



# Cybersecurity & Network Segmentation

Power/mation's Industrial Internet Solutions provide products and tools for network segmentation and cybersecurity for today's complex industrial control systems (ICS) and SCADA systems. The implementation of cybersecurity systems reduces the overall attack surface area of your network by identifying security weaknesses, prioritizing areas for improvement and mitigating immediate risks. Proper network segmentation provides full network visibility, control and protection.

## Security Must Always Come First

What is at risk when security is breached? An information technology (IT) attack could result in the theft of data and could divulge *confidential* business information. An operational technology (OT) attack could lead to damage in the physical world and losing *control* of equipment or a process. The diagram below shows the order of protection importance for each network segment, with security being first priority.



## Cybersecurity Framework Core

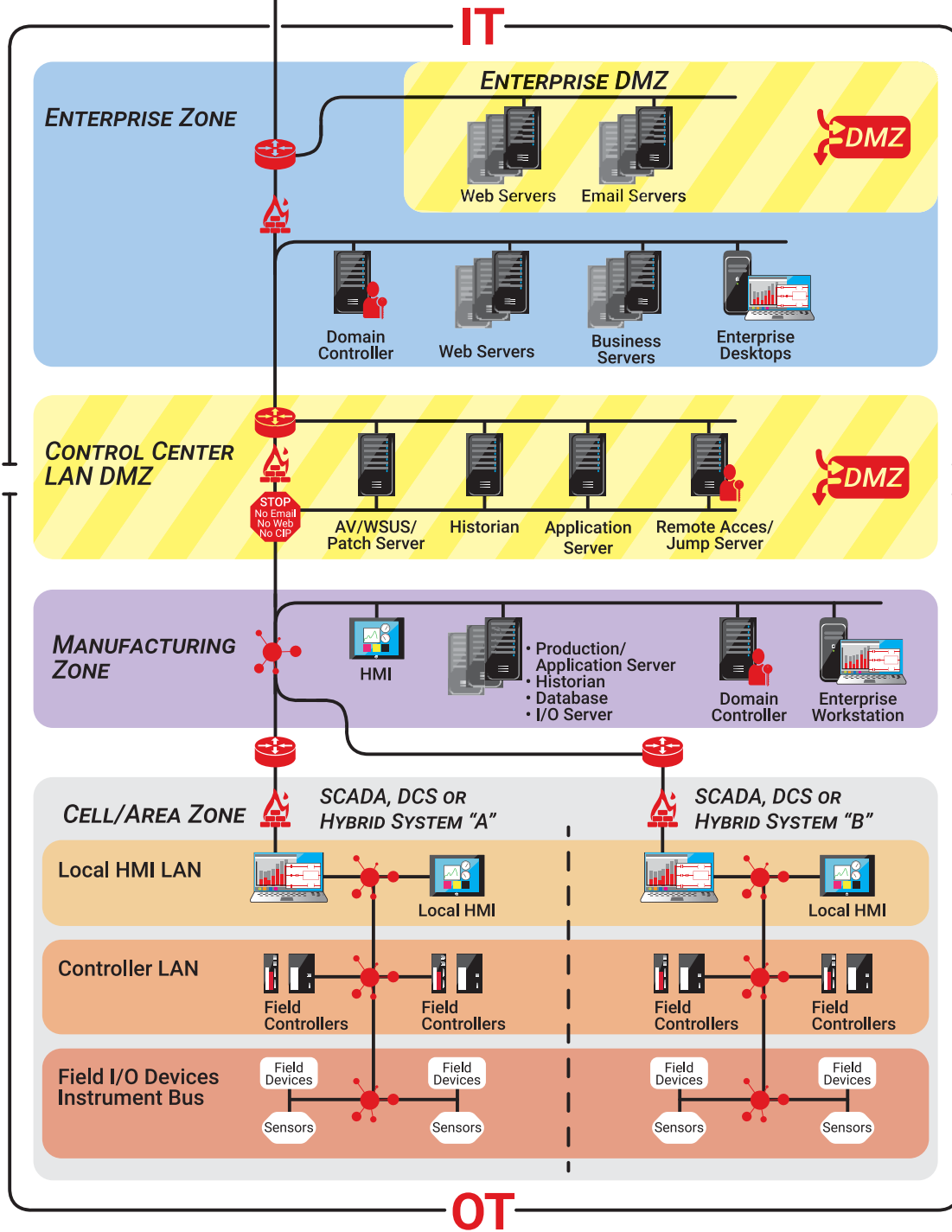
- 1. IDENTIFY** Establish an organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities.
- 2. PROTECT** Architect the appropriate safeguards to ensure delivery of critical infrastructure services. See reverse side for a modified Purdue model of secure architecture for ICS.
- 3. DETECT** Implement the intrusion detection and intrusion protection alert systems to identify the occurrence of a cybersecurity event.
- 4. RESPOND** Develop and execute the appropriate activities to take action regarding a detected cybersecurity event.
- 5. RECOVER** Restore any capabilities, services or data backups that were impaired due to a cybersecurity event.

## 7 ICS Defense Strategies

- Implement application whitelisting
- Ensure proper configuration and patch management
- Reduce surface attack area
- Build a defensible environment
- Manage authentication
- Monitor and respond
- Implement secure remote access



# Secure Architecture for Industrial Control Systems



## IT

### Information Technology

- Data Risks
- Office PCs
- Email & Web Browsing
- Business Data/ERP

## OT

### Operational Technology

- Physical Risks
- Machines
- SCADA
- Process Data/MES



### Demilitarized Zone

A DMZ exposes external-facing services to untrusted networks.



### Firewalls

- Stateful Firewalls
- IP & Port Filtering
- Bandwidth Throttling
- Deep Packet Inspection



### Gateways

- Routers
- Network Transitions
- Firewalls & ACLs



### User Access

- User Authentication
- Access Control Lists
- Jump Servers
- Remote Access



### Connectivity & Infrastructure

- Cordsets
- Switches



Distributor  
Automation & Controls



**Power/mation**

800.843.9859  
www.powermation.com

