Cyber-Physical Attack Lifecycle

Marina Krotofil

COINS summer school on Security Applications, Lesbos, Greece
26-27.07.2019

Note

This session is based on the talk:

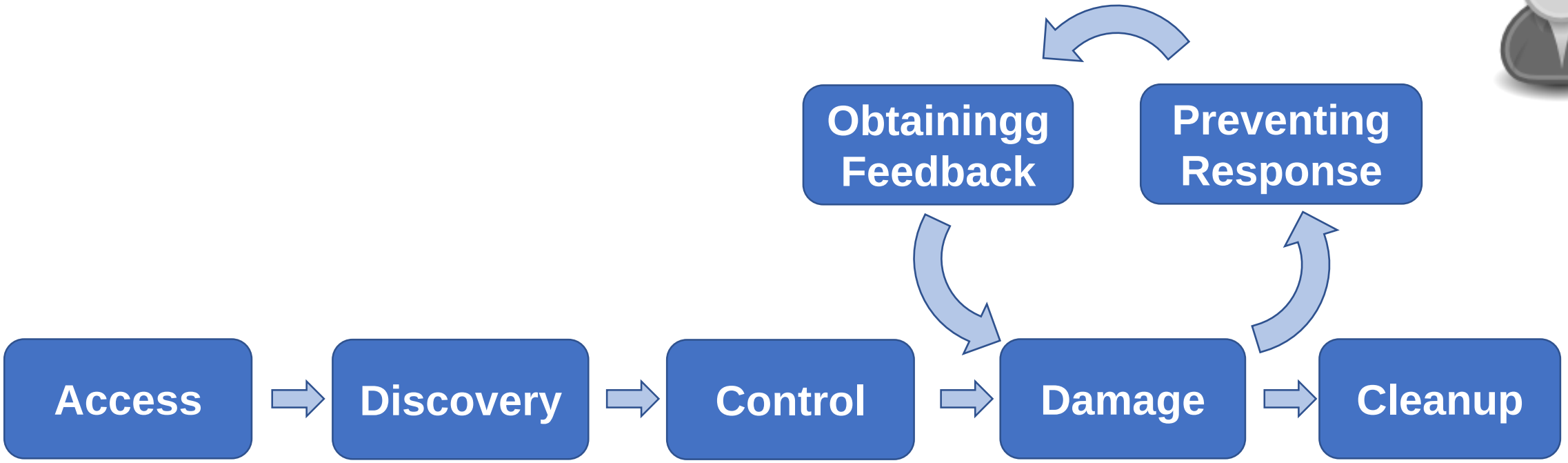
J. Wetzels, M. Krotofil “A Diet of Poisoned Fruit: Designing Implants and OT Payloads for ICS Embedded Devices”, TROOPERS, Heidelberg, Germany, 2019.

https://troopers.de/downloads/troopers19/TROOPERS19_NGI_IoT_diet_poisoned_fruit.pdf

Cyber-Physical Attack Development Lifecycle

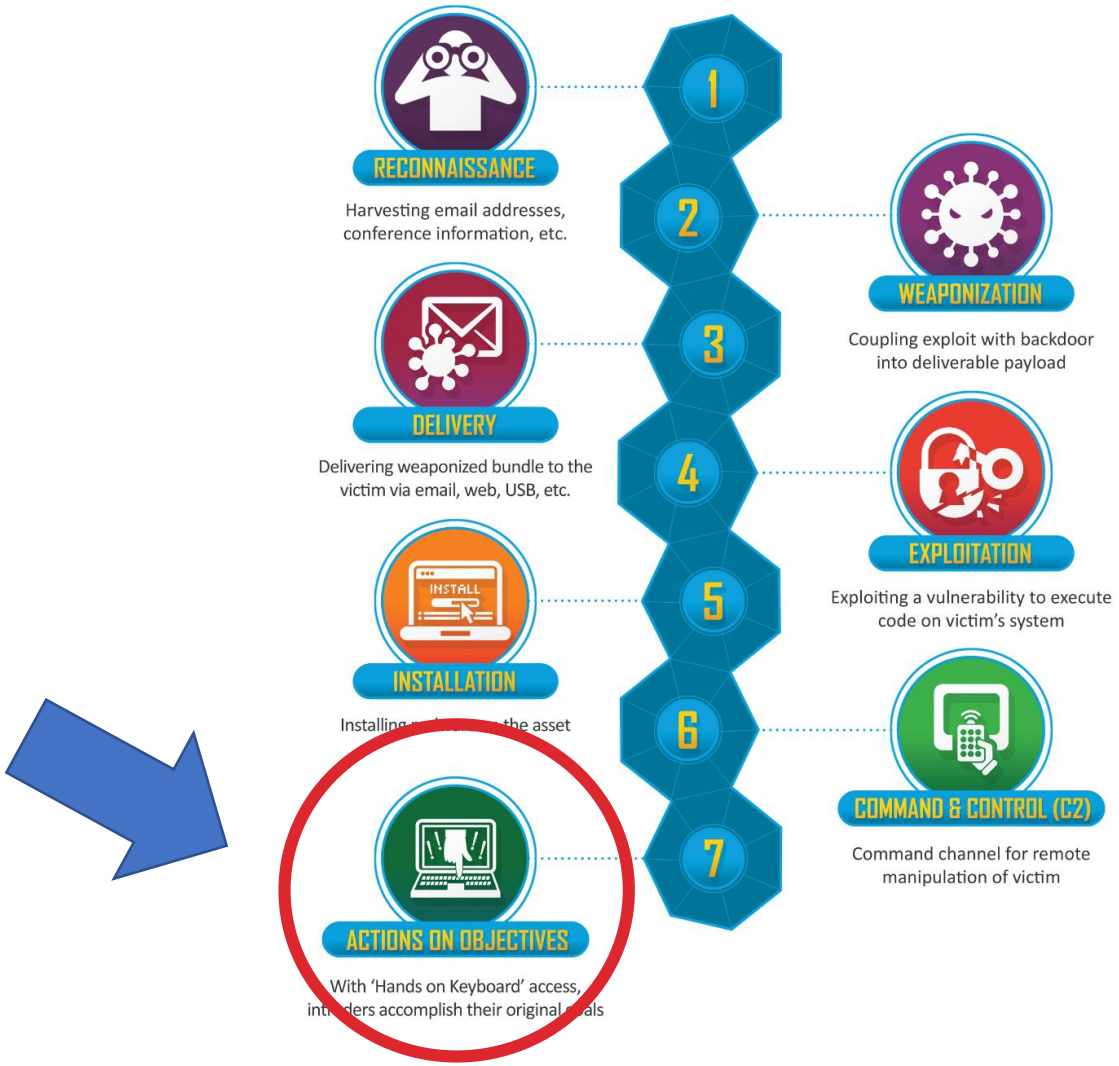
- **If you know how attackers work, you can figure out how to stop them**
- Attack lifecycle is a common method to describe a process of conducting cyber attacks

Cyber-Physical Attack Development Lifecycle



Lockheed Martin, the Cyber Kill Chain®

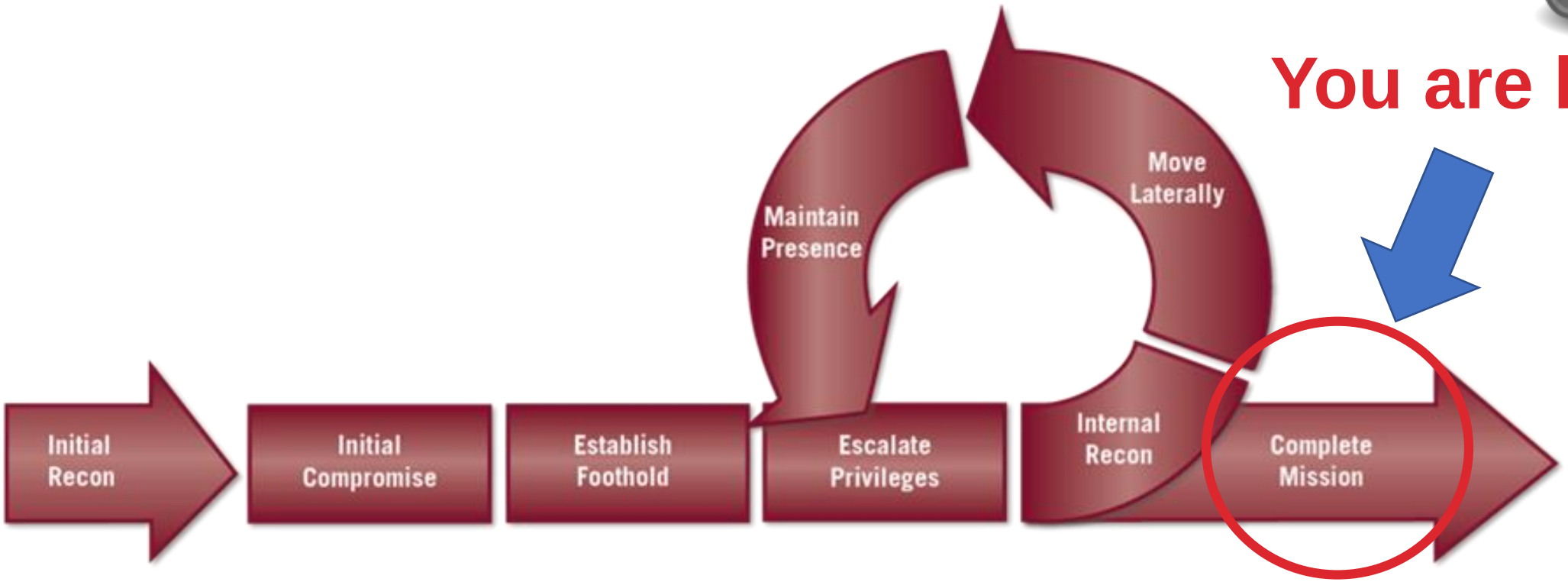
You are here



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

Mandiant Attack Lifecycle

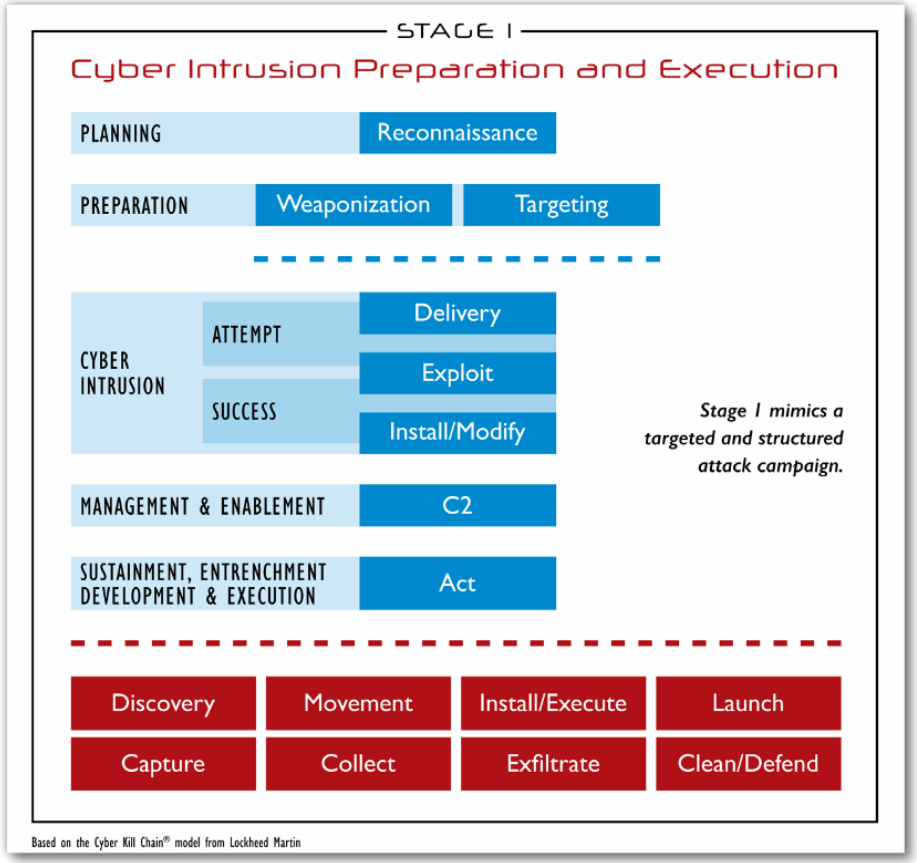
You are here

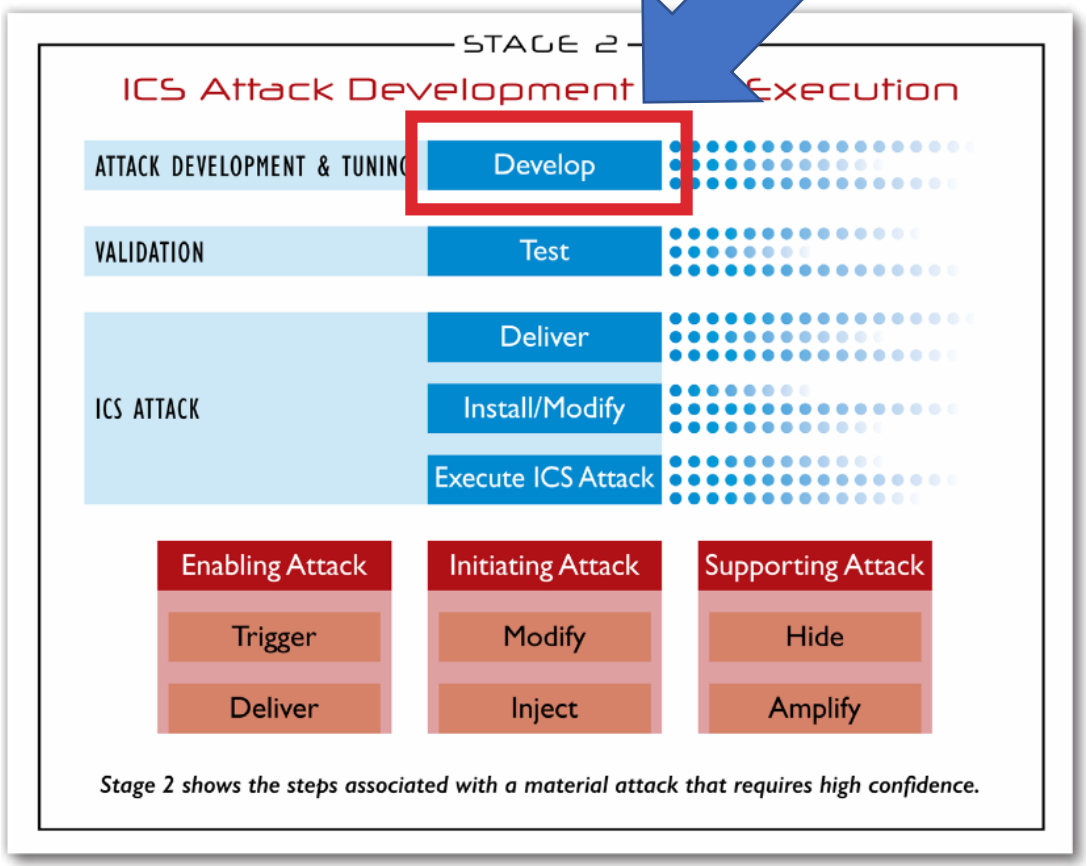


http://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/

SANS Industrial Control System Cyber Kill Chain

You are here





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

ICS MITRE ATT&CK

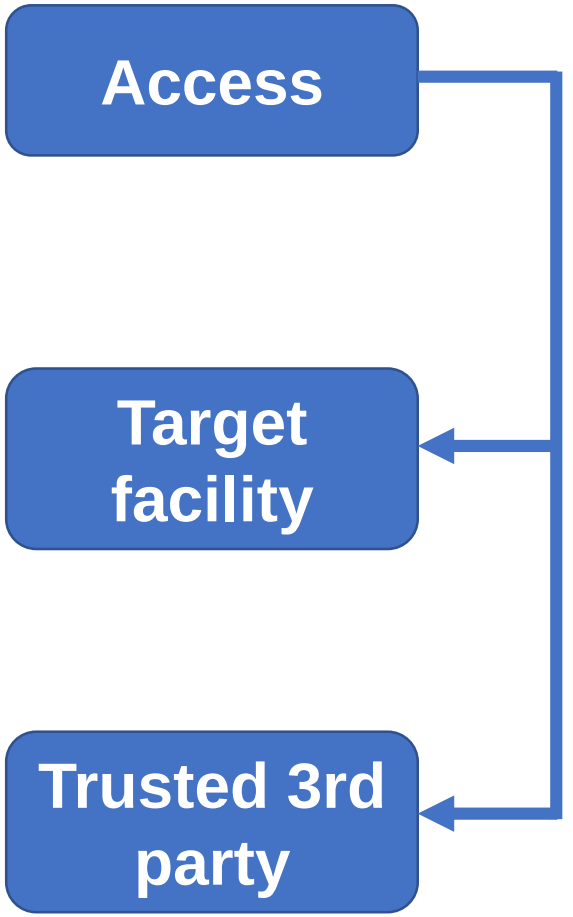
Persistence	Privilege Escalation	Defense Evasion	Operator Evasion	Credential Access	Discovery	Lateral Movement	Execution	Command and Control	Disruption	Destruction
Valid Accounts		Rootkit		Network Sniffing		Exploitation of Vulnerability		Connection Proxy	Module Firmware	
Module Firmware	Exploitation 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/

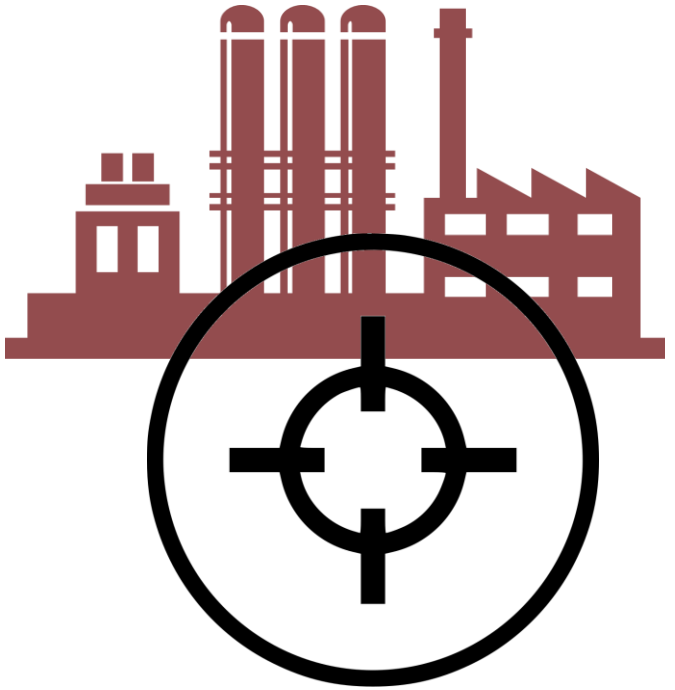
Access

- **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



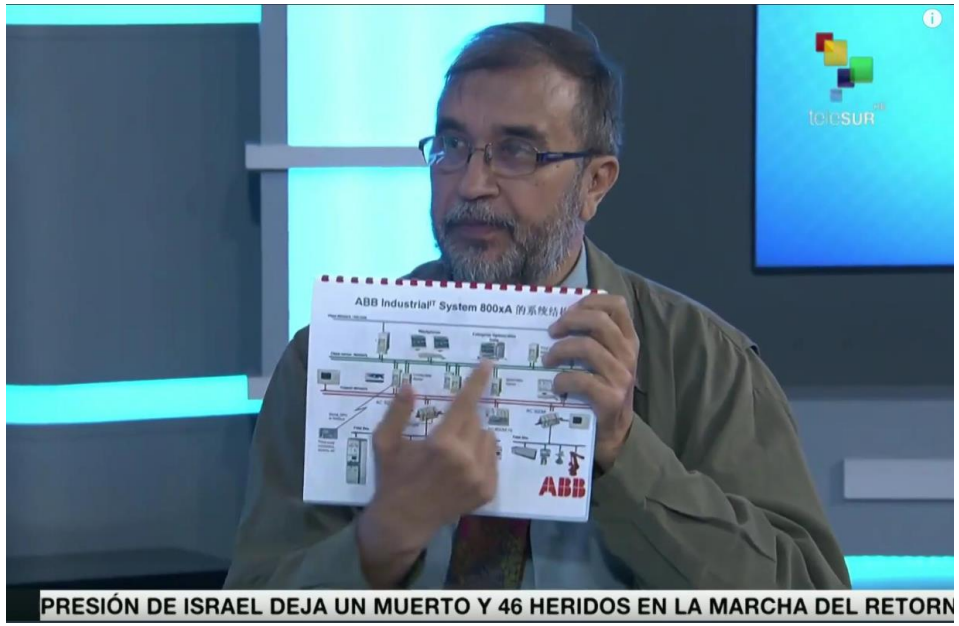
Targeting

- 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



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

Venezuela, 2019

IVC APPLICATION NOTE:

Monitoring Hydroelectric Dam Alarms

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

new control, protecti

the Francis turbines,

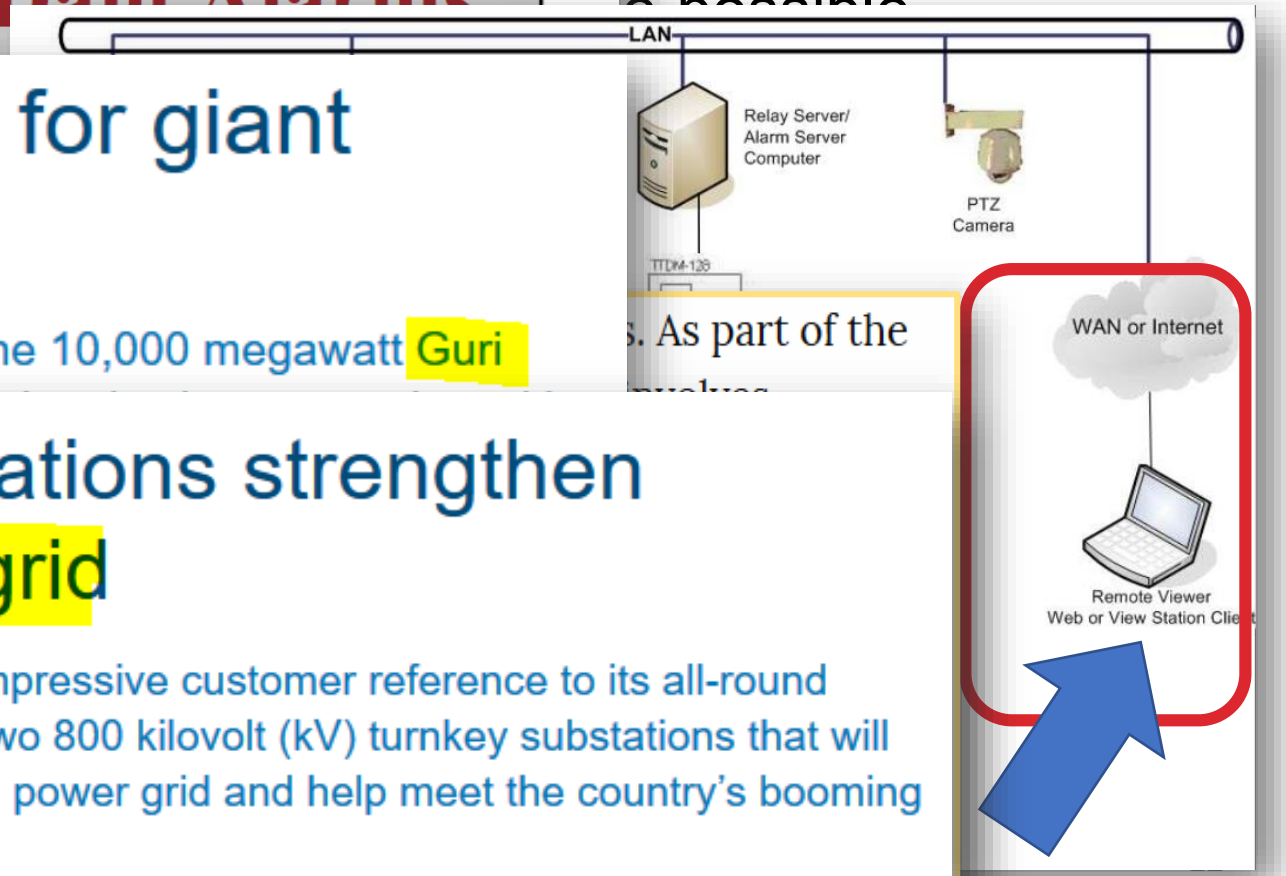
In May 2009, Alstom

generators of powerl

refurbishment of fou

ABB's 800 kV substations strengthen Venezuelan power grid

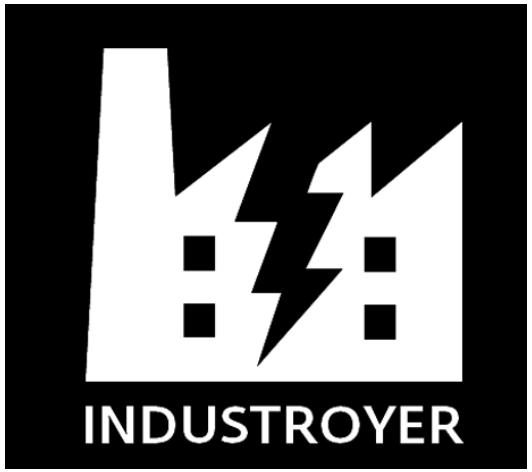
2007-10-16 - ABB has added another impressive customer reference to its all-round capability in bulk power transmission - two 800 kilovolt (kV) turnkey substations that will strengthen and stabilize the Venezuelan power grid and help meet the country's booming demand for electricity.



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

Ukraine, 2016

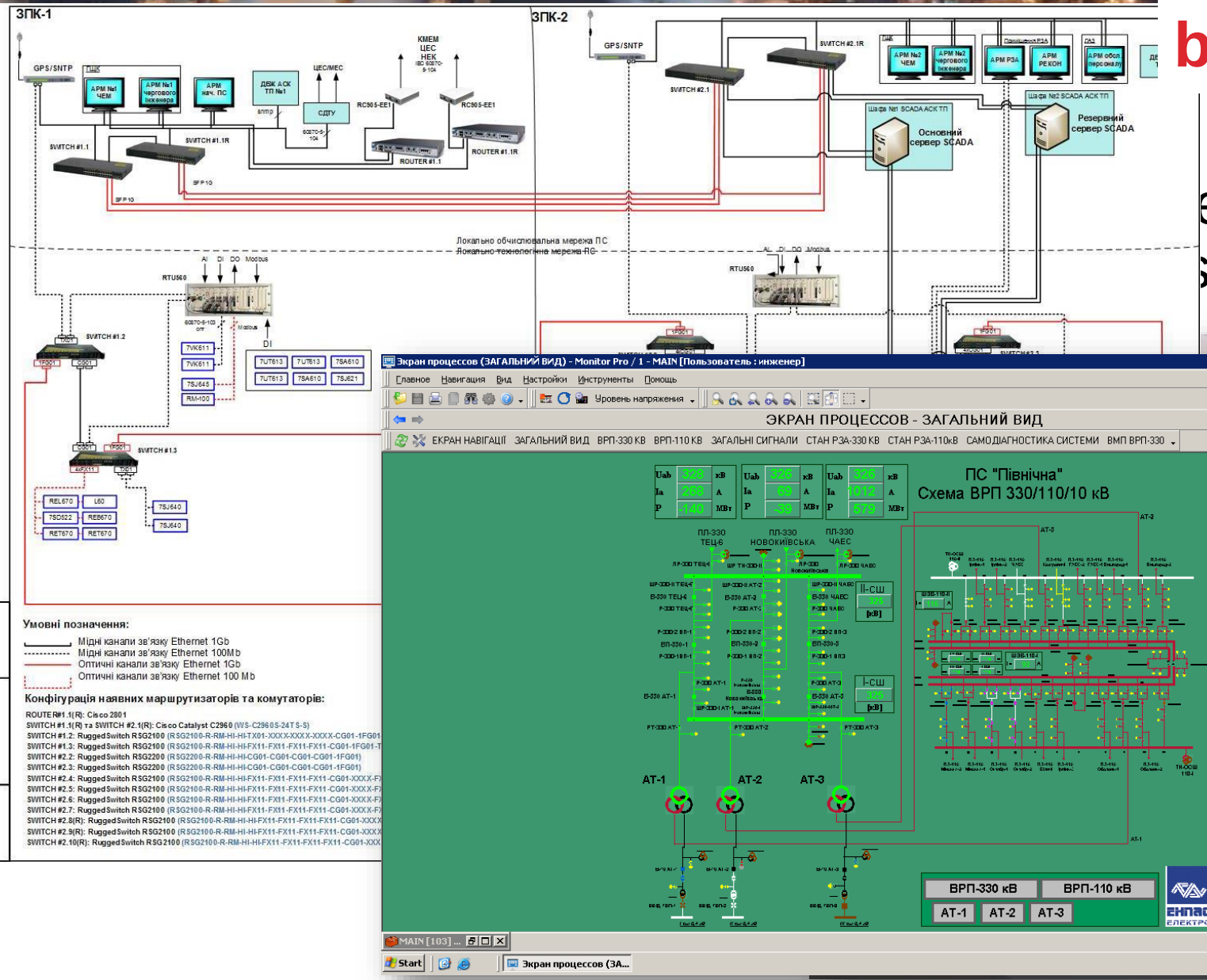
- INDUSTROYER malware was deployed to shutdown electricity distribution at Pivnichna substation
- There is no strong indications that victim substation was strategic target
- Details of substation upgrade are publicly available



Ukraine, 2016

Targeted by malware

ed to shutc
station



Saudi Arabia, 2018

- 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-rC-654x654.jpg

Saudi Arabia, 2018

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 excess of 900 trillion cu ft, or over nine per cent of the world's proven reserves. The project also involves the construction of two of the world's largest LNG trains. When these come on line in late 2007 and early 2008, the project will process 30 billion cu m per year of gas, 15.8 million tonnes per year (tpy) of LNG, 6 million tpy of condensates and 1.7 b tpy of propane and butane. The LNG will then be exported to a dedicated receiving terminal in Milford Haven, West Wales, UK, and carried by a new fleet of LNG carriers, currently under construction as part of a 1.3 billion euro contract awarded to three South Korean shipyards.

Each of the four cabinet-based control systems supplied by Invensys is responsible for one turbine-driven boiler feed water pump on the new project.

The design, control and operation of these pumps are identical. Each is based on the Triconex TS3000 turbomachinery control solution and includes

ctim was

ill and

get

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

Gas Oil Separation Plant

ect

h consisting of a DCS (CENTUM CS 3000),

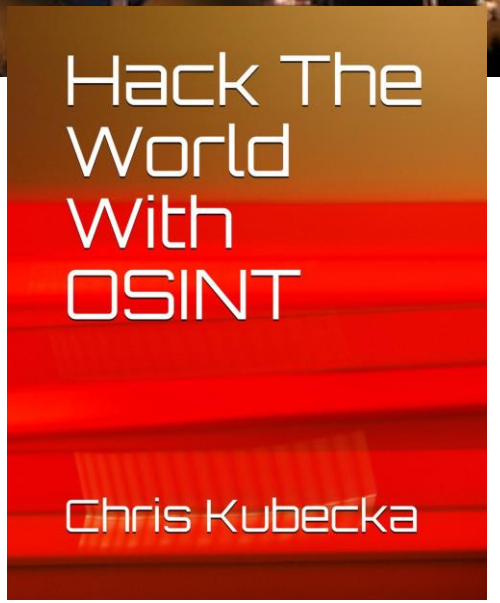
(Triconex), vibration monitoring system

trumentation.

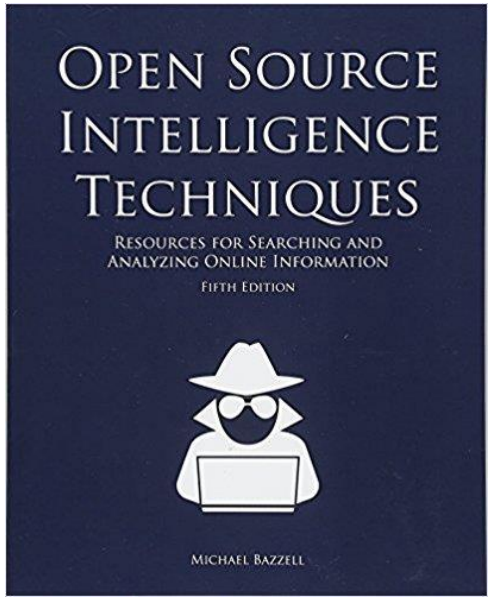
Role of OSINT in Targeting

- 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



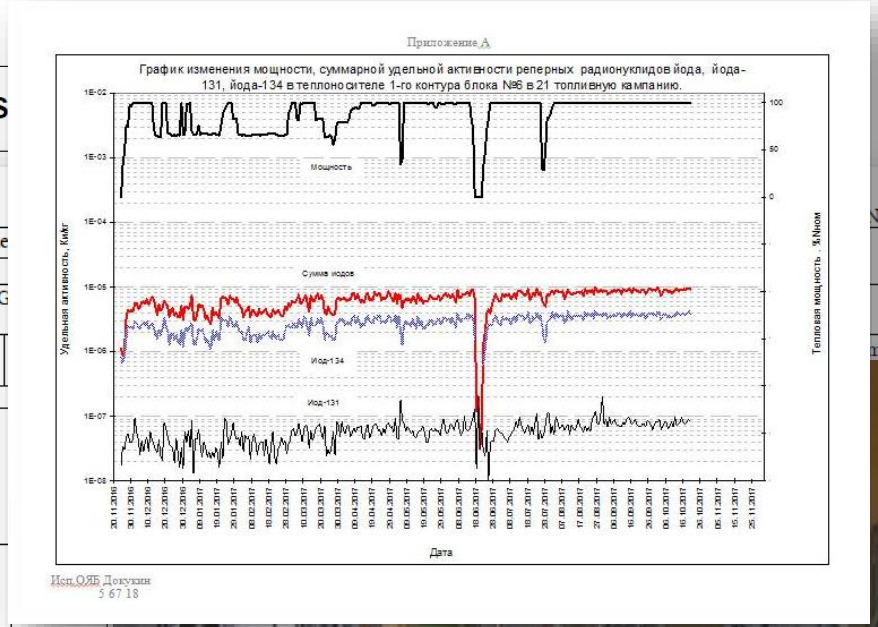
https://www.amazon.com/Open-Source-Intelligence-Techniques-Information/dp/1530508908



OSINT: Tons of confidential info on Internet

8.10.3 Alarm On-Delay and Off-Delay

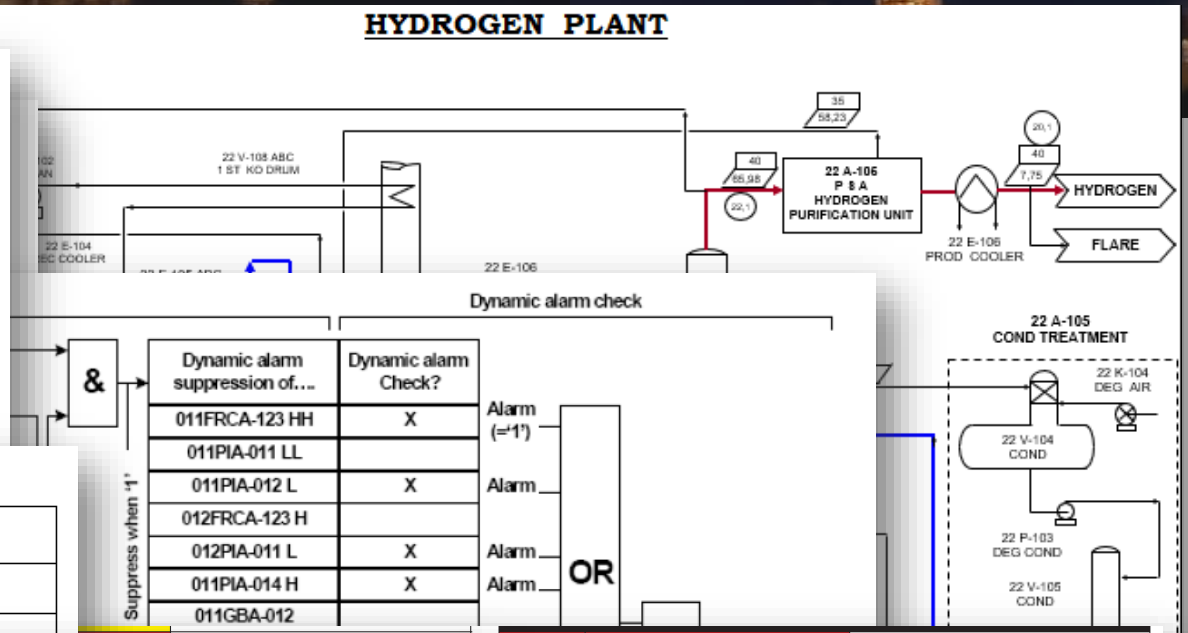
The On-Delay alarm attribute is used to avoid unnecessary alarms, by allowing alarms to be triggered once the signal has remained in the alarm state for a specified length of time. The Off-Delay alarm attribute is used to reduce chattering alarms by locking in the alarm indication for a specified period after it has cleared. On-Delay and Off-Delay times should be used after careful evaluation of potential control system operational effects. Table 8 [2] below provides recommended time delays based on signal types.



Bill of Material

Project : General Project Francis Turbine		
Project Code:		
Item Turbine Auxiliary Control And G Panel(TAGP)		
Rev 0	Part No	Description

	1	Master Trip Relay	
	2	Digital Speed Monitor Relay with Proximity Sensor	
	3	Digital Position Indicator GUIDE VANE	GVI%
	4	Annunciator for Trip & Alarm	30A
		Auto/Test Switch	SW1



Dynamic alarm check

Dynamic alarm suppression of...	Dynamic alarm Check?	
011FRCA-123 HH	X	Alarm (='1')
011PIA-011 LL		
011PIA-012 L	X	Alarm
012FRCA-123 H		
012PIA-011 L	X	Alarm
011PIA-014 H	X	Alarm
011GBA-012		

Suppress when '1'

OR

00071	Bad F2 or F3 Fuse	Report and repair immediately.
00072	Bad F4 or F6 Fuse	Report and repair immediately.
00073	No A/C Power – Check Cord	Switch to Diesel Operation & Repair
00074	AC Phase Reversed	Unit will restart*, report reactivation.
00075	Compressor Motor Overload	Unit will restart*, report reactivation.
00076	Condenser Motor Overheated	Unit will restart*, report reactivation.
00077	Evap Motor Overheated	Unit will restart*, report reactivation.
00078	Check SV1 Circuit	Reset*, report reactivation.
00079	Check SV4 Circuit	Reset*, report reactivation.
00080	Check SV3 Circuit	Reset*, report reactivation.
00081	Check FHR Circuit	Check and repair at end of trip.
00082	Check Remote Out of Range Light	Check and repair at end of trip.
00083	Check Remote Defrost Light	Check and repair at end of trip.
00084	Check Remote Alarm Light	Check and repair at end of trip.
00085	Check UL1 Circuit	Check and repair at end of trip.
00086	Check UL2 Circuit	Check and repair at end of trip.

Attackers C2

Злоумышленник подготавливает сервер к атаке. Работа ведется через обыкновенный WSO веб-шелл с паролем по умолчанию	176.[redacted].210 - - [19/Jan/2016:11:19:32 +0200]
	176.[redacted].210 - - [19/Jan/2016:12:18:48 +0200]
	176.[redacted].210 - - [19/Jan/2016:13:25:49 +0200]
	176.[redacted].210 - - [19/Jan/2016:16:36:13 +0200]
Жертва 1 скачивает бэкдор	82.[redacted].102 - - [19/Jan/2016:18:12:41 +0200]
Жертва 2 скачивает бэкдор	217.[redacted].41 - - [19/Jan/2016:18:14:41 +0200]
Жертва 3 скачивает бэкдор	176.[redacted].22 - - [20/Jan/2016:08:42:36 +0200]
Жертва 4 скачивает бэкдор	194.[redacted].10 - - [20/Jan/2016:09:11:38 +0200]
Жертва 5. Из пределов этого энергетического предприятия (г. Одесса) 4 сотрудника скачали бэкдор	91.[redacted].220 - - [20/Jan/2016:09:13:27 +0200]
	91.[redacted].220 - - [20/Jan/2016:09:53:16 +0200]
	91.[redacted].220 - - [20/Jan/2016:09:53:42 +0200]
	91.[redacted].220 - - [20/Jan/2016:10:08:21 +0200]
Жертва 4 скачивает бэкдор	194.[redacted].10 - - [
Sandbox скачивает бэкдор	184.[redacted].147 - - [
Жертва 6 скачивает бэкдор	82.[redacted].70 - - [

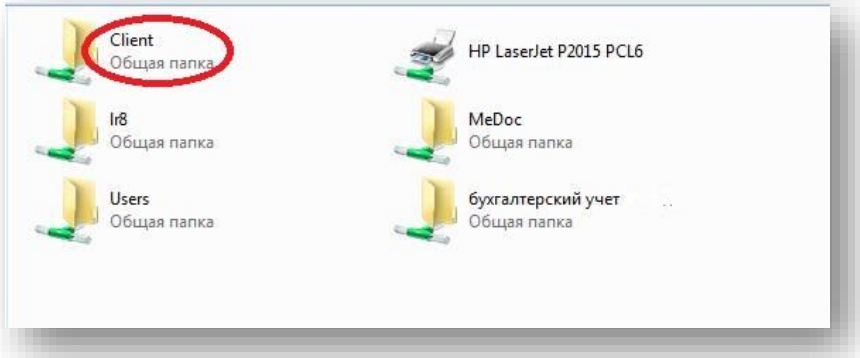
			8	9	10	11	12	13	14	15	16	17	21	22	
2015	7	6				1									1
	10	19										1			1
2016	1	13					1								1
		16								7					7
	3	1										1			1
	4	13			1	1									2
	5	6										1			1

Infrastructure recon

8	1				1									1
	2						1							1
	3			1										1
	4				1									1
	12		1											1
	15										1			1
	18								1	1				2
	22		3		16	11	16	29	14					89
	23		14	29	11	17	14	3	13					101
	25	5	22	12		3	1							43
	26	1	5			5	1							12
	29		9											9
	30	10	1		2	2	5	2						22
	31	2	5											7

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.



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

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

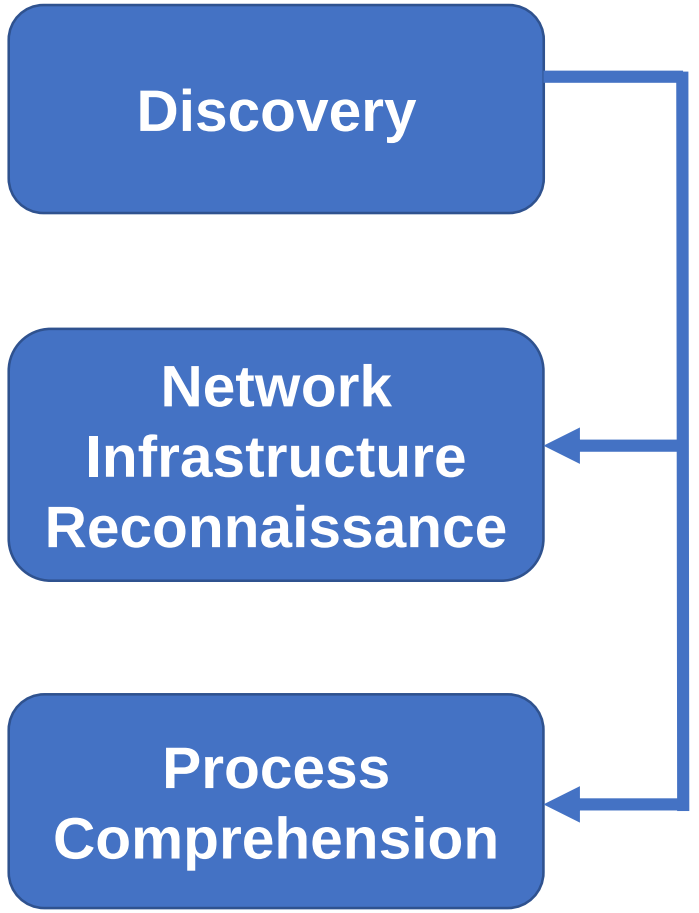
https://www.morganlewis.com/pubs/data-exposure-by-vendor-leads-to-2-7-million-nerc-penalty-for-utility

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 & 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

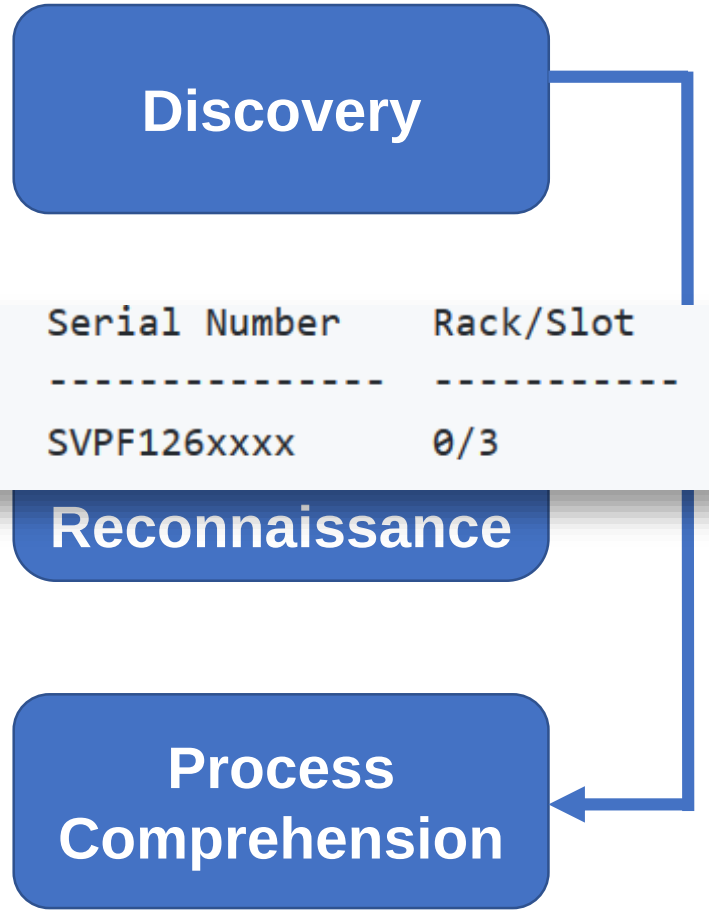
http://eprints.lancs.ac.uk/88089/1/sample_sigconf.pdf

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

how it is built, configured & 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

OT network recon

- Industroyer and TRITON malware included capabilities for asset discovery/enumeration,
- Some open-source OT asset scanners could be found here: https://github.com/dark-lbp/isf

```
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
```

```
Device Name    Device Type    MAC Address        IP Address      Netmask         GateWay
-------------  -------------  -----------------  --------------  --------------  --------------
plcxb1d0ed     S7-400         00:1b:1b:a7:xx:xx  192.168.1.10    255.255.255.0   192.168.1.10
```

61850 payload then enumerates all possible IP addresses for each of these subnet masks, and tries to connect to port 102 on each of those addresses. Therefore, this component has the ability to discover relevant devices in the network automatically.

```
Rack/Slot    IP Address
-----------  --------------
0/3          192.168.1.10
```

In TRITION:

TsLow.py (lines 84-120) contained function to autodetect Triconex controllers on the network by sending a specific UDP broadcast packet over port 1502:

```
def detect_ip(self)
ip_list = set()
...
TS_PORT = 1502
ping_message = '\x06\x00\x00\x00\x00'
...
```

```
ER = ['Order Code', 'Module Type Name', "Firmware Version",
'Module Name", "Serial Number", "Rack/Slot", "IP Address"]
S7_DEVICES = []
```

```
13  TABLE_HEADER = ['Order Code', 'Module Type Name', "Firmware Version", "Module Name", "Serial Number", "Rack/Slot", "IP Addr
14  S7_DEVICES = []
```

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

Use Case: Killing UF filter in water treatment facility

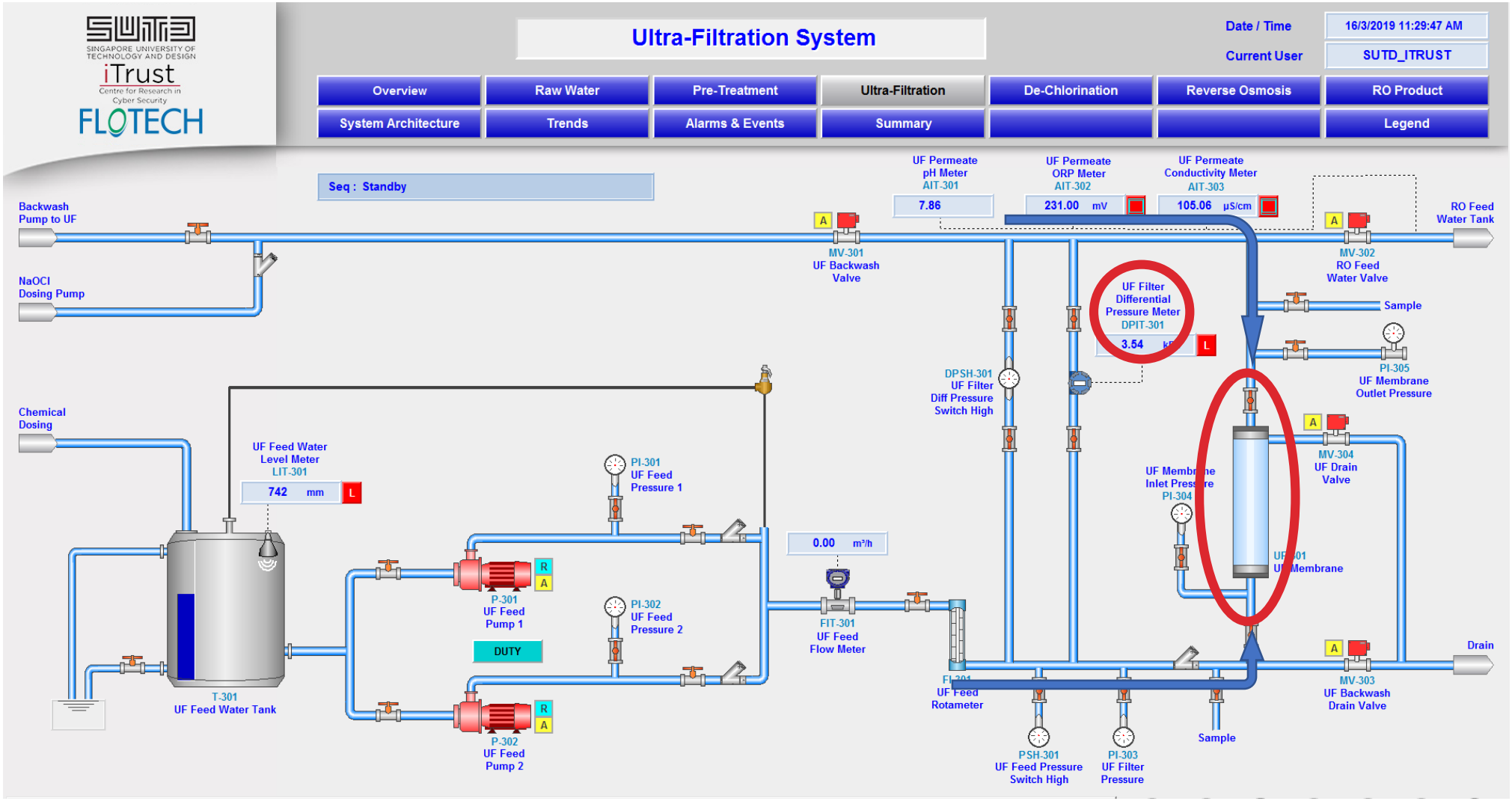
Acknowledgement: Sridhar Adepu and Prof. Aditya Mathur, SUTD, Singapore for kindly conducting this experiment on request

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

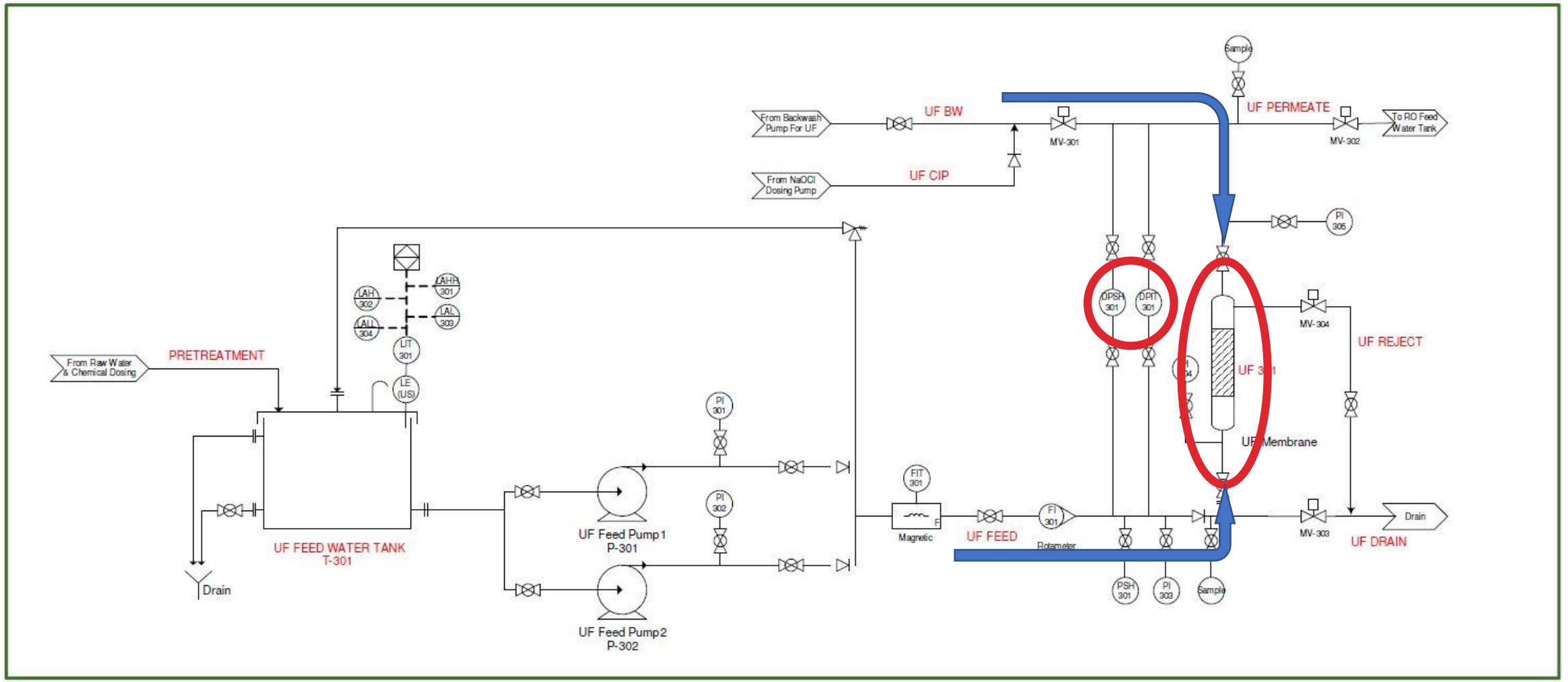
Use Case: Killing UF filter in water treatment facility

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

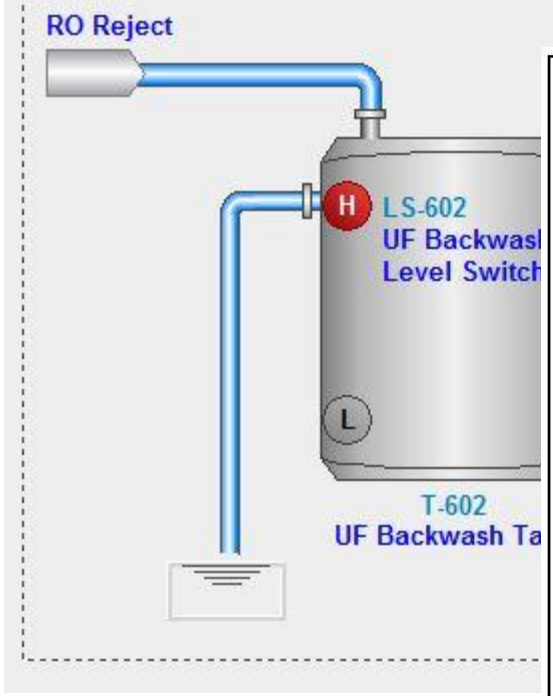
UF filtering: HMI Screen

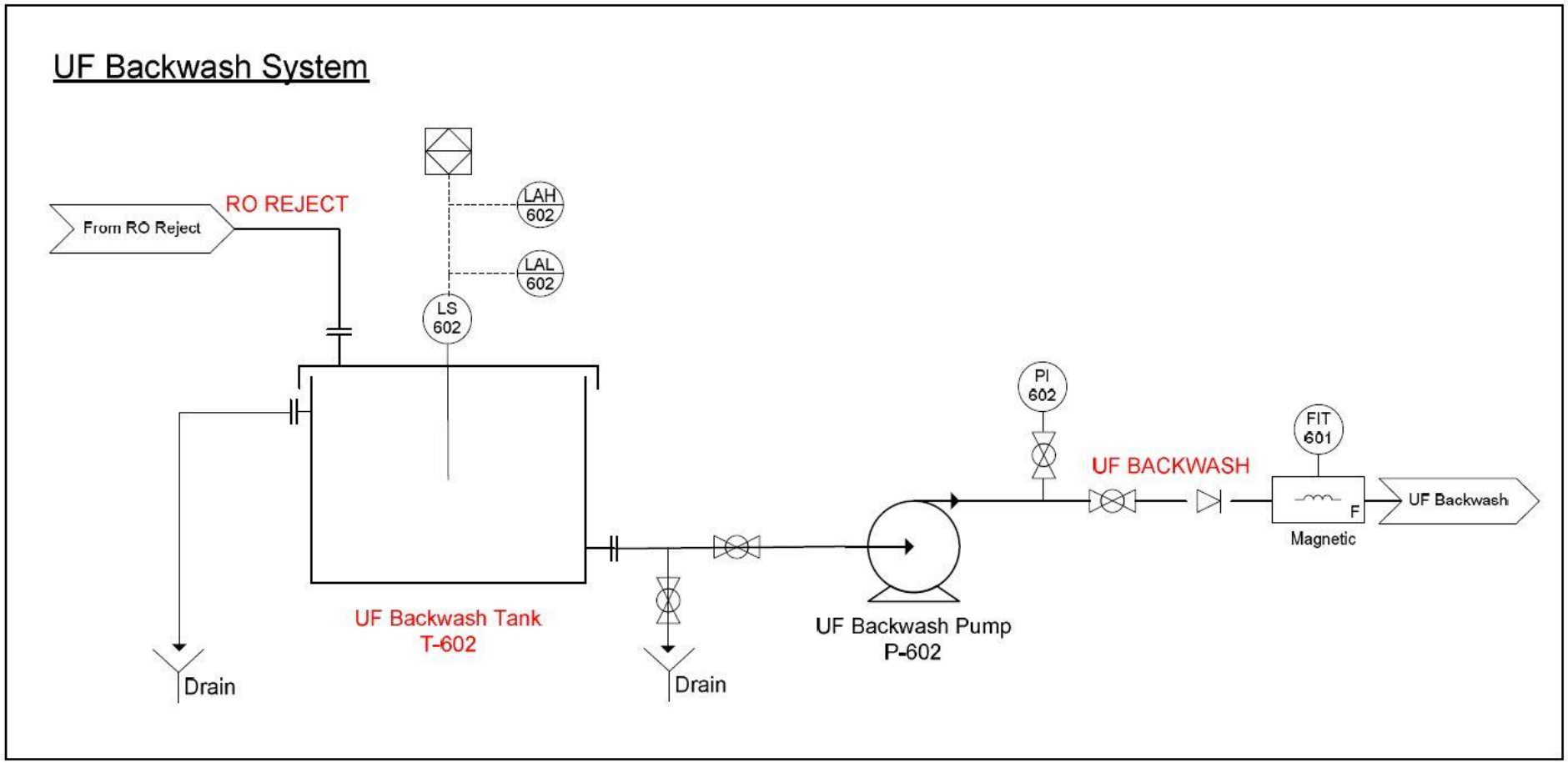


UF filtering: PI&D diagram



UF backwash: HMI and PI&D diagram





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

How do we pull this off?

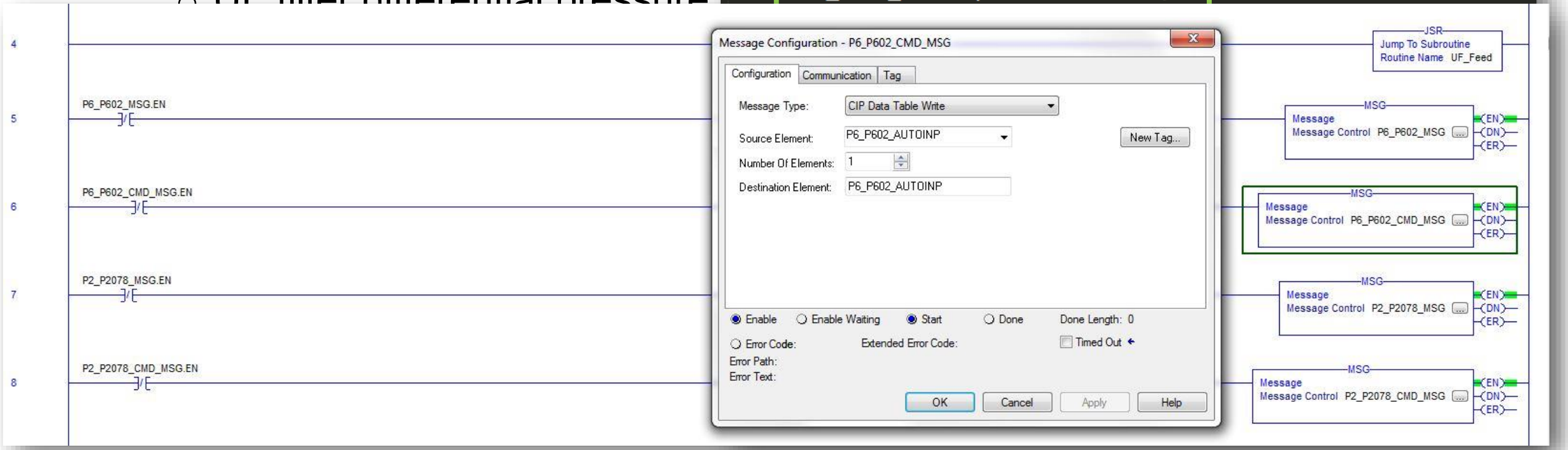
- There are tree conditions w
  process, each guided by a s
  - Preset timer (every 30 m
  - UF filter differential press
  - Plant shutdown

```
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;
```

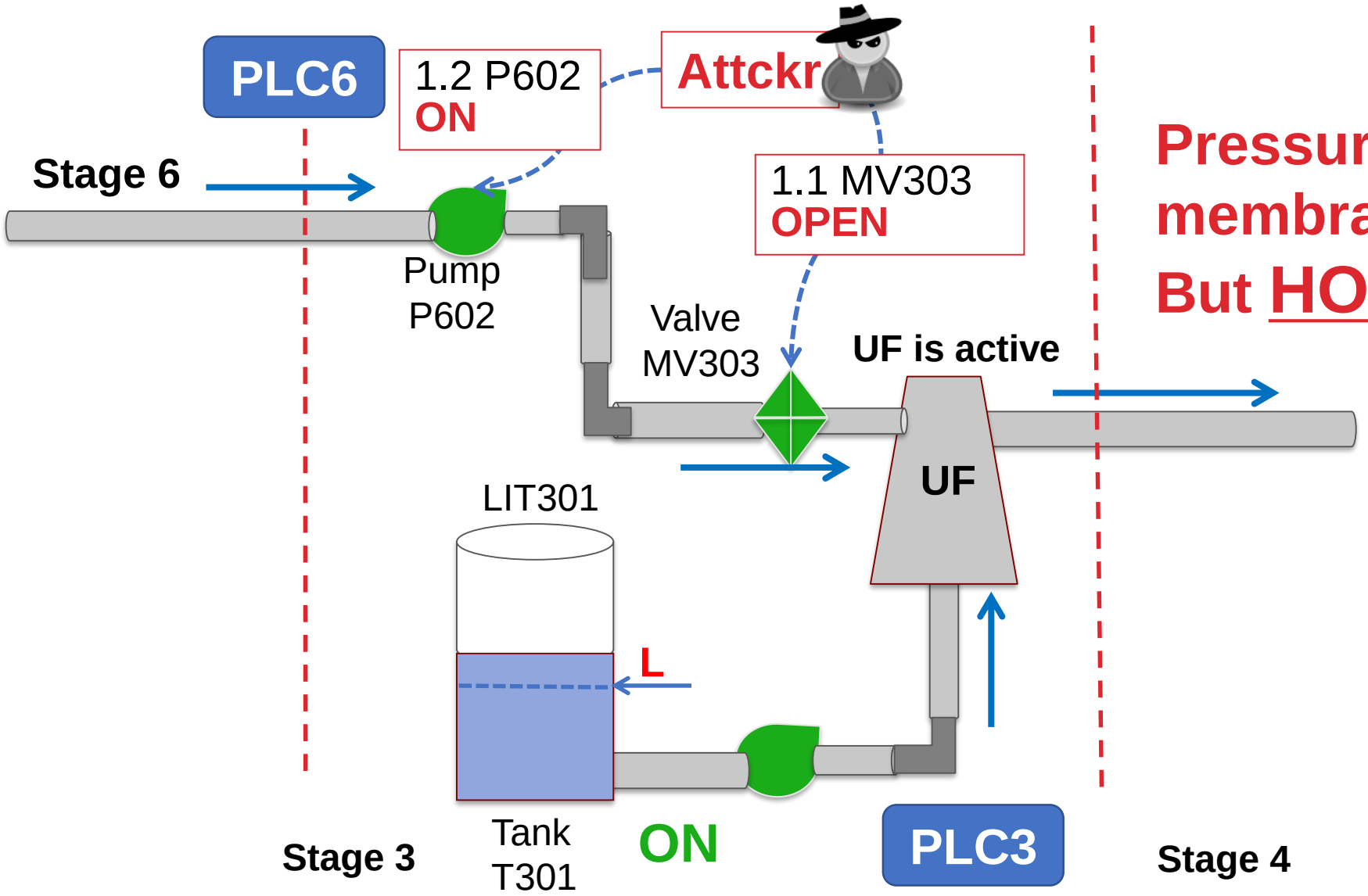
How do we pull this off?

- There are tree conditions w
  process, each guided by a s
  - Preset timer (every 30 minute
  - UF filter differential pressure

```
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

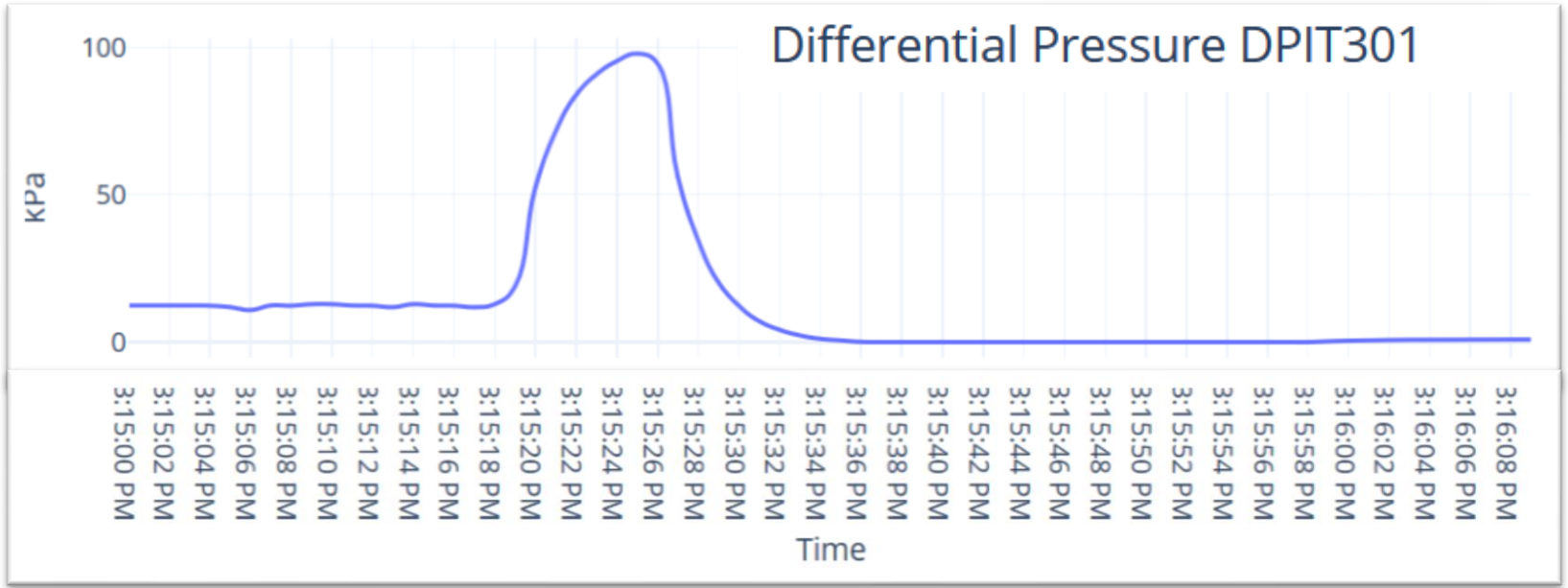


Pressure in UF membrane will increase.

But HOW MUCH?

Understanding of dynamic behavior of process

- 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



Understanding of dynamic behavior of process

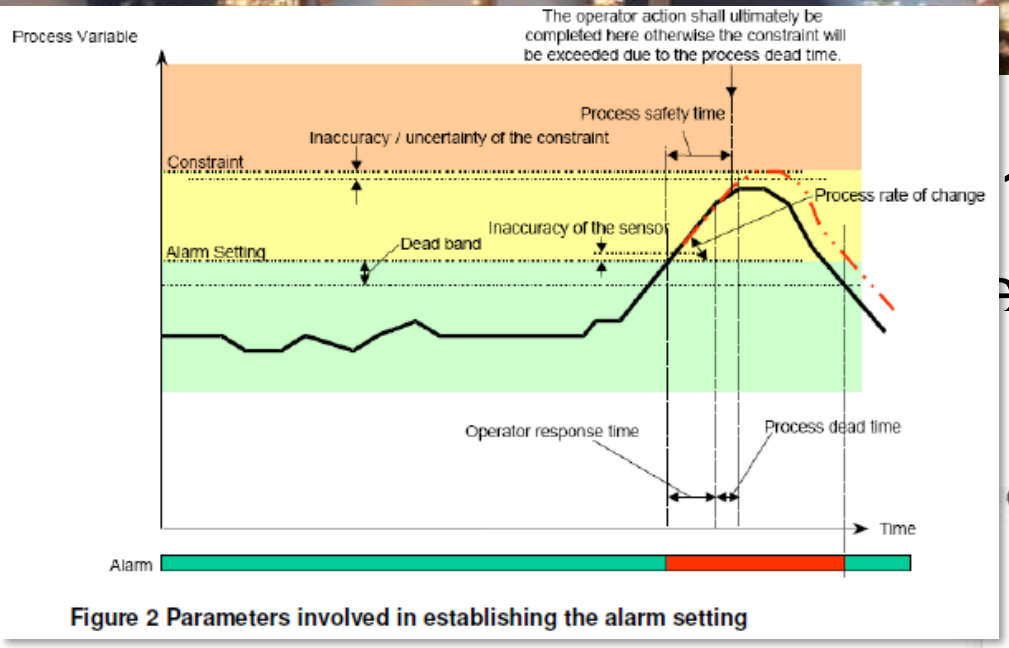
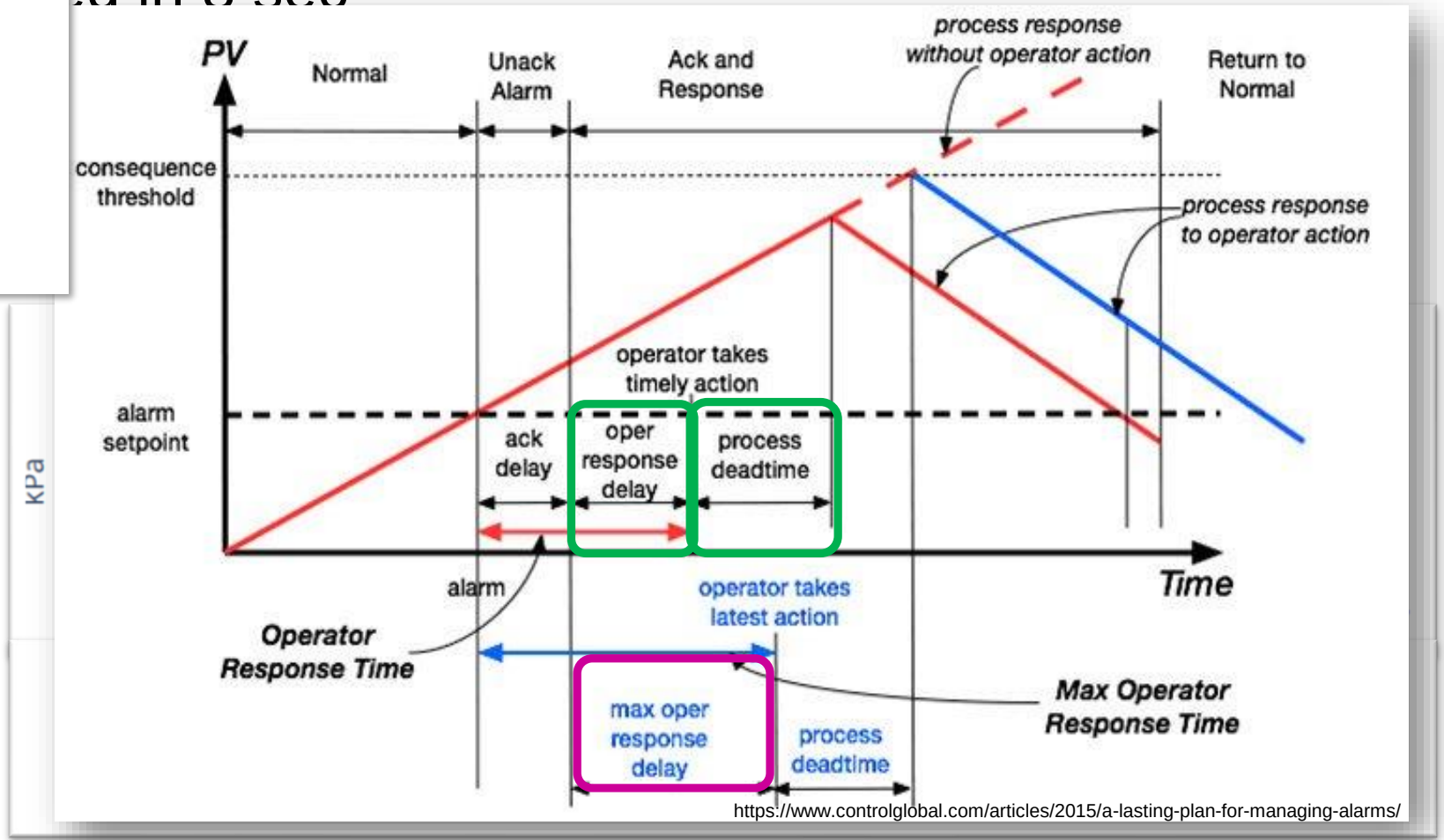


Figure 2 Parameters involved in establishing the alarm setting

12-13 kPa

ed in 8 sec



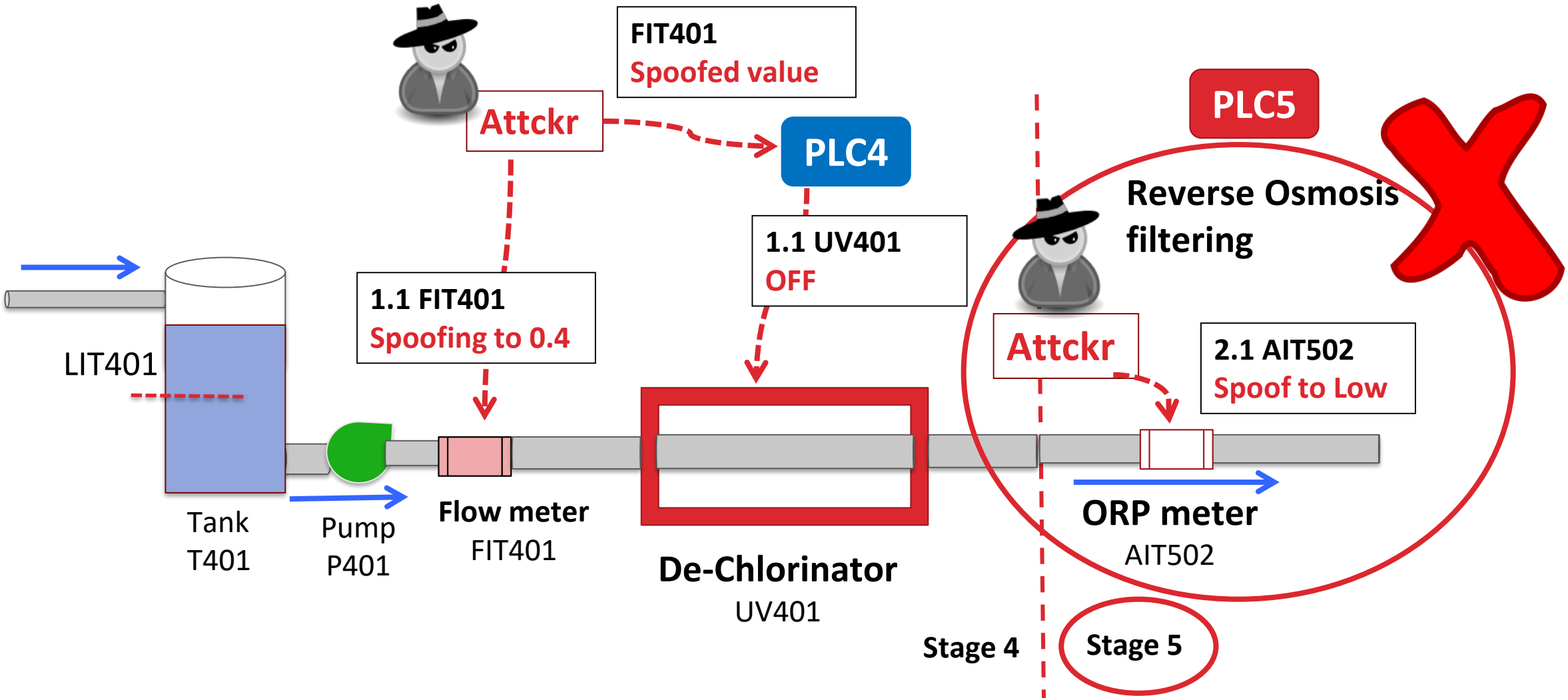
https://www.controlglobal.com/articles/2015/a-lasting-plan-for-managing-alarms/

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

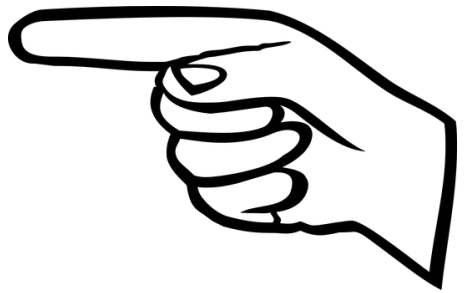
Attack Design != Implementation



Cleanup

- In traditional (IT systems) hacking the goal is to stay undetected. In cyber-physical exploitation it is not an option because of physical effect
  - Changes things in physical world which cannot hidden by e.g. “erasing logs”
  - Visible to observers

- Create forensic footprint of
  - What operators think is currently causing process upset
  - What the investigators should identify as cause of the incident/accident
  - E.g. time attack to specific employee shift or modify attack in response to process troubleshooting



Why TRITON-like implant is a good idea

‘Dormant’ implant in controller memory

Engineering workstation

trilog.exe

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

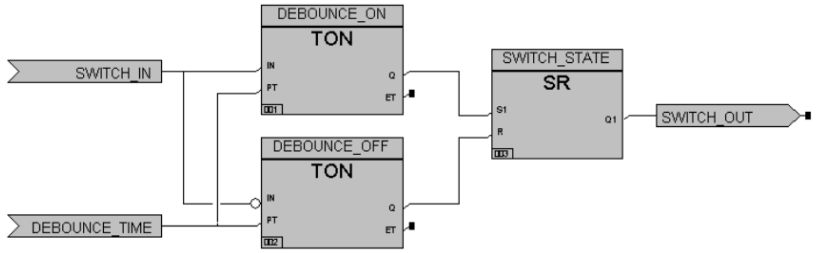
TriStation Engineering Protocol

Logic Download

(compiled for PPC, executed on CPU)

“Execute my shellcode please”

“Your wish is my command”



Cyber-physical attack components

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)

Often hardest to achieve

2

Prevent response

Operators

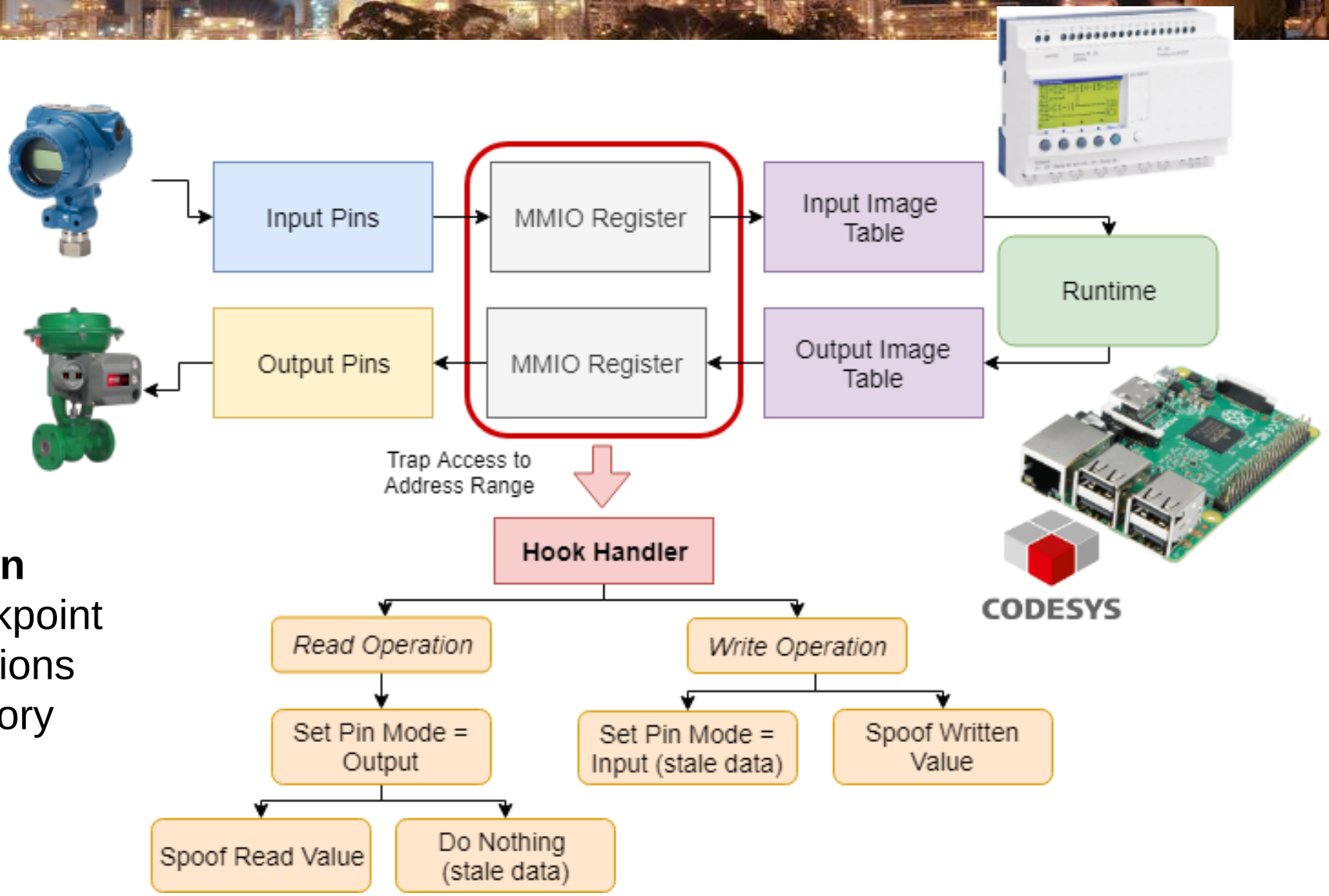
- Blind
- Mislead

Control / Safety System

- Modify operational / safety limits
- Blind about process state

OT Payload

One-stop shopping: Manipulate process



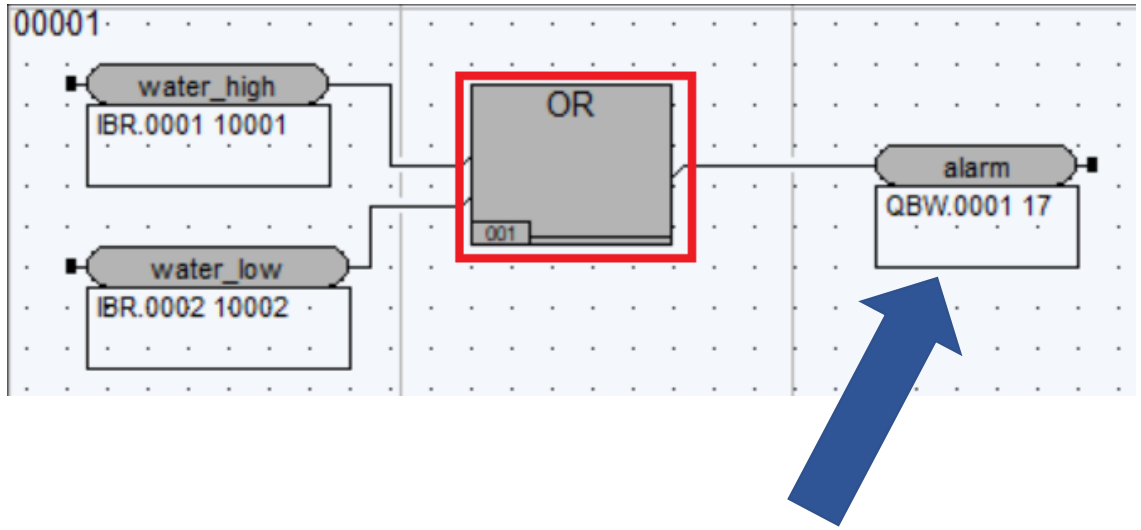
I/O manipulation

- Memory breakpoint
- Patch instructions
- Change memory permissions

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

One-stop shopping: Prevent responce

Alarm suppression

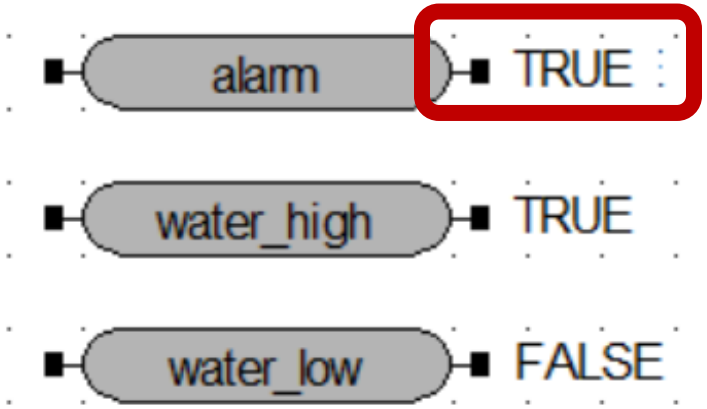


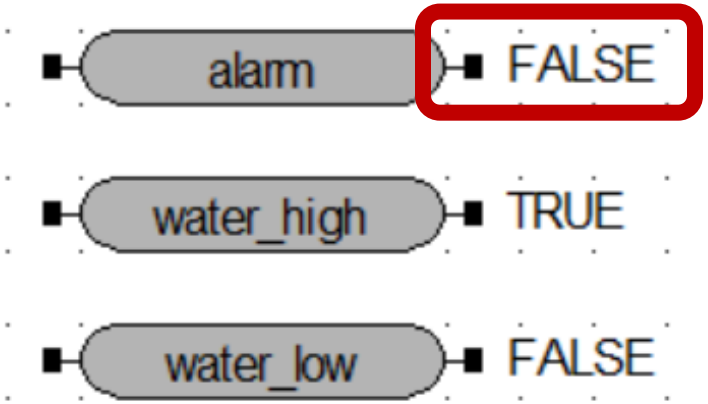

```
                                # CODE XREF: end_loop+1C↓j
li          r28, 0
stw         r28, -4(r2)
lis         r27, _water_high@ha
lwz         r28, _water_high@l(r27)
clrlwi      r28, r28, 31  # r28 := water_high
lis         r26, _water_low
lwz         r27, _water_low(r26)
clrlwi      r27, r27,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

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

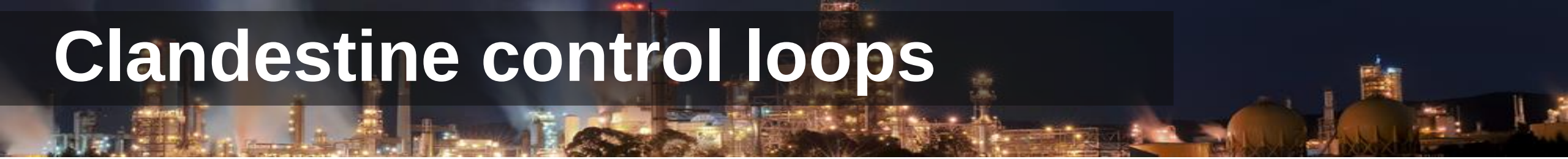
One-stop shopping: Alarm suppression

```
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)
```





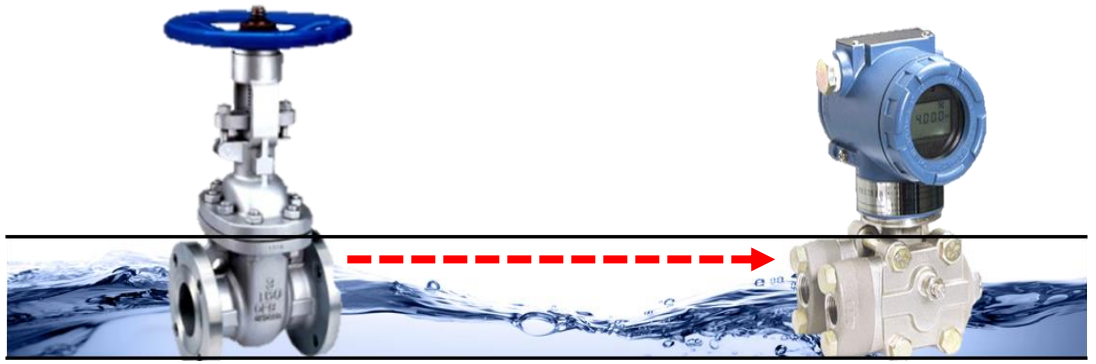
Clandestine control loops



- Cyber-physical attack cycle of process observation & manipulation to achieve desired (damaging) state
- Attack timing is crucial
  - Processes aren’t vulnerable all the time
  - Many damage scenarios take time to execute
- Attack coordination is crucial
  - Observation of state A in component B needs to trigger payloads X, Y, Z (next slide)
- **Requires granular control across process**
  - Manage task quantity & timing

One-stop shopping: Implant comms

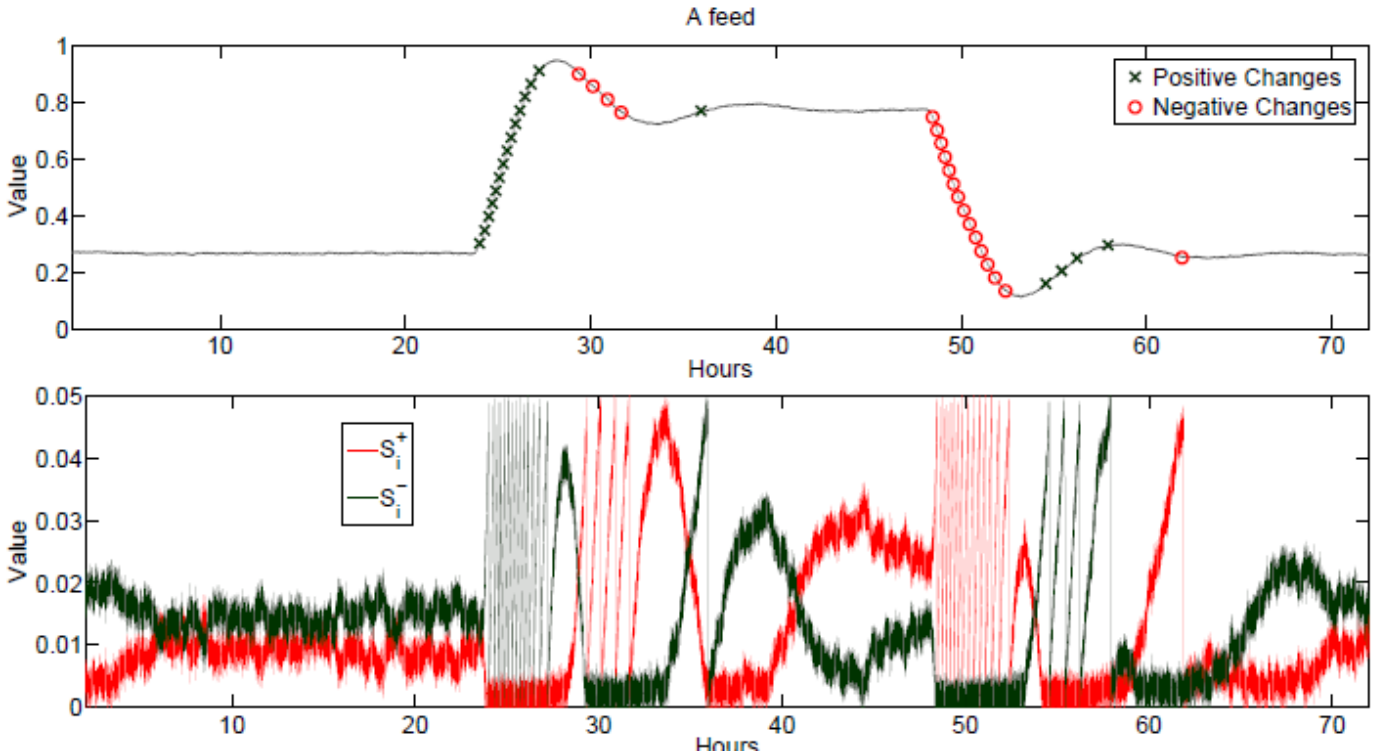
```
    1 2018-03-20 14:05:51.071836… 192.168.1.88  192.168.1.2   TRISTATION   48 33279 → 1502 Len=6
    2 2018-03-20 14:05:51.082132… 192.168.1.2   192.168.1.88  TRISTATION   64 1502 → 33279 Len=6 [ETHERNET FRAME CHECK SEQUENCE
    3 2018-03-20 14:05:51.090787… 192.168.1.88  192.168.1.2   TRISTATION   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  380 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 b
▸ Ethernet II, Src: 40:00:00:00:00:02 (40:00:00:00:00:02), Dst: Vmwa
▸ 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
        singleScan: 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

0000  00 0c 29 28 dd c5 40 00  00 00 00 02 08 00 45 00   ..)(..@. ......E.
0010  00 e6 05 d5 00 00 1e 11  12 88 c0 a8 01 02 c0 a8   ........ ........
0020  01 58 05 de 81 ff 00 d2  00 00 05 00 c4 00 01 01   .X...... ........
0030  6c 00 00 00 3d 18 c4 00  01 00 00 00 0d 00 01 01   l...=... ........
0040  00 00 00 50 80 00 00 00  80 00 00 00 40 00 00 00   ...P.... ....@...
0050  60 00 00 50 fe 00 ff af  ff 00 00 20 00 20 00 20   `..P.... ... . .
0060  00 00 00 00 00 00 20 1b  00 00 c8 00 c8 00 b9 00   ...... . ........
0070  5c 98 00 00 02 00 fa 75  ab 5a 4e 4f 5a 4f 4d 49   \......u .ZNOZOMI
0080  00 05 02 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 06 00   ........ ........
00a0  02 00 00 04 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 f0 0f 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 f1 64 64 ec 69 82  83 42 00 00 4d 61 6e 61   ...dd.i. .B..Mana
00e0  67 65 72 00 00 00 00 00  00 00 00 00 00 00 00 00   ger..... ........
00f0  00 00 1a a5                                       ....
```



EXPECTATION vs. REALITY

Detection of process state change

Non-Parametric Cumulative Sum (NCUSUM)




```
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 ~= 0.11% of DRAM
(*unoptimized*)

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

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

* 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/

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

Q & A

Marina Krotofil
@marmusha
marmusha@gmail.com