ICS Security Architecture

Chris Hankin

Network Segmentation and Segregation

- Segmentation establishes security domains – uniform level of trust
- Minimise traffic across domain boundaries
- Segregation involves ruleset that defines which communications can happen across boundaries
- Network traffic different in OT layer – no email, internet or remote(?)

Common techniques

- Logical network separation enforced by encryption or network device enforced
  - VLANS
  - Encrypted VPNs
  - Uni-directional gateways – for example data diodes
- Physical network separation
- Network traffic filtering – network layer, state-based, port and/or protocol layer, or application layer

OSI Model – 7 layers

1. Physical – raw bit streams
2. Data link – reliable transmission of data frames
3. Network – addressing, routing and traffic control

4. Transport – segmentation, ack and multiplexing
5. Session
6. Presentation – encryption/decryption
7. Application – high level APIs

Defense in Depth

- Apply techniques at more than the network layer
- Use the principle of least privilege and need-to-know
- Separate information and infrastructure based on security requirements
- Implement whitelisting rather than blacklisting

Defense in Depth Layers

1. Security Management – incorporating risk management
2. Physical Security – access; people and asset tracking
3. Network Security – segmentation etc…
4. Hardware Security – various schemes (TPM, etc) but should not impact performance, safety etc…
5. Software security – allowlisting, patching, etc…

Boundary protection

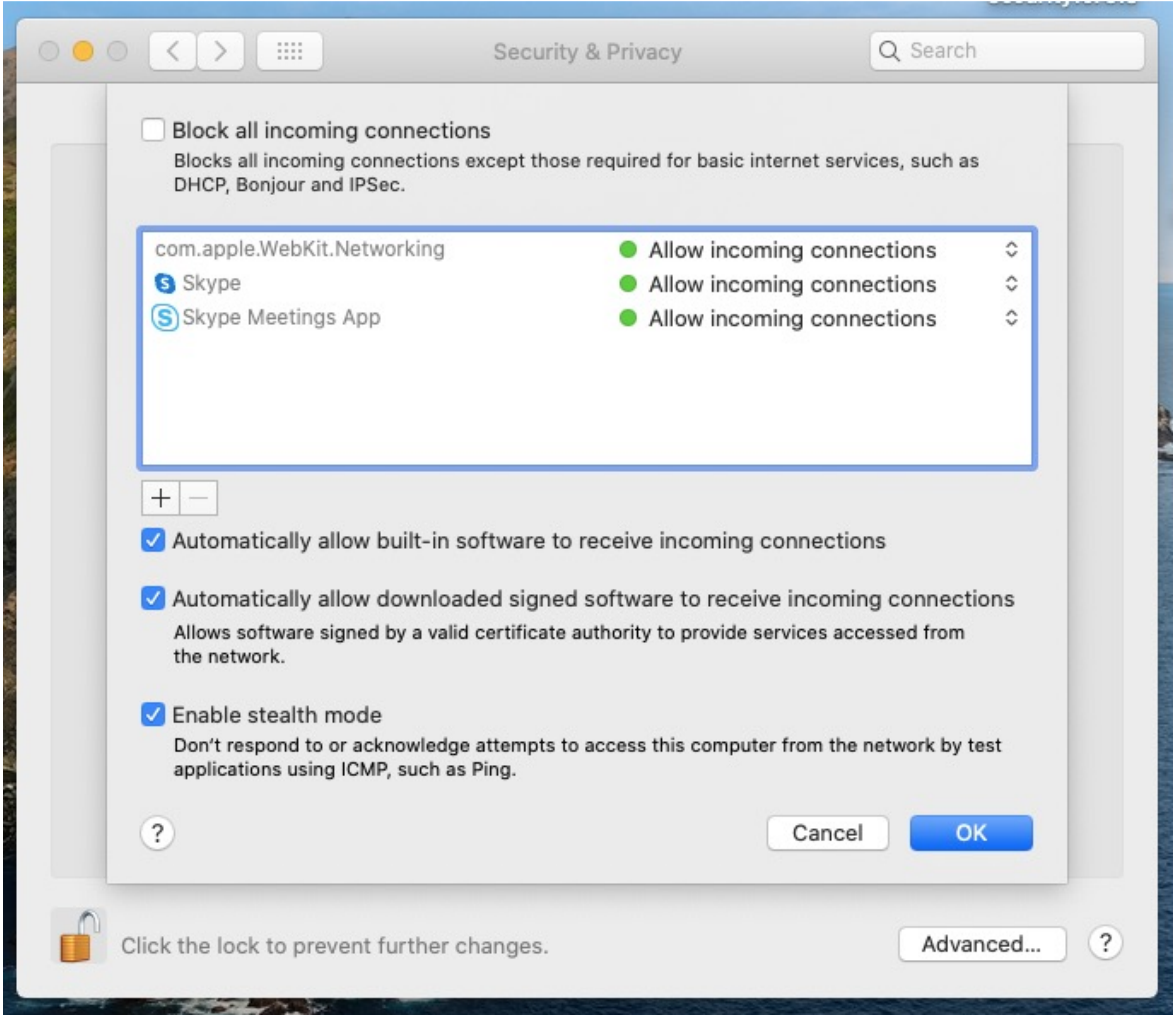
- Gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, HIDS and NIDS, encrypted tunnels, managed interfaces, mail gateways and uni-directional gateways.
- Demilitarized Zones (DMZ) – host or network segment between security domains.
- Configuration of boundary protection devices to fail in predetermined state – safety versus security

Firewalls

- Packet Filtering – access controlled by a ruleset; operate at network layer: drop, forward or send message to originator
- Stateful Inspection – transport layer firewall keeping track of sessions
- Application-Proxy Gateway – application layer firewall
- High security but performance overheads
- Internal or between ICS and Corporate network

Firewalls contd

- Blocking communications except those specifically allowed
- Enforcing secure authentication
- Enforcing destination authorization
- Recording information flow
- Implementation of ICS operational policies
- Designed with documented and minimal connections outside the ICS



□ Block all incoming connections

Blocks all incoming connections except those required for basic internet services, such as DHCP, Bonjour and IPSec.

com.apple.WebKit.Networking	● Allow incoming connections
Skype	● Allow incoming connections
Skype Meetings App	● Allow incoming connections

☑ Automatically allow built-in software to receive incoming connections

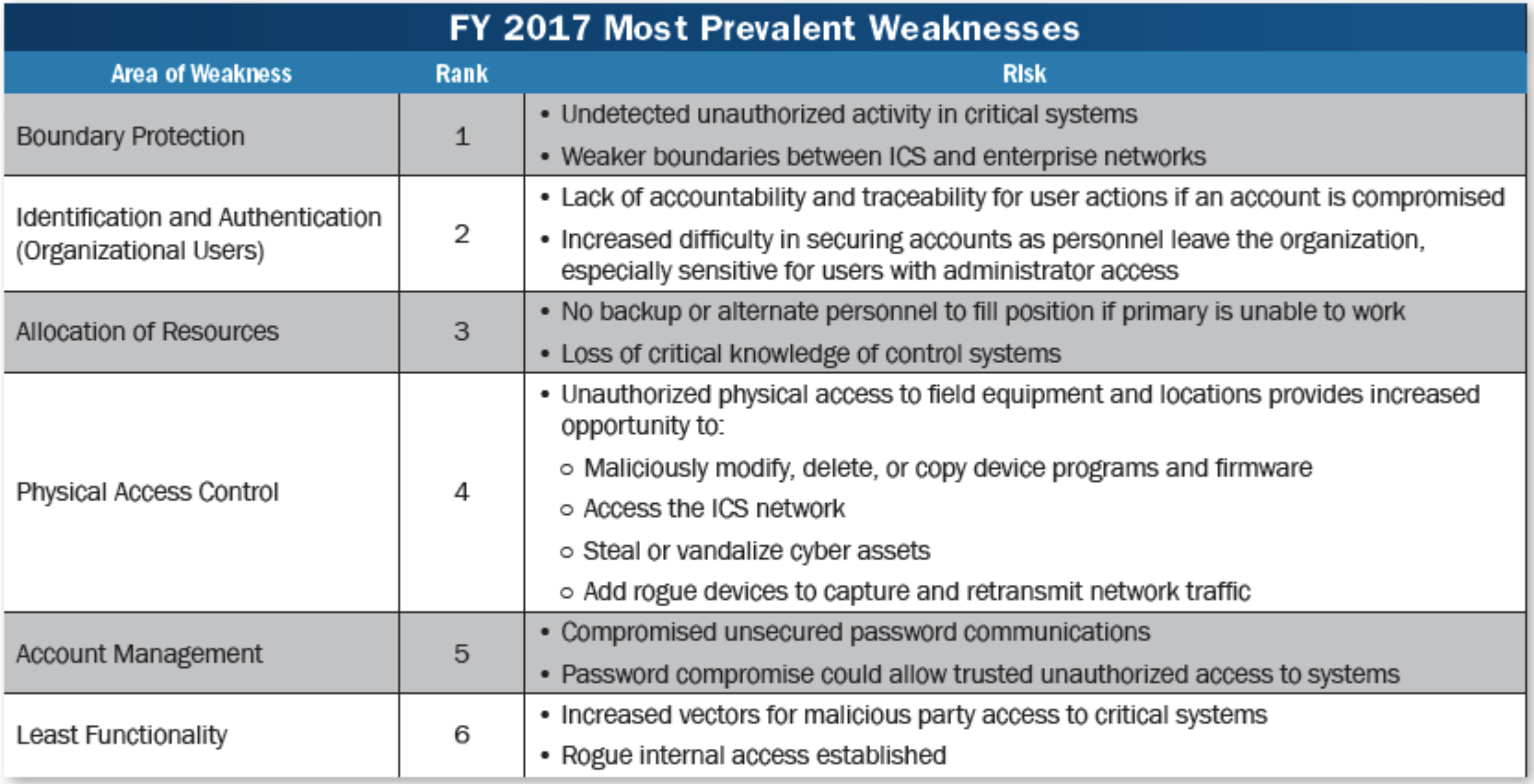
☑ Automatically allow downloaded signed software to receive incoming connections

Allows software signed by a valid certificate authority to provide services accessed from the network.

☑ Enable stealth mode

Don't respond to or acknowledge attempts to access this computer from the network by test applications using ICMP, such as Ping.

Click the lock to prevent further changes.



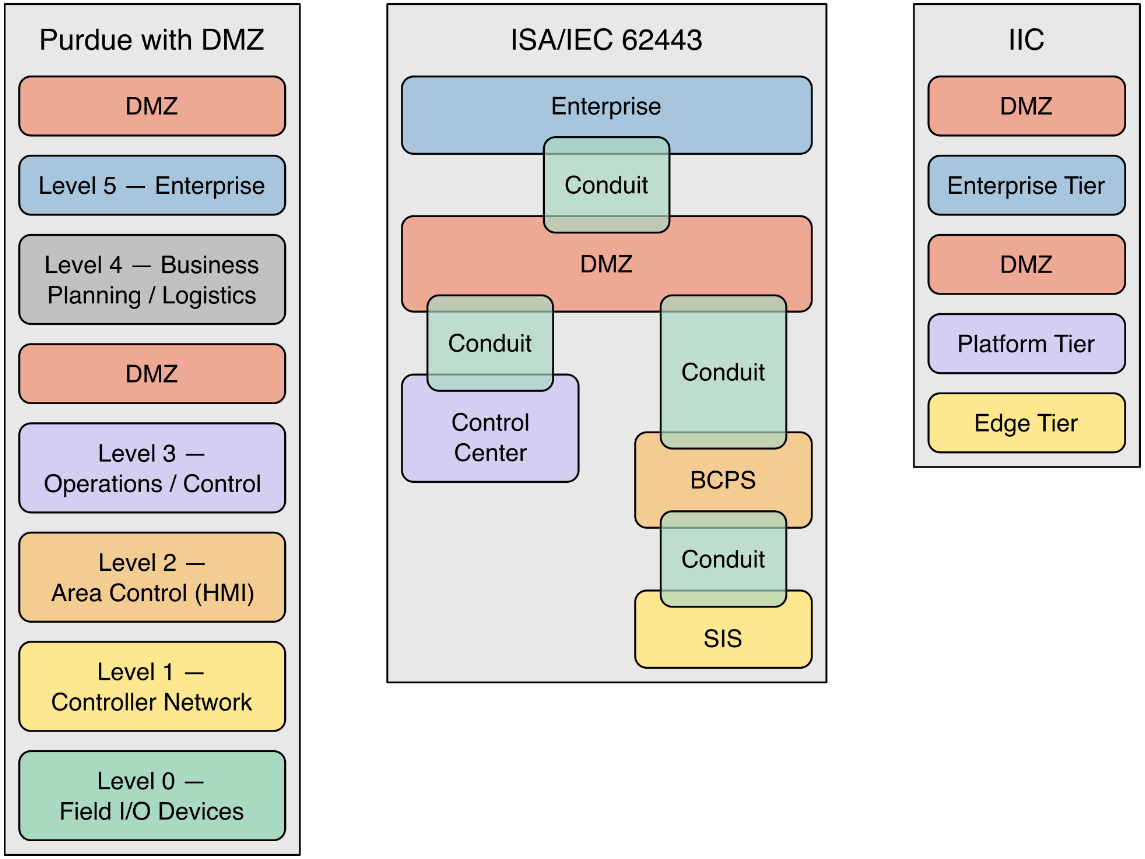
FY 2017 Most Prevalent Weaknesses

Area of Weakness	Rank	Risk
Boundary Protection	1	• Undetected unauthorized activity in critical systems • Weaker boundaries between ICS and enterprise networks
Identification and Authentication (Organizational Users)	2	• Lack of accountability and traceability for user actions if an account is compromised • Increased difficulty in securing accounts as personnel leave the organization, especially sensitive for users with administrator access
Allocation of Resources	3	• No backup or alternate personnel to fill position if primary is unable to work • Loss of critical knowledge of control systems
Physical Access Control	4	• Unauthorized physical access to field equipment and locations provides increased opportunity to: ○ Maliciously modify, delete, or copy device programs and firmware ○ Access the ICS network ○ Steal or vandalize cyber assets ○ Add rogue devices to capture and retransmit network traffic
Account Management	5	• Compromised unsecured password communications • Password compromise could allow trusted unauthorized access to systems
Least Functionality	6	• Increased vectors for malicious party access to critical systems • Rogue internal access established

Network Segregation

- Dual-homed computers can pass traffic from one network to another
- Only firewalls should be configured as dual-homed systems in an ICS
- In the next slide the Data Historian is a possible source of weakness
- The routers offer basic packet filtering services
- The architectures in the following slides are from NIST sp 800-82r3

Architecture Models with DMZ



Purdue with DMZ

DMZ

Level 5 — Enterprise

Level 4 — Business Planning / Logistics

DMZ

Level 3 — Operations / Control

Level 2 — Area Control (HMI)

Level 1 — Controller Network

Level 0 — Field I/O Devices

ISA/IEC 62443

Enterprise

Conduit

DMZ

Conduit

Control Center

Conduit

BCPS

Conduit

SIS

IIC

DMZ

Enterprise Tier

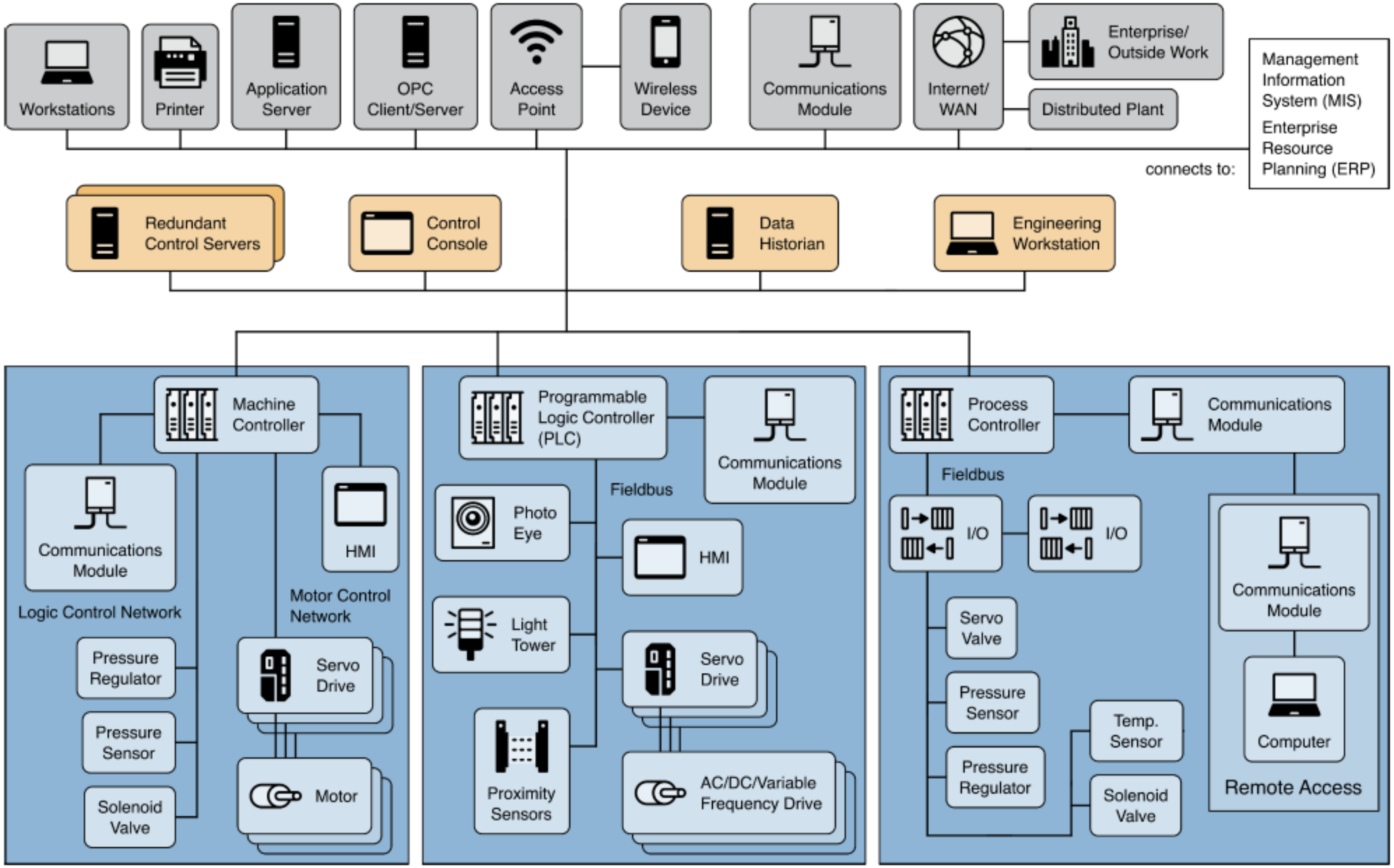
DMZ

Platform Tier

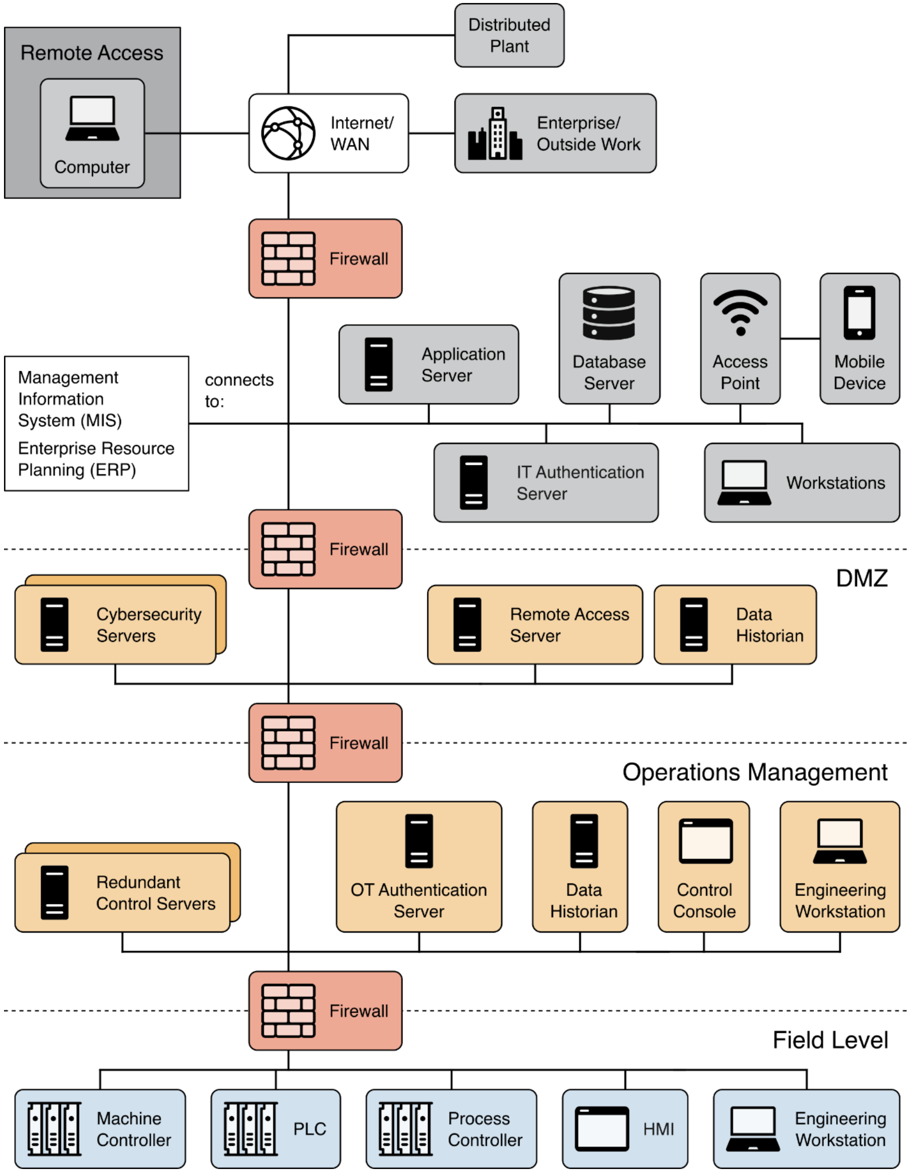
Edge Tier

BPCS – Basic Process Control System; IIC – Industrial IoT Consortium

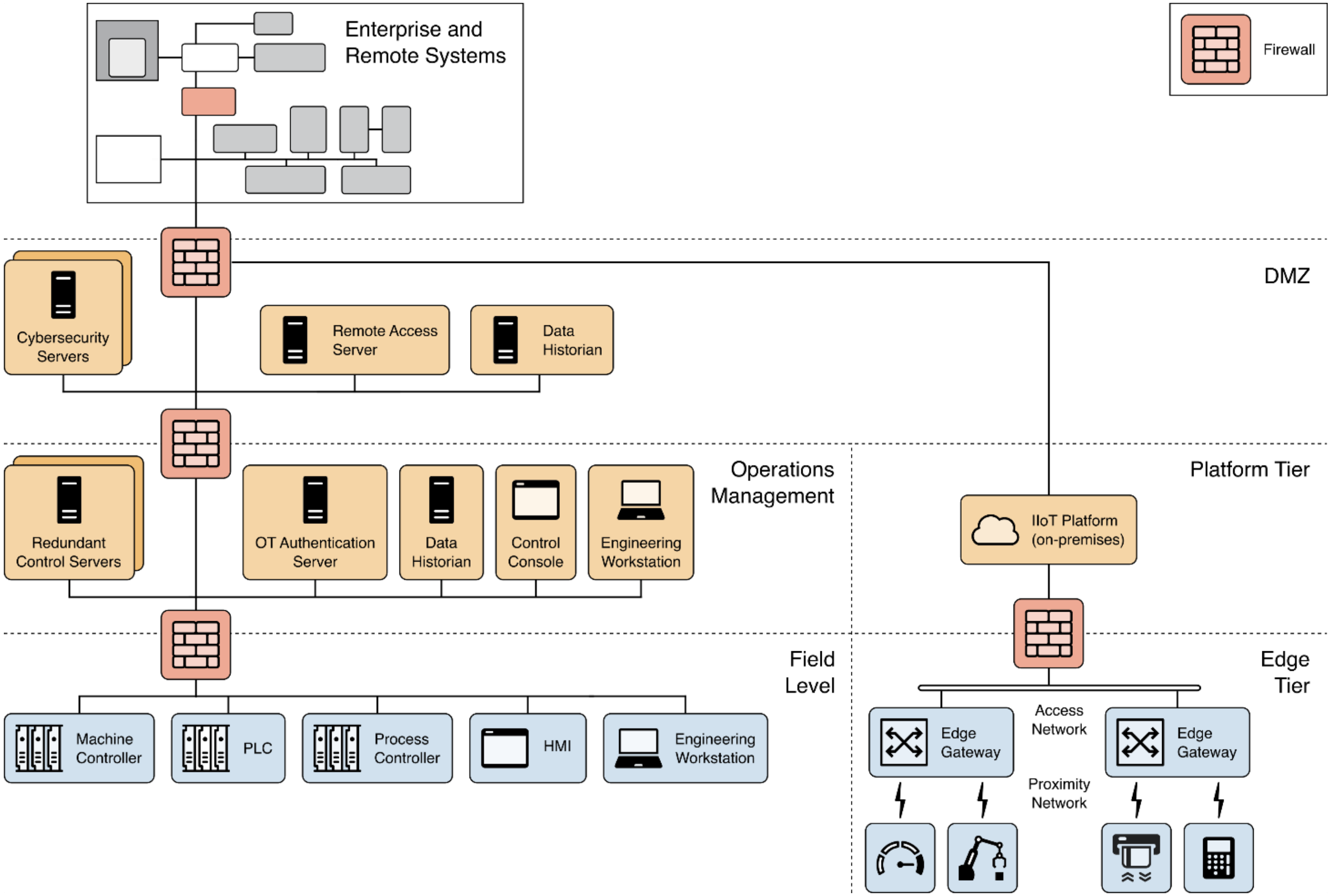
DCS Example


Workstations
Printer
Application Server
OPC Client/Server
Access Point
Wireless Device
Communications Module
Internet/ WAN
Enterprise/ Outside Work
Distributed Plant
Management Information System (MIS)
Enterprise Resource Planning (ERP)
connects to:
Redundant Control Servers
Control Console
Data Historian
Engineering Workstation
Machine Controller
Communications Module
HMI
Logic Control Network
Motor Control Network
Pressure Regulator
Pressure Sensor
Solenoid Valve
Servo Drive
Motor
Programmable Logic Controller (PLC)
Communications Module
Fieldbus
Photo Eye
HMI
Light Tower
Servo Drive
Proximity Sensors
AC/DC/Variable Frequency Drive
Process Controller
Communications Module
Fieldbus
I/O
I/O
Servo Valve
Pressure Sensor
Pressure Regulator
Temp. Sensor
Solenoid Valve
Communications Module
Computer
Remote Access

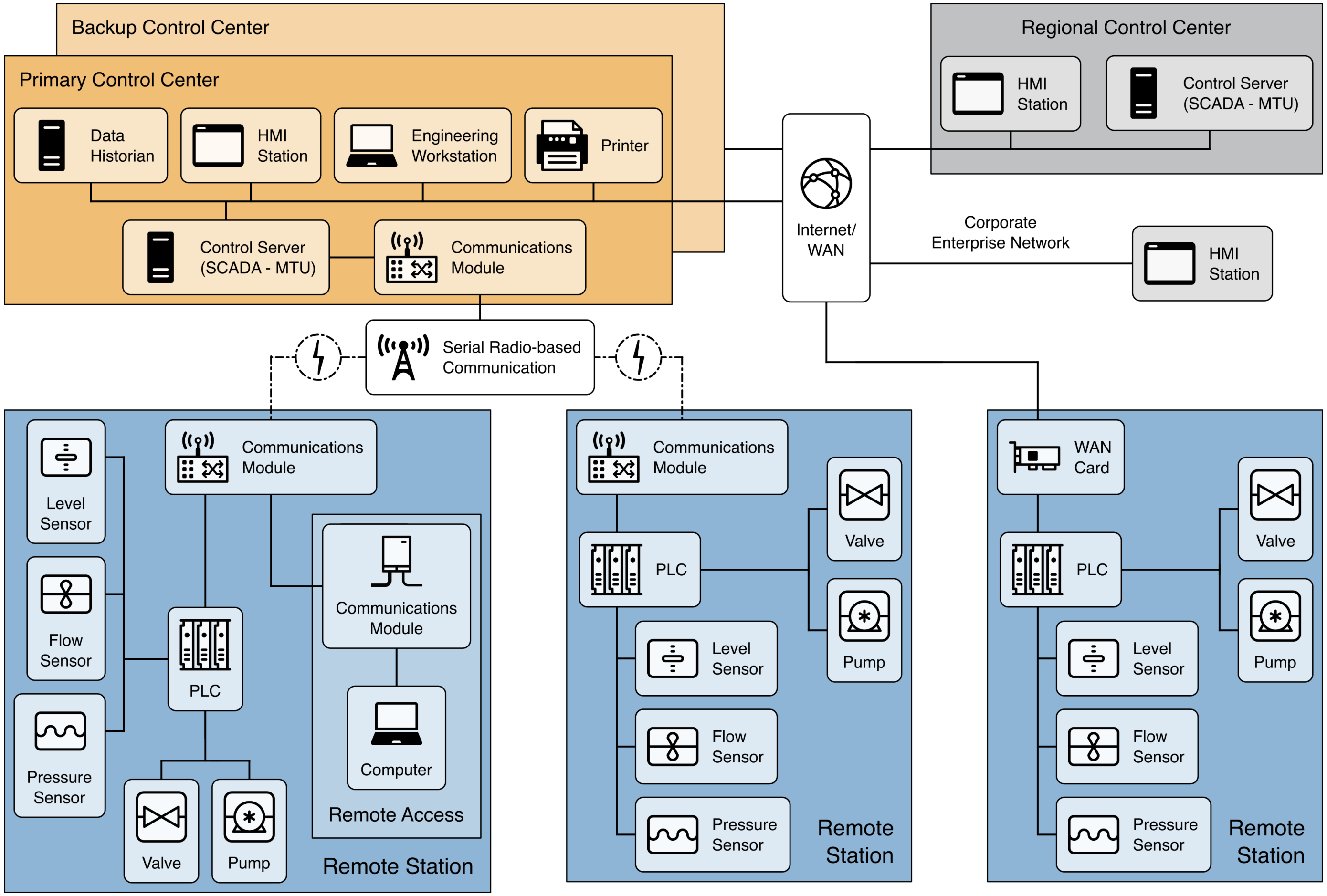
DCS with Defense-in-Depth



DCS with IIoT

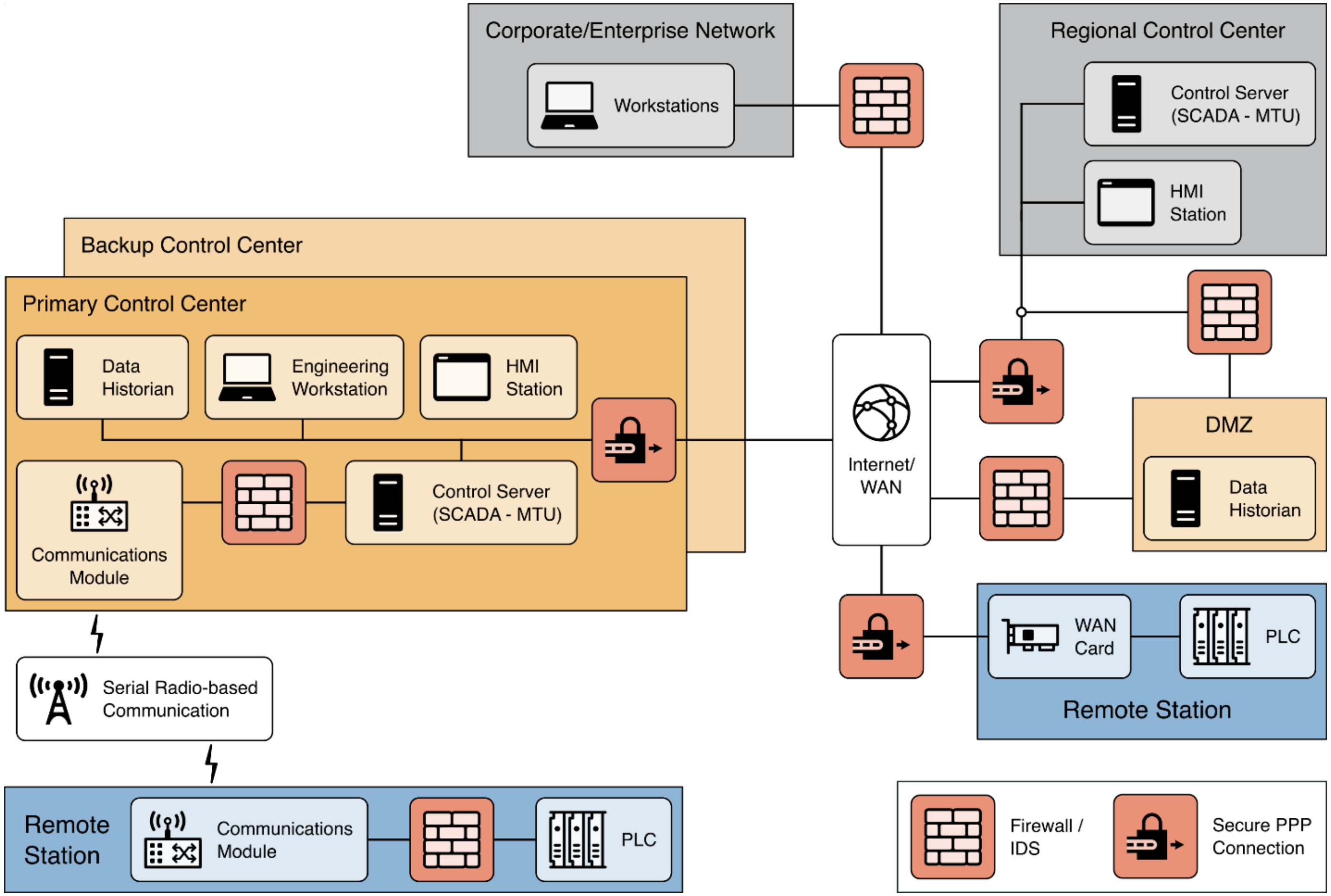


SCADA



Backup Control Center
Primary Control Center
Data Historian
HMI Station
Engineering Workstation
Printer
Control Server (SCADA - MTU)
Communications Module
Regional Control Center
HMI Station
Control Server (SCADA - MTU)
Internet/ WAN
Corporate Enterprise Network
HMI Station
Serial Radio-based Communication
Level Sensor
Communications Module
Flow Sensor
PLC
Communications Module
Pressure Sensor
Computer
Remote Access
Valve
Pump
Remote Station
Communications Module
Valve
PLC
Level Sensor
Pump
Flow Sensor
Pressure Sensor
Remote Station
WAN Card
Valve
PLC
Level Sensor
Pump
Flow Sensor
Pressure Sensor
Remote Station

SCADA with Defense-in-Depth



PPP – Point-to-Point Protocol

Some issues

- Use different anti-virus software in the Corporate and ICS systems
- Actively patch servers in DMZ
- Firewall should only allow connections between the control network and the DMZ that are initiated by control network devices
- For multiple firewall solutions use firewalls from different providers

Attack vectors

- Backdoors and holes in network perimeter
- Vulnerabilities in common protocols
- Attacks on field devices
- Database attacks
- Comms hijacking and man-in-the-middle attacks
- Spoofing attacks
- Attacks on privileged and/or shared accounts

Firewall Policies

- Stateful rules that are both IP address and port (application) specific
- Restriction to secure protocols such as HTTPS; HTTP, FTP and other unsecured protocols represent a security risk
- Deny hosts outside the control network establishing connections to hosts inside
- If there is a DMZ insecure protocols can be used between the control network and the DMZ (Modbus/TCP) and the corporate network and the DMZ (HTTP)

Outbound rules

- Limited to essential communications

- Source and destination restricted by service and port

- Outbound filtering to prevent forged IP packets

- Internet access by devices on the control network should be strongly discouraged.

Firewall Rules for Specific Services

- Domain Name Service (DNS): No DNS requests into control network, No DNS requests from control to corporate, control to DMZ on a case-by-case basis
- HTTP should not be allowed to cross from the public/corporate to the control network
- FTP and Trivial FTP (TFTP): TFTP has no authentication, so disallow; FTP should only be used if secured by some other means
- Telnet is unencrypted so disallow inbound and only allow outbound over VPN or encrypted tunnel

Firewall Rules for Specific Services

- Dynamic Host Config. Protocol (DHCP): recommended to use static configuration, otherwise enable DHCP snooping to identify rogue servers
- SSH recommended for access into control network if necessary
- Simple Object Access Protocols should only be used with deep packet inspection and/or application layer protocols
- SMTP (Mail Transfer) should not be allowed into the control network; outbound could be used for alerts

Firewall Rules for Specific Services

- SNMP (Network Mgt) should only be used in secure versions (V3 and above)
- Distributed Component Object Model (DCOM) underpins OPC which dynamically opens a wide range of ports. Should only be used between the control network and the DMZ.
- SCADA protocols (Modbus/TCP, Ethernet/IP, IEC 61850, ICCP and DNP3) should only be used within the control network

Specific ICS Firewall Issues

- Network Address Translation: private subnet IP 192.168.1.xxx to corporate net 192.6.yyy.zzz
- Placement of the Data Historian is problematic in two zone architectures
- Remote support access
- Multicast traffic (for example Ethernet/IP and Fieldbus) – good for time synchronization between multiple devices – and Network Address Translation issues.

Man-in-the-Middle Attacks

- Poisoning Address Resolution Protocol (ARP) caches. The ARP tables map between MAC addresses (Layer 2) and IP addresses (Layer 3).

- Replay attack

- False negative of false positive messages

Mitigations

- MAC Address Locking – locks a specific MAC address to a specific port on a managed switch
- Statically coded ARP tables
- Encryption prevents reverse engineering of protocol messages but has an overhead
- Strong authentication also provides resilience against MITM attacks
- Monitoring for ARP poisoning

Hardware Security

- Monitoring and Analysis
- Secure configuration and management
- Endpoint hardening
- Integrity protection
- Access control
- Device identity
- Root of trust
- Physical Security

Software Security

- Application allowlisting
- Patching – testing and validation
- Secure code development
- Configuration management including application hardening

Other considerations

- Cyber-related safety – physical vs logical separation, fail-safe
- Availability
    - Data, Applications and Infrastructure – backup-in-depth
    - Primary and alternate power sources
    - Other utilities – UPS, HVAC, fire alarm systems, compressed air, …
    - All these to be protected against cyber attack

Other considerations, …

- Geographically distributed systems – encrypted and authenticated end-to-end
- Regulatory requirements – for example NIS2
- Environmental hazards
- Field I/O Devices – digital twins, Field I/O monitoring network
- IIoT devices – cloud issues, endpoint security capabilities