

Task 3

Data Collection and Aggregation

Status

5.10.2023

Recap - The Task Overview - Recap



- Task Leader - ASU
- Participants - ASU, BGU, OTORIO, DK Innovation, DLC, Nexant, Delek, Arava
- Task Goal - Provide **reliable & comprehensive IT/OT datasets** that will include Cyber attacks simulated in various of ways and logged 360°
- Task objectives - Lab environments operations, Advisory emulation + Datasets generation

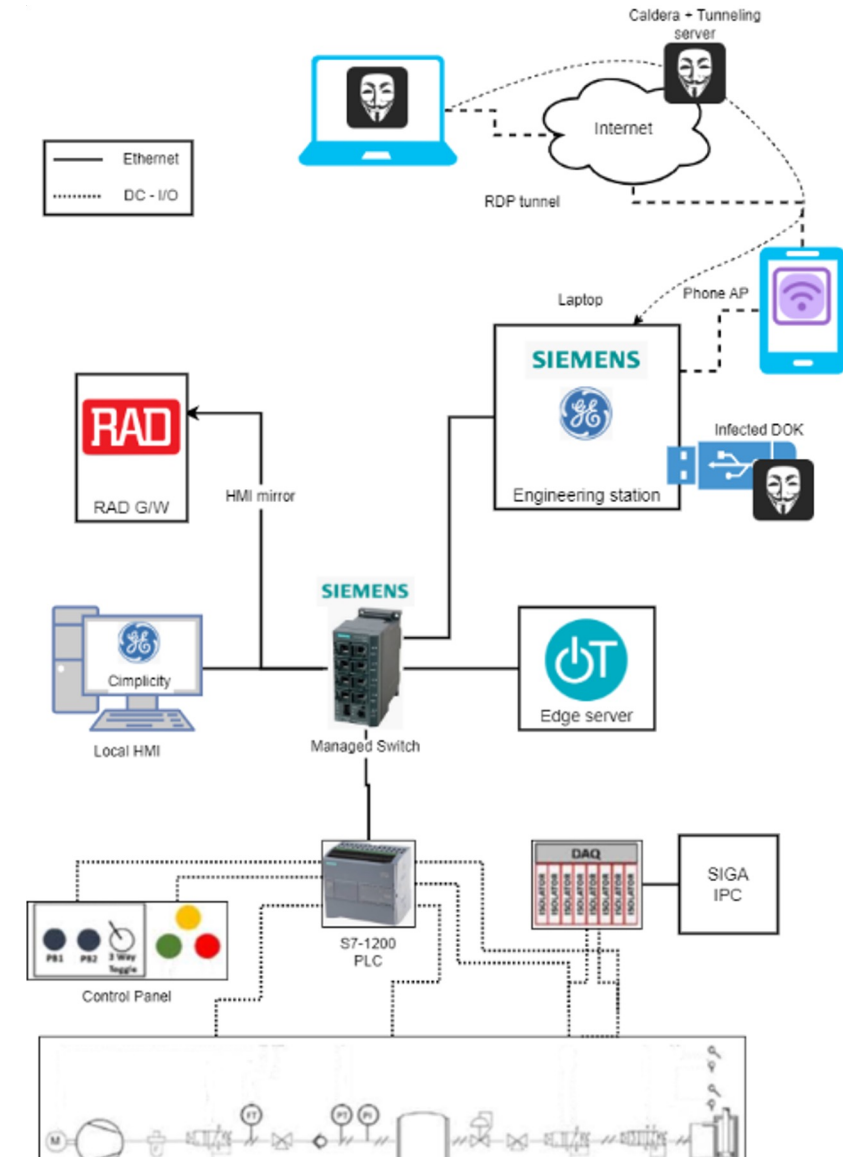
How -

- Setting up multiple lab environments
- Setting up multiple sensors to monitor the network from different aspects
- Setting up RAM² as central logging system + build necessary plugins
- Execute live attack scenarios

Last accomplishment (collection)




- Collection of real IT/OT attacks on the Meptagon lab
- Executed various live attacks on the physical lab including Modbus MITM
- Windows logs, PCAPs, Tag values...
- Some members analyzed the data
 - Got initial feedback



What was done in Q2-Q3



- Delek US lab discussions
 - Architecture
 - Various simulators (physical/virtual)
 - Design with third party
- Exploring physical lab alternatives
 - Conveyor belt bought
 - Reverse engineering attempt
- Design new lab with Meptagon :



BIRD Foundation

Process Control Simulation System

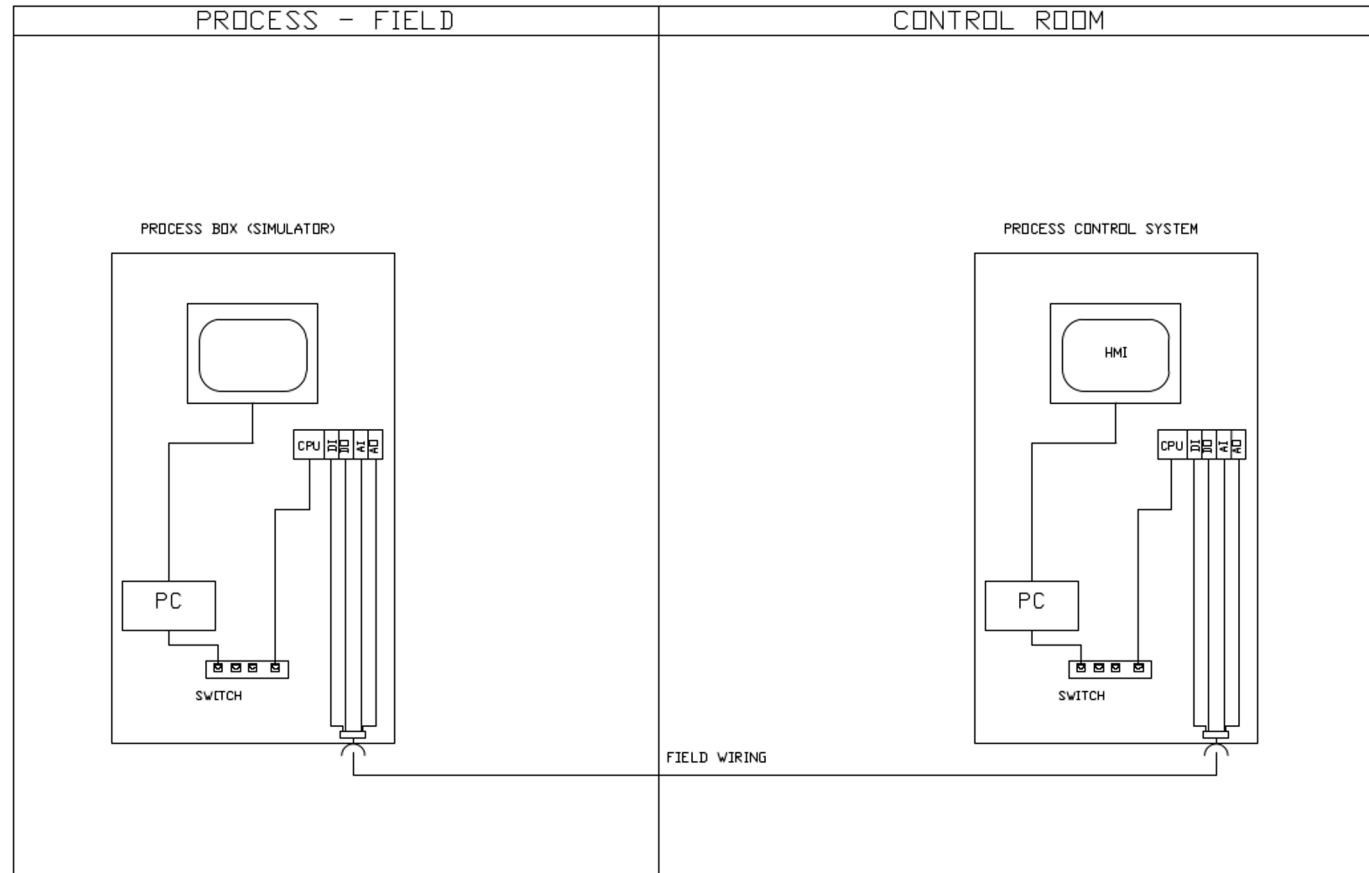
Basic System Presentation

Description

- A Conceptual Process Control Simulation System for one generic distillation unit that separates liquids
- The system is a standalone simulation system
- Process Control from the “Control Room” is based on:
 - Operator standard capabilities :
 - *Setting typical parameters such as: Set points, alarm levels and shut down values.*
 - *Manual control of certain automated elements.*
 - Process Control is realized by Siemens S7 PLC and WinCC HMI
 - Process data after running a simulation can be accessed from an SQL table.
 - All critical process parameters shall be displayed and recorded in WinCC
- Process Simulator is based on:
 - *A PC application integrated with a Siemens S7 PLC and WinCC HMI*

Architecture

- Cabinet for Process Simulation and visualization
- Cabinet for Control Room Operator Station

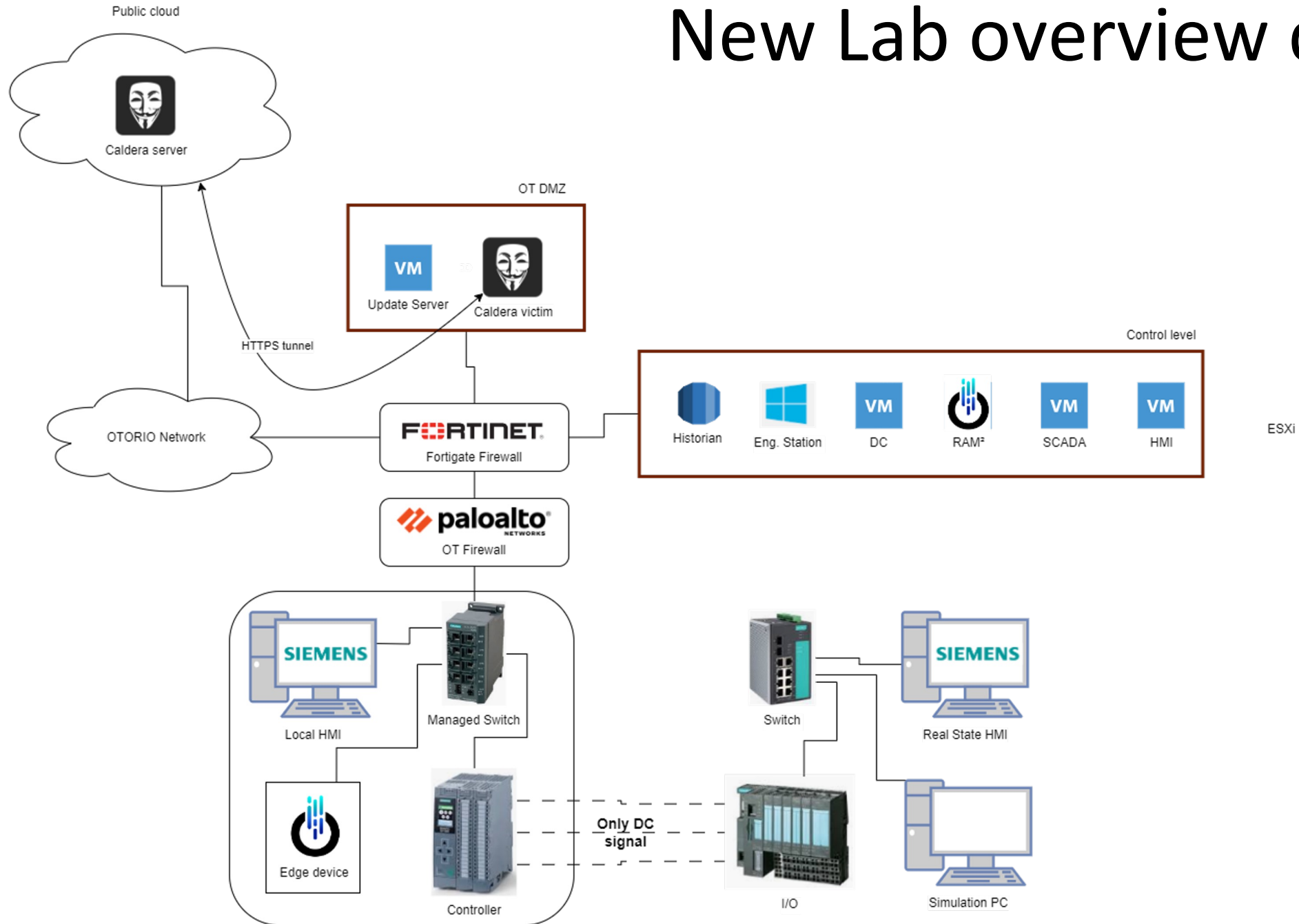


New Meptagon Lab



- Innovative, cost effective lab that uses real OT devices and is able to simulate real life distillation process
- Will use common Siemens PLC and HMI
- Experienced engineers will write both the automation logic and the simulation software
- Simulation software will show the “real state” process while the regular HMI can be fooled by cyber attacks
- From the environment perspective, the lab will look like a real OT environment and the data will be genuine
- The I/Os will be physically attached to the simulation I/O controller for a true simulation.
- Attack scenarios will be built with the Mepragon engineers and implemented by the OTORIO team
- Collection from multiple IT/OT sources - PCAPs, tag value, switches, endpoint logs...

New Lab overview diagram



Previous status

(Only for reference , no need to present)

Recap - Existing datasets



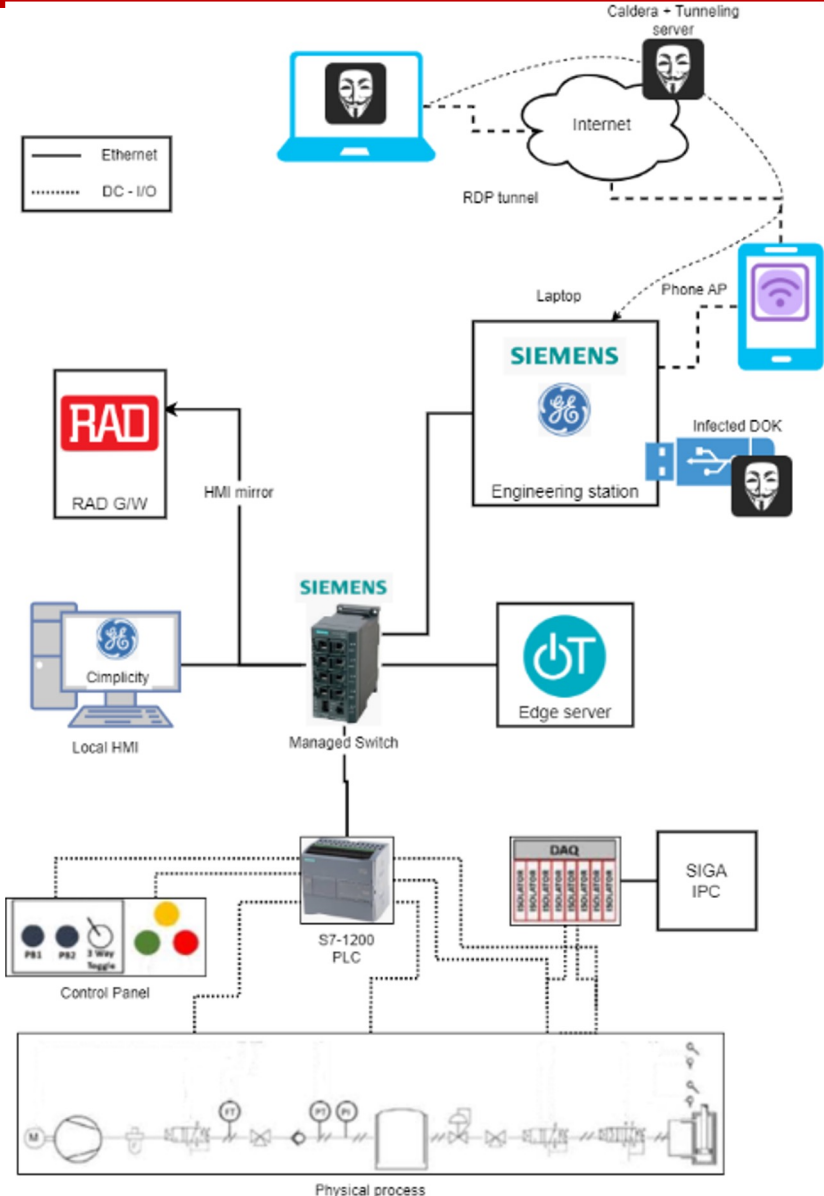
Dataset Name	Sensors Data	Network Data	Electrical Data
OTORIO Labs	X	V	X
Arava Power Dataset	X	X	V
Delek US Dataset	V	X	X
Energy Management	V	X	V
Gas Pipeline & Water Tank	V	X	X
HAI	V	X	X
OPC UA Dataset	X	V	X
Kaggle Faulty Sensor Dataset	V	X	X
Power System Attack Dataset	V	X	V
BATADAL/CISSDataset	V	X	X
EPIC Dataset	V	V	V
WADI Dataset	V	X	X
SWaT Dataset	V	V	X
Meptagon/OTORIO	V	V	V

Meptagon Lab ID



Process	? (Subprocess / air pressure)
Vendors	Siemens, GE, Microsoft
High level architecture	S7-1200 PLC talks to GE Cimplicity HMI using Modbus protocol
Attack scenario 1	Engineering laptop got infected by a malicious DOK
Attack scenario 2	Attacker did various IT exploitation and gathered information about the OT
Attack scenario 3	Attacker performed a MITM attack on the OT network and fixed values in the HMI
Testing environment	Meptagon physical lab + OTORIO laptops
Data sources	Full PCAPs, Tag values, Event logs, SNMP traps, Asset inventory

Architecture



Attack scenario - IT



- Engineering machine accidentally connects to the hotspot....
- USB was connected to the station to download a new Cimplicity project, infected with setup.exe file
- User executed the setup.exe file which cause him connect with a reverse HTTP shell to Command and Control server in the cloud
- The attacker has executed some scans, added user for backdoor and executed a file that create an RDP tunnel with the C&C server
- The tunnel allowed the attacker to connect port 7676 on its C&C server and the connection opened an RDP session to victim - NAT bypassing
- The attacker connected with RDP to the victim

Attack scenario - OT



- MITM modbus (ARP Based) project were moved to the victim via RDP
- The attacker executed MITM attack between the HMI device and the PLC on the OT network
- The attacker manipulated the HMI and PLC:
 - Made several tries of changing both the HMI and PLC values
 - Successfully “Lied” to the HMI about a static value even though it changed
- The attacker finished the session

Attack scenario



A	B	C	D	E
Time	What happened	Notes		
~10:00	Arrived on site and started connecting laptops	Pre-requisites		
10:55	Started PCAP on Edge	Verified that snmp traps from scalance are working		
11:04	Started port mirroring of the PLC (port 5)			
12:03	S7 Monitoring started			
12:04	Clear logs Eng.			
12:06	Wireshark started eng.			
12:06	PCAP started on HMI			
12:15	moved to hmi setpoints mode (process has stopped for sec)			
12:20	moved to manual mode (HMI)			
12:43	starting HMI again			
12:48	Increased physical switch speed to 3 and 6			
12:50	decreased to 2.5 6.5			
13:53	WIFI connected to victim + DOK inserted			
13:55	setup.exe ran + connected to Caldera			
13:56-14:05	S7 scan, Network share discovery, Admin created, DCE_RPC scan	Various IT/OT attacks		
14:13	Dropped reverse tunnel on the victim			
14:14	RDP session started			
14:17	Siga tech. opened the valve (physical maintenance op.)			
	14:21 RDP session started			
	14:26 RDP started			
	14:28 ARP poisoning on both PLC and HMI	Start of Main OT attack		
	14:29 HMI copy from the share			
	14:30 "Lie to the HMI that the values are SP 1 and 100 (I and H)	HMI false data injection		
	14:37 Change the HMI			
	14:41 Siga tech. increased level (Physical change maintenance)			
	14:56 Starting shutting down everything	End of scenarios		

What was collected



- PCAPs file from
 - VICTIM machine (Engineering station)
 - HMI
 - PLC via port mirror from SCALANCE switch
 - OTORIO Edge device
- Events log -
 - VICTIM (Engineering station) monitored with sysmon
 - HMI - windows event log
- TAGS -
 - PLC tag values over time
- SNMP traps
- Asset inventory CSV

What can we do with that?



- Analyze!
 - Try to correlate the different data sources together
 - Build new detection methods
- Open Source / Present in conferences
 - Gather more feedback and partners
- Commercialize
 - Offer the data in a commercial package
 - (Too basic?)

Next Steps



- Get Feedback from you!
 - Going back for additional collection?
- Additional labs!