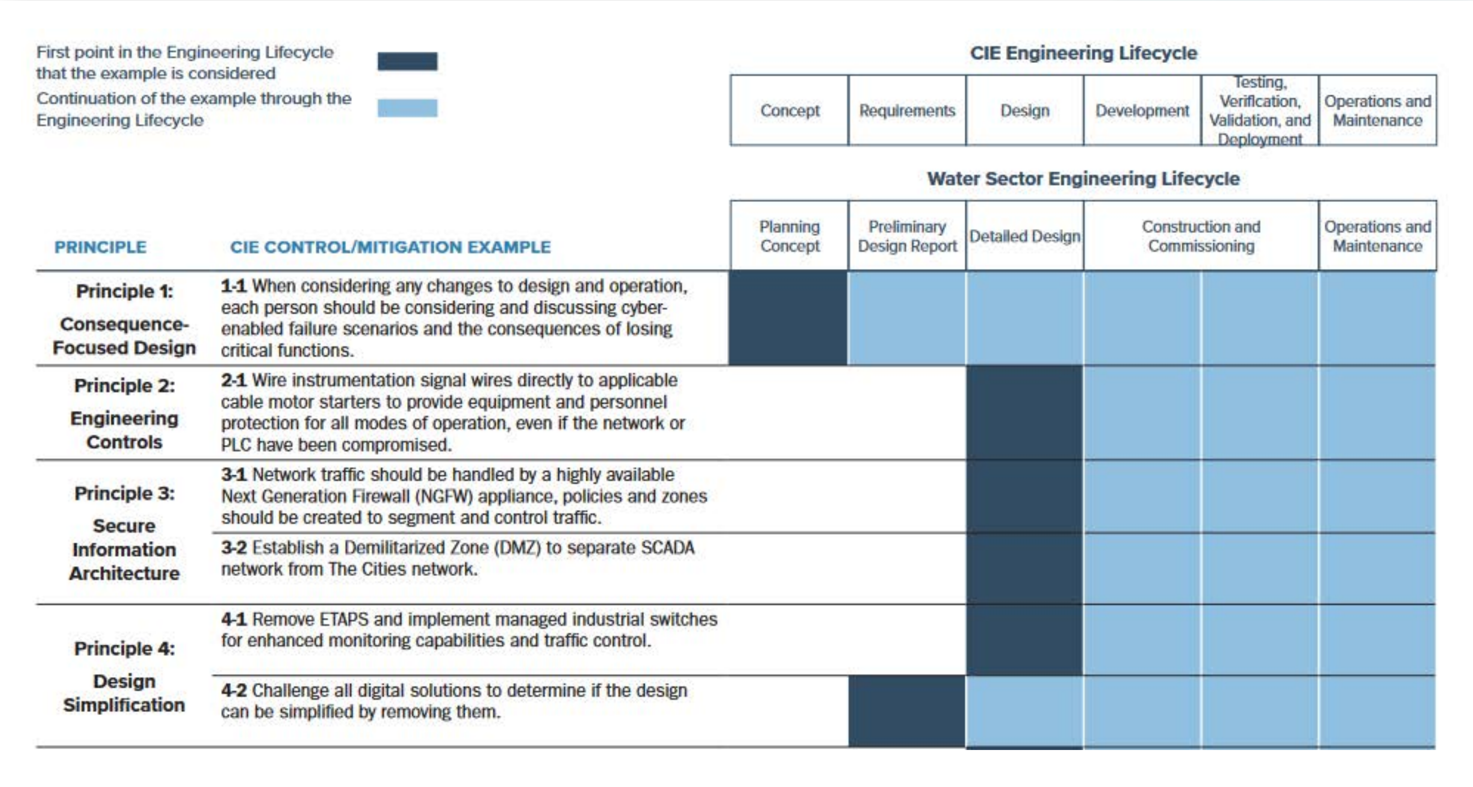
- Engineering controls for the site for cost/consequence.
- Secure information and digital asset management evaluation.
  - Data citizenship, consent on movement, type of cloud.
- Simplification and interdependency
  - Data flows: GIS example.
  - Data policy development, segmentation, data classification.
  - Redundancy and failover, required length of data storage.
- Secure supply chain and DAA
  - Do you have an asset inventory (if no – provide tools)?
  - Cloud supply chain questions.

Step 3 – 8: Solutions Assessment *(continued)*

- Planned resilience modeling
  - What can be diminished in operation and for how long
  - Prioritization of applications
  - What needs hybrid or non-cloud solutions (look at the consequences).
- Current security posture, resilient layered, and active defense
  - Monitoring
  - Staffing
  - Training
  - Compliance.
- Culture
  - Training and responsibility.

Engineering Case Study:
Water and Wastewater Utility

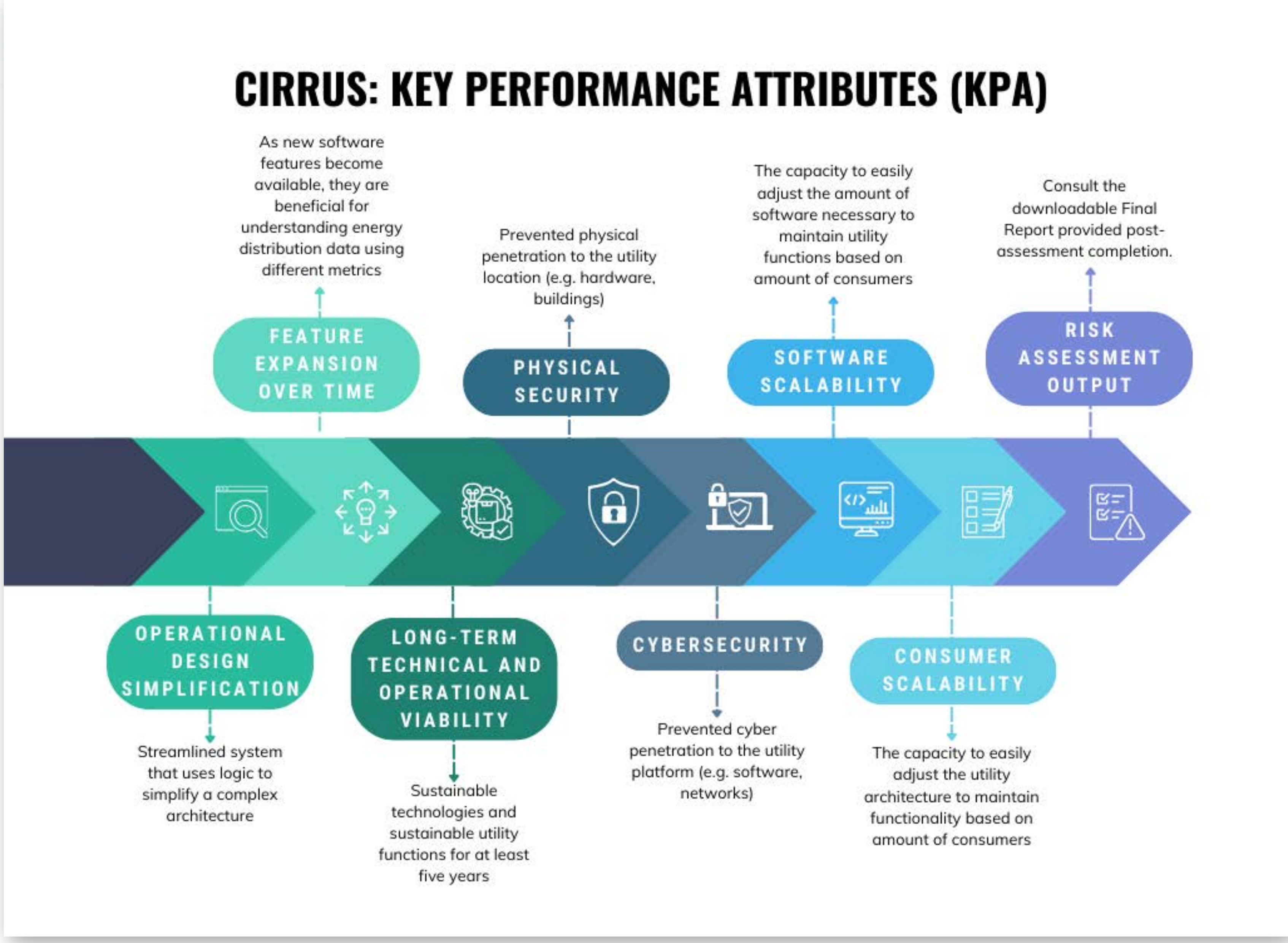
- Serves 500,000 and ~100 square miles
- Since 1990, has deferred asset renewal to save money
- Attracts unwanted attention due to the decline in asset conditions
- Time for new investments, including application of CIE principles



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

Continuation of the example through the Engineering Lifecycle ▒

		CIE Engineering Lifecycle					
		Concept	Requirements	Design	Development	Testing, Verification, Validation, and Deployment	Operations and Maintenance
		Water Sector Engineering Lifecycle					
PRINCIPLE	CIE CONTROL/MITIGATION EXAMPLE	Planning Concept	Preliminary Design Report	Detailed Design	Construction and Commissioning		Operations and Maintenance
Principle 1: Consequence-Focused Design	1-1 When considering any changes to design and operation, each person should be considering and discussing cyber-enabled failure scenarios and the consequences of losing critical functions.	■	▒	▒	▒	▒	▒
Principle 2: Engineering Controls	2-1 Wire instrumentation signal wires directly to applicable cable motor starters to provide equipment and personnel protection for all modes of operation, even if the network or PLC have been compromised.			■	▒	▒	▒
Principle 3: Secure Information Architecture	3-1 Network traffic should be handled by a highly available Next Generation Firewall (NGFW) appliance, policies and zones should be created to segment and control traffic.			■	▒	▒	▒
	3-2 Establish a Demilitarized Zone (DMZ) to separate SCADA network from The Cities network.			■	▒	▒	▒
Principle 4: Design Simplification	4-1 Remove ETAPS and implement managed industrial switches for enhanced monitoring capabilities and traffic control.			■	▒	▒	▒
	4-2 Challenge all digital solutions to determine if the design can be simplified by removing them.		■	▒	▒	▒	▒



CIRRUS: KEY PERFORMANCE ATTRIBUTES (KPA)

OPERATIONAL DESIGN SIMPLIFICATION

Streamlined system that uses logic to simplify a complex architecture

FEATURE EXPANSION OVER TIME

As new software features become available, they are beneficial for understanding energy distribution data using different metrics

LONG-TERM TECHNICAL AND OPERATIONAL VIABILITY

Sustainable technologies and sustainable utility functions for at least five years

PHYSICAL SECURITY

Prevented physical penetration to the utility location (e.g. hardware, buildings)

CYBERSECURITY

Prevented cyber penetration to the utility platform (e.g. software, networks)

SOFTWARE SCALABILITY

The capacity to easily adjust the amount of software necessary to maintain utility functions based on amount of consumers

CONSUMER SCALABILITY

The capacity to easily adjust the utility architecture to maintain functionality based on amount of consumers

RISK ASSESSMENT OUTPUT

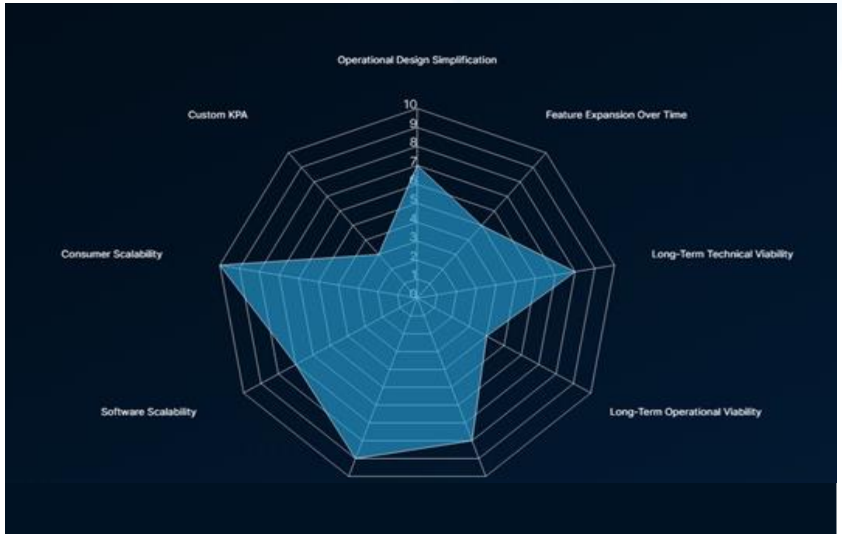
Consult the downloadable Final Report provided post-assessment completion.

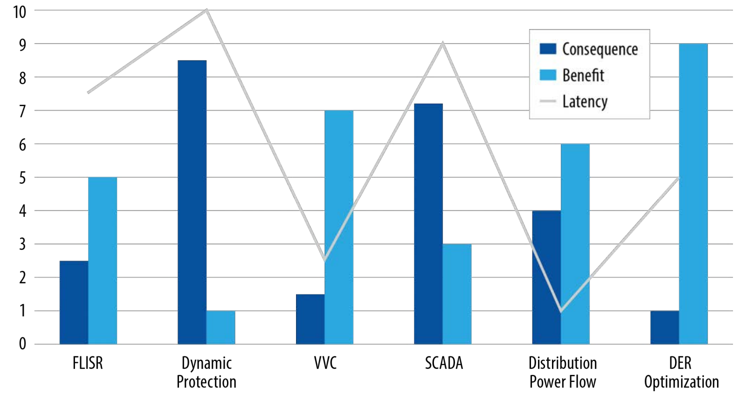
Output: *So You Did the Framework, What Do You Get at the End?*

Cloud Solution Utilities: your use case

- **Infrastructure Evaluation:** audit existing systems for seamless cloud integration
- **Benefits:** (e.g., efficiency, scalability)
- **Risk Areas and Consequences:** (e.g., cyber threats, data breaches)
- **RFP Guideline**

- **Key Guidelines for Cloud Integration:** (e.g., infrastructure evaluation, regulatory compliance, workforce capability, etc.)
- **Cost-benefit Analysis:** analyze costs for justifying cloud migration investment
- **Workforce Capability:** equip your workforce for a smooth cloud transition
- **Path Forward:** strategize your path with informed decision-making





Apply

Today:

- Consider **interdependent consequences and benefits** of a cloud deployment for electric grid controls and applications
- Develop understanding of framing cloud applications.

Tomorrow:

- **Apply lessons** learned and driven cybersecurity-informed frameworks.

Later:

- **Evaluate trends** in cloud deployment in infrastructure.

Key Takeaways

- Language matters
- Application of the solution matters – bulk security controls do not work
- Cyber-informed engineering and consequence-based approaches help get to a “yay or nay” quicker

Contact me: emma.stewart@inl.gov.