DUKE ENERGY®

BUILDING A **SMARTER** ENERGY FUTURE℠

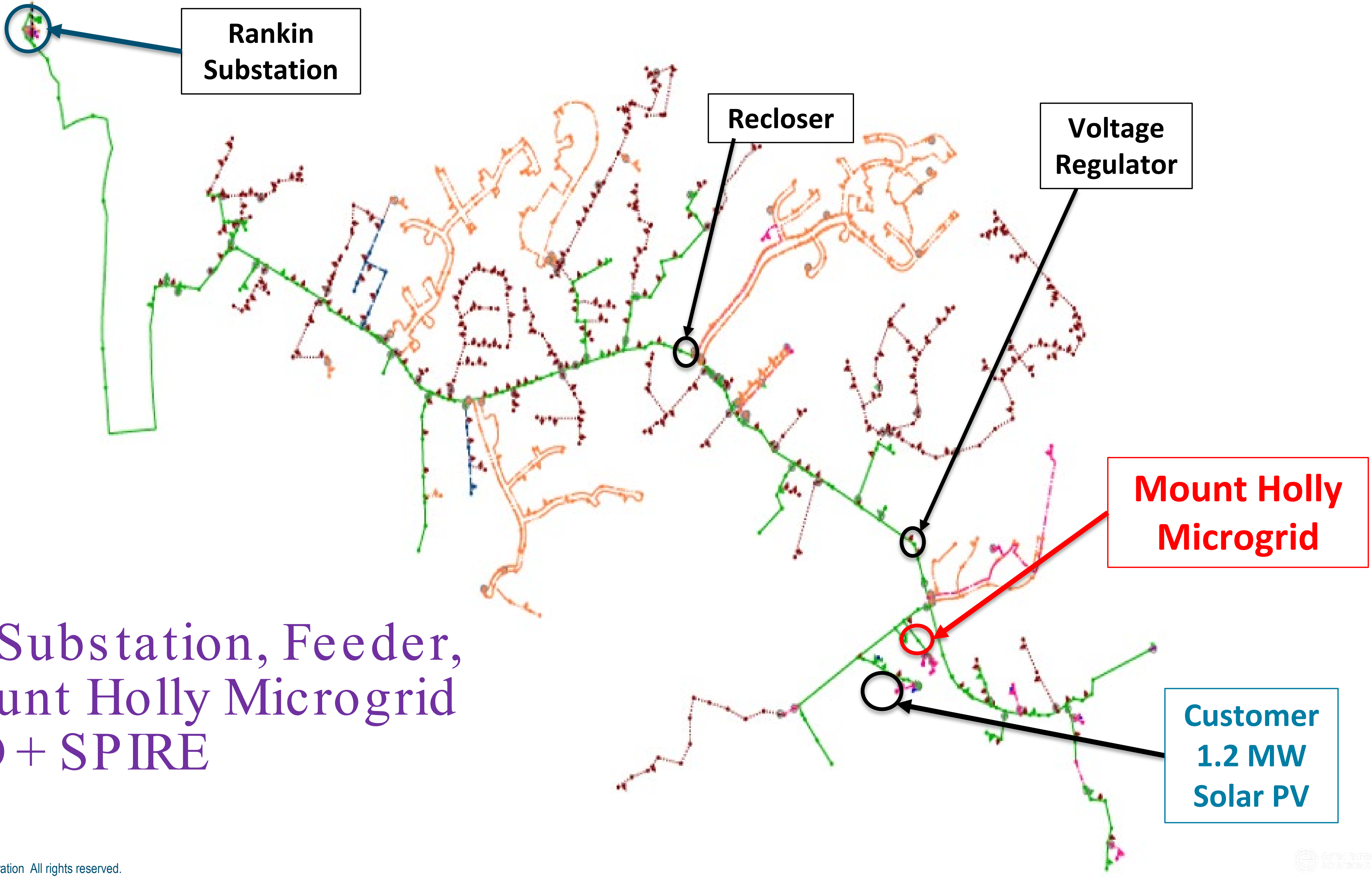
Zero-Trust Applications for the Grid (ZTAG)

CI/CD + SPIRE (Distributed PKI) --> Grid

David Lawrence - Emerging Technology

7/14/2022

Rankin Substation, Feeder, and Mount Holly Microgrid – CI/CD + SPIRE




Mount Holly – Microgrid Test Lab
Autonomous Energy System - 1

Source Hydropanels

AES - 2

Lab Building

Bay 4 – HIL Simulation

Bay 5 DC Microgrid

THE FUTURE IS DC

Bay 5 DC Microgrid – Outside: Solar, PCS, EV Charger


DC Home
AES - 4

Microgrid Feeder Extension – 1.5 mile distribution test circuit

The Path for Distributed Security at Duke Energy

There have been many successes for Distributed Intelligence to date and distributed security is the latest accomplishment

Defense in Depth

Substation Hack

TPM2.0

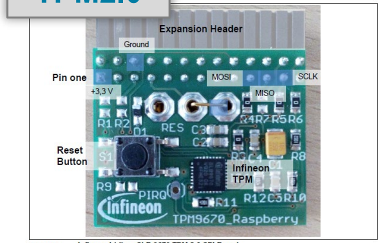
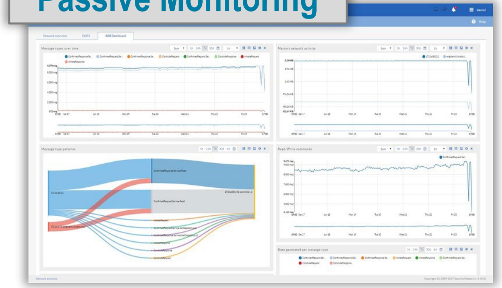
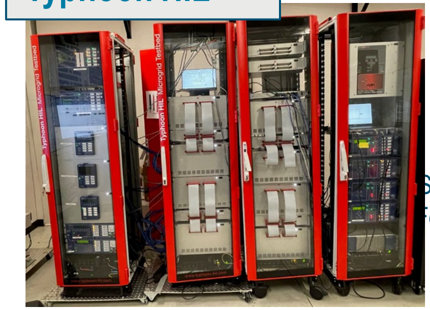


Figure 2 Infineon Iridium SLB 9670 TPM 2.0 SPI Board

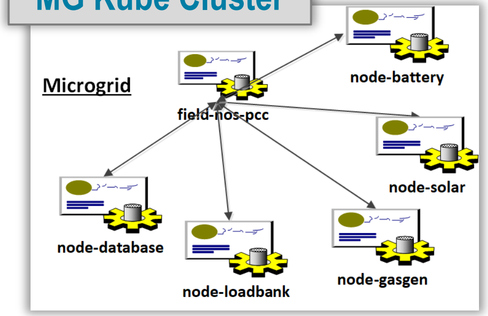
Passive Monitoring



Typhoon HIL



MG Kube Cluster



- 2013 — R&D Efforts Begin
- 2014 — ICS Security DOE Demo at SANS
- 2016 — Distributed PKI Security efforts launch (MQTT)
- 2017 — Silent Defense MTH Lab Deployment
- 2018 — Trusted Platform Module (TPM) prototyping
- Silent Defense Bake-off leads to Substation rollout
- Top 6 DI Cyber use cases
- MTH Lab OpenFMB Secure Demo
- OpenFMB Secure on MTH Microgrid
- Rankin DI PoC Kick-Off
- OpenFMB Secure on HIL Rankin Simulation
- DI Hardware Pen testing
- Segment Feeder

2013 2014 2015 2016 2017 2018 2019 2020 2021 2022

● Complete ○ In-Process / Planned

Why pursue ZTAG?

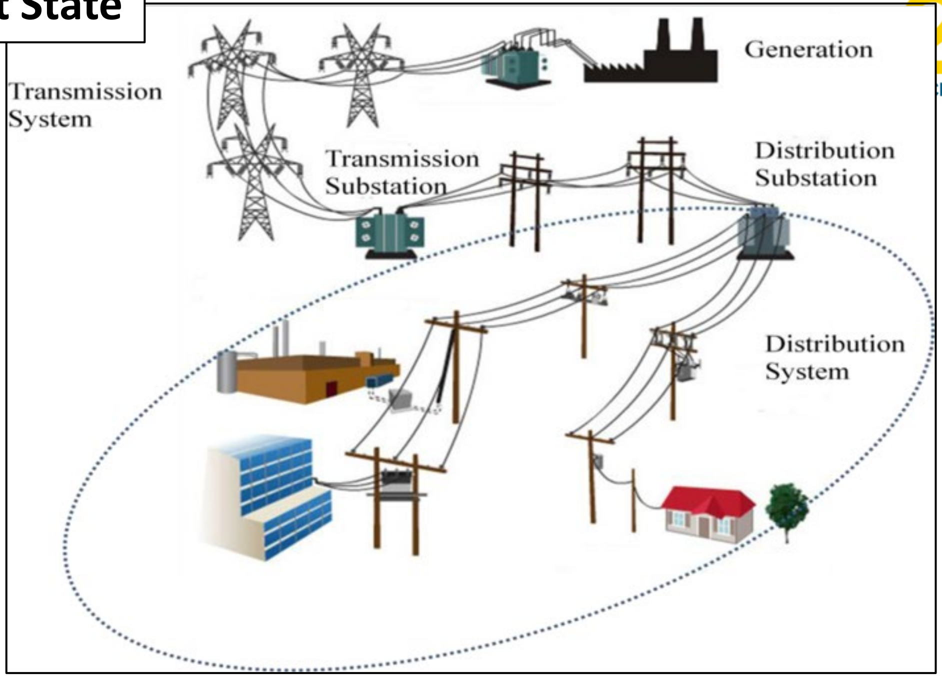
The grid of the future must be designed, secured, and operated differently to mitigate increasing vulnerabilities

1. Zero-trust approach leveraging identity and mutual transport layer security (mTLS)
2. Deploying and patching remote OT applications
3. Enabling and demonstrating end-to-end live Situational Awareness
4. Configurable abstraction layers and common interfaces drive interoperability
5. Hybrid Cloud / On-Prem microservices

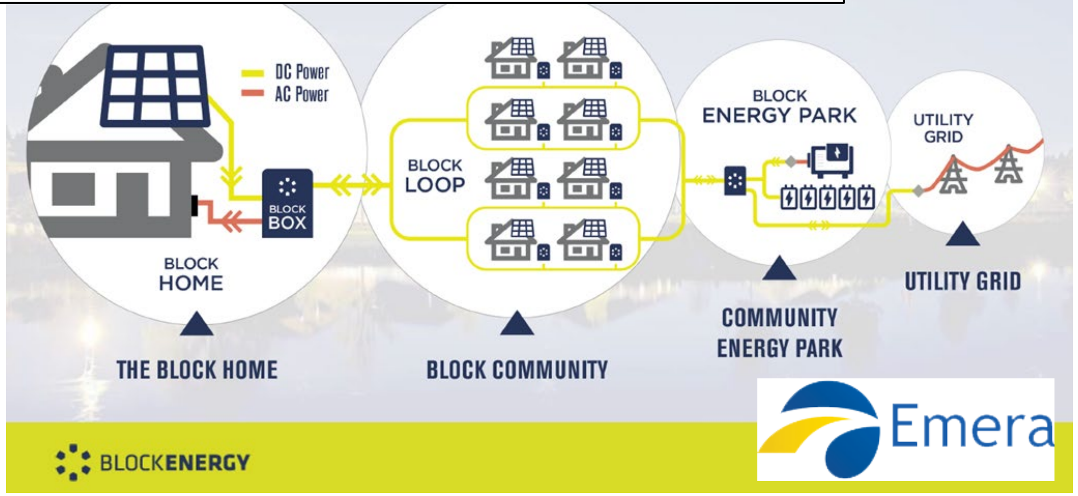
Key Opportunities in Grid Operational Technologies (OT) Cybersecurity (ZTAG coming soon)

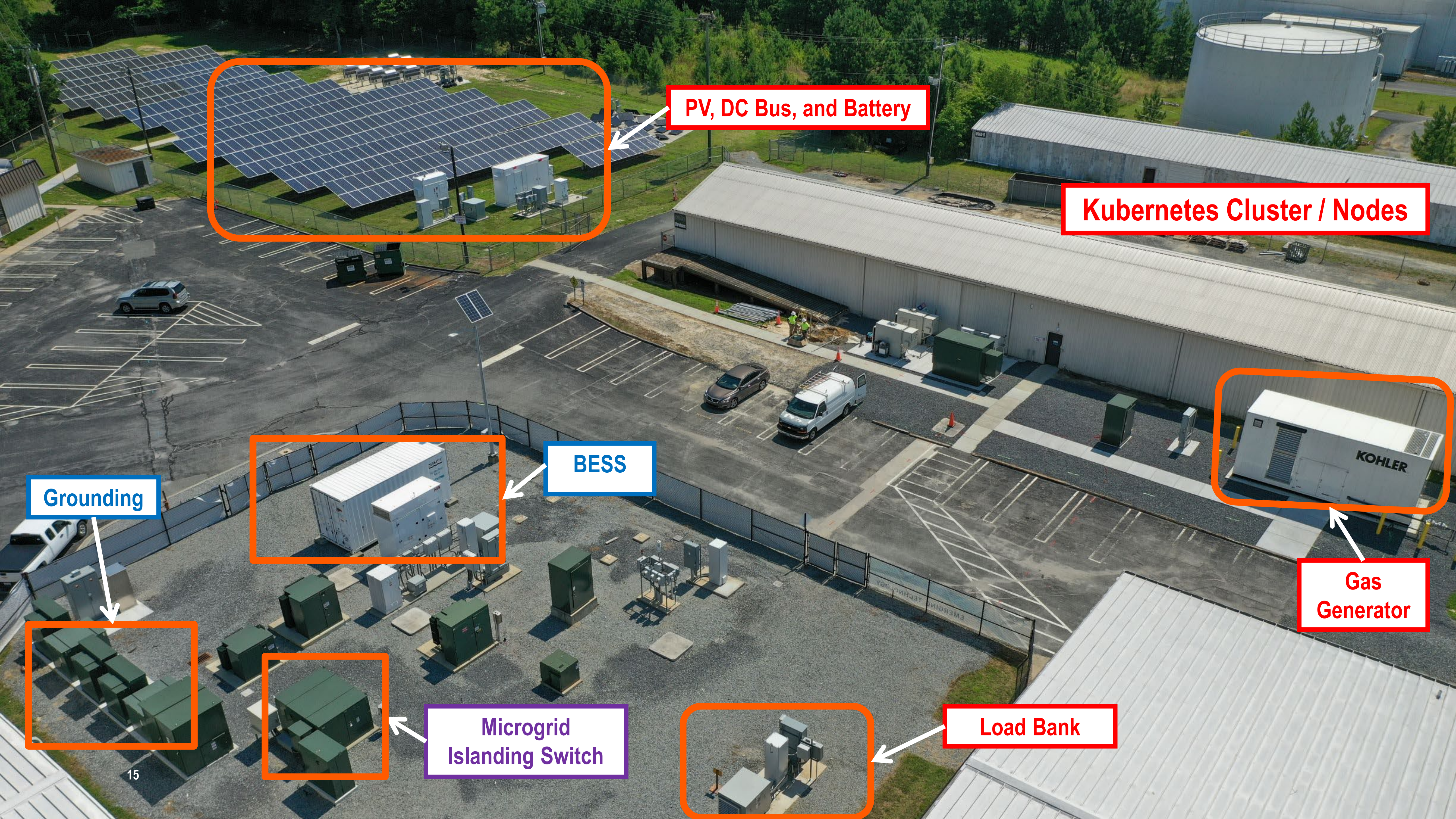
- No Cryptographic Device Identity -> No "Zero-Trust" Implementations (Legacy unsecured protocols)
- Limited Situational Awareness
- Grid Device Patching and New App Deployment is next to impossible
- Slow Adoption of DAF (Distributed Autonomous Function) Concepts
  - Abstraction Layers and Interoperable Interfaces
  - Distributed Intelligence (DI) and Analytics
  - Best Use of Cloud Services
- Non-Standard Standards
- Slow Build-up of ICS (Industrial Control System) Cyber Programs
  - OT Skills / Knowledge Missing in IT and Cyber
  - IT/Cyber Skills Missing in OT

Current State

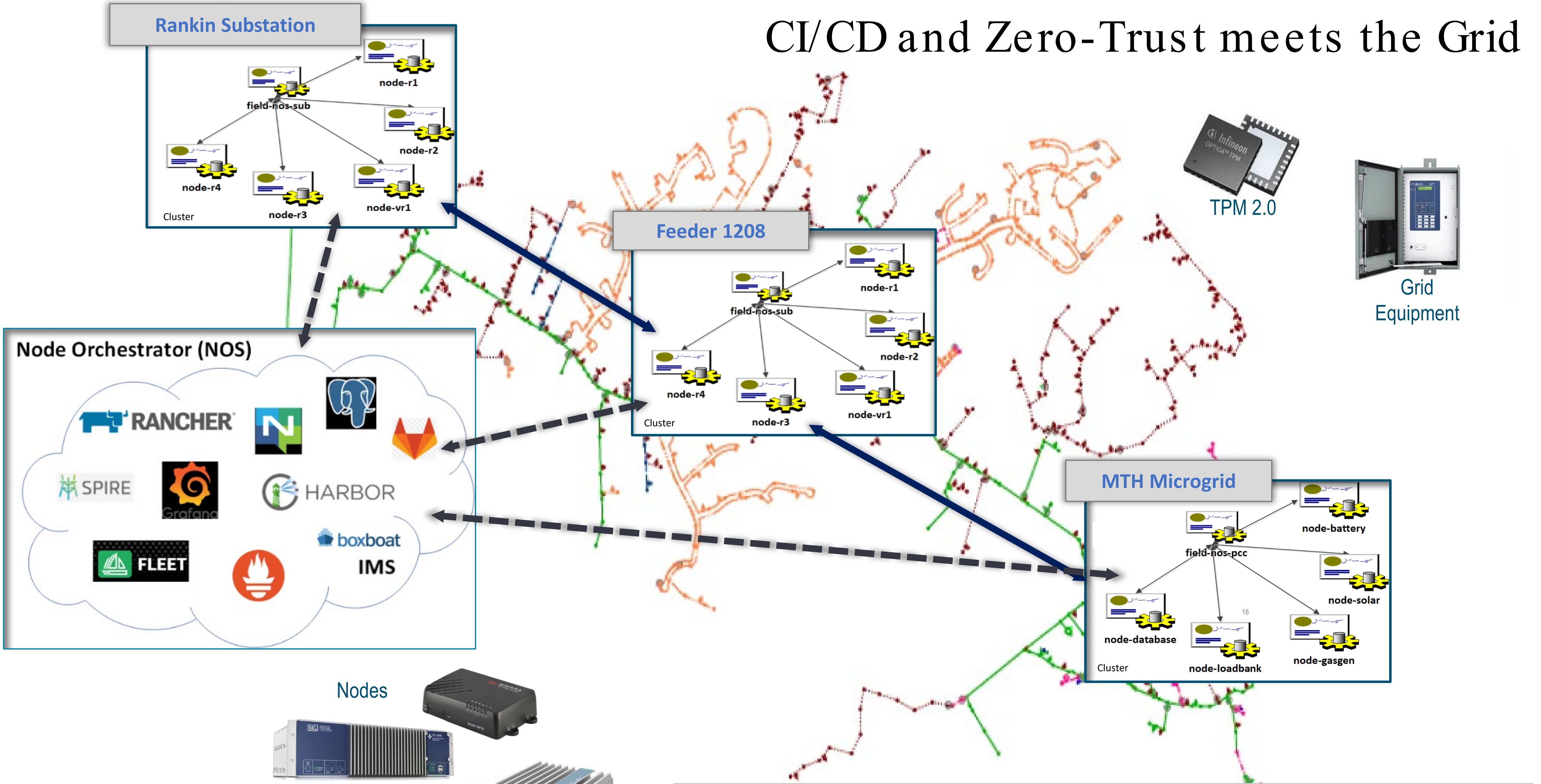


Future Grid – Distributed, Autonomous, Virtual Power Plants




PV, DC Bus, and Battery
Kubernetes Cluster / Nodes
BESS
Grounding
Gas
Generator
KOHLER
Microgrid
Islanding Switch
Load Bank

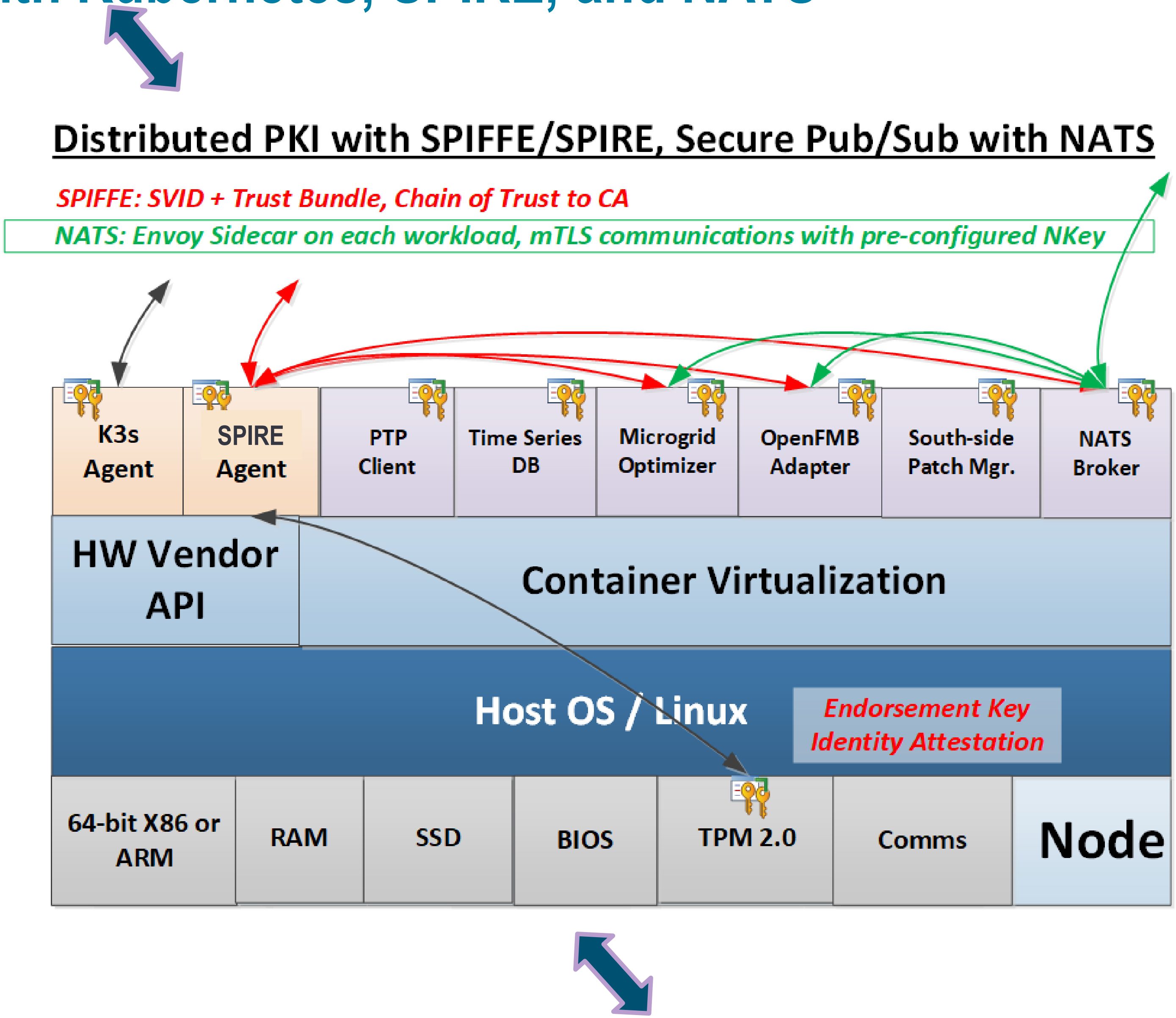
CI/CD and Zero-Trust meets the Grid



**The Node Orchestrator can be deployed in the cloud or on-prem*

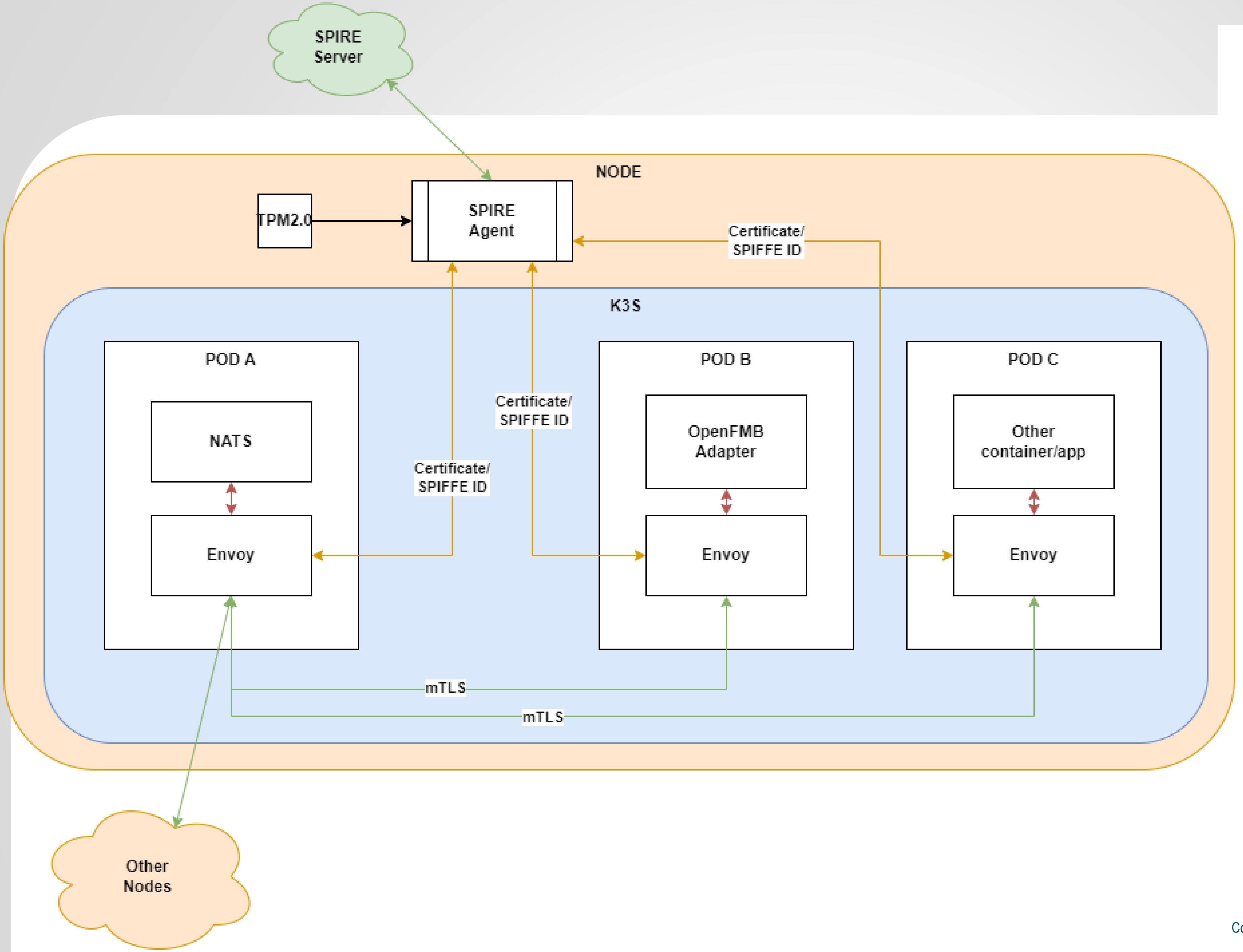
Future-proof the North-side with Kubernetes, SPIRE, and NATS

- Only **trusted hardware** can effectively join the network.
- Only **trusted applications** can run on trusted hardware.
- Trusted apps running on Trusted HW get certificates **ensuring both parties are trusted when communicating.**
- Solution validates trusted apps and hardware by **refreshing short-lived certificates and keys**.
- Edge Devices will **evolve and adopt the Node architecture with K3s, SPIRE, its App, and NATS.**

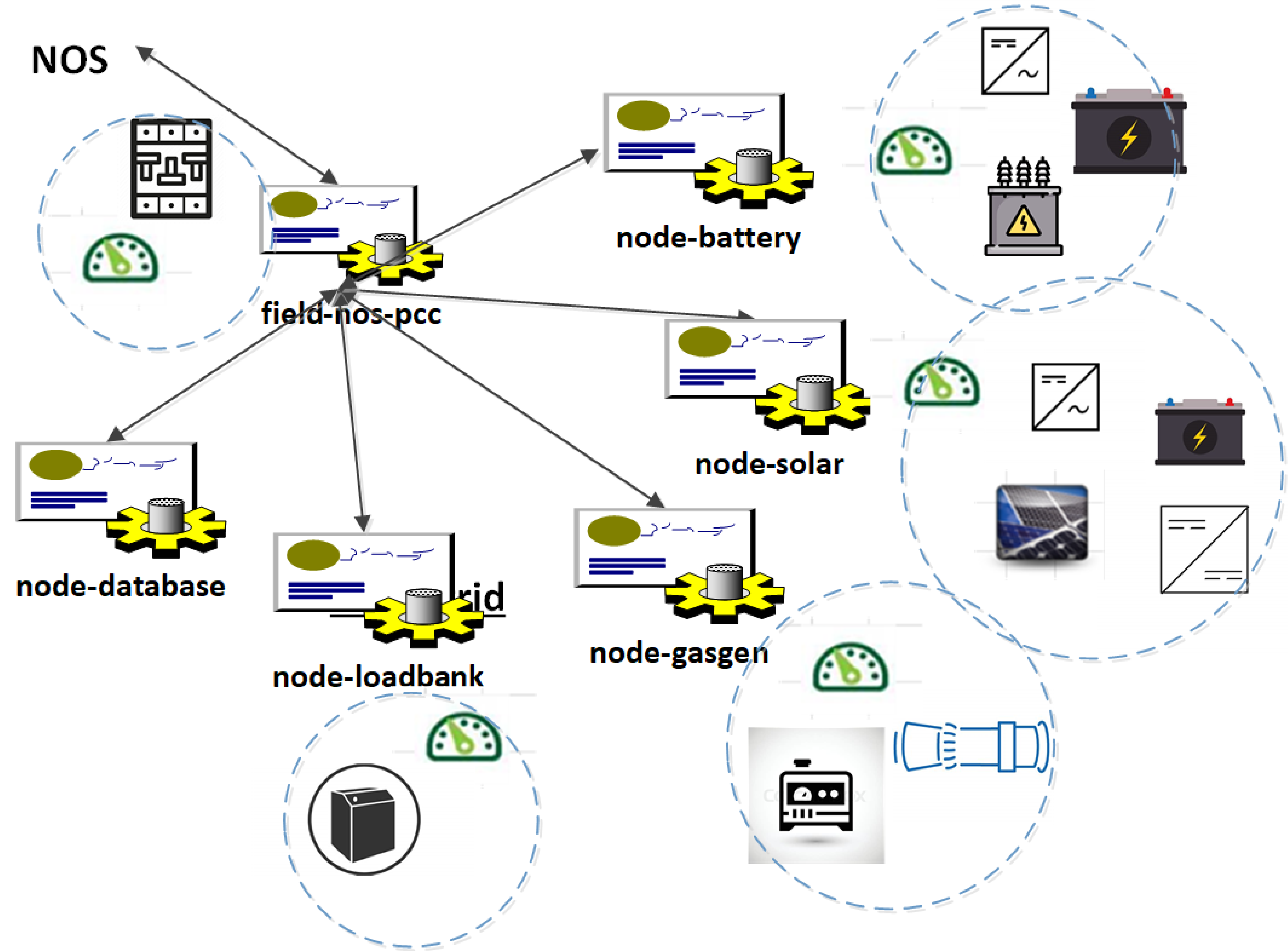


Hide South-side legacy devices and insecure protocols

Abstracting Security with Envoy



Inside the Microgrid Kube Cluster



Key Outcomes

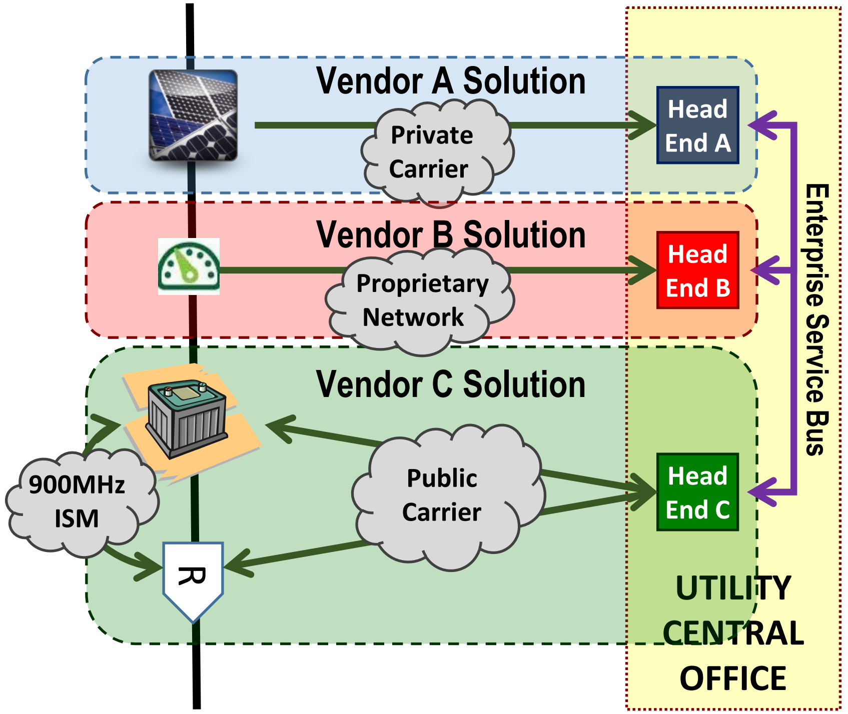
When wholly deployed the solution eliminates cybersecurity risk through a zero-trust approach to security

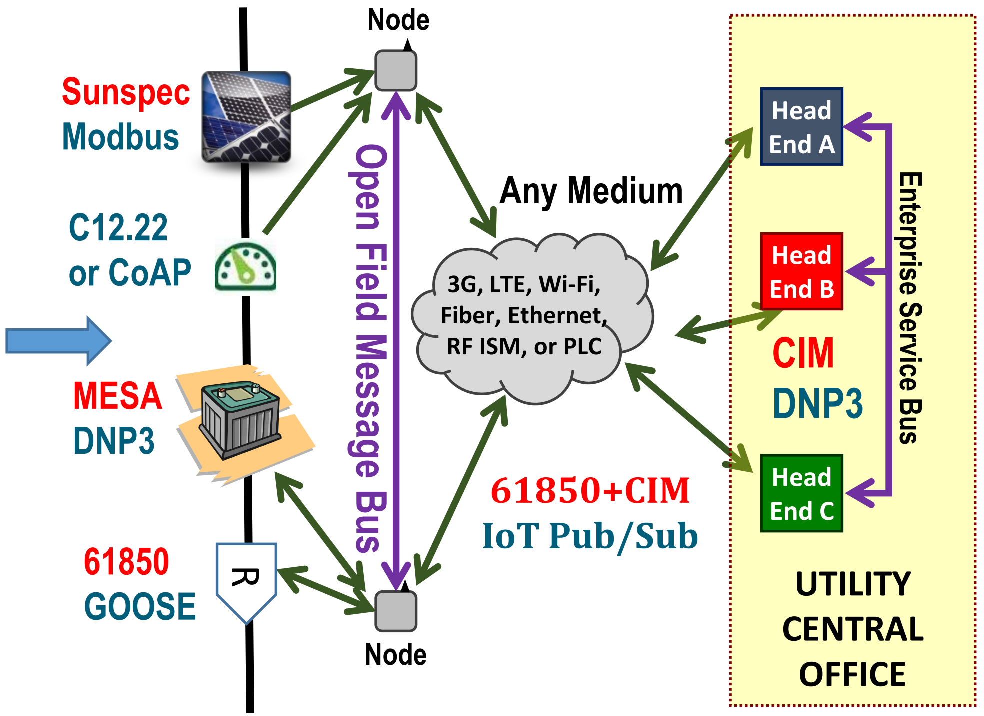
- Provides a Zero-trust environment
- Facilitates deploying and patching remote grid applications
- Enables end-to-end live Situational Awareness
- Drives interoperability
- Integrates with legacy devices
- Secures peer-to-peer communications at the edge
- Enables Distributed Intelligence (DI) grid applications

Duke Energy: keeping the lights on so you can sleep peacefully!

"Working to Secure the Grid, One Distributed Autonomous Function at a Time!"

Node Definition, Edge Compute…OpenFMB: Enabling DI





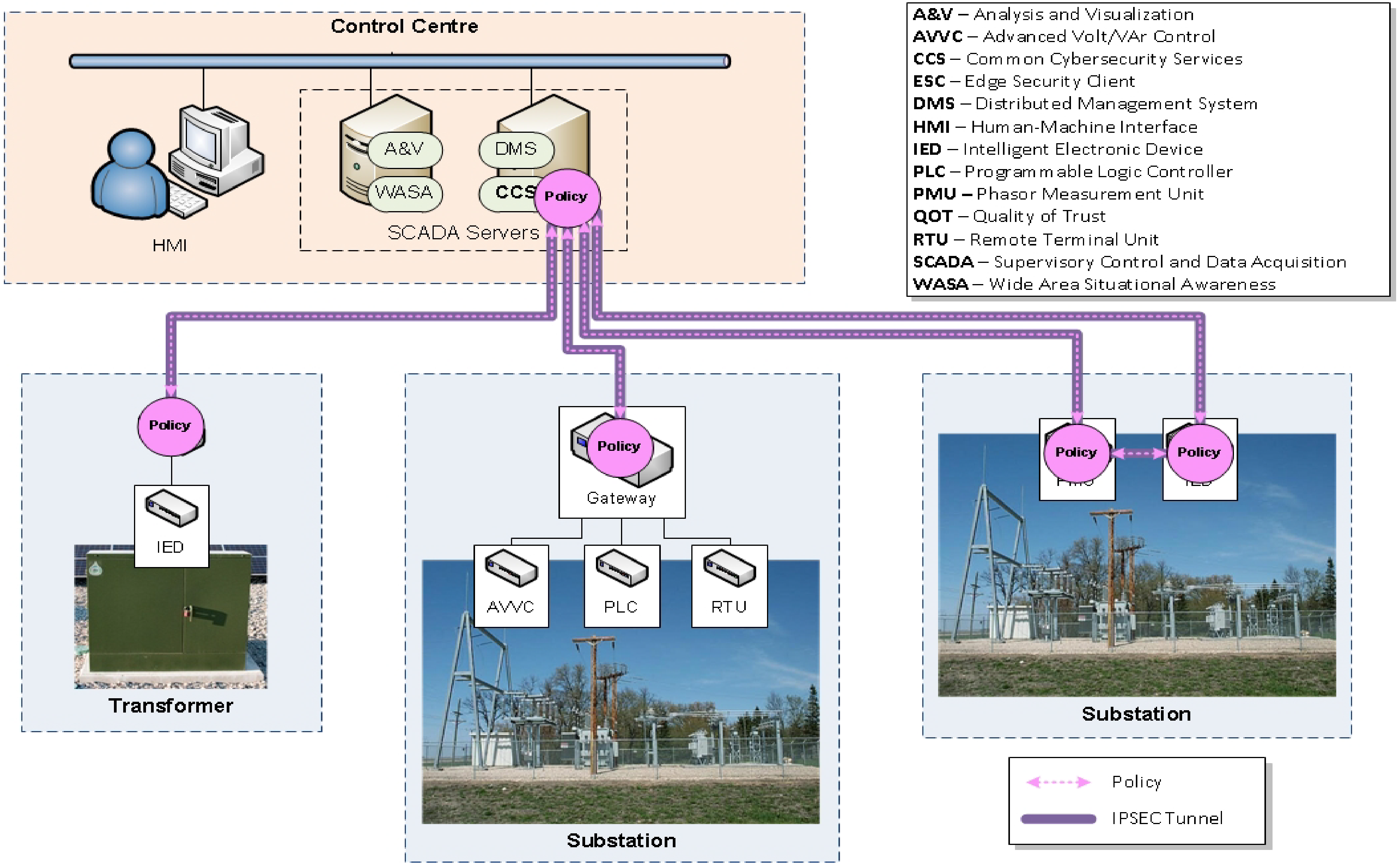
Key Observations:

1. Single-Purpose Functions
2. Proprietary & Silo'ed systems
3. Latent , Error-prone Data
4. OT/IT/Telecom Disconnected
5. **No Field Interoperability!**

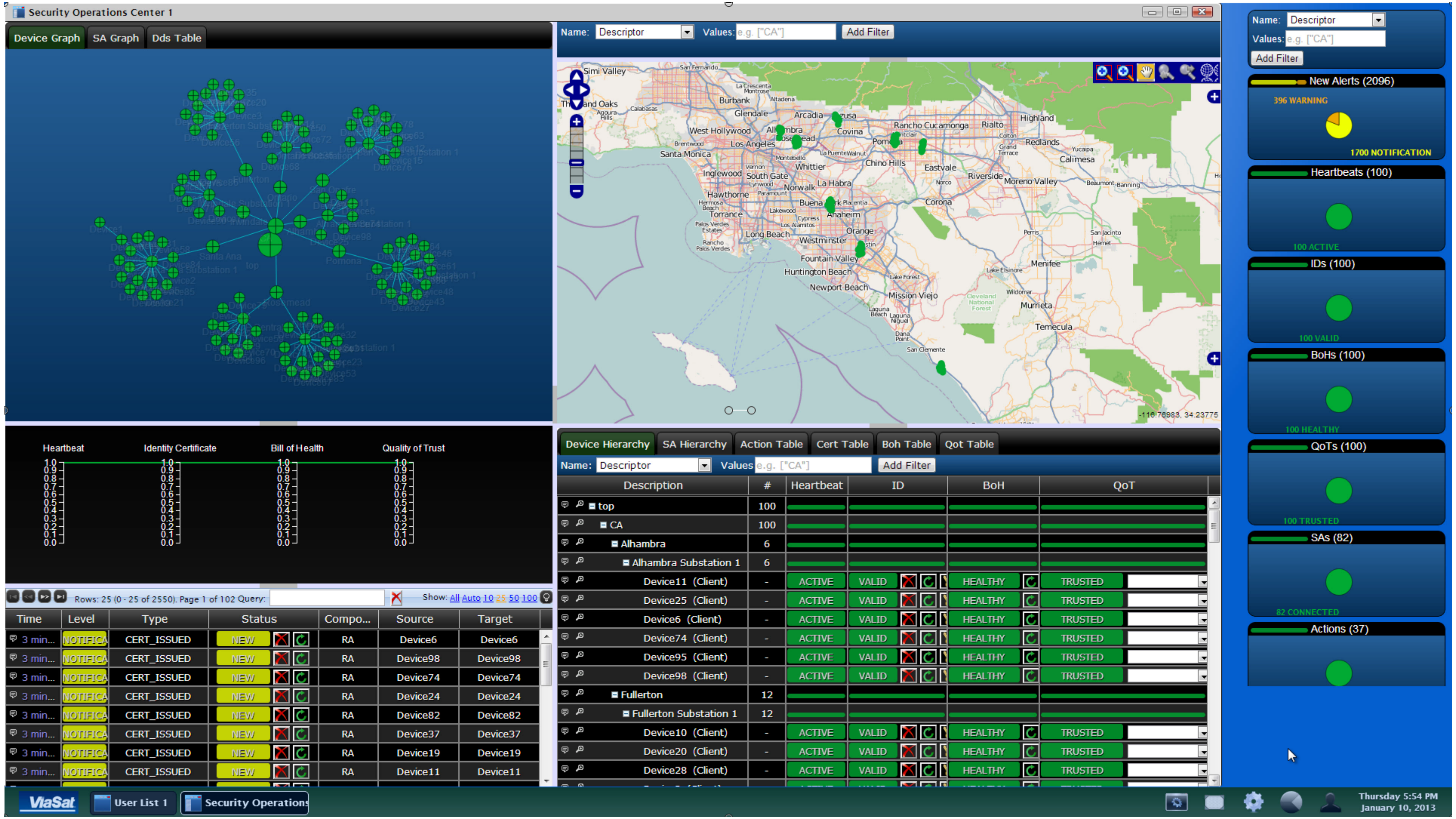
Key Observations:

1. Multi-Purpose Functions
2. Modular & Scalable HW&SW
3. End-to-End Situational Awareness
4. OT/IT/Telecom Convergence
5. **True Field Interoperability!**

Policy Based Response to Sensor Inputs / Grid Behavior



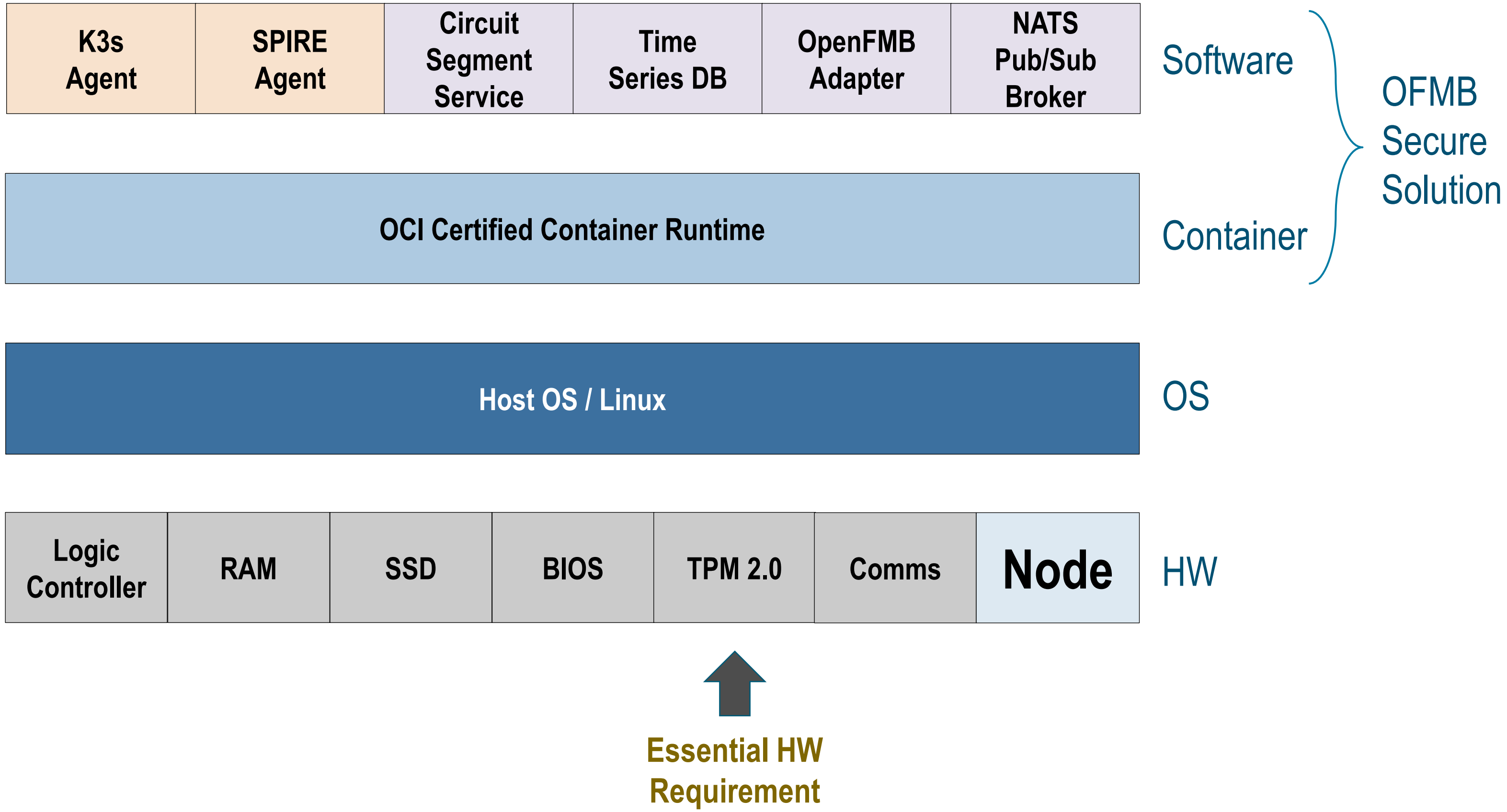
DOE FOA797 – Trusted Network Platform (TNP) Grid Security Visualization



ZTAG at its Core

ZTAG's architecture facilitates Container Orchestration and embeds Zero-Trust Security

- Only **trusted hardware** can effectively join the network.
- Only **trusted applications** can run on trusted hardware.
- Trusted apps running on Trusted HW get certificates and/or keys **ensuring both parties are trusted when communicating.**
- Solution validates trusted services and hardware by **refreshing short-lived certificates and keys**.



Microgrid Kube Cluster – Rancher View

pcc:
- envoy-spire-mutating-webhook
- helm
- k3s
- nats (leaf)
- nats-gateway
- openfmb-adapter
  - grounding breaker
  - islanding switch
- nats (server)

gen:
- k3s
- fleet
- nats (leaf)
- openfmb-adapter
  - micro-turbine
  - micro-turbine-breakers
- nats (server)

db:
- circuit-segment
- grafana
- nats (leaf)
- openfmb-adapter
  - historian
- postgres
- prometheus (for nats statistics)
- k3s

ess:
- nats (leaf)
- openfmb-adapter
  - abb-ess
- nats (server)
- k3s

load:
- nats (leaf)
- openfmb-adapter
  - ev-meter-1
  - ev-meter-2
  - load bank
  - load bank meter
  - load bank plc
  - shop meter
- nats (server)
- k3s

solar:
- nats (leaf)
- openfmb-adapter
  - sma-in
  - sma-out
  - solar-parker
  - traffic-light-inside
  - traffic-light-outside
  - weather-station
- nats (server)
- k3s

Functional Deployment Objectives

The 22 DI use cases could be associated with a set of four Functional Deployment Objectives.

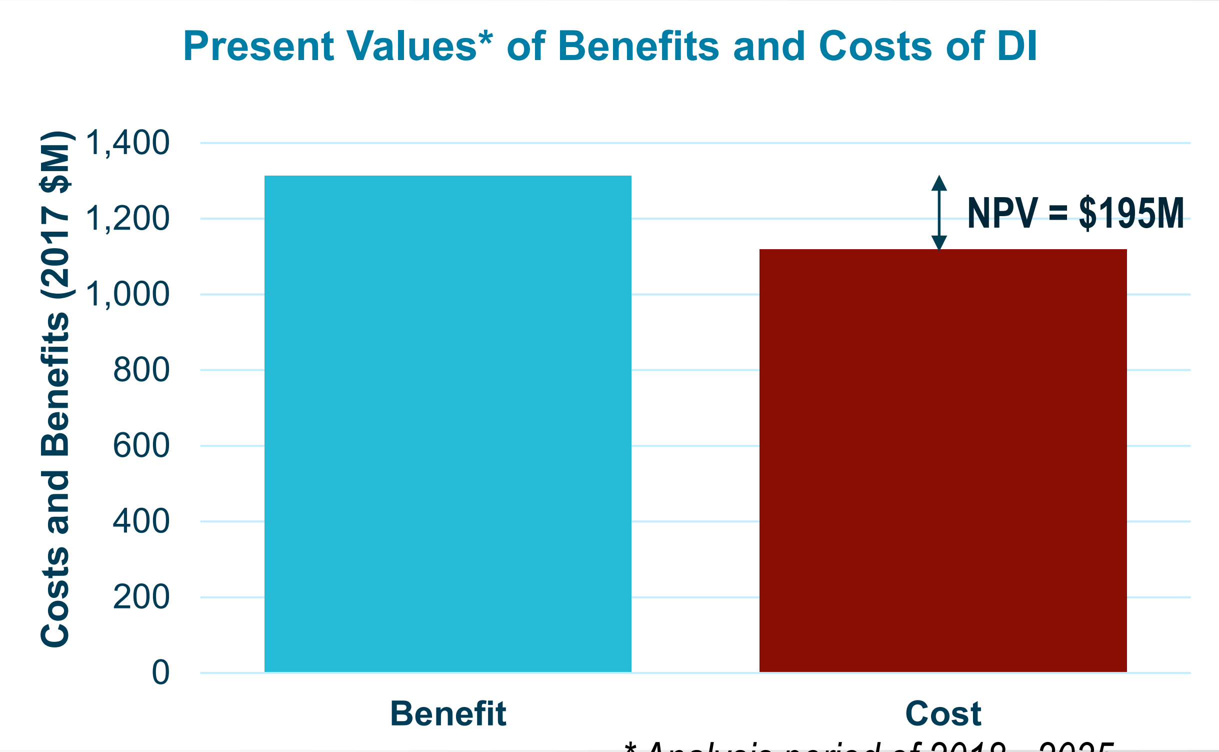
Use Case	Capacity Management	Voltage Management	DER Management	Utility Operations
DER Circuit Segment Management	✓	✓	✓	✓
Baseload Storage Monitoring/Mgmt.	✓		✓	
Peak Power Management	✓		✓	
DER Forecasting w/ Meters	✓		✓	
DER Forecasting w/ Weather Stations	✓		✓	
DER Optimization (Cust. Inverter)	✓		✓	
DER Optimization (DE Inverter)	✓		✓	
Demand Response Optimization	✓			
PCC Monitoring/Mgmt./Opt. (DE μgrid)	✓	✓	✓	
PCC Monitoring/Mgmt. (Cust. μgrid)	✓	✓	✓	
Volt/VAR Management	✓	✓	✓	✓
Grid Connectivity Discovery				✓
Remote Device Configuration			✓	✓
SCADA Point Aggregation			✓	✓
Enhanced COMS Network Ops. Status				✓
Improve Asset Maint. Practices				✓
Localized Protection Alarms & Events			✓	✓
Self Healing Radial Network			✓	✓
Solar Smoothing		✓	✓	
Solar Smoothing (+Battery)		✓	✓	
Inadvertent Island Detection			✓	
DER Integration & Interconnection			✓	

Overall Value of distributed intelligence (DI) to DEC

The analysis shows that DI technologies could provide a benefit-cost ratio of 1.17 to Duke Energy Carolinas (DEC) service territory.

- NPV = $195M
- Overall benefit present value = $1,315M
- Overall cost present value = $1,120M

→ **Benefit-Cost Ratio = 1.17**



** Analysis period of 2018 - 2035*