Figure MES and Enterprise Software IT/OT Environment

By April Zheng 4 min 9

0. Overview

Key tasks, best practices, and action items for maintaining the OT/IT production environment for the MES system and enterprise software landscape.

1. OT Infrastructure / Industrial Control Systems (ICS) and Network Configuration

Owners: @Matt DeDonato @April Zheng

VLAN Segmentation

- **Action:** @Matt DeDonato configure VLAN segmentations (Fig.1) across the OT network to secure manufacturing field devices for the manufacturing line (Fig.2), including:
  - Atlas Copco Tools
  - Barcode Scanners
  - HMIs
  - Laser Machines
  - Testers

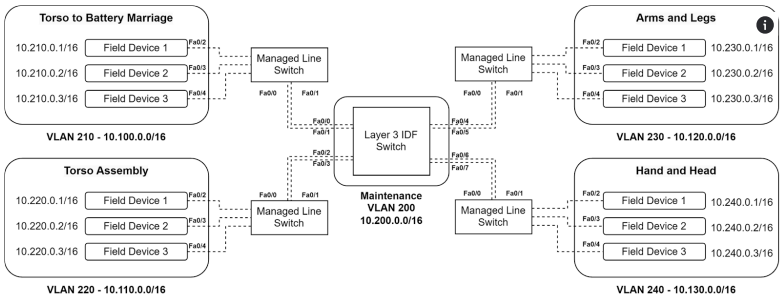

Fig.1 Sample Redundant Star Topology of Main Lines

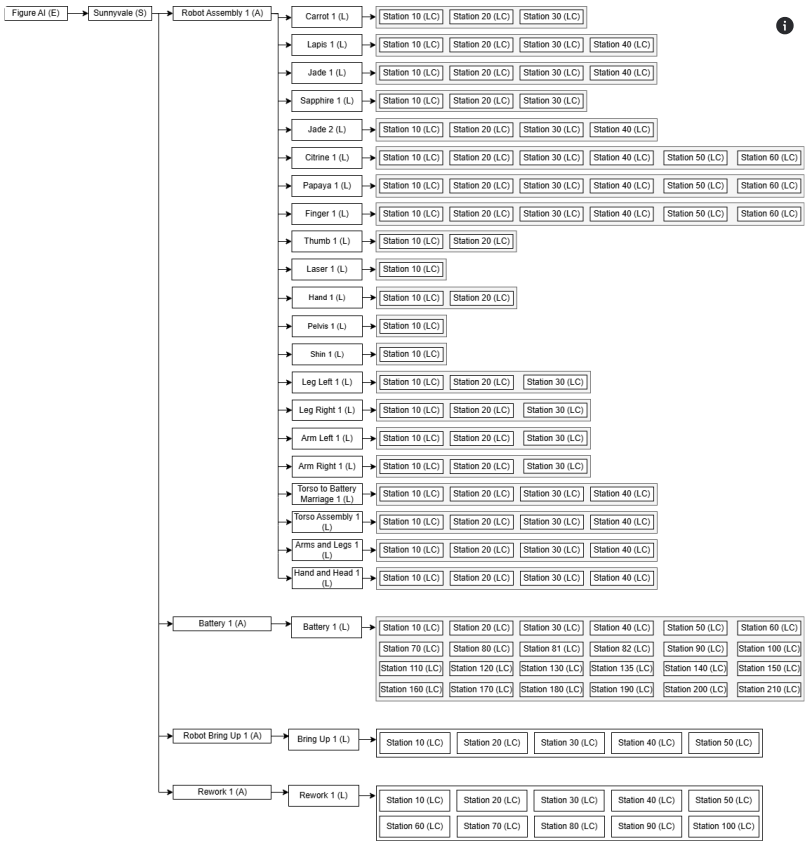

Fig.2. ISA -95 Equipment Tree Diagram

Field Device Setup

- **Action:** @April Zheng will configure all field devices and provide @Matt DeDonato with a list for:
  - Firewall IP whitelisting
  - MAC filtering
  - Additional network configurations (if applicable)

OT Security Best Practices

- **Secure Web Access:** MES will use **HTTPS** instead of HTTP for all web clients @April Zheng .
- **ICS / OT Asset Management:** Workstations and HMIs **must not** communicate directly with the internet @Matt DeDonato .
- **Account Security & Password Management:**
  - Implement **LDAP** for centralized user management (@April Zheng **for MES,** @Matt DeDonato **for Active Directory/Okta**).
  - Role-Based Access Control (RBAC) for all HMIs and workstations (@April Zheng).

---

2. MES Server Management and Full IT/OT Architecture Diagram

Owners: @Jared Rodgers @Damien Bardon @April Zheng

OT/IT Architecture Diagram

Here is an overview of the full OT/IT architecture diagram (Fig.3) and server architecture diagram (Fig.4).

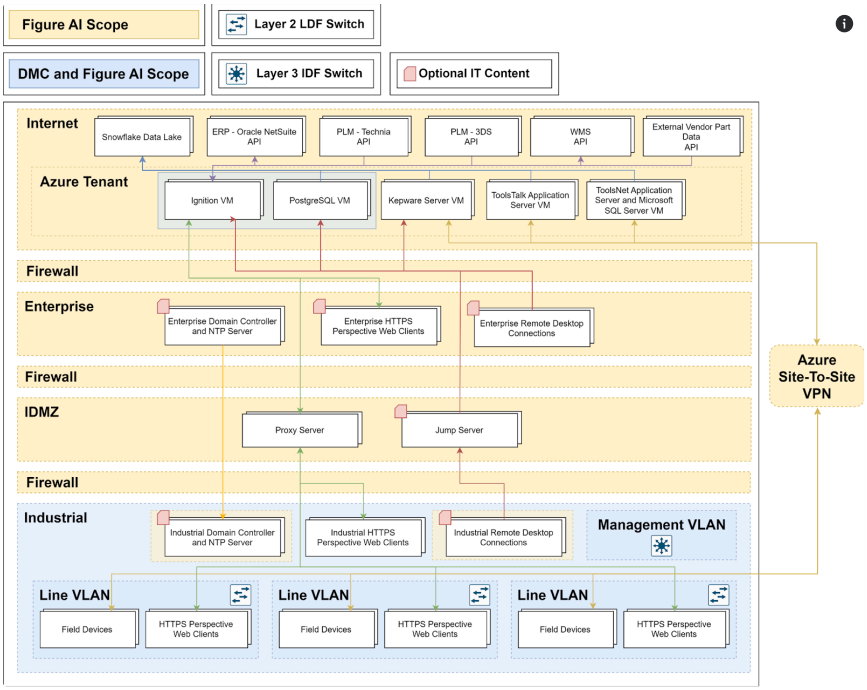

Fig.3 Full OT/IT Architecture Diagram

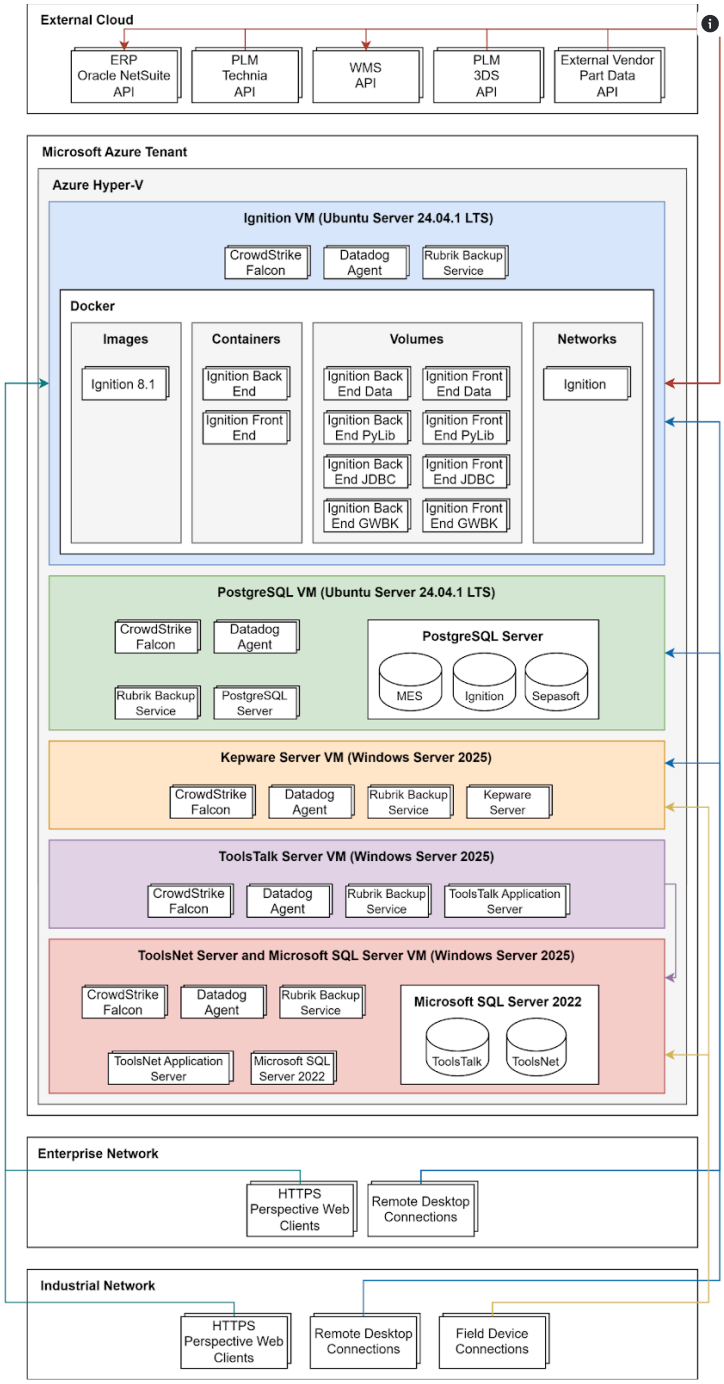

Fig.4 Server Architecture Diagram

Virtual Machine (VM) Deployment

- **Cloud Deployment (Initial Phase):**
  - High availability ensured with four internet connections.
- **On-Prem Consideration:**
  - Logan is recruiting an OT/IT specialist.
  - On-prem solution will be revisited in May.
  - Logan to help allocate resources as needed.

MES Server Configuration & Maintenance

- **Initial Setup:** Jared and Damien's team to configure and maintain three low-spec VMs:
  - **MES Frontend Server**
  - **MES Backend Server**

- **Database Server** (Specs in Table 1)

Table 1: Server Requirements

Function	Processor (Cores)	Memory (GB)	Storage (GB)	Operating System
Ignition Front-End Gateway	12	32	128	Ubuntu Server 24.04.1 LTS
Ignition Back-End Gateway	12	32	128	Ubuntu Server 24.04.1 LTS
PostgreSQL Database	4	8	1500	Ubuntu Server 24.04.1 LTS
Microsoft SQL Server 2022	4	8	1500	Ubuntu Server 24.04.1 LTS
Kepware Server	Negligible	Negligible	Negligible	Windows Server 2025
ToolsTalk Server	12	16	100	Windows Server 2025
ToolsNet Server	8	32	1500	Windows Server 2025

System specifications are chosen according to following sizing guides:

- Inductive Automation's Ignition server sizing recommendations
- Sepasoft's MES server sizing architecture guide
- Atlas Copco's ToolsTalk 2 installation guidelines
- Atlas Copco's ToolsNet 8 installation guidelines
- PTC's Kepware+ system requirements

Estimations account for 125%+ processing power and networking bandwidth to support 120 workstations, 150 HMI clients, and numerous devices. Server storage capacity is based on a maximum data retention policy of two (2) years.

Sizing estimations do not account for future applications or additions to the MES architecture. To properly account for expanded uses, specifications should be increased at Figure AI's discretion.

Identity Provider

To provide user authentication and role assignments to Figure AI users, the existing Figure AI Okta identity provider will be integrated and used as Ignition's identity provider. OIDC is recommended as a protocol for identity provider integration due to its advantages in authentication for mobile devices. If OIDC is not permitted by Figure AI requirements, SAML integration is additionally available.

Okta should only need the redirect URI of the gateway that will be used to perform testing, which is http://[HOST]:[PORT]/data/federate/callback/oidc. For the sandbox gateway, this will be http://192.168.4.6:8088/data/federate/callback/oidc. Once Ignition is added as an application in Okta, Ignition just needs the Client ID and Client Secret of that application to continue testing.

Software Version Control

- **Action:** Create a Git repository within the Figure repo for manufacturing software revision control, dns server configuration and security certification installation (**April, Jared, Damien**).
- **Access:** Git repo will be shared with MES integrators.

CI/CD and Server Maintenance

- **Action:** Jared and Damien to establish and maintain CI/CD pipelines and server environments.

Backup Strategy

- **Current Backup Solution:**
  - Azure Backup will be used for **server and database backups** (**Managed by Damien and Jared**).
- **Rubrik Backup:**
  - Currently on hold; noted by Michael that **Rubrik is air-gapped**, unlike standard Azure backup solutions.

---

3. Data Warehouse (Long-Term Plan)

Owners: All

Data Segmentation & Integration

- **MES Database Usage:**
  - Strictly for **controls and production data collection**.
  - Data mining and analysis will be performed in a separate **data lake**.
- **Proposal:** April suggested using **Snowflake** (or a similar platform) to:
  - Integrate **Figure data silos** (manufacturing, business, controls, etc.).
  - Enable **centralized analytics and visualization** across supply chain, manufacturing, field deployment, and service.

Unified Namespace & MQTT Integration

- **Action:**
  - MES and other systems should **share data** via **MQTT and a Unified Namespace**.
  - April will provide Ivan with necessary queries for further discussion.
- **Priority:** Not required for **Day 1**, but essential for long-term scalability.

---

4. Next Steps & Action Items

- **April:** Configure field devices, implement LDAP for MES, set up role-based access control, and establish a Git repository.
- **Matt:** Configure VLAN segmentation, enforce OT security best practices, and oversee network configurations.
- **Jared & Damien:** Configure MES servers, establish CI/CD pipelines, and maintain server environments.
- **Logan:** Hire an OT/IT specialist and revisit on-prem solutions in May.
- **Ivan:** Collaborate with April on queries for data lake integration.
- **April:** Need to get help for asset management.