S4 – Proof of Concept (POC) Pavilion

Simulated Automotive Manufacturing Plant Environment

Prepared for S4x26

Version 1.0

5 November 2025

Booz Allen®

Table of Contents

Table of Figures

Overall Environment Description

The POC Pavilion environment consists of two skids and a half-height server rack designed to simulate key stages of an automotive manufacturing plant, specifically Paint Shop and Assembly. Each area is built around a dedicated skid equipped with representative industrial control systems, physical devices, and network infrastructure as well as a half-height server rack for applicable network infrastructure and servers.

Figure 1 Photograph of Two Production Skids

Paint Shop Skid

The Paint Shop skid simulates the vehicle E-Coat process. It begins with the vehicle body arriving from a pre-treatment stage, followed by immersion in an E-Coat bath to bind paint particles. The process continues through a rinsing phase and concludes with oven baking to cure the finish.

Assembly Skid

The Assembly skid simulates the mechanical and cosmetic assembly of vehicle components. The process includes:

- Marriage Station (joining chassis and body)
- Door Installation
- Exterior Panel Assembly
- Glass Installation
- Exterior Trim & Finish
- Completion Marking

Server Rack

In addition to the two skids, the POC Pavilion environment includes a 25U half-height standard depth server rack. This rack is included as part of the environment to contain various network switch infrastructure, servers, and provide space if needed for any vendor solutions. Due to the electrical capabilities of the S4 conference hotel environment, only standard 120V electrical power will be available on the PDU.

Production Line Overview

Paint Shop Skid (E-Coat)

This line simulates the electrocoating (E-Coat) stage of an automotive paint shop.

The process flow includes:

- **Vehicle Arrival from Pre-Treatment**

  The vehicle body enters the E-coat line after undergoing surface cleaning and preparation.
- **E-Coat Bath (Electrocoating)**

  The vehicle is submerged in a bath containing electrically charged paint particles. A DC current is applied, causing the paint to adhere uniformly to the metal surface. This ensures corrosion resistance and a consistent coating thickness.
- **Rinsing Stage**

  After the E-Coat bath, the vehicle is rinsed to remove excess paint and any contaminants. This step ensures surface cleanliness before curing.
- **Curing Oven**

  The coated vehicle is baked in an oven to cure the paint, hardening the coating and ensuring durability.

E-COAT HMI

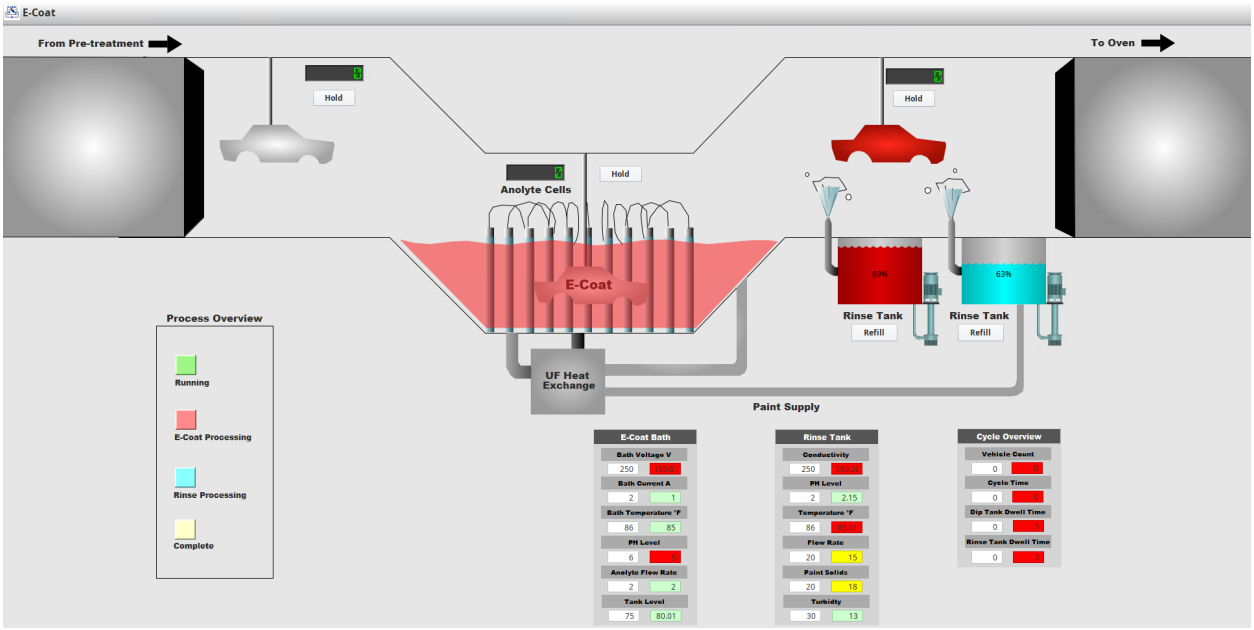

Figure 2 E-Coat HMI Diagram

PAINT SHOP KPIS

- OEE (Overall Equipment Effectiveness)
- Target Production
- Stage Metrics

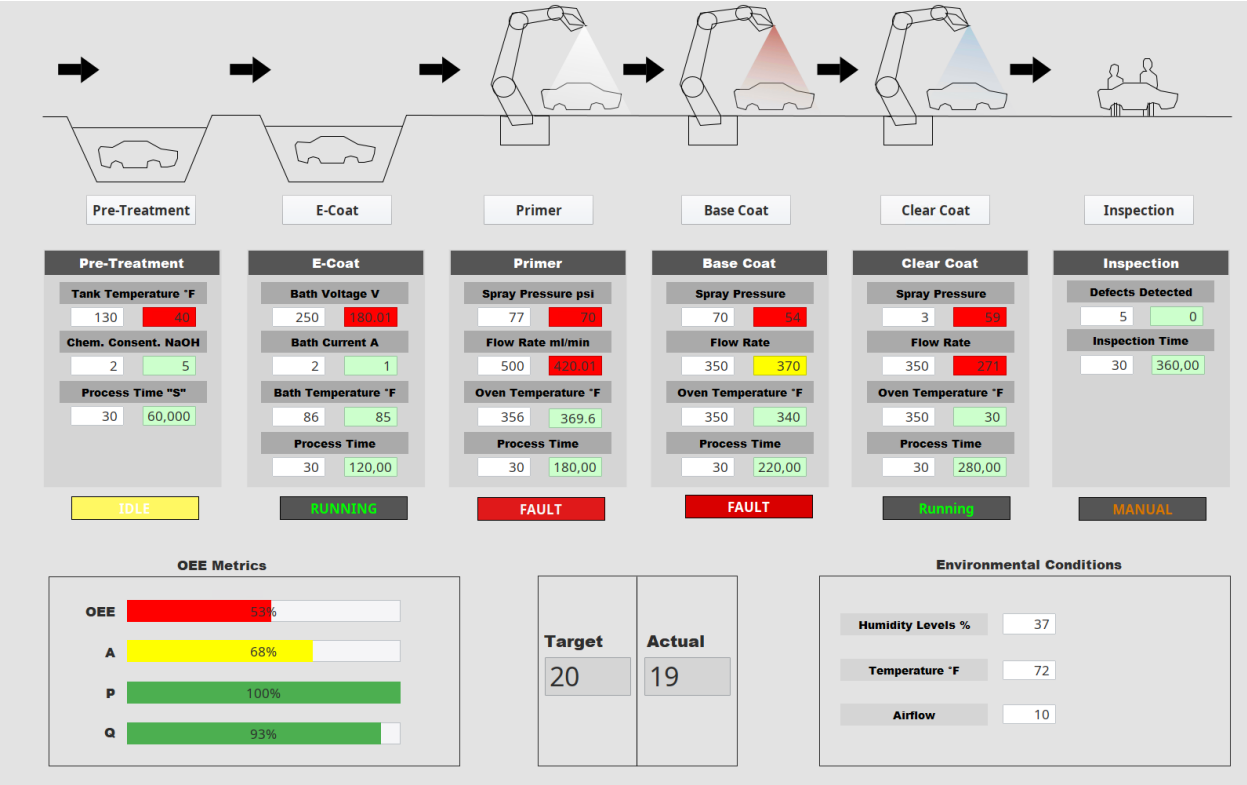

Figure 3 Paint Shop KPI diagram

Assembly Skid (Exterior Assembly)

This line simulates the exterior assembly stage of an automotive production line. It focuses on the integration of major vehicle components.

The process flow includes:

- **Marriage**

  The vehicle chassis and body are joined together.
- **Door Installation**

  Doors are installed and aligned.
- **Exterior Panel Assembly**

  Panels such as fenders, bumpers, and hoods are attached.
- **Glass Installation**

  Windshields and windows are installed.
- **Exterior Trim & Finish**

  Final cosmetic components like lights, badges, and trim are added.
- **Inspection & Completion**

  The vehicle undergoes a final inspection and is marked as complete.

EXTERIOR ASSEMBLY HMI

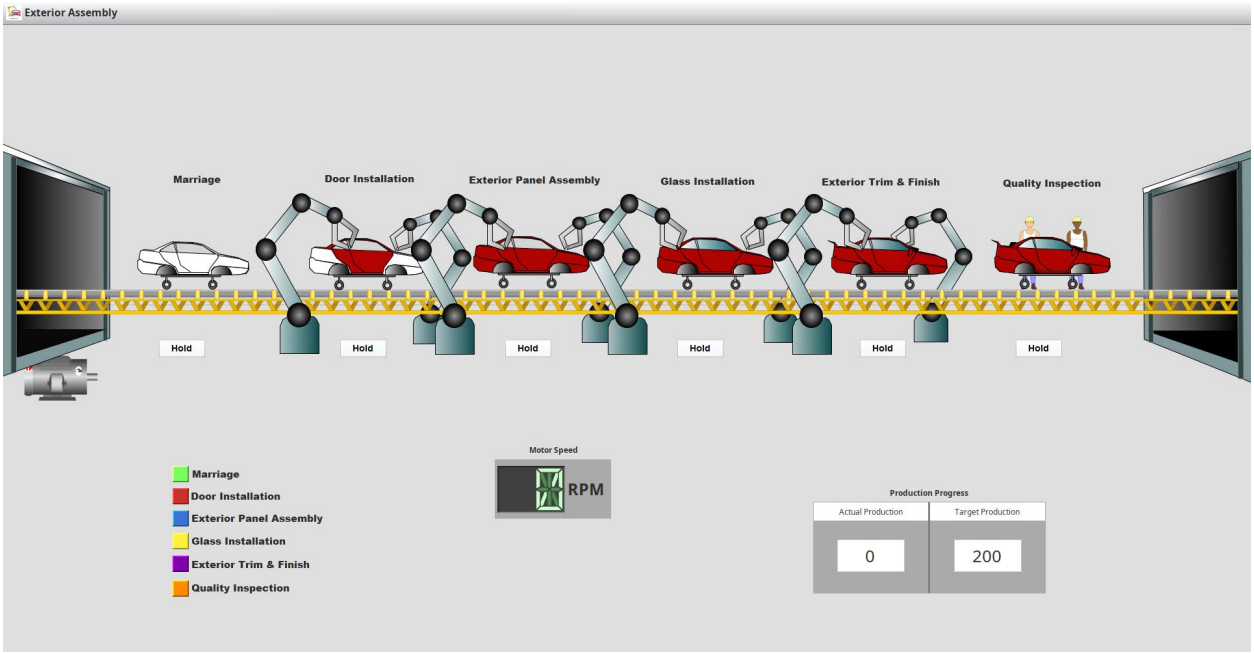

Figure 4 Exterior Assembly HMI Diagram

ASSEMBLY KPIS

- OEE
- Target Production
- Stage Metrics

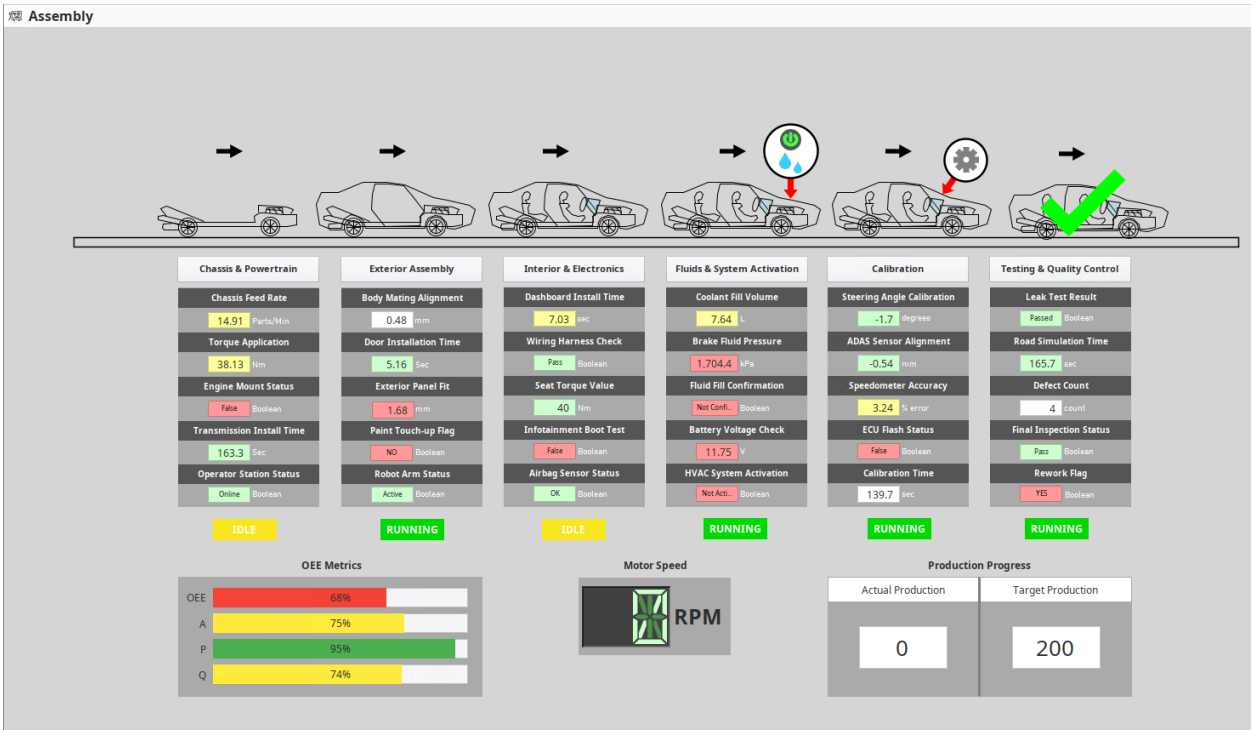

Figure 5 Assembly KPI diagram

Workflow from Scheduling to Completion

PAINT SHOP WORKFLOW

- A production order is created to process a batch of vehicles (e.g., 5 units).
- Vehicles are scheduled for the E-Coat bath.
- Each vehicle progresses through the E-Coat, rinse, and oven stages.
- Completion is tracked and recorded in the SCADA system.

ASSEMBLY WORKFLOW

- A production order is created for a batch of vehicles (e.g., 10 units).
- Vehicles are scheduled for exterior assembly.
- Each vehicle progresses through the marriage, installation, and inspection stages.
- Completion is tracked and recorded in the SCADA system.

OT Environment Description

The OT environment is structured according to the Purdue Model (Levels 0-4), with each skid containing representative devices and systems that reflect real-world industrial operations. Below is a breakdown of the components and layout across both skids.

Paint Shop Skid

LEVEL 0 – PHYSICAL PROCESSES

- MQTT-based temperature & humidity sensors
- Physical control panel with I/O indicators and manual controls

LEVEL 1 – INTELLIGENT DEVICES

- Siemens LOGO!
- SIMATIC S7-1200
- SIMATIC S7-1500
- SIMATIC HMI touchscreen mounted on the control panel

LEVEL 2 – SUPERVISORY CONTROL

- Siemens Engineering Workstation (Windows 11, physical)
- Ignition Operator Workstation (Windows 10, physical)
- All level 0-2 devices connect to a Moxa EDS-508A switch, with uplink to level 3 via Cisco IE9300

Assembly Skid

LEVEL 0 – PHYSICAL PROCESSES

- Motor and Allen Bradley PowerFlex Variable Frequency Driver (VFD)
- Physical control panel with I/O indicators and manual controls

LEVEL 1 – INTELLIGENT DEVICES

- Allen Bradley CompactLogix 5370
- Allen Bradley MicroLogix 1400
- Allen Bradley Micro 820
- Allen Bradley PanelView 5000 touchscreen mounted on the control panel

LEVEL 2 – SUPERVISORY CONTROL

- Rockwell Engineering Workstation (Windows 11, physical)
- Ignition Operator Workstation (Windows 7, physical)
- All level 0-2 devices connect to a Stratix 5200 switch, with uplink to level 3 via Cisco IE9300

Shared Systems & Infrastructure

LEVEL 3 – PLANT OPERATIONS

- Ignition Plant Ops OWS (Windows Server 2022, VM) – Provides operator access to SCADA visualizations and controls for both Paint Shop and Assembly skids through the Ignition platform
- Ignition MES Console (Windows Server 2022, VM) – Provides access to MES-related views and dashboards within the Ignition platform. Used for monitoring production workflows, scheduling and KPI tracking.
- Kepware OPC Server (Windows Server 2022, VM) – Used to pull a small number of tags from select PLCs. Most PLCs communicate directly with Ignition via OPC UA.
- Historian (Windows Server 2022, VM) – Logs and stores process data
- All systems connected to Cisco IE 9300 switch

LEVEL 3.5 – INDUSTRIAL DMZ

- Palo Alto PA-220 Firewall to control flow in and out of the DMZ
- Ignition Server (Windows Server 2022, VM) – Running Ignition version 8.3. Hosts SCADA projects for both Paint Shop and Assembly skids, with MES functionalities configured within the Ignition platform
- Jump Server (VM) – Secure remote access
- Tools/MQTT Server (Windows Server 2022, VM) – Handles IIoT sensor data. MQTT functionality will be handled through Ignition's licensed modules. This server also hosts OT cybersecurity tools and software. Configuration is still in progress
- Active Directory Server (Windows Server 2022, Physical) – Used to manage user authentication, access control, and centralized identity management across the environment.

LEVEL 4 – ENTERPRISE

- Cisco 9200L switch connected to a second Palo Alto PA-220 Firewall
- User Workstations (Windows 11 VMs) for enterprise-level interaction

Network Architecture

Architecture Drawing

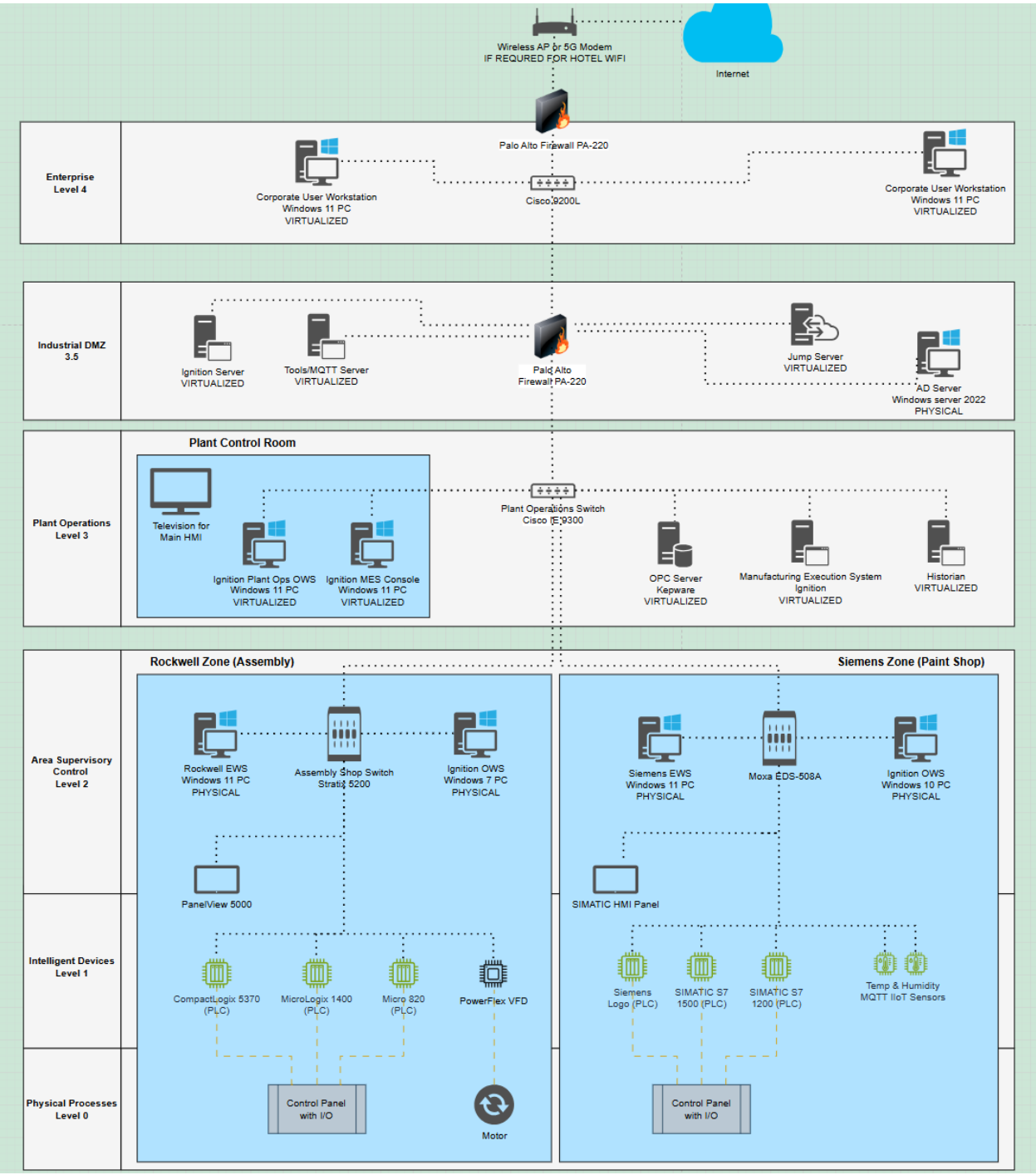

Figure 6 Network Architecture

IP Adress Schema

Enterprise Level 4	10.128.40.0/24
Industrial DMZ Level 3.5	10.128.35.0/24
Plant Operations Level 3	10.128.30.0/24
Area Supervisory Control L0-2 – Rockwell Zone	192.168.25.0/24
Area Supervisory Control L0-2 – Siemens Zone	192.168.20.0/24

Routing/VLANS

Currently, only the Enterprise network (10.128.40.0/24) is configured on the Enterprise firewall and the 9200L switch utilizing VLAN 40. From the Enterprise firewall out to the Internet, there is a static default route allowing all unknown traffic out Ethernet 1/1 which will also go through NAT on the outside interface. There are also static routes on the Enterprise firewall that point to the iDMZ firewall for devices on Levels 3.5 to Level 0.

All other networks reside on the iDMZ firewall and the IE9300 switch, their VLANs are as follows:

- Industrial DMZ – VLAN 35
- Plant Operation – VLAN 30
- Rockwell Zone – VLAN 25
- Siemens Zone – VLAN 20

At this current time, the Enterprise firewall has an ‘Any Any’ Rule in place but is subject to change as the network matures. On the iDMZ firewall, direct communication between the Plant Operations zone and Enterprise Zone in both directions is not allowed. Also, communication between the Rockwell network and the Siemens network are blocking all traffic between the networks. This is also subject to change as needed.

Firewall Rule Sets

The OT network is segmented into distinct zones (Control, DMZ, Enterprise), with firewall rules in place to manage traffic and ensure security. The table below summarizes key rules:

Enterprise Zone	Plant Operation Zone	Any	Blocked
Plant Operations Zone	Enterprise Zone	Any	Blocked
Rockwell Zone	Siemens Zone	Any	Blocked
Siemens Zone	Rockwell Zone	Any	Blocked

Software & Asset Inventory

Software Application

Ignition SCADA	SCADA visualization & control	Virtual SCADA Server
Siemens TIA Portal	Engineering and programming (Siemens PLCs)	Physical PLC Programming Server
Studio 5000	Engineering and programming (Allen-Bradley PLCs)	Physical PLC Programming Server
Kepware	Communication bridge and data aggregation	Virtual Kepware Server
Proxmox	Hypervisor for virtualization	Physical Proxmox Server
Crowdstrike	Endpoint protection and threat detection	All Windows Systems
Active Directory	Identity and access management	Virtual AD Server

Hardware Asset Inventory

Paint Shop	Intel	NUC8i5BEH	NUC (PC)
Paint Shop	Intel	NUC8i5BEH	NUC (PC)
Paint Shop	Beetronics	19TS7M	19 in. Touch Screen Monitor
Paint Shop	Beetronics	19TS7M	19 in. Touch Screen Monitor
Paint Shop	Moxa	EDS-508A	Industrial Managed Switch
Paint Shop	MokerLink	IND-F041FP	Industrial Managed Switch
Paint Shop	Monigear	MN-NTHM	Temperature and Humidity Sensor
Paint Shop	Monigear	MN-NTHM	Temperature and Humidity Sensor
Paint Shop	Siemens	Simatic S7-1500	PLC
Paint Shop	Siemens	LOGO!	PLC
Paint Shop	Siemens	Simatic S7-1200	PLC
Paint Shop	Siemens	Simatic HMI	HMI
Paint Shop	NVVV	DR-120-24	AC to DC DIN-Rail Power Supply
Paint Shop	CHTAIXI	DZ47N-63	AC Circuit Breaker
Assembly Shop	Intel	NUC8i5BEH	NUC (PC)
Assembly Shop	Intel	NUC8i5BEH	NUC (PC)
Assembly Shop	Beetronics	19TS7M	19 in. Touch Screen Monitor
Assembly Shop	Beetronics	19TS7M	19 in. Touch Screen Monitor

Assembly Shop	Stratix	5200	Industrial Managed Switch
Assembly Shop	Allen Bradley	PowerFlex 523	Variable Frequency Drive (VFD)
Assembly Shop	IronHorse	MTR-P33-3BD36	General Purpose Industrial Motor
Assembly Shop	Allen-Bradley	PanelView 800	HMI
Assembly Shop	Allen-Bradley	MicroLogix 1400	PLC
Assembly Shop	Allen-Bradley	CompactLogix L30ER	PLC
Assembly Shop	Allen-Bradley	Micro820	PLC
Assembly Shop	Mean Well	DR-120-24	AC to DC DIN-Rail Power Supply
Assembly Shop	CHTAIXI	DZ47N-63	AC Circuit Breaker
Server Rack	Palo Alto	PA 220	Firewall
Server Rack	Palo Alto	PA 220	Firewall
Server Rack	Cisco	IE9300	Switch
Server Rack	Cisco	9200L 48 PoE+ 4x1G	Switch
Server Rack	Dell	PowerEdge R430	Proxmox Hypervisor
Server Rack	Dell	PowerEdge R330	Proxmox Hypervisor

Corp Workstation 1	Win 10	Enterprise L4	Enterprise user
Corp Workstation 2	Win 11	Enterprise L4	Enterprise user
Tools/MQTT Server	Server 2022	iDMZ L3.5	OT tools and software
Jump Server	Server 2022	iDMZ L3.5	Remote access
Ignition Server	Server 2022	iDMZ L3.5	SCADA server
OPC Server	Server 2022	iDMZ L3.5	Communication server

Security Access

User Roles & Access Control

Access to the simulated OT environment is segmented by user roles, each with defined permissions. The table below outlines the roles and their access levels:

Operator	Limited (HMI Only)	Ignition SCADA	Limited access to production data
Engineer	Full (PLC & SCADA)	TIA Portal, Studio 5000, Ignition SCADA	Can modify PLC logic and troubleshoot
Administrator	Full (All systems)	Proxmox, Virtual Servers, Switches, Firewalls	Manages user roles and system configs
Vendor (Demo)	Restricted	Virtual Servers	Temporary access for testing tools

MES Functions (Integrated into Ignition)

MES functionalities are embedded directly into the Ignition SCADA, rather than by a separate MES system. These functions include:

- **Production scheduling**

  Vehicle batches (e.g., 5 for E-Coat, 10 for Assembly) are scheduled through Ignition interfaces.

- **Process Tracking**

  Ignition monitors each vehicle's progress through the Paint Shop and Assembly stages using simulated PLC data.

- **KPI Monitoring**

  OEE, target production, and stage-specific metrics are visualized within Ignition dashboards.

Note: All MES-related data is simulated and managed within Ignition

PLC & Program Details

Siemens PLC	S7-1500	TIA Portal	Paint Shop control	OPC UA (direct to Ignition)	Ignition Vision
Siemens PLC	S7-1200	TIA Portal	Paint Shop control	OPC UA (direct to Ignition)	Ignition Vision
Siemens PLC	LOGO!	LOGO! Soft Comfort	Paint Shop control	OPC UA via Kepware OPC Server	Ignition Vision
Rockwell PLC	Micrologix 1400	RSLogix 500	Assembly control	OPC UA (direct to Ignition)	Ignition Vision
Rockwell PLC	CompactLogix L30ER	Studio 5000	Assembly control	OPC UA (direct to Ignition)	Ignition Vision
Rockwell PLC	Micro820		Assembly Control	OPC UA via Kepware OPC Server	Ignition Vision
VFD + Motor	General Motor + VFD	N/A - (controlled via PLC)	Conveyor movement (Assembly)	Ethernet/IP → PLC → OPC UA	Ignition Vision
Environmental Sensors	Temp & Humidity Sensors	N/A (MQTT-based)	Paint shop environmental monitoring	MQTT → Ignition	Ignition Vision

Additional Notes

- Tag Communication:
  - Most PLCs communicate directly with Ignition via OPC UA.
  - Two PLCs (LOGO!, Micro820) route tags through Kepware OPC Server.
  - Environmental sensors use MQTT to send data to Ignition.