Dockerized OT Training Range (DOTTR)

A Cloud Native Operational Technology/Industrial Control System (OT/ICS) Simulation

Russia maintains its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States….

– Office of the Director of National Intelligence's 2024 Annual Threat Assessment

If Beijing believed that a major conflict with the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets.

...impeding U.S. decision making, inducing societal panic, and interfering with the deployment of U.S. forces.

– Office of the Director of National Intelligence's 2024 Annual Threat Assessment

Where network effects have real world results…

- OT – Operational Technology
- ICS – Industrial Control Systems
- PCS – Process Control Systems
- SCADA – Supervisory Control and Data Acquisition
- Control Systems – DAFGM Nomenclature

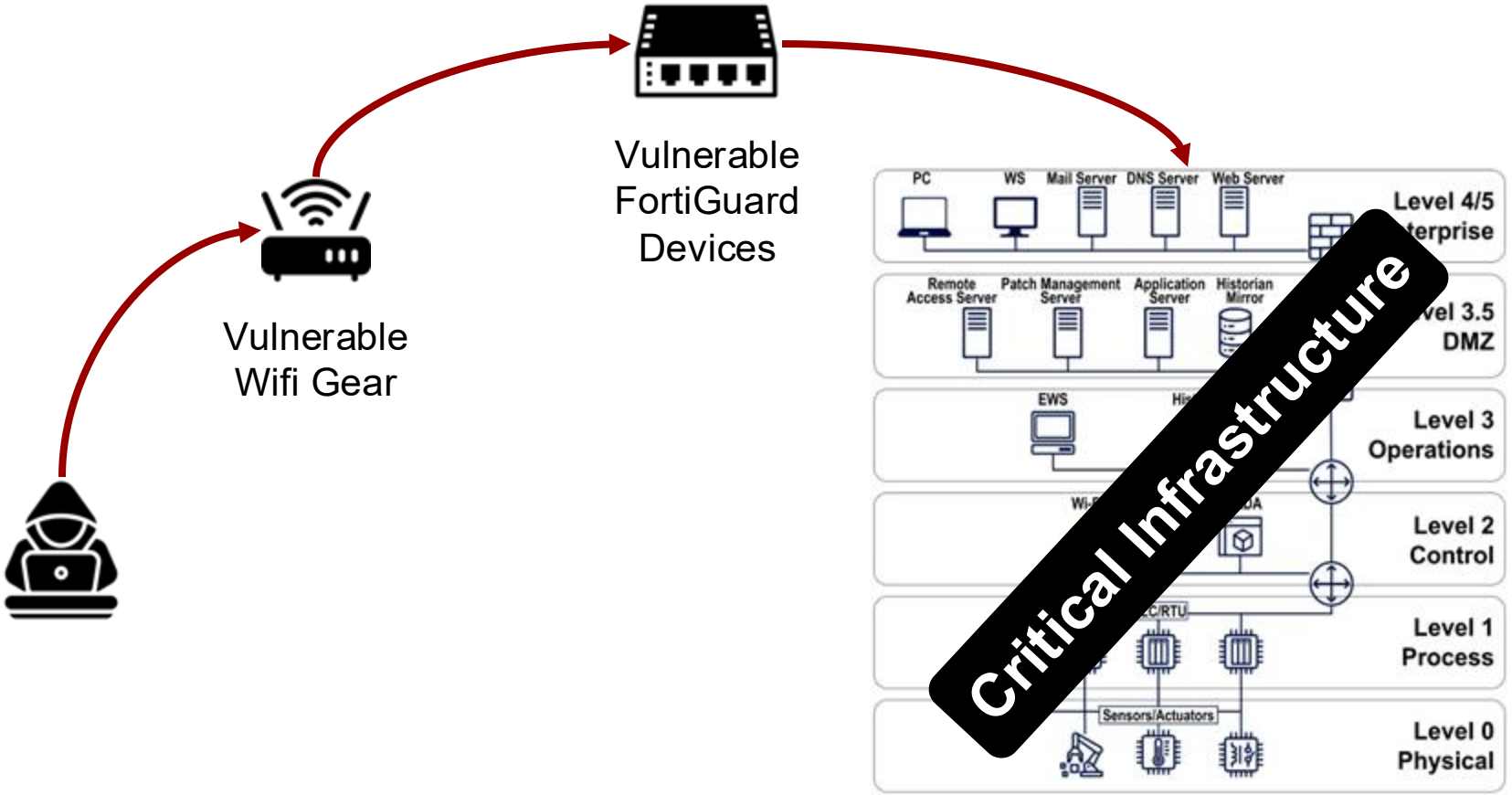
- Chemical
- Commercial Facilities
- Communications
- Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Services
- Healthcare
- Information Technology
- Nuclear
- Transportation
- Water and Wastewater

Air Force Control Systems:

- Natural gas distribution
- Water/wastewater distribution and treatment
- Electrical distribution and generation, UPSs
- Building Automation – HVAC, Lighting, Fire Alarm & Suppression
- Mass Notification Systems
- Airfield / Ramp Lighting, Runway Ice Detection
- Traffic control systems

Date	Target	Attacker, Method
Oct 2022	Iranian Atomic Energy Organization	Hacktivists, Data Breach
Oct 2022	Electricity Company of Ghana	Ransomware
May 2023	Denmark, 22 energy companies	Coordinated Attack, Possible Nation/State
Jun 2023	Multiple, including VA & DoE entities	MOVEit Data Breach
Nov 2023	Trans-Northern Pipeline, Canada	Ransomware, Data Breach
Jan 2024	American Critical Infrastructure	Volt Typhoon
Mar 2024	Negev Nuclear Research Center, Israel	Hacktivists, Data Breach & Erasure

Volt Typhoon



In the civilian ICS/OT sector:

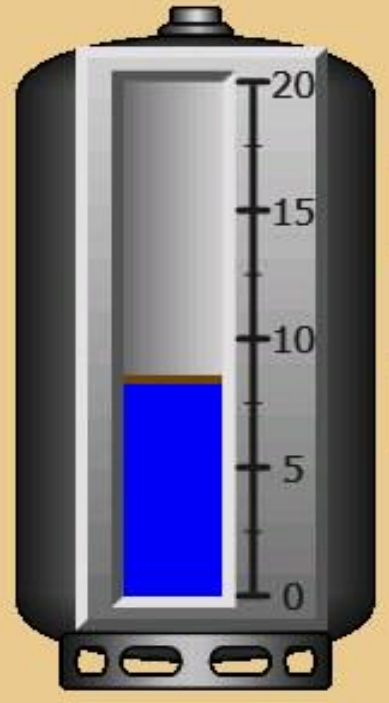
- More than 25% had a security incident last year
- Only 56% have a response plan
- Only 31% have an ICS/OT capable SOC
- Only 12% have extensive monitoring – 30% have none!

- Designers' and Operators' concerns are:
  - Safety
  - Uptime
  - Not Security
- Updates are less frequent, deferred, ignored
- Security is network segmentation, firewalls, and VPNs

BACK

[redacted]

NORTH WATER TANK



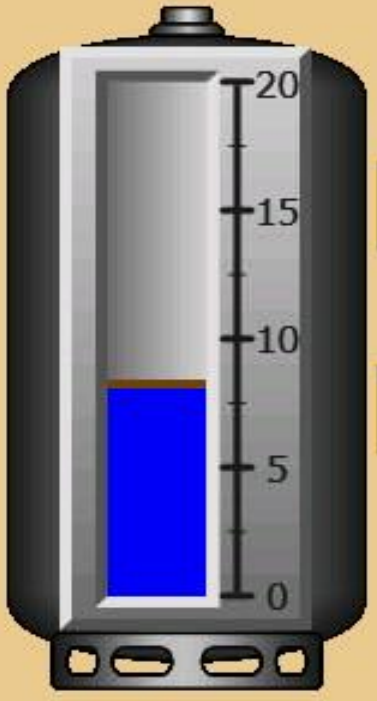
Top Level

8.58 FT

Interface

8.25 FT

SOUTH WATER TANK



Top Level

8.42 FT

Interface

8.08 FT

Remote access active

BMS STATUS

Running

6H

5H

10H

8H

6H

4H

GPU ALARMS

	LL	HH
CASING		
TUBING		
FLOWLINE		
VESSEL		

	HH
INSIDE LEL	

	LL	HH
VESSEL LSH		
VESSEL LSL		

CHOKE VALVE

67.6

LIQUID DATA

SPOT RATE	0.000
TODAYS FLOW	121.172
YESTDY FLOW	160.266
ACCUM FLOW	44071.766
BATT VOLTAGE	3.443

WELL DATA

CASING	1990.605
TUBING	1992.113
FLOWLINE	1488.634
VESSEL	948.982
LEL	-0.253

WELL MEASURMENT

SPOT RATE	13115.485
TODAYS FLOW	7855.694
YESTDY FLOW	10860.702
ACCUM FLOW	346562.906
FLOW TEMP	65.170
STATIC	945.458
DIFF	192.479

BMS SETTNGS

FLAME STRENGTH	1.00
OUTLET TEMP	66.90
BATH TEMP	101.80

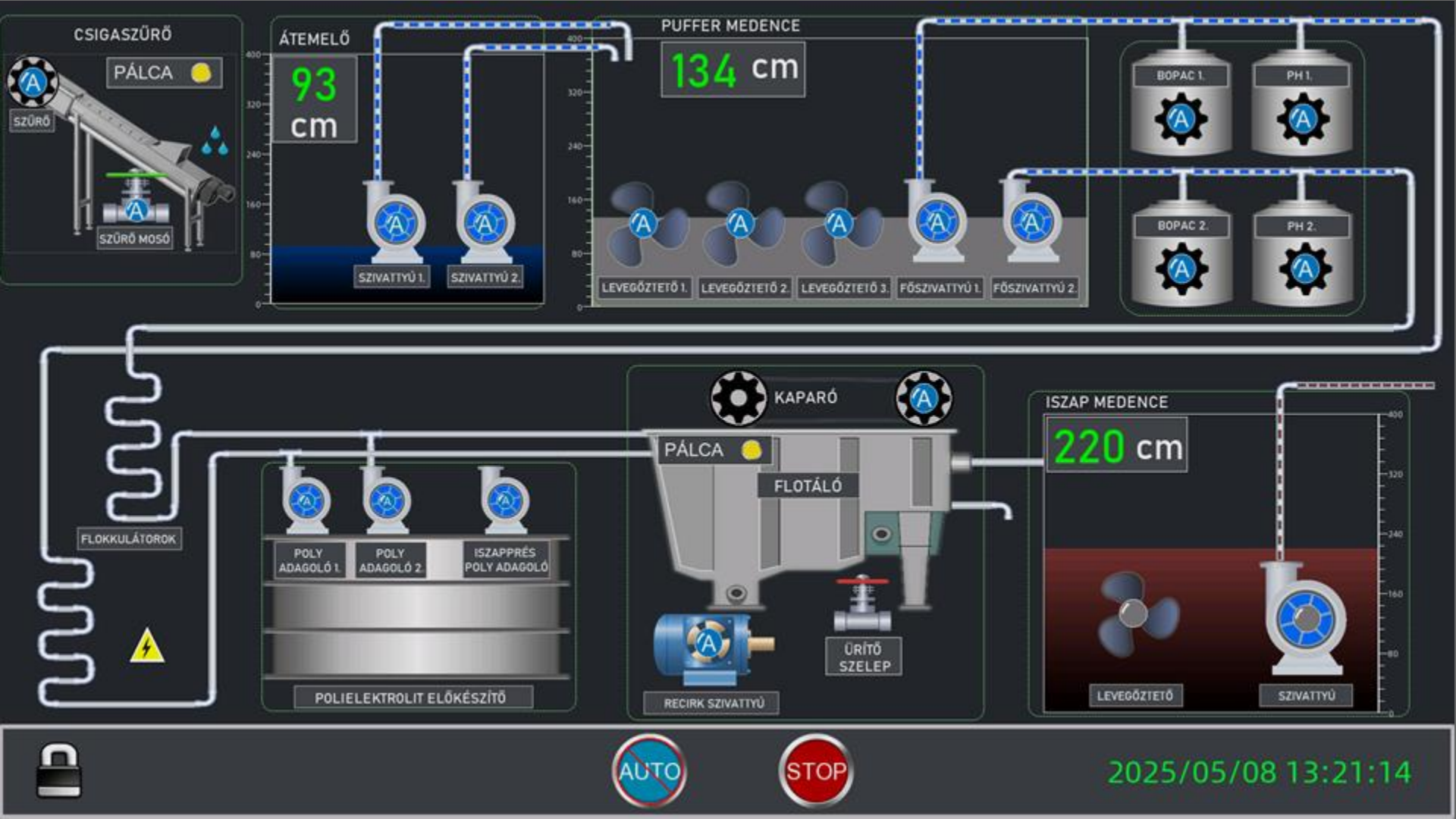
PILOT ON

WELL PERM

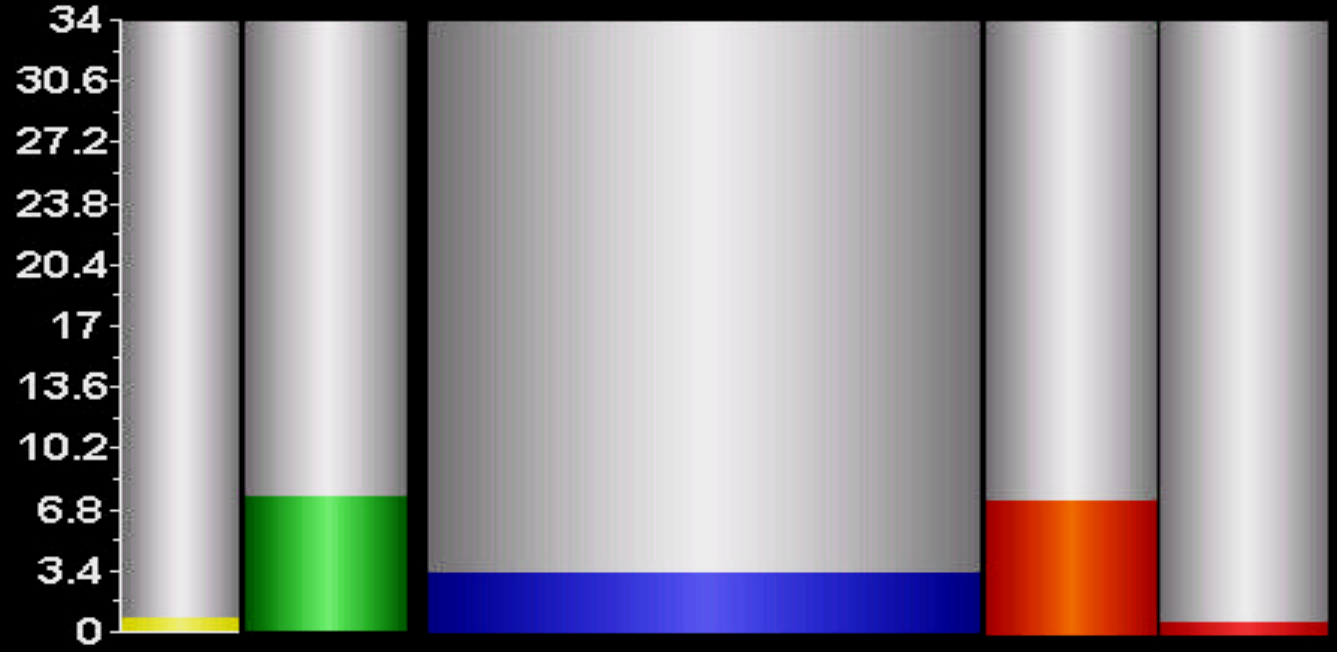
BMS PERM

Reset

HOME


CSIGASZŰRŐ
PÁLCA
SZŰRŐ
SZŰRŐ MOSÓ
ÁTEMELŐ
93 cm
SZIVATTYÚ 1.
SZIVATTYÚ 2.
PUFFER MEDENCE
134 cm
LEVEGŐZTETŐ 1.
LEVEGŐZTETŐ 2.
LEVEGŐZTETŐ 3.
FŐSZIVATTYÚ 1.
FŐSZIVATTYÚ 2.
BOPAC 1.
PH 1.
BOPAC 2.
PH 2.
FLOKKULÁTOROK
POLY ADAGOLÓ 1.
POLY ADAGOLÓ 2.
ISZAPPRÉS POLY ADAGOLÓ
POLIELEKTROLIT ELŐKÉSZÍTŐ
KAPARÓ
PÁLCA
FLOTÁLÓ
ÜRÍTŐ SZELEP
RECIRK SZIVATTYÚ
ISZAP MEDENCE
220 cm
LEVEGŐZTETŐ
SZIVATTYÚ
AUTO
STOP
2025/05/08 13:21:14

LAKE LEVEL SETTINGS



Function

Auto

START LEVEL	7.5
STOP LEVEL	0.8
High Level	7.5
Low Level	0.8

Low Level Alarm

3.4 ft

Actual Level

FILL ON TIMER	FILL OFF TIMER	LOW LEVEL TIMER
0 SEC	0 SEC	0 SEC

MAIN

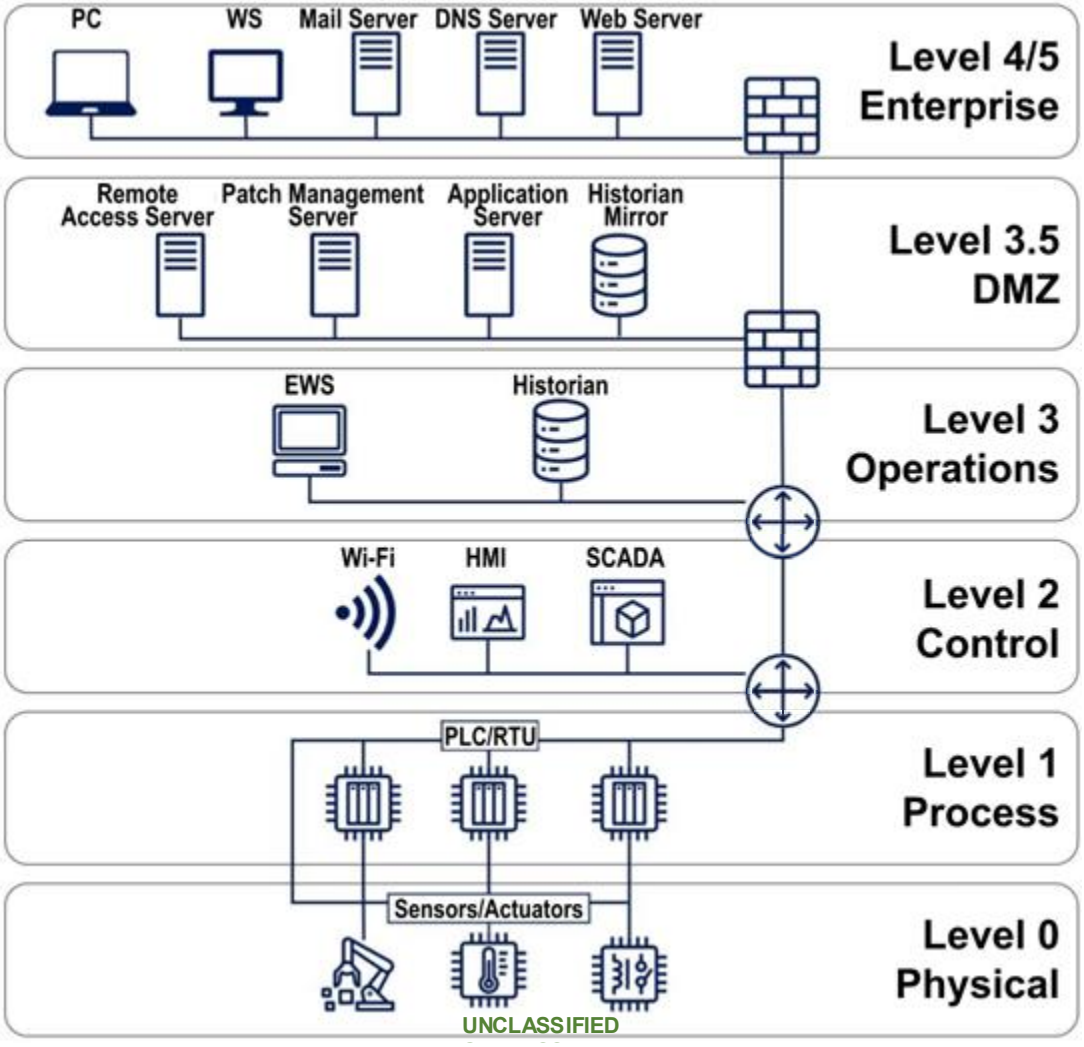
SETUP

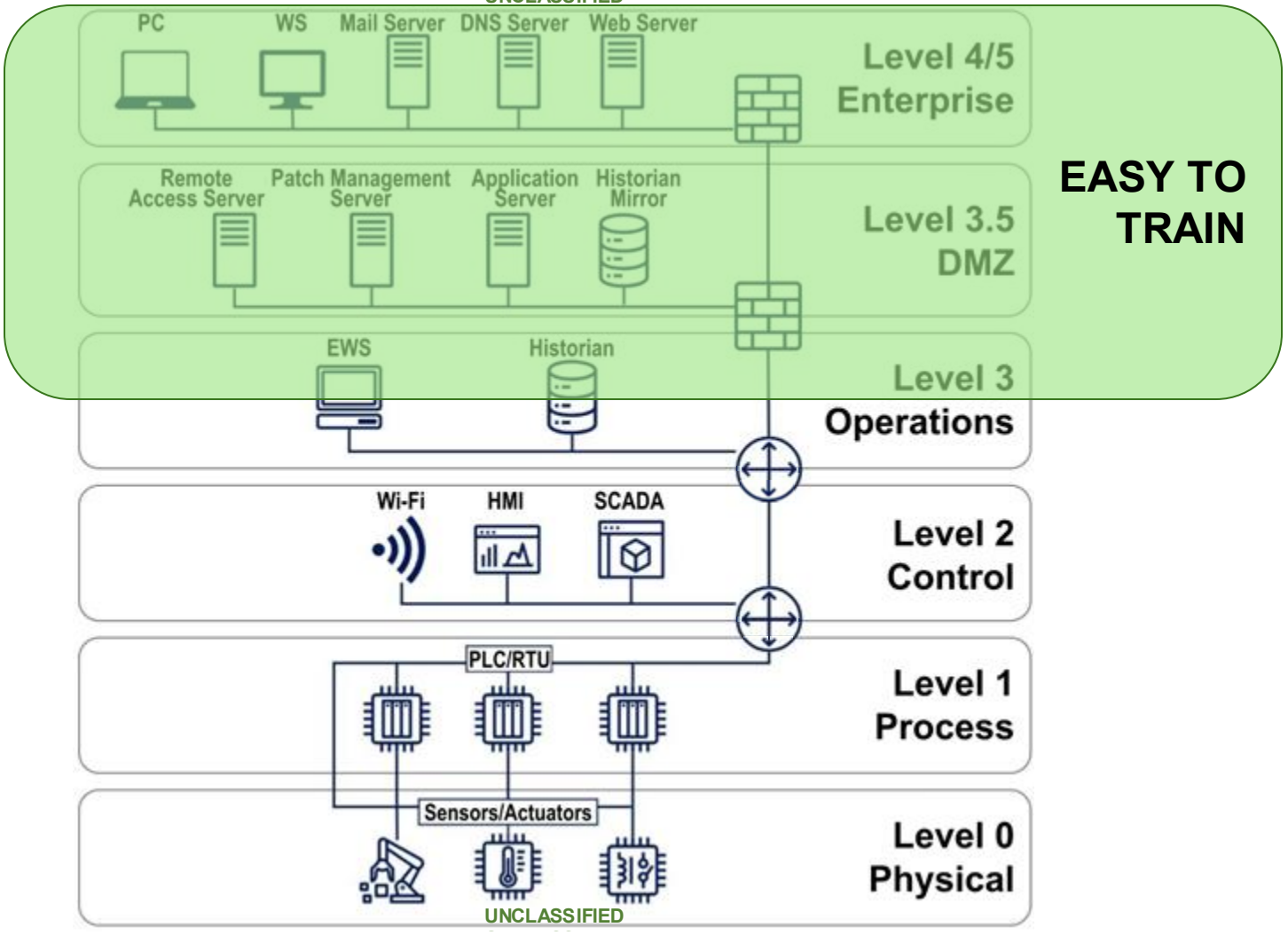
PREV PAGE

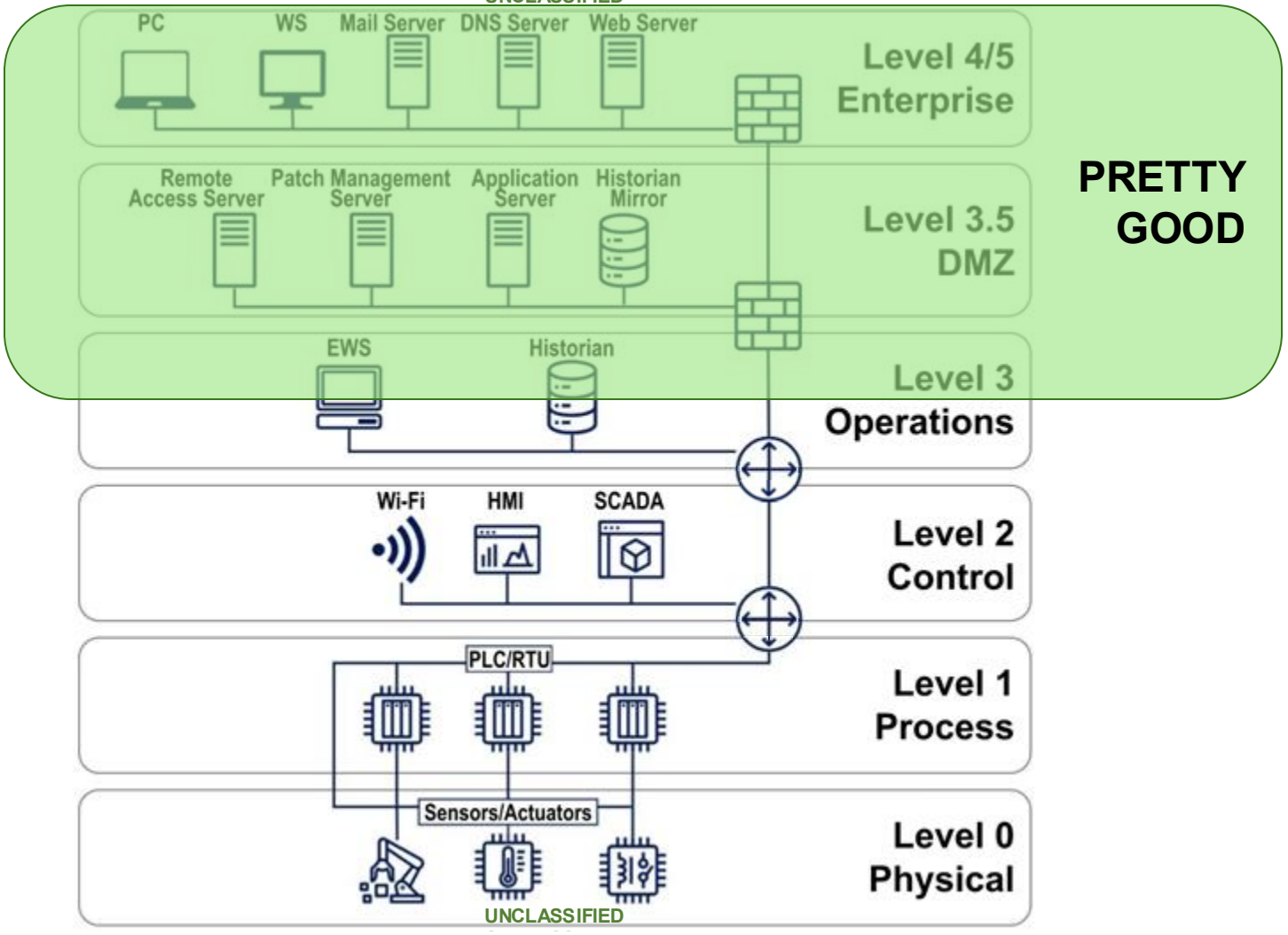
- Hardware and Software refresh cycle is decades long
- Outdated, insecure protocols
- End-Of-Life and Out-of-Support equipment

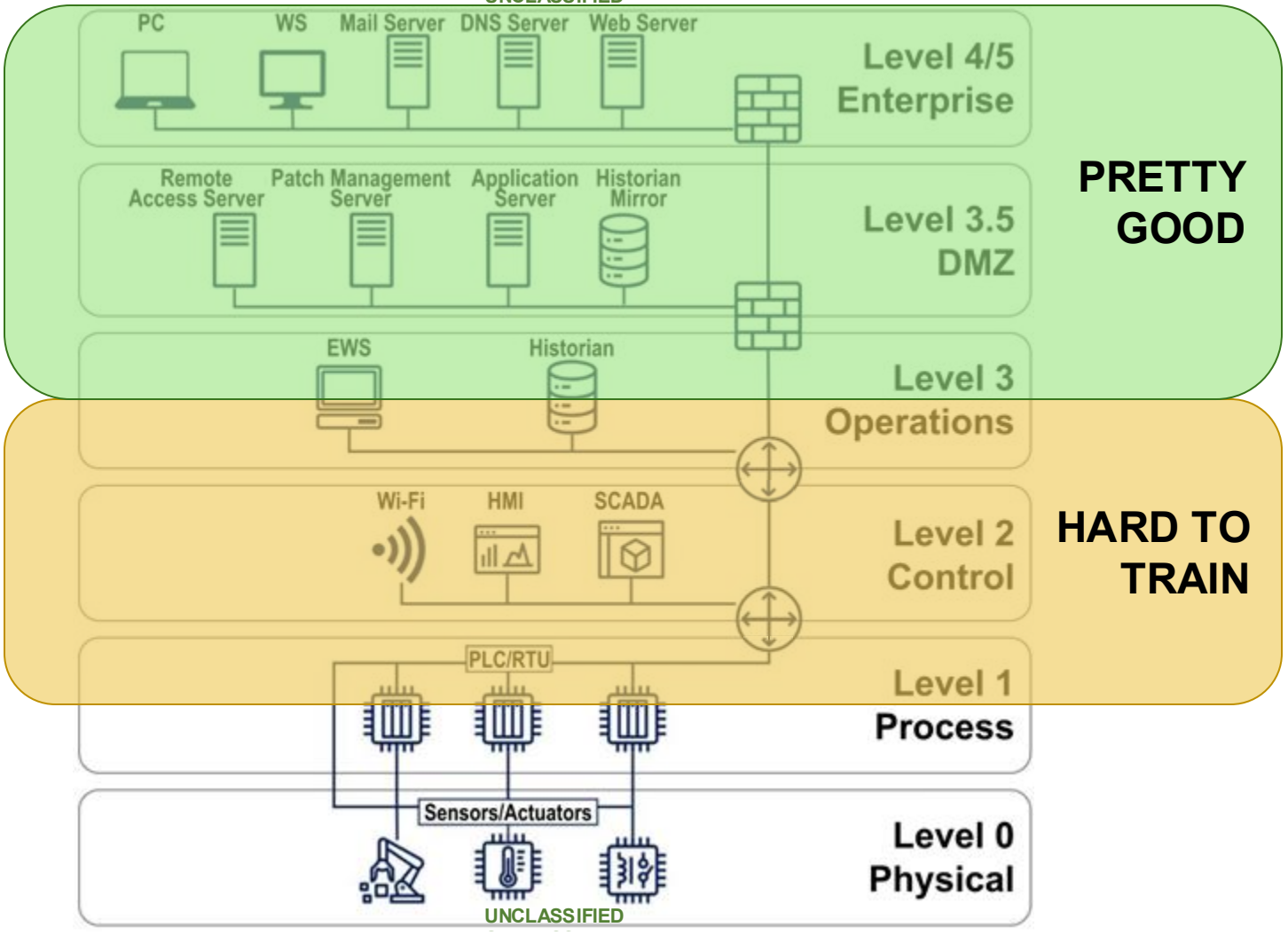
- Obscure systems and protocols – Not Linux or Windows
- Lack of tools – No AntiVirus / EDR
- Scanning can break the network
- Sensoring is hard:
  - Segmentation impedes observability
  - Obscure / outdated protocols and media

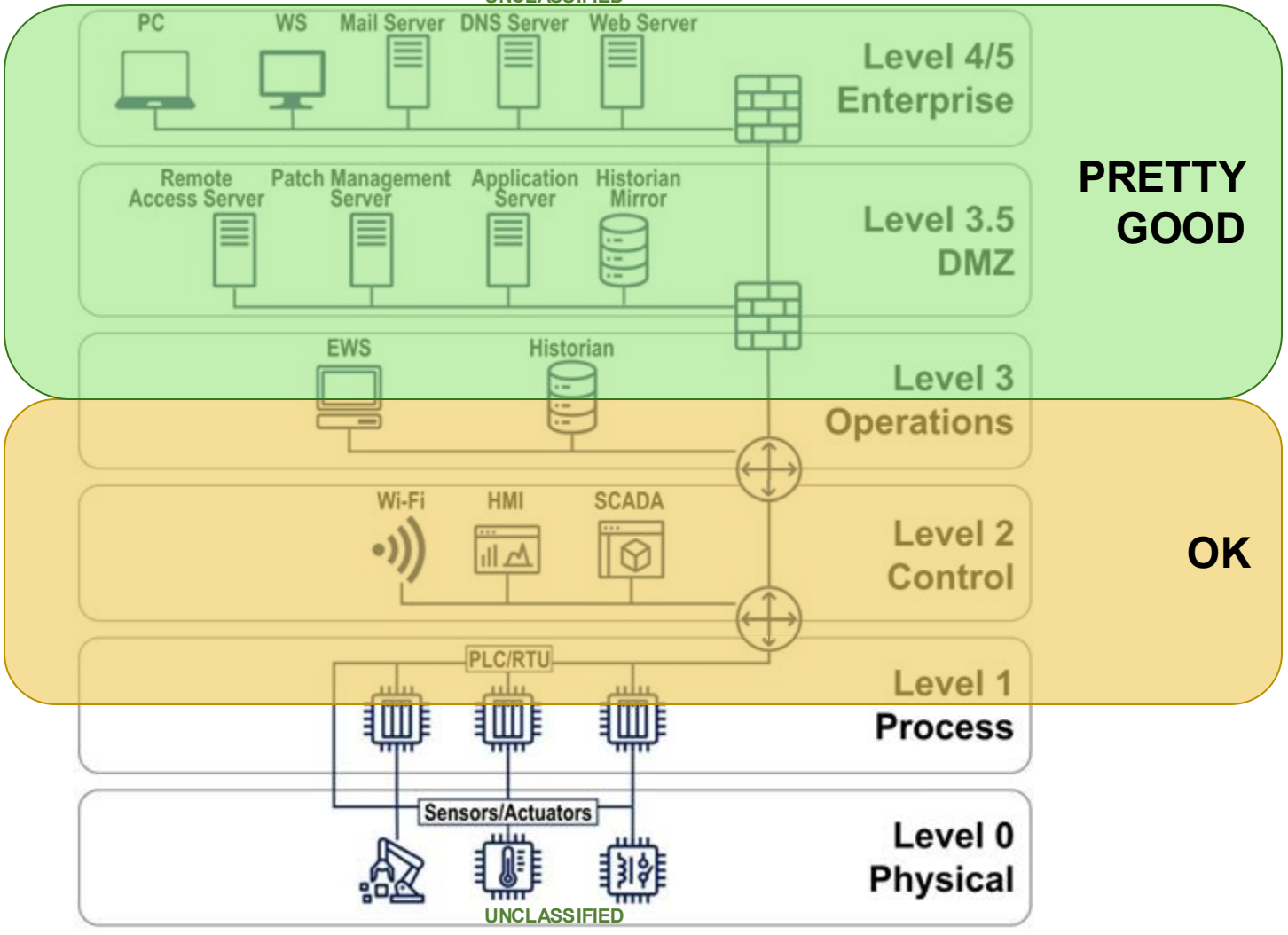
- Half of defenders have:
  - Less than five years experience
  - Have never held an ICS/OT certification
- Training is:
  - rare
  - sparse
  - expensive

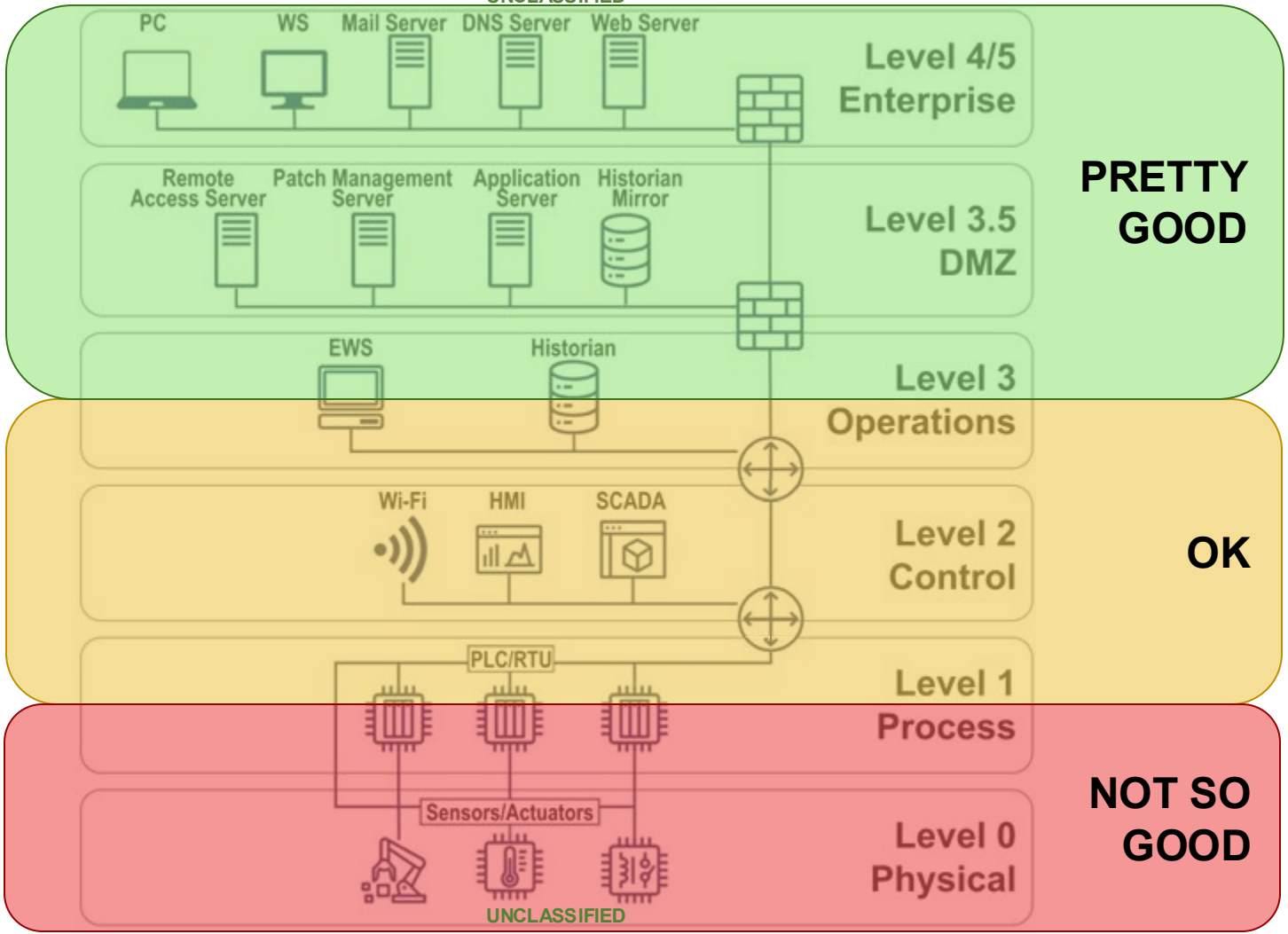

PC
WS
Mail Server
DNS Server
Web Server
Level 4/5
Enterprise
Remote
Access Server
Patch Management
Server
Application
Server
Historian
Mirror
Level 3.5
DMZ
EWS
Historian
Level 3
Operations
Wi-Fi
HMI
SCADA
Level 2
Control
PLC/RTU
Level 1
Process
Sensors/Actuators
Level 0
Physical

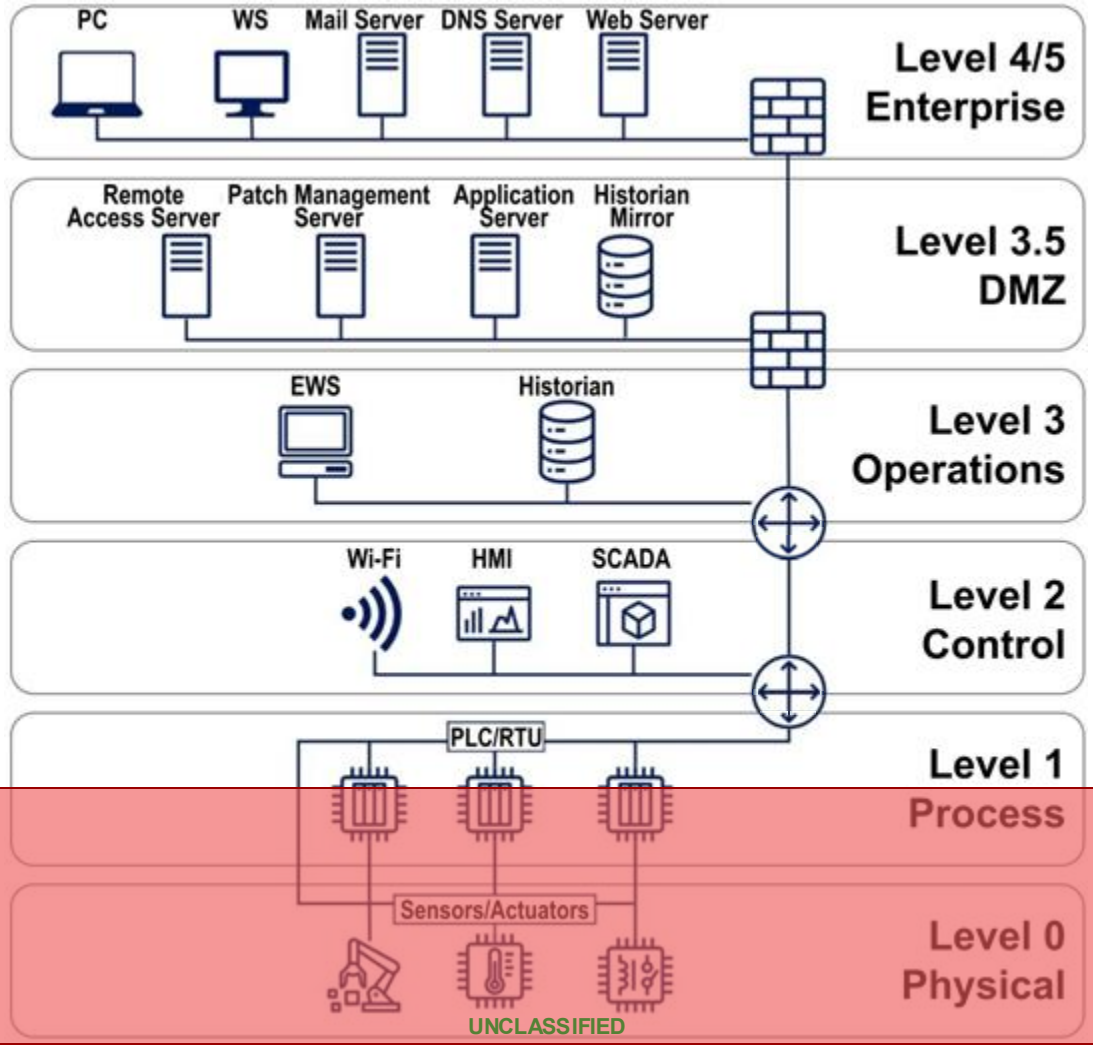

PC
WS
Mail Server
DNS Server
Web Server
Level 4/5
Enterprise
Remote
Access Server
Patch Management
Server
Application
Server
Historian
Mirror
Level 3.5
DMZ
EWS
Historian
Level 3
Operations
Wi-Fi
HMI
SCADA
Level 2
Control
PLC/RTU
Level 1
Process
Sensors/Actuators
Level 0
Physical
EASY TO
TRAIN


PC
WS
Mail Server
DNS Server
Web Server
Level 4/5
Enterprise
Remote
Access Server
Patch Management
Server
Application
Server
Historian
Mirror
Level 3.5
DMZ
PRETTY
GOOD
EWS
Historian
Level 3
Operations
Wi-Fi
HMI
SCADA
Level 2
Control
PLC/RTU
Level 1
Process
Sensors/Actuators
Level 0
Physical


PC
WS
Mail Server
DNS Server
Web Server
Level 4/5
Enterprise
Remote
Access Server
Patch Management
Server
Application
Server
Historian
Mirror
Level 3.5
DMZ
PRETTY
GOOD
EWS
Historian
Level 3
Operations
Wi-Fi
HMI
SCADA
Level 2
Control
HARD TO
TRAIN
PLC/RTU
Level 1
Process
Sensors/Actuators
Level 0
Physical


PC
WS
Mail Server
DNS Server
Web Server
Level 4/5
Enterprise
Remote
Access Server
Patch Management
Server
Application
Server
Historian
Mirror
Level 3.5
DMZ
PRETTY
GOOD
EWS
Historian
Level 3
Operations
Wi-Fi
HMI
SCADA
Level 2
Control
OK
PLC/RTU
Level 1
Process
Sensors/Actuators
Level 0
Physical


PC
WS
Mail Server
DNS Server
Web Server
Level 4/5
Enterprise
Remote
Access Server
Patch Management
Server
Application
Server
Historian
Mirror
Level 3.5
DMZ
PRETTY
GOOD
EWS
Historian
Level 3
Operations
Wi-Fi
HMI
SCADA
Level 2
Control
OK
PLC/RTU
Level 1
Process
Sensors/Actuators
Level 0
Physical
NOT SO
GOOD



RARELY TRAINED!

Current Ranges

- Hardware-based or…
- Hardware-In-The-Loop

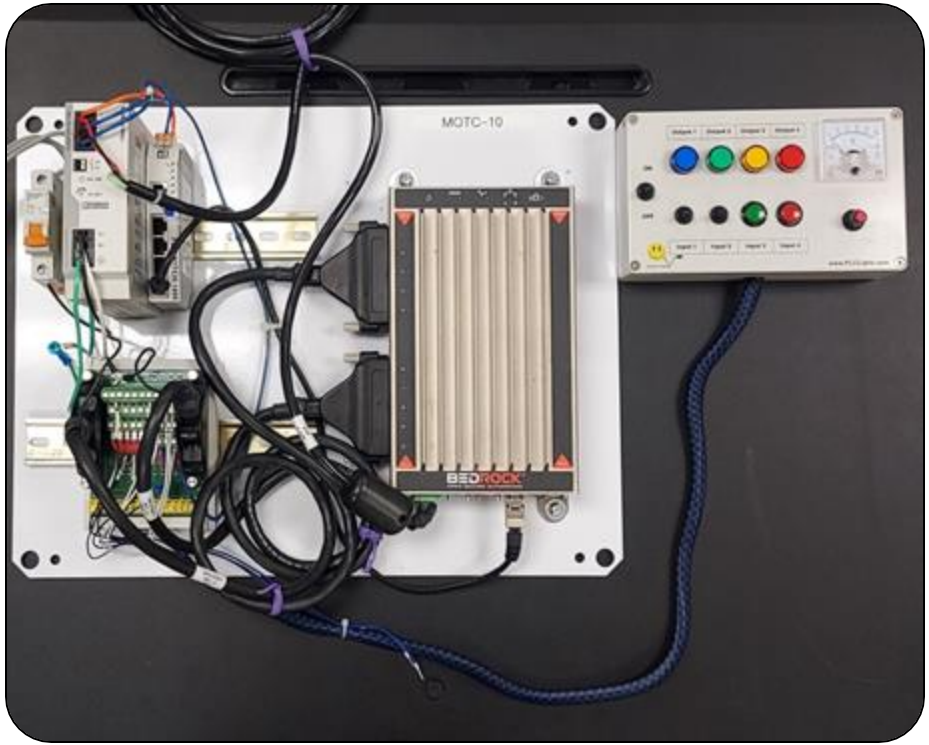
- Realistic traffic
- Physical effects
- Students can see the consequences

223 COS, Little Rock AFB

- Expensive
- Fragile
- Inflexible
- Hard to Transport
- Simplistic
- Long Lead Times
- Not Scalable

223 COS, Little Rock AFB

- Thousands of dollars
- Single protocol
- One controller hardwired to devices
- Lead time up to a year



Masaryk University,
Czech Republic

- Multi-Protocol
- Expensive
- Not Portable
- Reasonably Realistic
- No Visibility Between Controllers and Devices

223 COS, Little Rock AFB

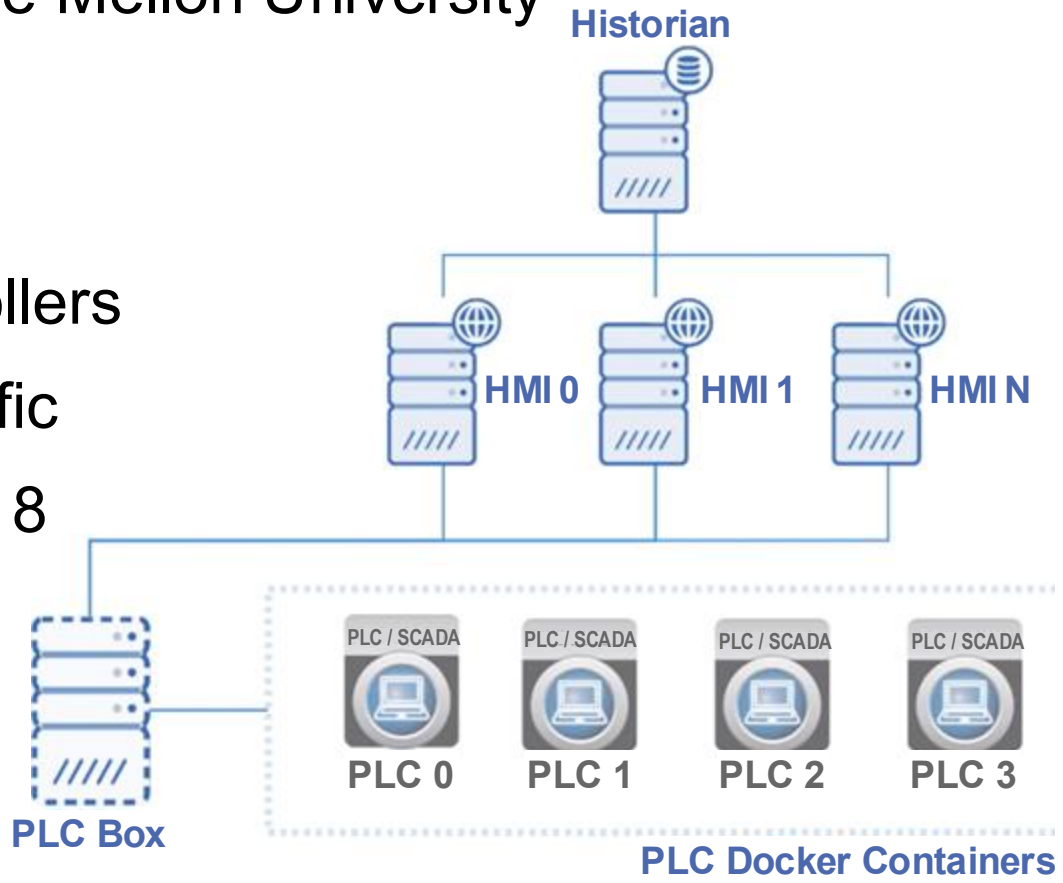
- Very Realistic
- Very Expensive
- Not Portable
- Not at all flexible
- Two year lead

Idaho National Labs

- Incredibly realistic
- Incredibly expensive
- Very Long Lead Time
- Not Easy to Transport

SCADASim by Carnegie Mellon University

- One protocol
- No Physics Engine
- Only Models Controllers
- No Lower Level traffic
- Last Updated in 2018

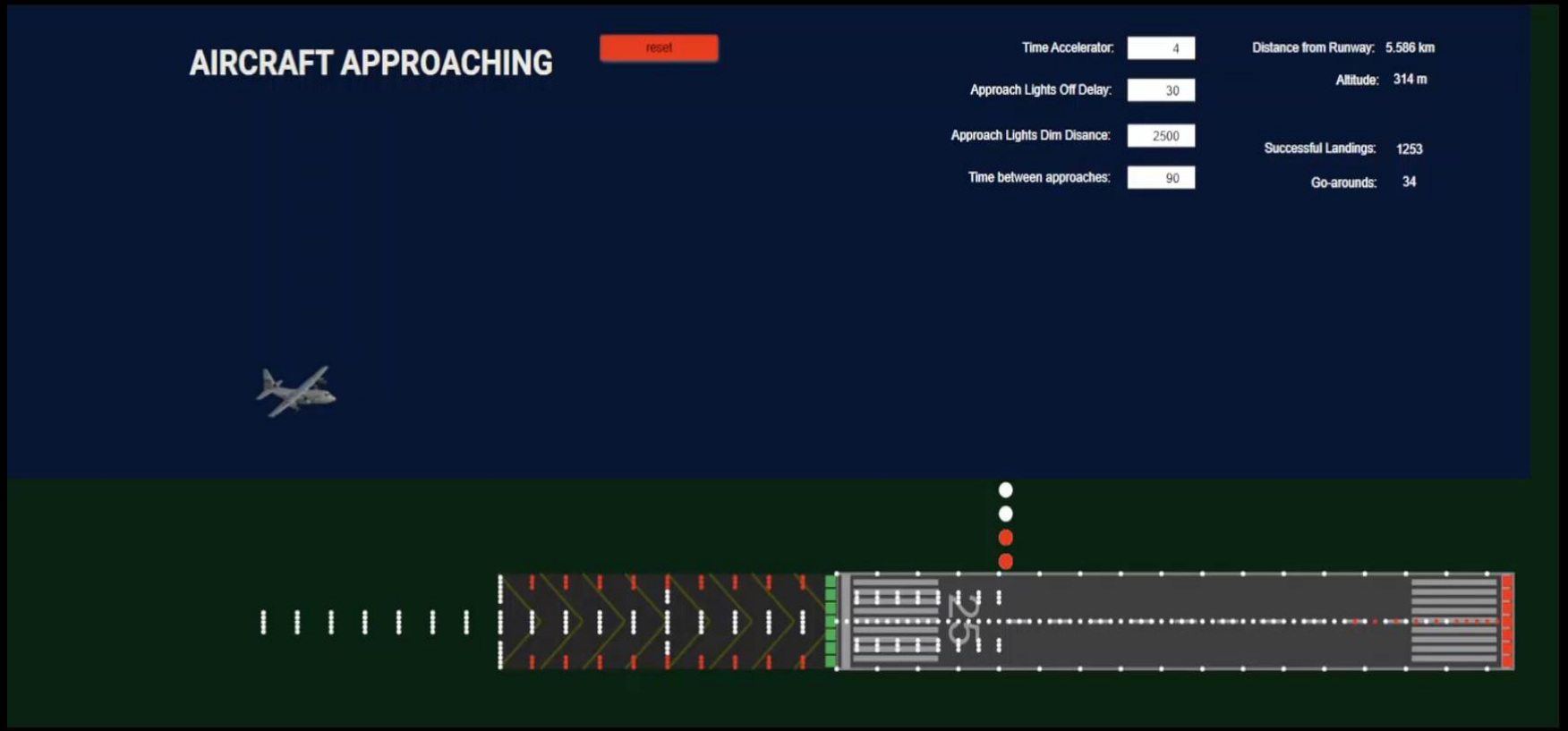


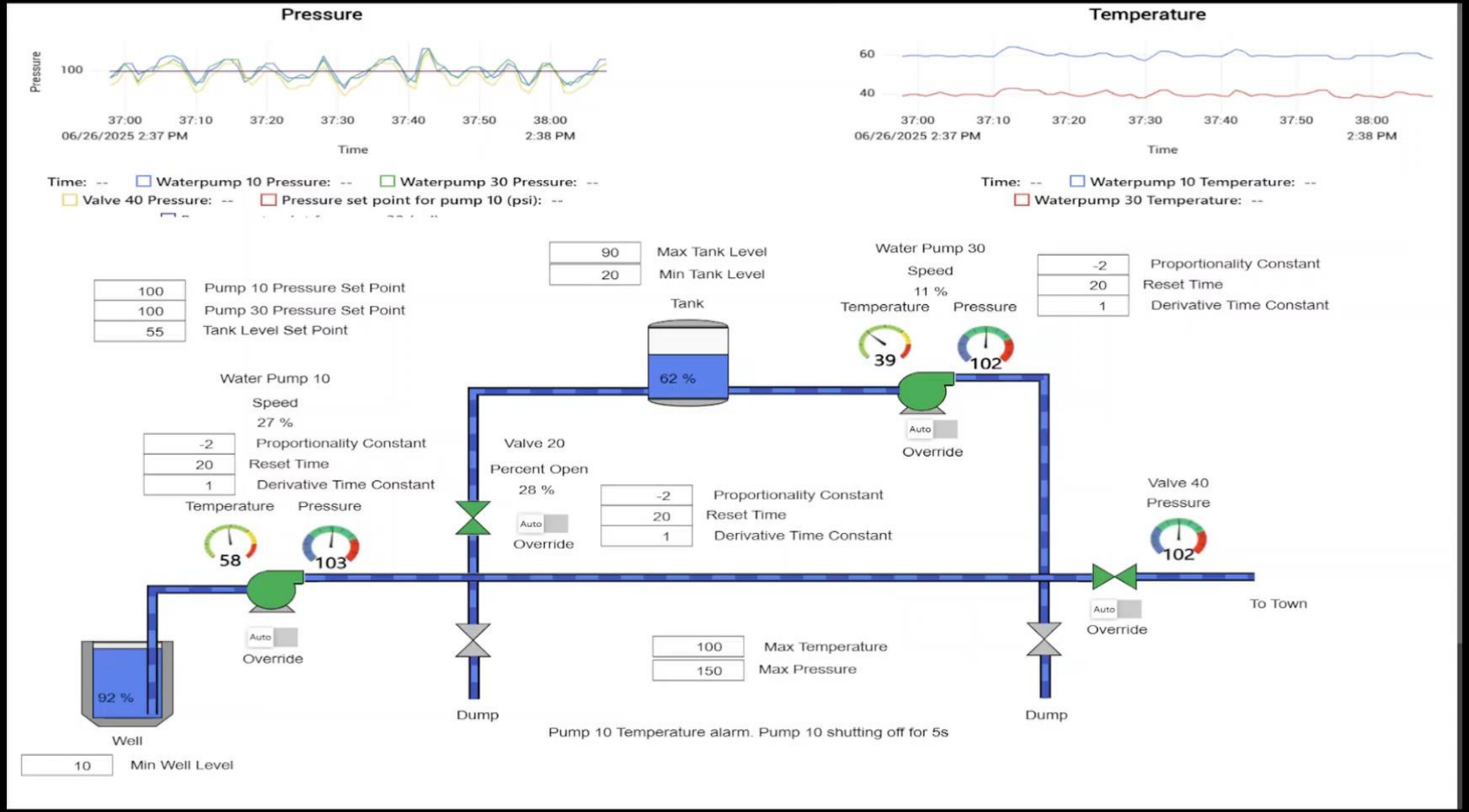
Dockerized OT Training Range (DOTTR)

Hardware-In-The-Loop – Without the hardware

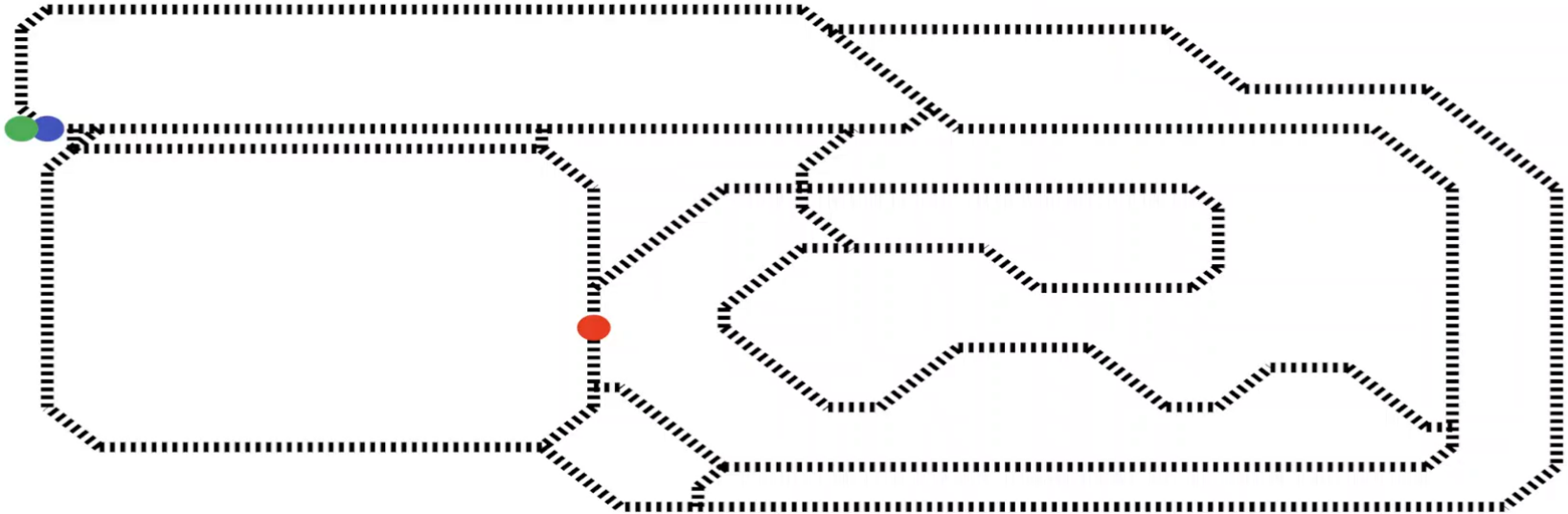
- Docker containers simulate an entire ICS/OT network
- Runs in a single virtual machine

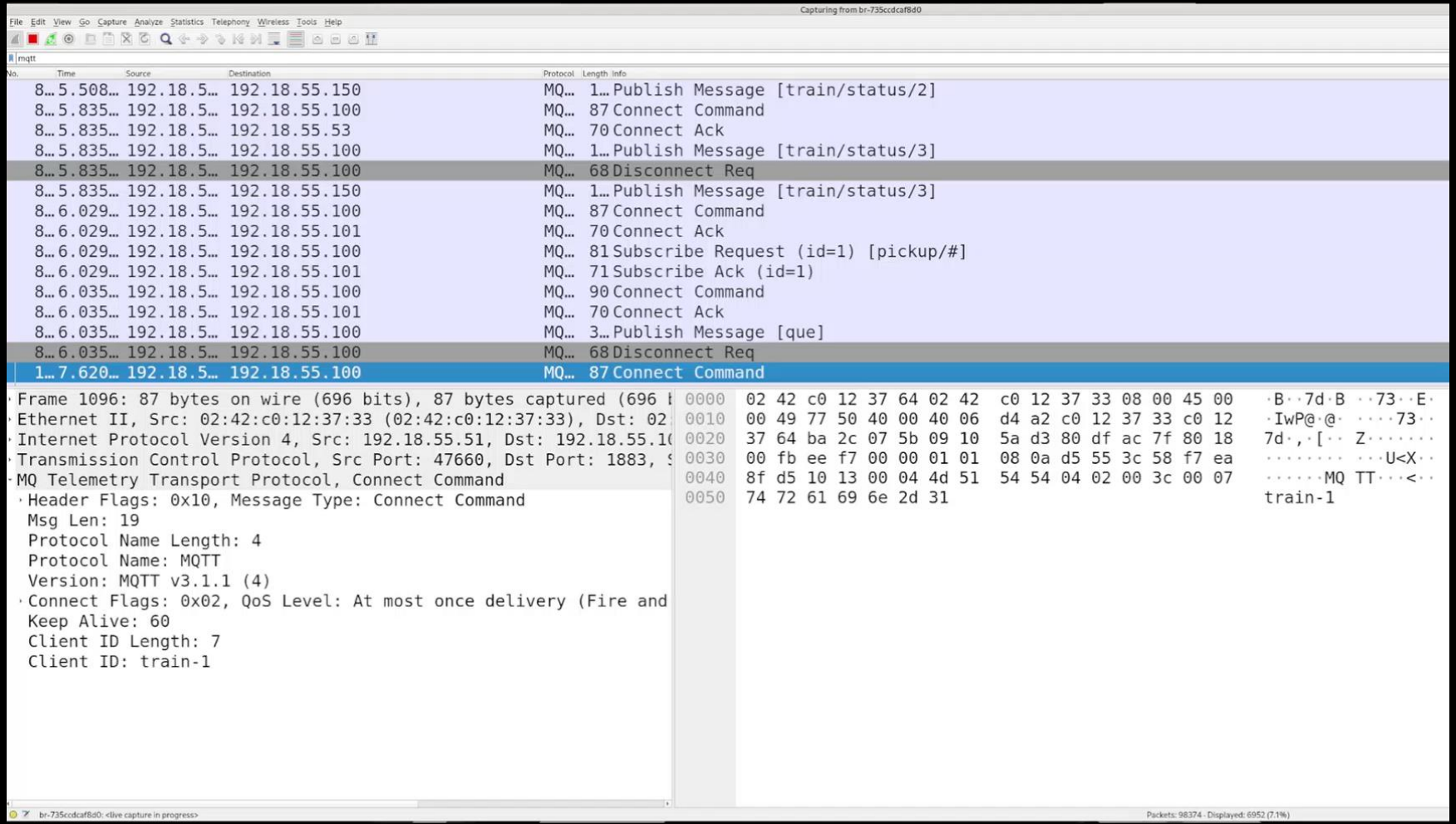
- Observable
- Controllable
- Attackable
- Defendable


AIRCRAFT APPROACHING
reset
Time Accelerator:
4
Approach Lights Off Delay:
30
Approach Lights Dim Disance:
2500
Time between approaches:
90
Distance from Runway:
5.586 km
Altitude:
314 m
Successful Landings:
1253
Go-arounds:
34


Pressure
Pressure
100
37:00
37:10
37:20
37:30
37:40
37:50
38:00
06/26/2025 2:37 PM
2:38 PM
Time
Time: --
Waterpump 10 Pressure: --
Waterpump 30 Pressure: --
Valve 40 Pressure: --
Pressure set point for pump 10 (psi): --
Temperature
60
40
Time: --
Waterpump 10 Temperature: --
Waterpump 30 Temperature: --
90
Max Tank Level
20
Min Tank Level
100
Pump 10 Pressure Set Point
100
Pump 30 Pressure Set Point
55
Tank Level Set Point
Tank
62 %
Water Pump 30
Speed
11 %
Temperature
Pressure
39
102
-2
Proportionality Constant
20
Reset Time
1
Derivative Time Constant
Auto
Override
Water Pump 10
Speed
27 %
-2
Proportionality Constant
20
Reset Time
1
Derivative Time Constant
Temperature
Pressure
58
103
Valve 20
Percent Open
28 %
Auto
Override
-2
Proportionality Constant
20
Reset Time
1
Derivative Time Constant
Valve 40
Pressure
102
Auto
Override
To Town
92 %
Well
Auto
Override
100
Max Temperature
150
Max Pressure
Dump
Dump
Pump 10 Temperature alarm. Pump 10 shutting off for 5s
10
Min Well Level

Train 1		Train 2		Train 3	
X Position:	30	X Position:	240	X Position:	20
Y Position:	240	Y Position:	340	Y Position:	240
Passengers:	2	Passengers:	2	Passengers:	3




Capturing from br-735ccdcaf8d0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
mqtt
No. Time Source Destination Protocol Length Info
8… 5.508… 192.18.5… 192.18.55.150 MQ… 1… Publish Message [train/status/2]
8… 5.835… 192.18.5… 192.18.55.100 MQ… 87 Connect Command
8… 5.835… 192.18.5… 192.18.55.53 MQ… 70 Connect Ack
8… 5.835… 192.18.5… 192.18.55.100 MQ… 1… Publish Message [train/status/3]
8… 5.835… 192.18.5… 192.18.55.100 MQ… 68 Disconnect Req
8… 5.835… 192.18.5… 192.18.55.150 MQ… 1… Publish Message [train/status/3]
8… 6.029… 192.18.5… 192.18.55.100 MQ… 87 Connect Command
8… 6.029… 192.18.5… 192.18.55.101 MQ… 70 Connect Ack
8… 6.029… 192.18.5… 192.18.55.100 MQ… 81 Subscribe Request (id=1) [pickup/#]
8… 6.029… 192.18.5… 192.18.55.101 MQ… 71 Subscribe Ack (id=1)
8… 6.035… 192.18.5… 192.18.55.100 MQ… 90 Connect Command
8… 6.035… 192.18.5… 192.18.55.101 MQ… 70 Connect Ack
8… 6.035… 192.18.5… 192.18.55.100 MQ… 3… Publish Message [que]
8… 6.035… 192.18.5… 192.18.55.100 MQ… 68 Disconnect Req
1… 7.620… 192.18.5… 192.18.55.100 MQ… 87 Connect Command
Frame 1096: 87 bytes on wire (696 bits), 87 bytes captured (696 b
Ethernet II, Src: 02:42:c0:12:37:33 (02:42:c0:12:37:33), Dst: 02
Internet Protocol Version 4, Src: 192.18.55.51, Dst: 192.18.55.10
Transmission Control Protocol, Src Port: 47660, Dst Port: 1883, S
MQ Telemetry Transport Protocol, Connect Command
Header Flags: 0x10, Message Type: Connect Command
Msg Len: 19
Protocol Name Length: 4
Protocol Name: MQTT
Version: MQTT v3.1.1 (4)
Connect Flags: 0x02, QoS Level: At most once delivery (Fire and
Keep Alive: 60
Client ID Length: 7
Client ID: train-1
0000 02 42 c0 12 37 64 02 42 c0 12 37 33 08 00 45 00 ·B··7d·B ··73··E·
0010 00 49 77 50 40 00 40 06 d4 a2 c0 12 37 33 c0 12 ·IwP@·@· ····73··
0020 37 64 ba 2c 07 5b 09 10 5a d3 80 df ac 7f 80 18 7d·,·[·· Z·····
0030 00 fb ee f7 00 00 01 01 08 0a d5 55 3c 58 f7 ea ·····U<X··
0040 8f d5 10 13 00 04 4d 51 54 54 04 02 00 3c 00 07 ·····MQ TT···<··
0050 74 72 61 69 6e 2d 31 train-1
br-735ccdcaf8d0: <live capture in progress>
Packets: 98374 · Displayed: 6952 (7.1%)

Realistic:

- Full stack from devices to enterprise network
- Fully segmented and routed networking
- Physics that mirror the real world
- Controllable with HMI, SCADA, command line

Portable:

- Runs on any Linux machine
- Can be cloud hosted
- Accessible from anywhere
- Enables Mobile or Virtual Training
- Independent / Asynchronous Exercises

Fast:

- New Model Development – months
- Installation in new environment – hours
- Exercise deployment – minutes
- Range reset – seconds

Scalable & Adaptable:

- Develop once, Deploy many
- Single or multiple simultaneous users
- Network restructure is just a few config files
- Programmed in common languages
- Can be integrated with existing ranges

Affordable:

- Development costs less than a single hardware model
- Based on Free Open Source Software
- No Licensing or Subscriptions
- Under $0.25 per hour running in the cloud

Current Status

Models:

- Water Plant (Modbus) – Production
- Runway Lights (Modbus) – Production
- Tramway (MQTT) – Final development
- Airframe (1553 over IP) – Early development
- Electrical Grid (DNP3) – Early development

In Use At:

- MDT/MACCE Schoolhouse (Little Rock AFB)
- Persistent Cyber Training Environment (PCTE)

Future Plans

- Data Center (BACnet)
- Enterprise IT network simulation
- Grey Traffic Generation
- Interconnection with Hardware-in-the-Loop

- FOSS & Government owned
- Packaged with Software Bills of Materials (SBoMs)
- Available for mil-to-mil transfer with authorization

Mil-to-Mil Coordination:

- Katie.A.Riegel@SAIC.com
- Kayla.R.Sturgeon@SAIC.com

Lead Developer:

- John.A.Timaeus@SAIC.com

Questions?