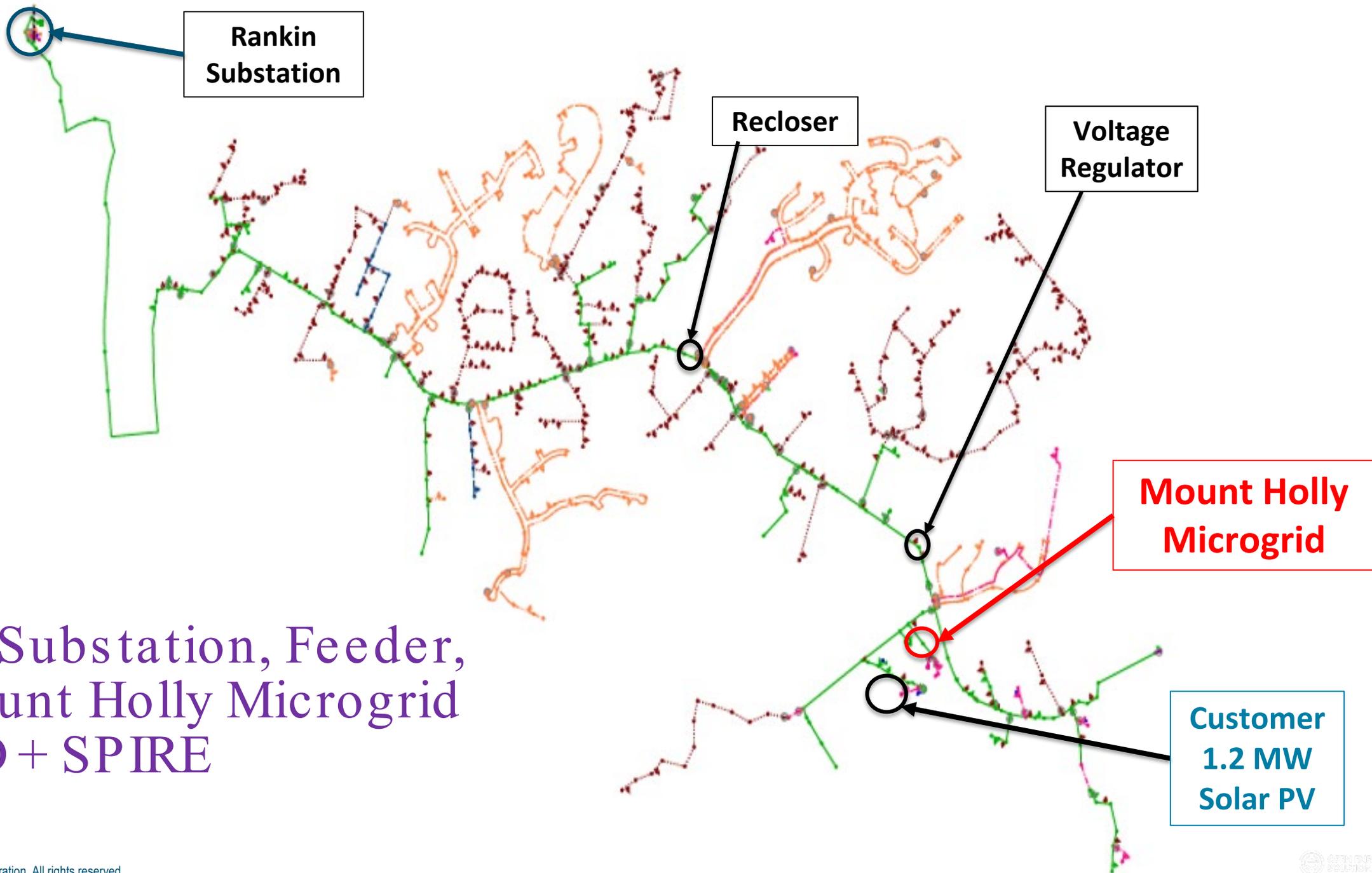




BUILDING A SMARTER ENERGY FUTURESM

Zero-Trust Applications for the Grid (ZTAG)

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



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

AJ EYKBRVEQ
PFR THEK V X N
T FUTURE K D B
D C I S N E D C T G
E J Y A B R V E Q D

THE FUTURE IS DC

AES - 3





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

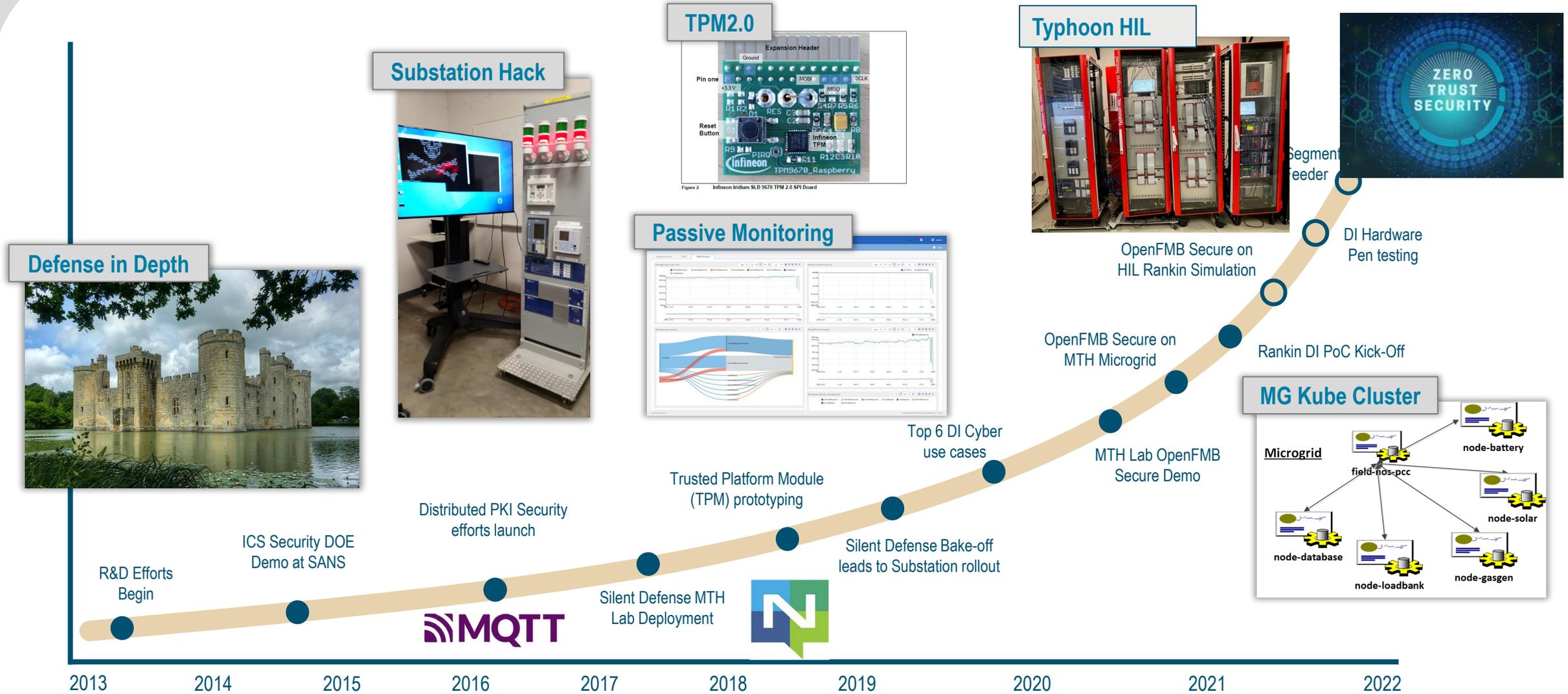


Microgrid Feeder Extension – 1.5 mile distribution test circuit



The Path for Distributed Security at Duke Energy

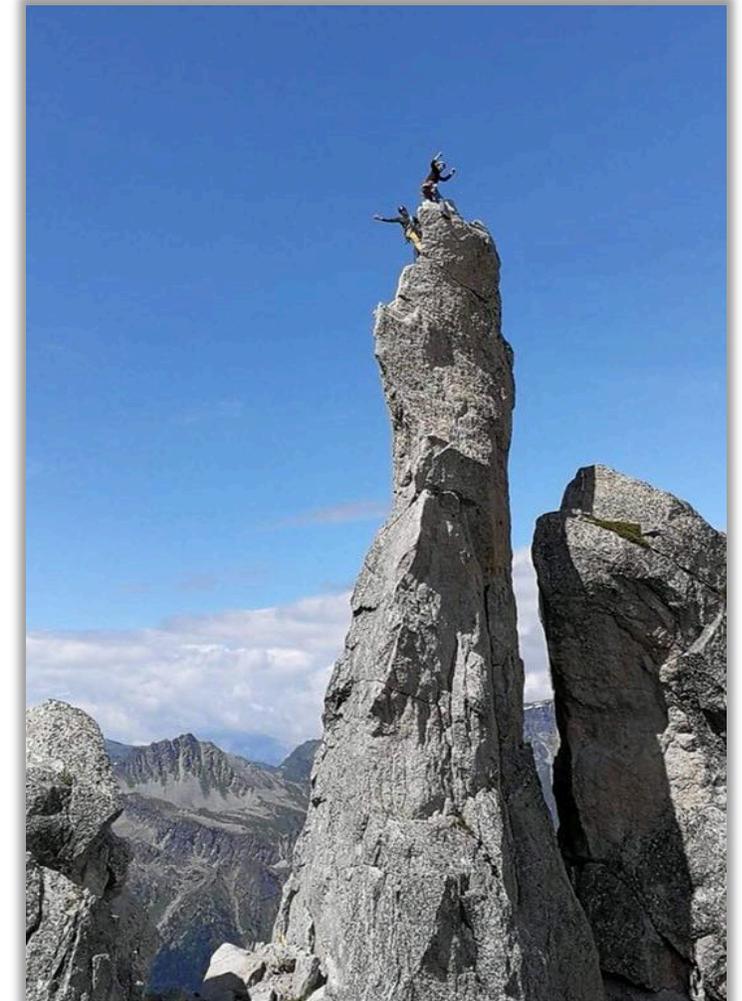
There have been many successes for Distributed Intelligence to date and distributed security is the latest accomplishment



Why pursue ZTAG?

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

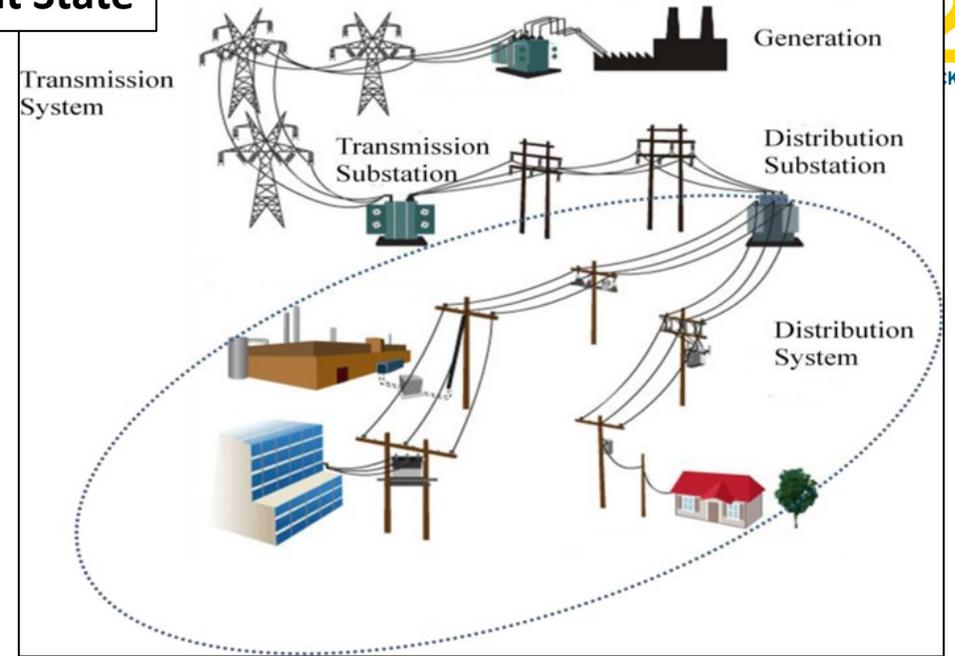
1. Zero-trust approach leveraging identity and mutual transport layer security (mTLS)
2. Deploying and patching remote OT applications
3. Enabling and demonstrating end-to-end live Situational Awareness
4. Configurable abstraction layers and common interfaces drive interoperability
5. Hybrid Cloud /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



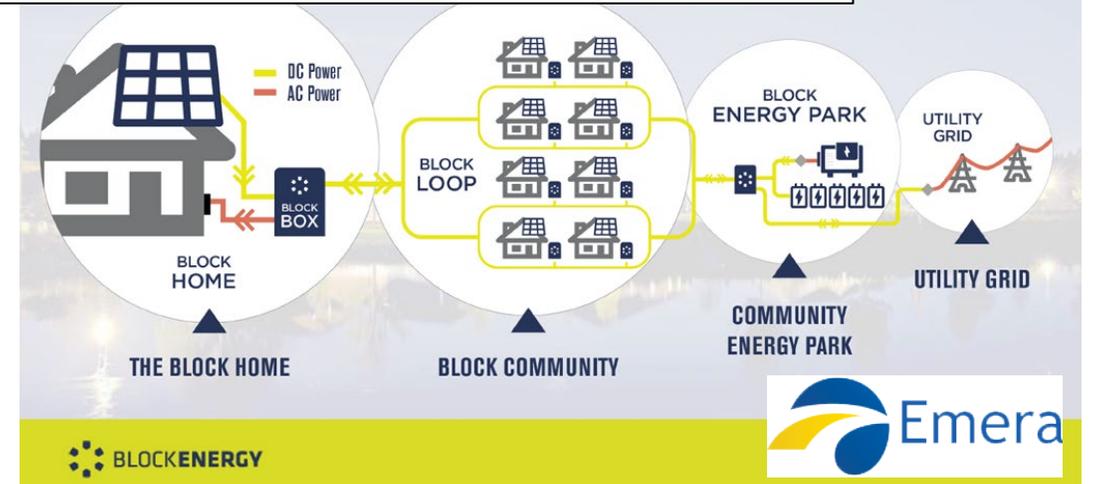
Key Opportunities in Grid Operational Technologies (OT) Cybersecurity (ZTAG coming soon)

- 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

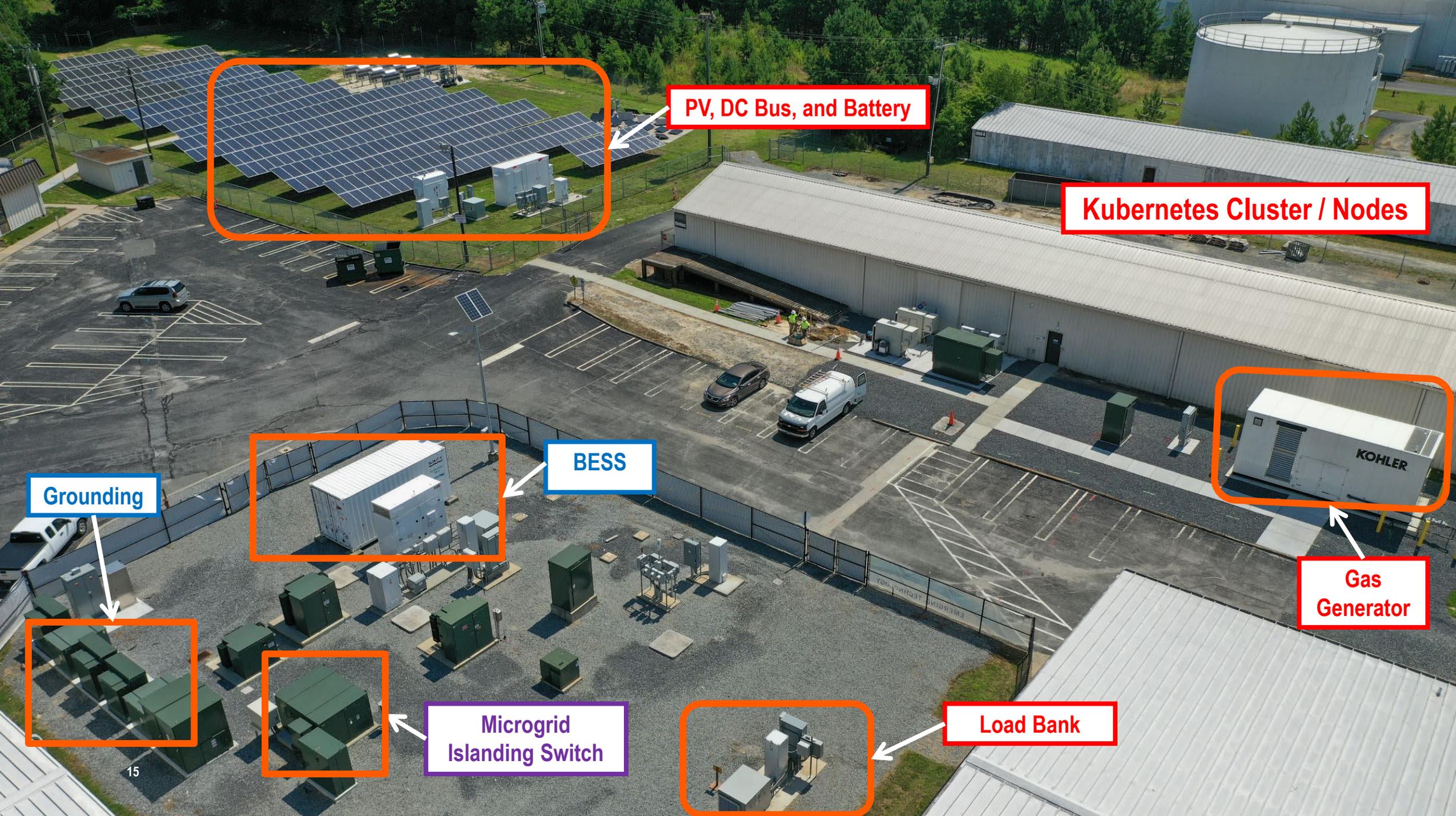
Current State



Future Grid – Distributed, Autonomous, Virtual Power Plants







PV, DC Bus, and Battery

Kubernetes Cluster / Nodes

Grounding

BESS

KOHLER

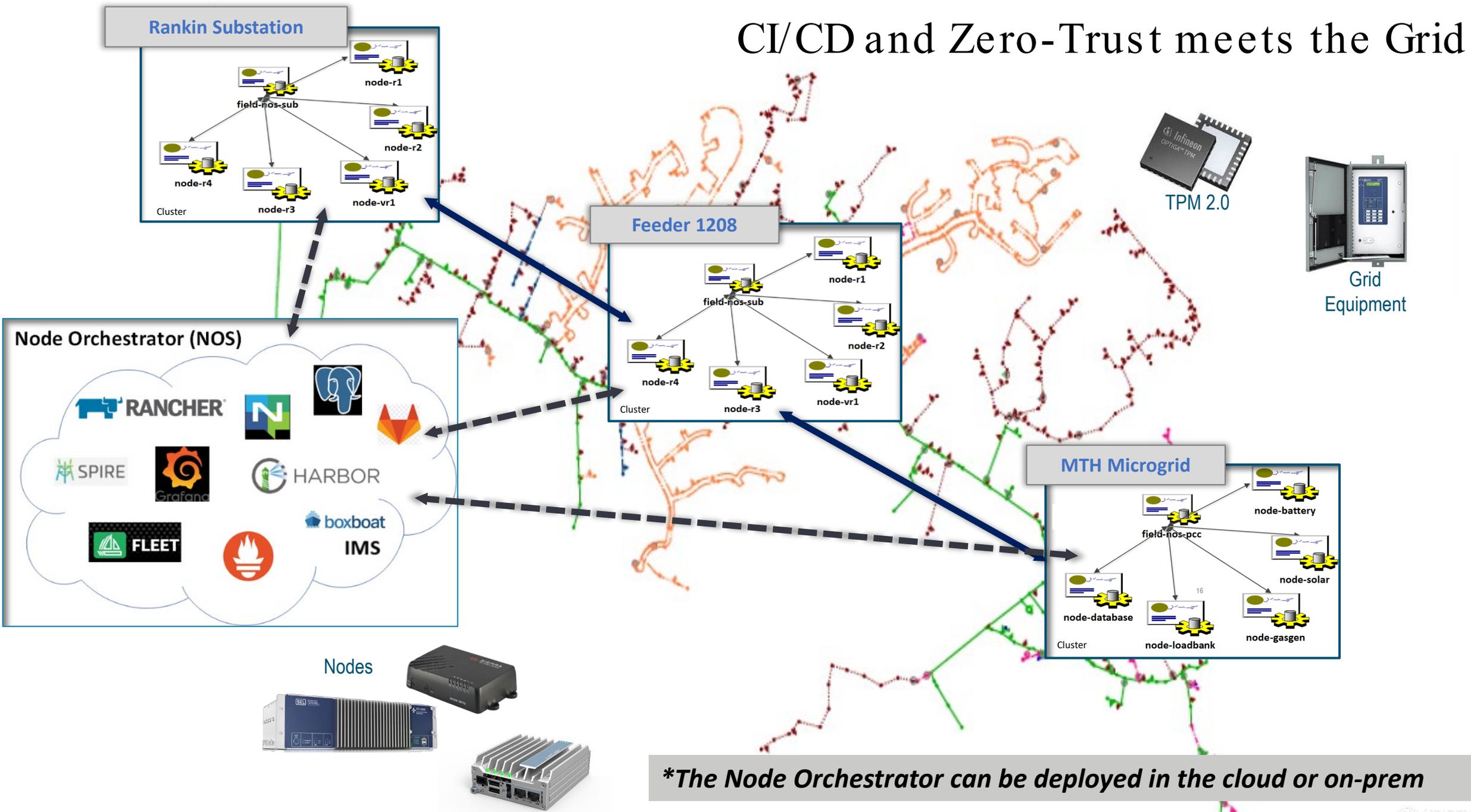
Gas Generator

15

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*

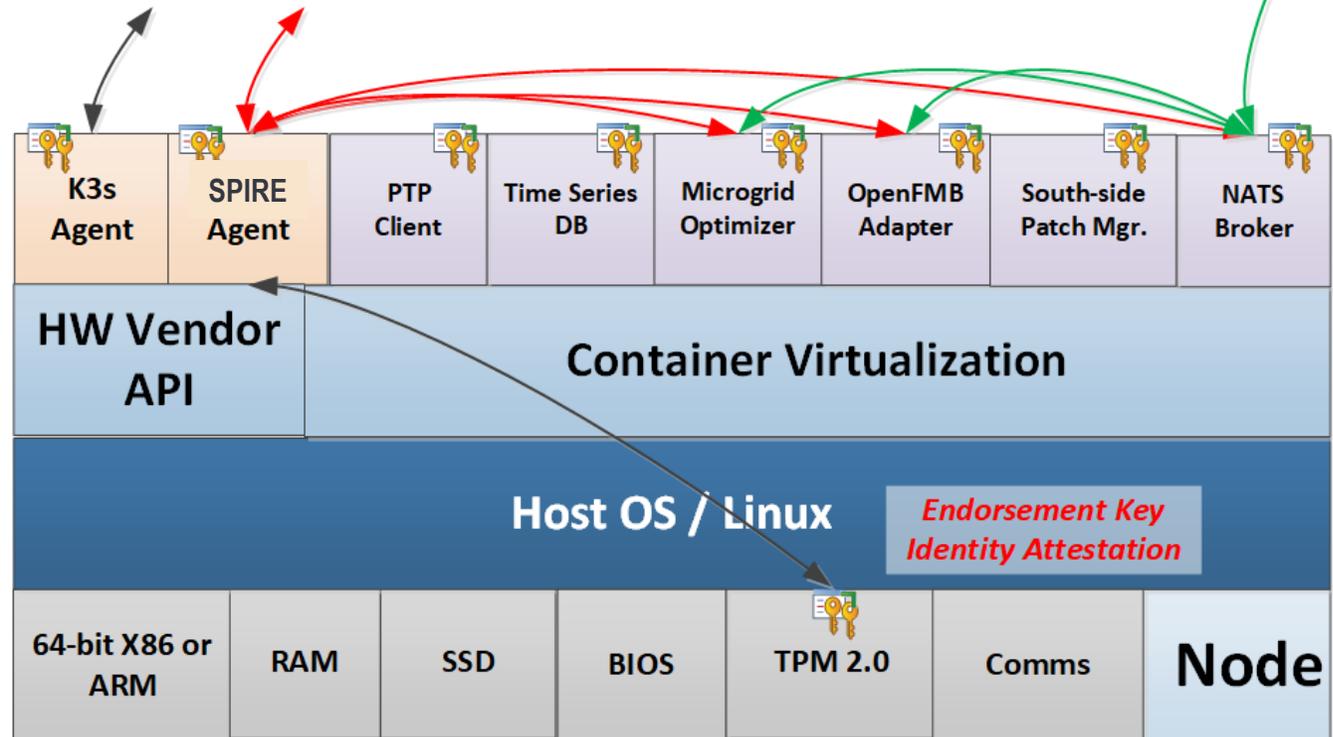
Future-proof the North-side with Kubernetes, SPIRE, and NATS



Distributed PKI with SPIFFE/SPIRE, Secure Pub/Sub with NATS

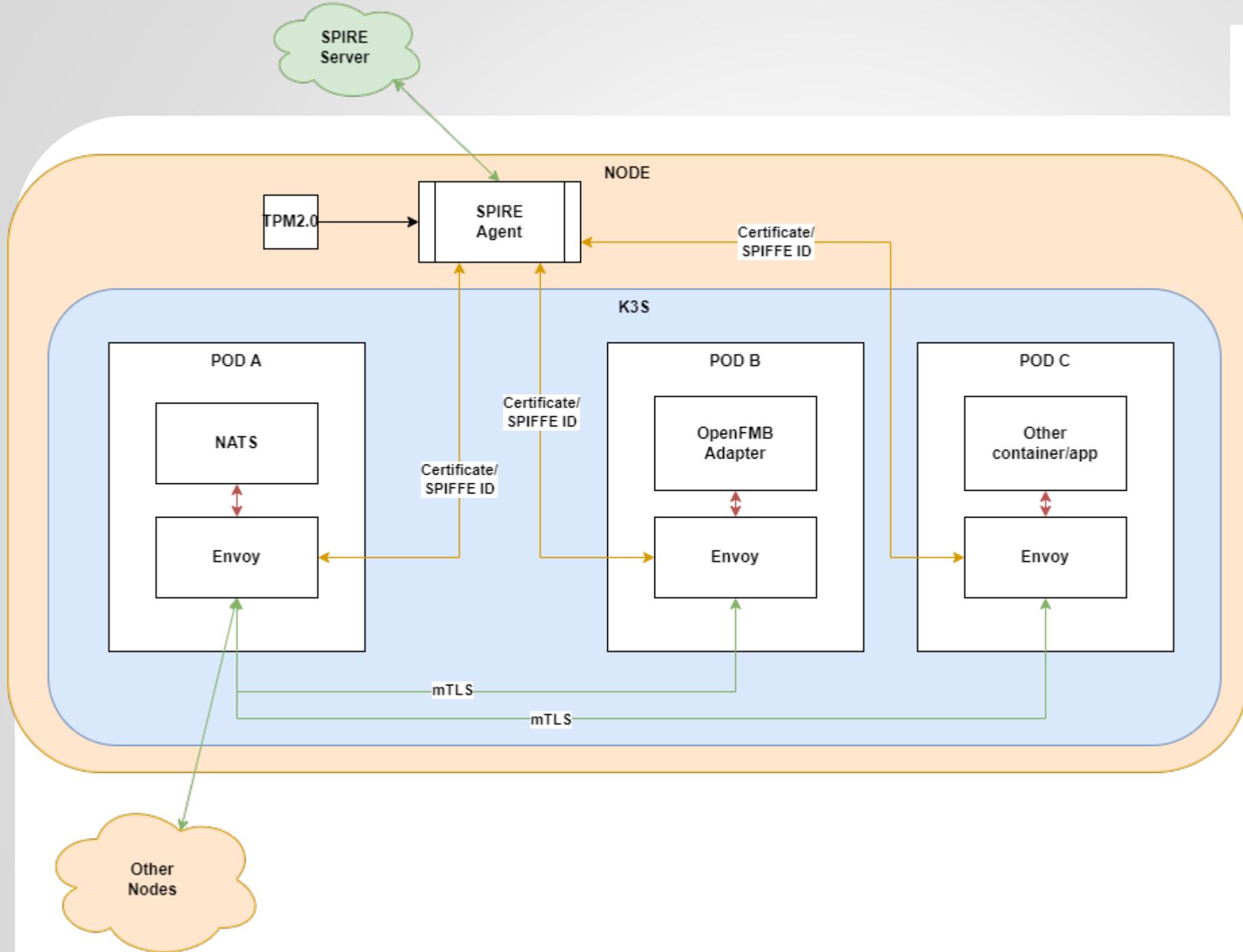
SPIFFE: SVID + Trust Bundle, Chain of Trust to CA

NATS: Envoy Sidecar on each workload, mTLS communications with pre-configured NKey



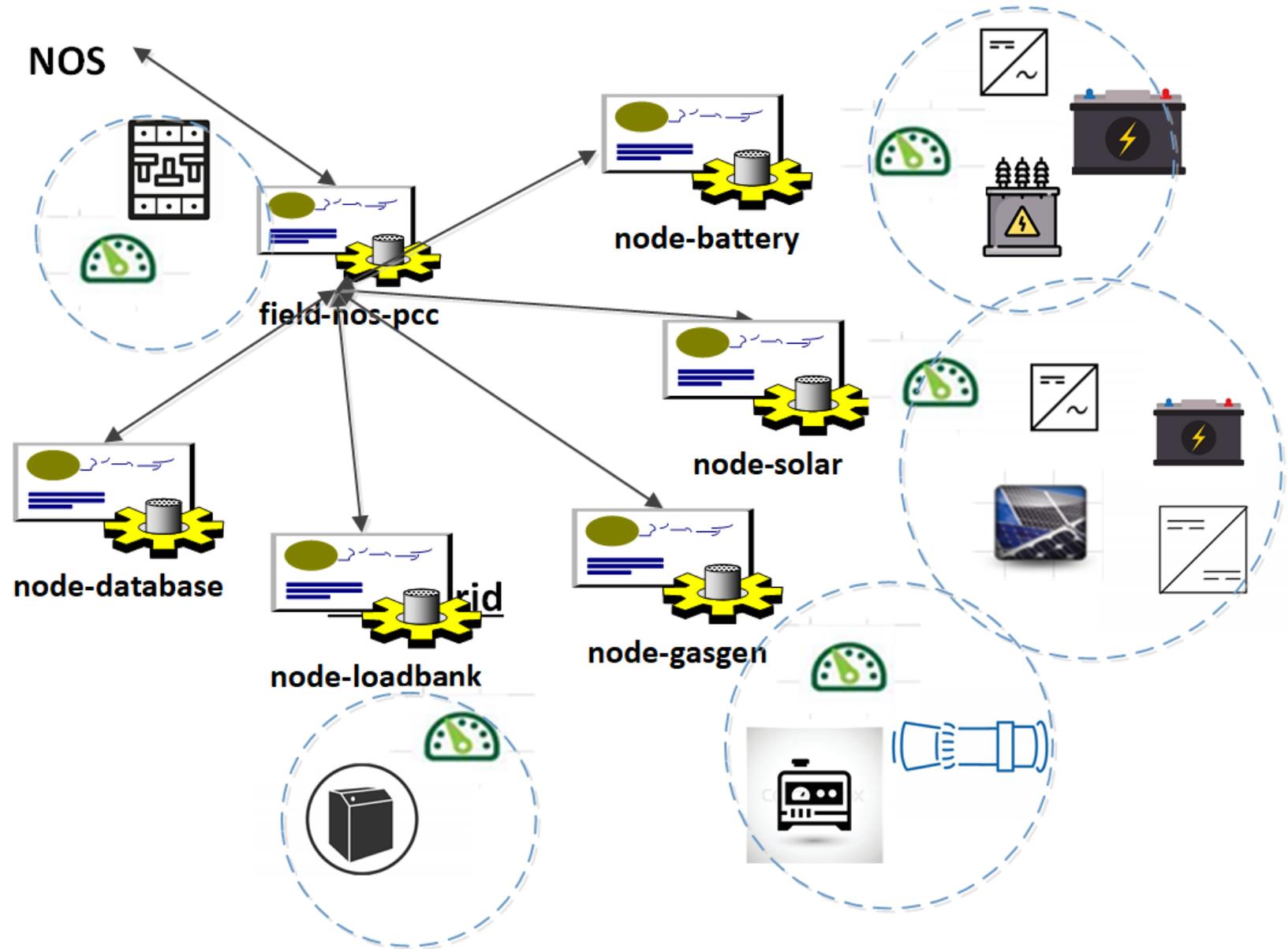
Hide South-side legacy devices and insecure protocols

- 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.**



Abstracting Security with Envoy

Inside the Microgrid Kube Cluster



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

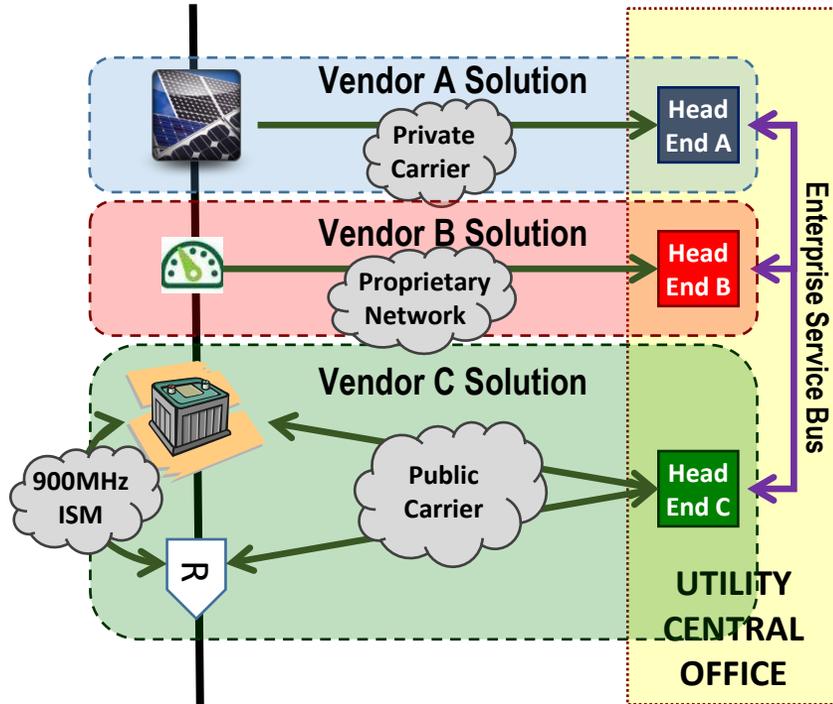
- Provides a Zero-trust environment
- Facilitates deploying and patching remote grid applications
- Enables end-to-end live Situational Awareness
- Drives interoperability
- Integrates with legacy devices
- Secures peer-to-peer communications at the edge
- Enables Distributed Intelligence (DI) grid applications

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



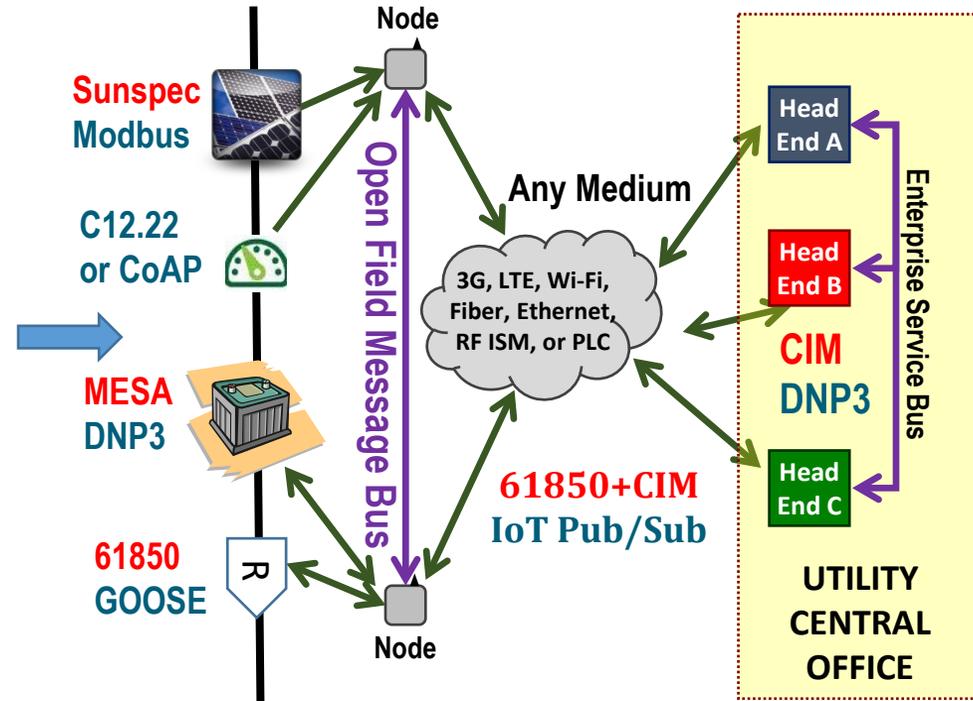
“Working to Secure the Grid, One Distributed Autonomous Function at a Time!”

Node Definition, Edge Compute...OpenFMB: Enabling DI



Key Observations:

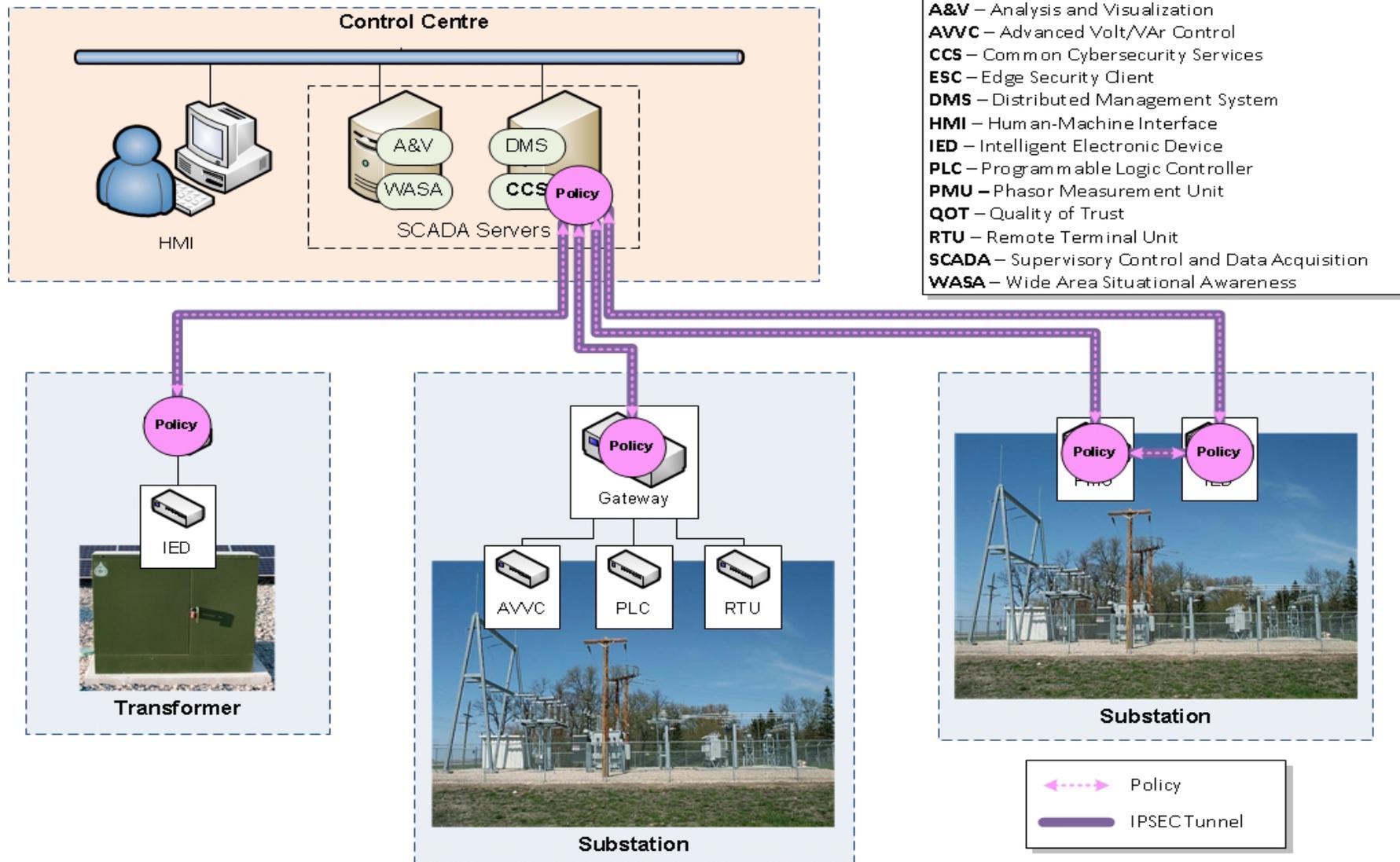
1. Single-Purpose Functions
2. Proprietary & Silo'ed systems
3. Latent , Error-prone Data
4. OT/IT/Telecom Disconnected
5. **No Field Interoperability!**



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



- A&V** – Analysis and Visualization
- AVVC** – Advanced Volt/VAR Control
- CCS** – Common Cybersecurity Services
- ESC** – Edge Security Client
- DMS** – Distributed Management System
- HMI** – Human-Machine Interface
- IED** – Intelligent Electronic Device
- PLC** – Programmable Logic Controller
- PMU** – Phasor Measurement Unit
- QOT** – Quality of Trust
- RTU** – Remote Terminal Unit
- SCADA** – Supervisory Control and Data Acquisition
- WASA** – Wide Area Situational Awareness

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

The screenshot displays the Security Operations Center 1 interface, which is divided into several functional areas:

- Top Left:** A network graph showing a complex web of green nodes representing devices and their interconnections.
- Top Center:** A map of California with various cities labeled, overlaid with a grid and green markers indicating device locations.
- Top Right:** A vertical dashboard of security metrics, including:
 - New Alerts (2096)
 - 396 WARNING
 - 1700 NOTIFICATION
 - Heartbeats (100)
 - 100 ACTIVE
 - IDs (100)
 - 100 VALID
 - BoHs (100)
 - 100 HEALTHY
 - QoTs (100)
 - 100 TRUSTED
 - SAs (82)
 - 82 CONNECTED
 - Actions (37)
- Bottom Left:** Four small line graphs showing metrics for Heartbeat, Identity Certificate, Bill of Health, and Quality of Trust, all plotted on a scale from 0.0 to 1.0.
- Bottom Center:** A table titled "Device Hierarchy" showing a list of devices and their status. The table has columns for Description, #, Heartbeat, ID, BoH, and QoT.

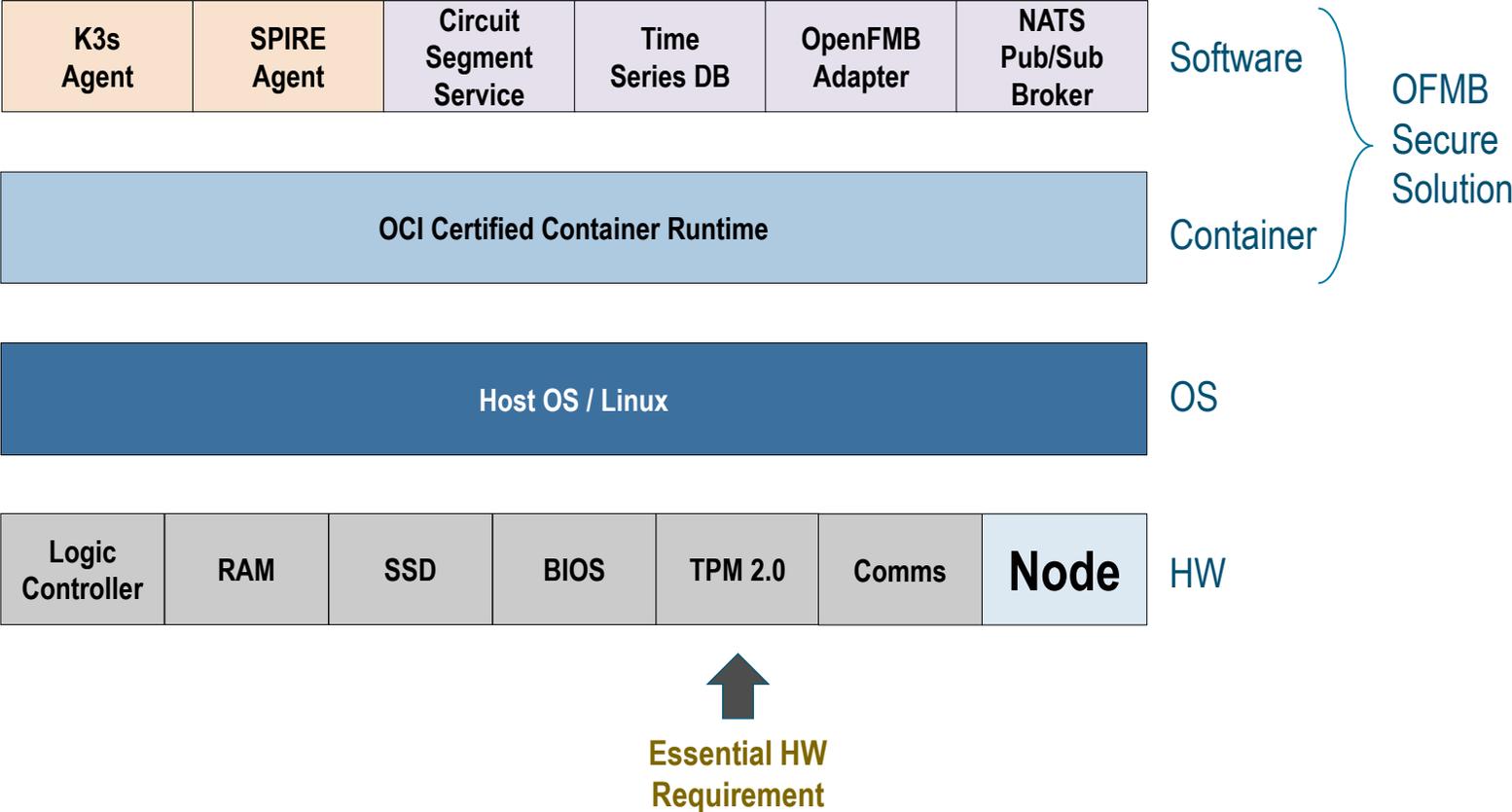
Description	#	Heartbeat	ID	BoH	QoT
top	100	[Green Bar]	[Green Bar]	[Green Bar]	[Green Bar]
CA	100	[Green Bar]	[Green Bar]	[Green Bar]	[Green Bar]
Alhambra	6	[Green Bar]	[Green Bar]	[Green Bar]	[Green Bar]
Alhambra Substation 1	6	[Green Bar]	[Green Bar]	[Green Bar]	[Green Bar]
Device11 (Client)	-	ACTIVE	VALID	HEALTHY	TRUSTED
Device25 (Client)	-	ACTIVE	VALID	HEALTHY	TRUSTED
Device6 (Client)	-	ACTIVE	VALID	HEALTHY	TRUSTED
Device74 (Client)	-	ACTIVE	VALID	HEALTHY	TRUSTED
Device95 (Client)	-	ACTIVE	VALID	HEALTHY	TRUSTED
Device98 (Client)	-	ACTIVE	VALID	HEALTHY	TRUSTED
Fullerton	12	[Green Bar]	[Green Bar]	[Green Bar]	[Green Bar]
Fullerton Substation 1	12	[Green Bar]	[Green Bar]	[Green Bar]	[Green Bar]
Device10 (Client)	-	ACTIVE	VALID	HEALTHY	TRUSTED
Device20 (Client)	-	ACTIVE	VALID	HEALTHY	TRUSTED
Device28 (Client)	-	ACTIVE	VALID	HEALTHY	TRUSTED
- Bottom Right:** A table showing a log of recent events, including Time, Level, Type, Status, and Source/Target information.

Time	Level	Type	Status	Source	Target
3 min...	NOTIFICA	CERT_ISSUED	NEW	Device6	Device6
3 min...	NOTIFICA	CERT_ISSUED	NEW	Device98	Device98
3 min...	NOTIFICA	CERT_ISSUED	NEW	Device74	Device74
3 min...	NOTIFICA	CERT_ISSUED	NEW	Device24	Device24
3 min...	NOTIFICA	CERT_ISSUED	NEW	Device82	Device82
3 min...	NOTIFICA	CERT_ISSUED	NEW	Device37	Device37
3 min...	NOTIFICA	CERT_ISSUED	NEW	Device19	Device19
3 min...	NOTIFICA	CERT_ISSUED	NEW	Device11	Device11

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

Detailed Analysis Results

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 μ grid)	✓	✓	✓	
PCC Monitoring/Mgmt. (Cust. μ grid)	✓	✓	✓	
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**

