Implementing A Secure Industrial Control Systems

Engr.Abiodun Odewale MNSE, MNIEEE, CISSP

About (me):

- Over 20 years experience in IT, Instrumentation, Control & Automation
- Masters Degree in Engineering Management from NorthWest University, South Africa
- Masters in Business Administration (MBA) from Lincoln University, USA
- Advanced Diploma in Industrial Automation from EIT Australia
- Post-Graduate Diploma in Electrical & Electronics Engineering from FUTA
- Certified Information Systems Security Professional, CISSP
- Certified OPC Professional, Level 4 from OPC Training Institute, Canada
- Certified Process Control Network CyberSecurity Practitioner
- Cisco Certified Internetwork Expert Data-Center (Written)
- Cisco Certified Network Professional, CCNP
- Microsoft Certified systems Administrator, MCSA
- A member of COREN, NSE, NIEEE, IEEE & ISA
- Strong Expertise in Yokogawa & Allen Bradley Control Systems Architecture
- Currently PCN / CyberSecurity Engineer for Chevron Nigeria

Discussion Outline:

- Some Terminologies
- Industrial Control Systems Basics
- The Need for securing an ICS
- ICS Cybersecurity Strategies

Different Types of Industrial Control

- Process control, both continuous and batch – typically a Distributed Control System (DCS)
- Discrete control, sequence control – typically a Programmable Logic Controller (PLC)
- Remote monitoring and dispatch – typically a Supervisory Control and Data Acquisition System (SCADA)
- Life Safety or Personnel Protection – typically a Safety Instrumented System (SIS) – this will be covered in a later session

All Industrial Control Systems are designed for one primary purpose – and that is to automate a physical process. They accomplish this through sensors to measure physical properties and actuators to manipulate those properties

OT – the all encompassing term

- Operational Technology (OT) – is often used to describe Industrial Control Systems (ICS) and other “cyber physical systems” – but is also used to describe automation systems that aren’t industrial in nature but use similar technology
  - Building Automation Systems
  - Transportation (Avionics, Positive Train Control, etc.)
  - Medical Devices and systems (many CAT scan / MRI use PLC technology)
- Many of these systems have developed independently from ICS system development, but they look remarkably similar and have many of the same vulnerable sub-systems!

Industrial Control Systems have been around a long time!

- As industrial processes became more complex – some degree of automation was required. In the early days, this was accomplished with complex pneumatic (think air pressure) controllers that were all 'piped' to the control room

Boiler Operator Jeff Craigie sits in the Boiler Room and monitors flows, temperatures and pressures of the boilers and feed-water system. Photo by Ryan Solomon

This is an example of an early pneumatic controller common in the 1950's – 1980's

Enter the era of electronics
… But still no networks

- This panel contains “stand alone” electronic controllers that are controlling flow in a pulp mill process. Each one will be hard wired from the sensor – flow meter to the controller, and then out to the control valve, which is manipulating the flow
- There are no networks here – each of the controllers is separate
- Also note that the push buttons below the controllers to open and close block valves, or to start and stop pumps in the process

- Panels like this were very common scattered around the pulp mill, and some smaller processes still use this format rather than going to a networked electronic system

Control System Basics – “The control loop”

Input / Output (IO), Controllers
Signals from the plant are connected to the controllers – where the controller decides what to do “The logic”

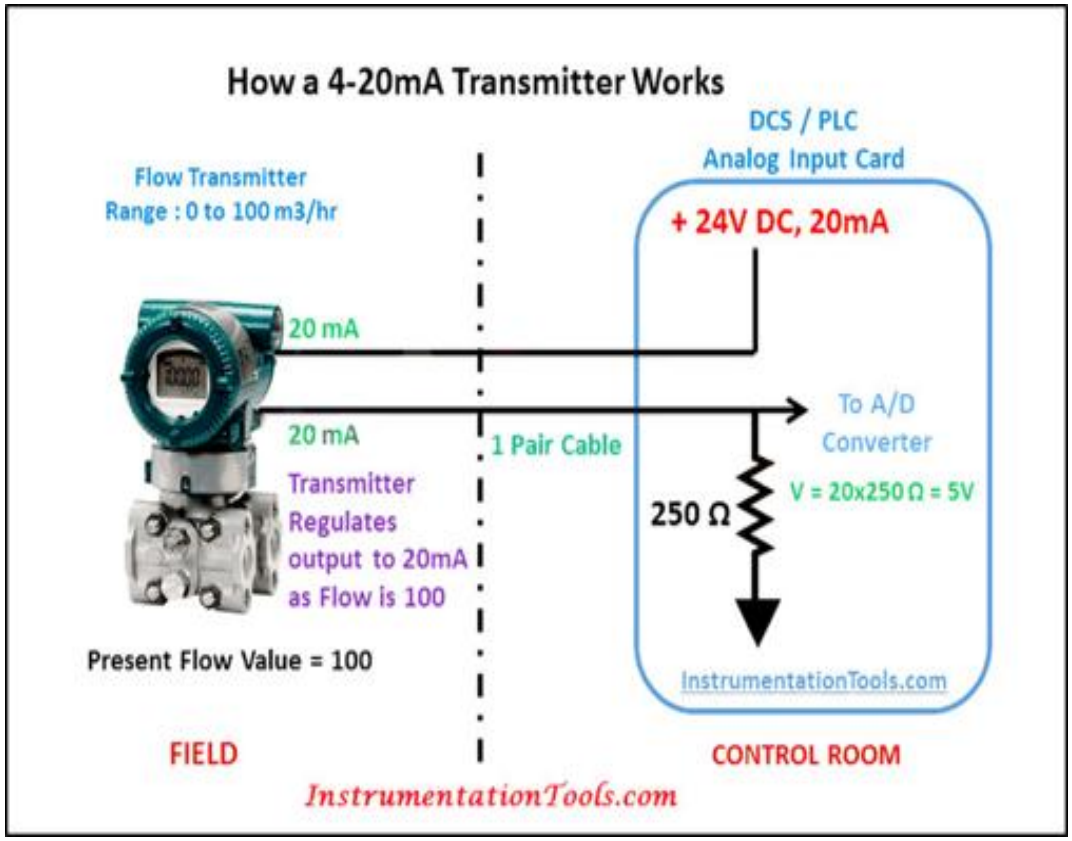
Sensors measure physical properties like temperature, pressure and level and transmit this information to the controller

Most of these interconnections are ‘hardwired’ and do not involve any type of digital ‘protocol based’ communication

Final Control Elements and actuators like valves and motors adjust physical attributes of the process or turn things on and off

Process, Sensors, Actuators
This is the actual factory floor – and the physical, chemical, mechanical process that is being automation or controlled

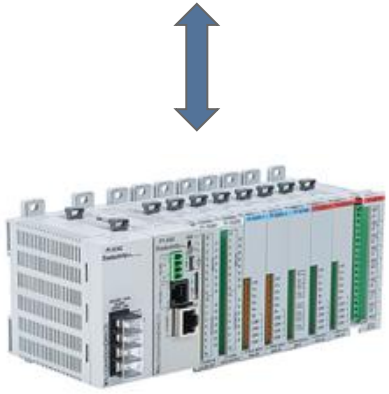
Basic ‘hardwired’ electrical theory and not every control system is controlling something…



- Sensors like this that are connected to the controller often don’t have any “control” algorithms attached at all.
- For instance they could be connected to an input just to display the value, or provide an alarm
- It is these types of “understanding the process” nuances that make cyber attacks more difficult if you are trying to achieve specific consequences
- If there isn’t anything wired to the system to control – then an attacker can’t manipulate it – unless they go into things like deceiving the operator to take manual actions

Each of the sensors that are wired to the control system manipulate the current or voltage in the wire that the control system interprets as the “input signal” from 0-100%

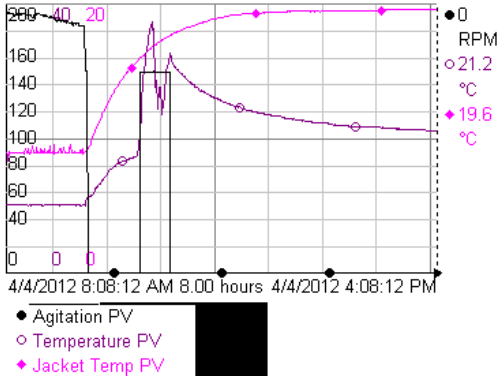
Control System Basics – “The Control Room”
… where the juicy Windows bits are



The controller could run the process by itself, but humans want to ‘see’ and ‘interact’ with the process

Because we want to see things, we connect the controllers to the “human machine interface” or HMI

This is where we represent the process on graphic displays – and can change parameters such as setpoints and tuning values

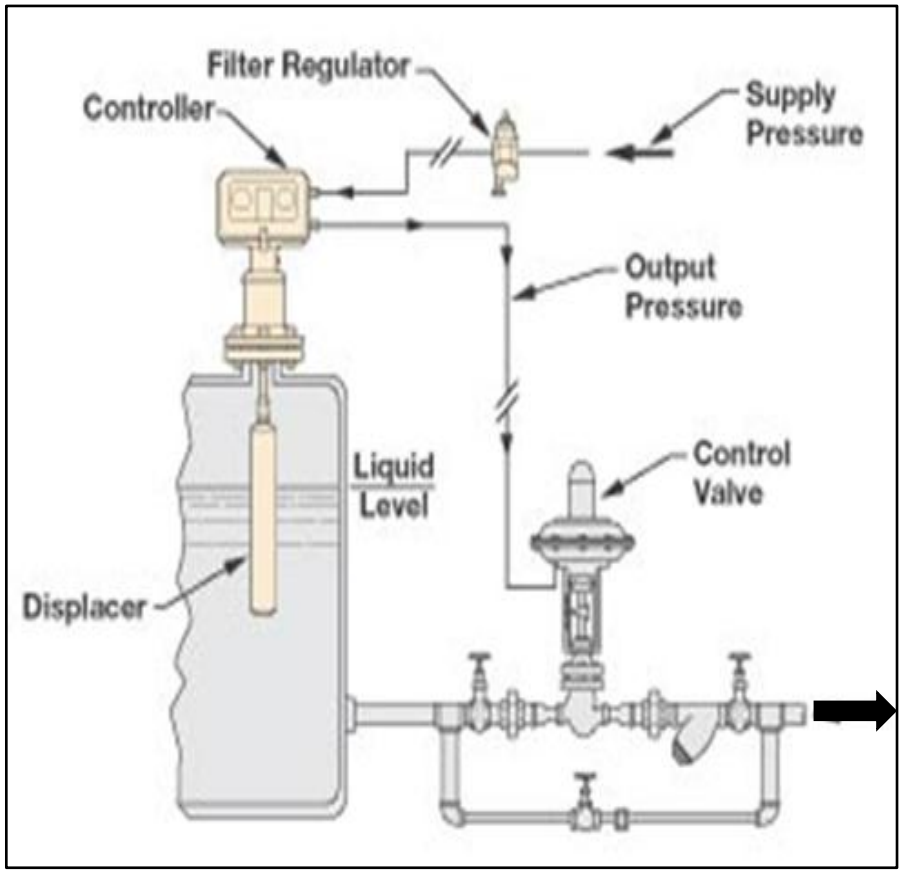


We also need a place to store all the settings and logic – so lets call this the “Engineering Workstation” Think of it as the master database holding all of the configuration data

Often it sits in the control room or “the rack room” beside the control room

We also need a place to record all of the values (called “points” or “tags”) and events that are happening in the plant in a master logfile. This is usually referred to as the “Historian”

Level Control Example



Objective – control the level in a tank

- Step 1 – measure the level in the tank – in this case with a displacer that is suspended in the liquid in the tank
- Step 2 – control the level – in this case the level controller is integrated into the displacer / sensor – this is where the operator would adjust the desired level setpoint (SP)
- Step 3 – manipulate the outlet flow. In this case there is a control valve that will throttle the flow out of vessel

Note the // slashed lines on the diagram – this indicates that the 'signal' between the controller and the valve is pneumatic (air pressure) typically between 3-15 psig

It Begins With A Security Perimeter

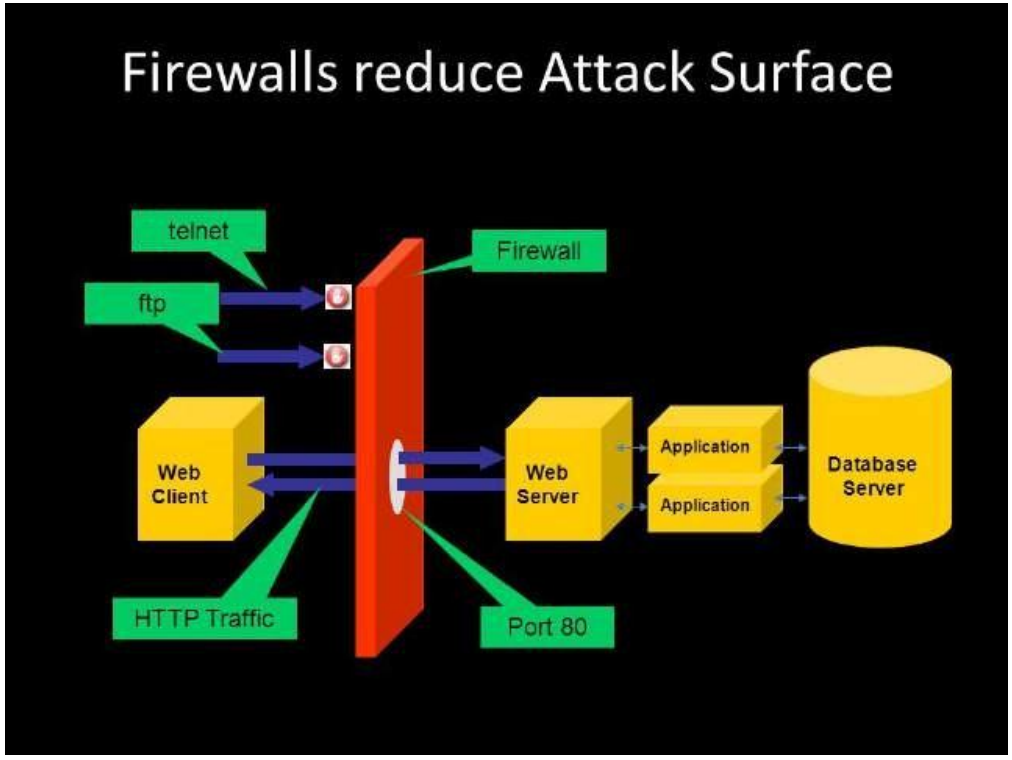
A barrier (wall, fence, etc.) that is not easily penetrated

A gate / door / opening where approved people and things are allowed through

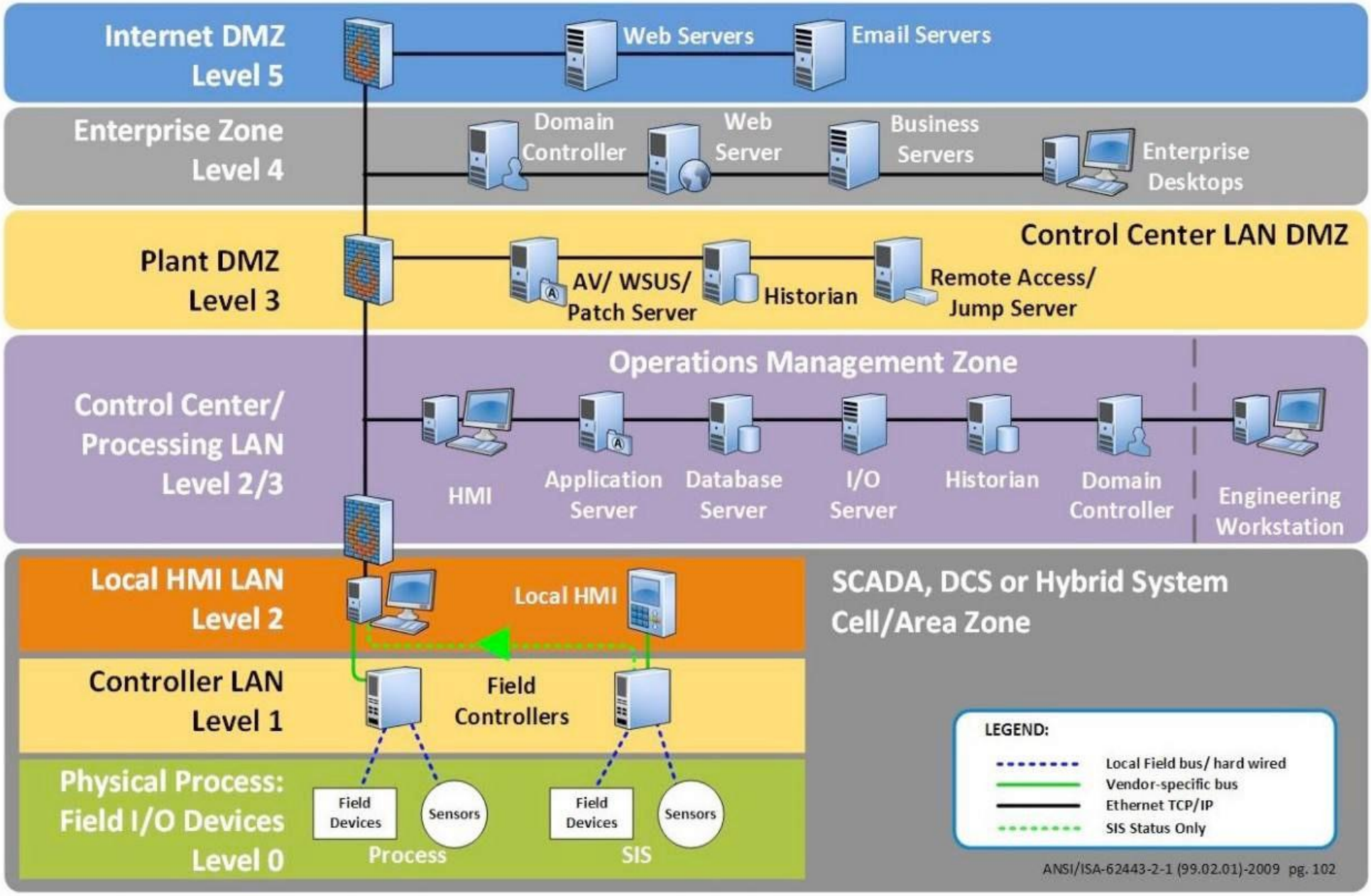
Cybersecurity Perimeter

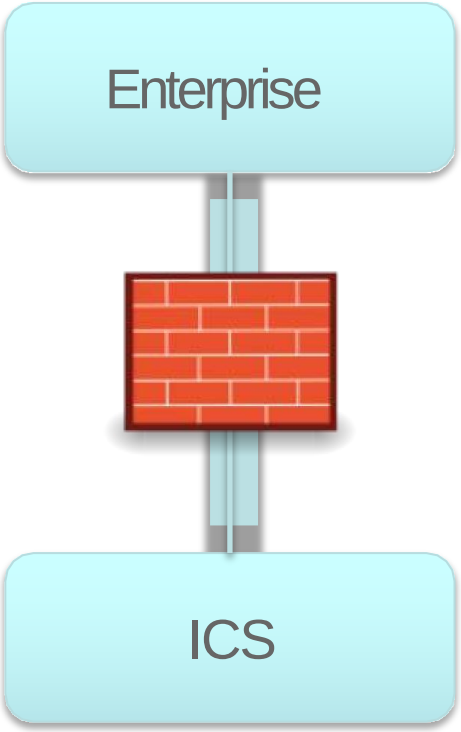
- It is tougher (near impossible?) to penetrate the barrier part of cybersecurity perimeter because it is air
  - Especially true for wired networks …no cable, no path to get through perimeter
  - Foreshadowing for wireless challenges
- Attacks come through the cyber equivalent of gates or doors
- Firewalls are most common cyber gates anddoors
  - Restrict by who (IP address), where (destination IP address) and what (TCP/UDP port)
  - What is allowed through cybersecurity perimeter is the attack surface

Attack Surface



- Minimize and Evaluate Risk
- **Least Privilege**
  - Whitelist Approach
- Minimize
  - What is allowed through perimeter
  - Listening services
  - Running software


Internet DMZ
Level 5
Web Servers
Email Servers
Enterprise Zone
Level 4
Domain Controller
Web Server
Business Servers
Enterprise Desktops
Plant DMZ
Level 3
Control Center LAN DMZ
AV/ WSUS/ Patch Server
Historian
Remote Access/ Jump Server
Control Center/ Processing LAN
Level 2/3
Operations Management Zone
HMI
Application Server
Database Server
I/O Server
Historian
Domain Controller
Engineering Workstation
Local HMI LAN
Level 2
Local HMI
SCADA, DCS or Hybrid System
Cell/Area Zone
Controller LAN
Level 1
Field Controllers
Physical Process:
Field I/O Devices
Level 0
Field Devices
Sensors
Process
Field Devices
Sensors
SIS
LEGEND:
Local Field bus/ hard wired
Vendor-specific bus
Ethernet TCP/IP
SIS Status Only
ANSI/ISA-62443-2-1 (99.02.01)-2009 pg. 102



Untrusted

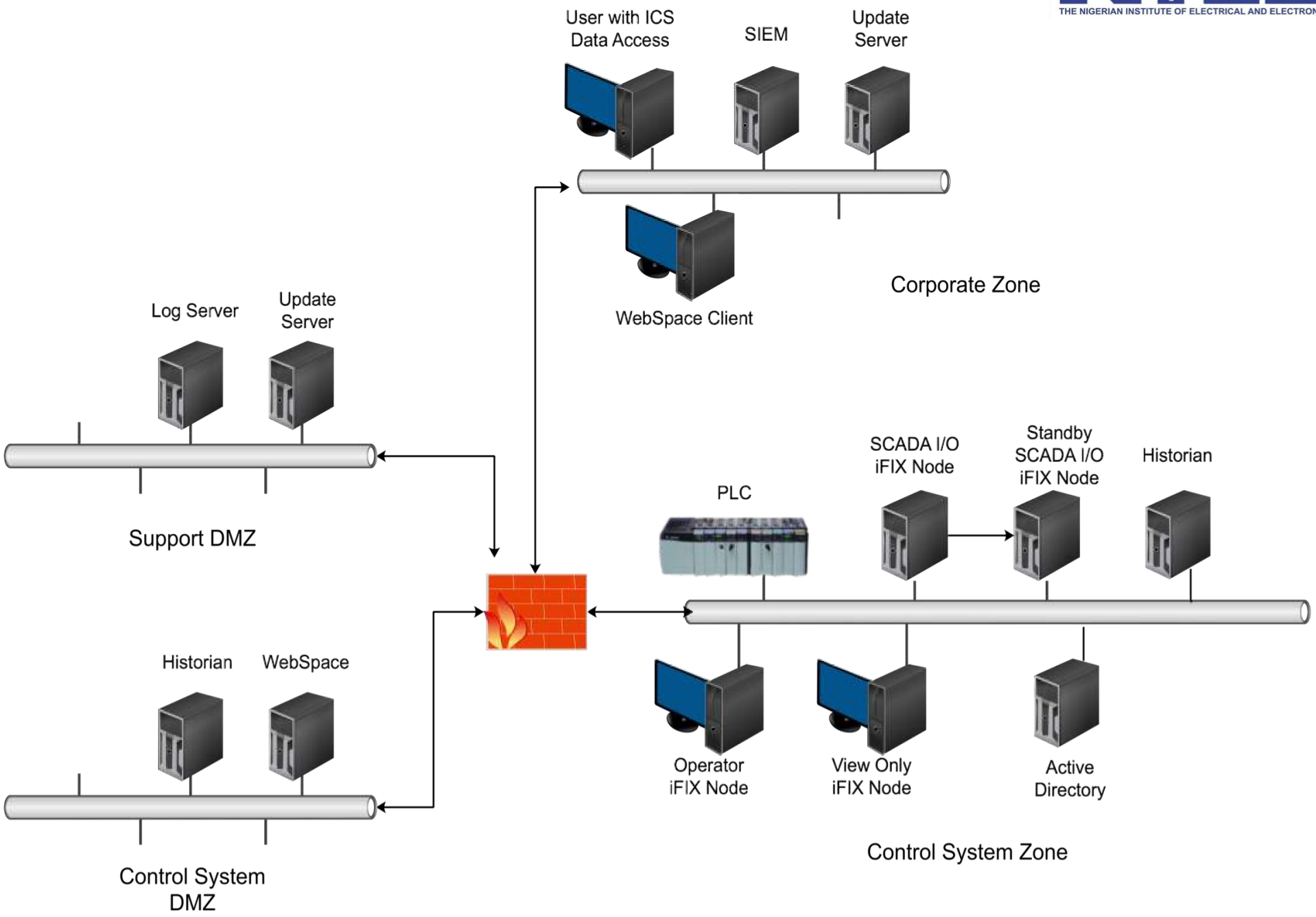
Kaspersky study showed 42% of ICS had Internet access. CyberX study had similar statistics.

Holes In The Cybersecurity Perimeter

- Again: Minimize …least privilege
  - Smallest number of source and destination IP addresses
  - Smallest number of TCP / UDP Ports
  - Initiate from the more trusted / sensitive zone
- Examples Good and Bad
  - Good: PI Server historical data export …1 port (TCP/5450) with source in the more sensitive zone (ICS) …from 1 server to 1 server
  - Bad: Server on the enterprise needs UDP comms or initiate TCP comms to more sensitive zone on numerous ports (ICS)

Diversion: Prioritized Security Patching

- Patching isn't a yes/no decision or a single patching interval decision
- Attack surface allowed through the cybersecurity perimeter should be top priority for patching
  - Example: RDP, web server
  - The tighter your cybersecurity perimeter / smaller your attack surface, the less high priority patching you have to do
  - **Insecure By Design**



Security Zones

- So far we have talked about two: Enterprise and ICS
  - And IEC 64443 / ISA 99 would call the communication allowed between these two zones a conduit.
- Common Question: Can I use the same hardware and software infrastructure between security zones?
  - Active Directory Domain/Tree/Forest, same physical switch with VLAN's for each security zone, shared virtualization infrastructure
  - It saves money and logical / cyber separation is be possible.
  - Good security practice answer is No (but it is a risk decision)
    - ICS AD domain, dedicated switches and dedicated virtual environment

Defense In Depth

Definition: **Defense in depth** is the coordinated use of **multiple security countermeasures** to protect the integrity of the information assets in an enterprise.

VLANs???

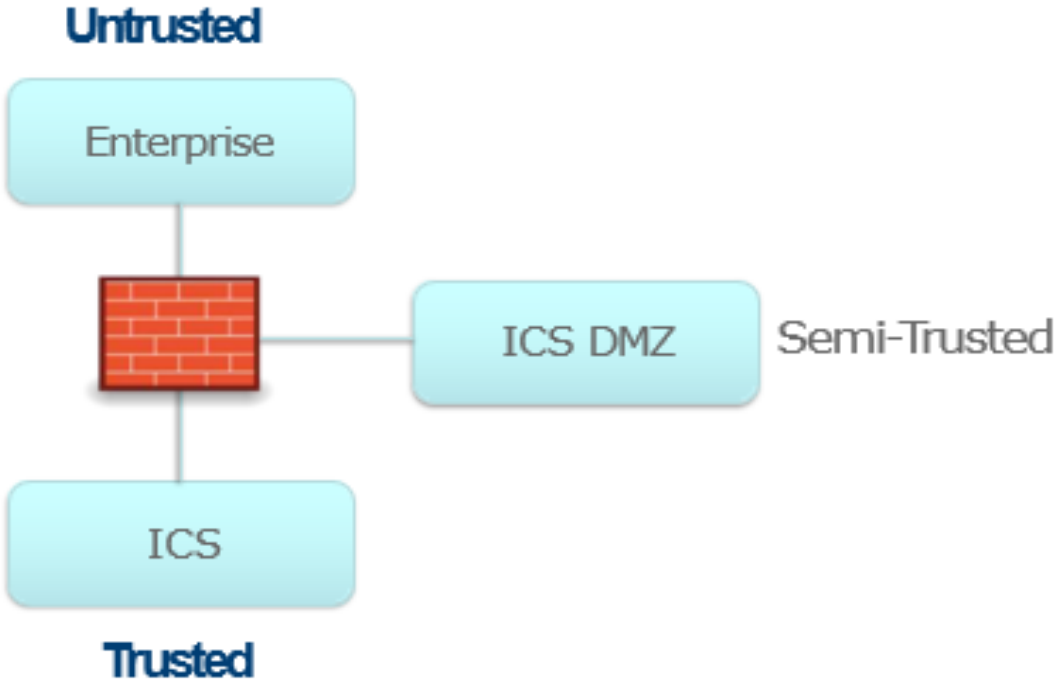
- Shared ICS / Enterprise Switch Example
  - Vulnerability that allows VLAN hoping or denial of service
  - Compromised switch administrator credentials on enterprise
  - Accidental misconfiguration
- Risk Acceptance Decision
  - Identify risk to appropriate level of management
  - They can accept risk (document)

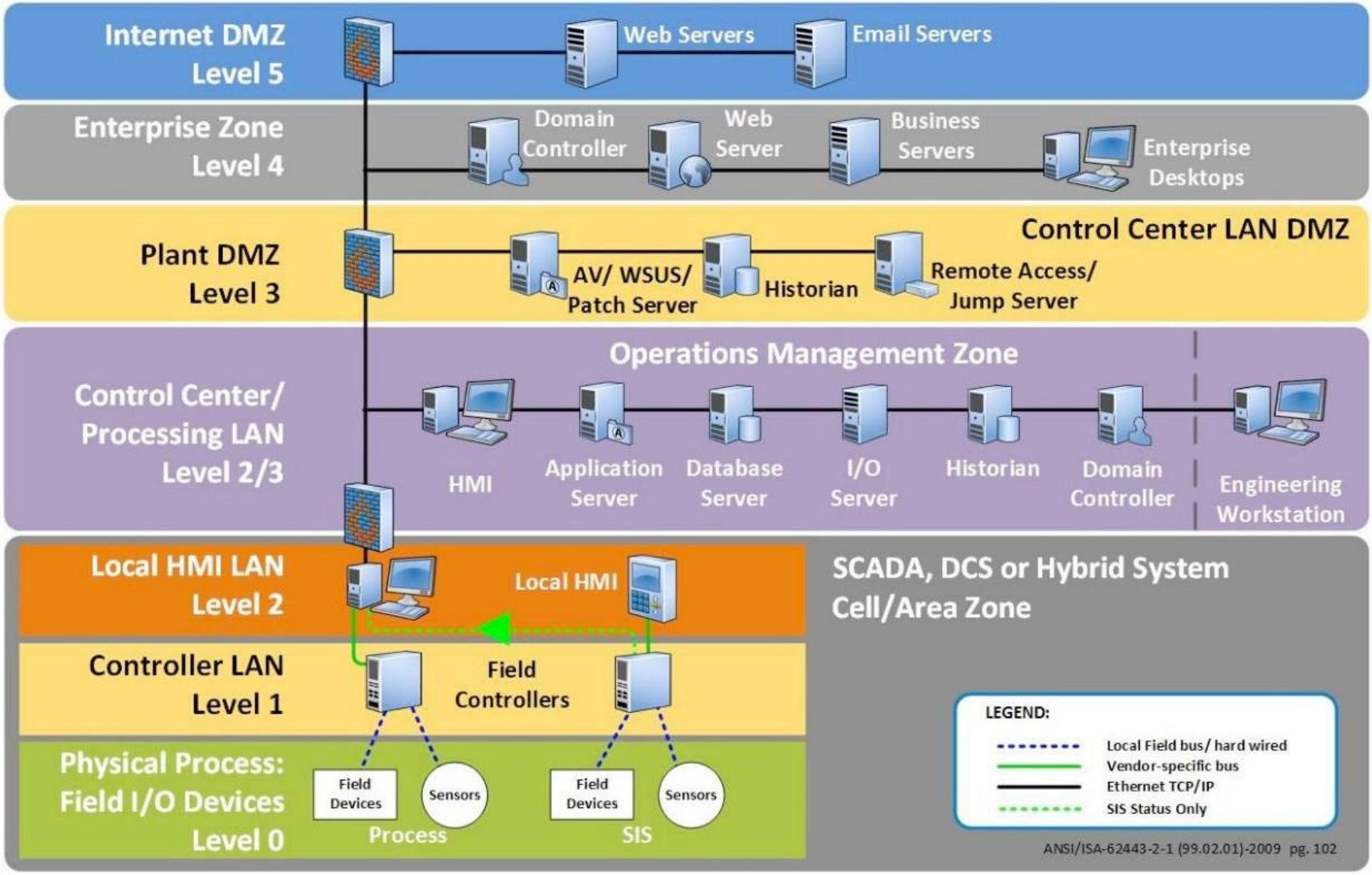
Infrastructure Administration

- Who will manage the ICS / OT infrastructure?
  - Do they have the necessary skills?
  - Lesson: Don't deploy without a cyber maintenance plan
  - Run To Fail Maintenance was/is common in OT
- From where will the cyber maintenance take place?
  - ICS Zone?
  - Enterprise?
  - Separate ICS Admin Zone?

De-Militarized Zones (DMZ)

- Another extension of defense-in-depth concept
  - No direct untrusted (enterprise) to trusted (ICS) communications
  - Mediate servers through one or more semi-trusted de-militarized zones (DMZ's)




Internet DMZ
Level 5
Web Servers
Email Servers
Enterprise Zone
Level 4
Domain Controller
Web Server
Business Servers
Enterprise Desktops
Plant DMZ
Level 3
Control Center LAN DMZ
AV/ WSUS/ Patch Server
Historian
Remote Access/ Jump Server
Control Center/ Processing LAN
Level 2/3
Operations Management Zone
HMI
Application Server
Database Server
I/O Server
Historian
Domain Controller
Engineering Workstation
Local HMI LAN
Level 2
Local HMI
SCADA, DCS or Hybrid System
Cell/Area Zone
Controller LAN
Level 1
Field Controllers
Physical Process:
Field I/O Devices
Level 0
Field Devices
Sensors
Process
Field Devices
Sensors
SIS
LEGEND:
Local Field bus/ hard wired
Vendor-specific bus
Ethernet TCP/IP
SIS Status Only
ANSI/ISA-62443-2-1 (99.02.01)-2009 pg. 102

De-Militarized Zones (DMZ)

- Another extension of defense-in-depth concept
  - No direct untrusted (enterprise) to trusted (ICS) communications
  - Mediate servers through one or more semi-trusted de-militarized zones (DMZ's)
- More than one DMZ may be warranted
  - Access to historical data
  - Security patches, schedules, information
  - DMZ's are inexpensive, consider adding another for different groups of users, risk, what is allowed through

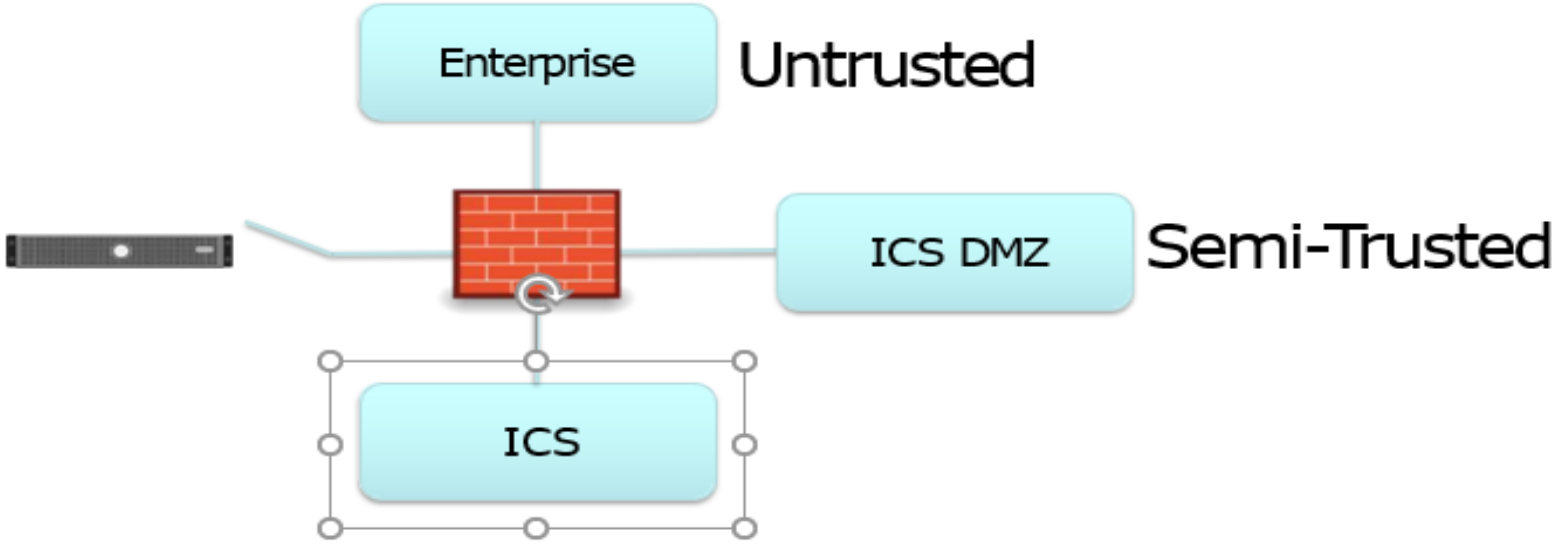
Remote Access … Primary Attack Path To ”Secured” ICS Today

Bad guy gets on enterprise, spearphish or other, finds user with highly privileged remote access, gets credentials and now has administrator or engineer rights on the ICS

Ukraine Power Outage, German Steel Mill, …

Secure Remote Access

- Perfect: None?
- Perfect: Emergency remote access capability that is unhackable / open circuit when not in use
  - Policy for on when it is turned on
  - Auto-timeout and logged

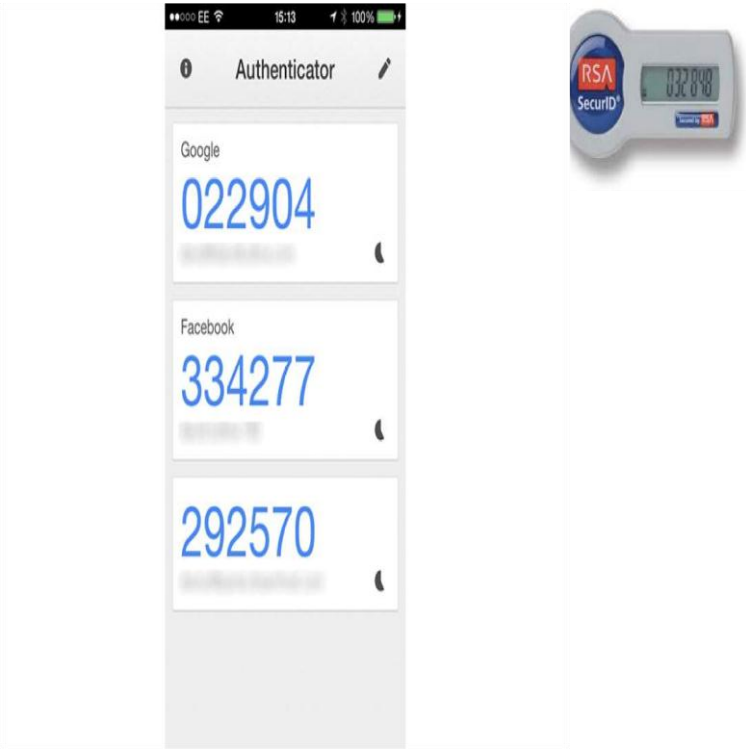


Secure Remote Access

- Reality is many organizations have people and processes that require everyday, frequent remote access
  - Insure it is not being used strictly for convenience (example of two computers on a desk)
  - **Push out data to the Enterprise whenever possible**
  - Risk acceptance (who and what are remotely accessing the ICS, from where, how often, what risk does this entail?)
  - User and machine access from outside the ICS zone is likely to increase

Secure Remote Access

- Encryption / VPN is not THE answer
  - Compromise of the other side will just mean the attack is encrypted
  - US Warning of High Value Target, Third Party Risk
  - GE OSM 1800 Turbines in 90 countries (5-year old number)
- **Two Factor Authentication**
  - Stolen username:password does not provide anytime access, also requires the physical token
  - Attacker could still “ride along” after two-factor authentication



Remote Access Solutions

- Specialized products that make this more secure
  - Terminal Services, Virtual Desktop Interface (VDI)
  - Extensive Logging
  - Screen capture / video files
  - Some have a lockbox / physically disconnected, require process
- Many asset owners create their own Jump Servers

One-Way Devices / Unidirectional

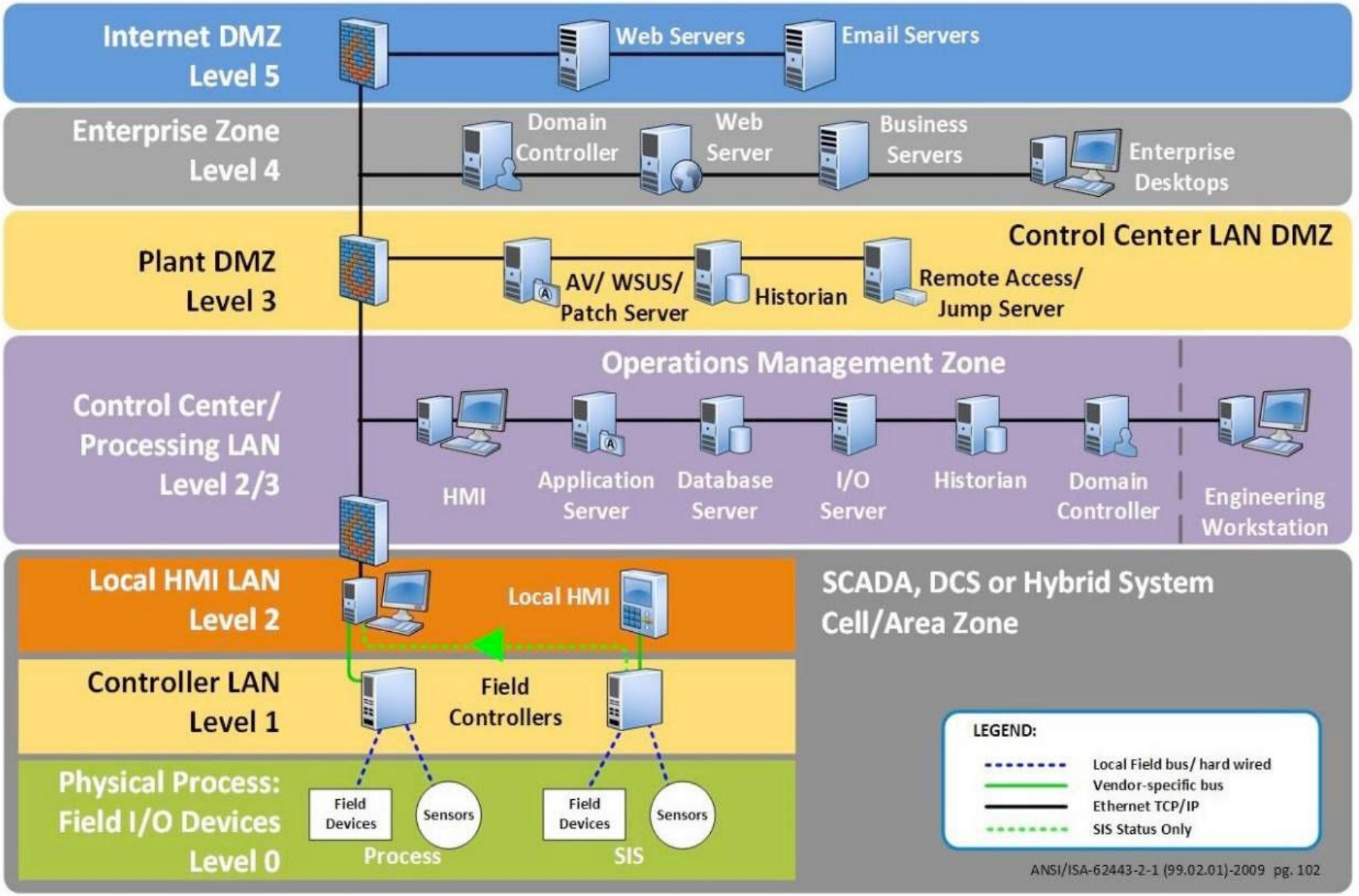
- Data diode / physics, not software so diode can't be "hacked"
  - There is some software on either side to provide mimic a two-way connection for each zone
- Only allows communications in one direction
  - Example: From ICS to cloud for predictive maintenance
  - Example: From safety system to ICS
  - Example: ICS to Enterprise for historical data or screen share
- Major Vendors include Owl and Waterfall

1 GATHERS DATA

2 TRANSMITS SAFELY

3 REPLICATES DEVICES

Internal Segmentation



Internal Segmentation

- **Efficient Risk Reduction**
  - Will additional segmentation reduce risk the most for the next $ or hour spent?
  - What communications would need to be allowed through the proposed security perimeter?
- Some areas that are common next segmentation steps based on efficient risk reduction
  - Safety Protection / ICS segmentation (Bryan Singer will discuss)

New-ish Technologies in ICS Architecture

- Deep Packet Inspection of ICS Protocols
  - Restrict by function code, points/tags, values
- Software Defined Networking
  - Like a firewall deployed across all of the switches in your network
  - Identify at a central application what is allowed (white list)
  - Push the configuration to SDN switches that enforce the restrictions
- The Edge
  - Perform some computing / analysis to restrict what needs to be sent
  - Secures the cloud connection

References

- ISA – International Society of Automation
  - https://www.isasecure.org/en-US/
- SANS Industrial Control System
  - https://ics.sans.org/ics-library
  - https://ics-community.sans.org/
  - http://www.robertmlee.org/a-collection-of-resources-for-getting-started-in-icsscada-cybersecurity/
- (ISC)2- International Information System Security Certification Consortium Blog
  - https://blog.isc2.org/
- IEEE Control Systems Society
  - http://ieeecss.org/
- OnRamp Event
  - https://onramp-3.s4xevents.com/
  - Marty Edwards & Dale Peterson Videos

Industrial Control Systems Architecture

Engr.Abiodun Odewale MNSE, MNIEEE, CISSP
abiodunode@gmail.com