Finals Briefing

Organised by

iTrust
Centre for Research in Cyber Security

Supported by

CSA SINGAPORE

DRAGOS

National Cybersecurity R&D Laboratory

TAL TECH


The Return to Control
CISS 2025

Congratulations to the Finalists!

0x90	ADFCSA	die_trying	RedCube A
Stanford Applied Cyber	T-Lao-Sec	Team Baguette	TuAMK Goblins
	UncleCY	YCelcnU	

Agenda

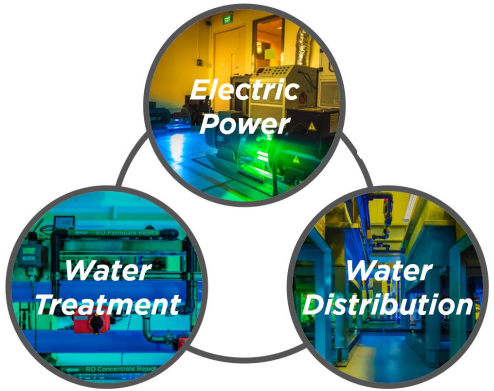
- ➔ Objectives
- ➔ Details
- ➔ Scenario
- ➔ Setup
- ➔ Network Access & Setup
- ➔ Token of Participation
- ➔ Road to Finals
- ➔ Q&A
- ➔ Technical Info
- ➔ OSINT Briefing and RT strategizing by Marina Krotofil

Objectives of CISS 2025

1. **Develop capabilities** for defending critical infrastructure (CI) / cyber-physical systems (CPS) under cyber-attacks

2. **Validate and assess** the effectiveness of technologies developed by researchers & commercial entities with iTrust

3. **Understand composite** Tactics, Techniques and Procedures (TTPs) for enhanced Operation Security



Access to world's largest interconnected industrial-grade critical infrastructure playground

Details of the Finals

- **OSINT Drop:** 3 Sep
- **VM Submission**: 8 Sep (by 2359, GMT+8)
- **Network Familiarisation:** 16 – 24 Sep, 3 hr session/team
- **Finals Dates:** 29 Sep – 3 Oct
- **Results + Closing Address:** 7 Oct, 1600 hrs (GMT+8)
- **Prizes:**
  - 1st place - S$5,000
  - 2nd place - S$3,000
  - 3rd place - S$2,000

OSINT: Intel Drop

- Having been informed of the impending siege of the Mordor army, Minas Tirth's Cyber Centre is currently conducting reconnaissance.
- By **3 September**, they intend to release a dataset collected and the info they have found.
- This dataset will contain **network packet captures** and **historian data** for the different infrastructures.
- Link will be sent via email.
- You may do what you wish with this dataset and info.
- Marina will share more OSINT information after this briefing.

RT Kali@FUA

RT Form-up Area

- 8 Kali Linux (2025.2) with 8 CPU cores, 16GB RAM, sudo rights
  - 9.9.0.[10-17]/16
  - Internet access (est. 400 Mbps bandwidth)

- VPN Profile and credentials to connect to the FUA network
  - Will be sent to team lead thru email soon after you have booked your session
  - SSH or RDP to your Kali@FUA
  - VPN accounts are
    - Disabled by default
    - Enabled 15 mins before your session starts
    - Disabled 5 mins after your session expires

RT Requests

- If RT requires a custom VM, email cyberex@sutd.edu.sg the following:
  - Upload VMDK or OVA to Google Drive (OS Language: English)
  - Provide requirements (CPU, RAM, etc)
  - Ensure all necessary tools are installed
  - Provide credentials to configure NIC
  - Deadline: 8 Sep, 2359 (GMT+8)

- We will allocate the IP address for this VM.

RT Form-up Area

Scenario for Network Fam Session

CISS Finals 2025 theme of LOTR continues from Stage 1. This network familiarisation session is about scouting of Minas Tirith's infrastructures.

As the threat of Mordor's final assault looms ever closer, the Steward Denethor has commanded that the elite Red Guard defenders be granted unprecedented access to scout and familiarise themselves with the sacred infrastructure they will soon be called upon to protect. **In the week before the great siege, these ten Red Guard teams are permitted to access each system.** Under the watchful eyes of the Citadel's master engineers, the Red Guards must try to learn and unlearn.

The Red Guards have but three hours to absorb the wisdom of centuries, studying the defensive networks that have protected the White City since the days of its founding, preparing for the ultimate test that awaits when the Enemy's horns sound across the Pelennor Fields. No attacks on the infrastructure are allowed during this period.

Your task is to setup your machines and conduct forensics in a **3-hour slot** of your choice from **16 to 24 Sep.**

Details for Familiarization Session

- 1 x 3hr session per team between 16 to 24 Sep
  - 0900 - 1200 (GMT+8)
  - 1400 - 1700 (GMT+8)
- Book your session
  - APAC Teams requested to take morning slots
- Check VPN Connection to Kali Linux 2025.2 (SSH/RDP)
- Install necessary tools, if any
- Request support from us through (cyberex@sutd.edu.sg)
- Snapshots will be taken only for FUA VMs

RT Form-up Area

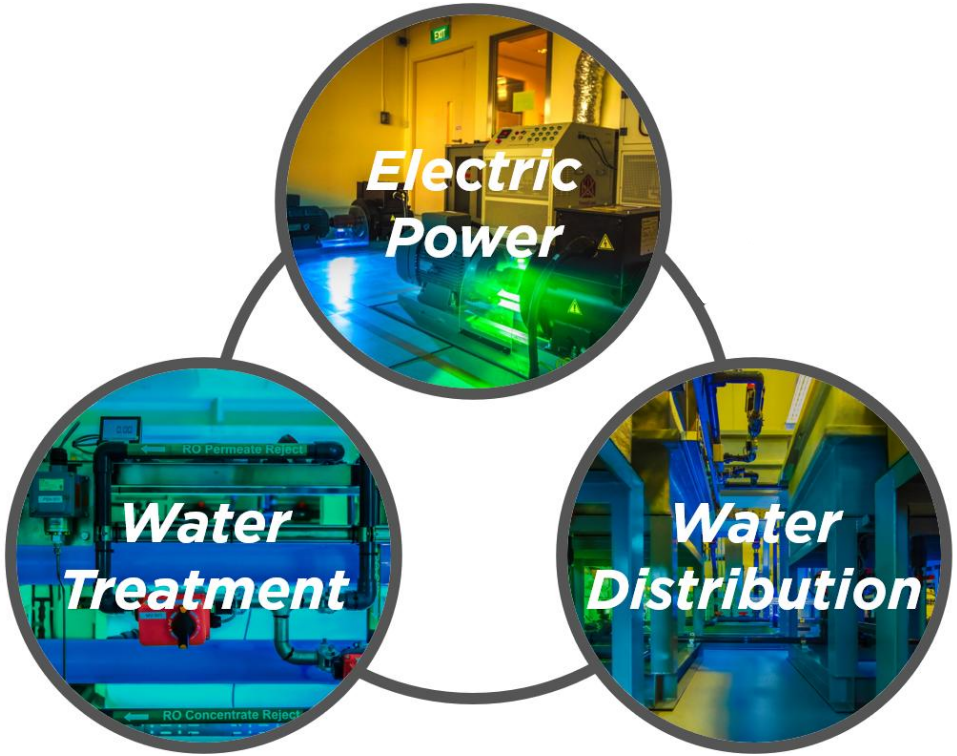
Scenario for Finals Execution

Preparing for the Siege of Minas Tirith –
The Final Defense
Having proven your worth as the ten most elite Red Guards in the preliminary trials, you now face the ultimate test as the forces of Mordor mass at the Pelennor Fields for the final assault on Minas Tirith.

The Enemy will be targeting all three critical infrastructure systems that sustain the White City's defences: the ancient Aqueduct of Mindolluin that provides life-giving waters, the water distribution network (The Fountains of Lebennin) that carries these waters throughout the seven levels, and the Luminous Spire that powers the city's mystical defences.

As the siege horns sound and darkness gathers, Denethor himself calls upon these elite Red Guards to conduct **the most crucial penetration testing of their careers - they are tasked with exposing and demonstrating vulnerabilities in Minas Tirith's infrastructure before the Enemy discovers them first.**

Exercise Platforms

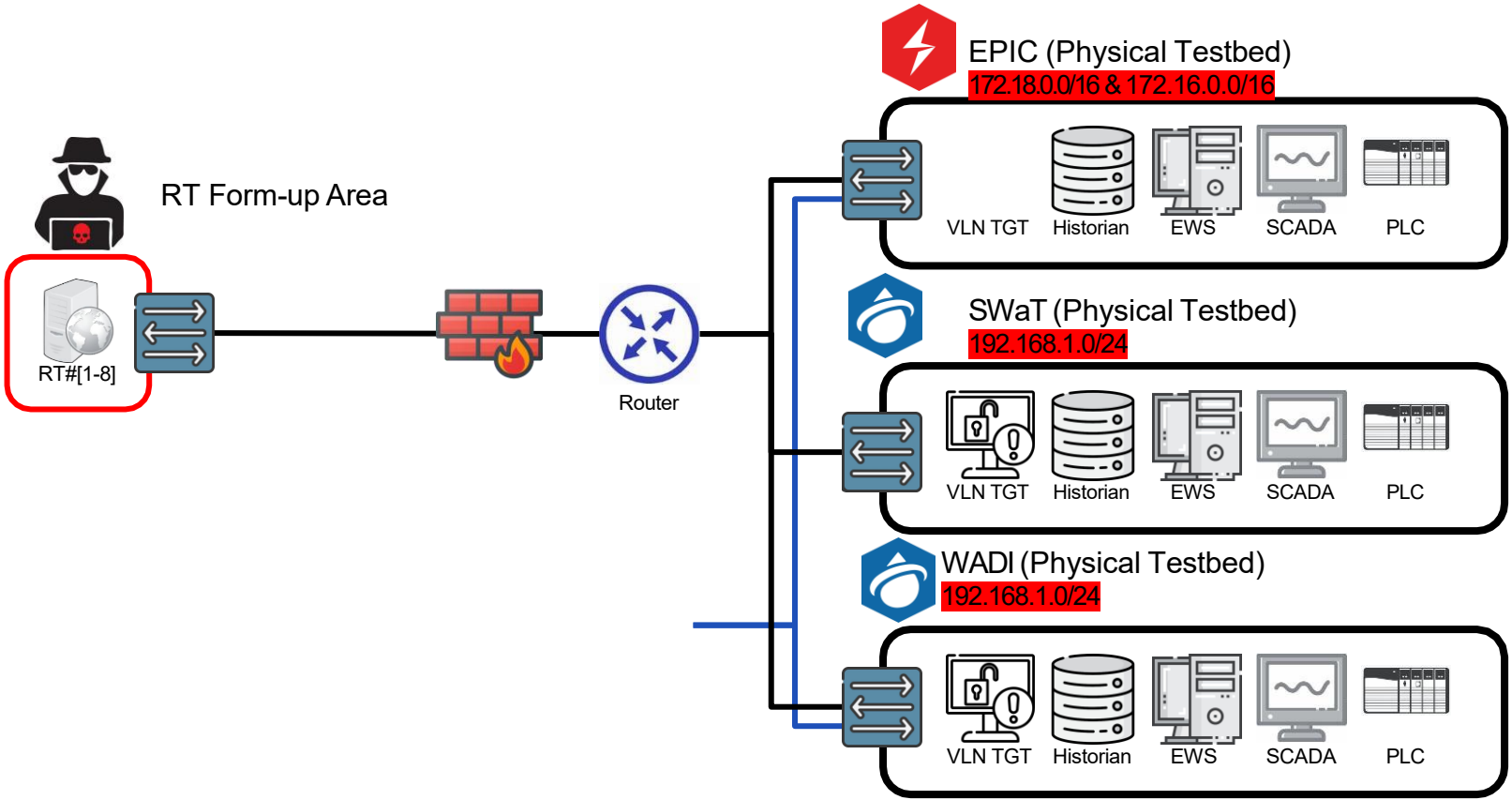


Details for Finals Session

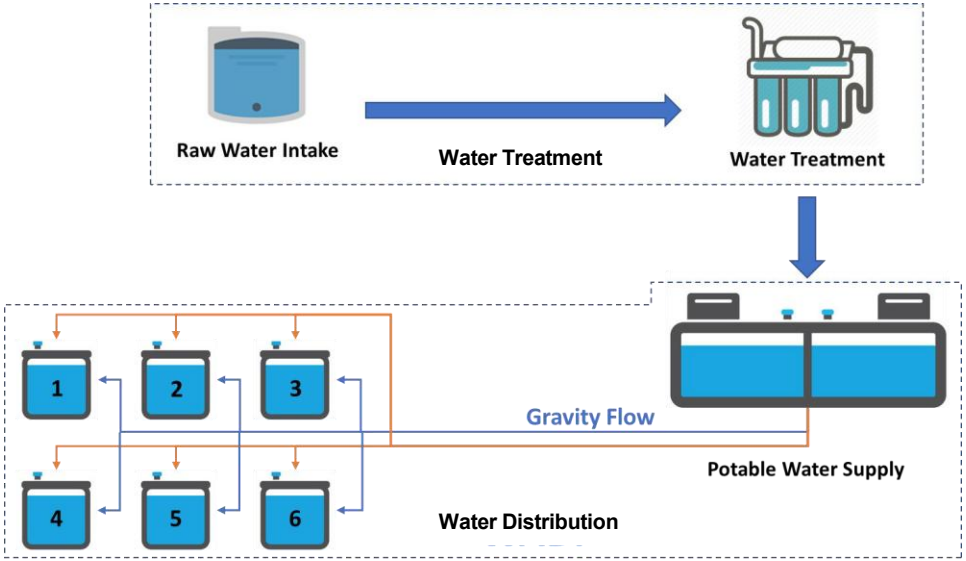
- 1 x 4hr session per team between 29 Sep to 3 Oct
  - 0900 - 1300 (GMT+8)
  - 1400 - 1800 (GMT+8)
- Book your session
  - APAC teams requested to take morning slots
- Complete as many objectives as possible.
- The attack objectives will be released on 9 September.
- 1 hour of power infrastructure exclusively, followed by 3 hours of access to all infrastructures

Technical Information

Network Architecture



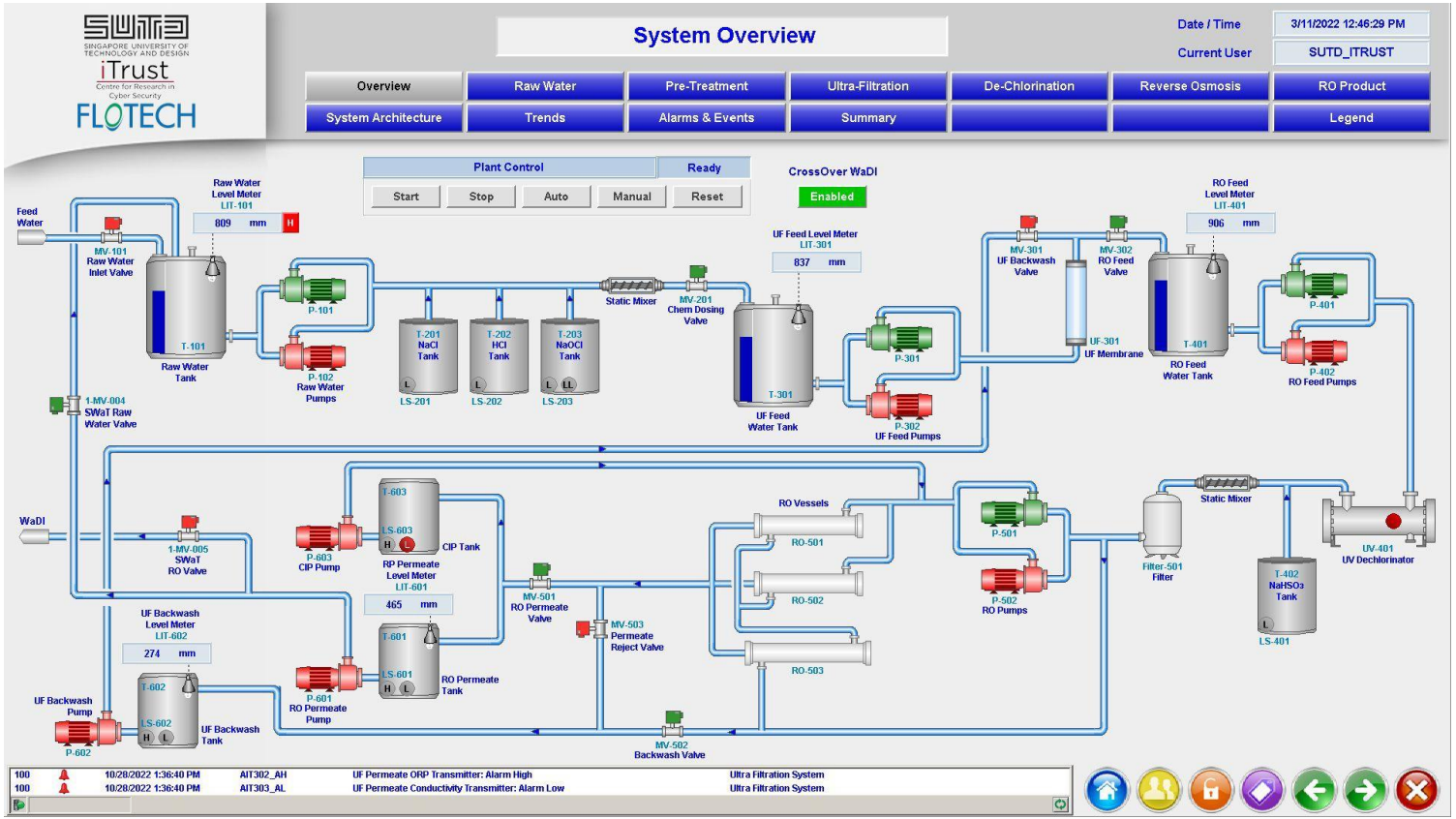
Water Network (Physical)



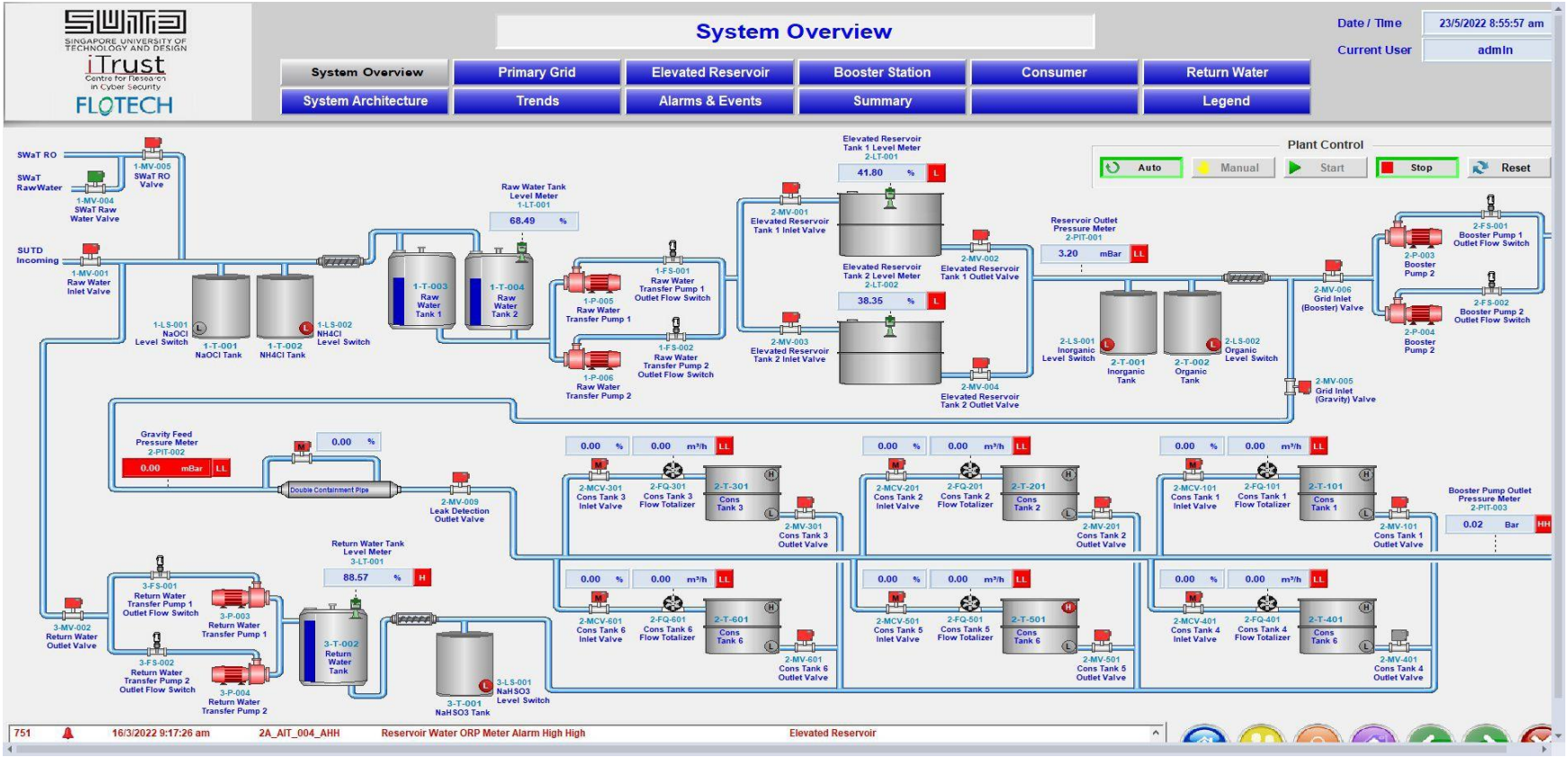
The White City has configured-

- **tanks 1 and 2** to supply water for cooling,
- **tank 3** for sanitation,
- **tank 4** for residential purposes,
- **tanks 5 and 6** for heavy-duty industrial use.

Water Treatment Process



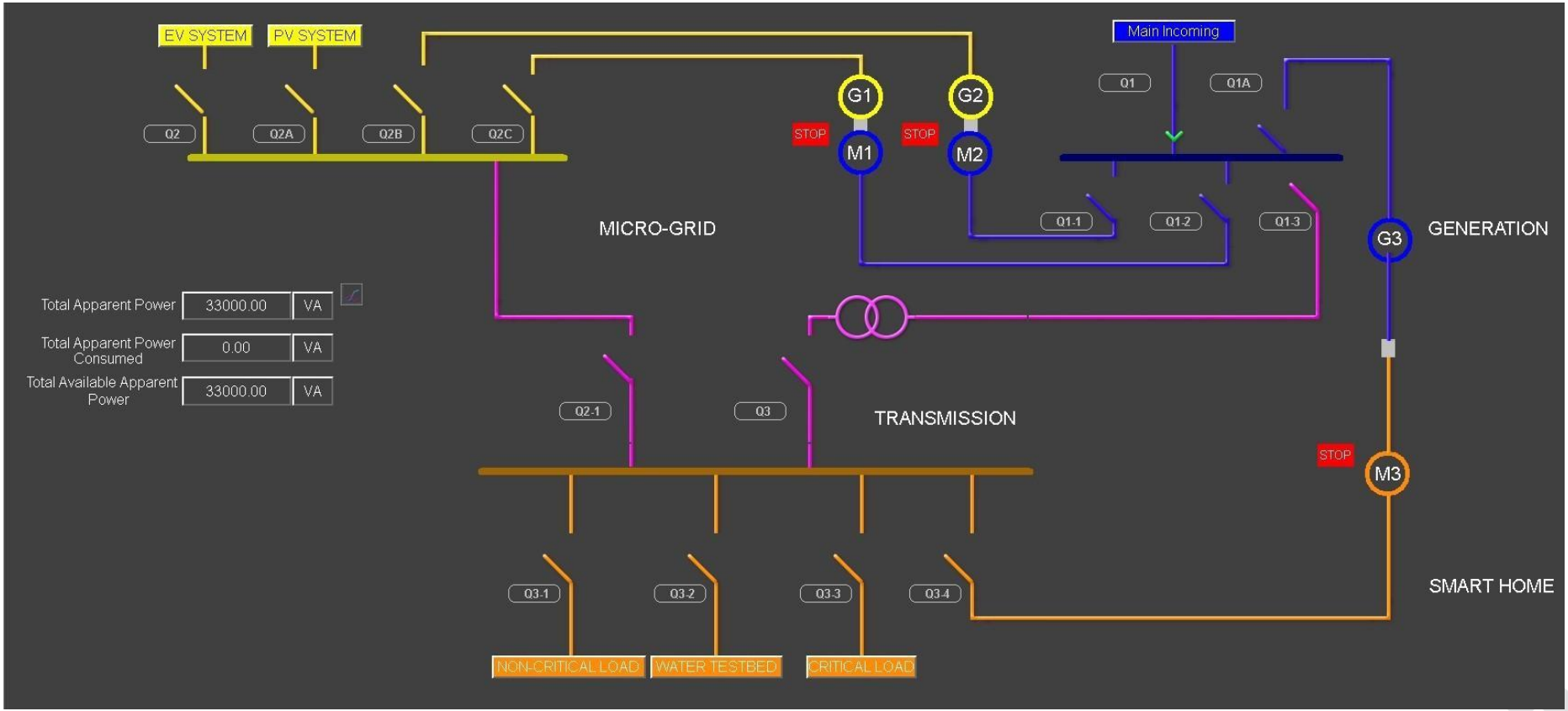
Water Distribution Process



Power Network (Physical)

1. The Power Grid has **two generators (G1, G2)** as its power sources.
2. **Electricity** is supplied to the **Critical Load**, **Non-Critical Load** and **Water Treatment & Distribution Network**.

Power Grid Process



Rules of Engagement

- 20 mins before your session
  - Dial in to MS Teams Rooms, link provided thru email
  - Connect to FUA using VPN credentials
- Communication and coordination between judge and RT will be via RT Lead
- All members are to share their screen during the session; **recording will be done** (for analysis purposes only; will not be published/shared without your permission)
- Clock starts when the Judge declares “Begin”: total 4 hours

Rules of Engagement

- Enumeration
  - No limit on the number of sessions for enumeration. Permission from judges is not required.
- Launch of Attack
  - Declare the attack objective you want to achieve and explain how the attack will be launched.
  - An attack is to be launched only after you receive a “Go-ahead” signal from the judge.
- Verification of attack objective
  - Teams are expected to verify their own attack

Scoring

Top 3 Winners

➔ Total Attack Objective Score

- Achieving an attack objective will be rewarded up to 400 points*, depending on their difficulty; sent on **9 September** via email.

Additional scoring-

➔ Most Stealthy and Undetectable

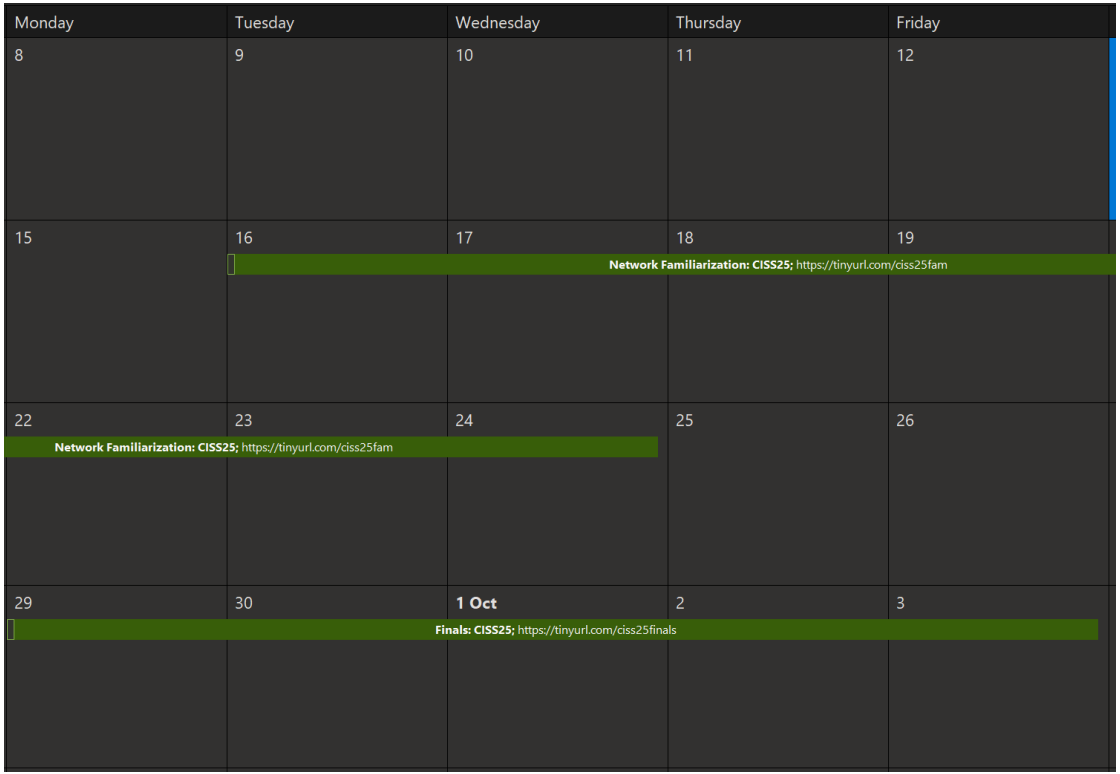
- Signature based IDS & Total packets generated

➔ Most Novel Attacks

- Novel, Storyline, Difficulty

Road to the Finals

SEPTEMBER



KEEP CALM AND CYBER EXERCISE

CISS 2025 Committee

Q&A

cyberex@sutd.edu.sg

OSINT Briefing by Marina Krotofil

Cyber-Physical Systems (CPS)

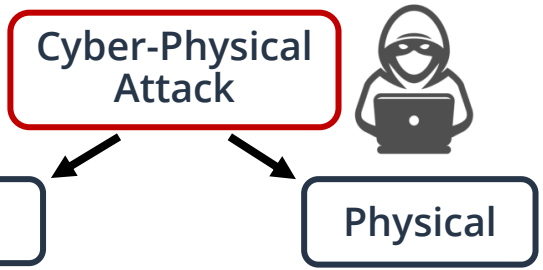
Cyber-Physical Systems

A system that relies on close interaction between digital and physical components, typically designed as a network of interacting elements with physical and digital inputs & outputs

Cyber-Physical Attacks

A digital malicious alteration of a cyber-physical system's operations to cause undesirable physical effects

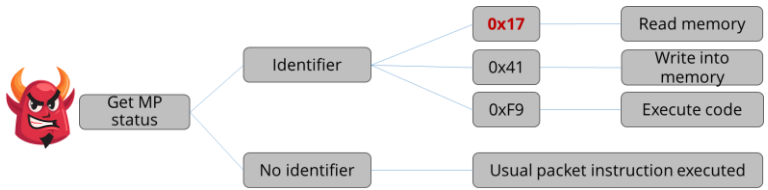
Cyber-Physical Attacks

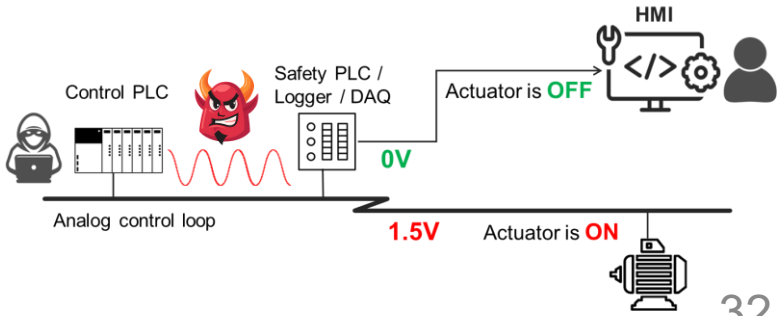


Compromising components of computing/ communication infrastructure

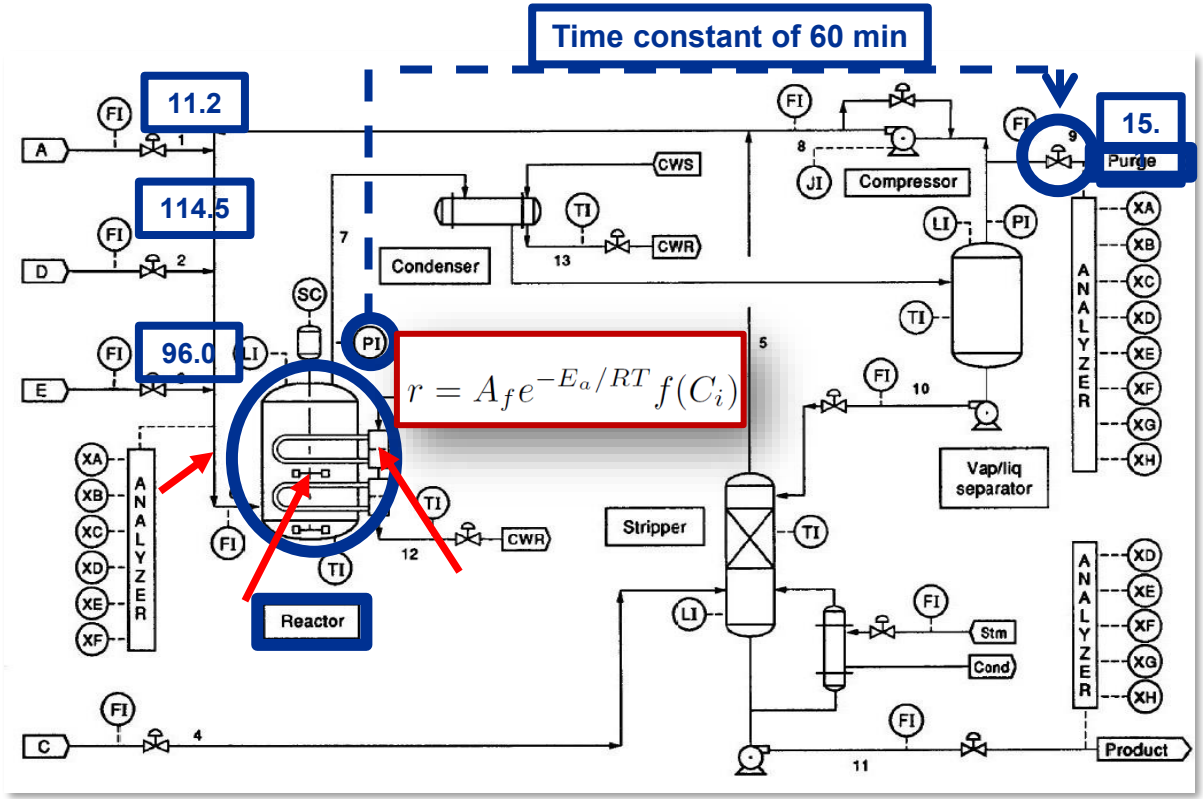
Engineering attack to cause physical impact on process, system or equipment

```
366     def ExplReadRam(self, address, size, mp=255):
367         if size > 1024 or size <= 0:
368             return None
369         else:
370             if ram_check(address, size) != 0:
371                 return None
372             return self.ExecuteExploit(23, struct.pack('<II', size, address))
```

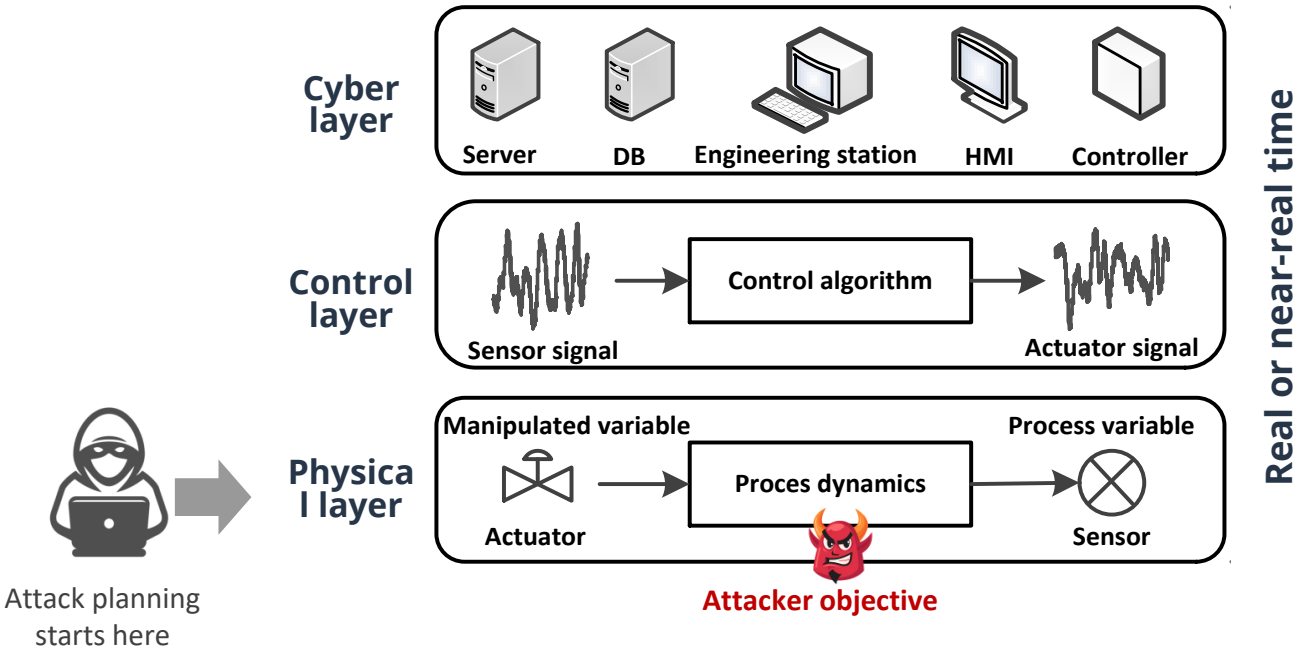




Physical Process Vulnerability

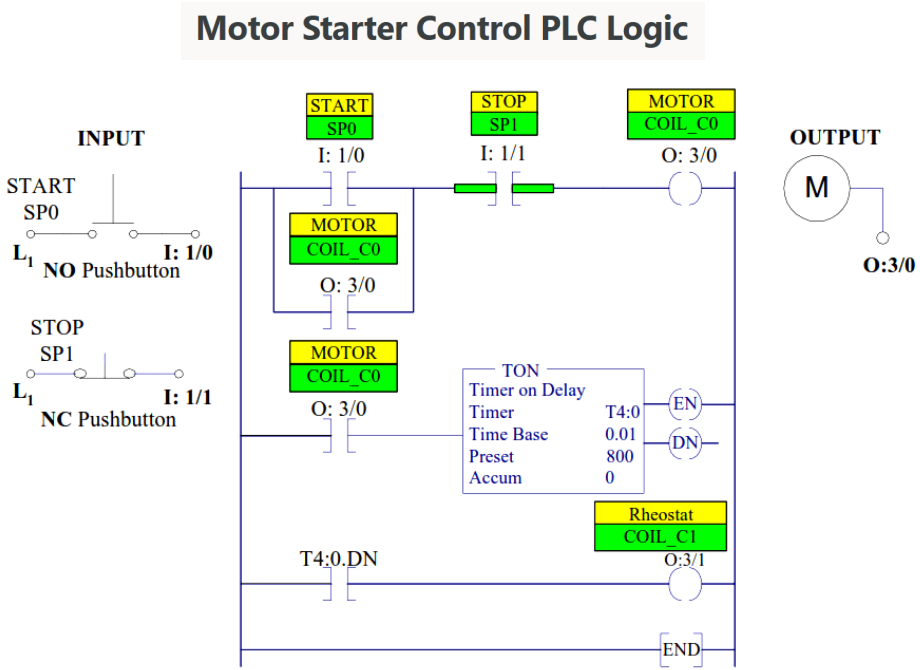


Layers of Cyber-Physical System



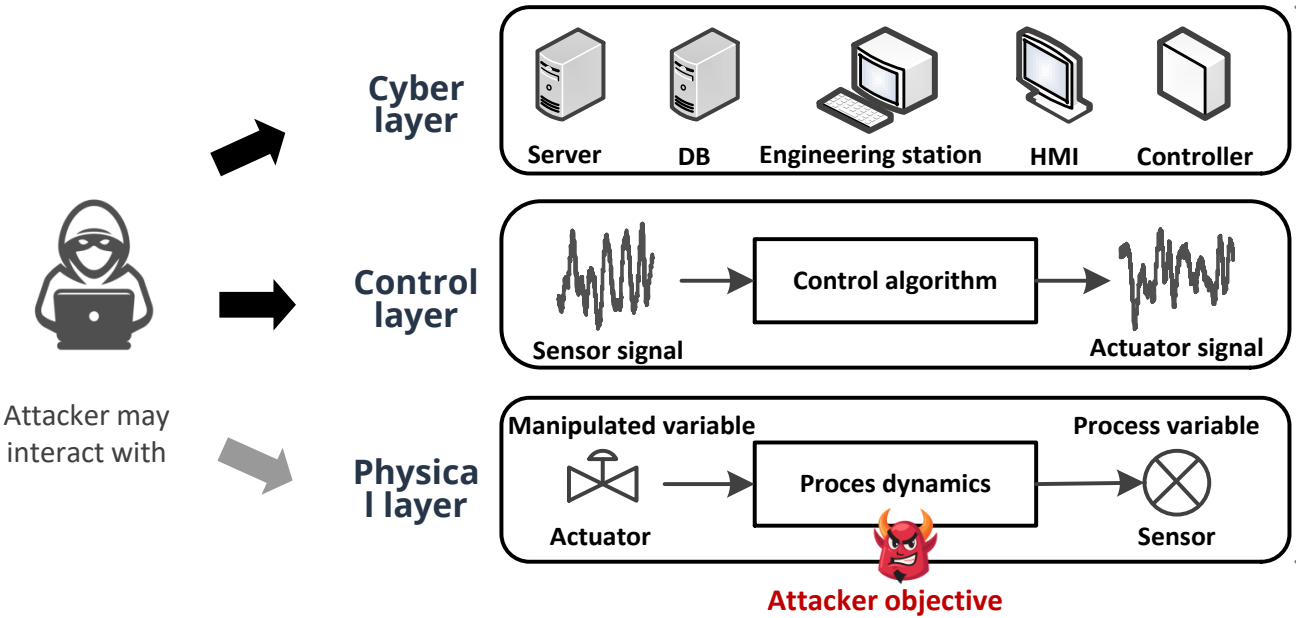
Control Logic

Control logic (also user program or project file) defines what operations should, when and under which conditions. It also contains so called interlocks that define mutually exclusive conditions to prevent undesired (harmful) states of the process.

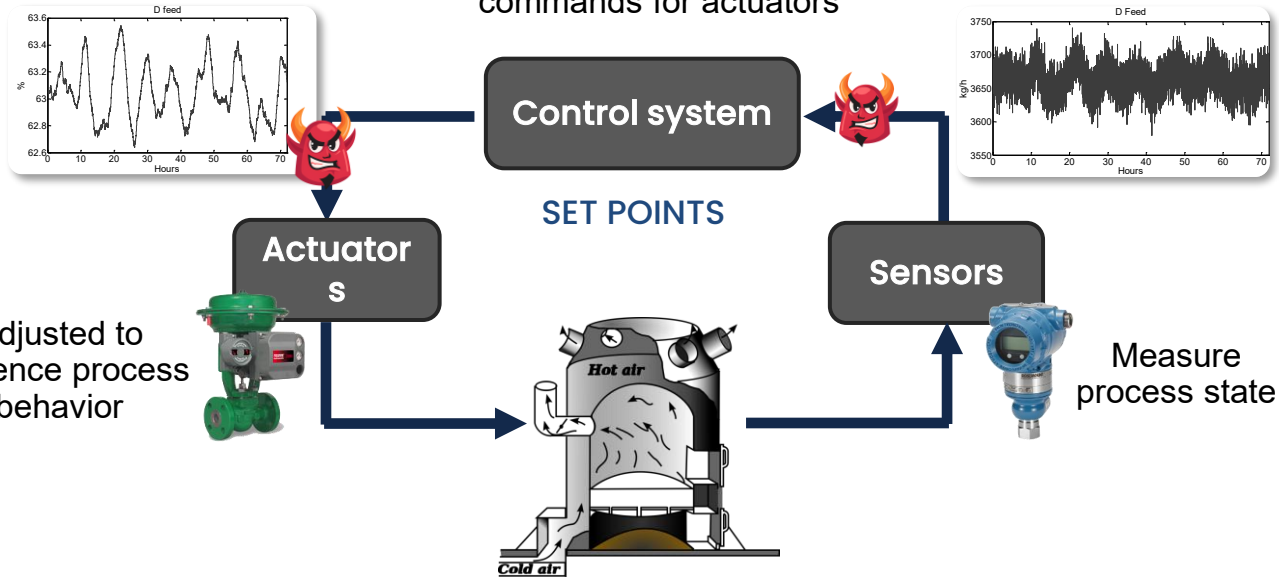


Motor Starter Control PLC Logic - Automation Community

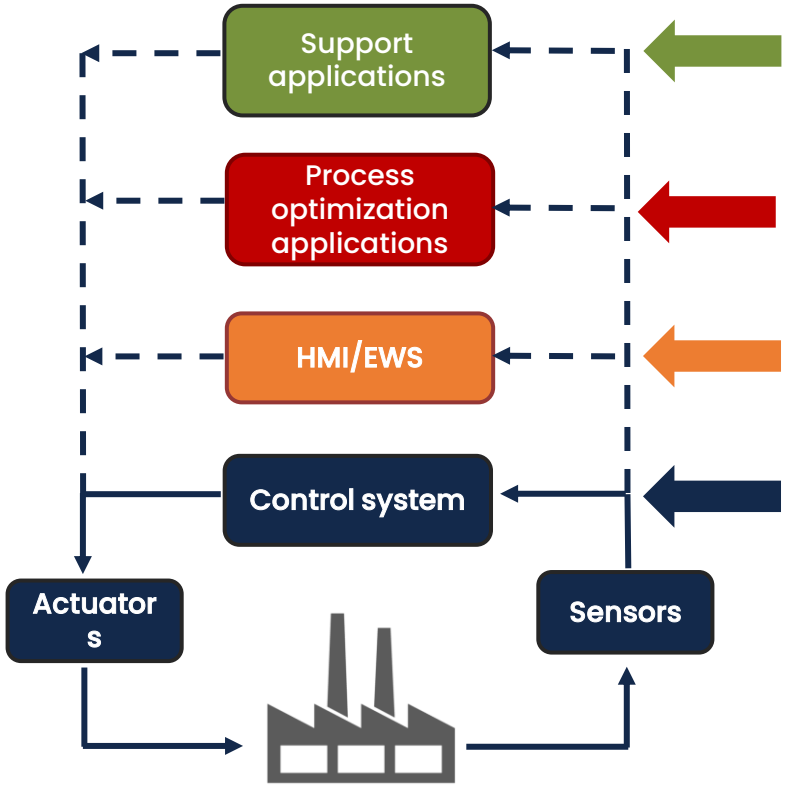
Layers of Cyber-Physical System



Control Loop as Fundamental Block



Hierarchical Control Loops



Indirect impact:
Work orders, logistics, billing, etc.

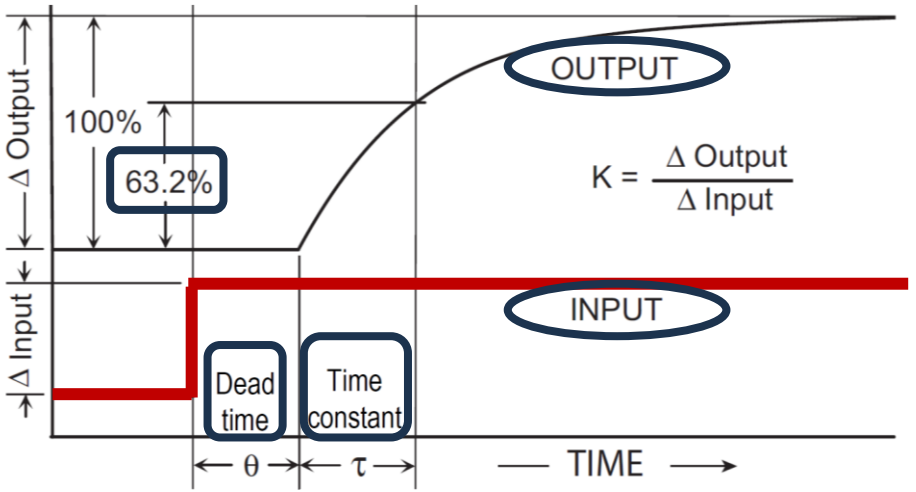
Degradation impact:
Causing process inefficiencies, etc.

High-fidelity impact:
Forcing point, manual control, safety bypass

Surgical impact:
Almost unrestricted, granular process control

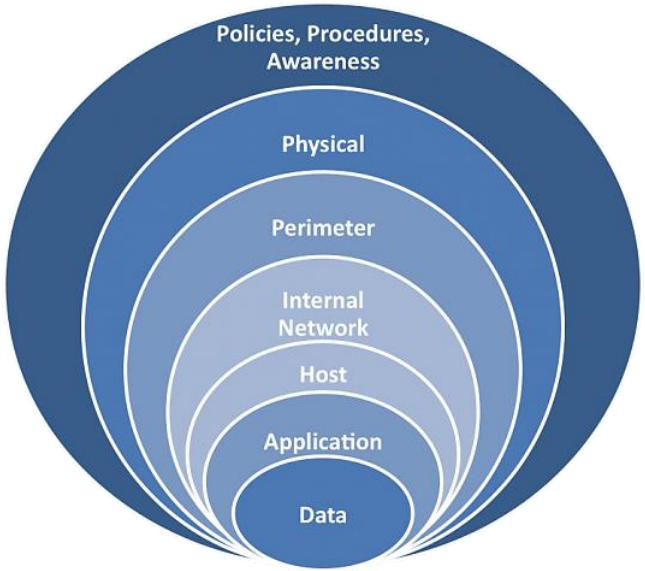
Control and Timing Parameters

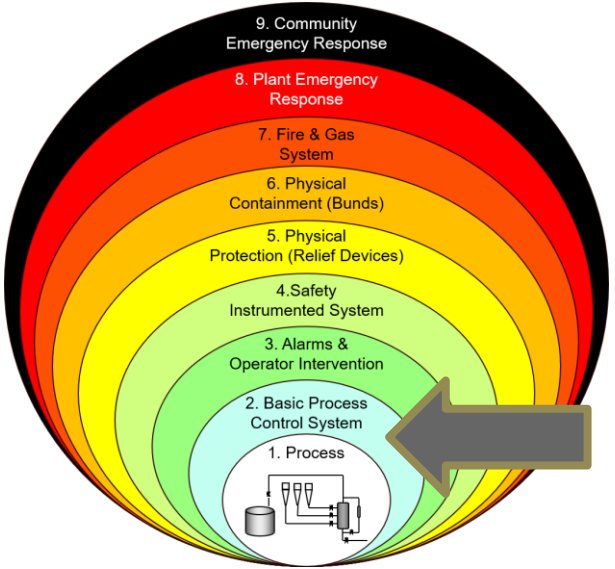
- **Dead time** is the delay from when a **controller output** (CO) signal is **issued** until when **its effect** is first **observed** in **process variable** (PV)
  - Caused by both various electronic components and process physics
- **Time constant** (lag) describes the speed with which the PV responds to the change in CO or disturbance. It is measured when PV reaches 63.2% of its total change
  - Smaller time constant means faster response (fast variables), larger one indicates slower response (slow variables)
- **Ratio** of **dead time** and **process lag** defines the difficulty of controlling the process
  - Dead time dominating variable is harder to control



IT vs. OT: Layers of Defense

Security





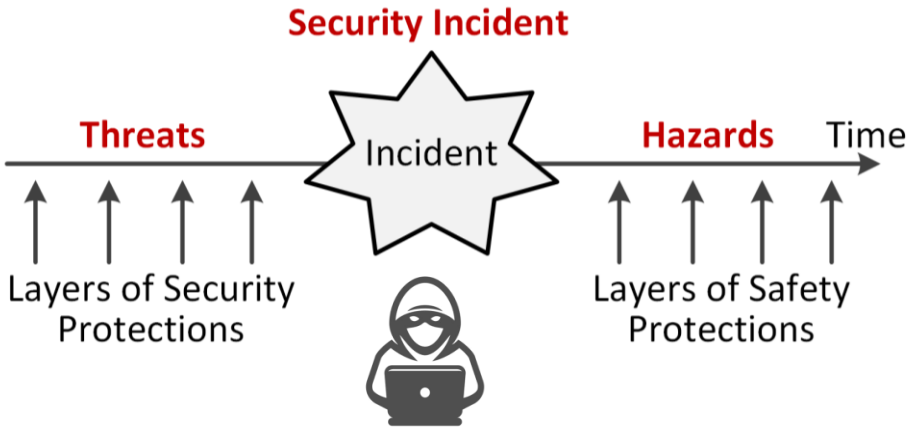
Safety

Security & Safety Relationship

Threats can be (always) traced back to humans and their will to perform an action

Desire of specific outcome

- **Hazards** are caused by the natural events (energy release/change – mechanical, chemical, electrical)
- Random events caused by physical conditions

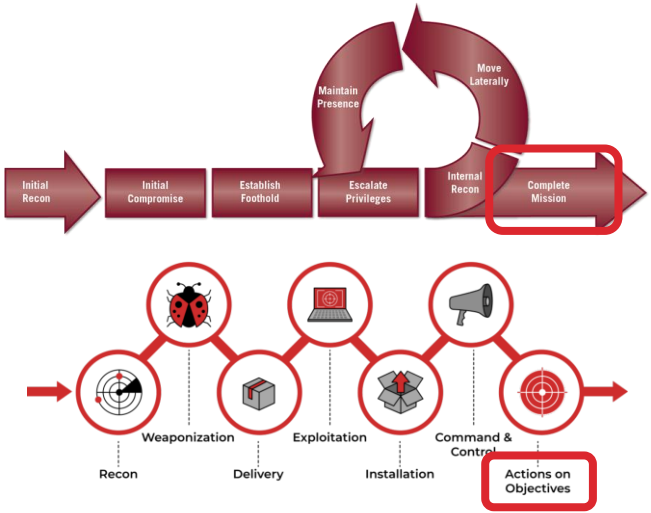


Key CPS Challenges

- Time-variant systems, often non-linear or with short time constants
- Tight coupling of control loops
- Managed by the Real-Time Operating Systems (RTOS)
- Physics cannot always be harnessed or/and defeated

Complex attacks are conceptualized with attack lifecycles/kill chains

Many Different Kill Chains*



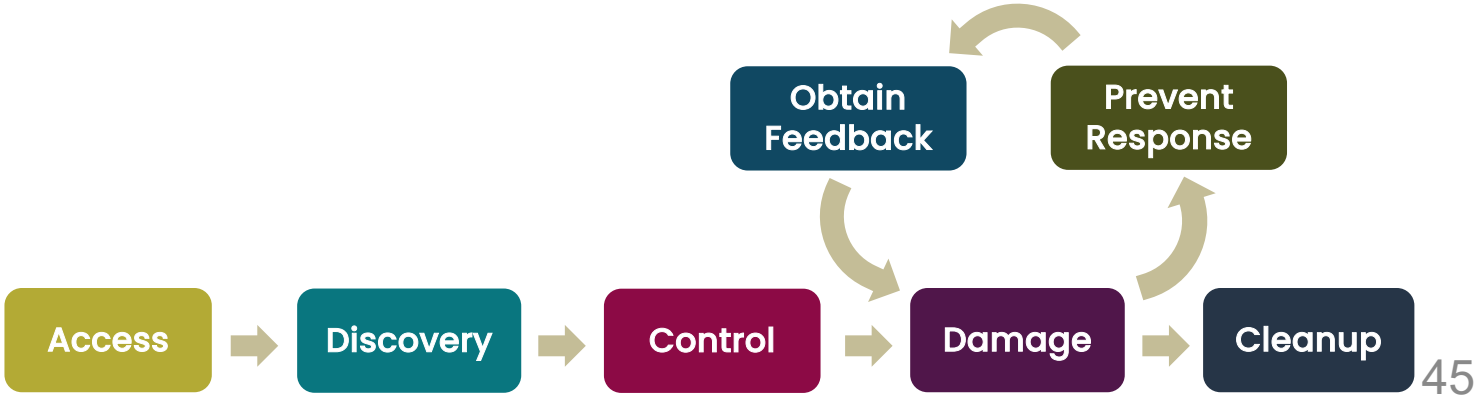
MITRE ATT&CK™

- Kill chain or attack lifecycle is a common method to describe the process of conducting cyberattacks
- Existing frameworks are IT-oriented or focused on "cyber" elements
- (Over)simplification of cyber-physical attack development and execution
- Does not address process-specificness/ engineering aspects of attack development
- Present attack execution as discrete & instant, instead of continuous & protracted
- **MITRE ATT&CK for ICS is applicable once the damage scenario is already constructed!**
  - Does not provide logical guidance on how the attacker would approach attack scenario design and payload development (nuanced, step-wise process)

** Mandiant, Lockheed, SANS ICS Stage 2, MITRE ICS ATT&CK*

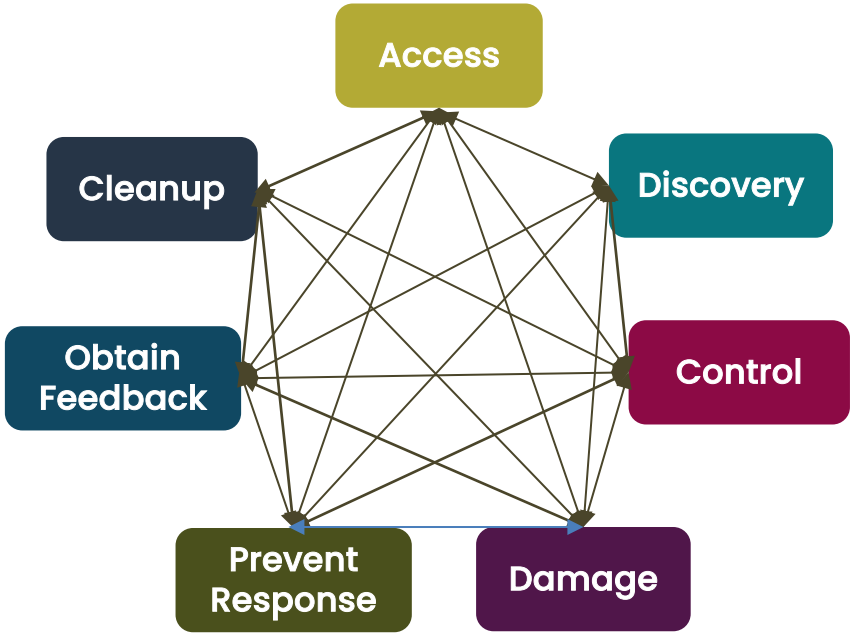
Cyber-Physical Attack Lifecycle

- Describes logical, step-wise process of constructing and executing a targeted cyber-physical attack
- Focused on the engineering aspects of cyber-physical exploitation process and constructing target payload
- The cyber elements are tailored to exploiting control system and physical process



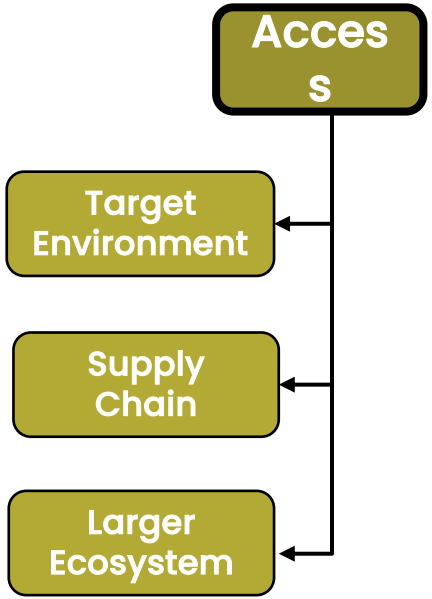
Step-Wise Process is not Always Linear

- Any exploitation process is messy and not strictly sequential
- The attacker may need to circle to the previous or even initial stage at any point
- The attacker may take pauses between attack stages and/or work on different stages in parallel
- Attack execution is a concatenation of attack activities and exploits across different stages



Access

- Refers to both methods of obtaining access and to what resources
  - **External** (entry points) and **internal** (assets) access
- Early identification of the assets of interest (information/ documentation, attack/code execution, jump/proxy host, attack monitoring, etc.)



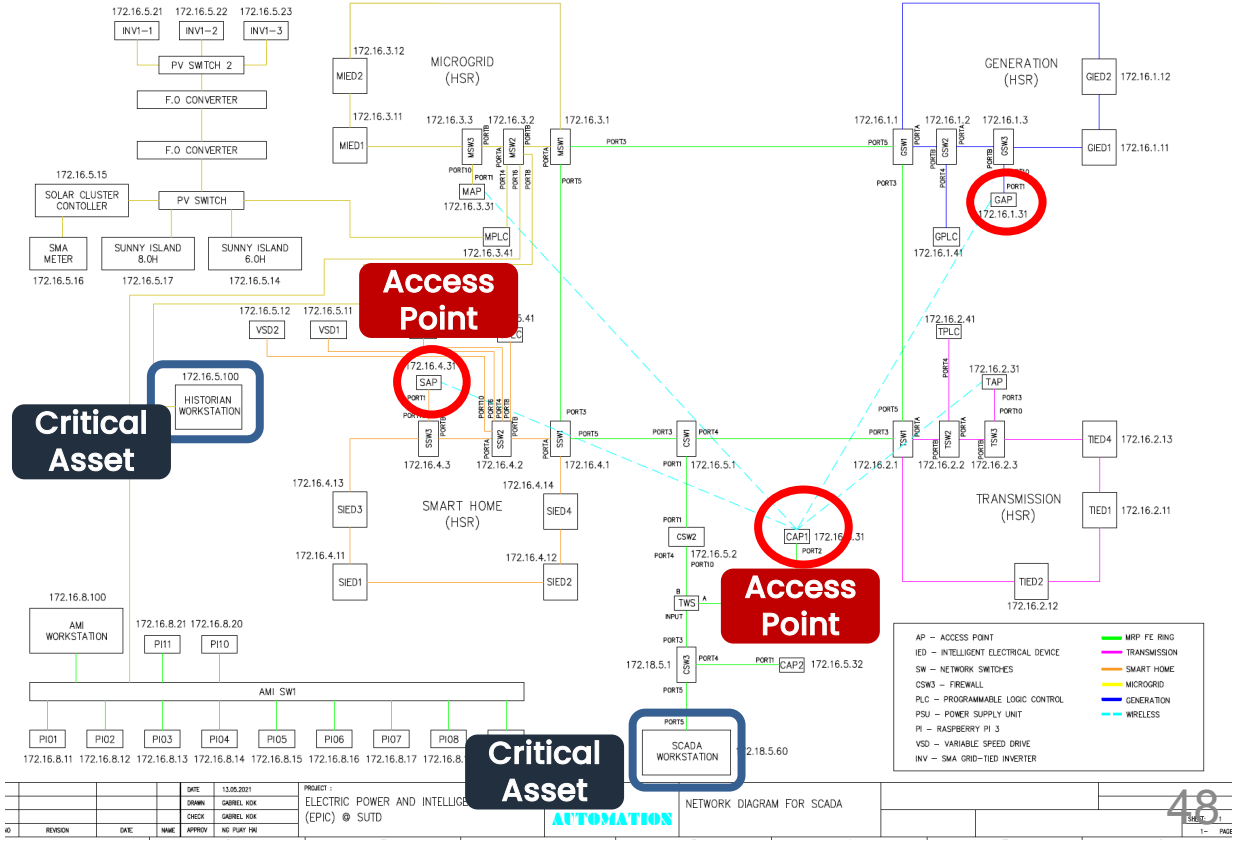
Guided by the following question:

- What kind of access and to which resources is needed for attack execution?

Preparation: Identify Access Points

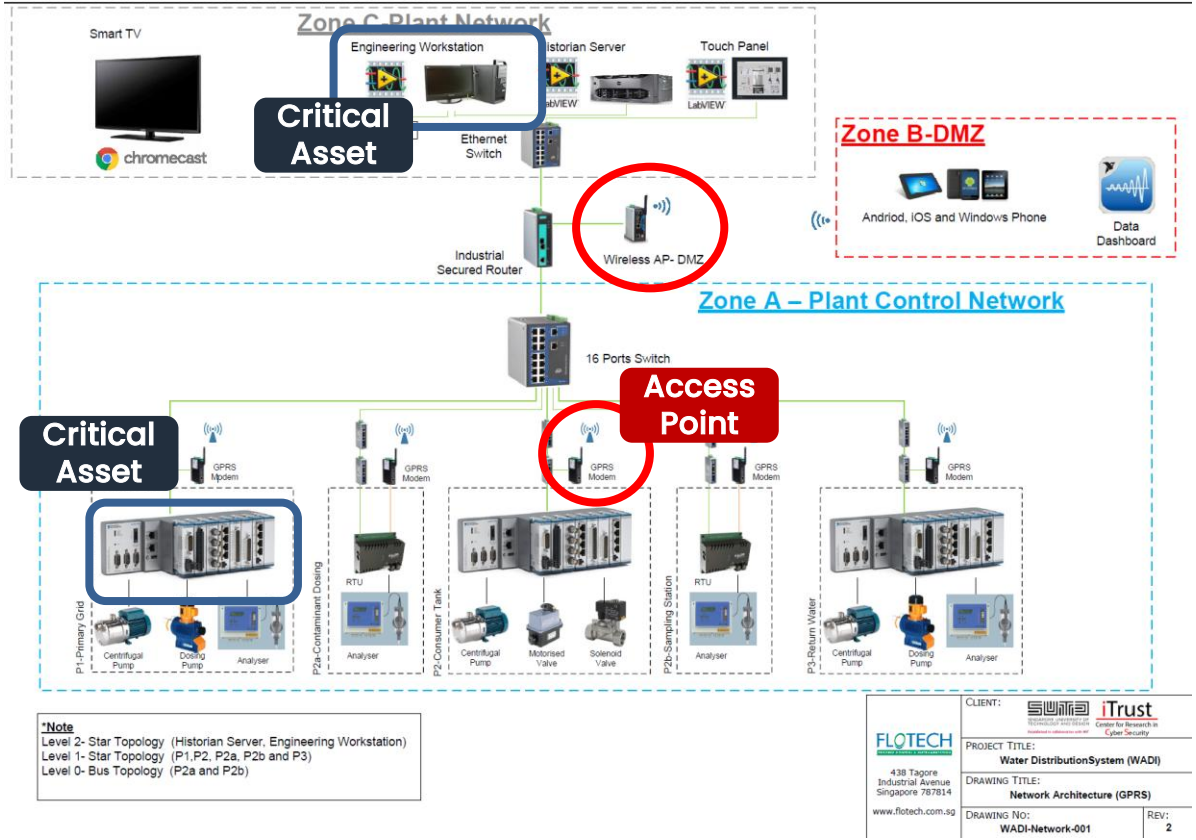
C. *Compromise through Wireless Network*

Following the first set of experiments on reconnaissance, further investigation was carried out on potential compromise by attacker B, an attacker within WiFi range of the plan control system. In particular, the SWaT testbed has the option to replace the wired Ethernet-based L1 network with a WiFi-based wireless solution. The alternate wireless network uses industrial access points (the MOXA AWK-5222-EU) to connect the devices, and employs the WPA2 security scheme with pre-shared keys. Assuming that the pre-shared key is strong enough to not be guessed outright, there are several options for the attacker: a) the attacker can try to perform a (cloud-based) brute force attack, b) the attacker can perform a well-known *evil twin attack*[11] to impersonate the legitimate AP, and trick the PLCs to connect to it instead. Suitable tools for both attacks exist, for example the Aircrack-Ng tool. The



Preparation

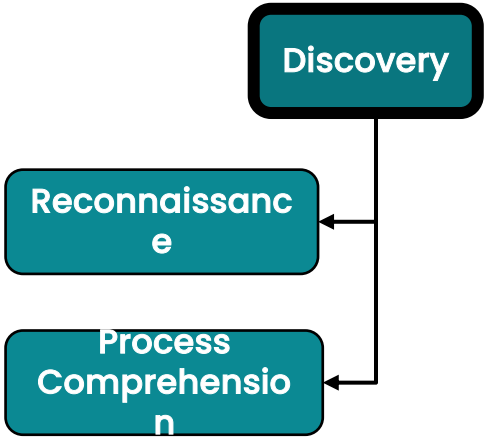
- Check diagrams for possible entry points*
- Pencil out potential assets of interest
- Collect relevant exploits and tool kits, review related research works, etc.



* Sometimes compromising specific access points is easier

Discovery

- ICS/OT are complex environments/systems, often unique and proprietary
- This stage is likely to be continuously executed during the entire operation
- Refers to discovery of the underlying computing and network infrastructure and target process (including control system)



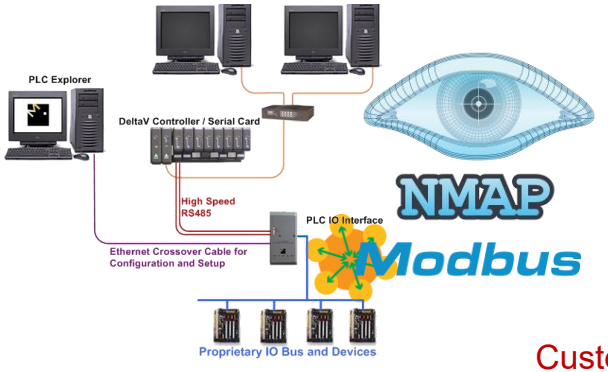
Guided by the following question:

What knowledge about target environment/system is needed to design, implement and execute a cyber-physical attack?

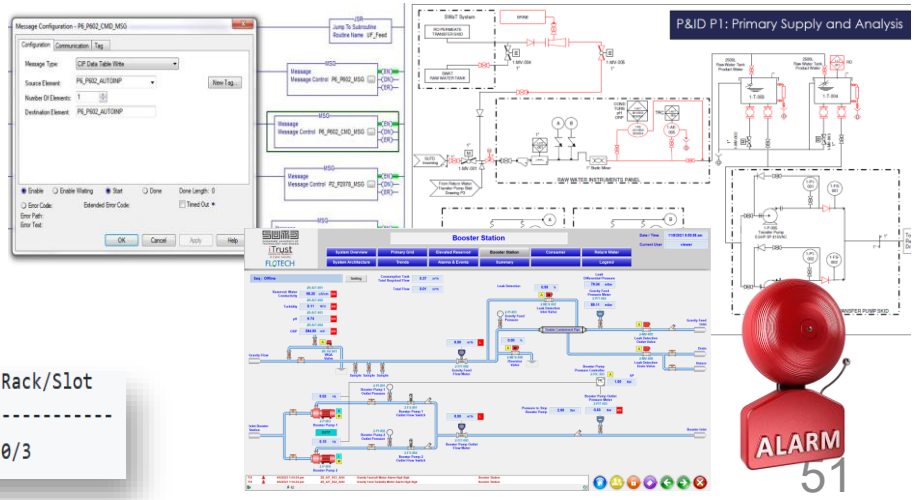
- Minimum and sufficient knowledge
- Static infrastructure process discovery

Discovery

Network/infra reconnaissance



Process comprehension

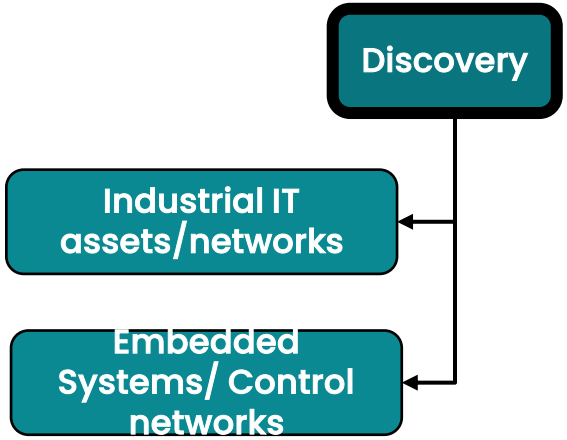


Custom scanners

Order Code	Module Type Name	Firmware Version	Module Name	Serial Number	Rack/Slot
6ES7 412-2EK06-0AB0	CPU 412-2 PN/DP	V 6.0.3		SVPF126xxxx	0/3

Reconnaissance

- Standard IT tools can be partially applicable
- nmap can help to identify certain specialized assets (HMI panels, PLCs, etc.) but provide only minimal asset information
- Wireshark supports only limited number of industrial protocols
- Need for specialized recon tools/approaches



Siemens HMI Panel

```
PORT     STATE SERVICE        VERSION
102/tcp  open  iso-tsap?
5001/tcp open  commplex-link?
5002/tcp open  rfe?
5900/tcp open  vnc            VNC (protocol 3.8)
```

nmap output for HMI panel (not very helpful)

Reconnaissance

- Reconnaissance of non-IT assets may require specialized/custom device and vulnerability scanners
- Some open-source tools exist:
  - PLCs scanners (various vendors)
  - PLC password databases
  - Modbus Unit ID enumerators
  - Vulnerability scanners for RTOS, protocol stacks, etc.
  - Open-source parsers/dissectors for exotic protocols
- Attackers may write own port scanners (Industroyer, Triton)
- Challenge: A huge diversity of proprietary devices and protocols
  - Network diagrams and engineering drawings are essential

Safe Active Scanning for Energy Delivery Systems Final Report

https://www.osti.gov/servlets/purl/1409972

Siemens PLC

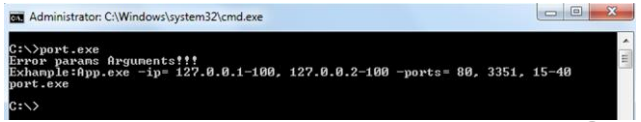
```
127.0.0.1:102 S7comm (src_tsap=0x100, dst_tsap=0x102)
   Module                : 6ES7 151-8AB01-0AB0  v.0.2
   Basic Hardware        : 6ES7 151-8AB01-0AB0  v.0.2
   Basic Firmware        :                      v.3.2.6
   Unknown (129)         : Boot Loader           A
   Name of the PLC       : SIMATIC 300(xxxxxxxxx)
   Name of the module    : IM151-8 PN/DP CPU
   Plant identification  :
   Copyright             : Original Siemens Equipment
   Serial number of module : S C-BOUVxxxxxxxx
   Module type name      : IM151-8 PN/DP CPU
```

```
PORT     STATE SERVICE
6626/tcp open  wago-service
| Wago Scan:
|   Device: WAGO 750-8202 PFC200 2ETH RS
|   Hardware_Version: 06
|   Serial_Number: X
|   Software_Version: 02.08.24(11)
|   Firmware_Loader_Version: 2014.11.0-w02.02.03 IDX 4
|   Baud: 100MBaud
|   Firmware_Burn_Date: 0000
|_  OS_String: 0000
MAC Address: 00:30:DE:42:AD:53 (Wago Kontakttechnik GmbH)
```

```
PORT STATE SERVICE 48899/udp open|filtered unknown | Beckhoff | Dissector: | Discovery_Analysis: |
| Hostname: BBECK9023 |
| AMS_NetID: 5.15.101.188.1.1 |
| Operating_System: Windows CE 6 |
| Twincat_Version: 3.1.4024 |
| Fingerprint: dd2326d2306dda4338c0205f14e27159ed9191ad603a7a5e827efc468a1f6076 | Devices: | Devices: |
CX5020: 70.00% | CX9020: 80.00% | Details: | SNMP: Enabled | NAT-t-IKE: Enabled | Webserver: Enabled | Telnet:
Disabled | CE Remote Display: Enabled | IPC Diagnostics: Disabled | ADS: Enabled | SSDP: Enabled | ISAKMP: Enabled |
Best_Match: |_ CX9020 with a score of 80.00% MAC Address: 00:01:05:0F:65:BC (Beckhoff Automation GmbH)
```

WIN32/INDUSTROYER

Additional tools: port scanner tool



Some Open-Source Offensive Tools

GitHub - hslatman/awesome-industrial-cohttps://github.com/hslatman/awesome-industrial-control-system-securityntrol-system-security: A curated list of resources related to Industrial Control System (ICS) security.

File modbus-discove

Script types: portrule
Categories: discovery, intrusive
Download: https://svn.nmap.org

S7 Password Offline Bruteforce Tool

CYBERSECURITY ADVISORY

APT Cyber Tools Targeting ICS/SCADA Devices

Last Revised: May 25, 2022 Alert Code: AA

Modbus Version Scanner
Disclosed: November 01, 2011

Beckhoff TwinCAT SCADA PLC 2.11.0.2004 DoS
Disclosed: September 13, 2011

TeeChart Professional ActiveX Control Trusted Integer D
Disclosed: August 11, 2011

RealWin SCADA Server DATAC Login Buffer
Disclosed: March 21, 2011

PLCinject

Brought to you by www.SCADACS.org.

MODULE

Industrial Security Exploitation Framework


```
28:63:36:9c:83:10 | agent-1215xatwoxalinkba57 | S7-1200          | 192.168.
1.11    | 002a
        b:0d:87:0b:9e | zhaotong          | SIMATIC-PC       | 192.168.0.118
          002a
        0:4c:68:22:1c | xxxx-pc           | SIMATIC-PC       | 8.8.1.231
                        cxb1d0ed          | S7-1200          | 192.168.1.17
                        151-3pn           | IM151-3          | 0.0.0.0
                        n-f51ldo7jhra     | SIMATIC-PC       | 192.168.1.123
```

SCADA Default Password (SDPD)

CRITIFENCE® CRITICAL INFRASTRUCTURE, SCADA, ICS AND IIOT DEFAULT PASSWORD DATABASE

WinCC Harvester

ClearEnergy | UMASploit v1.0.1

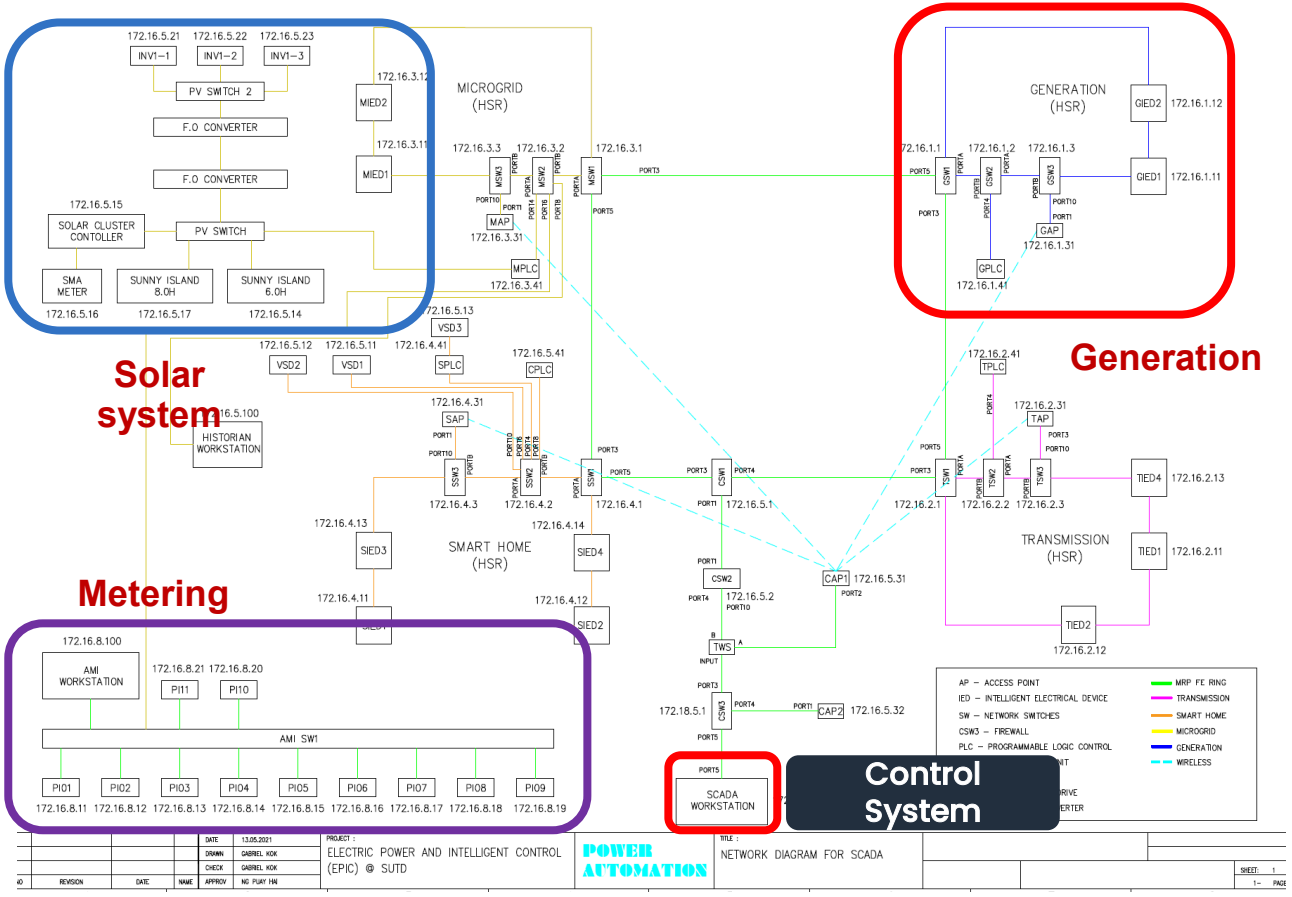

```
 ____ ____ ____ ____ ____ _    ____ ____ ____
|_  _/ ___|/ ___/ ___|  _ \| |  / __ \_  _|__  __|
  | || |   | (__| (___| |_) | | |  | | | || |  | |
  | || |    \___ \\___ \  __/| | |  | | | || |  | |
 _| || |___ ___) |__) | |   | | |__| |_| || |_ | |
|____\____|____/____/|_|   |_|\____/\___/____||_|
```

ICS Exploitation Framework

Modbus Unit ID and Station ID Enumerator

Preparation: High-Level Discovery

- Know relevant “crown jewels” assets (e.g., HMI, EWS, SCADA server, PLC/RTU/IED, OPC server, historian, etc.)



Sunny Island (SMA)

Sunny Island 4.4M /
6.0H / 8.0H

ResearchGate
https://www.researchgate.net › figure › a-Sunny-Island-...

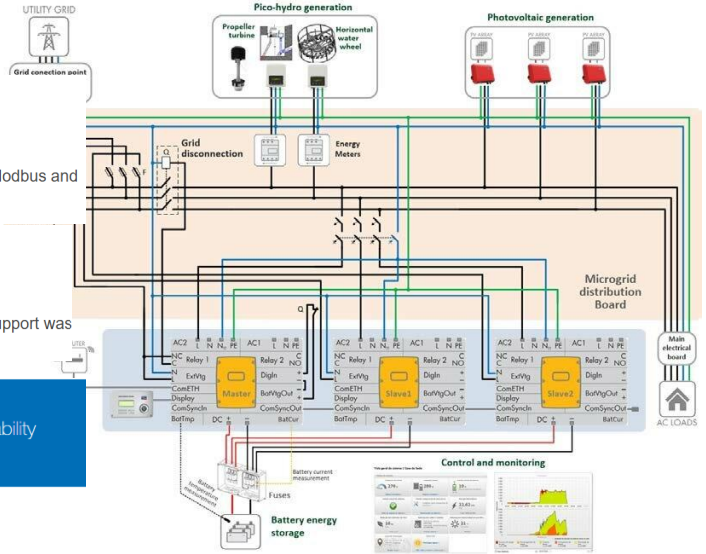
(a) Sunny Island 5048 battery inverter and (b) FLA ...

...vulnerability to cyber-attacks in accordance with the IEC61850 standard, including Modbus and TCP/IP standards for connecting with SCADA systems. Paper [12] ...

GitHub
https://github.com › SMAVenusDriver › blob › README

SMAVenusDriver/README.md at master

The **Sunny Island** was originally designed to use Lead Acid batteries, only. Lithium-ion support was added as a firmware update and does not contain any BMS logic ...



DIY Solar Power Forum

DIY Solar Power Forum
https://diysolarforum.com › threads › sma-webbox-vul...

SMA WebBox vulnerabilities

19 Jun 2021 — Web Box was able to see parameters inside **Sunny Island** as well. This being a GUI, there is some HTML language communication, a character string ...

2025-01-27 14:00 (CET)
SMA: Cluster Controller CSRF vulnerability

ID	VDE-2024-020
Published	2025-01-27 14:00 (CET)
Last update	2025-01-27 09:44 (CET)
Vendor(s)	SMA Solar Technology AG

The devices in the system come with the following default passwords:

"User": 0000

"Installer": 1111.

SUN:DOWN
Destabilizing the Grid via Orchestrated Exploitation of Solar Power Systems
March 27, 2025

Operating manual
SUNNY ISLAND 4.4M / 6.0H / 8.0H

Operating manual - SUNNY

SUN:DOWN Vulnerability

Preparation: Reconnaissance

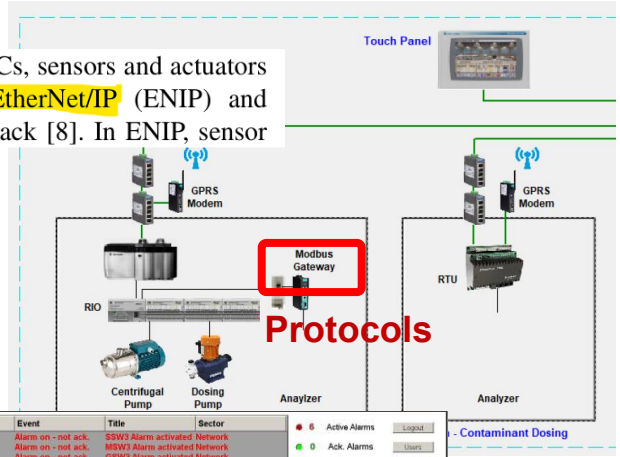
No.	Item Designation	Brand	Model Number
1	Smart Meters	Wasion	DTZ341 aMeter300
2	Reyrolle Relays	Siemens	7SR1205-2JA87-1CA0/EE
3	Earth Leakage Relay	MH	EL10
4	Circuit Breaker	ABB	DS SACE Tmax XT
5	Access Point	Hirschman	BAT-R
6	Firewall		EAGLE 30
7	Network Switches		RSL
8	16 Channel Digital Input Module	WAGO	750-1405
9	16 Channel Digital Output Module		750-1504
10	PLC-Controller w 24v input module		750-8202/025-001
11	End Module		750-600
12	Power Supply		787-1622
13	Serial Interface		750-652
14	AET Auto-Transformer	AET	VR105KVA-400V-5-4W/FS-1
15	Batteries Inverters	SMA Solar Technology	S18.0H-11
16	Battery Inverters		S16.0H-11
17	SMA Cluster Controller		CLCON-10
18	SMA Remote Controller		SRC-20

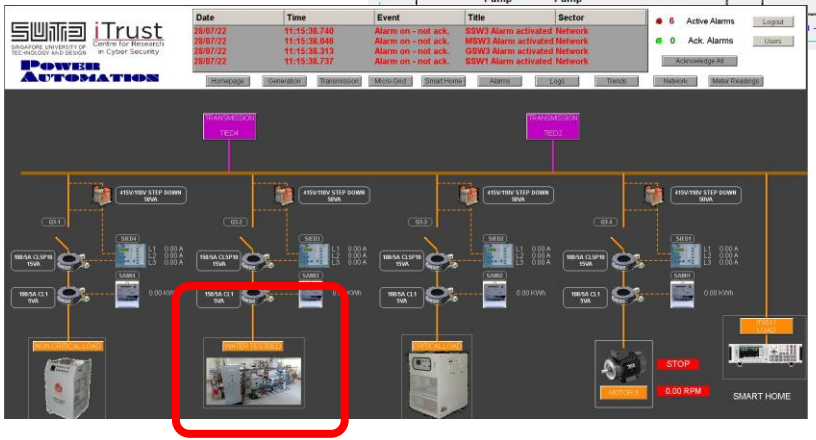
Asset inventory*

*It is always a good idea to assume that the documentation is incomplete or not entirely accurate

All network communication by PLCs, sensors and actuators in SWaT is using the industrial EtherNet/IP (ENIP) and Common Industrial Protocol (CIP) stack [8]. In ENIP, sensor

Protocols





Interdependancies

Preparation: Reconnaissance

B. System Reconnaissance

The experimental reconnaissance attack assumed the presence of an attacker A, that has access to the L1 plant network. We used a standard laptop with wired and wireless network interfaces, with open source networking tools such as Wireshark and Zenmap. With that setup, we were able to quickly map the local networking setup, and determine the available services on the hosts. We discovered a range of web interfaces on the local PLCs and networking devices. In particular, devices such as PLCs provide an informative web interface with a summary of their configuration and setup. In addition, the local HMI device (AB PanelView Plus Terminal) is running an embedded Windows OS, an FTP server that allows anonymous login, and a remote desktop protocol (RDP) server. Anonymous FTP login enabled the discovery of *hidden* files that appear to contain the complete HMI configuration in a proprietary format (Composite Document File V2).

As all PLCs, the HMI and the SCADA system are within the same Link-layer broadcast domain, it was possible to launch ARP spoofing attacks using Ettercap [3]. For more details on that attack, refer to [1]. As a result of the attack, the attacker is able to arbitrarily re-direct local traffic through his machine, and eavesdrop or manipulate the content. We found that the industrial protocol used, ENIP, does not feature any authentication or encryption in our testbed. Protocol analyzers such as Wireshark are able to decode ENIP to some degree, so that exchanged data can be extracted. We are currently also working on extensions for the Scapy tool, to enable automated processing and generation of ENIP traffic.

Preparation: Reconnaissance

3. Attacking Fieldbus Communications in SWaT

Based on the details we provided on SWaT, its fieldbus topologies, and the EtherNet/IP protocol, we now show results of practical MitM attacks. We start by introducing tools we used, and among them our custom *SWaT Assault* tool.

3.1. Tools

We used several tools to launch attacks against the fieldbus communications at the SWaT testbed:

SWaT Assault We developed a command-line interpreter (CLI) application which includes a library of attack modules capable of launching diverse spoofing and bad-data-injection attacks against the sensor and actuator signals of the SWaT testbed. The attack modules can be loaded, configured, and run independently of each other, allowing the attack of sensors and actuators separately. Attack modules also can be orchestrated and assembled in teams in order to force more complex behaviors over the physical process, while maintaining a normal operational profile on the HMI. SWaT Assault consists of 439 lines of Python [3] 2.7 code and its only external dependencies are Scapy and NetFilterQueue.

Scapy Making use of the Scapy[4] packet manipulation program we developed a new protocol parser for the Rockwell Automation proprietary message protocol used for signal communication between the RIO and the PLC, and for the EtherNet/IP Common Packet Format wrapper that encapsulates it. This parser (which we chose to call SWaT message parser) is specific for the SWaT's deployment (the SWaT Ring implementation makes use of User Datagram Protocol (UDP) for the transport of EtherNet/IP I/O implicit messages among ring devices) and its implementation follows SWaT's Control Panels and Electrical Drawings manual. Scapy was also used to sniff sensor readings from the EtherNet/IP Ring and to inject manipulated data on both, sensor readings and actuation commands. Our tool also automatically recomputes the data integrity checksums used by the Transport Layer protocol to match the false-data injection attack values.

NetFilterQueue In order to avoid duplication of packets and/or race conditions between original and injected packets, we employed the NetFilterQueue [2] Python bindings for libnetfilter_queue to redirect all the EtherNet/IP I/O messages between PLC and RIO to a handling queue defined on the *mangle* table of the Linux firewall *iptables*. The queued packets are later modified using Scapy and the previously mentioned SWaT message parser, and finally released to reach their original destination i.e. PLC or RIO. Likewise, this technique allowed us to avoid disruptions on the sequence of EtherNet/IP counters, and injection of undesirable perturbations in the EtherNet/IP connections established between ring devices.

The command we use to queue packets for modification is the following:

```
iptables -t mangle -A PREROUTING -p udp --dport <port> -j NFQUEUE
```

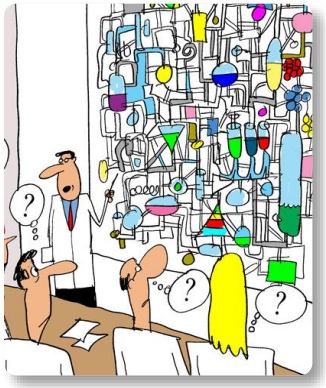
Wireshark We used Wireshark [5] to understand the nature of the communication between devices in the ring. We also used Wireshark together with the SWaT's Control Panel and Electrical Drawings manual, to derive the exact structure of the EtherNet/IP-wrapped messages used in SWaT.

Ettercap We used Ettercap [1], a Man-In-The-Middle attack suite, on our attempts to launch wireless attacks.

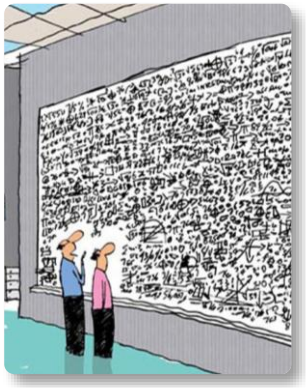
Attacking Fieldbus Communications in

Process comprehension

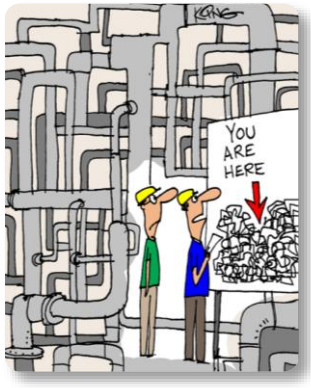
- Process comprehension
  - Understanding exactly what the process is doing, how it is built, configured & controlled
  - Information enumeration, exfiltration and analysis/correlation



What and how the process is producing



How it is controlled



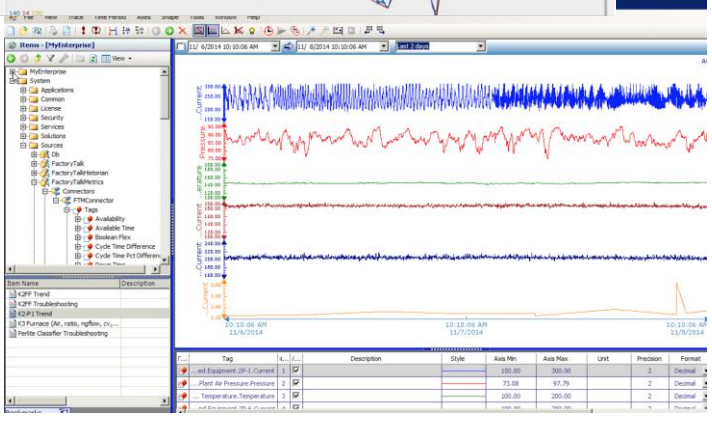
How it is built and wired

Operating & safety constraints

Process Comprehension

Instrument Datasheet					PRESSURE TRANSMITTER				
1	Tag No.				01-PT-510	Manufacturer: Yokogawa			
2	Loop Service				Reactor01-R-510	ModelNo: EJA110A			
3	P&ID No:	Line Number			01-220-004	01-P007-80-B1			
4	Area Classification				Zone 1, GrIIC, T3				
5	Ingress Protection				IP 57				
6					PROCESS CONDITIONS				
7	Fluid	State			HC	Vapour	Process Design Conditions		
8	Pressure	Normal	Max		1450 Kpag	1650 Kpag	Design Pressure	Min/Max	- -
9	Temperature	Normal	Max		100 C	149 C	Design Temperature	Min/Max	- -
10					TRANSMITTER				
11	Instrument Range	LRV / URV / Units		-0.5	14	MPa	Output Signal Type	4-20 mA	
12	Callibration Range	LRV / URV / Units		0	1700	KPag	Protocol/Version	HART	
13	Accuracy			+/- 0.75% of span			Burnout	Downscale	
14	Elevation	Supression		-		-	Installation Style	Horizontal Impulse	
15	LP Proc. Conn.	HP Proc. Conn.		1/4" NPT-F(Vent to Atm)		1/4" NPT-F	Mounting	Via Manifold	
16	Conduit Connection	Power Supply		2xM20 Female		Nominal 24VDC IS	Other	See Note 6	
17	Housing	Paint		Low Copper Cast Alu		Epoxy Resin Coating	Tag Plate	SS304 Permanent	
18									
19					ELEMENT				
20	Element Type	Element Material		DP Capsule		SUS316L	Temperature Limits	Min/Max	-40 C -
21	Measurement (Gauge / Abs / Vac etc)			Gauge			Pressure Limits	Min/Max	- -
22	Body Material	Body Rating		SCS14A		16 Mpa			
23	Bolts	Seals		SUS630		Teflon Coated SUS316			
25	Fill Fluid			Silicone Oil					

Control loop configuration



Historical process data

Process Comprehension (Example)

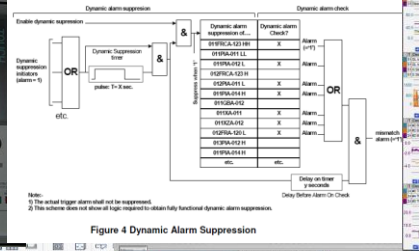
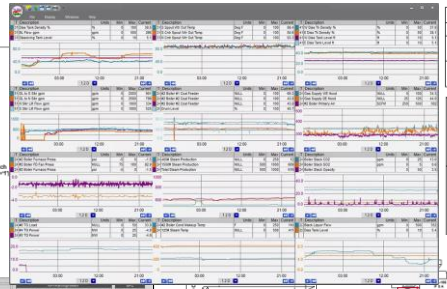
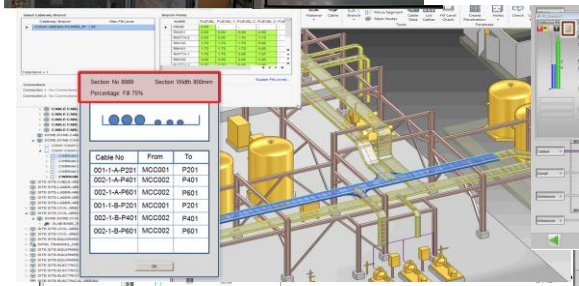
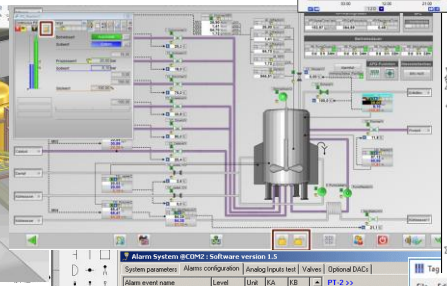
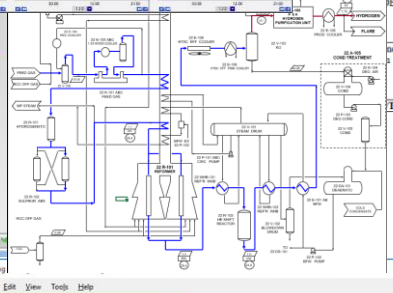


Figure 4 Dynamic Alarm Suppression









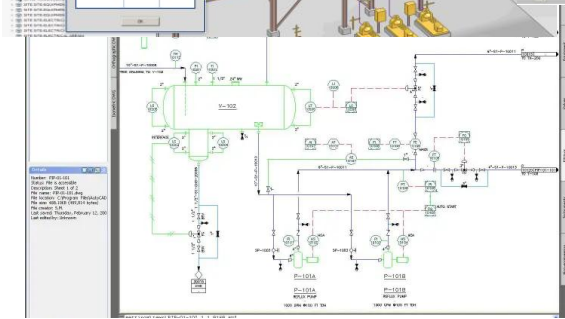
Bill of Material

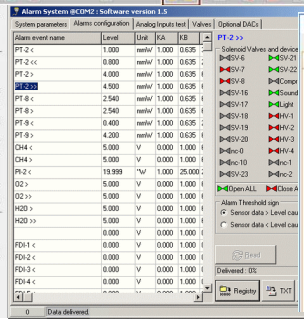
Document No:

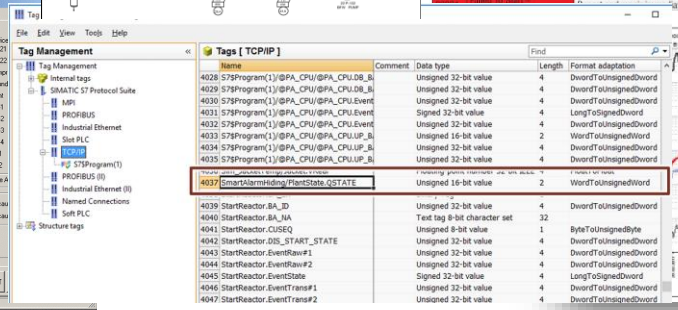
Project : General Project Francis Turbine					Ref :			
Project Code:								
Item Turbine Auxiliary Control And Governor Panel(TAGP)								
Rev 0	Part No	Description	Nomen	Make	Rating/Scale Range etc	Detail	Qty/ Unit	Total QTY	Remarks
	1	Master Trip Relay	86TU	Areva/Alstom	Aux voltage : 110V DC, 6NO+2NC Electrical reset contacts, with flag, case size : ½ NH Dim. H-124xW153xD-128mm Cutout-H-116mmXw145mm	MVAJH	1		
	2	Digital Speed Monitor Relay with Proximity Sensor	SM	Omron	1) Supply Voltage: 24V DC. Sensor Input : NPN input/Voltage input pulse I/P O/P 4-20mA 2) Optional Boards 4 Relay output board Size 96x48mm	K3HB-RNB DC/24 K34-C2	1		**With proximity sensor model no. E2A-M12KS04-M1-C1 XS2F-D422-GCO-A2**
		l Position Indicator E VANE	GVI%	Masibus/Omron/Rediron	% Indicator 24V DC Liner Inputs 4-20mA LOOPIN, LOOPOUT 2 nos. Relay Out put Size 96x48x248mm	LCS296H	1		
		iciator for Trip &	30A	Minilec	12 Windows, 110V DC Big Window- Size 32X32mm	MBAS0600 3	1		**12 Window**

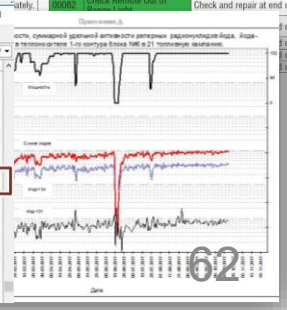
00019	Low Fuel Shutdown	Add fuel, unit will restart*.
00020	Maximum Compr Alarms	Report and repair immediately.
00021	Technician Reset Required	Report and repair immediately.
00022	Low Suction Superheat	Unit will restart*, report reactivation.
00023	A/C Current Over Limit	Unit will restart*, report reactivation.
00024	Compression Ratio Exceeded	Unit will restart*, report reactivation.
00027	High Suction Pressure	Unit will restart*, report reactivation.
00028	Check Refrig System	Unit will restart*, report reactivation.
00029	Check Heat Cycle	Reset, report reactivation
START-UP / ENGINE ALARMS		
00030	Failed To Run Min Time	Report and repair immediately.
	Failed To Start	

00071	Bad F2 or F3 Fuse	Report and repair immediately.
00072	Bad F4 or F6 Fuse	Report and repair immediately.
00073	No A/C Power – Check Gond	Switch to Diesel Operation & Repair
00074	AC Phase Reversed	Unit will restart*, report reactivation.
00075	Compressor Motor Overload	Unit will restart*, report reactivation.
00076	Condenser Motor Overheated	Unit will restart*, report reactivation.
00077	Evap Motor Overheated	Unit will restart*, report reactivation.
00078	Check SV1 Circuit	Reset*, report reactivation.
00079	Check SV4 Circuit	Reset*, report reactivation.
00080	Check SV3 Circuit	Reset*, report reactivation.
00081	Check FHR Circuit	Check and repair at end of trip.
00082	Check Remote Out of	Check and repair at end of trip.

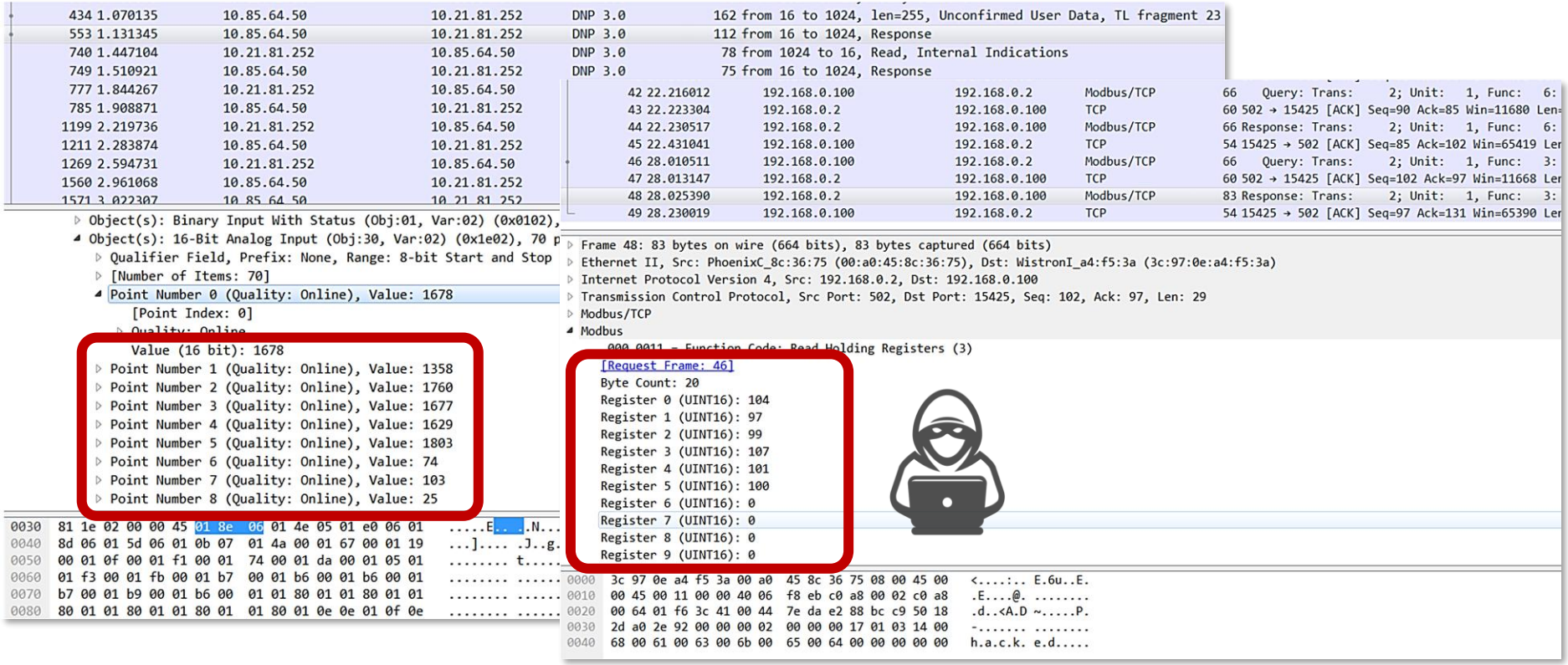






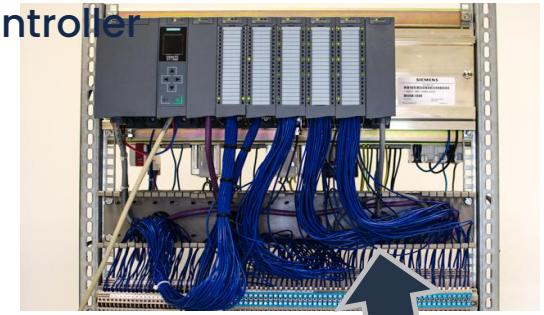


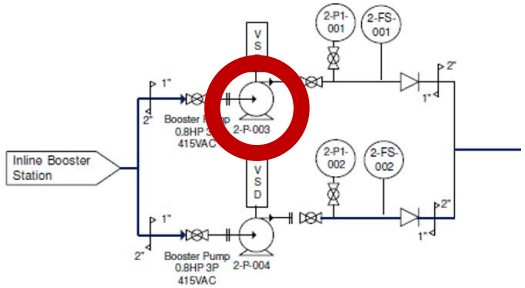
Watching Traffic is not Enough



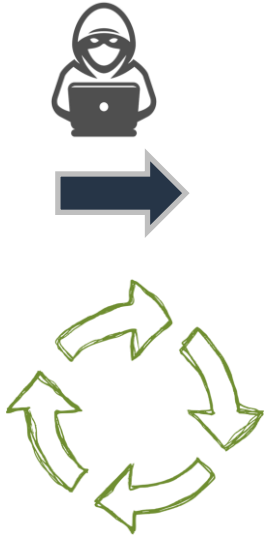
Mapping Diagrams, Points & Logic

Programmable Logic Controller

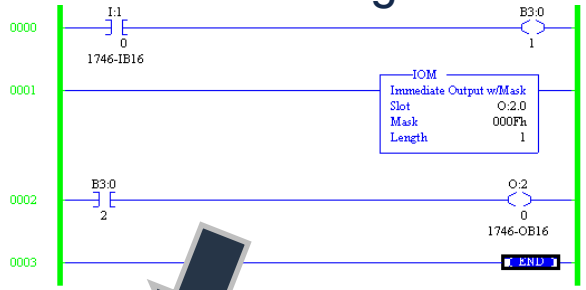


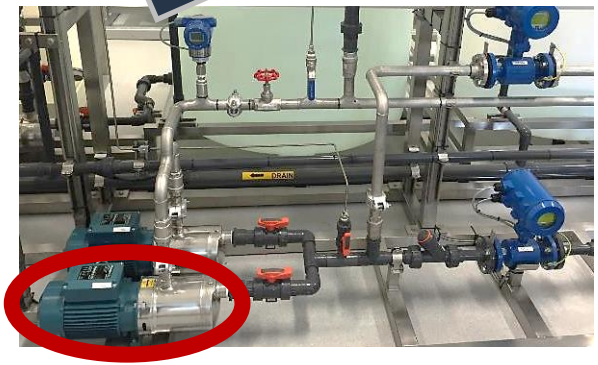


Piping and instrumentation



Ladder logic





Pump in the plant

Mapping Diagrams, Points & Logic

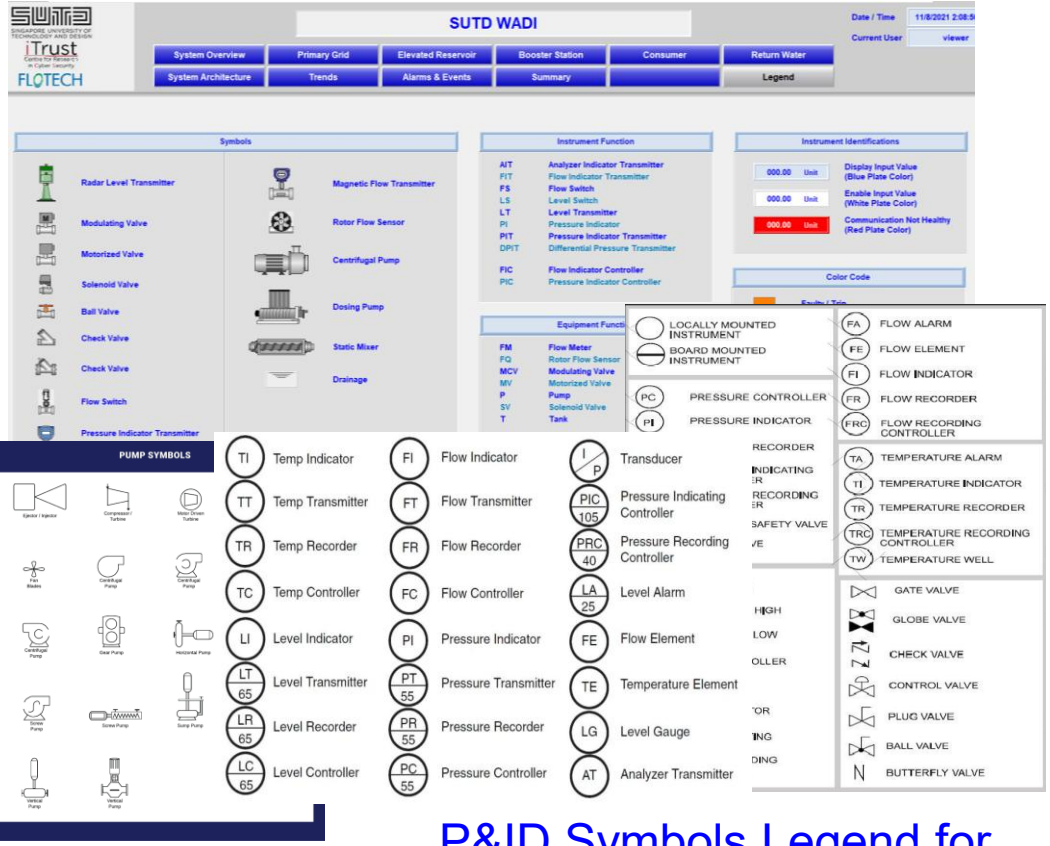
- OT operates on a concept of **"points"**: data sources or controllable functions
  - **Hard point:** physical input or output to/from sensors and actuators.
  - **Soft point:** results derived from mathematical calculations and control logic actions
- Points are defined by IDs and **tags**:
  - **ID:** typically control code specific and defined by input channel or memory location, e.g., "DB1.DBX1.1"
  - **Tag:** is descriptive name of a point, e.g., "Dosing pump_section5"
  - **Tag description:** tag attribute that provides additional information about point
  - Points can have different tags in different diagrams, documentation, software or configuration files
- Mapping of point IDs and tags is
  - Excell tables (documentation)
  - OPC server
  - HMI and other systems

On the Significance of Process Comprehension for Conducting Targeted ICS Attacks

Benjamin Green Marina Krotofil Ali Abbasi

On the Significance of Process Comprehension for

Preparation: Learn Symbols & tags



P&ID Symbols Legend for

Common Industrial Protocol (CIP) stack [8]. In ENIP, sensor values or actuator settings are mapped to *tags*. Each tag can be addressed either via a string descriptor defined by the system designer (e.g., MV101 for motorized valve 1 in process 1), or a more direct mapping to bank number and pin number or similar (directly referring to digital/analog pins of a unit's IO panel). Communications among sensors, actuators, and

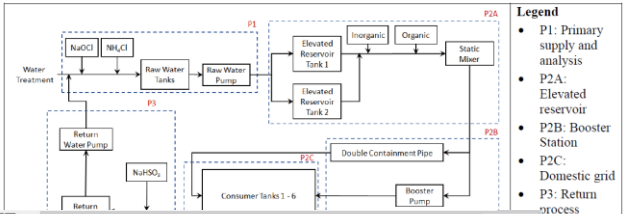
Each PLC has memory locations, known as *tags*, to save sensor data. There is one tag for each sensor connected to a PLC. These tags are accessible across the entire SWaT. Thus, for example, the level of tank T301 in stage P3, can be obtained by PLC 1 to decide whether to start pump P101. Tag values are also sent to SCADA on demand. All sensor data, at every time instant, can be sent to the historian and saved for future analysis. Note that the historian resides in a separate computer connected via the Level 1 network to the PLCs and SCADA system. The availability of tag values at

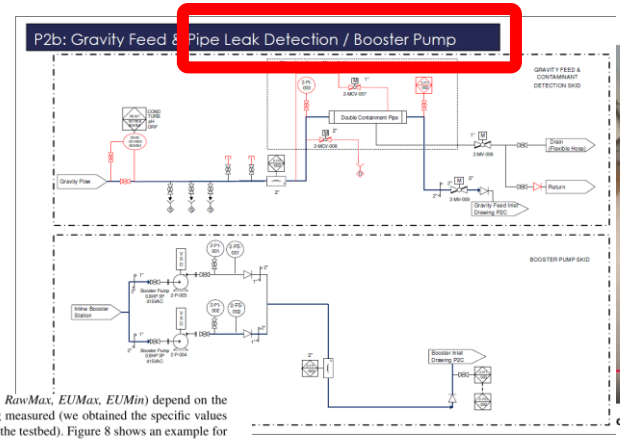
[SWaT: A Water Treatment Testbed for Research]

Preparation: Process Comprehension

PROCESS OVERVIEW

Each of the three sub-processes, referred to as P1 through P3, is controlled by Allen-Bradley PLCs. The operation status of the PLCs is monitored by the SCADA system. These sub-processes are shown in Figures 1, 2 and 3. Details of the components can be found in Section 3.





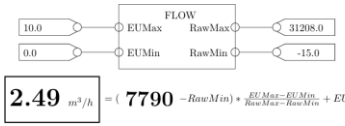
Introduction to SWaT Testbed

Introduction to SWaT Testbed

ction to WaDi Testbed

being 0.5m). The constant values (*RawMin, RawMax, EUMax, EUMin*) depend on the deployment and the physical property being measured (we obtained the specific values for each constant from the HMI software of the testbed). Figure 8 shows an example for the scaling of the water flow in SWaT.

$$Out = (In - RawMin) * \frac{EUMax - EUMin}{RawMax - RawMin} + EUMin \quad (1)$$



$$2.49\ m^3/h = (\ 7790\ - RawMin) * \frac{EUMax - EUMin}{RawMax - RawMin} + EUMin$$

Figure 8. Scaling from 4-20 mA signals to water flow. The 4-20mA signal is scaled by the RIO to another value (7790 in this case) and this value sent over the network is the one we capture and convert to physical observations using Equation (1) with the respective constants for each signal.

Water Distribution (WaDi)

Characteristics of dataset (WaDi.A1)

1. 16 days of continuous operation: 14 under normal operation & 2 days with attack scenarios
2. Data from all the 123 sensors and actuators
3. Attack Scenarios: Derived from the attack models developed by our research team. The attack model considers the intent space of a CPS as an attack model. 15 attacks were launched during the 2 days.

Updates on dataset

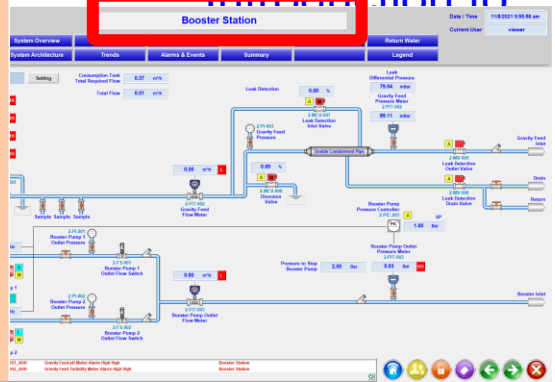
19 Dec 19 (WaDi.A2)

As the plant was unstable for certain periods during the operation, the affected readings have been removed and a new csv file "WADI_14days_new.csv" uploaded. A second csv file "WADI_attackdataLABLE.csv" now contains labels on whether there was an attack (-1) or not (1). The updated attack table with the corrected dates has also been uploaded.

WaDi Dec 2023 (100-hour run)

Characteristics of the Datasets 18 Dec – 22 Dec 2023 SWaT.A9_18 Dec 2023 & WaDi.A3_18 Dec 2023 datasets, i.e., 100 Hour Run Dataset

1. 105 hours of continuous operations of both SWaT and WaDi testbeds under [illegible]
2. The first 4 hours of continuous run of both testbeds was not in CrossOver mode,



WADI: A Water Distribution Testbed for Research in the Design of Secure Cyber Physical Systems*

Chuadhry Mujeeb Ahmed
Singapore University of Technology and Design

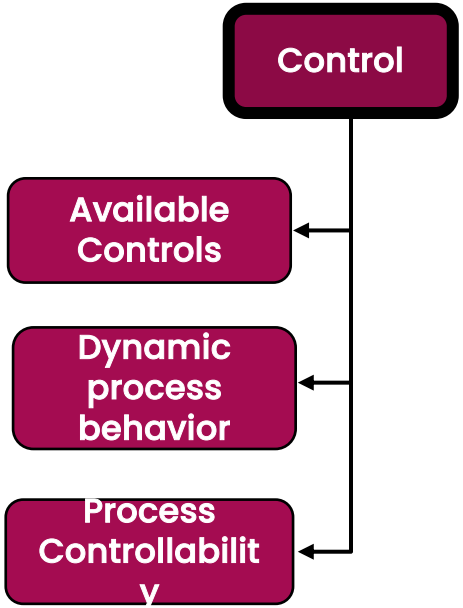
Venkata Reddy Palleti
Singapore University of Technology and Design

Aditya P. Mathur
Singapore University of Technology and Design

Discovering Attack Signature and Its Travel Path using Graphical Model in CPS: A Case Study | ACM Transactions on Cyber-Physical Systems

Control

- The key distinction of IT and CPS systems is time-dependency and dynamic behavior with well-defined operational limits
  - Guided by laws of physics and control logic
- No documentation can convey entire/precise dynamic behavior of the system
  - If I change one process parameter, what else is changing and how much?
- "Obtaining control is not to being in control"

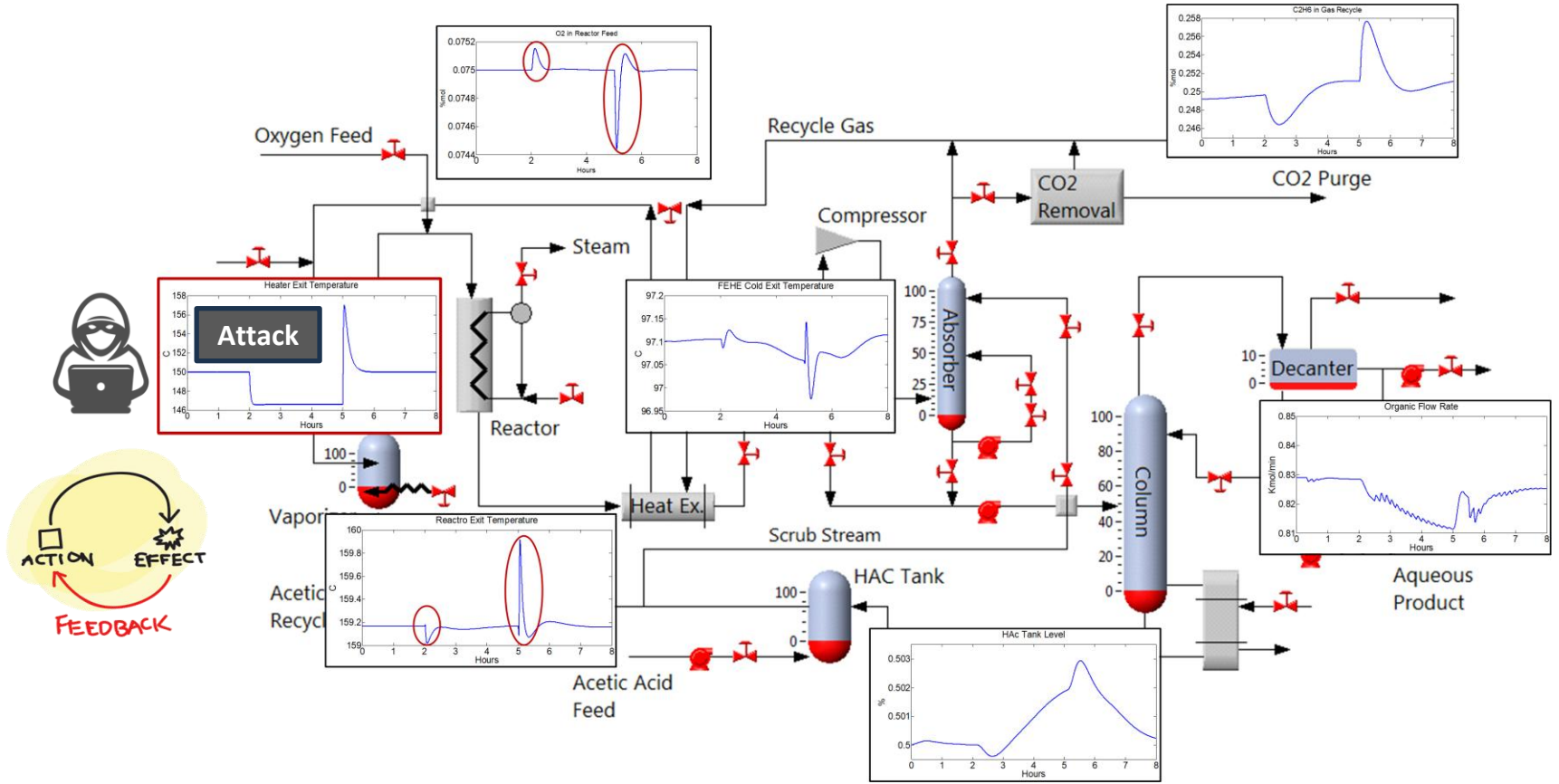


Guided by the following question:

What control elements are available for process manipulation, how much the process can be changed and how much/far attack effect propagates through the process?

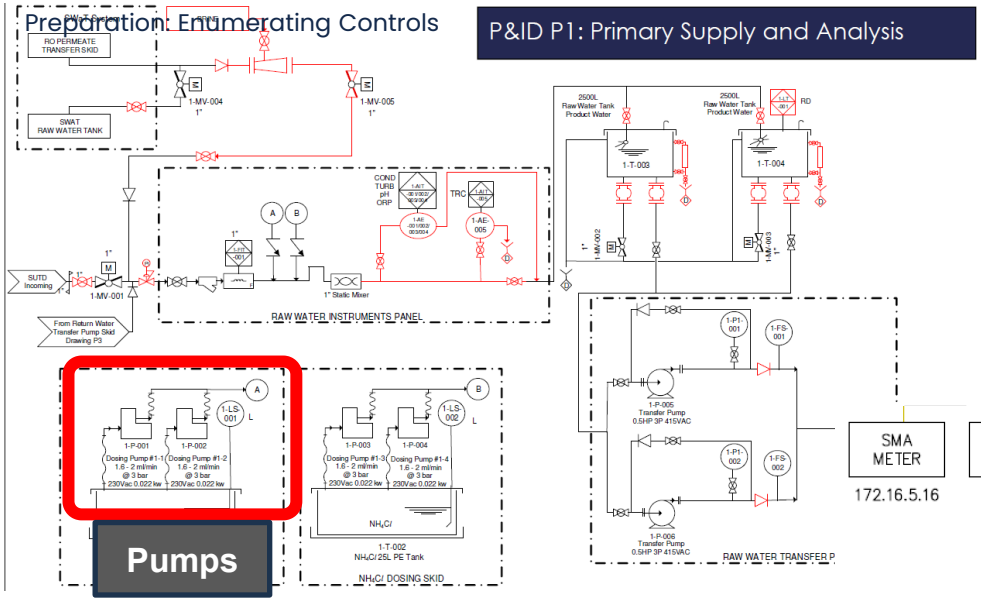
- Attack can move the process into "weird states" with unpredictable behavior

Dynamic Process Behavior (Example)



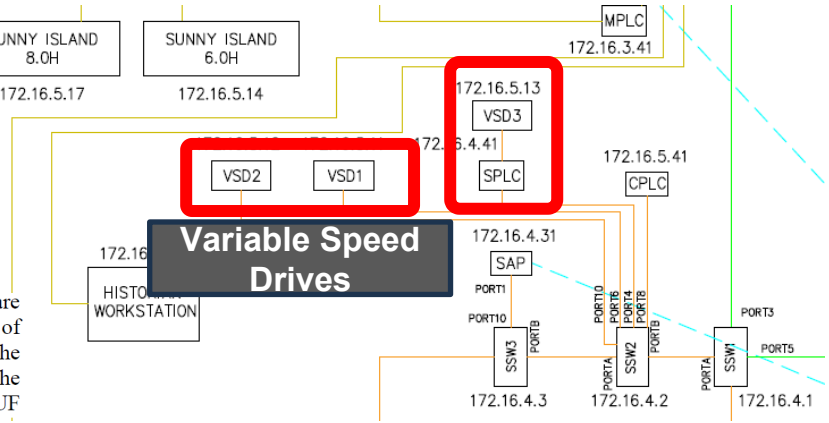
Preparation: Enumerating Controls

P&ID P1: Primary Supply and Analysis



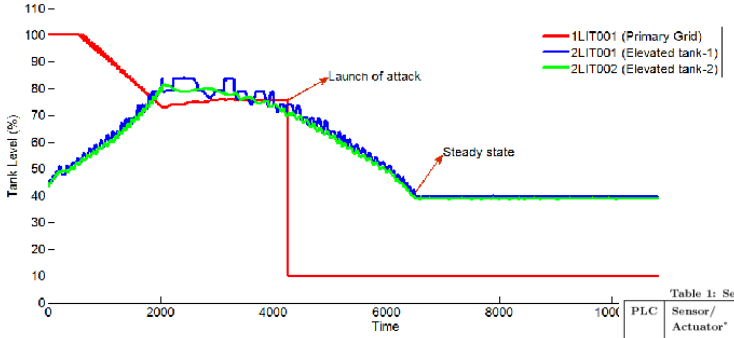
WADI consists of an array of actuators to ensure its safe operations. These are:

- Pump (P) with Running or Stopped status
- Motorised Valves (MV) with Open, Closed or Transition status
- Solenoid Valves (SV) with Open, Closed or Transition status
- Modulating Valve (MCV) measures in %



backwashing process, the HMI shall indicate the backwashing process. All backwash sequential steps are displayed on HMI. Backwash step duration shall be programmable via HMI. Under a semi-automatic mode of operation, the operator manually initiates the backwashing process, and the PLC would automatically complete the backwash process and place the UF membrane system back into the filtration service. The operator shall have the flexibility to manually control the operation of the filters. The backwash pump (P602) is used to backwash the UF

Preparation: Dynamic Process Behavior



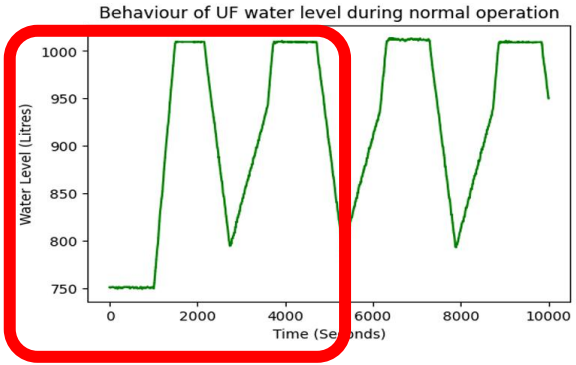
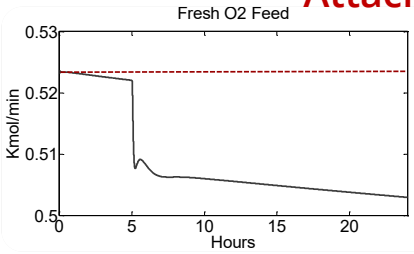


Table 1: Sensors, actuators and state variables used in the attack detection experiments.

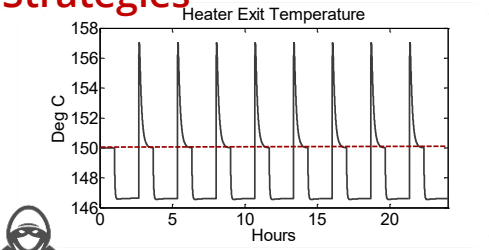
PLC	Sensor/ Actuator*	State variable	States	Purpose
1	si: FIT101	v_1	No flow: $v_1 \leq \delta$ Flow: $v_1 > \delta$	Measures flow rate of water entering tank T101.
	sio: LIT101	v_2	$v_2 \in \{LL, L, H, HH\}$	Indicates water level in tank T101.
	ai: MV101	v_3	Closed: $v_3 = 0$ Open: $v_3 = 1$	Motorized valve; water flows into tank T101 only when MV101 is open.
	ao: P101	v_4	OFF: $v_4 = 0$ ON: $v_4 = 1$	Pump to move water from stage 1 to stage 3 via stage 2.
	so: FIT201	v_{14}	No flow: $v_{14} \leq \delta$ Flow: $v_{14} > \delta$	Measure flow rate of water from T101 to T301.
2	sio: FIT201	v_{14}	$v_5 \in \{LL, L, H, HH\}$	Measures flow rate of water entering tank T301.
	ai: P101	v_4	OFF: $v_4 = 0$ ON: $v_4 = 1$	
	ao: MV201	v_8	Closed: $v_8 = 0$ Open: $v_8 = 1$	Motorized valve must be open when P101 is ON for water to flow into tank T301.
3	sio: LIT 301	v_5	$v_5 \in \{LL, L, H, HH\}$	
	so: FIT301	v_6	No flow: $v_6 \leq \delta$ Flow: $v_6 > \delta$	
	so: DPIT301	v_7	No backwash: $v_7 \leq \sigma$ Backwash: $v_7 > \sigma$	
	ai: P101	v_4	OFF: $v_4 = 0$ ON: $v_4 = 1$	

Distributed Detection of Single-Stage Multipoint Cyber Attacks in a Water Treatment Plant

Attack Strategies



Step attack



Periodic attack

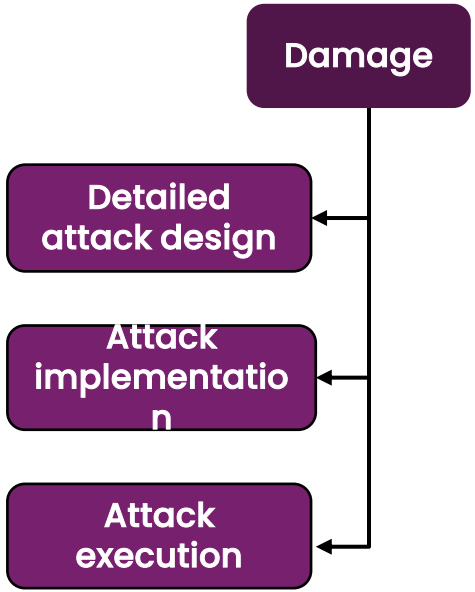
me :-)

Discovery and documentation of the dynamic process behavior is mostly a manual process (no helpful tools exist)

Attack Pattern Mining to Discover Hidden Threats to Industrial Control Systems

Damage

- Design/engineering of the detailed damage/attack scenario and its practical implementation
- Translation of high-consequence events (e.g., vessel overpressure) into a set of specific attack instances and cyber-physical exploits/payloads
  - Based on the outcomes of the previous stages (Discovery, Control)
- Remote or autonomous execution of the attack



Guided by the following questions:

What specific physical outcome is desired? How can it be achieved in reliable way? What payloads need to be developed and deployed in which assets?

- Damage stage is tightly coupled with Prevent Response and Obtain Feedback stages (control loop principle)

What Can be Done to the Process

Equipment damage

- Equipment overstress
- Violation of safety limits

Production damage

- Product quality or production rate
- Operating costs
- Maintenance efforts

Paracetamol

Purity	Relative price, EUR/kg
98%	1
99%	5
100%	8205

Source: http://www.sigmaaldrich.com/

Compliance violation

- Safety
- Pollution
- Contractual agreements

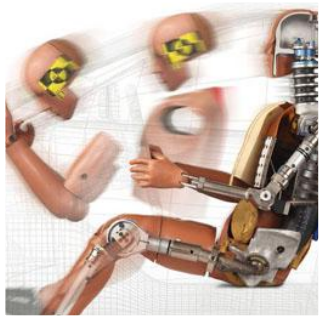
Service Uptime

- Degrade service quality/safety/ trustworthiness
- Make service unavailable

Basic Physical Damage Taxonomy

- Requires subject-matter knowledge (engineering)
  - Among least familiar stages to IT hackers/Red Teamers
- Accident data is a good starting point:
  - National governmental agencies (regulations and incident reports)
  - Public/commercial accident data bases, research, blog posts

Inertia



Exclusion

Resonance

Wear

Surge

Latent Abilities

* J. Larsen & M. Krotofil – Beyond the Firewall: Physical Exploitation

Preparation: Check Existing Scenarios

On Practical Threat Scenario Testing in an Electric Power ICS Testbed

Ahnaf Siddiqi
Singapore University of Technology and Design, Singapore

Nils Ole Tippenhauer
Singapore University of Technology and Design, Singapore

On Practical Threat Scenario Testing in an Electrical Power ICS Testbed

Example 1: The purpose of this attack is to degrade the performance of SWaT from the nominal 5 gallons/minute to a lower value. To understand how this could be done, consider the fact that the UF unit contains micrometer sized membranes to remove small particles from the water to be filtered. PLC 6 (stage P6 in Figure 2) is programmed to clean the UF every 30 minutes by using a backwash process. However, depending on the quality of the incoming water, UF may need to be cleaned sooner. PLC 3 (stage P3 in Figure 2) is responsible

SWaT: A Water Treatment Testbed for

11	P101=Off, FIT201<0.5, MV201=Close, P203=Off, P205=Off, FIT301<0.5, MV301=Close, MV302=Open, FIT601<0.5 ->P302=Off	N/A	10:09	10:12	Backwash unable to start
12	FIT101>0.5, P101=Off, MV201=Open, MV301=Close, MV304=Close, P302=On ->FIT301>0.5	N/A	10:14	10:17	The UF membrane could be overused, Level of RO Feed tank is increasing faster

Attack Pattern Mining to Discover Hidden

TABLE 2. Description of the attack scenarios on the SWaT testbed.

Attack	Description	Impact	Attacker intent met?
1	MV-101 is open while it should be closed	Tank overflow	Yes
2	P-102 is turned ON while it should be OFF	Pipe bursts	Yes
3	LIT-101 reading is increased 1 mm per second	Tank underflow and damage P-101	Yes
4	MV-504 is open while it should be closed	No impact	No
5	AIT-202 reading is reduced below the nominal value	AIT-504 increased, and drainage did not start	No
6	LIT-301 reading is increased above the maximum limit	Tank underflow and damage P-101	Yes
7	DPIT-301 reading is increased above the nominal value	Backwash process re-started, decrease Tank-401 water level, increase Tank 301 water level	Yes
8-9	FIT-401 reading is reduced below the nominal value	UV process shutdown and P-501 turns OFF;	Yes
10	MV-304 is closed while it should be open	MV-304 was closed	No
11	MV-303 is stuck at the closed position	No impact	No
12	LIT-301 reading is decreased by 1 mm per second	Tank overflow	Yes
13	MV-303 is stuck at the closed position	Halt stage 3 operation	Yes
14-15	AIT-504 reading is increased above the nominal value	No impact	No
16	MV-101 is stuck at the open position, and LIT-101 reading is set as 0.7 m	Tank overflow	Yes
17	UV-401 is OFF while it should be ON, AIT-502 reading is increased above the nominal value, and P-501 is stuck at ON mode	Reduced output at FIT-502	No
18	DPIT-301 reading is increased above the nominal value, MV-302 is stuck at the open position, and P-602 is stuck at OFF mode	System freeze	Yes
19	P-203 and P-205 are turned OFF while they should be ON	No impact	No
20	LIT-401 reading is increased above the nominal value, and P-205 is stuck at ON mode	Tank overflow	Yes
21	P-101 is stuck at ON mode while it should be OFF, and LIT-301 reading is set at 0.8 m	Tank-101 underflow and Tank-301 overflow	Yes
22	P-302 is stuck at ON mode, and LIT-401 reading is set at 0.6 m	Tank overflow	Yes
23	P-302 is turned OFF while it should be ON	Inflow to Tank-401 stops	Yes
24	P-201, P-203, and P-205 are turned ON while they should be OFF	No impact	No
25	P-101 and MV-101 are stuck at ON mode while they should be OFF, and LIT-101 reading is set at 0.7 m	Tank-101 underflow and Tank-301 overflow	Yes

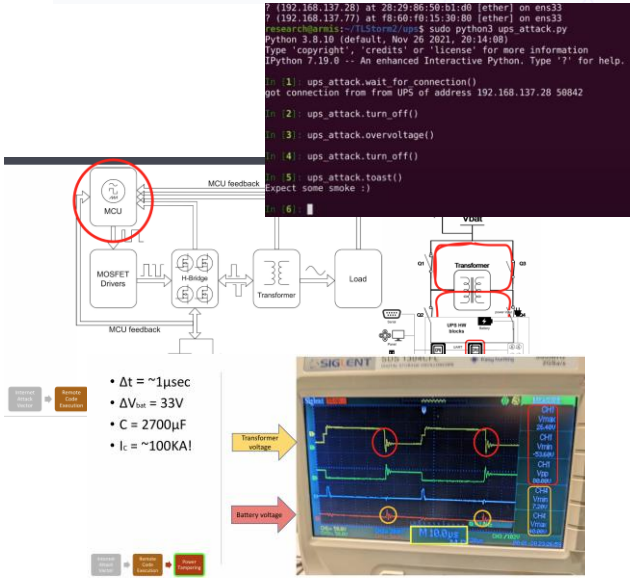
TABLE 3. Description of the attack scenarios on the WADI testbed.

Attack	Description	Impact	Attacker intent met?
1	1-MV-001 is open while it should be closed	Tank overflow	No
2	1-FIT-001 reading is tampered with	Change Water quality	Yes
3-4	1-AIT-001 reading is tampered with	Tank underflow	Yes
5	2-MCV-101 to 2-MCV-601 are closed while they should be open	Interfere with the water distribution process	Yes
6	2-MCV-101 and 2-MCV-201 are open while they should be closed	Interfere with the water distribution process	Yes
7	1-AIT-002 reading is tampered with and open 2-MV-003 while it should be closed	Change Water quality	Yes
8, 11, 12	2-MCV-007 is open while it should be closed	Interfere with the water distribution process	No
9	1-P-006 is turned ON while it should be off	Pipe bursts	Yes
10	Cause damage to 1-MV-001 and raw water pump	Tank underflow	Yes
13	Reduce pressure pump setpoint	Interfere with the water distribution process	Yes
14	Stop chemical dosing pumps	Change Water quality	Yes
15	AIT-001 reading is tampered with	Tank overflow	Yes

A Dual-Isolation-Forests-Based Attack Detection Framework for Industrial Control Systems

Preparation: Check Existing Research

Armis Finds Three Critical Zero-Day Vulnerabilities in APC Smart-UPS Devices, Dubbed "TLStorm," Exposing More than 20 Million Enterprise Devices



How Hackers Can Use 'Evil Bubbles' to Destroy Industrial Pumps

WIRED

Exploring Ransomware Attacks on Smart Inverters

Publisher: IEEE Cite This PDF

BoHyun Ahn ; Alycia M. Jenkins ; Taesic Kim ; Jianwu Zeng ; Lifford McLauchlan ; Sung-won Park

A Dark Side to Power Grids

The final payload

	Meaning	Value
n Buffer	parse_mqtt_packet `a0`	memcpy gadget address
	parse_mqtt_packet `a1`	`A + 0xbc`
	shellcode `a1`	`A + 0x9c`
	imaginary `a1`	`A + 0x100`

Grid destabilization

Like Lightning From the Cloud: Finding RCEs in an Embedded TLS Library and Toasting a Popular Cloud-connected UPS - Black Hat Asia 2022 | Briefings Schedule

Evil Bubbles or How to Deliver Attack Payload via the Physics of the Process

A Closer Look at the Gaps in the Grid: New Vulnerabilities and Exploits Affecting

Successful implementation of attack scenario and its cyber execution will not necessarily result in successful damage outcome

Example: Breaking UF filter in water treatment facility (SWaT)

Filter as High-Consequence Target

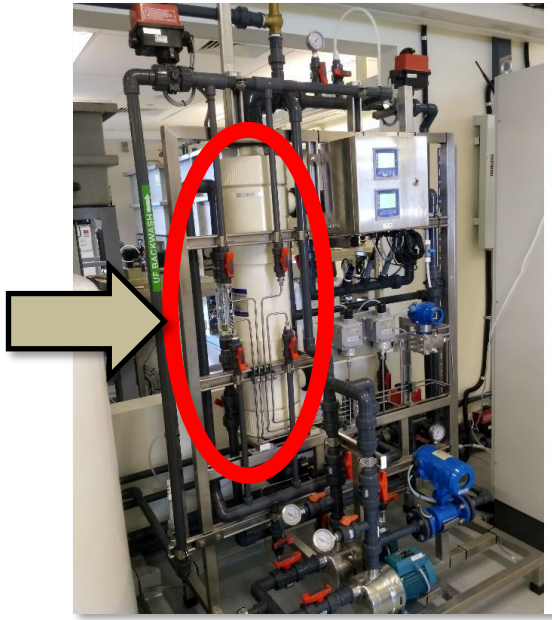
Water treatment process consists of multiple stages, including several stages of filtering

- Water filters are expensive
- When broken, water supply is interrupted

https://en.wikipedia.org/wiki/Ultrafiltration

https://en.wikipedia.org/wiki/Reverse_osmosis

Ultrafiltration Stage in SWaT



https://itrust.sutd.edu.sg/testbeds/secure-water-treatment-swat/

Finding Plausible Damage Scenario

Danger of damage to the UF membrane!

Caution — Ingress of oil or grease will damage the UF membrane irreversibly.

Make sure, that no oil or grease gets into the feed water.

Danger of damage to the UF membrane!

Caution — Pressurising the UF membrane with more than 2 bar will damage it irreversibly.

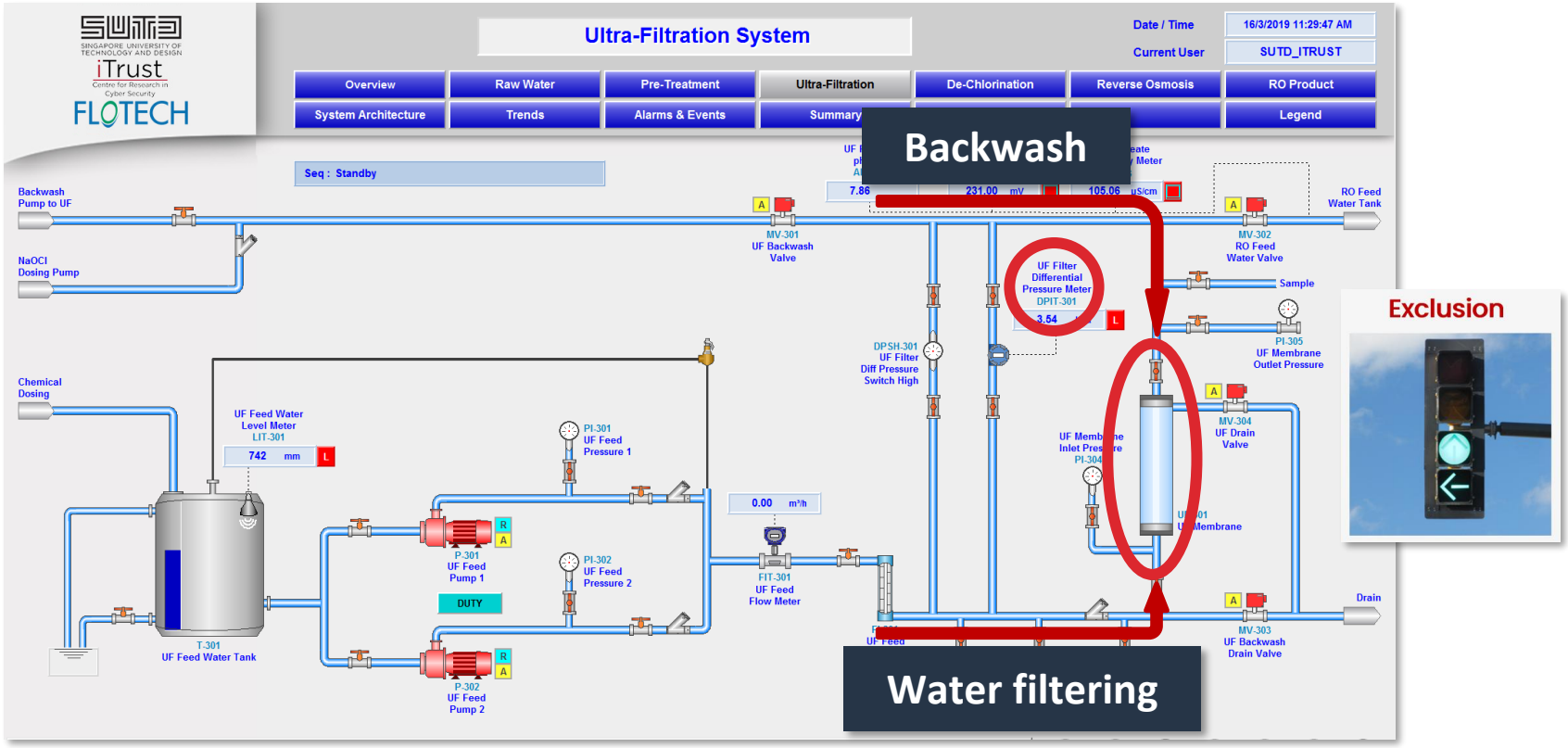
Make sure, that a maximum of 2 bar at the outlet of the non-return valve is not exceeded. Use a pressure regulator.

Extended peak-load operation of the system can lead to damage or destruction of the ultrafiltration membranes.

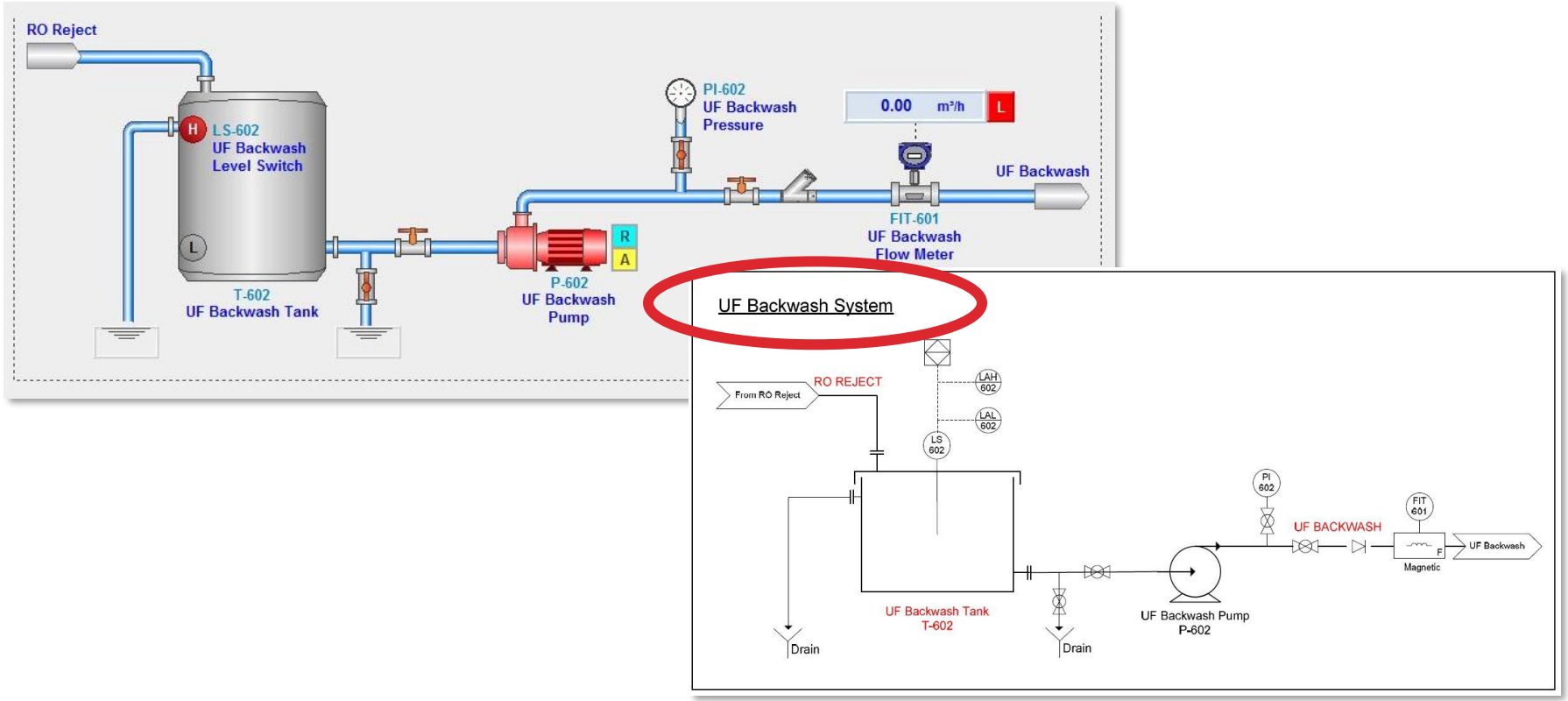
net.grundfos.com/Appl/ccmsservices/public/literature/filedata/Grundfosliterature-5606062.pdf

https://www.gruenbeck.de/fileadmin/user_upload/produkte/membransysteme/pdf_en/ba-561940-inter_084_geno-ultrafil_450-900.pdf

Process Discovery (1)



Process Discovery (2)



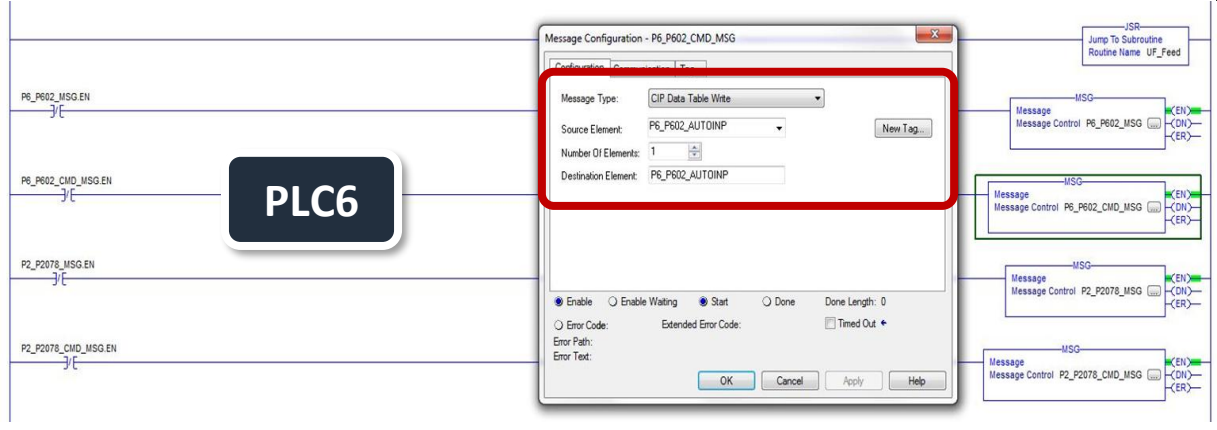
Process Discovery (3)

There are **tree conditions** which can **trigger backwash** process, each **guided** by a **state machine** in a **PLC:**

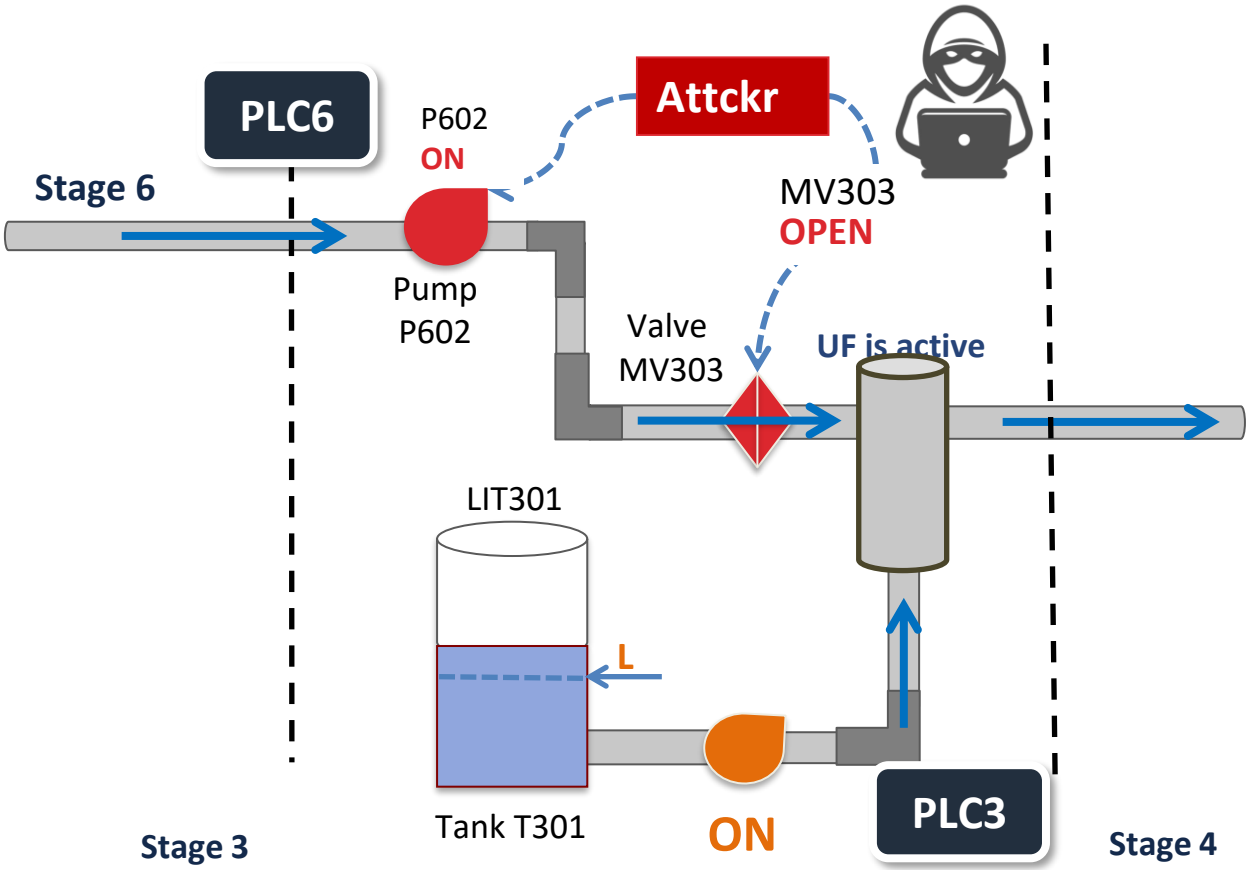
- Preset timer (every 30 minutes)
- UF filter differential pressure (DP) ≥ 40 kPa
- Plant shutdown

PLC3

```
7:(*FILTRATION FOR PRESET TIMER*)
        LAST_STATE:= HMI_P3_STATE;

        _MV301_AutoInp           :=0;
        _MV302_AutoInp           :=1;
        _MV303_AutoInp           :=0;
        _MV304_AutoInp           :=0;
        _P_UF_FEED_DUTY_AutoInp  :=1;
        _P602_AutoInp            :=0;
        _P_NAOCL_UF_DUTY_AutoInp:=0;

        HMI_UF_REFILL_SEC        :=0;

        HMI_BACKWASH_SEC         :=0;
        HMI_CIP_CLEANING_SEC     :=0;
        HMI_DRAIN_SEC            :=0;

    IF HMI_TMP_HIGH THEN
        HMI_P3_STATE:=8;
    ELSE
        IF _MIN_P THEN
            HMI_UF_FILTRATION_MIN:= HMI_UF_FILTRATION_MIN+1;

        END_IF;
    END_IF;
```



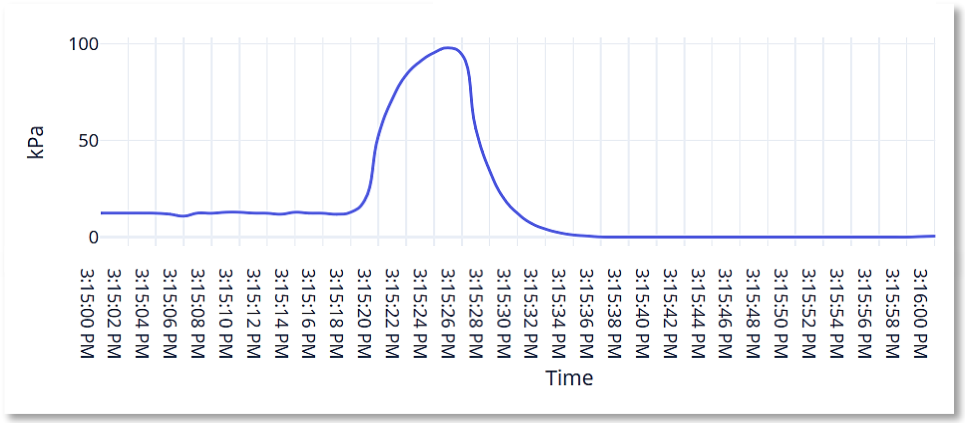
Execution of Attack



Let's see what max pressure can be achieved

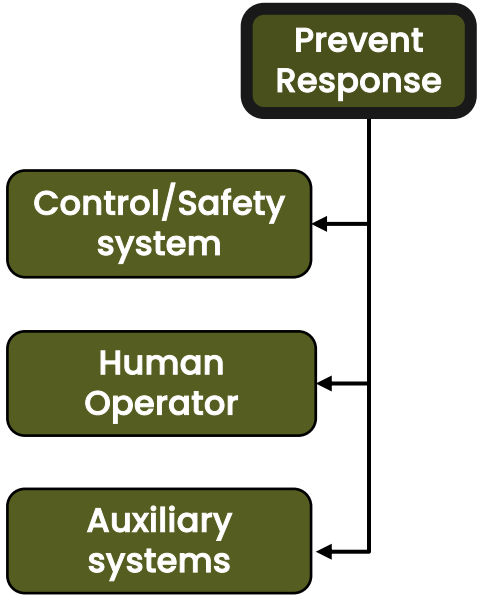
Attacker is not Almighty

- Average UF filter DP is ≈ 12-13 kPa
- Max DP is **98 kPa (~ 1 bar)**
- **Not enough for breakage**
- Such information can only be figured out on a live process
  - Control stage: probing control loop potential to achieve desired physical state



Prevent Response

- During attack execution the control/safety systems and possibly human operator will be working “against” attacker trying to keep the process in efficient/safe state
  - Attack interference or interruption
- May include “racing” conditions (be faster than control/ safety system) and violation of predefined permitted process states
  - Spoofing process state is effective method to prevent response



Guided by the following questions:

What systems might interfere with the attack execution and in what way? How attack effects can be concealed to prevent counter-reaction?

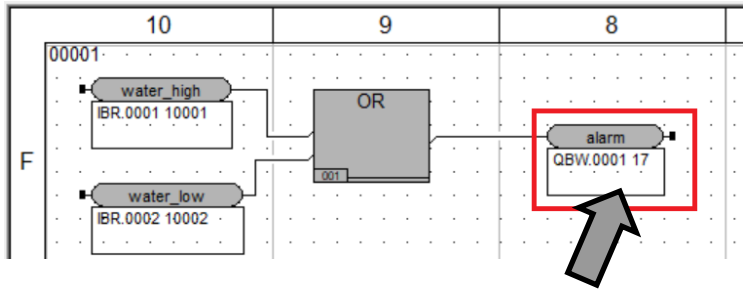
- This attack stage can be avoided by remaining below “response” threshold

Approaches to Preventing Response

- Alarm suppression/hiding/relaxation
  - Patch instructions in the PLC (alarm suppression) or change alarm limits
  - Cause alarm flood/storm (to hide critical alarm), etc.
- DoS protective equipment
  - Protective relays or safety PLCs
- Patch "interlock" conditions in control logic

```
li      r28, 0
stw     r28, -4(r2)
lis     r27, _water_high@ha
lwz     r28, _water_high@l(r27)
clrlwi  r28, r28, 31  # r28 := water_high
lis     r26, _water_low
lwz     r27, _water_low(r26)
clrlwi  r27, r27, 31  # r27 := water_low
li      r26, 0        # alarm := FALSE
addi    r27, r2, -4
lwz     r28, 0(r27)
insrwi  r28, r26, 1,31
stw     r28, 0(r27)
lwz     r28, -4(r2)
clrlwi  r28, r28, 31
lis     r26, _alarm
mr      r26, r26
lwz     r27, 0(r26)
insrwi  r27, r28, 1,31
stw     r27, 0(r26)
```

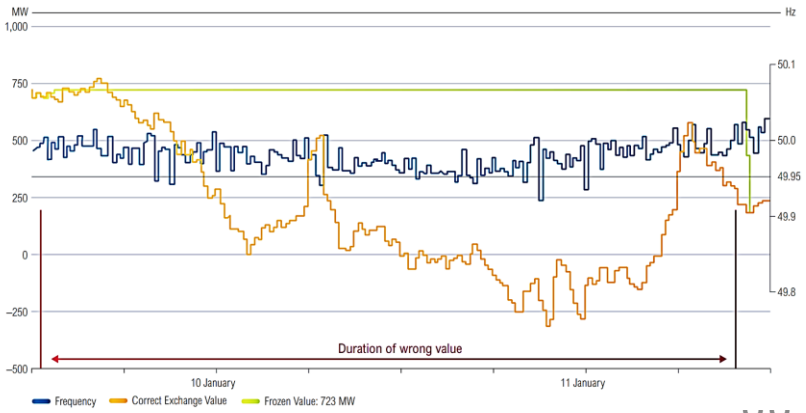
Water tank level alarm



Safety program resides in memory as code, modify to set alarm to fixed FALSE

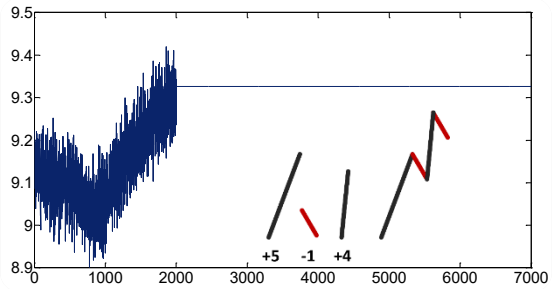
Stale Data Attack

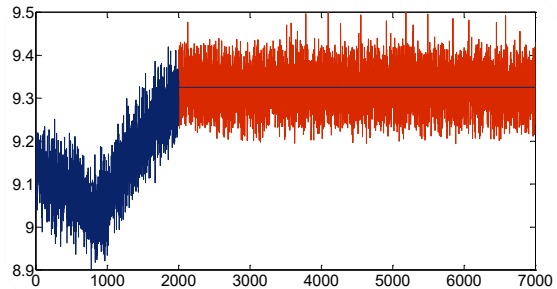
- Loss of observability in a single control loop almost collapsed EU power grid
  - On 10 Jan 2019, the Continental Europe Power System registered the largest absolute frequency deviation since 2006*.
- The failure of a telecommunication link led to the grid control be based on the last received process values from a remote load frequency controller
  - DoSing communication link (including packet drop or delay) is an effective method to prevent real process state reaching control system

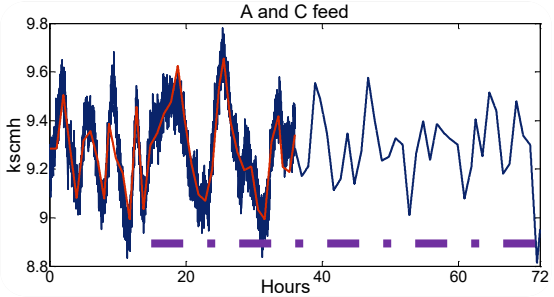


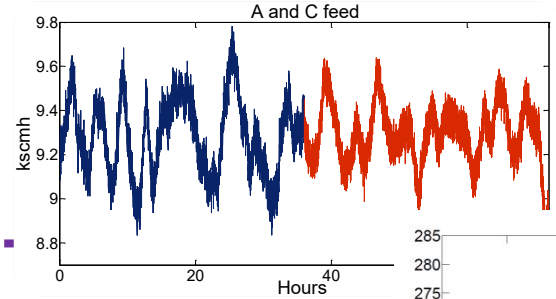
*https://eepublicdownloads.entsoe.eu/clean-documents/news/2019/190522_SOC_TOP_11.6_Task%20Force%20Significant%20Frequency%20Deviations_External%20Report.pdf

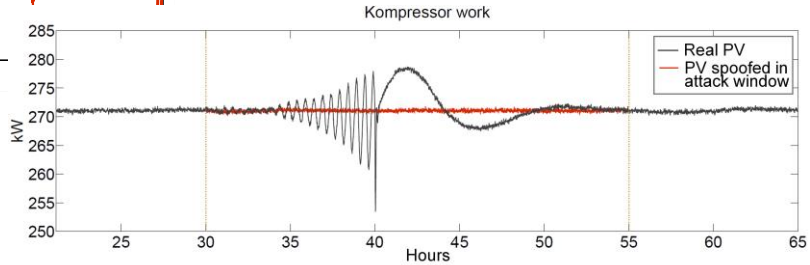
Spoofing Sensor Signals in Transmitter











M. Krotofil, J. Larsen, D. Gollmann. The Process Matters: Ensuring Data Veracity in Cyber-Physical Systems (ASIACCS, 2015)

Preparation: Unwanted Process States

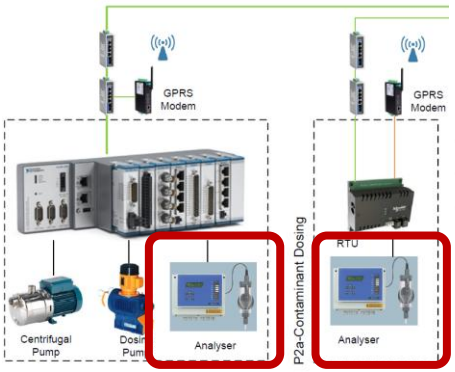
- Learn permissible and mutually exclusive control sequences and process states, the associated interlocks and the mechanisms of their detection and enforcement
  - E.g., verification of a certain condition being met or setting specific flag value
- Decide on most effective or convenient ways to prevent system response to envisioned attack instances/attack scenario

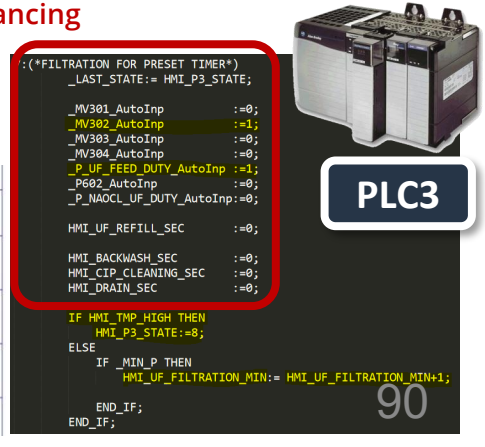
F. System Response to Attacks

It is important to know how a CPS will respond to cyber and physical attacks. This information is useful in designing

SWaT: A Water Treatment Testbed for Research

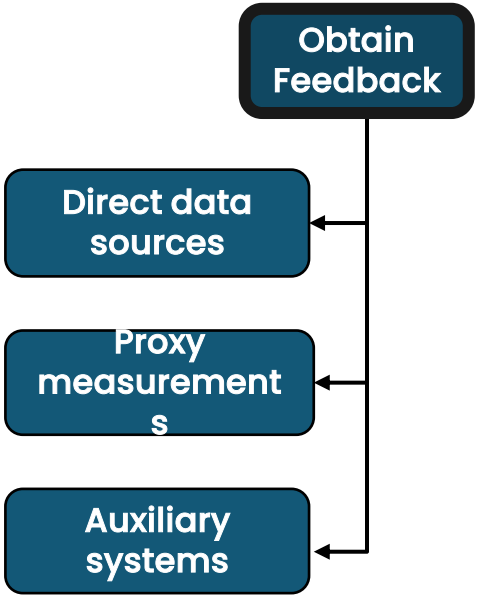
Detection of contamination or improper chemical balancing





Obtain Feedback

- If the attack impact is not instantaneous or reliably guaranteed, the attacker needs to monitor attack progress
- The attacker needs a way to compare effectiveness of several attack scenarios or coordinate implants
- If existing measurements are insufficient, proxy measurements or calculations can be used

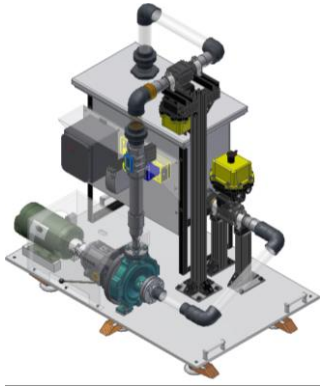


Guided by the following question:

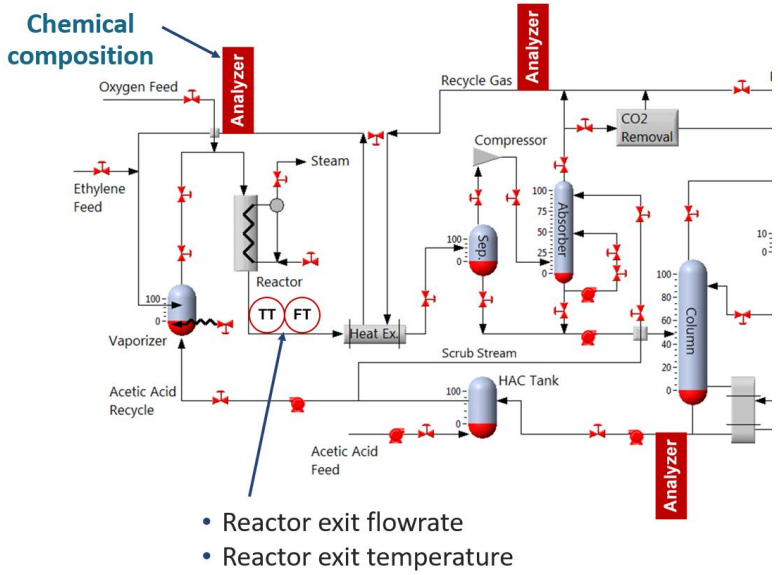
What measurements are required/helpful to monitor attack progress/failure, coordinate attack steps/payloads and detect the achievement of the final outcome?

Processes aren't Always Hacker Friend'...

There is no "Pipe Roundness" sensor



There is no sensor to detect cavitation bubbles



- Reactor exit flowrate
- Reactor exit temperature

No Analyzer in Reactor exit pipe to measure reduction of primary reaction

Preparation: Existing Measurements

WaDi: Sensors

- Level Transmitter (LT) measures in %
- Level Switch (LS) with HIGH, LOW, NORMAL status
- Flow Indication Transmitter (FIT) measures in m^3/hr
- Flow Totalizer measures in m^3/hr
- Rotor Flow Sensor (FQ) measures in m^3/hr
- Flow Switch (FS) with HIGH, LOW, NORMAL status
- Analyser Indicator Transmitter (AIT)
  - Conductivity measures in µS/cm
  - pH
  - Oxidation Reduction Potential (ORP) measures in mV
  - Turbidity (NTU)
  - Total Residual Chlorine (mg/L)
- Pressure Indicator Transmitter (PIT) measures in mBar
- Differential Pressure Indicator Transmitter (DPIT) measures in mBar

Example 1: The purpose of this attack is to degrade the performance of SWaT from the nominal 5 gallons/minute to a lower value. To understand how this could be done, consider

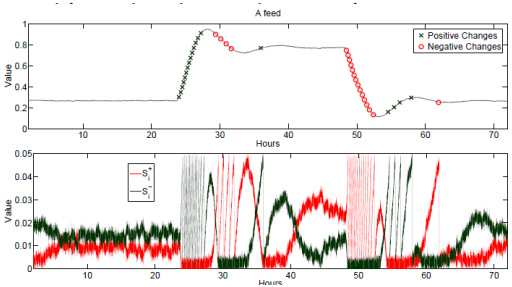
similar attack, sensor LIT401 was compromised. The impact of attacking sensor LIT401 was measured on the flow rate of water at the output of the RO unit. According to system specifications, this flow rate must remain at about 1.2cm/hr which leads to nearly 5 gallons/minute of treated water. The single point attack on LIT401 changed the level of the RO feed

SWaT: A Water Treatment Testbed for

SWaT: Sensors (25 in total)

- Level Indicator Transmitter (LIT) measures in mm
- Level Switch (LS) with HIGH, LOW, NORMAL status
- Flow Indication Transmitter (FIT) measures in m^3/hr
- Analyser Indicator Transmitter (AIT)
  - Conductivity, measures in µS/cm
  - pH
  - Oxidation-Reduction Potential (ORP) measures in mV
  - Hardness measures in ppm
- Differential Pressure Indicator Transmitter (DPIT) measures in kPa
- Differential Pressure Switch (DPSH) with control setpoints to trigger an action
- Pressure Indicator Transmitter (PIT) measures in kPa
- Pressure Indicator (PI) measures in kPa
- Pressure Switch (PSH or PSL) with control setpoints to trigger an action

The RO system feed water is protected by a set of sodium bisulphite ($NaHSO3$) dosing systems with ORP analysers (AIT402/AIT502) on the feed line to prevent residual chlorine breakthrough from the UV chlorine destruction unit. The $NaHSO_3$ dosing system is to provide a stock solution of $NaHSO_3$ to be added to the UF filtered water to maintain an ORP below 250mV. The dosing rate is determined based on the ORP meter reading linked to the maximum residual chlorine level.

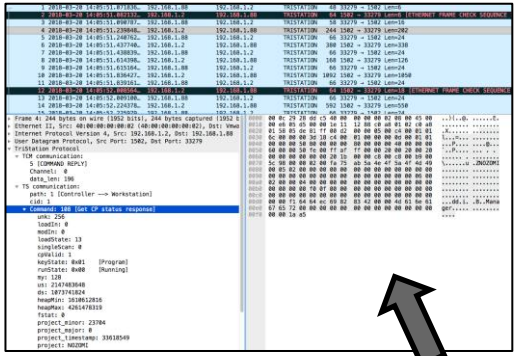


Process **state change detection** with **lightweight** Non-Parametric Cumulative Sum (NCUSUM) **algorithm**

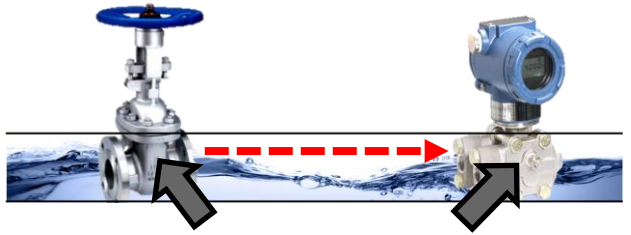
```
check(double):
        stwu 1,-48(1)
        mflr 0
        stw 0,52(1)
        stw 31,44(1)
        mr 31,1
        stfd 1,24(31)
        lfd 1,24(31)
        bl compute_score(do
        stfd 1,8(31)
        lis 9,m_current_sum@ha
        lfd 12,m_current_sum@l(9)
```

17640 bytes ~= 0.11% of DRAM

(*...mized*)



Implant coordination via digital comms is non-trivial

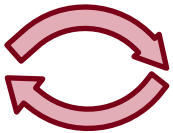


These can be in completely different parts of the process, on different networks

E.g., observation of state *A* in component *B* needs to trigger payloads *X*, *Y* , *Z* (C2 mechanism for embedded implants via feedback)

- C2 server
- Human operator

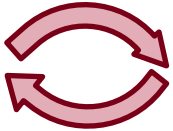
Command & Control



Feedback

- Human attacker
- Software implant

Command & Control



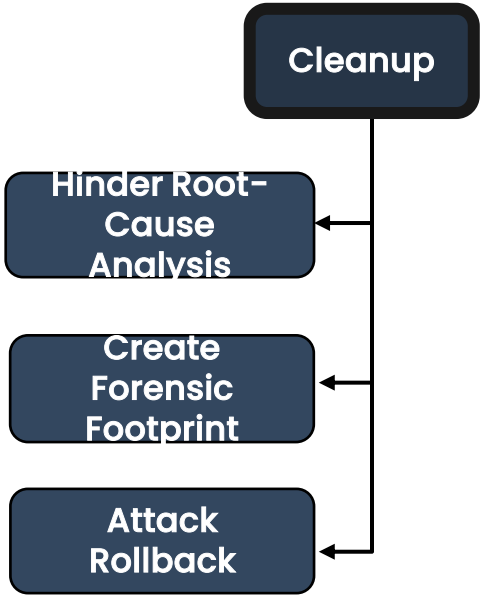
Feedback

- Field instrumentation
- (Other) implants

* CPS: Driving Cyber-Physical Systems to Unsafe Operating Conditions by Timing DoS Attacks on Sensor Signals – M. Krotofil et al.

Cleanup

- In IT domain it is possible to execute the entire attack without being ever detected. In CPS/OT domain it is not an option because of physical effect
  - One cannot “erase” changed physics
  - Cleanup is primarily focused on human operators & investigators
- During attack execution make operators believing “something else” is causing process upset
- Create forensic footprint of what the investigators should identify as cause of the incident/accident



Guided by the following questions:

What the attack should look like to external observers? How to avoid attribution to intentional actions? What the investigators should identify as the cause of the incident?

Preparation: Monitoring & Data Storage

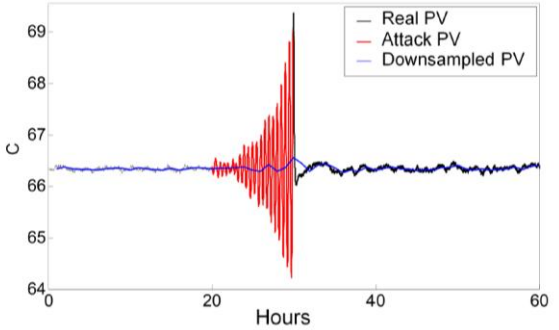
- Identify sources of process monitoring (e.g., HMIs) and potential data storage (e.g., historian, OPC server, SCADA database, etc.)

- Think of scenarios to create forensic confusion
  - Influence "recorded" timing of events (e.g., state Y changed before X)
  - Hide attack traces (e.g., filter out certain sensor signal frequencies)
  - Modify consistency of data across different sources
  - Present "wrong" process state on the HMI forcing operator to take "wrong" action (and become responsible for process upset), etc.
  - Avoid being "noticed" by the in-built anomaly detection algorithms

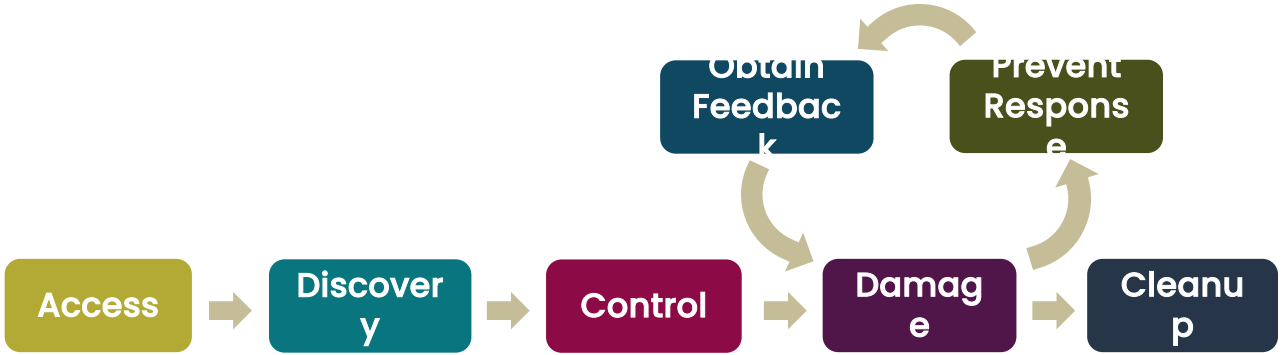
emerged. For example, in intermittent attacks, an attacker may control the width of the attack pulse to thwart the detection algorithm. Perhaps the most interesting outcome of these experiments was the realization that an attack launched on a sensor immediately prior to power outage, or immediately following power outage, is the most difficult to detect using invariant based approaches.■

SWaT: A Water Treatment Testbed for Research

Control loop oscillations are filtered out with a low-pass filter (through down sampling)



Cyber-Physical Attack Lifecycle



Access – Gaining entry to the target environment and supply chain for documentation and achieving code execution on assets

Discovery – Familiarizing with the environment through infrastructure reconnaissance and process comprehension

Control – Understanding dynamic process behavior, what and how much can be changed and achieving reliable control over process

Damage – Designing a detailed targeted damage scenario, developing and deploying cyber-physical exploits

Prevent Response – Preventing control/safety systems and operators from interfering with or interrupting attack execution

Obtain Feedback – Measuring or observing attack progress, coordinating exploits, detecting failure, registering success