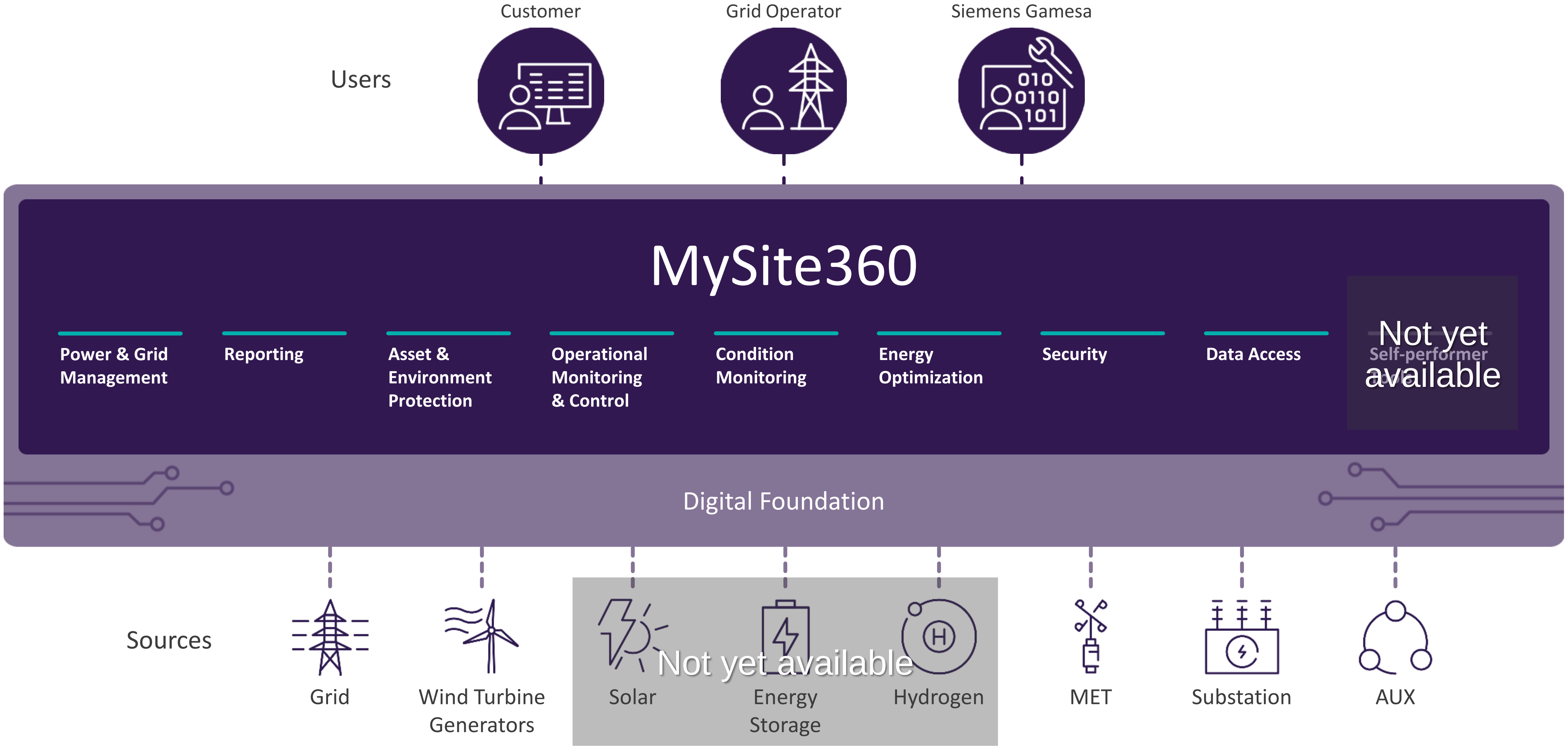
SIEMENS Gamesa
RENEWABLE ENERGY

MySite Next Generation Technology evaluation

October 18th

MySite360® visualization – breakdown & context



Users

Customer

Grid Operator

Siemens Gamesa

MySite360

Power & Grid Management

Reporting

Asset & Environment Protection

Operational Monitoring & Control

Condition Monitoring

Energy Optimization

Security

Data Access

Self-performer Tools

Not yet available

Digital Foundation

Sources

Grid

Wind Turbine Generators

Solar

Energy Storage

Hydrogen

Not yet available

MET

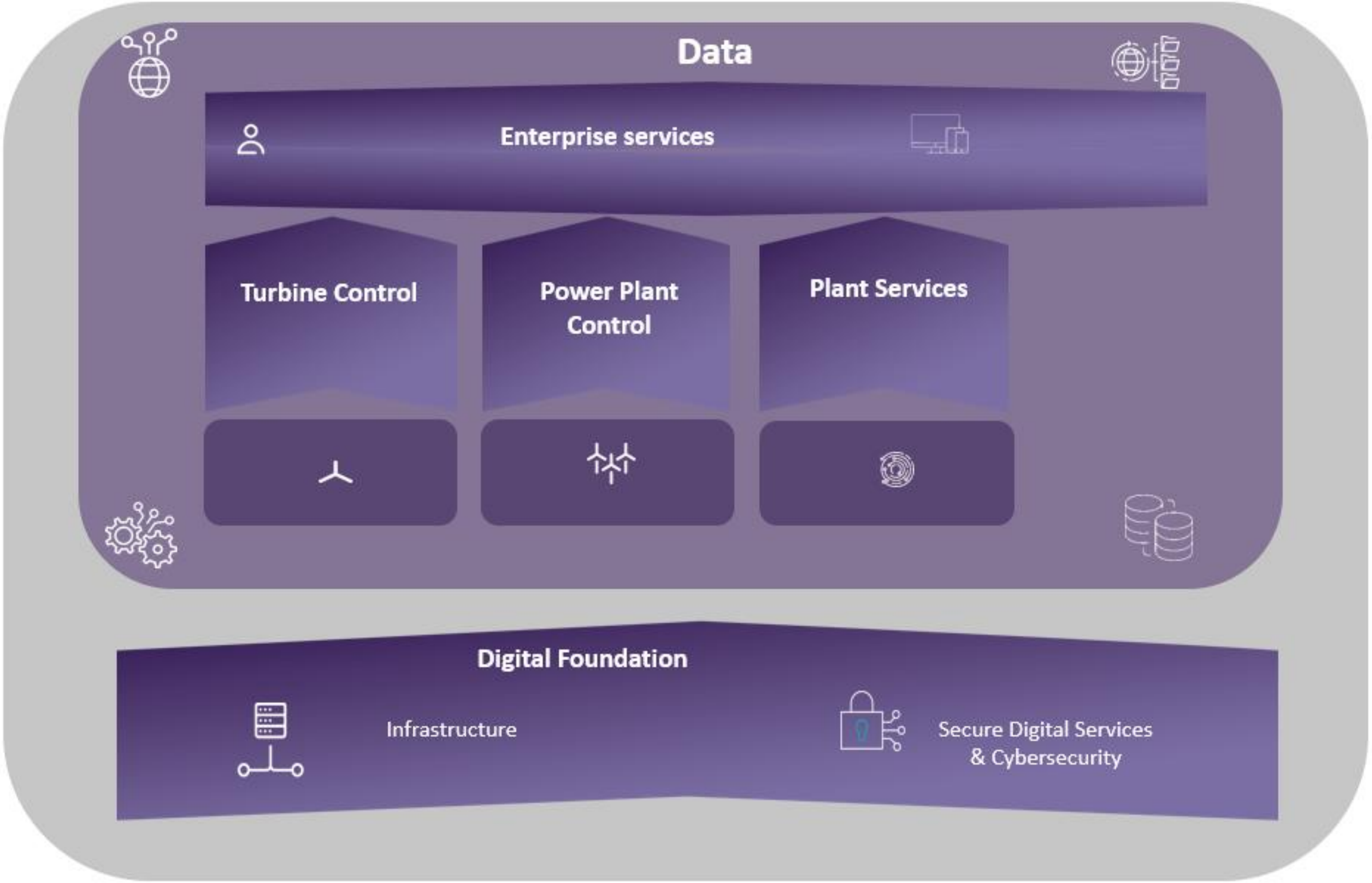
Substation

AUX

Mysite 360 Solution (Simplified View)

High Level Overview of major Mysite 360 building blocks within OT SW Platform

Digital foundation is the Foundation of OT SW platform

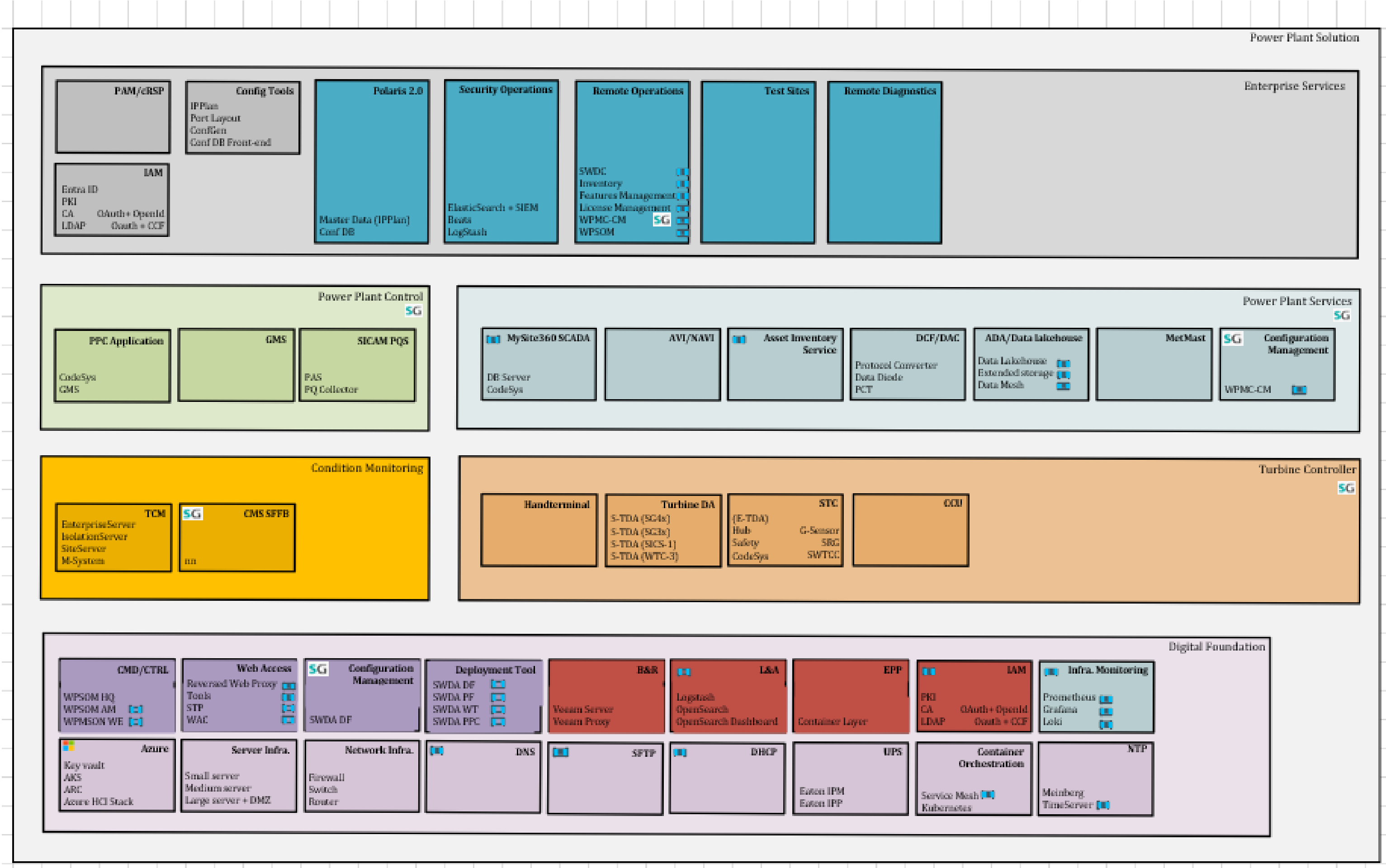


Mysite 360 Solution (Detailed View)

Simplified Overview of systems and sub systems within Mysite360 OT Platform

Mysite360 is not simply SCADA, it is a unified ecosystem of software, embedded software and associated hardware

PPS is not the unique contributor to Mysite360, Wind Turbine Control and HQ are also part of it.



Power Plant Solution

Enterprise Services

PAM/cRSP

Config Tools
IPPlan
Port Layout
ConfGen
Conf DB Front-end

IAM
Entra ID
PKI
CA OAuth+ OpenId
LDAP Oauth + CCF

Polaris 2.0
Master Data (IPPlan)
Conf DB

Security Operations
ElasticSearch + SIEM
Beats
LogStash

Remote Operations
SWDC
Inventory
Features Management
License Management
WPMC-CM
WPSOM

Test Sites

Remote Diagnostics

Power Plant Control

PPC Application
CodeSys
GMS

GMS

SICAM PQS
PAS
PQ Collector

Power Plant Services

MySite360 SCADA
DB Server
CodeSys

AVI/NAVI

Asset Inventory Service

DCF/DAC
Protocol Converter
Data Diode
PCT

ADA/Data lakehouse
Data Lakehouse
Extended storage
Data Mesh

MetMast

Configuration Management
WPMC-CM

Condition Monitoring

TCM
EnterpriseServer
IsolationServer
SiteServer
M-System

CMS SFFB
nn

Turbine Controller

Handterminal

Turbine DA
S-TDA (SG4x)
S-TDA (SG3x)
S-TDA (SICS-1)
S-TDA (WTC-3)

STC
(E-TDA)
Hub G-Sensor
Safety SRG
CodeSys SWTCC

CCU

Digital Foundation

CMD/CTRL
WPSOM HQ
WPSOM AM
WPMSON WE

Web Access
Reversed Web Proxy
Tools
STP
WAC

Configuration Management
SWDA DF

Deployment Tool
SWDA DF
SWDA PF
SWDA WT
SWDA PPC

B&R
Veeam Server
Veeam Proxy

L&A
Logstash
OpenSearch
OpenSearch Dashboard

EPP
Container Layer

IAM
PKI
CA OAuth+ OpenId
LDAP Oauth + CCF

Infra. Monitoring
Prometheus
Grafana
Loki

Azure
Key vault
AKS
ARC
Azure HCI Stack

Server Infra.
Small server
Medium server
Large server + DMZ

Network Infra.
Firewall
Switch
Router

DNS

SFTP

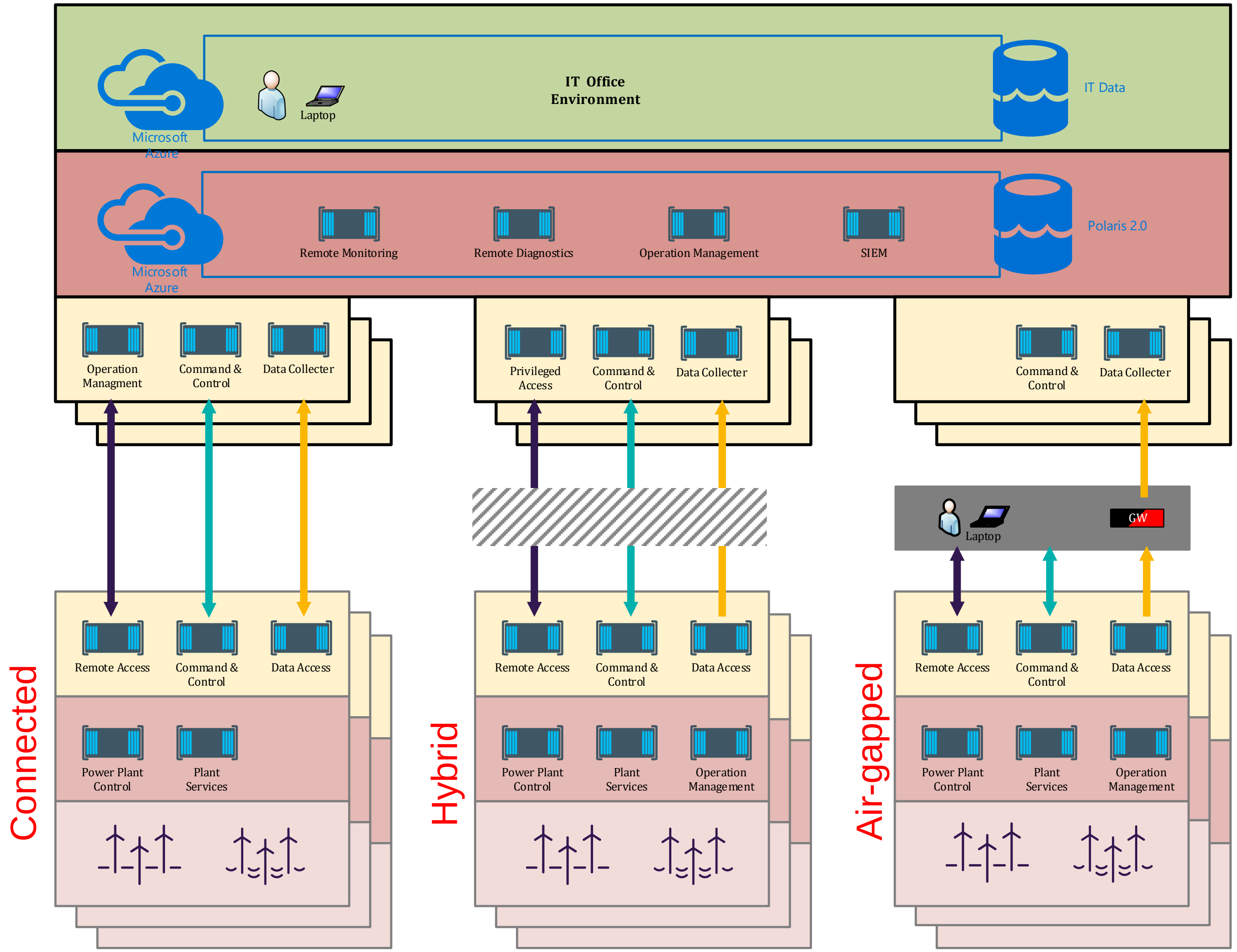
DHCP

UPS
Eaton IPM
Eaton IPP

Container Orchestration
Service Mesh
Kubernetes

NTP
Meinberg
TimeServer

MySite360 Connectivity Types



Connected

- Only SGRE and TSO (Transmission System Owner) has connectivity
- Most Digital Foundation features can be moved to RSC (Remote Service Centers)

Hybrid

- Multi vendor connectivity
- All features must run on the Wind Power plant

Air-gapped

- TSO direct connectivity, no other CMD/CTRL from outside (operation through local control center)
- Data through data diode

⟷ Remote Interactive Access

⟷ Command & Control

⟷ Data Access

1: Percentage of Megawatts for each scenario

Scenarios considered for CAPEX analysis

Customer segments	Variant	Park size	Connectivity mode	System availability
• Variants for Onshore market	**Tower**	**1 WTG**	Connected	Standard
	ON VSI – SA (Basic)	**1 – 9 WTGs**	Hybrid	Standard
	ON VSI – SA	**1 – 24 WTGs**	Hybrid	Standard
	ON VSI – HA	**25-200 WTGs**	Hybrid	High Availability
• Variants for Offshore market	**OF VSI – HA**	**1-200 WTGs**	Hybrid	High Availability

Scenarios selected to be comparable current vs next gen.
Today, Tower is not a variant itself

1) Number of WTG are indicated, subject to change
2) WTG: Wind turbine generator

Problem Statement of Current Mysite 360 OT Software Platform

Current Solution Issues & Limitations

Quality & Deployment

- **Difficult to Deploy and Upgrade** resulting in 88-120 hours effort per site
- **High Maintenance Effort** of ~17m Euro per annum and rising.
- **High Defect rate**

High Cost

- **Total Cost of Ownership, TCO, is >30% too high** due to issues across capital, development and operating costs including maintenance.

Security Standards

- **Partial compliance to IEC62443** and key market national legislation with roadmap through **2027** to deliver full regulatory compliance

Poor Development Speed & Innovation

- **Complex software** with **>10,000,000 lines** of code. Lack of defined interfaces create **tightly coupled monolithic** code

End of Life & Fit For Future

- Number of **end of life** deadlines on hardware and software components.
- Poor **Data governance** using many protocols

Limitation of Current Design

- Deployment unable to achieve target of <16hours without reduction in components.
- Maintenance effort also proportionate to complexity of system and components.
- Defects driven by complexity

- Lack of scalability within current design adversely affects smaller sites CAPEX and OPEX costs.
- Development velocity low due to tightly coupled monolithic architecture.
- Maintenance costs high due to lack of standardization

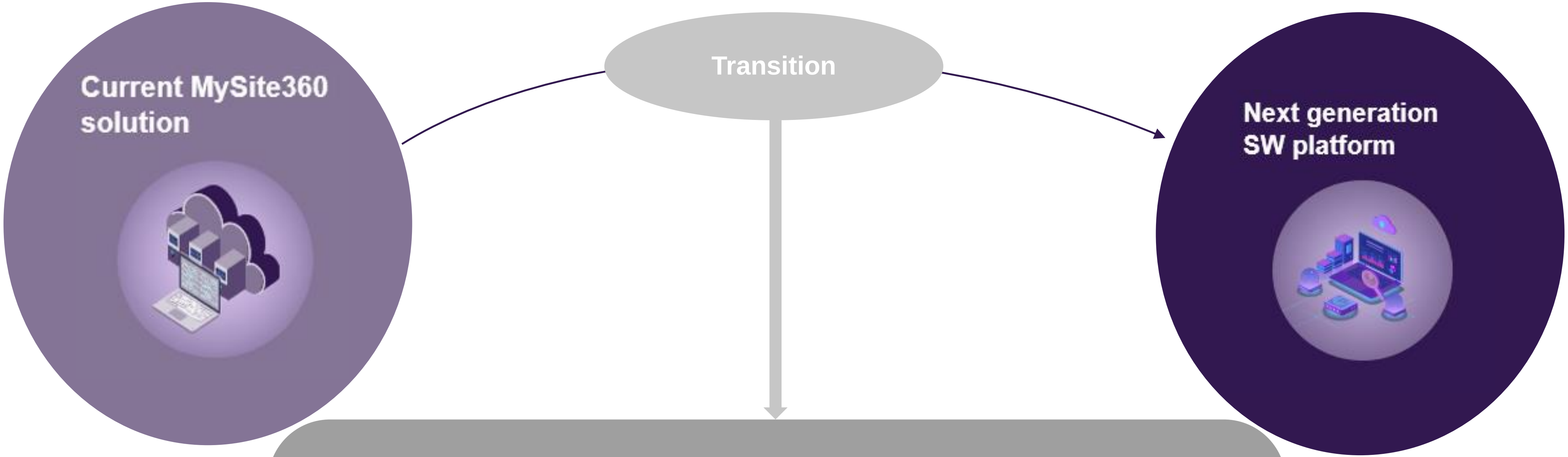
- Current design relies on high physical segmentation driving hardware cost up to comply with cybersecurity
- Lack of standardization and monolithic code base makes security more difficult.
- End of support deadlines requires continuous lifecycle management

- Demand for new features and innovation is increasing evidenced by 2.8x backlog.
- New feature development on a complex software code base results slow velocity and high defects.
- Lack of standard APIs

- Many physical and software components are reaching end of life and require new design elements.
- Lack of data centric architecture will limit possibility for AI and autonomous operations.
- Missing licensing and toggling capabilities to monetize digital services

To remedy pain points fully and achieve cybersecurity compliance in software platform for current and future needs requires modern architecture

From Current MySite360 to Next Gen MySite360



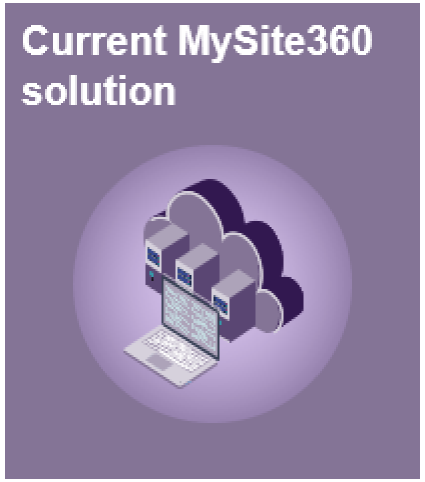
Current MySite360 solution

Transition

Next generation SW platform

- Key decisions for transition from current to Next generation:
  - Digital foundation technology stack (Microsoft or Multivendor)
  - Partnership for Digital foundation solution integration
- Key impacts:
  - Organizational commitment and alignment required
  - Mysite360 operating model and business model adaptations

MySite360 transformation



- The Windows server stack takes several hours to run through (configuration and apps)
- Hard to automate
- Patching is uncontrollable
- Unable to read all Windows settings (Compliance issue)
- Network dependencies, more than 50K ACL, must be updated on new features deployments
- Problematic ownership between teams

- Reduced server stack complexity by using immutable and harden hyperconverged platform
- Data centric architecture, lead to simple interfaces between Wind Turbine Controllers, Wind Power Plant controllers and the Data mesh
- Stable L2 segmentation between Wind Turbines, Power plant controllers and API gateway
- Data mesh provides non L2 connectivity for the Wind Power Plant Services to consume and produce data.
- API governance through API contracts.
- Segmentation within the Container Orchestration is done through in L3/L4.
- Segmentation is achieved through standard network functionality with the eBPF standard and name space segmentation.

Part of the PPS TE strategy

MySite360 trip overview

From

Current MySite360 solution

Four core transition elements, …

Modularization	Convert **monolithic software code** into **business-oriented microservices** with a **data-centric architecture**
Cloudification	Segmentation of **OT HQ setup**. Introduce **cloud technologies** in **on-premise** solutions. Moving selected appl. from **edge to cloud** [1] with **built-in cybersecurity**
Licensing	**Eliminate** high **licensing costs** within existing sol. whilst enabling SGRE to **sell features** via license and subscription model **to cust.**
Automation	Enabling the solution to **reduce manual configurations**, ensuring **single sources of code**

To

Next generation SW platform

… building on five principles

Make or buy decision

- Increase usage of **commercial ready SW** and focus on **value-adding development activities**
- **Establish key software partnerships** including with hyperscalers

Data-centric architecture

- Utilize standard **data collectors** and **data mesh** with easy **data subscription**
- Conv. plant services to use **data models** for **online**, **alarms,** and **historical data**

Agnostic solutions

- Disconnect **architecture** from HW and operating systems
- **Container Orchestration** and **embedded devices** instead of server-based technologies
- Open model and flexible architecture

Testing philosophy

- Testing to be shifted towards **earlier stages** of the SW development lifecycle
- **End-to-end testing** of full solution
- Pre-validation of **third-party** components

Development culture

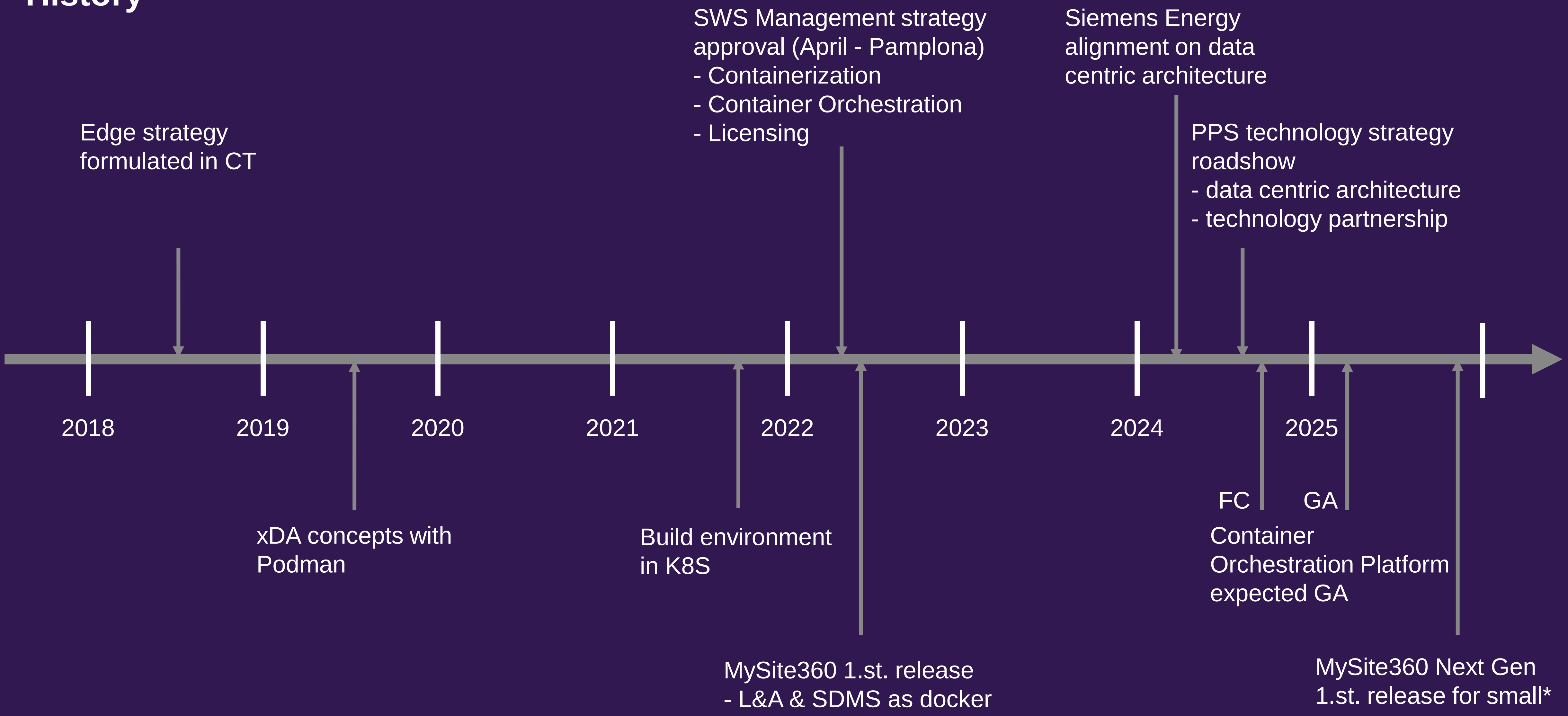
- Shift culture in develop. applying **DevSecOps** and a robust **release mgmt.** process
- **Microservices architecture** fosters the ability for teams to **work independently**

Notes: OTCS 2.0 is already being implemented and thus not specifically being mentioned here as part of the transformation

[1] With private phasing access

MySite360 – Trip to target architecture

History



Edge strategy formulated in CT

xDA concepts with Podman

Build environment in K8S

SWS Management strategy approval (April - Pamplona)
- Containerization
- Container Orchestration
- Licensing

MySite360 1.st. release
- L&A & SDMS as docker

Siemens Energy alignment on data centric architecture

PPS technology strategy roadshow
- data centric architecture
- technology partnership

FC GA

Container Orchestration Platform expected GA

MySite360 Next Gen 1.st. release for small*

** Deadline not consolidated, update required when finishing Transition plan*

Digital Foundation Technology stack - Solutions overview

Microsoft

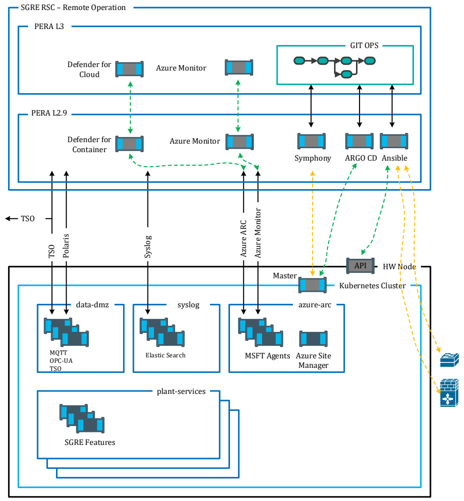
Multivendor

Connected

Microsoft

Technology Stack

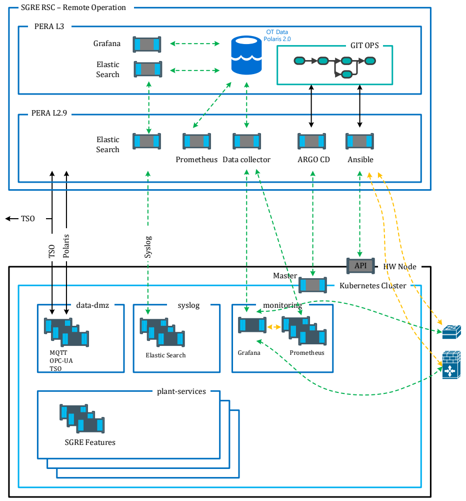
- Single HW node bare metal Kubernetes
- Azure Arc enabled Kubernetes
- Azure Entra ID
- Symphony
- ARGO CD
- Defender for Kubernetes & Cloud
- Azure Monitor
- Ansible
- Elastic Stack



Multivendor

Technology Stack

- Single HW node bare metal Kubernetes
- ARGO CD
- Grafana + loki & Prometheus for monitoring
- Siesta
- KubeBench & Falco
- Ansible
- Elastic Stack

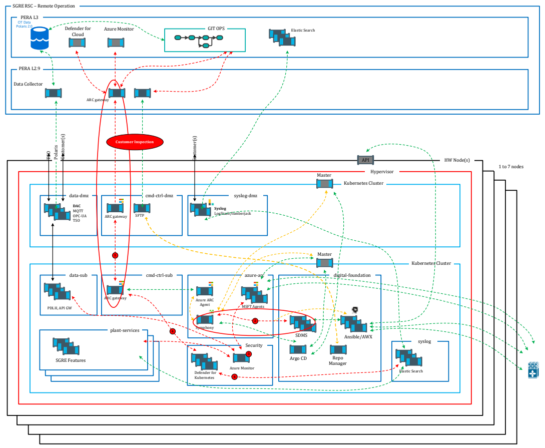


Hybrid

Microsoft

Technology Stack

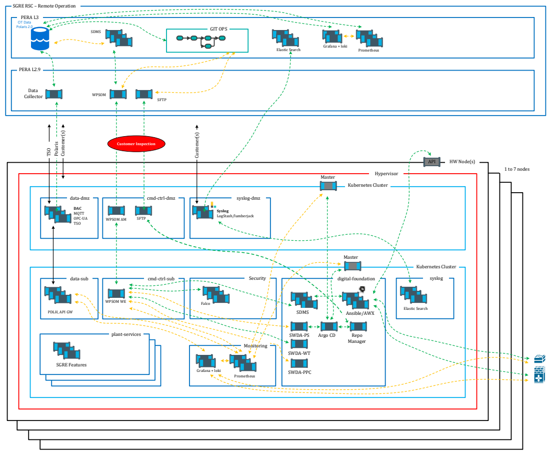
- Single or multiple HW nodes
- Hypervisor
- Multi node Kubernetes clusters (DMZ, Substation)
- Azure Arc enabled Kubernetes
- Azure Entra ID @ RSC & Duende IAM solution @ Wind Power Plant
- SGRE or vendor stitching CMD/CTRL GW
- ARGO CD
- Defender for Kubernetes & Cloud
- Azure Monitor
- Ansible
- Elastic Stack



Multivendor

Technology Stack

- Single or multiple HW nodes
- Hypervisor
- Multi node Kubernetes clusters (DMZ, Substation)
- ARGO CD
- Grafana + Loki & Prometheus for monitoring
- Siesta (CI/CD Tools)
- KubeBench & Falco
- Elastic Stack



Digital Foundation – Connected sites (Microsoft Integration)

Technology Stack

- Single HW node bare metal Kubernetes
- Azure Arc enabled Kubernetes
- Azure Entra ID
- Symphony
- ARGO CD
- Defender for Kubernetes & Cloud
- Azure Monitor
- Ansible
- Elastic Stack

OS Distribution
Linux, windows does not currently provide the handles we need for configuration monitoring (standard compliance)

Container Orchestration
Single node bare metal Kubernetes cluster

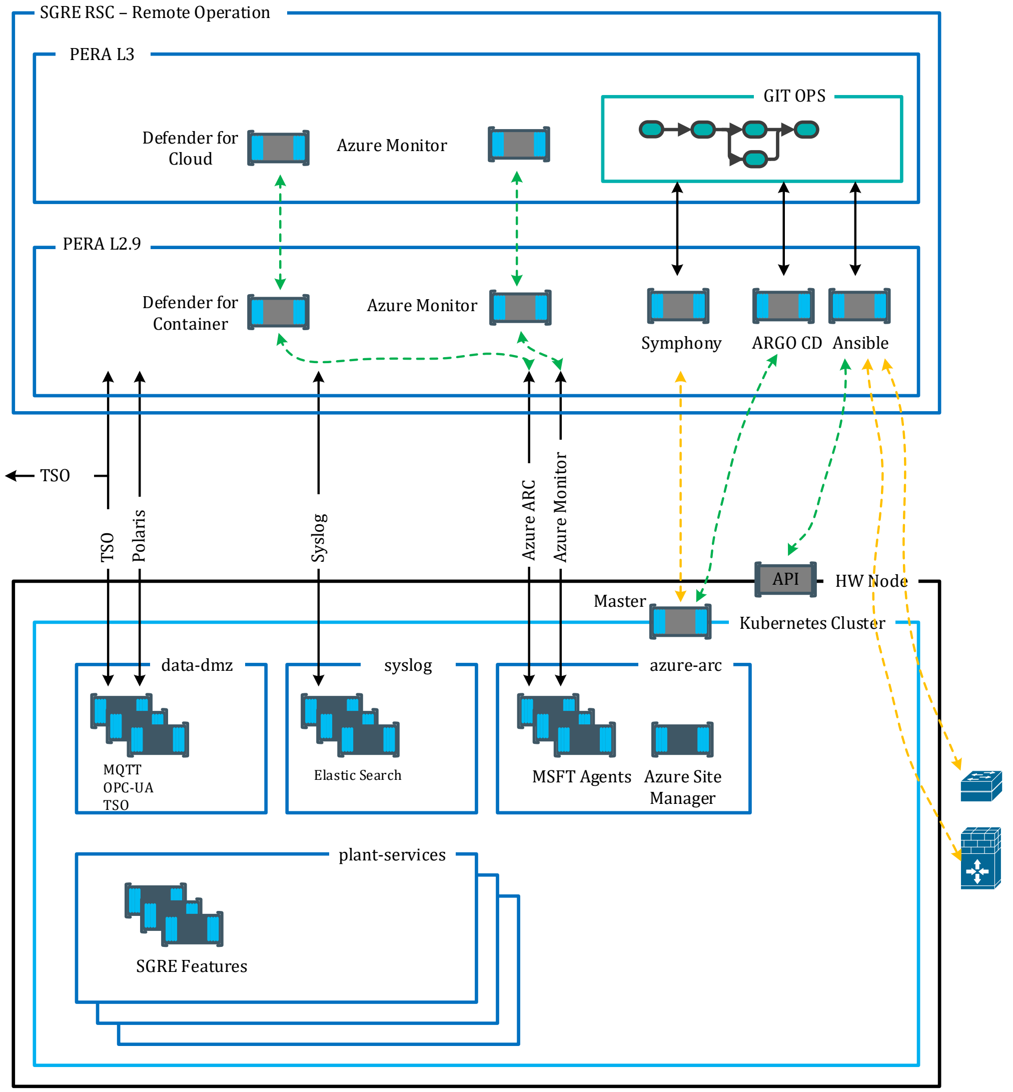
Deployment
Deployment through GitOps principles with ARGO CD and Symphony integration. Server directly through the API. Network and Aux infrastructure through Ansible.
Feature deployment through GitOps and ARC APIs

IAM
Azure Entra ID in SGRE RSC PERA level 2.9.
No local deployment.

Infrastructure Monitoring
ARC and Open telemetry enabled products through Azure Monitoring

Cyber Security

- Server and Container Orchestration detection through defender products
- Server and Container orchestration hardening though Azure Policy
- Logging and Auditing through Elastic family
- Backup Restore not required due to data push and no retention requirements



Digital Foundation – Connected sites (Multivendor Integration)

Technology Stack

- Single HW node bare metal Kubernetes
- ARGO CD
- Grafana + loki & Prometheus for monitoring
- Siesta (Siemens AG Sec. tool)
- KubeBench & Falco (EPP)
- Ansible
- Elastic Stack

OS Distribution
Linux, windows does not currently provide the handles we need for configuration monitoring (standard compliance)

Container Orchestration
Single node bare metal Kubernetes cluster

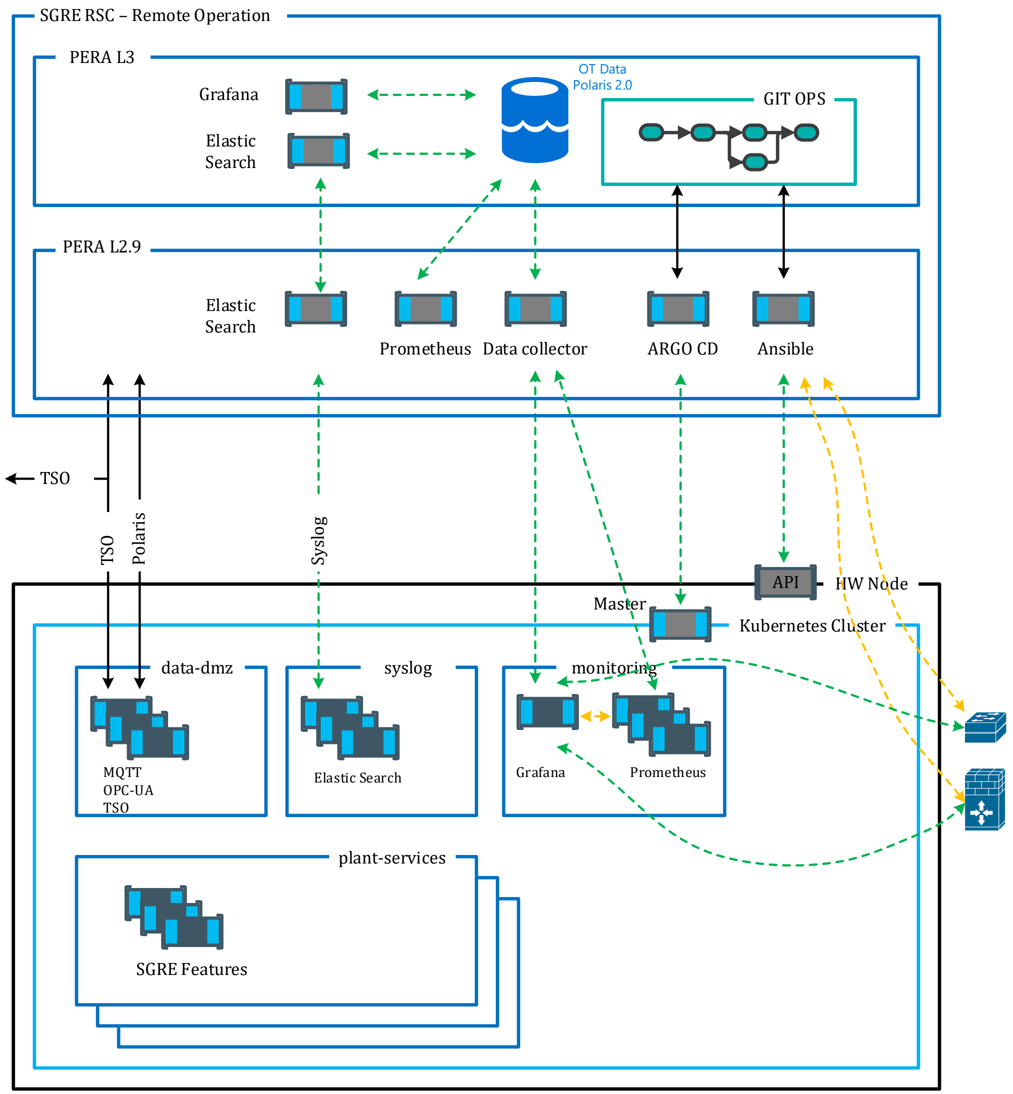
Deployment
Deployment through GitOps principles with ARGO CD and Ansible.
Server directly through the API. Network and Aux infrastructure through Ansible.
Feature deployment through GitOps and ARC APIs

IAM
Azure Entra ID in SGRE RSC PERA level 2.9.
No local deployment.

Infrastructure Monitoring
Grafana and Prometheus for monitoring

Cyber Security

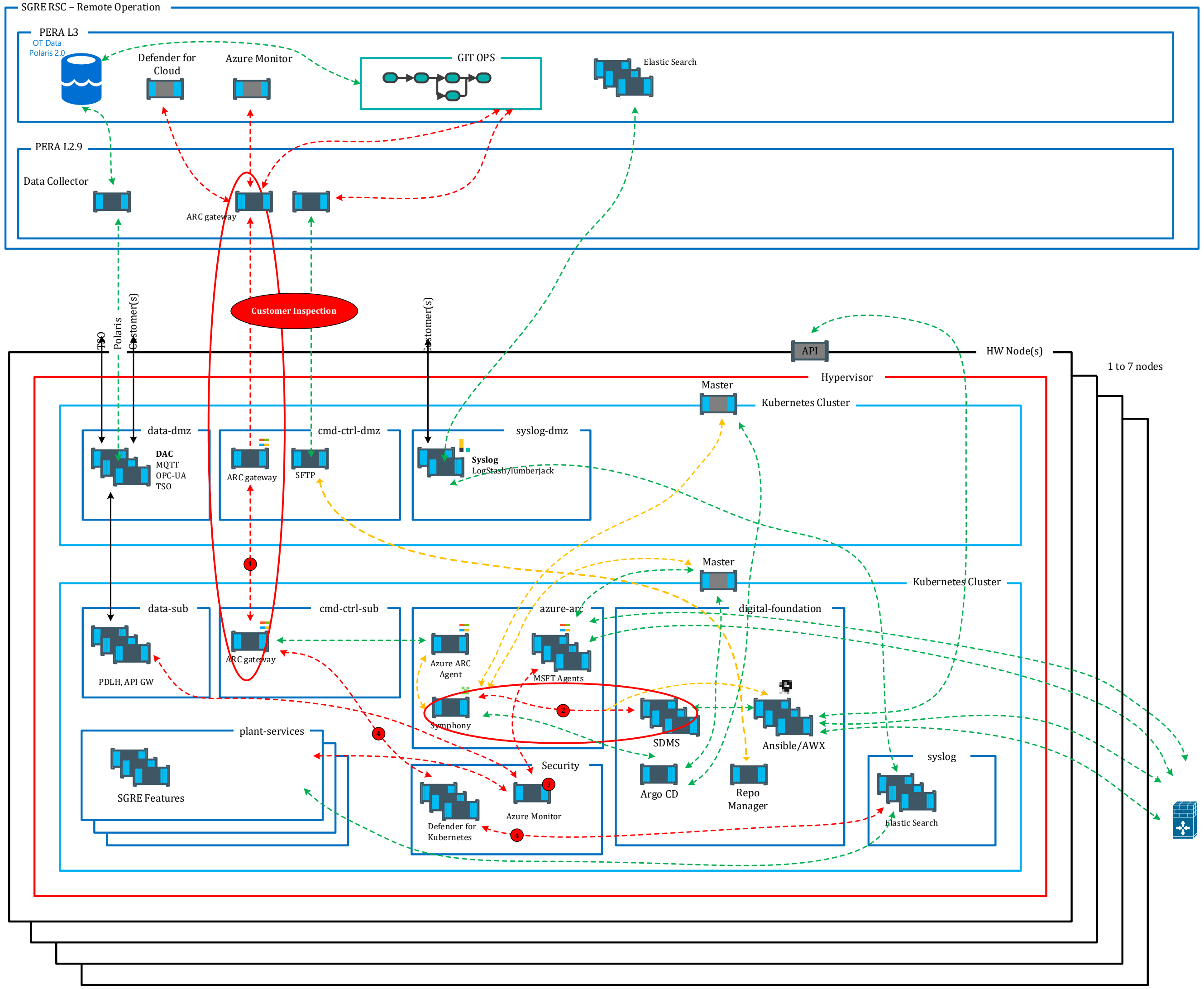
- Protection and Hardening through immutable OS and Container orchestration hardening validated by Siesta scans and KubeBench
- Detection in Container orchestration layer through Falco
- Logging and Auditing through Elastic family
- Backup Restore not required due to data push and no retention requirements



Digital Foundation – Hybrid connected sites (Microsoft Integration)

Technology Stack

- Single or multiple HW nodes
- Hypervisor
- Multi node Kubernetes clusters (DMZ, Substation)
- Azure Arc enabled Kubernetes
- Azure Entra ID @ RSC & Duende IAM solution @ Wind Power Plant
- SGRE or vendor stitching CMD/CTRL GW
- ARGO CD
- Defender for Kubernetes & Cloud
- Azure Monitor
- Ansible
- Elastic Stack



Digital Foundation – Hybrid connected sites (Microsoft Integration)

Technology Stack

- Single or multiple HW nodes
- Hypervisor
- Multi node Kubernetes clusters (DMZ, Substation)
- Azure Arc enabled Kubernetes
- Azure Entra ID @ RSC & Duende IAM solution @ Wind Power Plant
- SGRE or vendor stitching CMD/CTRL GW
- ARGO CD
- Defender for Kubernetes & Cloud
- Azure Monitor
- Ansible
- Elastic Stack

HW Scalability
Single HW node support
Multi HW nodes setup, Physical HA cluster for DMZ and HA cluster for Substation zone

OS Distribution
Linux, optimized for Container orchestration, windows does not currently provide the handles we need for configuration monitoring (standard compliance)

Hypervisor
Microsoft Hyper-V

Container Orchestration
DMZ & Substation zone cluster Kubernetes 3x Control nodes, 3 x worker node

1 **CMD & Control**
<u>Option 1</u>
MSFT develops features in the ARC gateway for protocol break and command allowlisting in substation zone component. (Winfield not in scope)

<u>Option 2</u>
Stitching and integration of multivendor products to support the cyber security products. This requires that MSFT provide APIs for CMD/CTRL integration and for data injection. (Waterfall integration)

IAM
Azure Entra ID in SGRE RSC PERA level 2.9.
Duende Implementation in Wind Power Plant

- Trust to Customers IAM
- Trust and bidirectional sync to Siemens Energy Wind Power mote Service Center (RSC)

2 **Deployment**
Deployment through GitOps principles through the CMD & control gateway.
Deployment tools deployed on the wind power plants
Creating custom resource for SDMS integration (Symphony does not support configuration monitoring and alarming)

3 **Infrastructure Monitoring**
ARC and Open telemetry enabled products through Azure Monitoring. Deployments in HQ and wind power plants MSFT needs to provide data extraction, injection APIs and alarming. Thresholds are required (Models)

4 **Cyber Security**

- Server and Container Orchestration detection through defender products deployed in the wind power plants. Requiring control API for integration and logging for alarming
- Server and Container orchestration hardening though Azure Policy (Not possible according to Redmond meeting)
- Logging and Auditing through Elastic family, 5 yeas retention and on win power plant alarming
- Backup Restore solution through Veeam.
  5 years retention and offloading to customers.

Digital Foundation – Hybrid connected sites (Microsoft Integration) Integration Requirements

Technology Stack

- Single or multiple HW nodes
- Hypervisor
- Multi node Kubernetes clusters (DMZ, Substation)
- Azure Arc enabled Kubernetes
- Azure Entra ID @ RSC & Duende IAM solution @ Wind Power Plant
- SGRE or vendor stitching CMD/CTRL GW
- ARGO CD
- Defender for Kubernetes & Cloud
- Azure Monitor
- Ansible
- Elastic Stack

1

Generic Requirements

1. Any MSFT product or agent must be able to create Audit and system log in OTel format

CMD & Control

Option 2

Stitching and integration of multivendor products to support the cyber security products. This requires that MSFT provide APIs for CMD/CTRL integration and for data injection. (Waterfall integration)

Requirements Azure ARC (Azure part)

1. Azure ARC commands must be able to integrate into a third-party command/ctrl GW on a RESTful API (HTTPS)
2. Azure ARC must provide a RESTful API (HTTPS) for command and acknowledgement and status information

Requirement Azure ARC Agent

1. The Azure ARC agent must be able to receive commands from the command/ctrl GW on a RESTful API (HTTPS)
2. Azure ARC Agent must provide a RESTful API (HTTPS) for command and acknowledgement and status information

Other Azure Agents (not yet clear how many agents that are required)

1. The Azure “nn” agent must be able to receive commands from the command/ctrl GW on a RESTful API (HTTPS)
2. Azure “nn” Agent must provide a RESTful API (HTTPS) for command and acknowledgement and status information

3

Infrastructure Monitoring

ARC and Open telemetry enabled products through Azure Monitoring. Deployments in HQ and wind power plants MSFT needs to provide data extraction, injection APIs and alarming. Thresholds are required (Models)

Requirements

1. Azure Monitor (@ power plant) must be able to run autonomously at power plant (both reduced and no connectivity)
2. It must be possible to create Alerts and forward these either through web hooks and syslogs
3. It must be possible to stream raw data to MQTT or provide the raw data on a RESTFul API (HTTPS)

4

Cyber Security

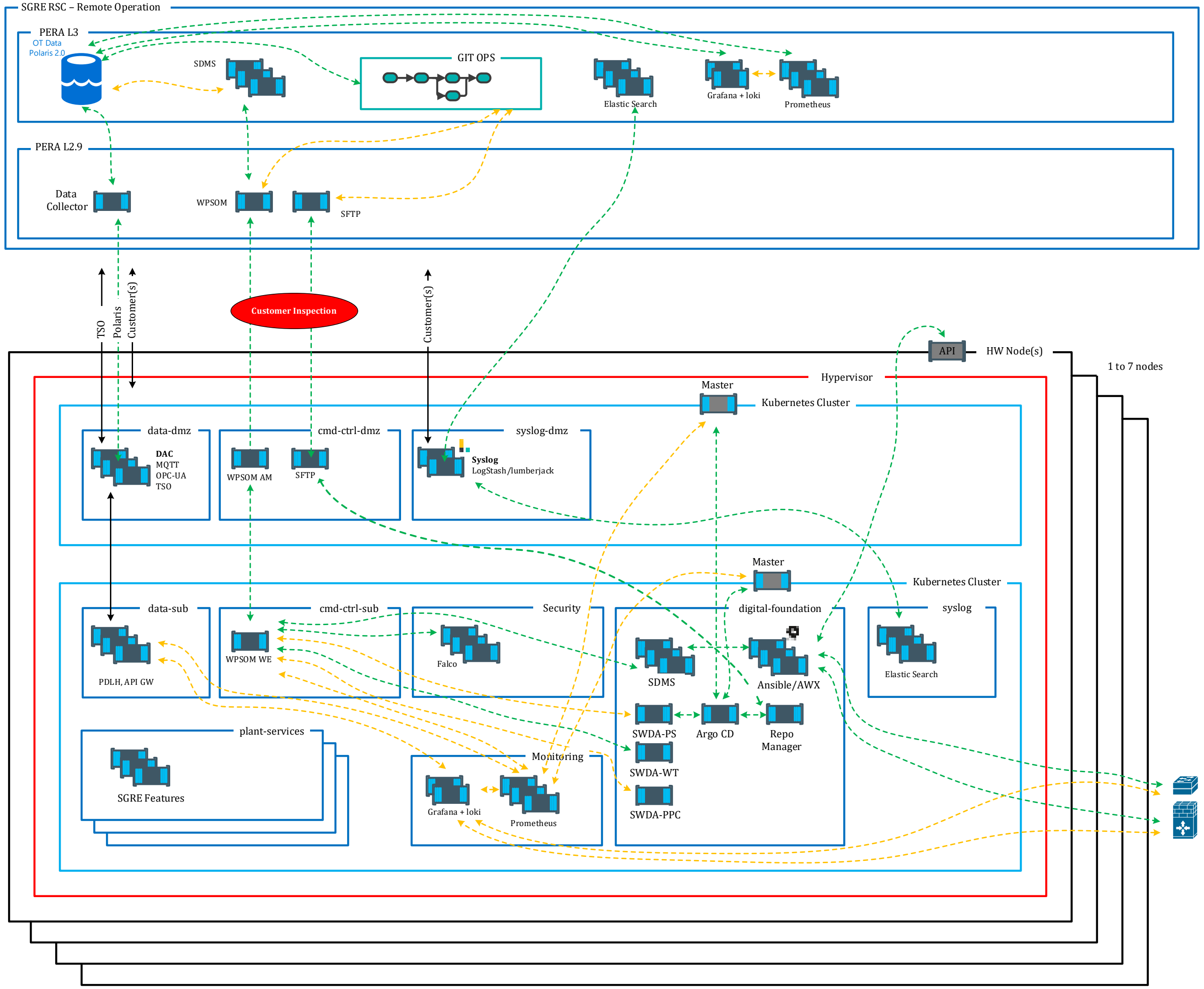
Server and Container Orchestration detection through defender products deployed in the wind power plants.

1. Defender for Containers must provide a RESTFul API (HTTPS) for control and feedback
2. Defender for container must throw syslog events on any detections or issues
3. Server and Container orchestration hardening though Azure Policy deployed at wind power plants (Not possible according to Redmond meeting)

Digital Foundation – Hybrid connected sites (Multi vendor Integration)

Technology Stack

- Single or multiple HW nodes
- Hypervisor
- Multi node Kubernetes clusters (DMZ, Substation)
- ARGO CD
- Grafana + Loki & Prometheus for monitoring
- Siesta (CI/CD Tools)
- KubeBench & Falco (EPP)
- Elastic Stack



Digital Foundation – Hybrid connected sites (Multi vendor Integration)

Technology Stack

- Single or multiple HW nodes
- Hypervisor
- Multi node Kubernetes clusters (DMZ, Substation)
- ARGO CD
- Grafana + Loki & Prometheus for monitoring
- Siesta
- KubeBench & Falco
- Ansible
- Elastic Stack

HW Scalability
Single HW node support
Multi HW nodes setup, Physical HA cluster for DMZ and HA cluster for Substation zone

OS Distribution
Linux, optimized for Container orchestration, windows does not currently provide the handles we need for configuration monitoring (standard compliance)

Hypervisor
Microsoft Hyper-V, Proxmox VE, Red Hat KVM or Canonical KVM

CMD & Control
<u>Option 1</u>
Modularize and containerize current product WPSOM

<u>Option 2</u>
Stitching and integration of multivendor products to support the cyber security products. This requires that MSFT provide APIs for CMD/CTRL integration and for data injection. (Waterfall integration)

IAM
Azure Entra ID in SGRE RSC PERA level 2.9.
Duende Implementation in Wind Power Plant

- Trust to Customers IAM
- Trust and bidirectional sync to Siemens Energy Wind Power mote Service Center (RSC)

Deployment
Deployment through GitOps principles through the CMD& control gateway. (Current Architecture)
Deployment tools deployed on the wind power plants

Infrastructure Monitoring
Prometheus and Grafana integration supporting Open Telemetry standard (Zabbix cannot integrate to OTel !).
Integration with CMD/CTRL (deployment of Models) and Data Access for operations in SGRE RSC

Cyber Security

- Protection and Hardening through immutable OS and Container orchestration hardening validated by Siesta scans and KubeBench
- Detection in Container orchestration layer through Falco
- Logging and Auditing through Elastic family
- Backup Restore solution through Veeam.
  5 years retention and offloading to customers.

Risk & Opportunities – Digital Foundation Technology stack options comparison

Microsoft scenario

- Immaturity of technologies to be implemented in our product may affect timeline
- Stakeholder commitment
- Intellectual property
- Vendor lock-in
- Air gapped not supported
- Cyber security threat

- Access to Expertise- No need to develop knowledge on subject matter areas
- Share capacity to develop with Microsoft, offered
- Risk sharing
- Enhance focus on other activities
- Cybersecurity partner that supports the Cybersecurity threat

Multivendor scenario

- Development of internal knowledge not ready on time
- Deliver on time due to resources focus activities
- Complexity on orchestration supply chain
- Cyber security threat

- Internal valuable knowledge
- Multivendor approach ensures not single supplier dependency
- Time to market
- Caching technologies
- All scenarios (connected, Hybrid & Air gapped) covered by the same team

Both options may require a 3rd party partnership for Digital Foundation