ICS/OT/IIoT/IoT security: Introduction

Marina Krotofil

COINS summer school on Security Applications, Lesbos, Greece (online)
14-18.11.2021

About myself (1)

- **Current occupation:** Cyber Security Product Owner: Connected Vessels, Terminals and Warehouses at Maersk
- **Research specialization:** Offensive cyber-physical security in Critical Infrastructures and advanced defense methods

  Focus:

  - Physical damage or how to make something going bad, wrong, crash or blow up by means of cyber-attacks
  - Physical Process/application-aware defense methods

About myself (2)

- Ukrainian German who also worked in India/Netherlands/USA/UK
- Two engineering Masters and MBA , and *almost* PhD
- Previously worked as:
  - Senior Cyber Security Engineer at BASF (Germany)
  - Principal Analyst and Subject Matter Expert at FireEye (USA)
  - Lead Security Researcher at Honeywell (USA)
  - Senior Security Consultant at the European Network for Cyber Security (Netherlands)
  - Research assistant at Hamburg University of Technology (Germany) who had to teach
  - Telecommunication Engineer (Ukraine)

https://www.securityworldmarket.com/Renderers/showmedia.ashx?id=MediaArchive:74a0813e-4a67-40bf-9d68-9ff34

About myself (3)

- Member of the Black Hat Review Board
- Track Lead for Cyber-Physical Systems (CPS) security

A cyber-physical system (CPS) is any system where one, or more, computing elements monitor, manage and control a physical process. From wearable IoT devices to smart homes/buildings, from drones to self-driving vehicles, from Industrial Control Systems to avionics, these applications share common characteristics: the threat model relates to the physical process, the attacker goals are similarly linked to it, and both vulnerabilities and defence mechanisms need to encompass both the physical and the digital side of the systems. Talks in this track are directed at CPSs, either specific ones or on the concept as a whole, focusing on the systemic attacks and defences. Note that the purely cyber or data components research may fit better in other primary tracks such as Hardware/Embedded or AI

https://www.blackhat.com/html/tracks.html

Teaching objectives

- Introduction to ICS/OT/IIoT/IoT applications
- Emphasize the importance of taking specifics of the underlying application into consideration when considering cyber security aspects
- Keep applied focus
- Highlight relevant research questions
- Relevant summer school topics:
  - Risk assessment, threat modelling and cascading threats (IoT-enabled)
  - Introduction to Usable Security
  - Risk-Based Authentication
  - Reading Security Protocol Specifications is Difficult and Error Prone

Agenda

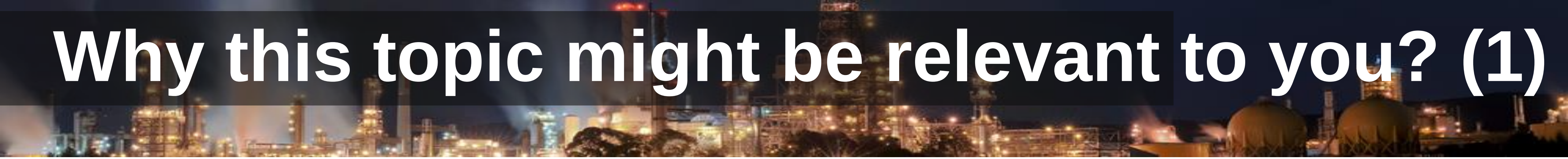
- **Part 1:** Introduction to ICS/OT/IIoT/IoT systems/applications. Intro to ICS/OT security and cyber-physical exploitation

- **Part 2:** Cyber-physical attack lifecycle. Use-case: Hacking chemical plant

- **Part 3:** OT/IoT network architectures. Cyber-Physical Systems (CPS)-specific attacks

- **Part 4:** OT vs. IT: Comparison of security and process monitoring approaches (SOC vs. Control Room)

https://www.securityworldmarket.com/Renderers/showmedia.ashx?id=MediaArchive:74a0813e-4a67-40bf-9d68-9ff34040f158



Why this topic might be relevant to you? (1)

- IoT systems becoming pervasive
- ICS/OT systems are transforming from proprietary and isolated to COTS and cloud-connected
- Pretty much any security area/specialization is or becoming relevant
  - Microsoft, Amazon, Intel, IBM, Tesla – big players in the field
- Example: Maersk – Cyber Security Platform

Automated/smart/connected terminals

Smart/connected vessels

Automated/smart/connected warehouses

Why this topic might be relevant to you? (1)

- IoT systems becomi
- ICS/OT systems are d to COTS and cloud-connecte
- Pretty much any sec levant
  - Microsoft, Amazon,
- Example: Maersk –

https://www.clydeco.com/en/insights/2020/12/casualty-update-one-apus

Automated/smart/connected terminals

Smart/connected vessels

Automated/smart/connected warehouses

Why this topic might be relevant to you? (1)

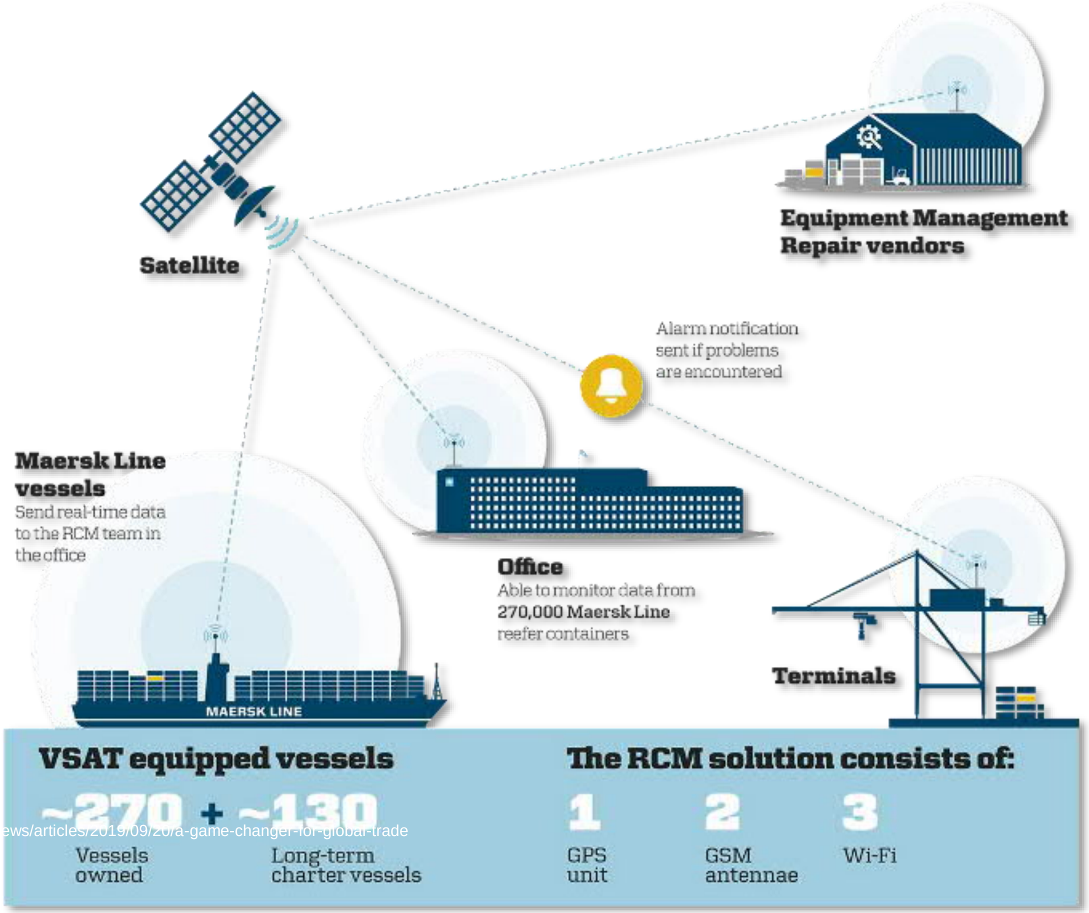
- IoT systems becoming pervasive
- ICS/OT systems are transforming from proprietary and isolated to COTS and cloud-connected
- Pretty much any security area/specialization is or becoming relevant
  - Microsoft, Amazon, Intel, IBM, Tesla – big players in the field
- Example: Maersk – Cyber Security Platform

Automated/smart/connected terminals

Smart/connected vessels

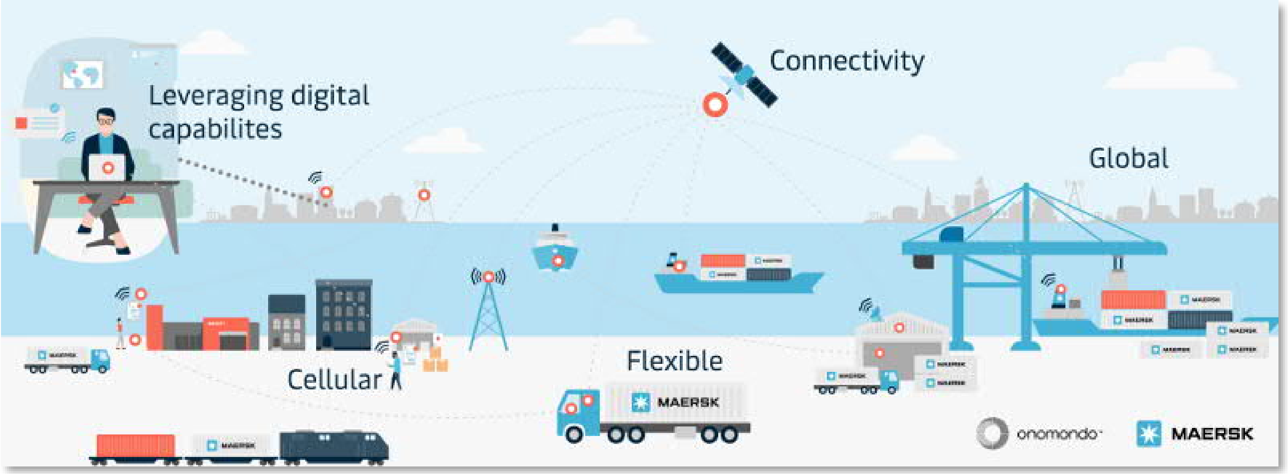
Automated/smart/connected warehouses

IoT-enabled business

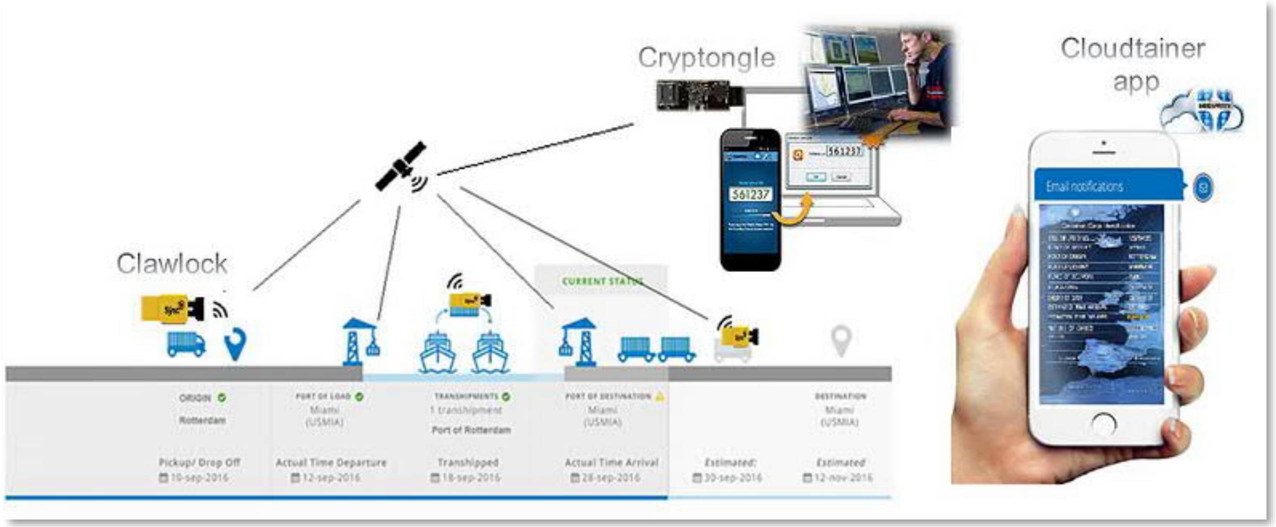

Satellite
Equipment Management Repair vendors
Alarm notification sent if problems are encountered
Maersk Line vessels
Send real-time data to the RCM team in the office
Office
Able to monitor data from 270,000 Maersk Line reefer containers
Terminals
MAERSK LINE
VSAT equipped vessels
~270 + ~130
Vessels owned
Long-term charter vessels
The RCM solution consists of:
1
GPS unit
2
GSM antennae
3
Wi-Fi

ews/articles/2019/09/20/a-game-changer-for-global-trade

https://digital.hbs.edu/platform-rctom/submission/maersk-reinventing-the-shipping-industry-using-iot-and-blockchain/



https://medium.com/maersk-growth/breaking-through-borders-our-partnership-with-onomondo-9543b03b7677



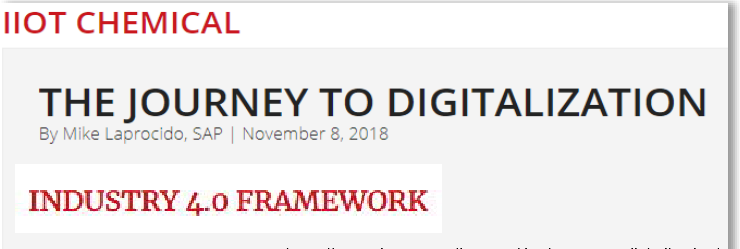
https://coins.newbium.com/post/18951-smart-containers-a-reliable-logistics-system

Why this topic might be relevant to you? (2)

Digitalization/ Digital Transformation is becoming #1 priority in all CPS domains/businesses

https://medium.com/swlh/digital-transformation-in-practice-showcasing-actionable-strategies-for-oems-on-autonomous-driving-31d412aad849

https://www.linkedin.com/pulse/digitalization-agriculture-suryakant-galav/



IIOT CHEMICAL

THE JOURNEY TO DIGITALIZATION

By Mike Laprocido, SAP | November 8, 2018

INDUSTRY 4.0 FRAMEWORK

https://www.chemengonline.com/the-journey-to-digitalization/

Digitalization: Welcome to the City 4.0

Home / Smart Cities, Buildings & Infrastructure / Smart Cities / Digitalization: Welcome to the City 4.0

September 20, 2019 Smart Cities, Smart Cities, Buildings & Infrastructure

Stay connected!

https://iiot-world.com/smart-cities-buildings-infrastructure/smart-cities/digitalization-welcome-to-the-city-4-0/

Digitalization and the future of energy

https://www.dnv.com/power-renewables/themes/digitalization/index.html

An industry study that goes beyond the hype – to find out how to create value by combining digital technology, people and business strategy

Why this topic might be relevant to you? (2)

Digitalization/
Digital Transfor
becoming #1 pri
CPS domains/bu

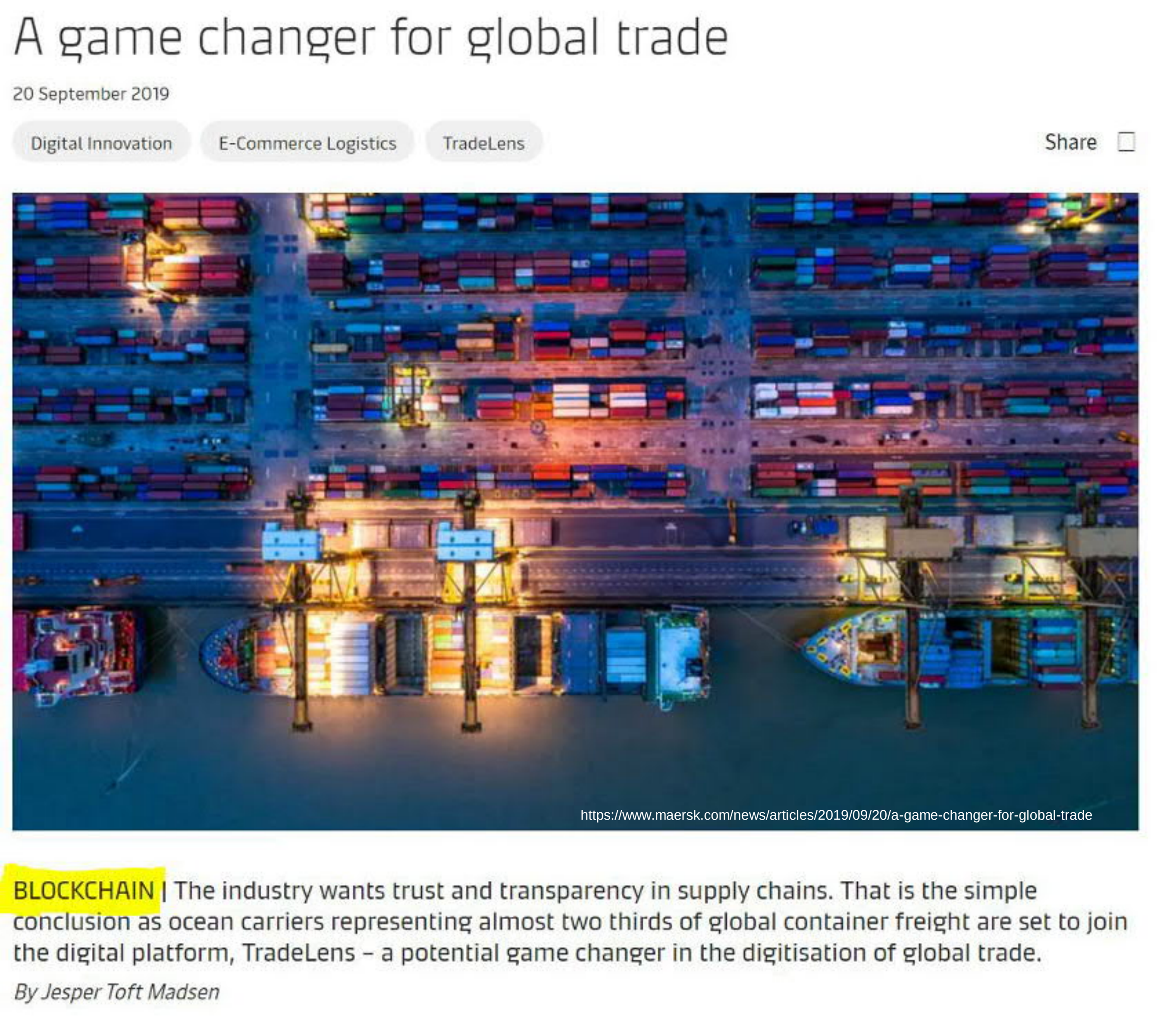
IIOT CHEMICAL

THE JOURNEY TO DIGIT

By Mike Laprocido, SAP | November 8, 2018

INDUSTRY 4.0 FRAMEWORK

https://www.chemengonline.c



A game changer for global trade

20 September 2019

Digital Innovation | E-Commerce Logistics | TradeLens

Share □

https://www.maersk.com/news/articles/2019/09/20/a-game-changer-for-global-trade

BLOCKCHAIN | The industry wants trust and transparency in supply chains. That is the simple conclusion as ocean carriers representing almost two thirds of global container freight are set to join the digital platform, TradeLens – a potential game changer in the digitisation of global trade.

By Jesper Toft Madsen

itaIization and the future of
rgy

wnloads

https://www.dnv.com/power-renewables/themes/digitalization/index.html

try study that goes beyond the hype – to find out how to
lue by combining digital technology, people and business

https://iiot-world.com/smart-cities-buildings-infrastructure/smart-cities/digitalization-welcome-to-the-city-4-0/

Introduction

Introduction to ICS/OT/IIoT/IoT

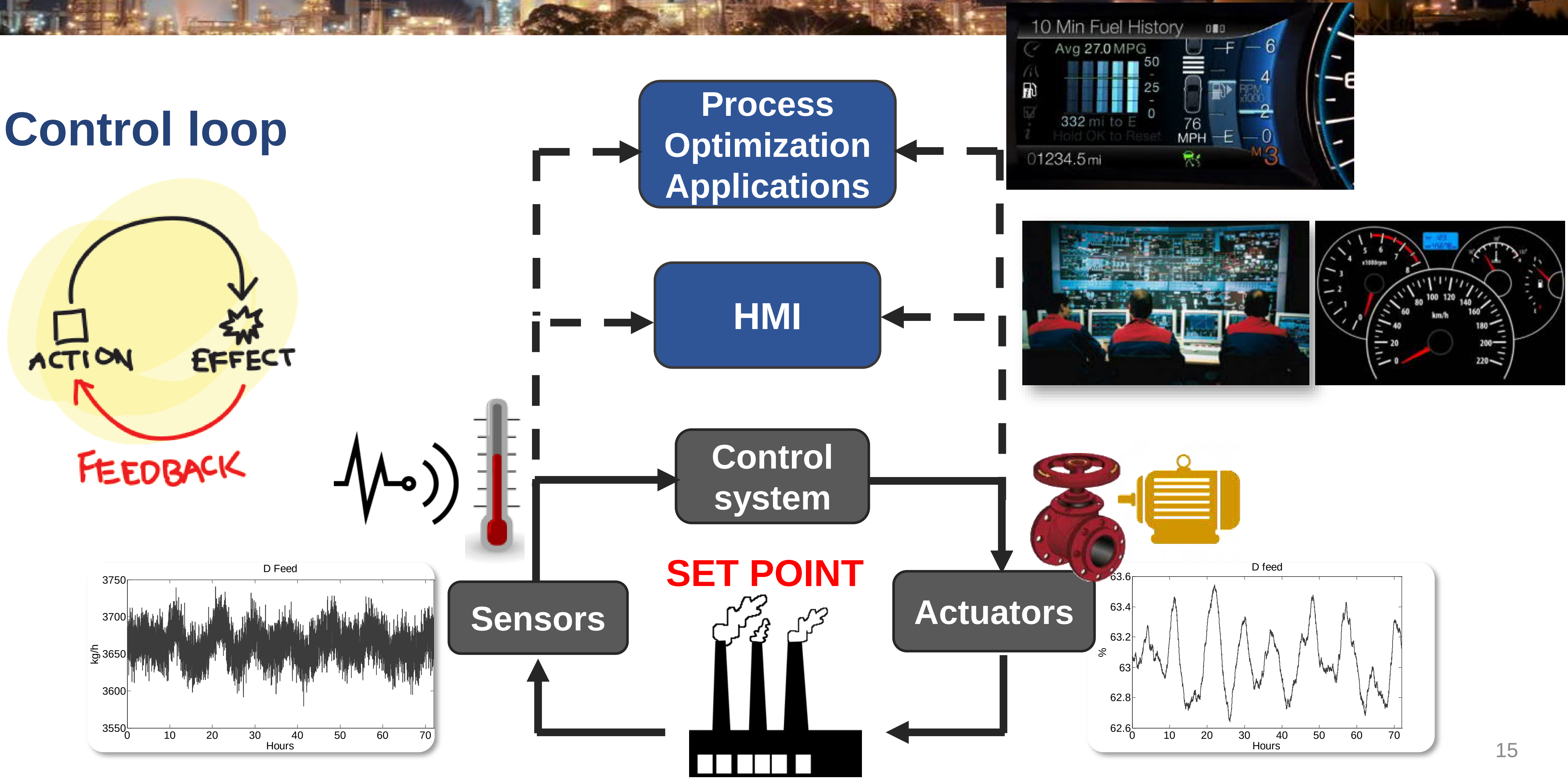
- **ICS/OT/IIoT** – types of CPS systems typically found in industrial environments **not directly** connected to the Internet
- **IoT** – a general type of CPS systems **directly** connected to the Internet

The architectures will be discussed tomorrow

- **ICS** – Industrial Control System
  - DCS – Distributed Control System
  - SCADA – Supervisory control and data acquisition
  - PCS – Process Control System
  - PLC – Programmable Logic Controller
- **OT** – Operational Technology
- **IIoT** – Industrial Internet of Things
- **IoT** – Internet of Things
  - Industrial / enterprise / consumer / wearable

Main concept behind CPS system

Control loop



OT/ICS applications

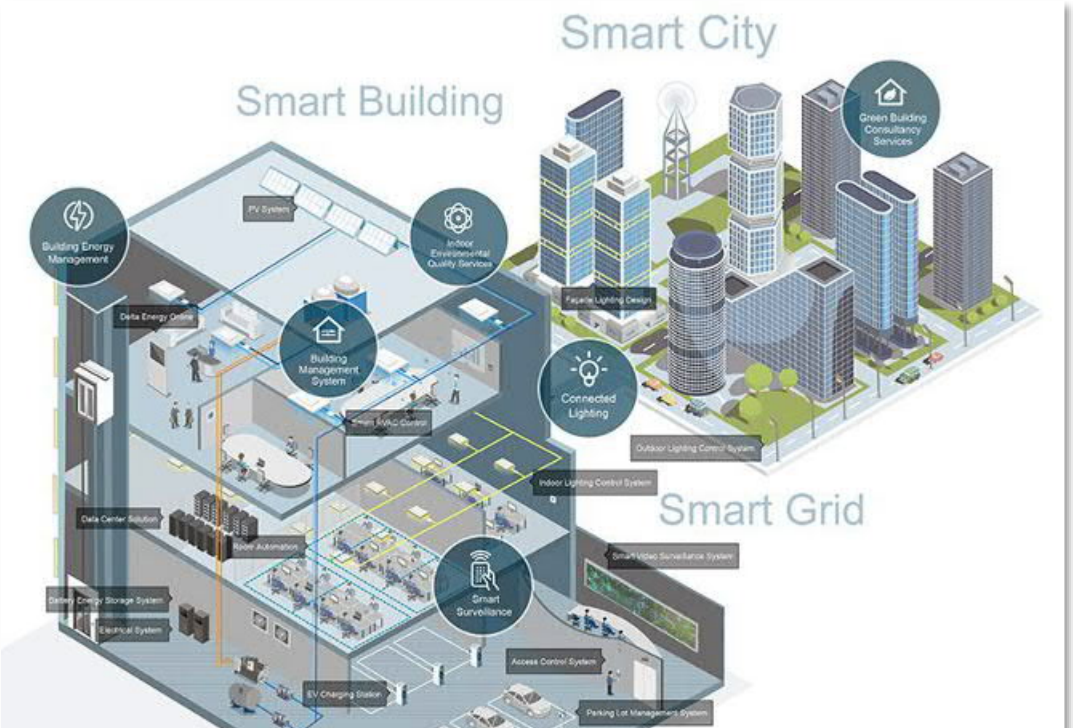
- Utilities, e.g., water and electricity supply
- (Petro)chemical sector
- Manufacturing sector (assembly lines, robots)
- Logistics
- Food industry
- Agriculture
- Etc., etc.

https://www.anttelecom.co.uk/blog/improve-communications-water-treatment

https://www.roboticsbusinessreview.com/manufacturing/7-key-robot-applications-in-automotive-manufacturing/

IoT applications

- Smart cities
- Building automation
- Vehicles/autonomous vehicles/UGVs
- Unmanned aerial vehicle (UAV) / drones
- Unmanned underwater vehicles (UUV)
- Lethal autonomous weapons
- Smart ships
- Consumer electronics/appliances
- Smart phones
- Wearable devices


Smart City
Smart Building
Green Building Consultancy Services
Building Energy Management
PV System
Indoor Environmental Quality Services
Facade Lighting Design
Delta Energy Online
Building Management System
Connected Lighting
Smart HVAC Control
Outdoor Lighting Control System
Indoor Lighting Control System
Data Center Solution
Room Automation
Smart Grid
Smart Video Surveillance System
Battery Energy Storage System
Smart Surveillance
Electrical System
Access Control System
EV Charging Station
Parking Lot Management System

https://deltaelectronicsindia.com/building-automation-solutions/

https://www.thedefensepost.com/2017/11/10/killer-robots-lethal-autonomous-weapons-systems-un/

One of the coolest CPS: Tesla car

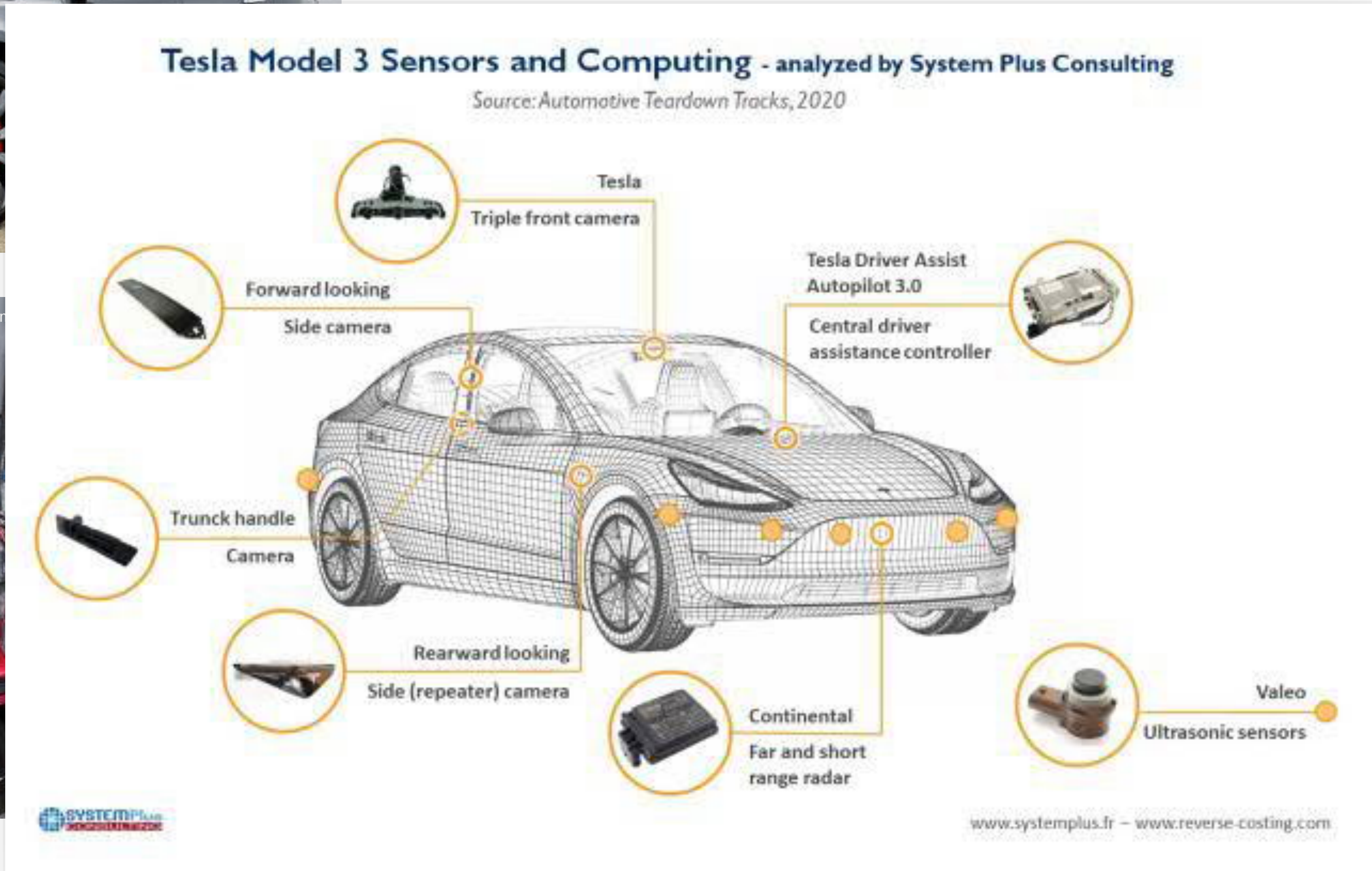
Tesla’s sensors: Autopilot system uses 8 cameras, 12 ultrasonic sensors & forward radar to read lane lines and detect nearby cars

https://www.popularmechanics.com/space/moon-mars/a16571489/elon-musk-space-tesla-mars/

One of the coolest CPS: Tesla car

Tesla’s sensors: Autopilot system uses 8 cameras, 12 ultrasonic sensors & forward radar to read lane lines and detect nearby cars

https://www.popularmechanics.com/space/moon-m



Tesla Model 3 Sensors and Computing - analyzed by System Plus Consulting

Source: Automotive Teardown Tracks, 2020

Introduction to ICS/OT/IIoT/IoT

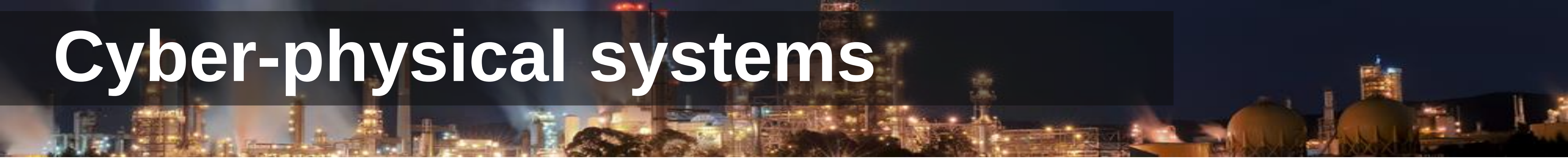
- **ICS/OT/IIoT** – types of CPS systems typically found in industrial environments not directly connected to the Internet
- **IoT** – a general type of CPS systems directly connected to the Internet

Focus of this year teaching block

- **ICS** – Industrial Control System
  - DCS – Distributed Control System
  - SCADA – Supervisory control and data acquisition
  - PCS – Process Control System
  - PLC – Programmable Logic Controller
- **OT** – Operational Technology
- **IIoT** – Industrial Internet of Things
- **IoT** – Internet of Things
  - Industrial / enterprise / consumer / wearable

Introduction

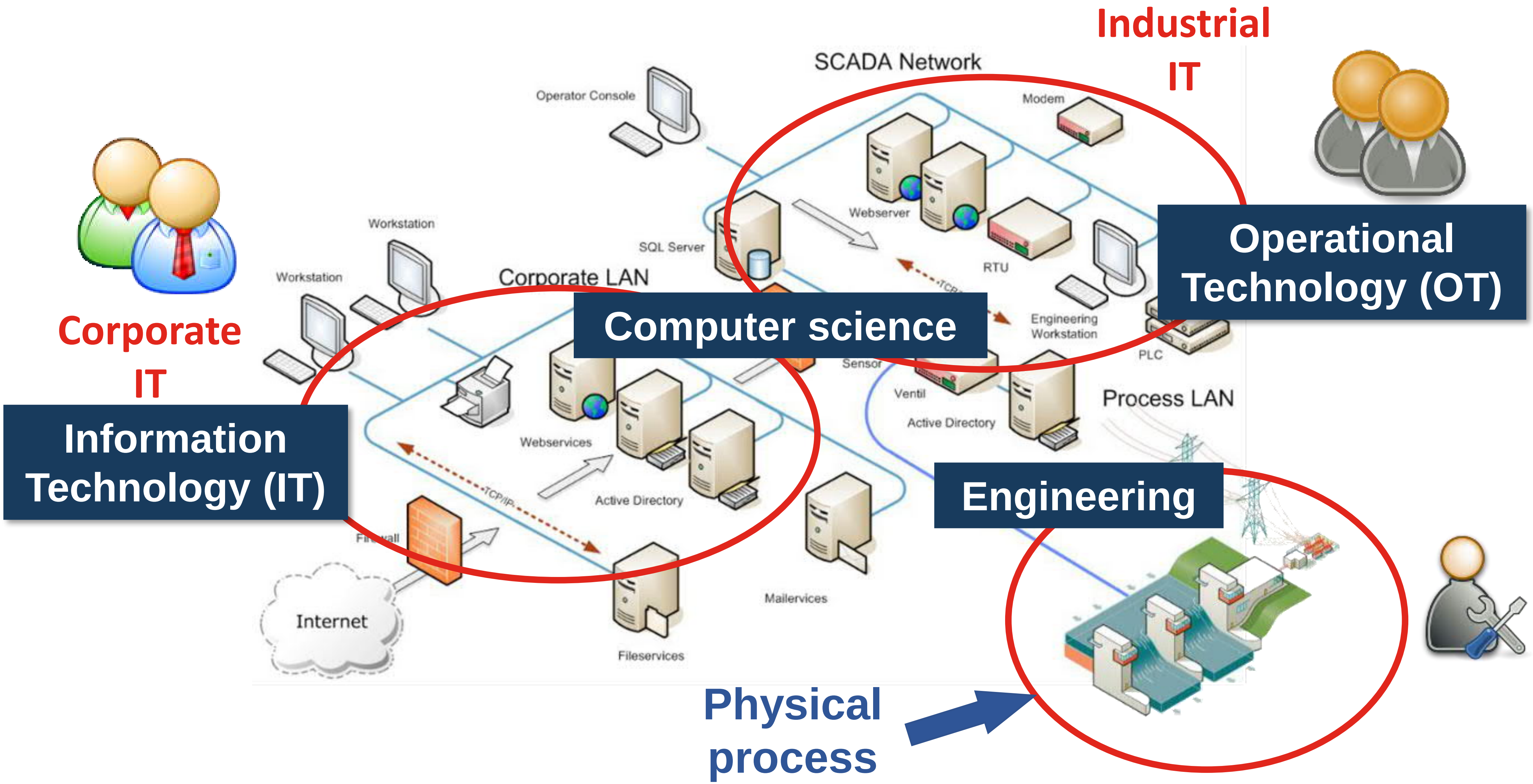
Use-case: Industrial plants



Cyber-physical systems

Cyber-physical systems are IT systems “embedded” in an application in the physical world

Typical ICS architecture



Industrial IT

Operational Technology (OT)

Corporate IT

Information Technology (IT)

Computer science

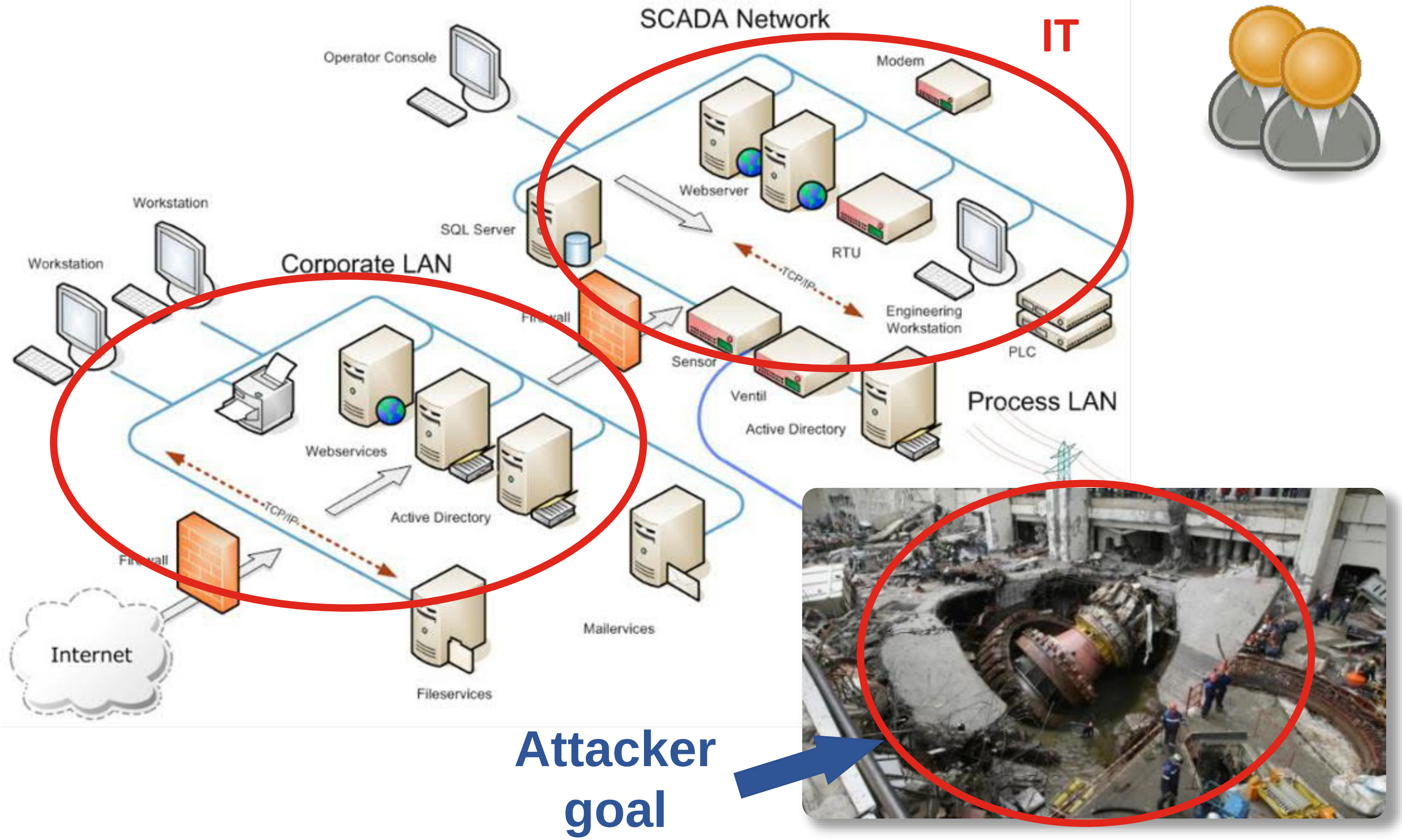
Engineering

Physical process

Attack goal considered in this module

Corporate IT

Industrial IT

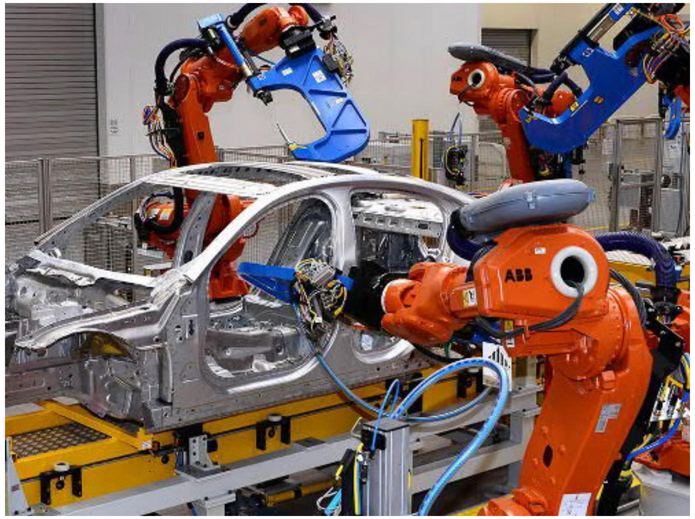


Attacker goal

Embedded ICS systems

https://vecer.mk/files/article/2017/05/02/485749-saudiska-arabija-ja-kupi-najgolemata-naftena-rafinerija-vo-sad.jpg

http://www.jfwhite.com/Collateral/Images/English-US/Galleries/middleboro9115kvbreakers.jpg



https://www.roboticsbusinessreview.com/wp-content/uploads/2016/05/jaguar-factory.jpg

https://www.oilandgasproductnews.com/files/slides/locale_image/medium/0089/22183_en_16f9d_8738_honeywell-process-solutions-rtu2020-process-controller.jpg

https://selinc.com/uploadedImages/Web/Videos/Playlists/Playlist_RTAC_1280x720.png?n=63584758126000

http://www02.abb.com/global/seitp/seitp202.nsf/0/0601d25ed243cfb0c1257d7e0043e50e/$file/7184_lvl2.jpg

Cyber-physical attack

PHYSICAL

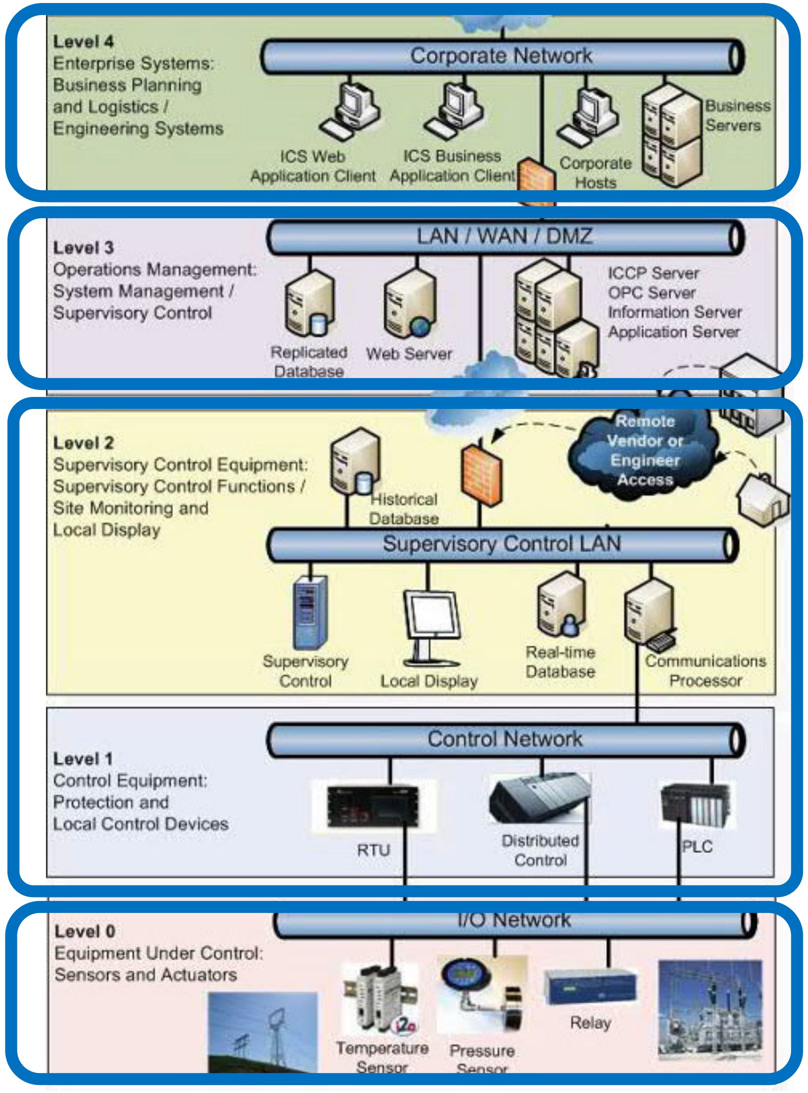
CYBER

https:

http://magazine.scientificmalaysian.com/wp-content/uploads/2013/12/Oil-refinery-explosion.png

Purdue network reference architecture

Main security standard: IEC-62443



Level 4
Enterprise Systems: Business Planning and Logistics / Engineering Systems
Corporate Network
ICS Web Application Client
ICS Business Application Client
Corporate Hosts
Business Servers
Level 3
Operations Management: System Management / Supervisory Control
LAN / WAN / DMZ
Replicated Database
Web Server
ICCP Server
OPC Server
Information Server
Application Server
Level 2
Supervisory Control Equipment: Supervisory Control Functions / Site Monitoring and Local Display
Historical Database
Remote Vendor or Engineer Access
Supervisory Control LAN
Supervisory Control
Local Display
Real-time Database
Communications Processor
Level 1
Control Equipment: Protection and Local Control Devices
Control Network
RTU
Distributed Control
PLC
Level 0
Equipment Under Control: Sensors and Actuators
I/O Network
Temperature Sensor
Pressure Sensor
Relay

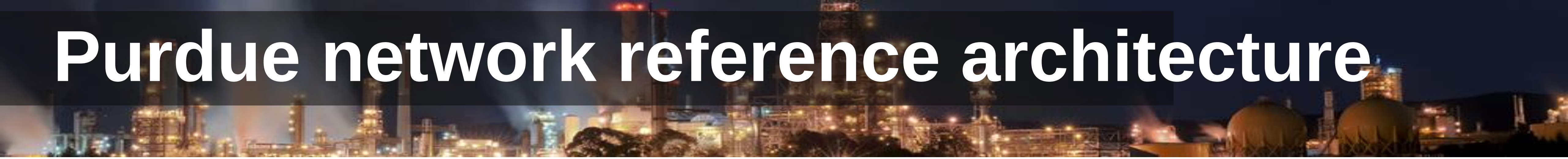
IT network

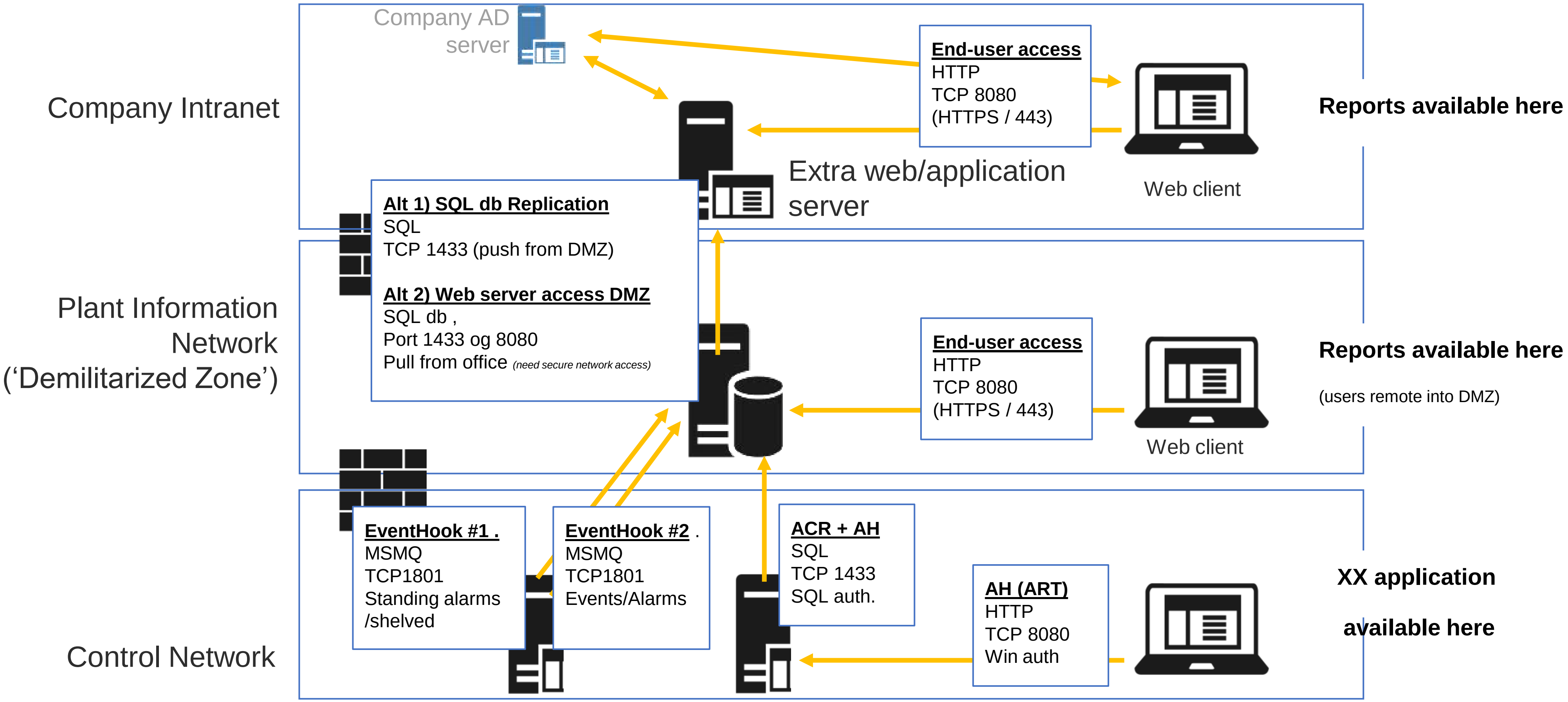
OT DMZ

OT network

Physical process

Purdue network reference architecture





Company Intranet

Company AD server

End-user access
HTTP
TCP 8080
(HTTPS / 443)

Web client

Reports available here

Extra web/application server

Alt 1) SQL db Replication
SQL
TCP 1433 (push from DMZ)

Alt 2) Web server access DMZ
SQL db ,
Port 1433 og 8080
Pull from office *(need secure network access)*

Plant Information Network (‘Demilitarized Zone’)

End-user access
HTTP
TCP 8080
(HTTPS / 443)

Web client

Reports available here

(users remote into DMZ)

Control Network

EventHook #1 .
MSMQ
TCP1801
Standing alarms /shelved

EventHook #2 .
MSMQ
TCP1801
Events/Alarms

ACR + AH
SQL
TCP 1433
SQL auth.

AH (ART)
HTTP
TCP 8080
Win auth

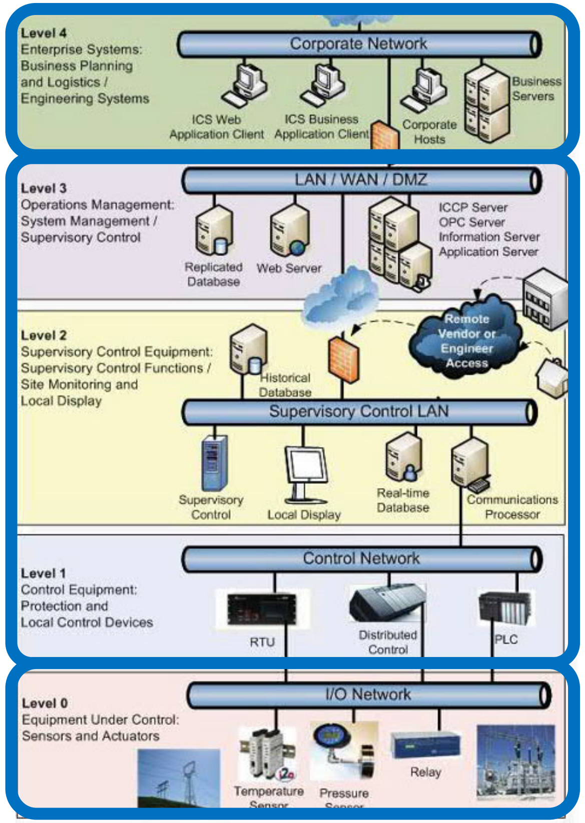
XX application

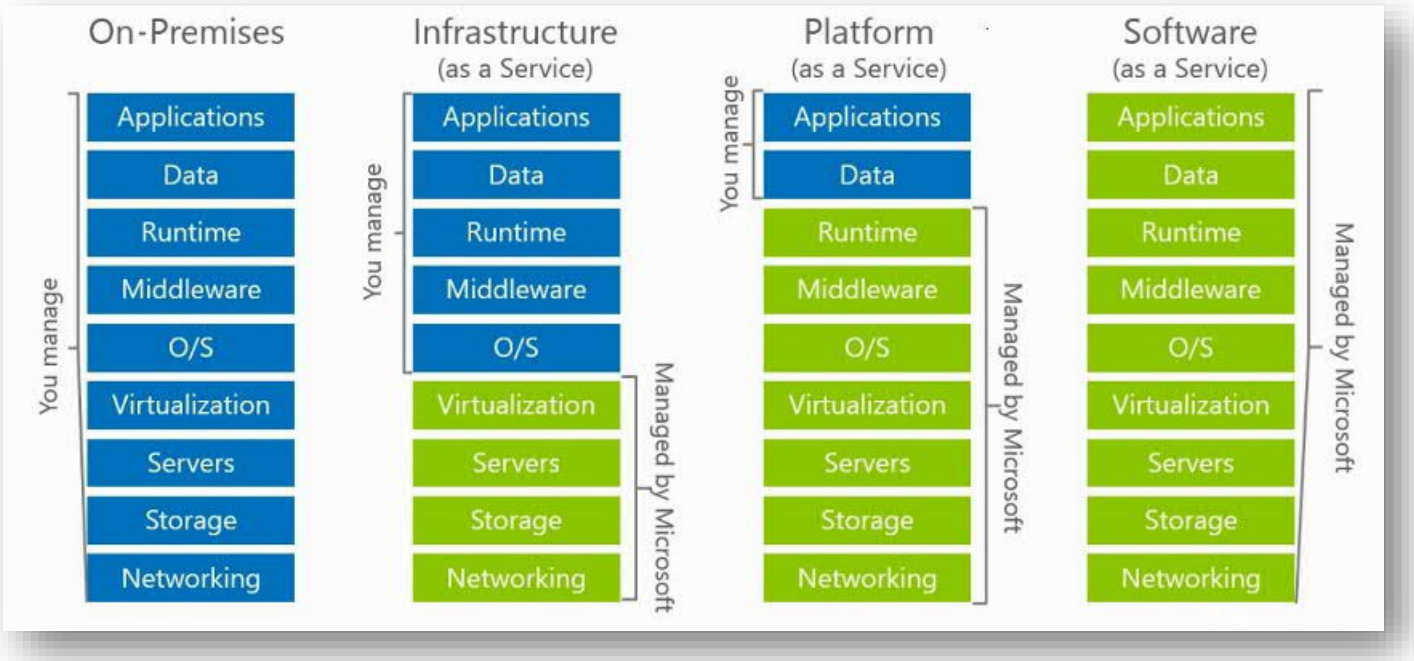
available here

Newly developed applications follow standard layered architecture

Purdue reference architecture: recent trends

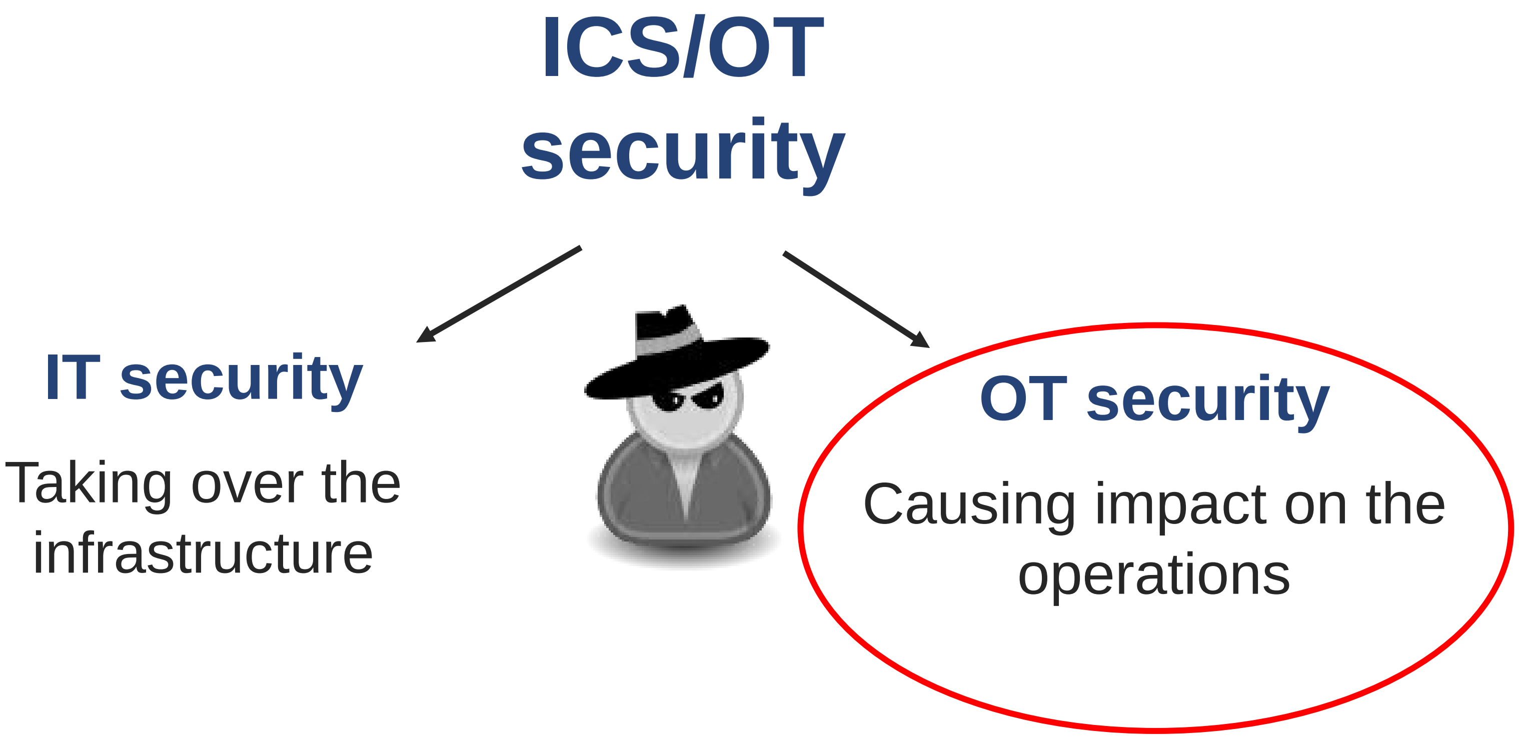
New trend: „Internet of Clouds“





On-Premises	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

ICS security



ICS/OT security

IT security

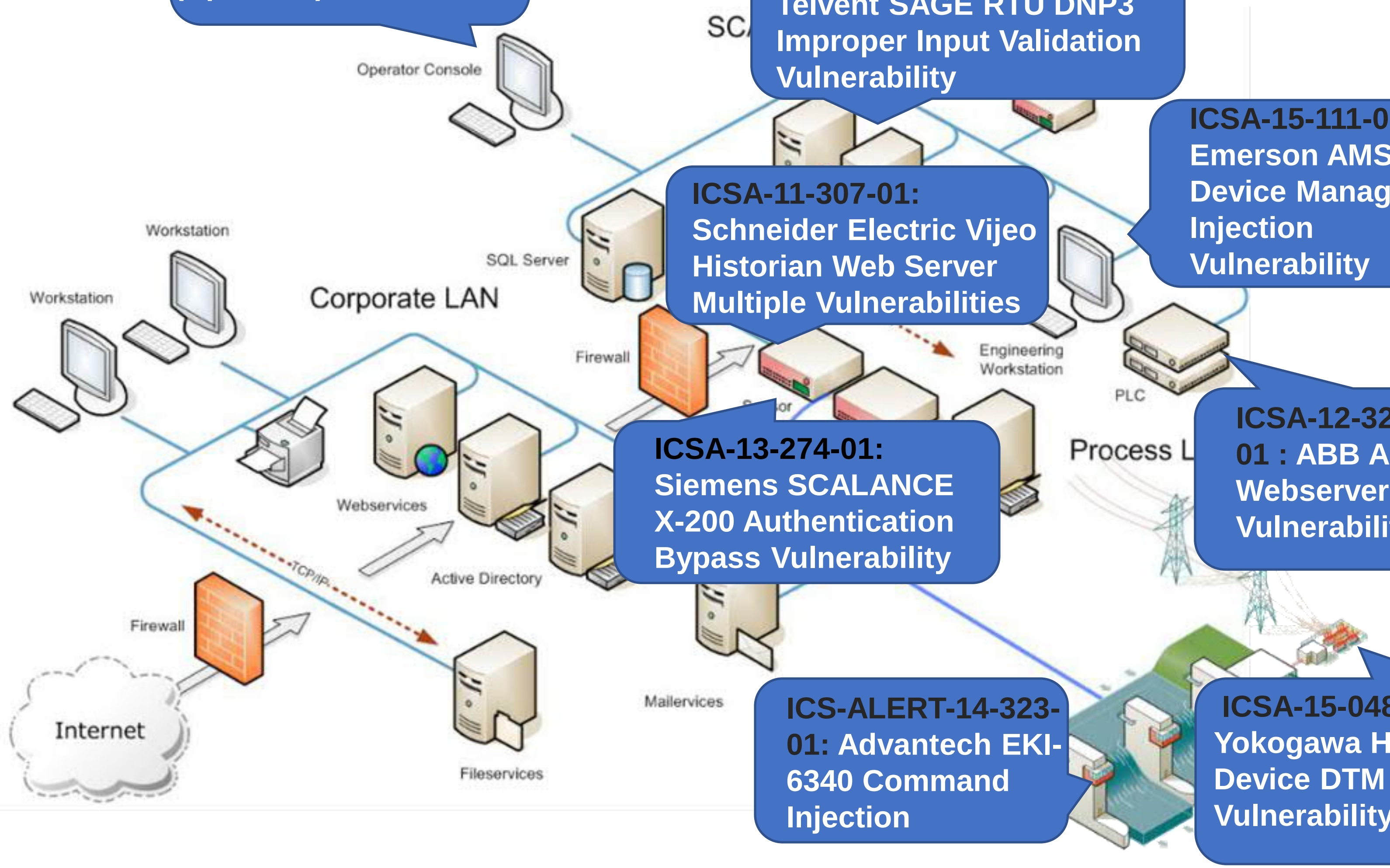
Taking over the infrastructure

OT security

Causing impact on the operations

Focus of this teaching module

Control equipment vulnerabilities



ICSA-15-099-01A: Siemens SIMATIC HMI Devices Vulnerabilities (Update A)

ICSA-13-274-01: Schneider Electric Telvent SAGE RTU DNP3 Improper Input Validation Vulnerability

ICSA-15-111-01: Emerson AMS Device Manager SQL Injection Vulnerability

ICSA-11-307-01: Schneider Electric Vijeo Historian Web Server Multiple Vulnerabilities

ICSA-13-274-01: Siemens SCALANCE X-200 Authentication Bypass Vulnerability

ICSA-12-320-01 : ABB AC500 PLC Webserver CoDeSys Vulnerability

ICS-ALERT-14-323-01: Advantech EKI-6340 Command Injection

ICSA-15-048-03: Yokogawa HART Device DTM Vulnerability

ICS-CERT advisory

ICSA-13-274-01: Siemens SCALANCE X-200 Authentication Bypass Vulnerability

IMPACT

Successful exploitation of this vulnerability **may allow attackers to perform administrative operations** over the network without authentication.

Impact to individual organizations depends on many factors that are unique to each organization*. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.*

Impact evaluation

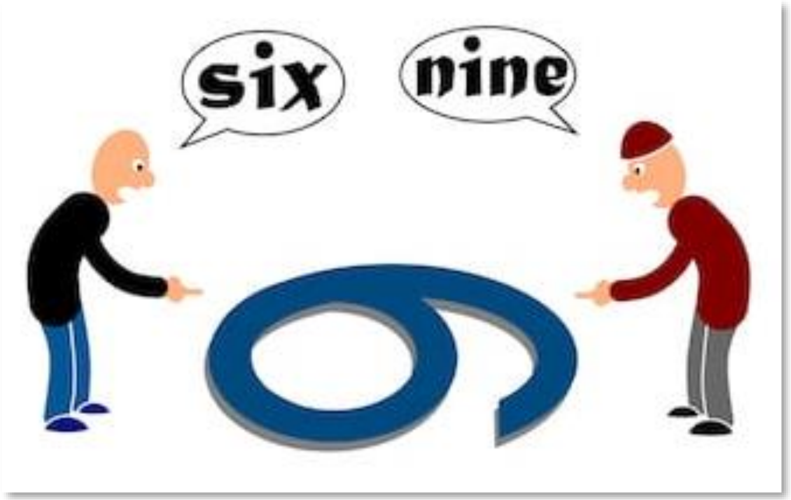
- What exactly the attacker can do with the vulnerability?
- Any further necessary conditions required?
- How severe the potential physical impact?

Answering these questions requires understanding how the attacker interacts with the control system and the process

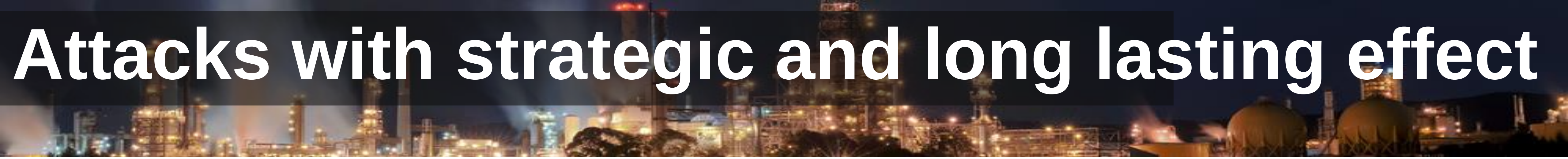
Two common views on cyber-physical attacks

- “Trivial! Look at the state of ICS security!”

- “Borderline impossible! These processes are extremely complex & engineered for safety!”



https://www.shutterstock.com/image-illustration/six-nine-matter-perspectives-1024980271



Attacks with strategic and long lasting effect

- Attacks with strategic, lasting damage will be process specific & require good process comprehension
- Wil require attacker to develop detailed ‘**damage scenario**’
  - What causes a pipeline to explode?
  - What causes the ***right*** pipeline to explode?
  - What causes the ***right*** pipeline to explode at the ***right*** moment?

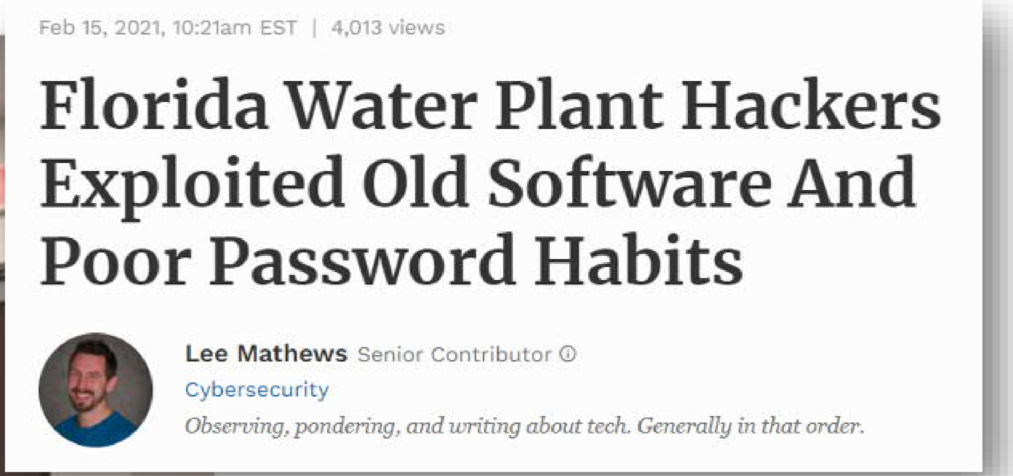
Magic “damage” button

(does not exist!)

Recent attack on water treatment utility

Treatment Plant Intrusion Press Conference

https://www.youtube.com/watch?v=MkXDSOgLQ6M



Feb 15, 2021, 10:21am EST | 4,013 views

Florida Water Plant Hackers Exploited Old Software And Poor Password Habits

Lee Mathews Senior Contributor ⓘ

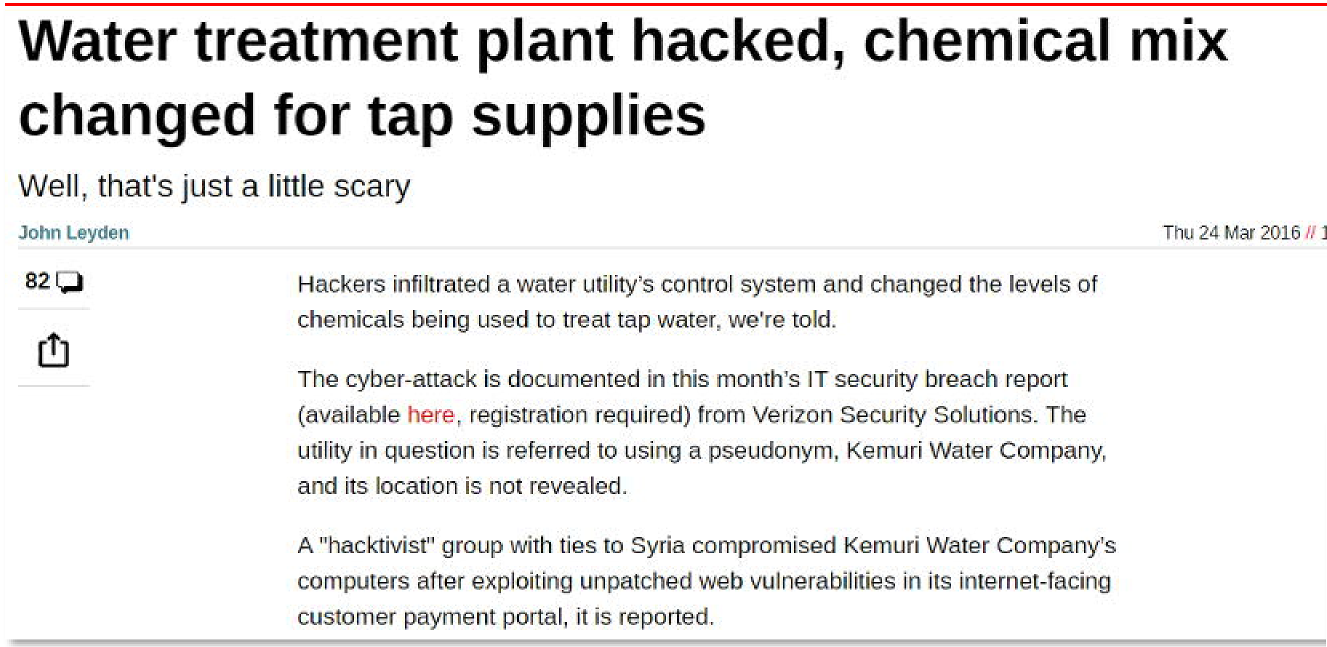
Cybersecurity

Observing, pondering, and writing about tech. Generally in that order.

Forbes

Changes done by the attacker were quickly reverted

Similar but less known incident in 2016



Water treatment plant hacked, chemical mix changed for tap supplies

Well, that's just a little scary

John Leyden

Thu 24 Mar 2016 // 12:19 UTC

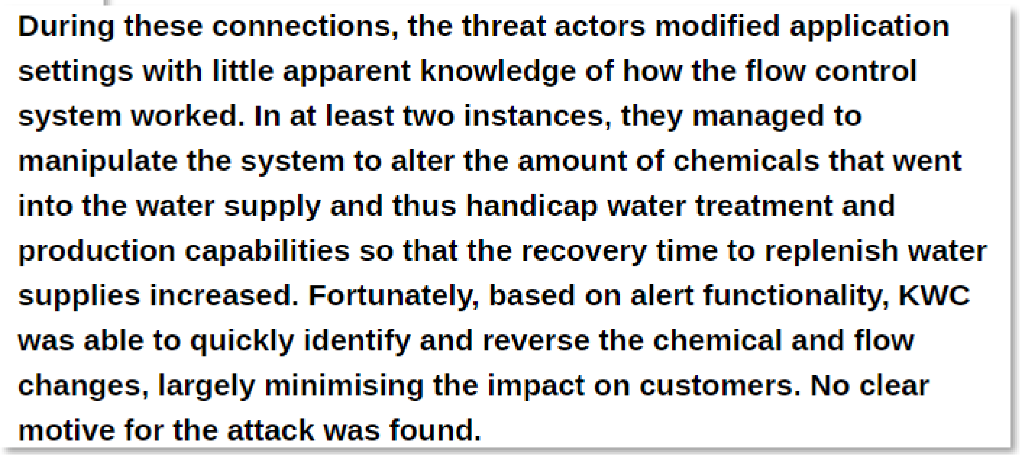
82

Hackers infiltrated a water utility's control system and changed the levels of chemicals being used to treat tap water, we're told.

The cyber-attack is documented in this month's IT security breach report (available here, registration required) from Verizon Security Solutions. The utility in question is referred to using a pseudonym, Kemuri Water Company, and its location is not revealed.

A "hacktivist" group with ties to Syria compromised Kemuri Water Company's computers after exploiting unpatched web vulnerabilities in its internet-facing customer payment portal, it is reported.

https://www.theregister.com/2016/03/24/water_utility_hacked/



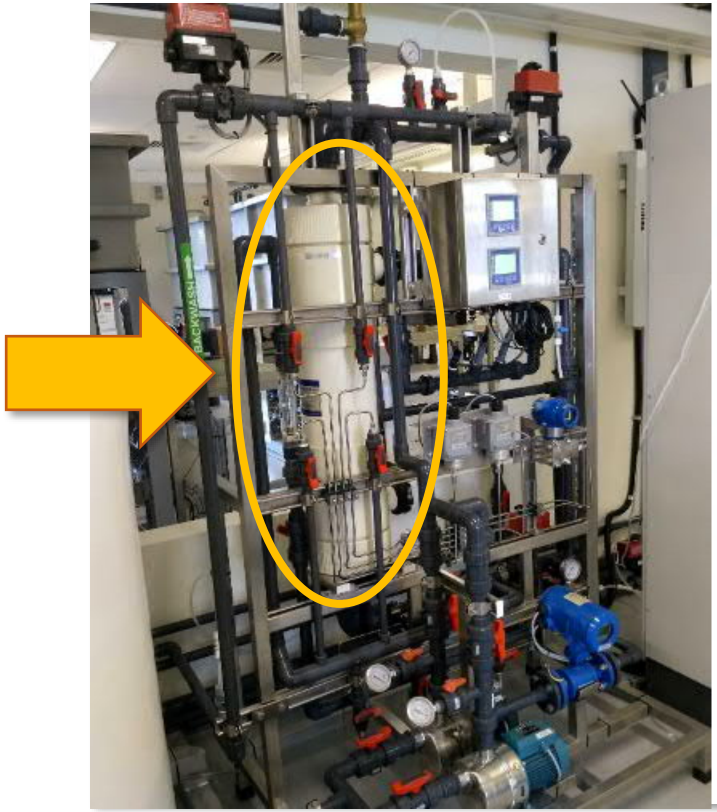
During these connections, the threat actors modified application settings with little apparent knowledge of how the flow control system worked. In at least two instances, they managed to manipulate the system to alter the amount of chemicals that went into the water supply and thus handicap water treatment and production capabilities so that the recovery time to replenish water supplies increased. Fortunately, based on alert functionality, KWC was able to quickly identify and reverse the chemical and flow changes, largely minimising the impact on customers. No clear motive for the attack was found.

An attacker with an objective beyond simple mayhem will need a strategic damage scenario

Damaging UF filter in water utility

- For prolonged effect target key equipment

Acknowledgement:
iTRUST Research Center, SUTD, Singapore for kindly conducting this experiment on request



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

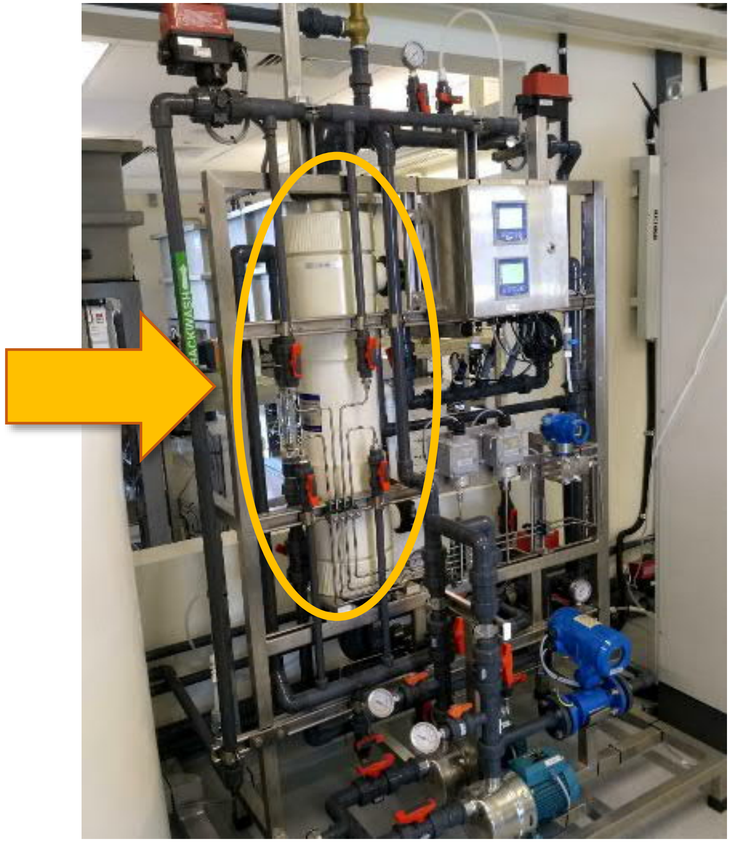
Use Case: Killing UF filter in water treatment facility

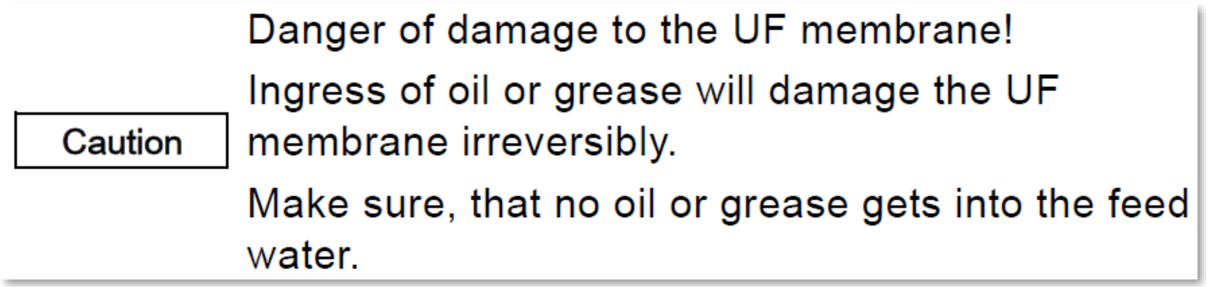
- Water treatment process consists of multiple stages, including several stages of filtering
  - Water filters are expensive
  - When broken, water supply is interrupted

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

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

Damaging UF filter in water utility



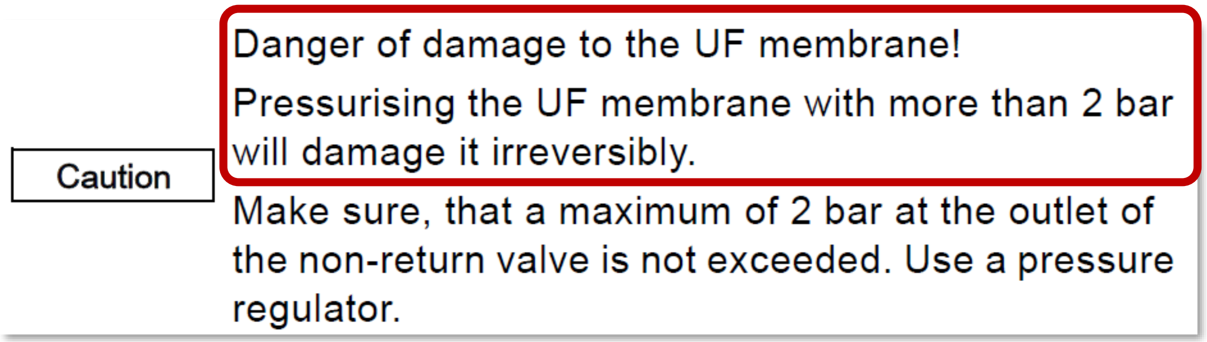


Caution

Danger of damage to the UF membrane!

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

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

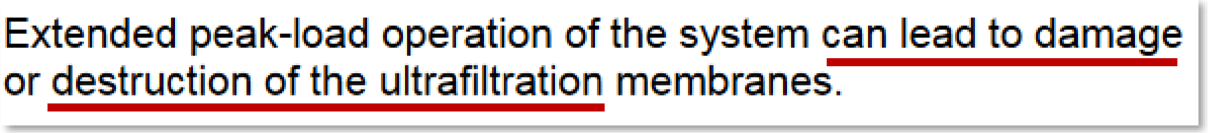


Caution

Danger of damage to the UF membrane!

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

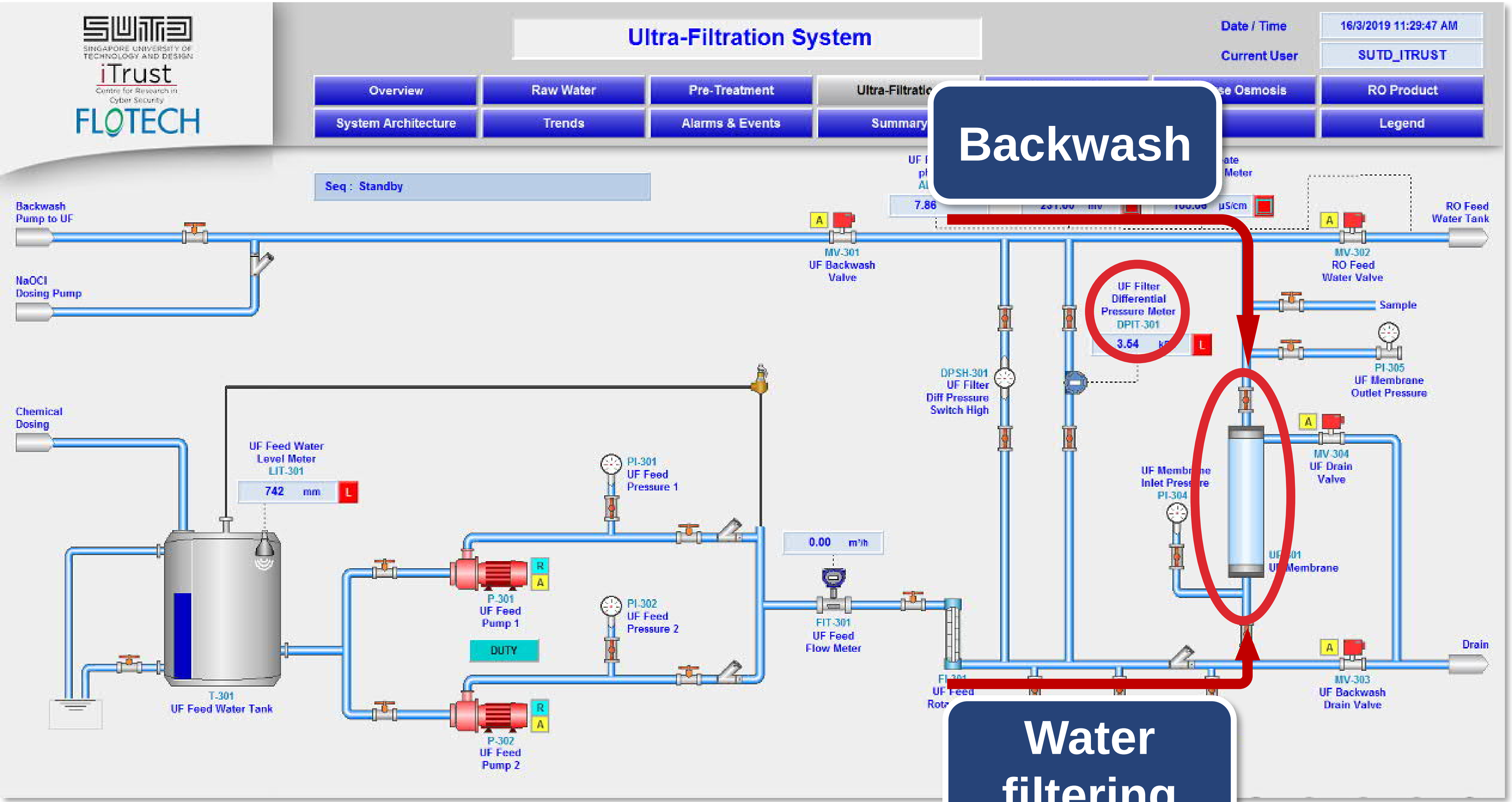
Make sure, that a maximum of 2 bar at the outlet of the non-return valve is not exceeded. Use a pressure regulator.



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

UF filtering: HMI screen



Ultra-Filtration System

Date / Time: 16/3/2019 11:29:47 AM

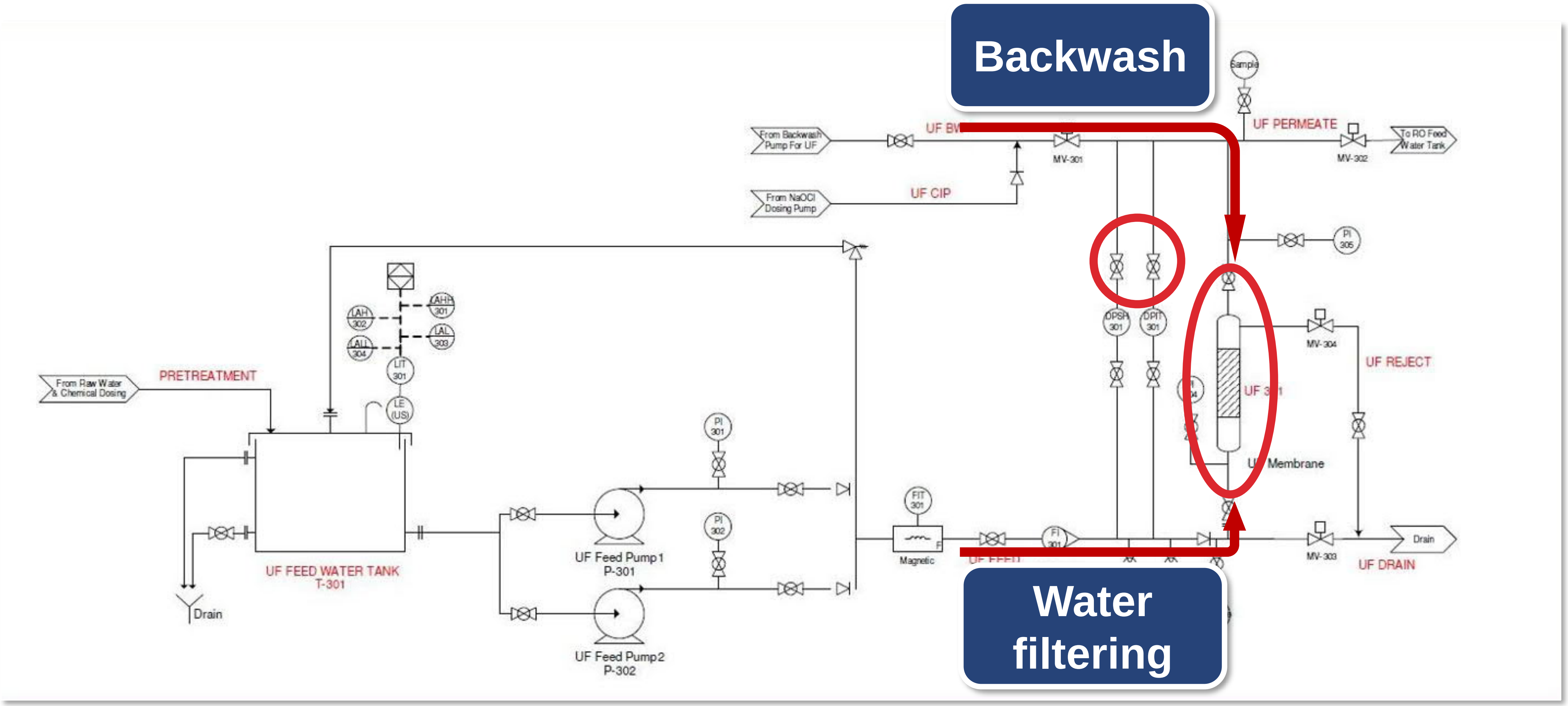
Current User: SUTD_ITRUST

Seq : Standby

Backwash

Water filtering

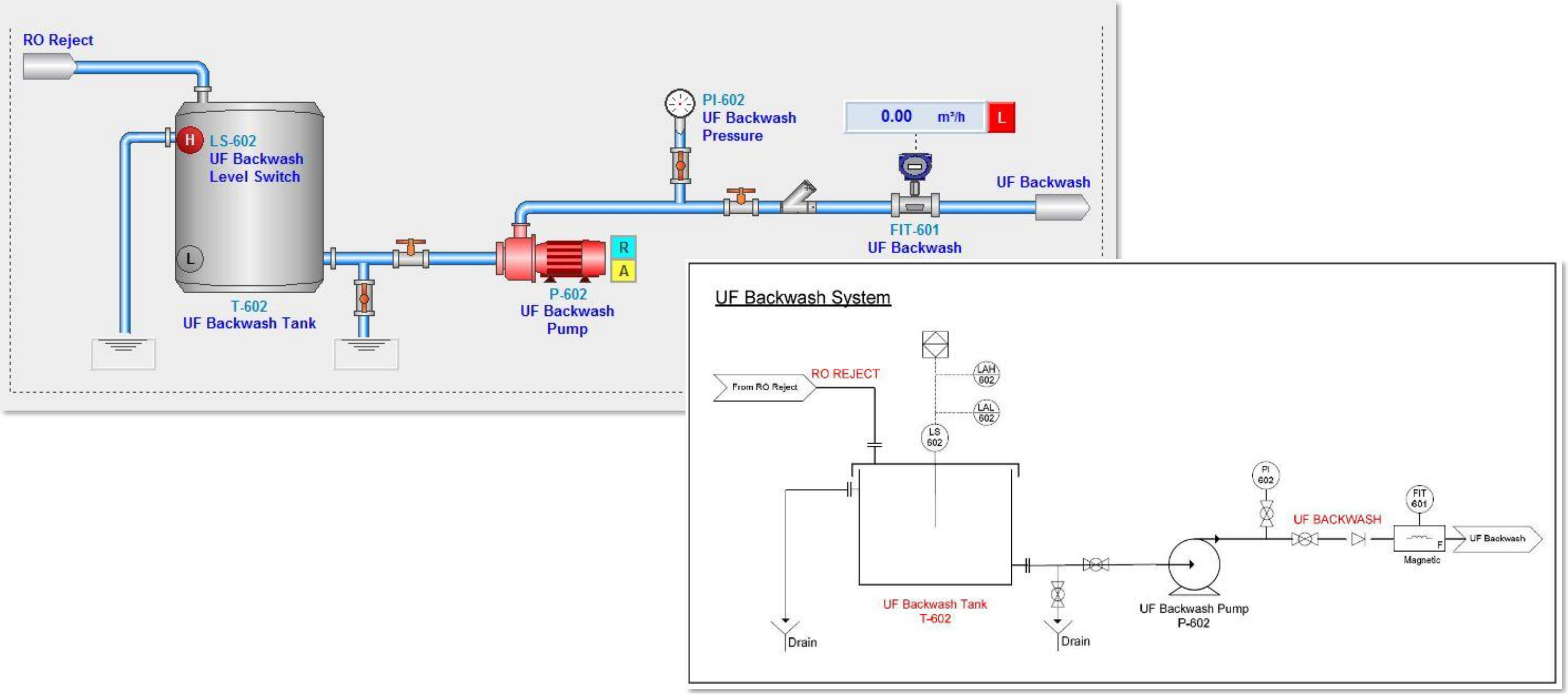
UF filtering: PI&D diagram

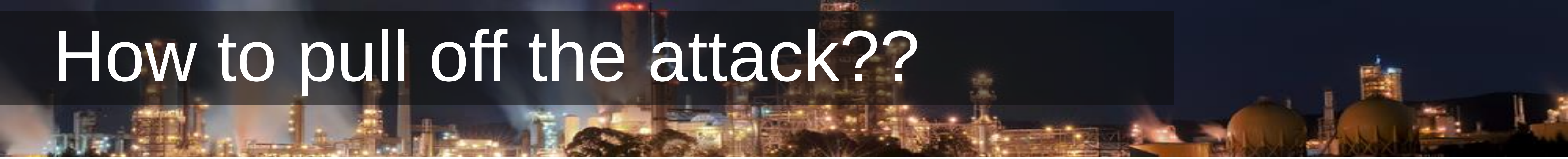


Backwash

Water filtering

UF backwash: HMI & PI&D diagram





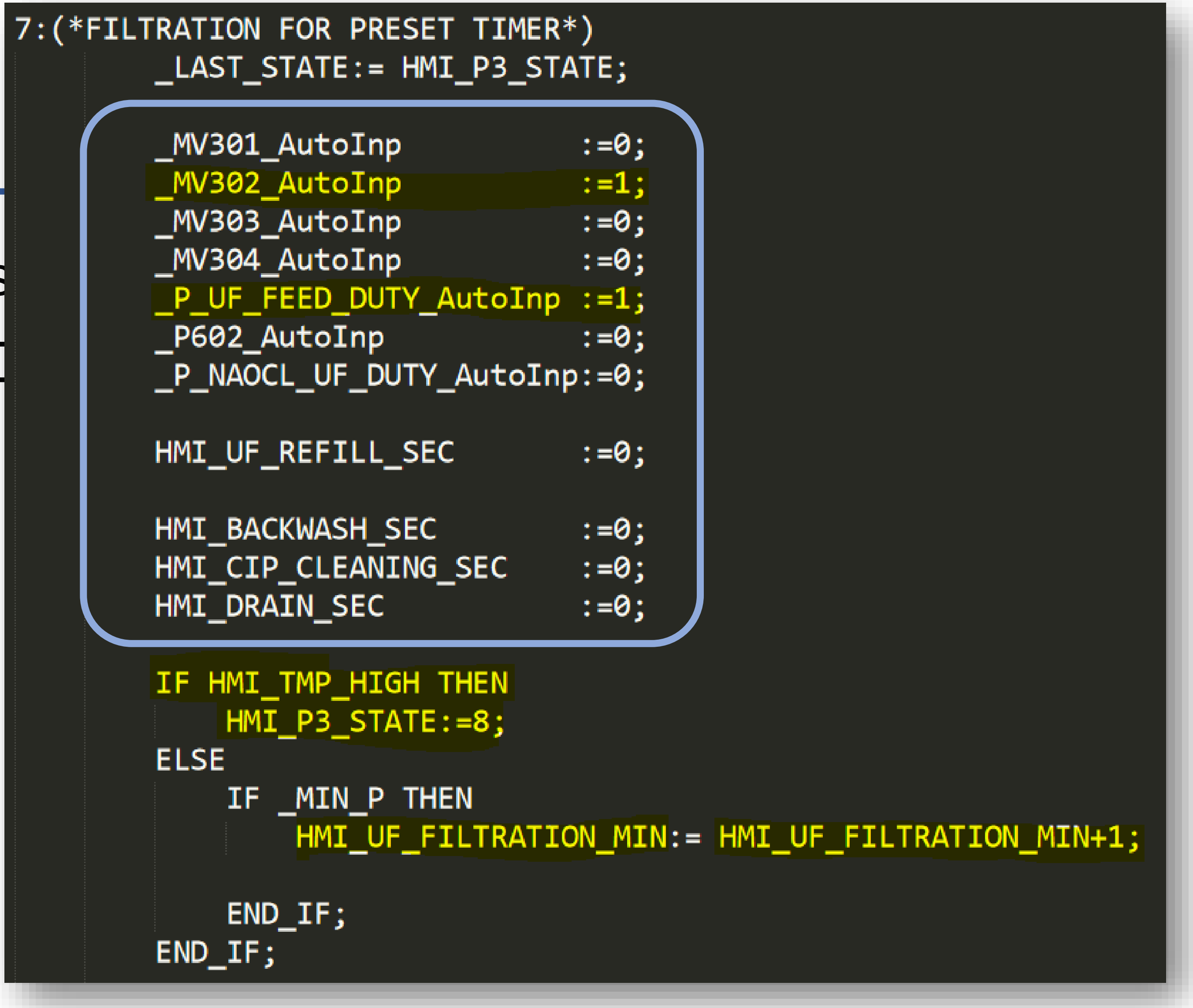
How to pull off the attack??

- There are tree conditions which can trigger backwash process, each **guided by a state machine in a PLC (controller):**
  - Preset timer (every 30 minutes)
  - UF filter differential pressure (DP) ≥ 40 kPa
  - Plant shutdown

How to pull off the attack??

- There are tree conditions which can **guided by a state machine in a PL**
  - Preset timer (every 30 minutes
  - UF filter differential pressure (D
  - Plant shutdown

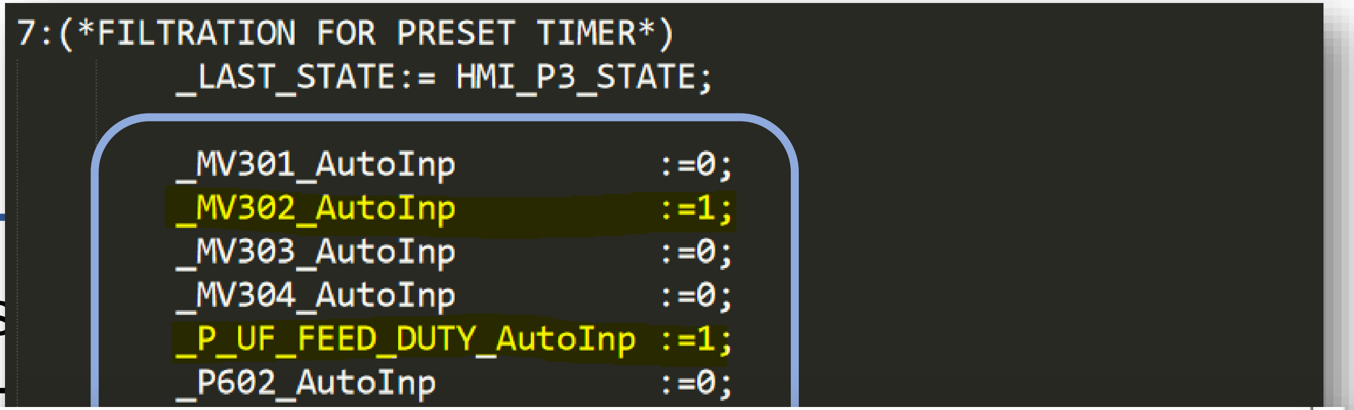
https://www.plc-city.com/shop/en/allen-bradley-controllogix-chassis/rockwell-1756-a4-nfs.html



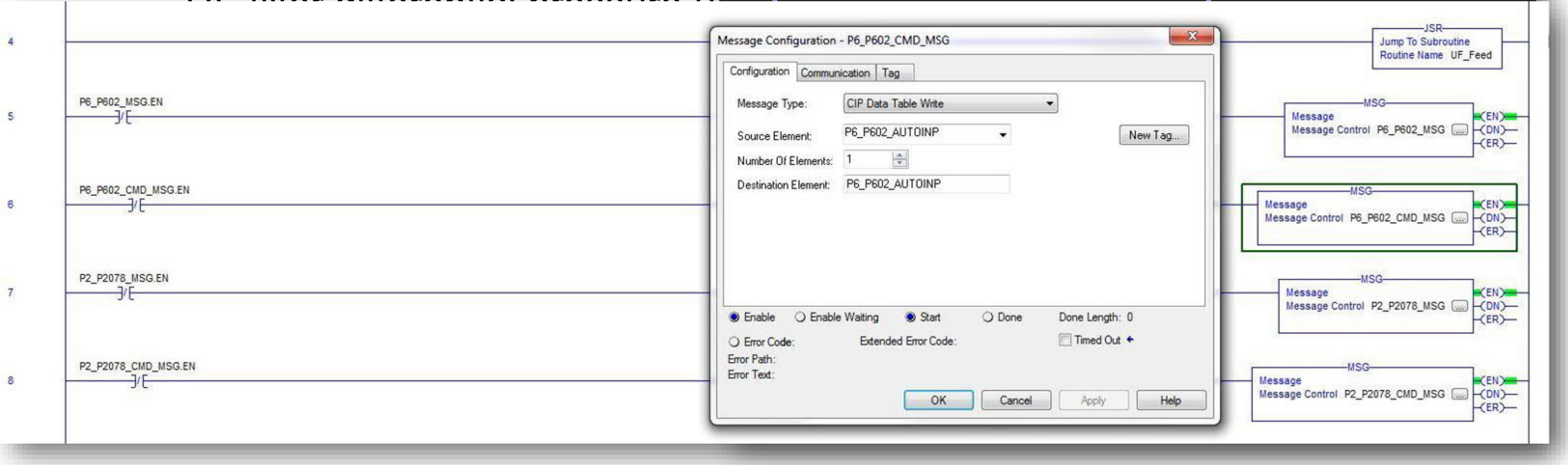
```
7:(*FILTRATION FOR PRESET TIMER*)
        _LAST_STATE:= HMI_P3_STATE;

        _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;
```

How to pull off the attack??

- There are tree conditions which can **guided by a state machine in a PL**
  - Preset timer (every 30 minutes
  - UF filter differential pressure (D



```
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;
```



Message Configuration - P6_P602_CMD_MSG

Configuration | Communication | Tag

Message Type: CIP Data Table Write

Source Element: P6_P602_AUTOINP

Number Of Elements: 1

Destination Element: P6_P602_AUTOINP

New Tag...

● Enable ○ Enable Waiting ● Start ○ Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out ←

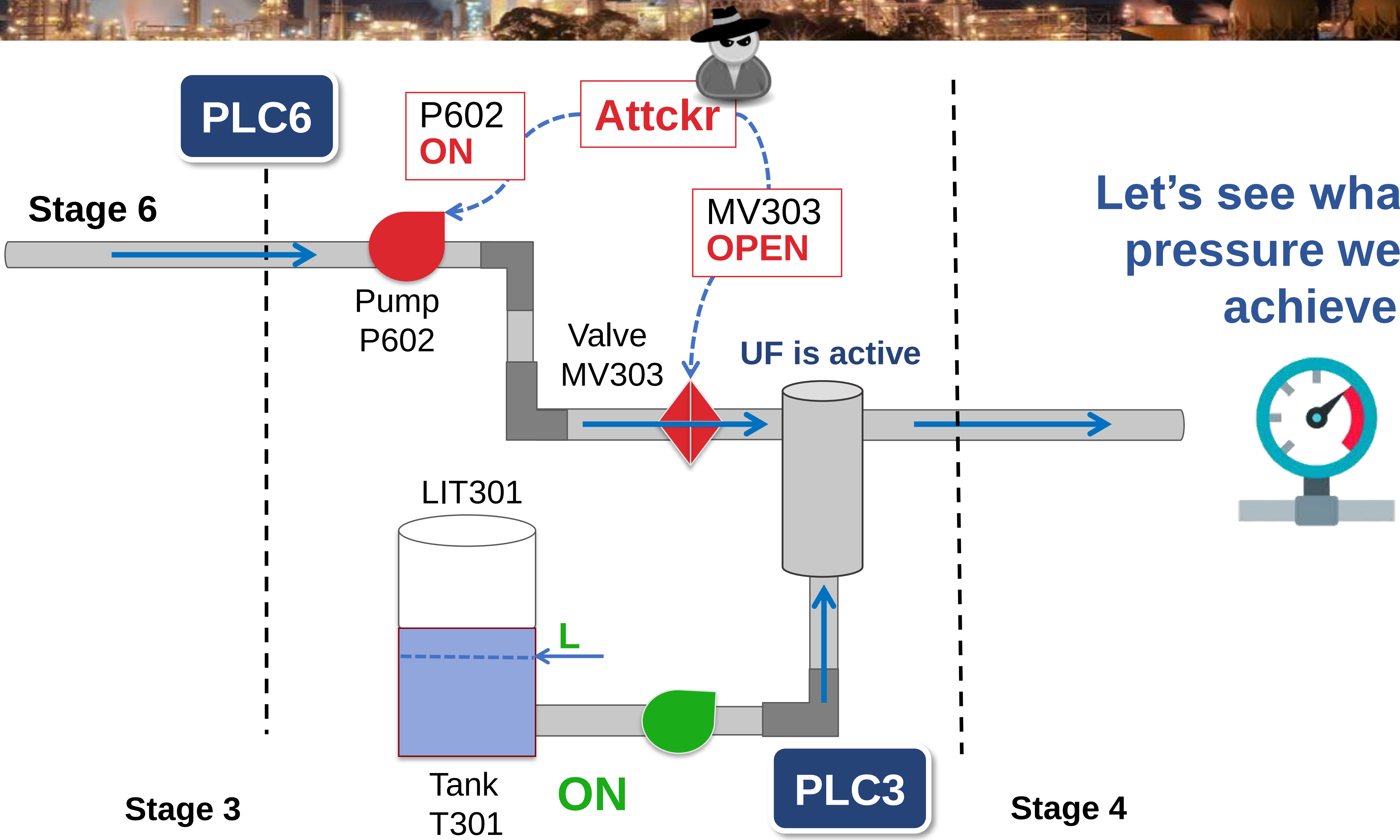
Error Path:

Error Text:

OK | Cancel | Apply | Help

```
4                                            JSR
                                             Jump To Subroutine
                                             Routine Name  UF_Feed
5  P6_P602_MSG.EN      ]/[                   MSG
                                             Message
                                             Message Control  P6_P602_MSG       (EN) (DN) (ER)
6  P6_P602_CMD_MSG.EN  ]/[                   MSG
                                             Message
                                             Message Control  P6_P602_CMD_MSG   (EN) (DN) (ER)
7  P2_P2078_MSG.EN     ]/[                   MSG
                                             Message
                                             Message Control  P2_P2078_MSG      (EN) (DN) (ER)
8  P2_P2078_CMD_MSG.EN ]/[                   MSG
                                             Message
                                             Message Control  P2_P2078_CMD_MSG  (EN) (DN) (ER)
```

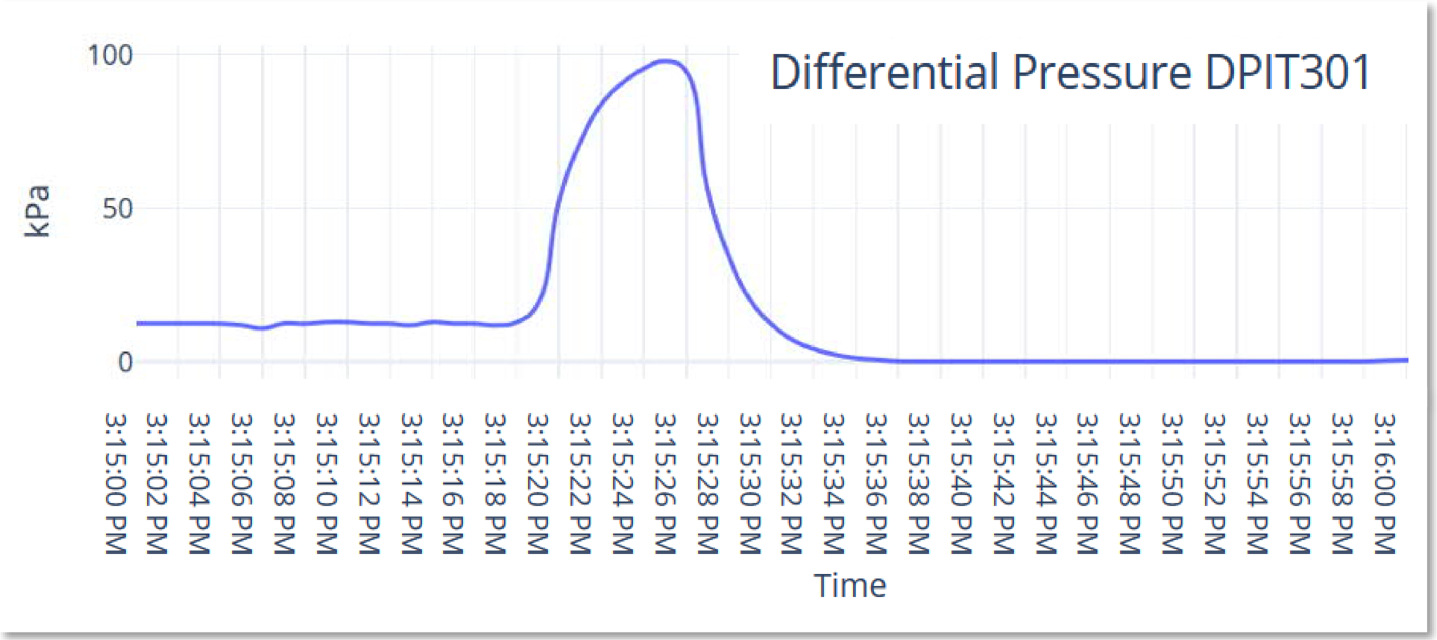
Execution of cyber attack



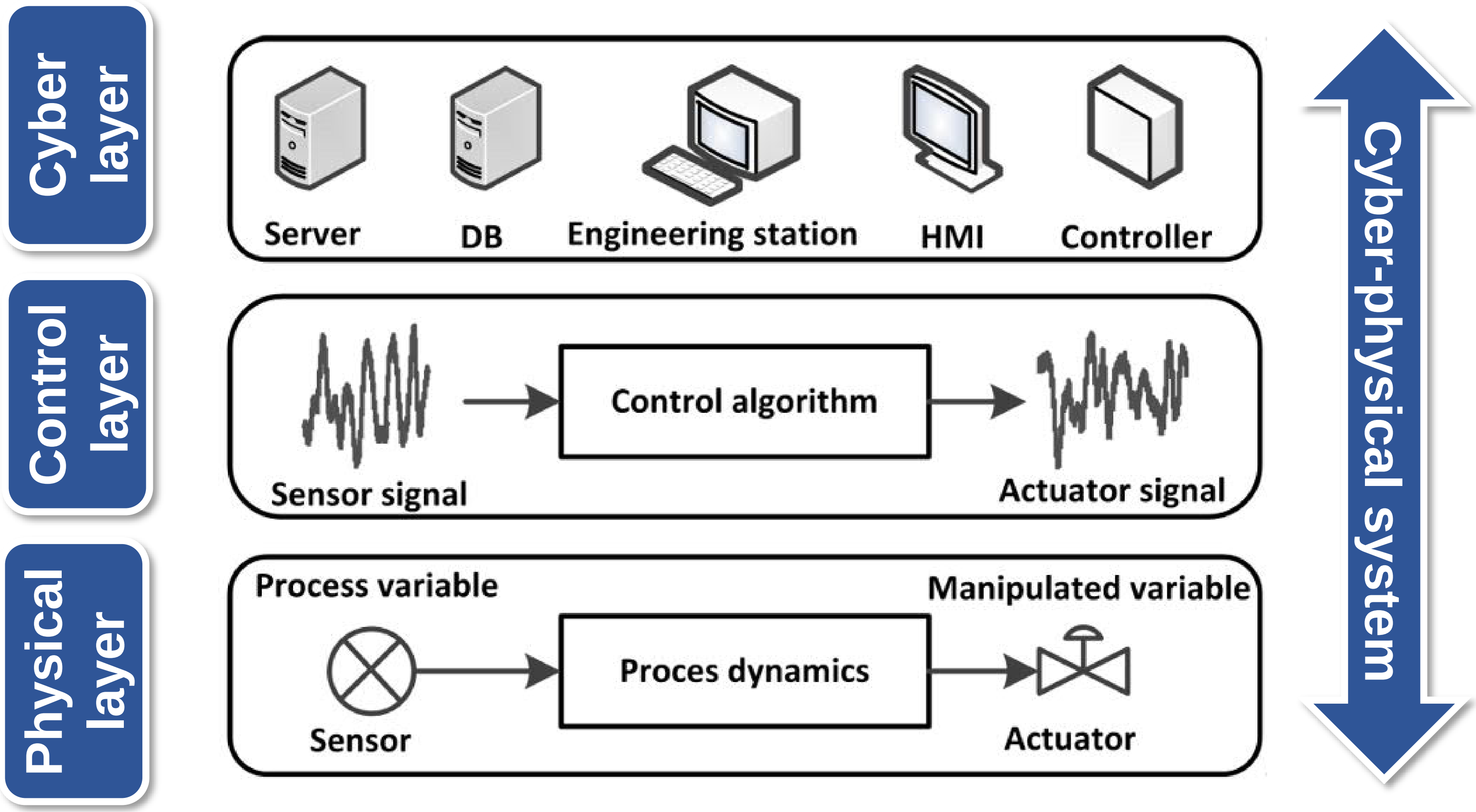
Let’s see what max pressure we can achieve

Surge attack on UF filter

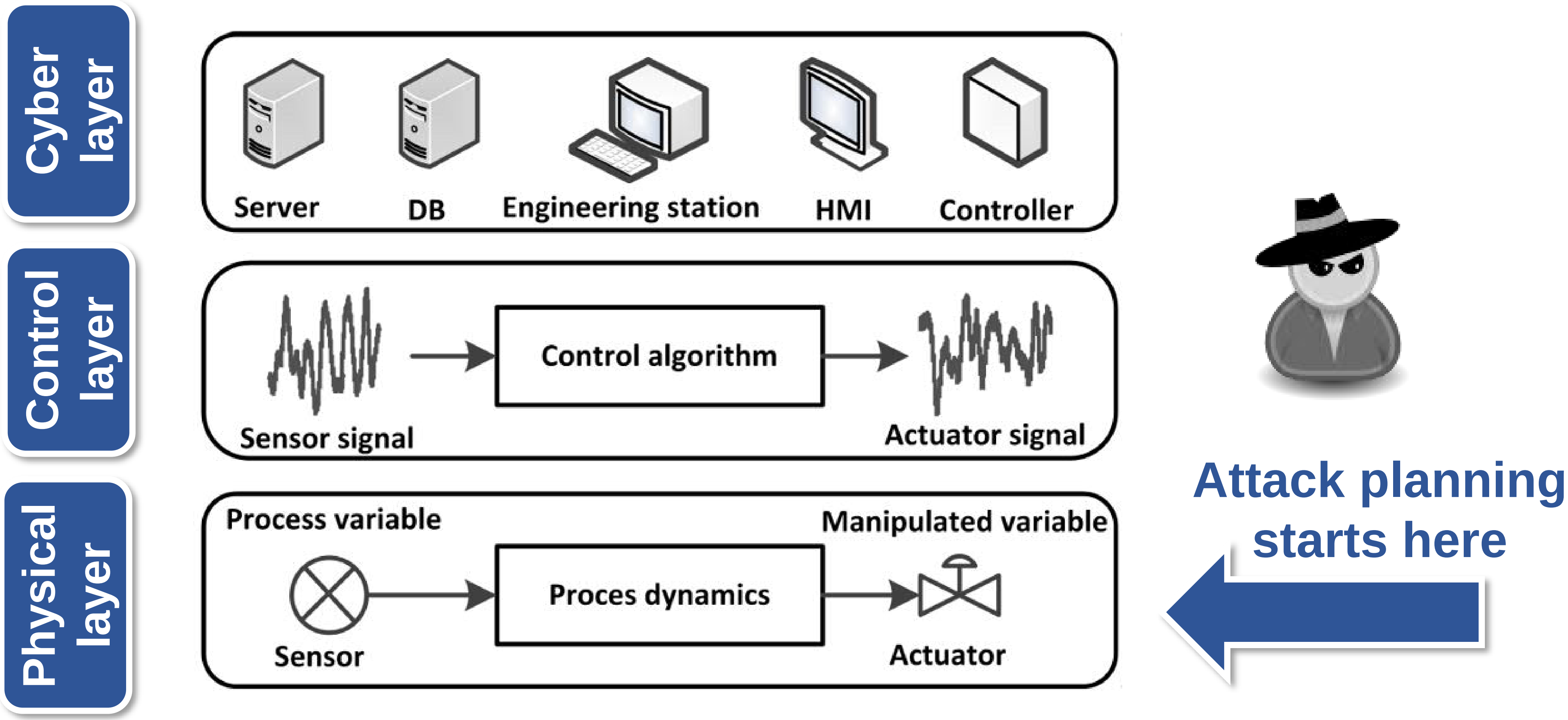
- Average UF filter DP is ≈ 12-13 kPa
- Max DP is **98 kPa (~ 1 bar)**
- Not enough for breakage…..
- Such information can only be figured out on a live process



Layers of cyber-physical system



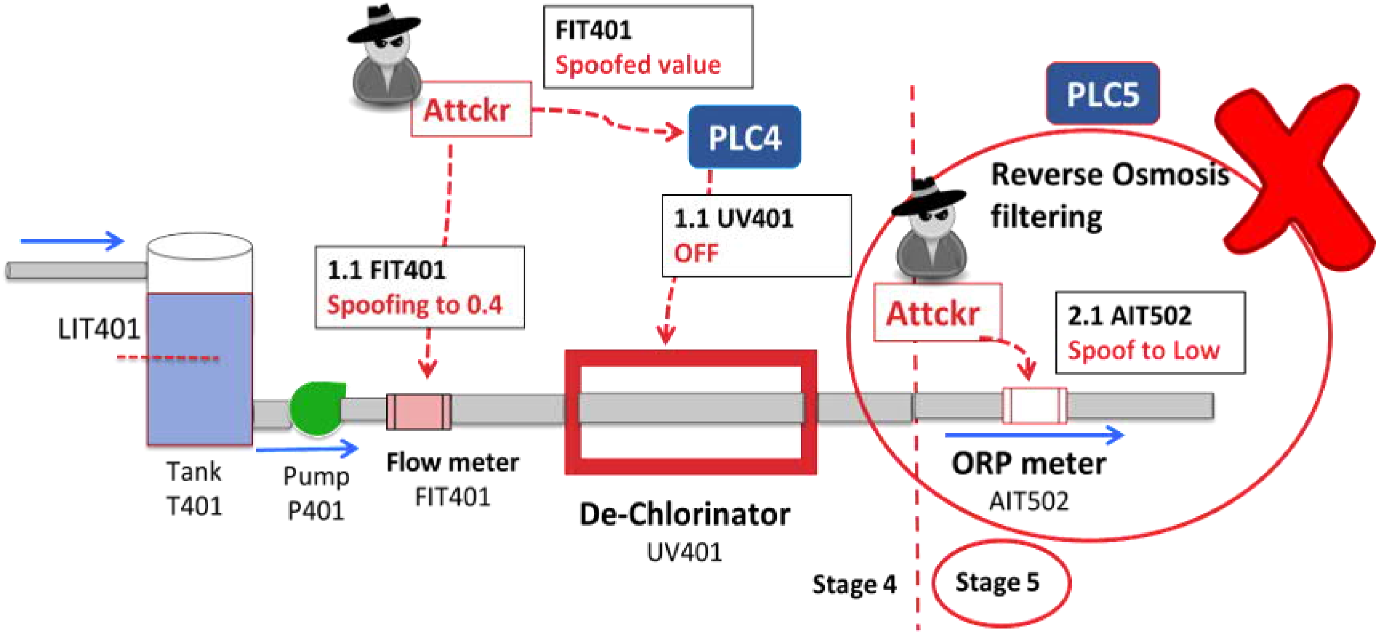
Layers of cyber-physical system

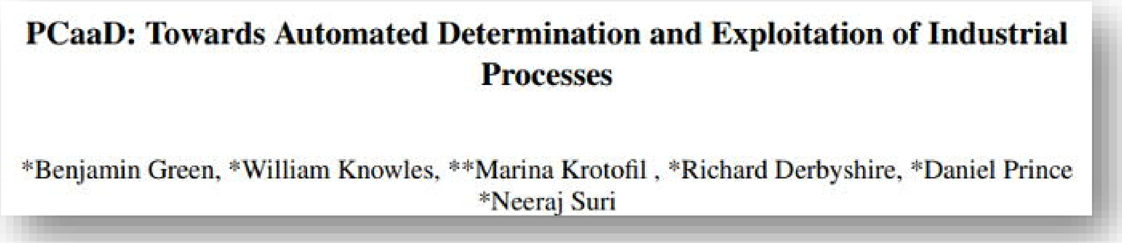


Attack planning starts here

Attack Design != Attack success

- **The attacker is not almighty**
- Successful implementation of damage scenario & its cyber execution will not necessarily result in successful attack
- Many targeted damage attacks require prolonged access to the process and equipment
  - **Limit/eliminate such option for the attacker**
- Cat & Mouse game: Myself and co-researchers recently came up with targeted automated payloads for ICS




PCaaD: Towards Automated Determination and Exploitation of Industrial Processes

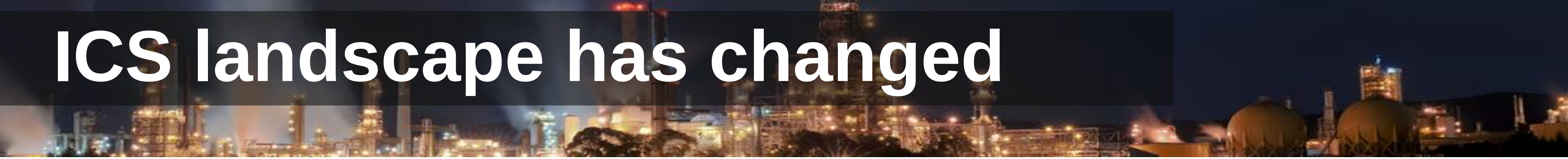
*Benjamin Green, *William Knowles, **Marina Krotofil , *Richard Derbyshire, *Daniel Prince
*Neeraj Suri

https://arxiv.org/pdf/2102.10049.pdf

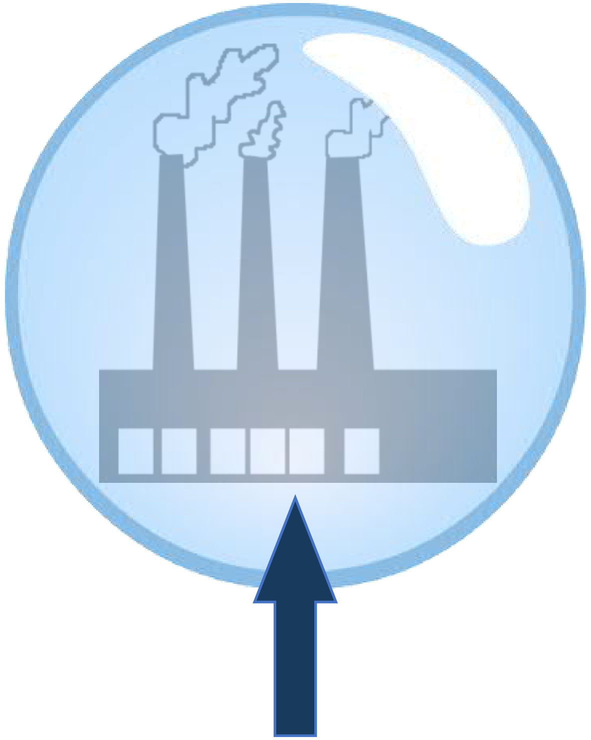
Q & A

Marina Krotofil
@marmusha
marmusha@gmail.com

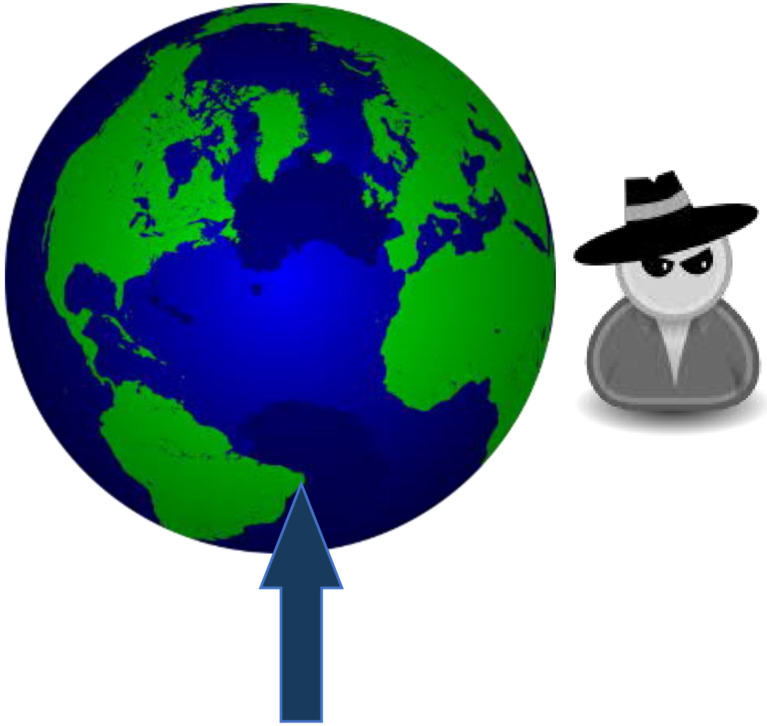
Race-to-the-Bottom in ICS



ICS landscape has changed



Nobody even knows about our existence



Crazy amount of hacking on a daily basis

Brief history of ICS attacks

Reconnaissance and weaponization of capabilities

It’s happening: Publicly known cyber-physical attacks

1999

First active recon & initial intrusion attempts

Successful *cyber-physical* experiments

2010

Planned operation to hinder Iran’s nuclear program (Stuxnet)

https://qph.fs.quoracdn.net/main-qimg-f741c6e5db32b87f282e54448a2129ce

2013

First publicly known OT recon activities (HAVEX)

2015

Ukraine power grid attack (BlackEnergy)

https://www.bankinfosecurity.com/ukrainian-power-grid-hacked-a-8779

2016

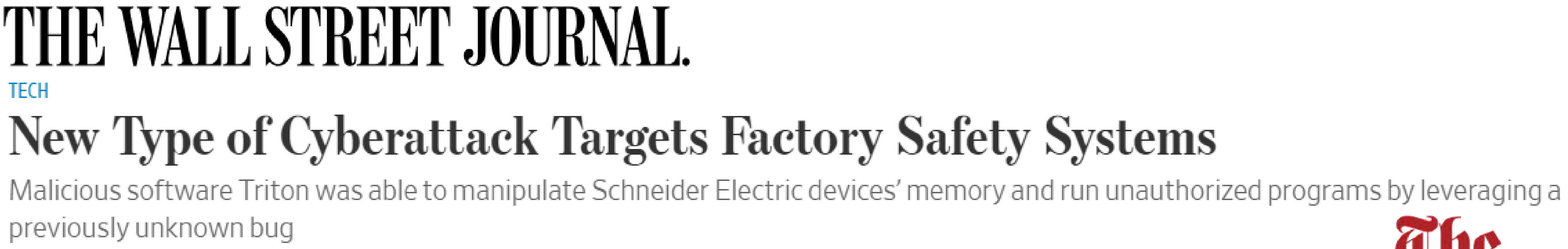
Ukraine power grid attack (Industroyer)

2017

TRITON

https://www.schneider-electric.com/ww/en/Images/tricon-IC-654x654.jpg

TRITON in the news



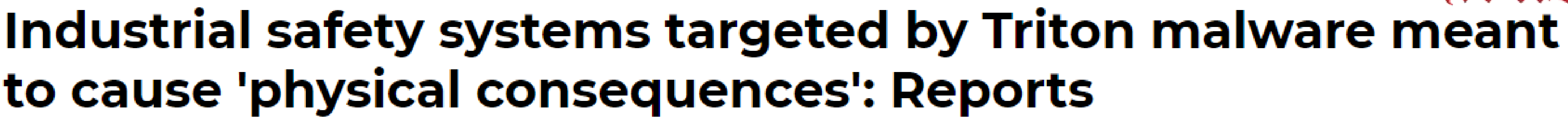
THE WALL STREET JOURNAL.

TECH

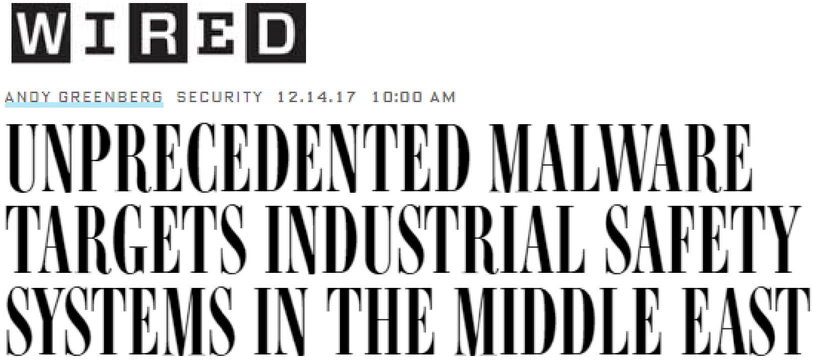
New Type of Cyberattack Targets Factory Safety Systems

Malicious software Triton was able to manipulate Schneider Electric devices' memory and run unauthorized programs by leveraging a previously unknown bug

The Washington Times



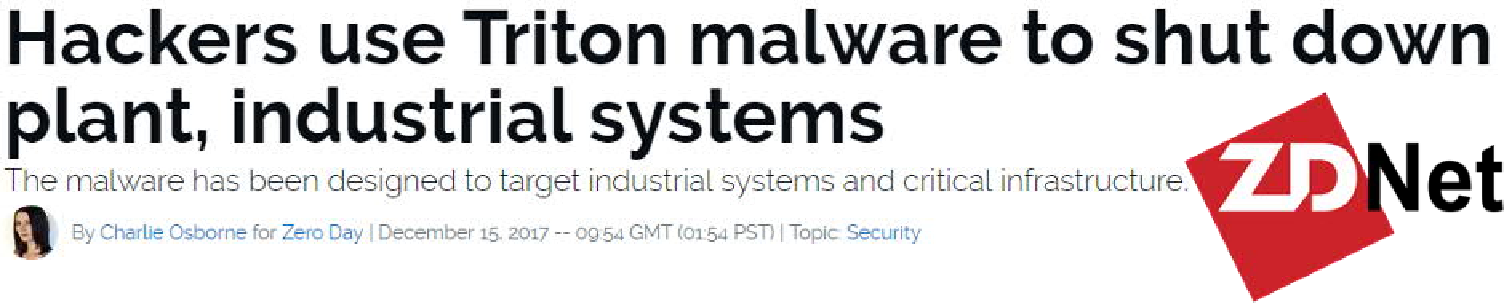
Industrial safety systems targeted by Triton malware meant to cause 'physical consequences': Reports



WIRED

ANDY GREENBERG SECURITY 12.14.17 10:00 AM

UNPRECEDENTED MALWARE TARGETS INDUSTRIAL SAFETY SYSTEMS IN THE MIDDLE EAST



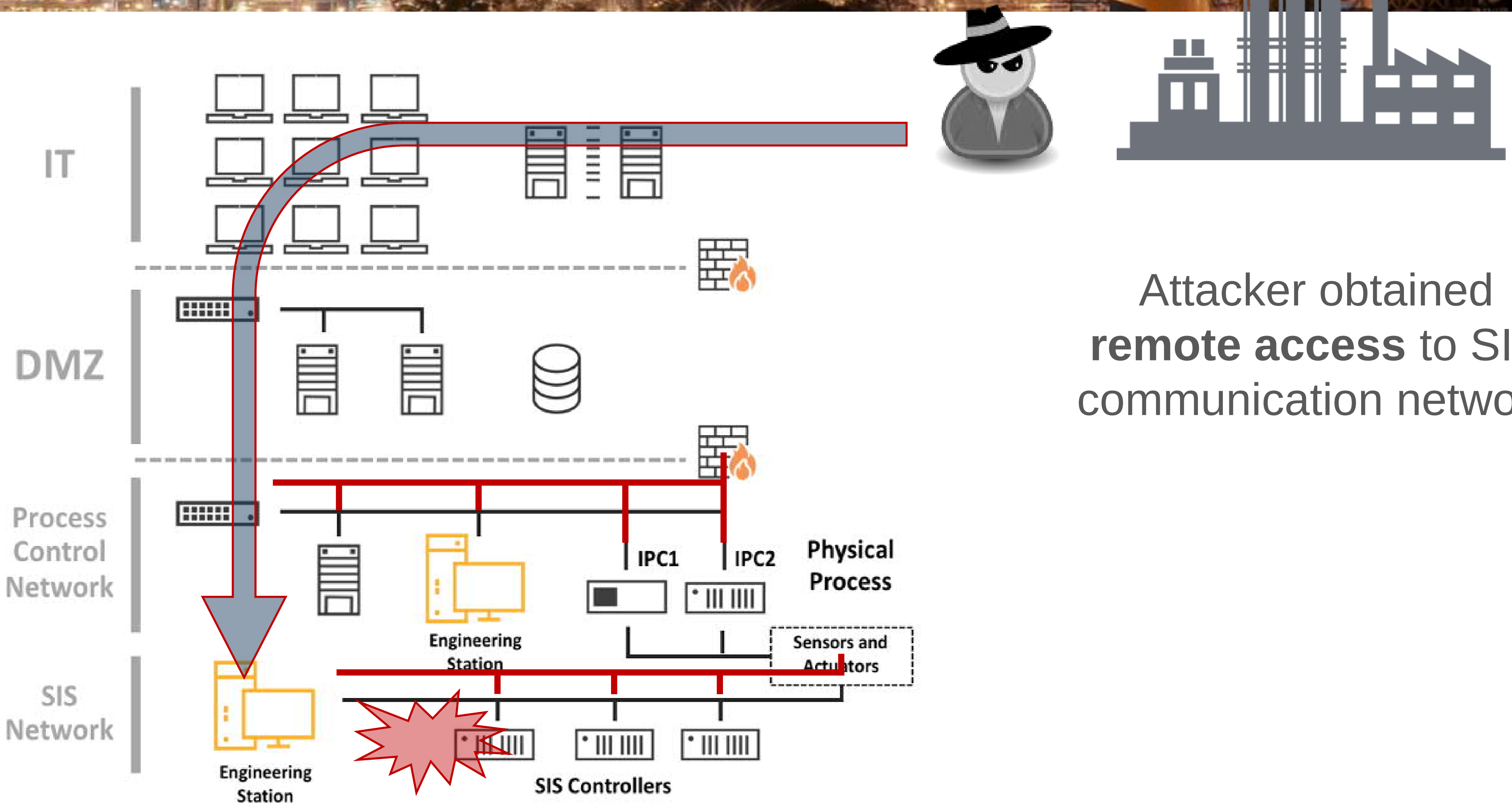
Hackers use Triton malware to shut down plant, industrial systems

The malware has been designed to target industrial systems and critical infrastructure.

By Charlie Osborne for Zero Day | December 15, 2017 -- 09:54 GMT (01:54 PST) | Topic: Security

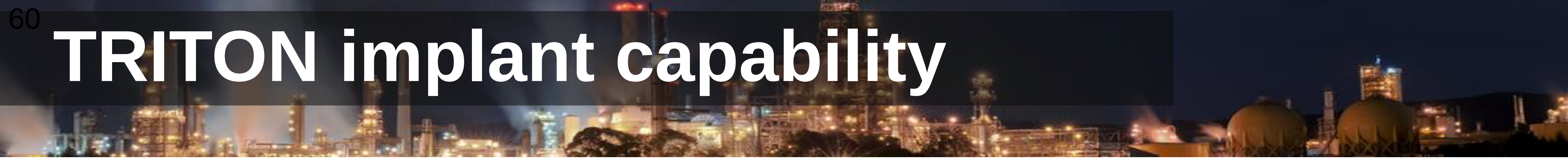
ZDNet

TRITON incident description



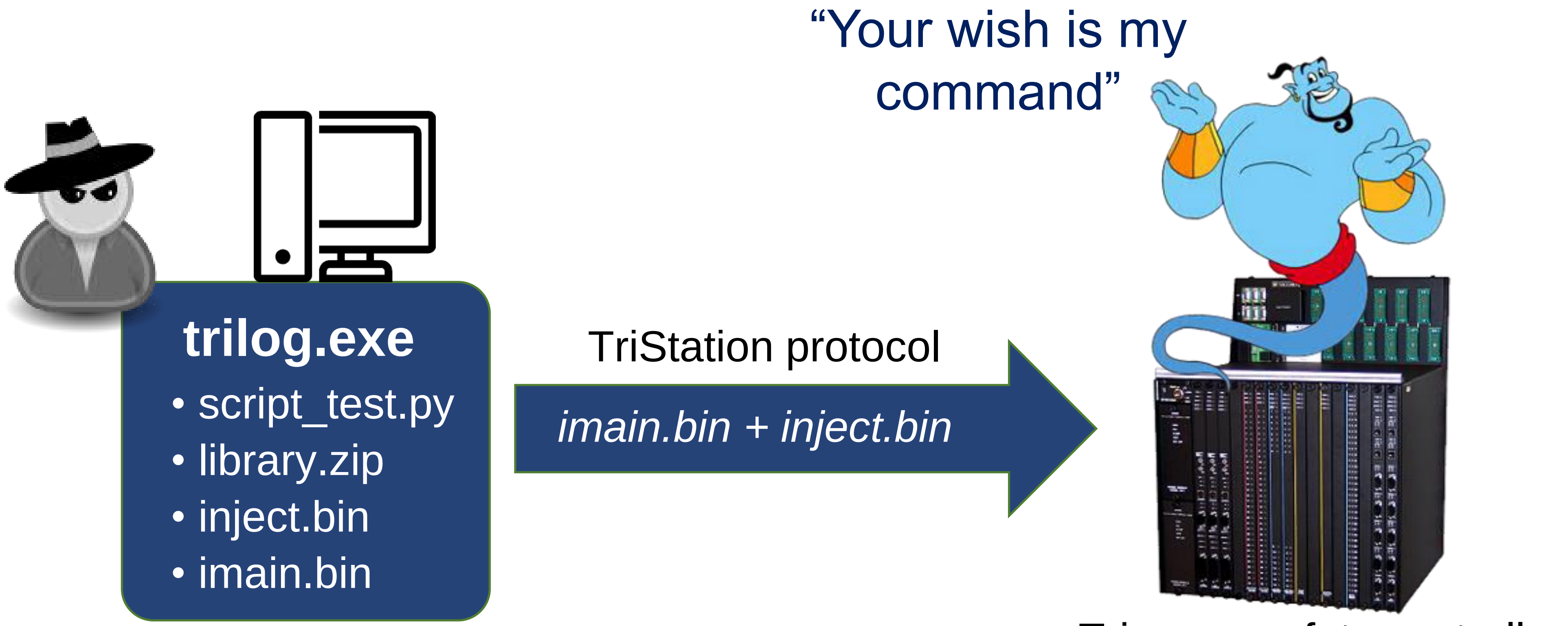
Dual-homed SIS Eng. Workstation

Attacker obtained **remote access** to SIS communication network



TRITON implant capability

- Attacker attempted to inject passive implant into safety controller
  - Runs as user program on controller, activated by special network packet
  - Read / Write / Execute memory



“Your wish is my command”

trilog.exe

- script_test.py
- library.zip
- inject.bin
- imain.bin

TriStation protocol

imain.bin + inject.bin

Triconex safety controller

TRICONEX: Safety Integrity Level (SIL3)

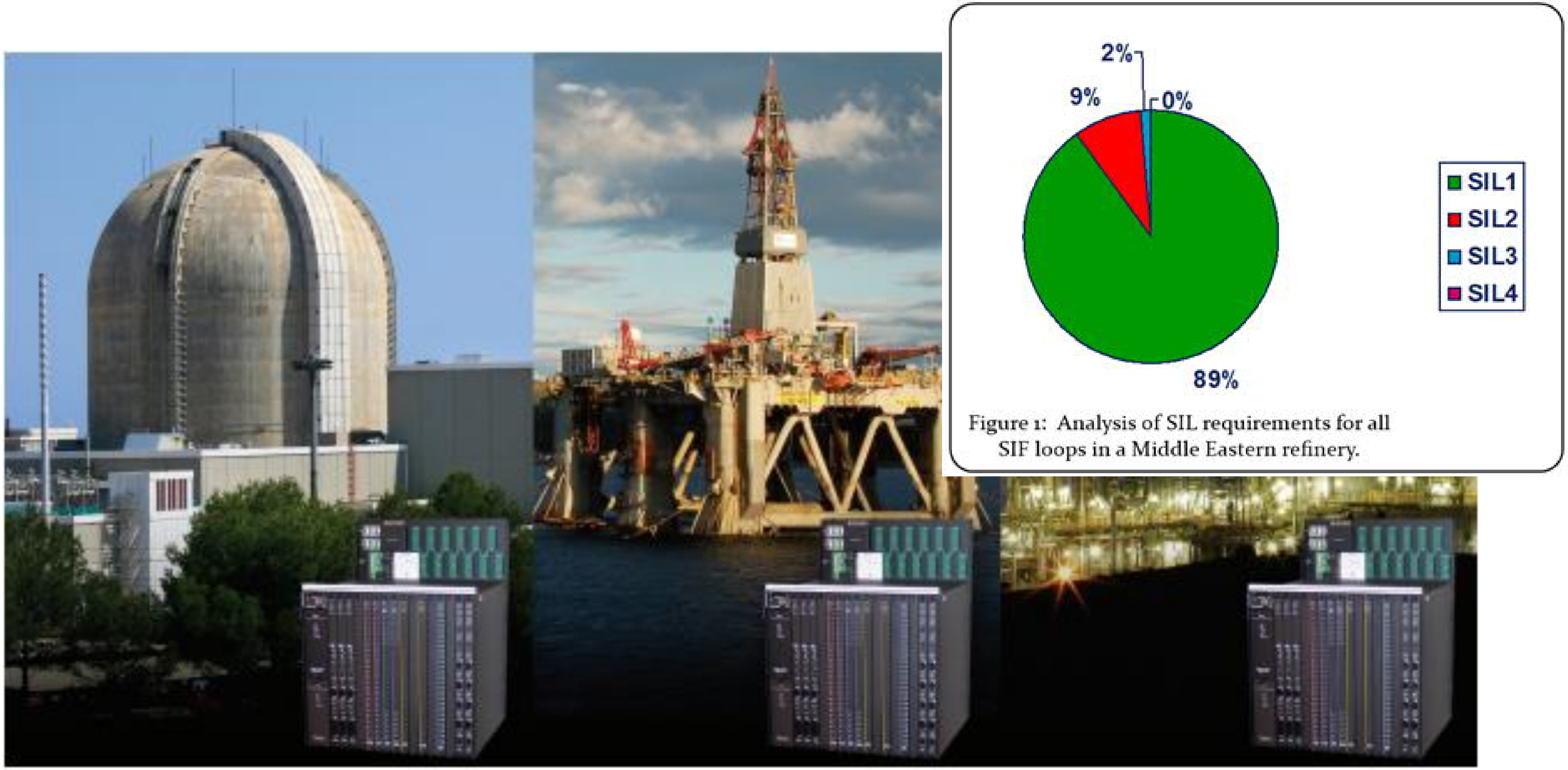
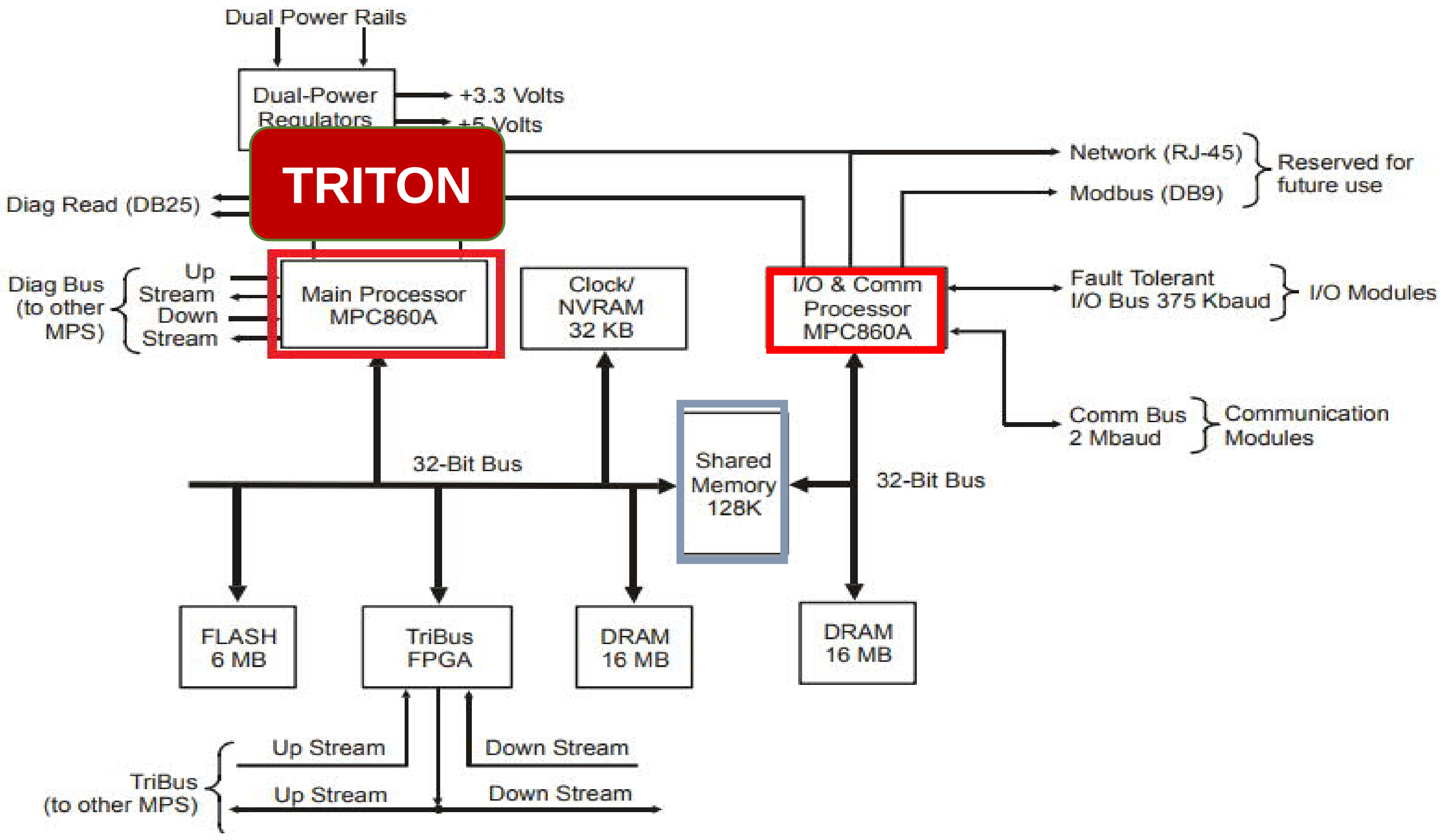


Figure 1: Analysis of SIL requirements for all SIF loops in a Middle Eastern refinery.

http://iom.invensys.com/EN/pdfLibrary/Datasheet_Triconex_TriconSIL3_06-11.pdf

TRITON worst case scenario

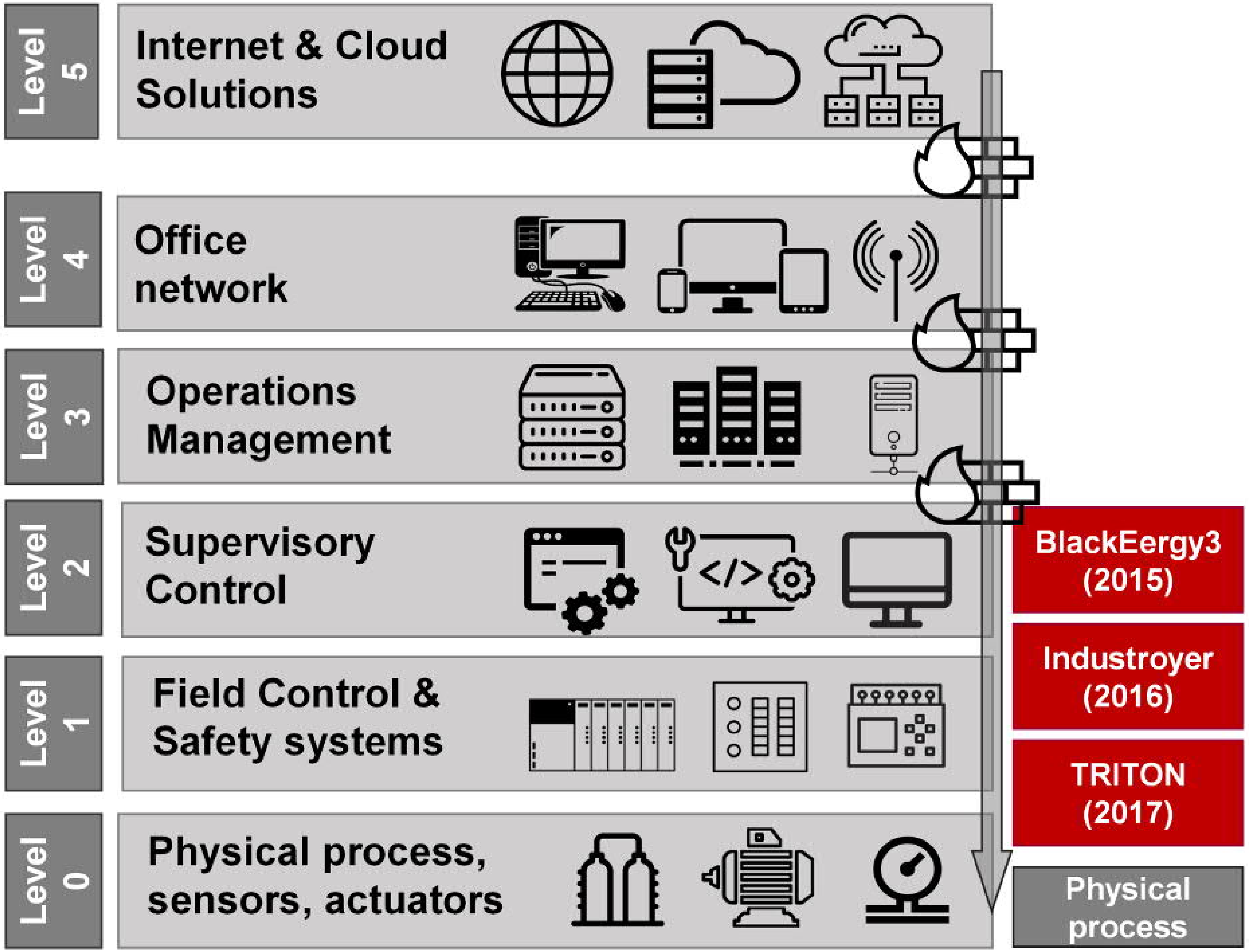


I/O signals

Architecture of model 3008 Main Processor

https://www.nrc.gov/docs/ML0932/ML093290420.pdf

Race-to-the-Bottom in ICS


Level 5
Internet & Cloud Solutions
Level 4
Office network
Level 3
Operations Management
Level 2
Supervisory Control
Level 1
Field Control & Safety systems
Level 0
Physical process, sensors, actuators
BlackEergy3 (2015)
Industroyer (2016)
TRITON (2017)
Physical process