Cyber-Physical Attack Lifecycle

Marina Krotofil

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

Note

This session is based on talks:

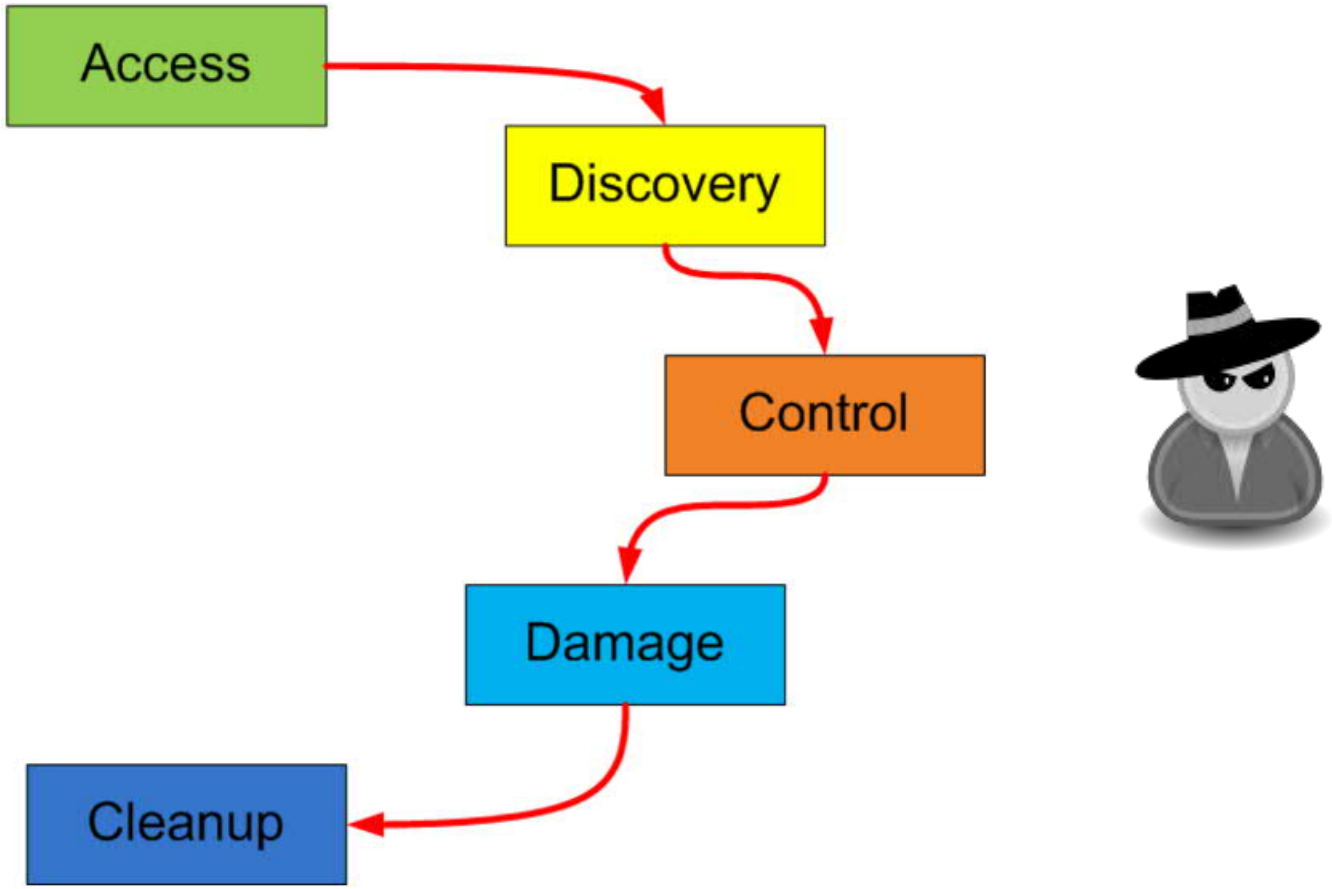
- M. Krotofil “Rocking the Pocket Book: Hacking Chemical Plants for Fun and Profit”, Black Hat, USA, 2015
- J. Wetzels, M. Krotofil “A Diet of Poisoned Fruit: Designing Implants and OT Payloads for ICS Embedded Devices”, TROOPERS, Germany, 2019

https://www.blackhat.com/docs/us-15/materials/us-15-Krotofil-Rocking-The-Pocket-Book-Hacking-Chemical-Plant-For-Competition-And-Extortion.pdf
https://troopers.de/downloads/troopers19/TROOPERS19_NGI_IoT_diet_poisoned_fruit.pdf

Cyber-Physical Attack Development Lifecycle

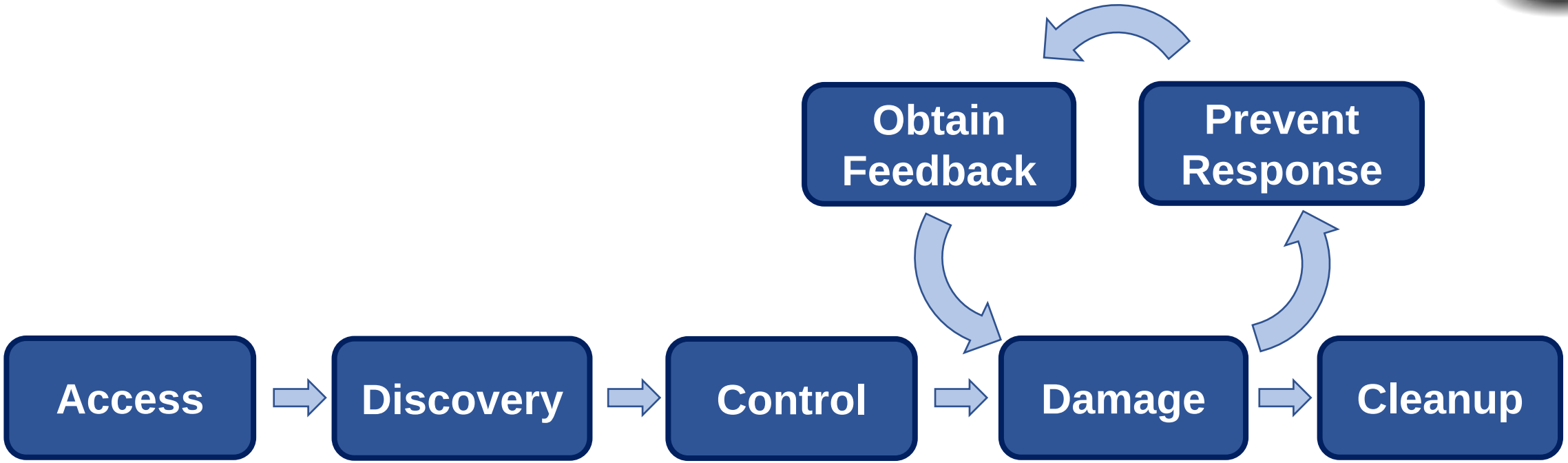
- **If you know how attackers work, you can figure out how to stop them**
- Attack lifecycle is a common method to describe a process of conducting cyber attacks

“Stages of SCADA attack”, 2007



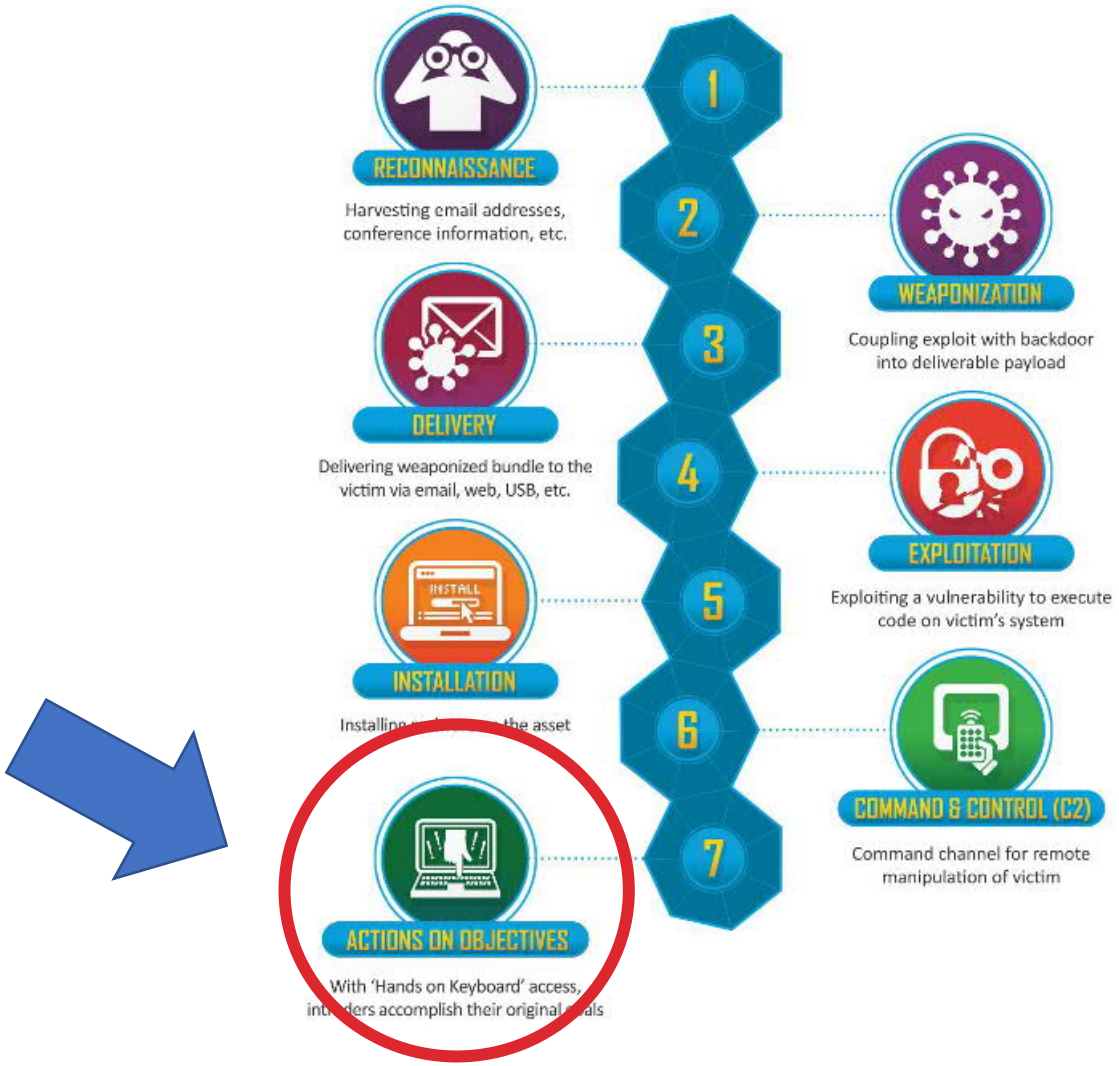
J. Larsen. Breakage. Black Hat Federal (2007)

Cyber-Physical Attack Lifecycle



Lockheed Martin, the Cyber Kill Chain®

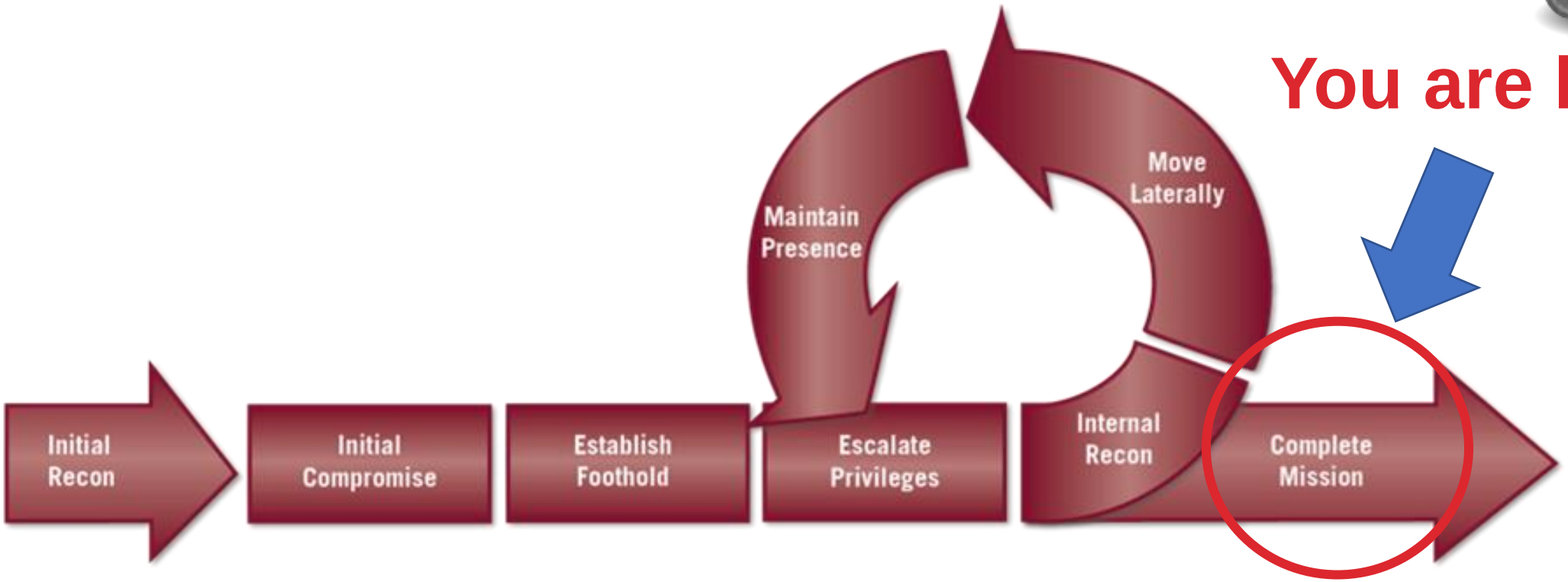
You are here



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

Mandiant Attack Lifecycle

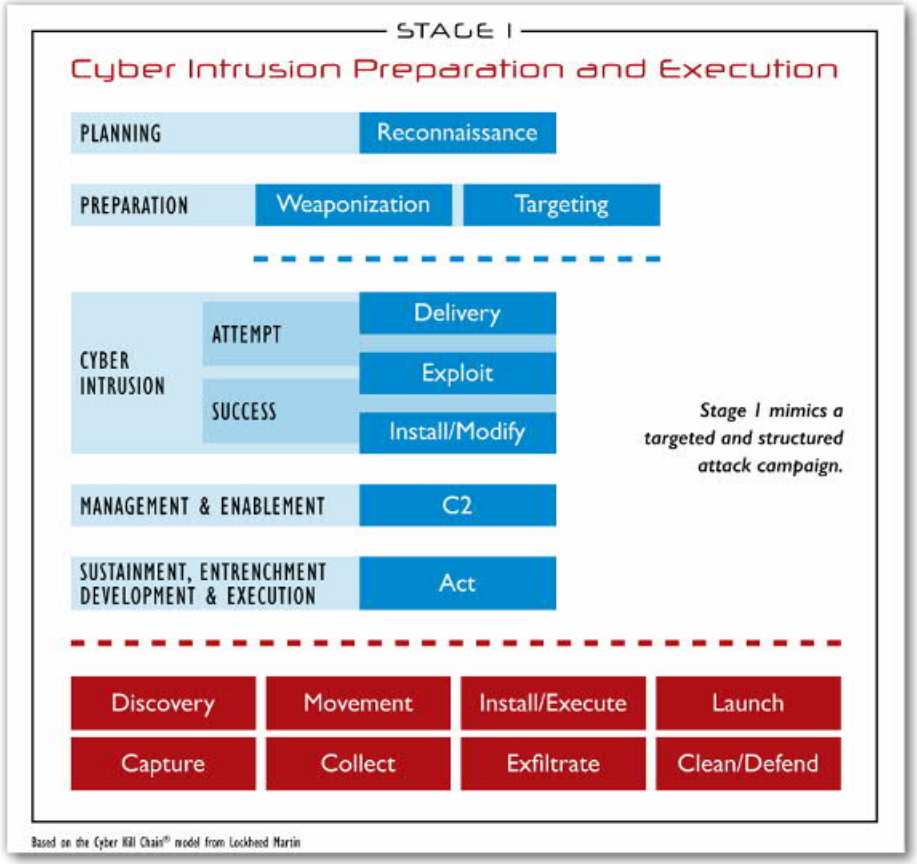
You are here

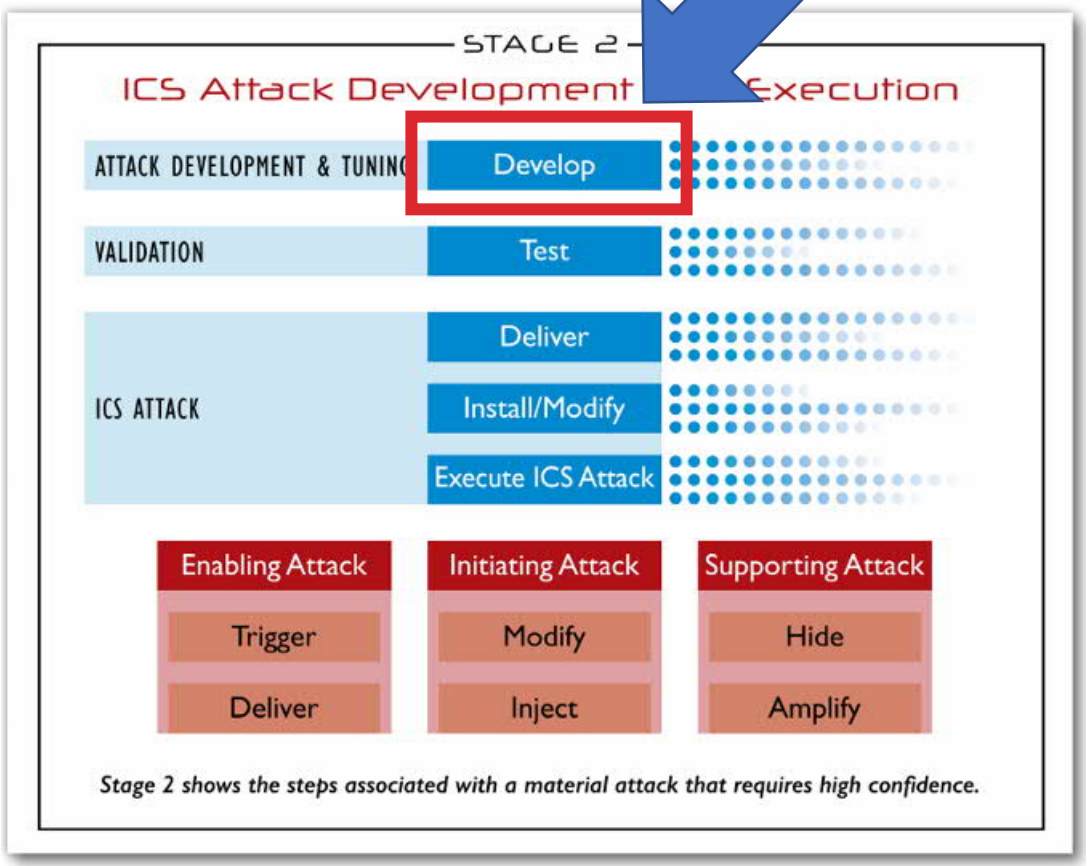


http://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/

SANS Industrial Control System Cyber Kill Chain

You are here





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

ICS MITRE ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter
Engineering Workstation Compromise	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction	**Impact**
Internet Accessible Device	Native API						Point & Tag Identification		Denial of Service	Damage to Property
Remote Services	Scripting						Program Upload		Device Restart/Shutdown	Denial of Control
Replication Through Removable Media	User Execution						Screen Capture		Manipulate I/O Image	Denial of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings	Loss of Availability
Spearphishing Attachment									Rootkit	Loss of Control
Supply Chain Compromise									Service Stop	Loss of Productivity and Revenue
Wireless Compromise									System Firmware	Loss of Protection
										Loss of Safety
										Loss of View
										Manipulation of Control
										Manipulation of View
										Theft of Operational Information

A bit everywhere :-)

https://collaborate.mitre.org/attackics/index.php/Main_Page

Why to attack ICS

Industry means big business

Big business == $$$$$$$

Why to attack ICS

Industry means big business
Big business == $$$$$$$

Alan Paller of SANS (2008):

In the past two years, hackers have in fact successfully penetrated and extorted multiple utility companies that use SCADA systems.

Hundreds of millions of dollars have been extorted, and possibly more. It's difficult to know, because they pay to keep it a secret. **This kind of extortion is the biggest untold story of the cybercrime industry.**

Attack scenario: Persistent economic damage

What can be done to the process

Equipment damage	Production damage	Compliance violation
❑ Equipment overstress ❑ Violation of safety limits	❑ Product quality and product rate ❑ Operating costs ❑ Maintenance efforts	❑ Safety ❑ Pollution ❑ Contractual agreements

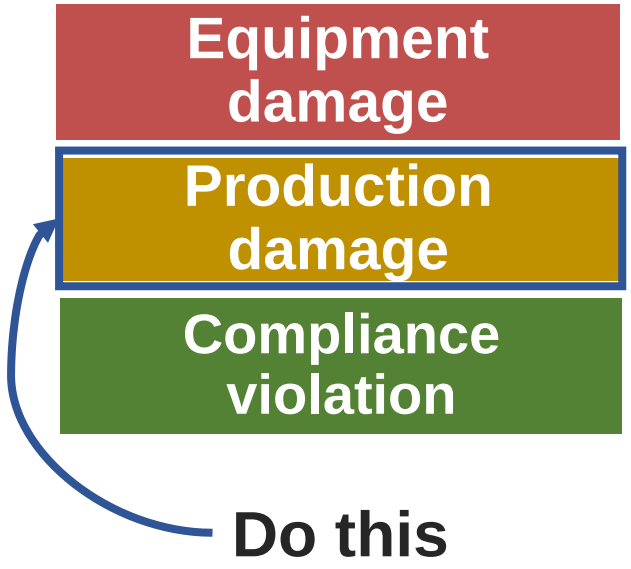
Paracetamol

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

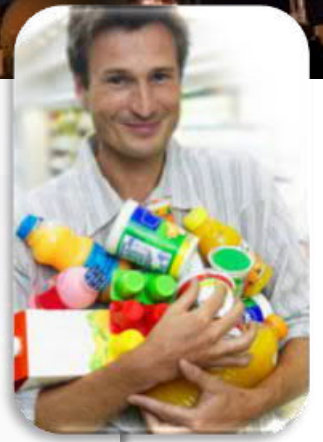
Source: http://www.sigmaaldrich.com/

Attack considerations

- **Equipment damage**
  - Comes first into anybody's mind (+)
  - Irreversible (∓)
  - Unclear collateral damage (-)
  - May transform into compliance violation, e.g. if it kills human (-)
- **Compliance violation**
  - Compliance regulations are public knowledge (+)
  - Unclear collateral damage (-)
  - Must be reported to the authorities (∓)
  - Will be investigated by the responsible agencies (-)



Vinyl Acetate Monomer plant (model)



Plants for sale

From LinkedIn

+Follow Tommy

Used VAM - Vinyl Acetate Monomer plant for sale & relocation! If any interest, please contact me!

Tommy Heino
Industrialist & Entrepreneur, Owner, XHL Business Engineering
Top Contributor

Like • Comment (4) • Share • Follow • 3 months ago

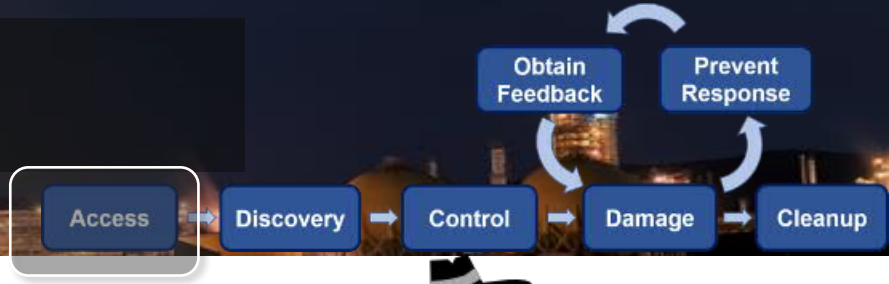
More plants offers:
http://www.usedplants.com/

Why models?

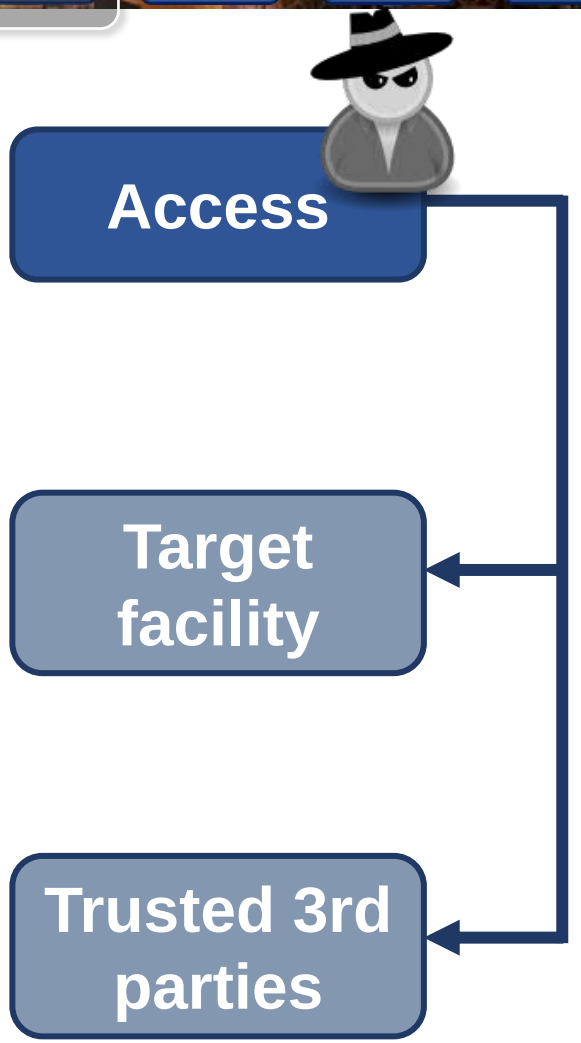
It is all about MONEY

Plants are ouch! how expensive
-> hence, researching on model

Access

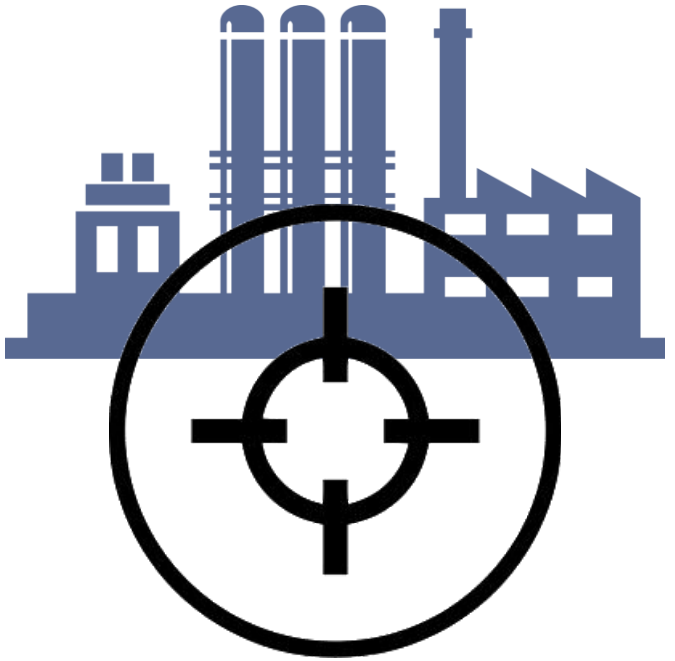


- **Target facility**
  - Discovery
  - Access to needed assets
  - Attack execution
- **Trusted 3rd party** (staging target)
  - Access to target facility
  - Access to needed assets
  - Process comprehension
- **Non-targeted**/Opportunistic



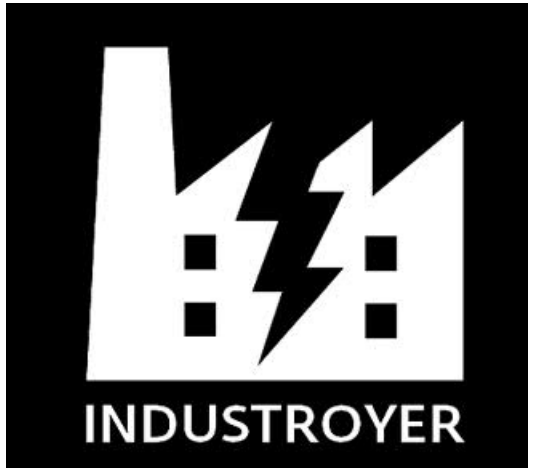
Targeting

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

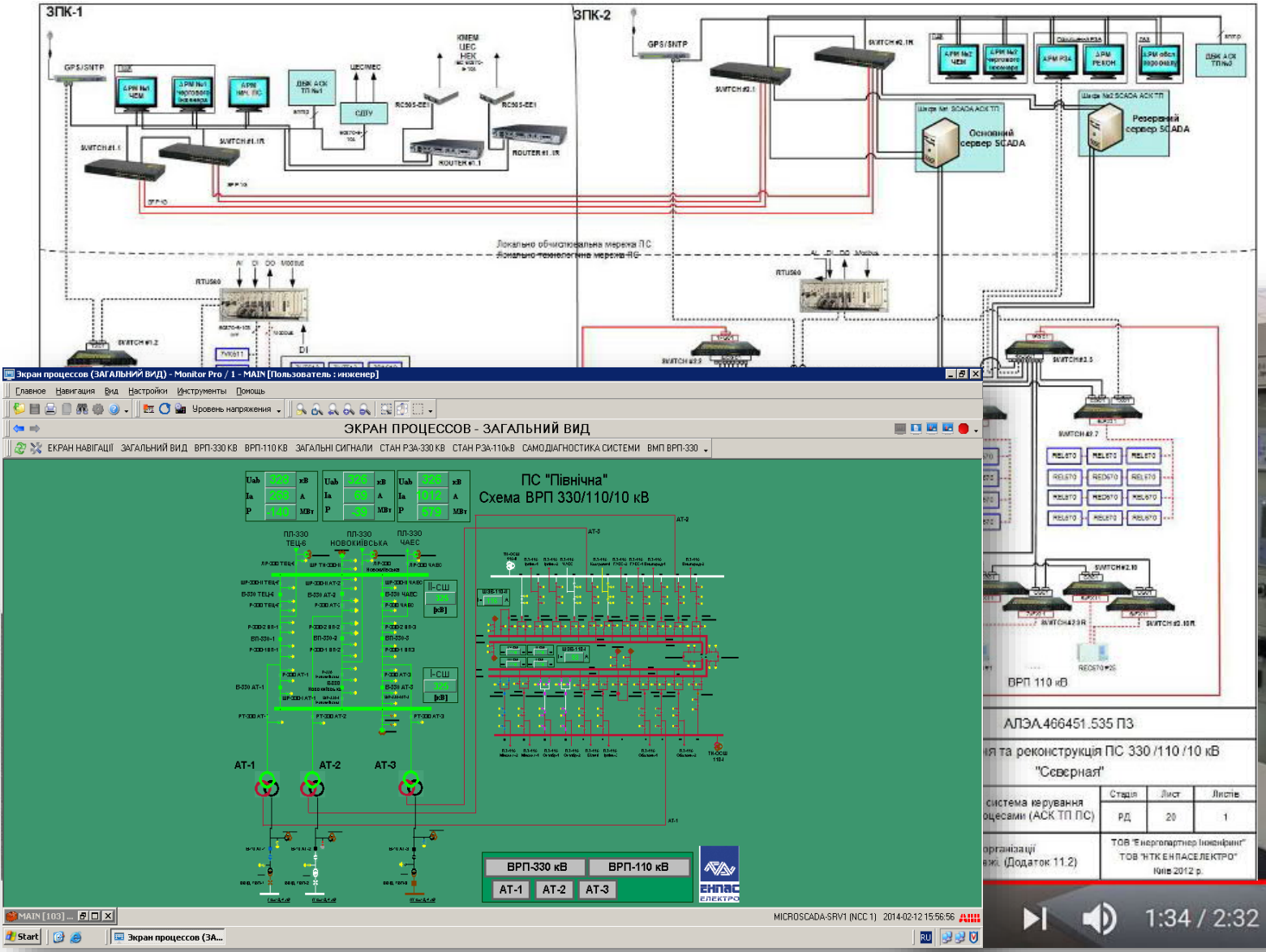


Ukraine, 2016

- 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 were publicly available

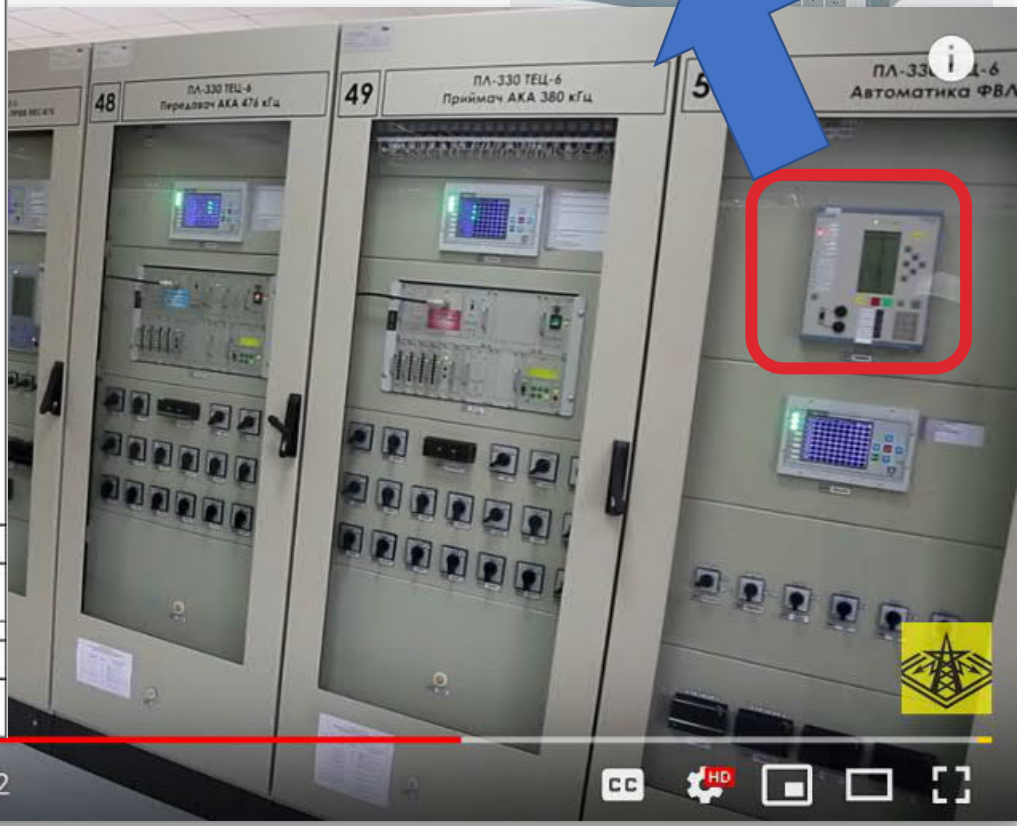


Ukraine, 2016



Targeted by malware

https://w3.siemens.com/smartgrid/global/en/products-systems-solutions/protection/distance-protection/pages/7sa63.aspx



OSINT: Tons of confidential info on Internet

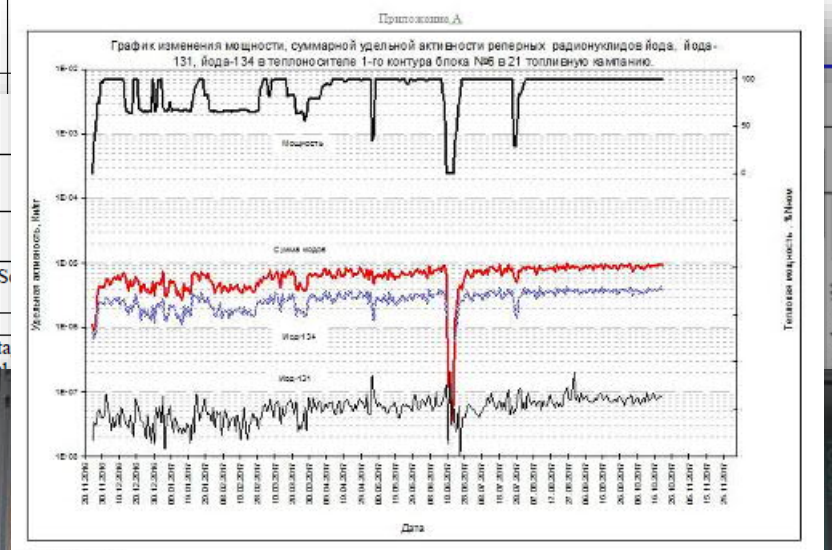
8.10.3 Alarm On-Delay and Off-Delay

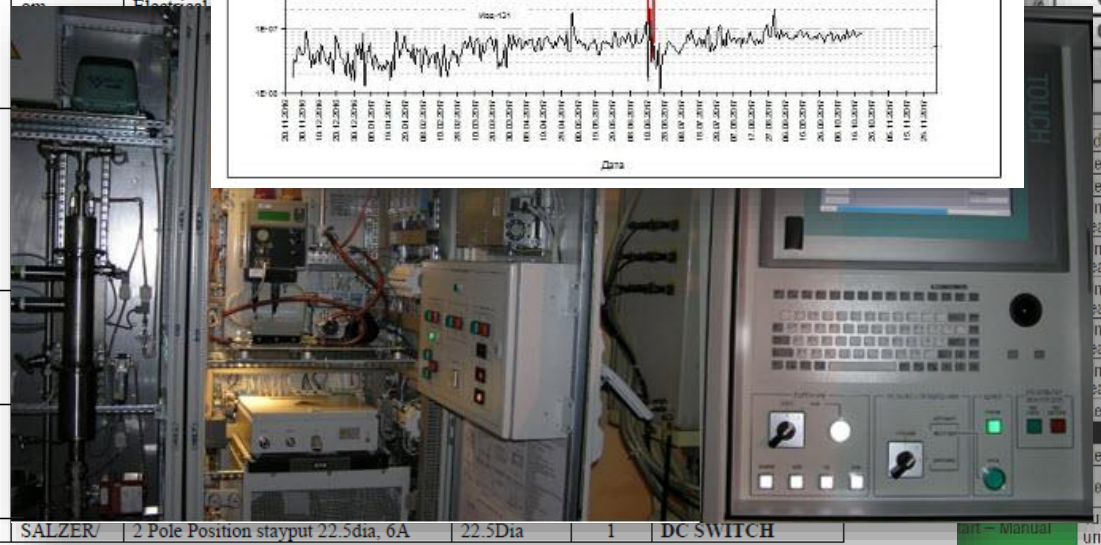
The On-Delay alarm attribute is used to avoid unnecessary alarms, by allowing alarms to be triggered once the signal has remained in the alarm state for a specified length of time. The Off-Delay alarm attribute is used to reduce chattering alarms by locking in the alarm indication for a specified period 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.

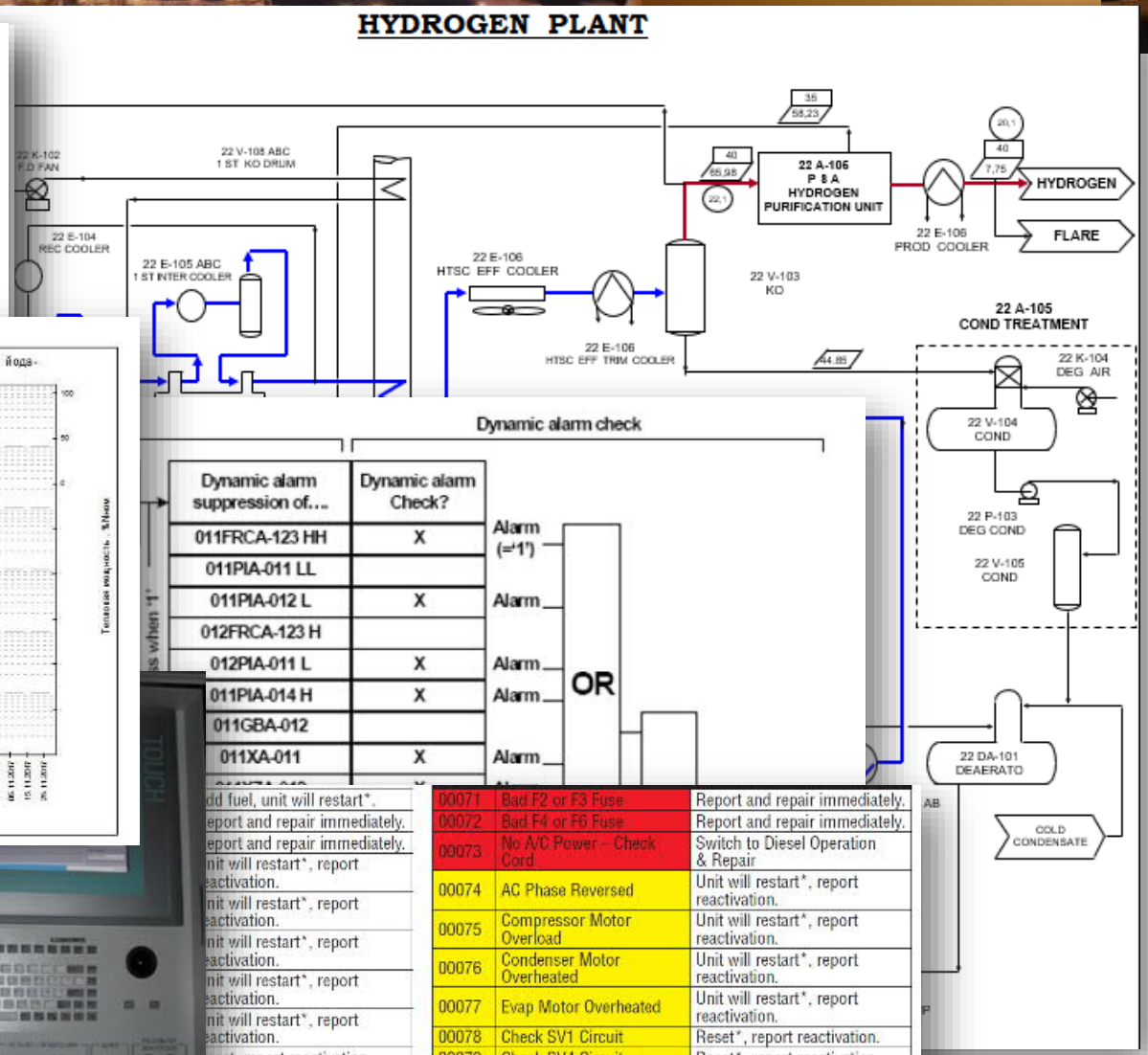
Signal type
Flow Rate

Bill of Material

Project : General Project Francis Turbine				Ref :	
Project Code:					
Item Turbine Auxiliary Control And Governor Panel(TAGP)					
Rev 0	Part No	Description	Nomen	Make	Rating/S
	1	Master Trip Relay	86TU	Areva/Alst	Aux volta
	2	Digital Speed Monitor Relay with Proximity Sensor	SM		
	3	Digital Position Indicator GUIDE VANE	GVI%		
	4	Annunciator for Trip & Alarm	30A		
		Auto/Test Switch	SW1	SALZER/	2 Pole Position staypu 22.5dia, 6A / 22.5Dia / 1 / DC SWITCH







Dynamic alarm check

Dynamic alarm suppression of...	Dynamic alarm Check?
011FRCA-123 HH	X
011PIA-011 LL	
011PIA-012 L	X
012FRCA-123 H	
012PIA-011 L	X
011PIA-014 H	X
011GBA-012	
011XA-011	X

Alarm (='1') — Alarm — Alarm — Alarm — Alarm — OR

dd fuel, unit will restart*.		
eport and repair immediately.		
eport and repair immediately.		
nit will restart*, report eactivation.		
nit will restart*, report eactivation.		
nit will restart*, report eactivation.		
nit will restart*, report eactivation.		
nit will restart*, report eactivation.		
eset, report reactivation		
eport and repair immediately.		
eport and repair immediately.		
urn switch off then back on, unit will start automatically.		
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.

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 - - [20/Jan/2016:09:44:13 +0200]
Sandbox скачивает бэкдор	184.[redacted].147 - - [20/Jan
Жертва 6 скачивает бэкдор	82.[redacted].70 - - [20/Jan

			Время												
Год	Месяц	День	8	9	10	11	12	13	14	15	16	17	21	22	Итог
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

Staging targets

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

Trojanized ICS Installers

TELVENT

Bit9

Security Centre

a part of GCHQ

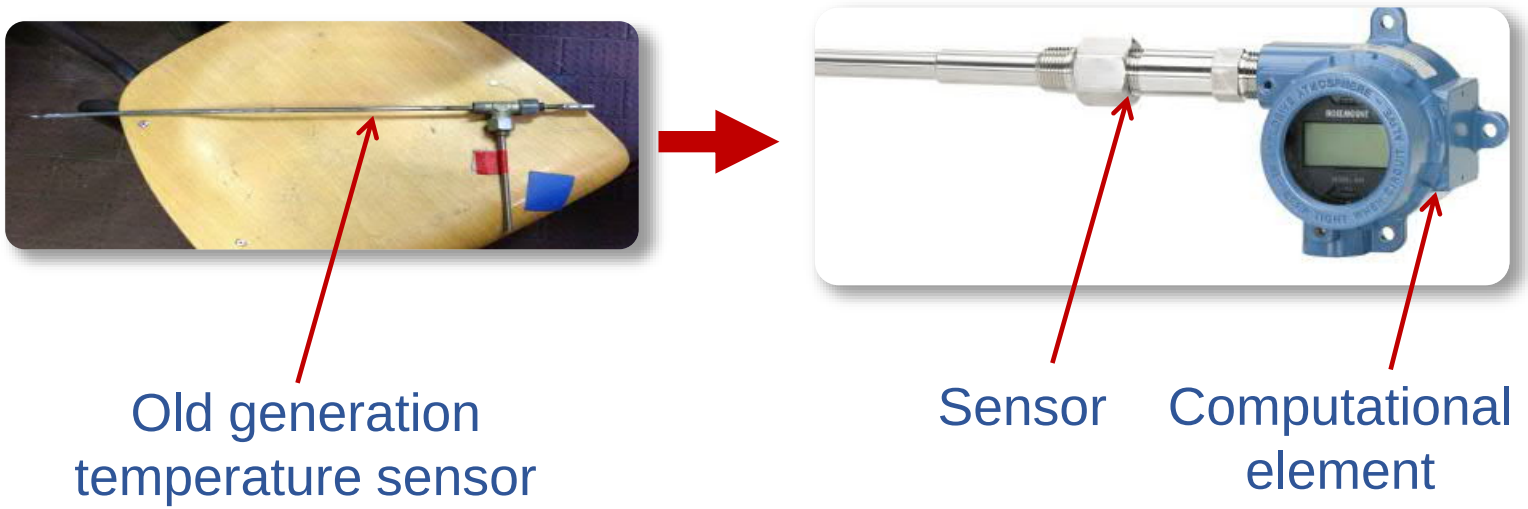
Advisory: Hostile state actors compromising UK organisations with focus on engineering and industrial control companies

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

Smart instrumentation

- **Smart instrumentation**
  - Converts analog signal into digital
  - Sensors pre-process the measurements
  - May send data directly to actuators
  - IP-enabled (part of the “Internet-of-Things”)



Promise from the vendors:

Expect instruments of the future to have multiple communication channels, much like a present-day Ethernet switch. These channels will be managed with IP adressing and server technology, **allowing the instrument to become a true data server**

Complication: Resource constraints

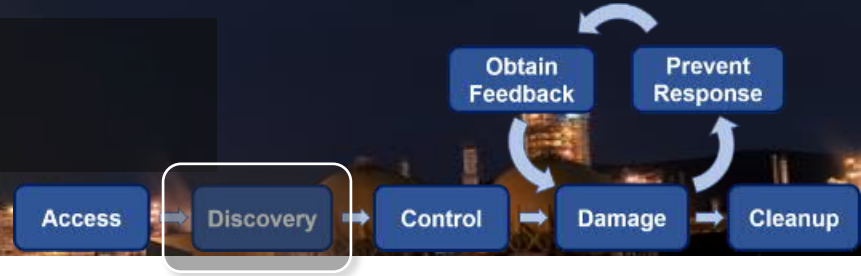
- MPC860, 50 MHz
- 6 MB Flash
- 16 MB DRAM
- 32 KB SRAM

You better enjoy XTREME programming…

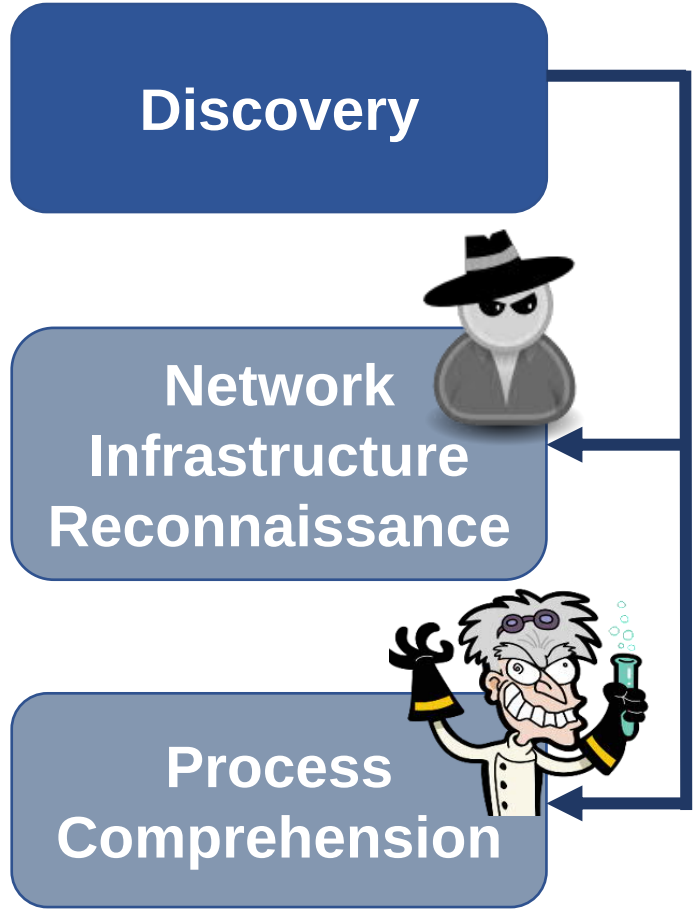
Will need to fit implant in there
Signals processing? Malicious logic? Comms?
Often stretched by normal functionality already

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

Discovery



- Network reconnaissance
  - Majority of this stage is similar to traditional IT recon process/attack life cycle, most tools will 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

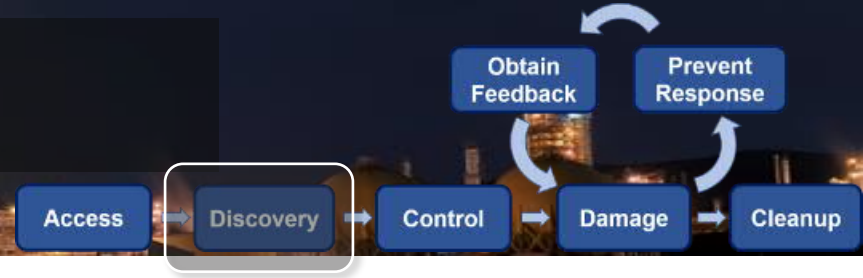
Benjamin Green
Lancaster University
Lancaster, United Kingdom
b.green2@lancaster.ac.uk

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

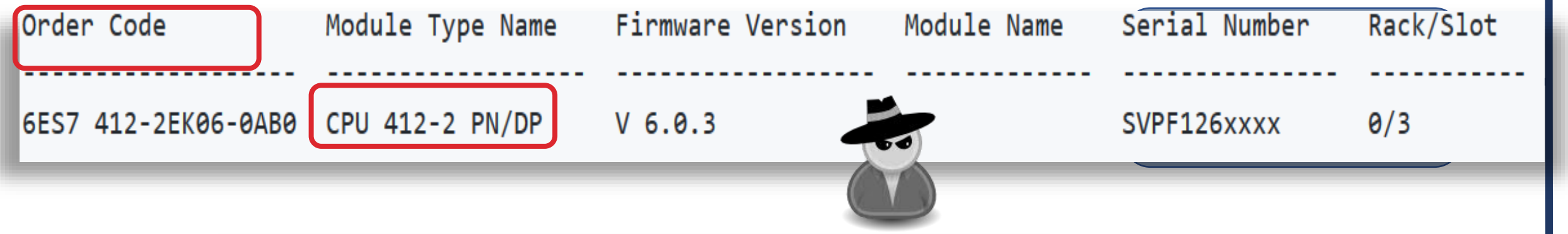
Ali Abbasi
University of Twente
Enschede, Netherlands
a.abbasi@utwente.nl

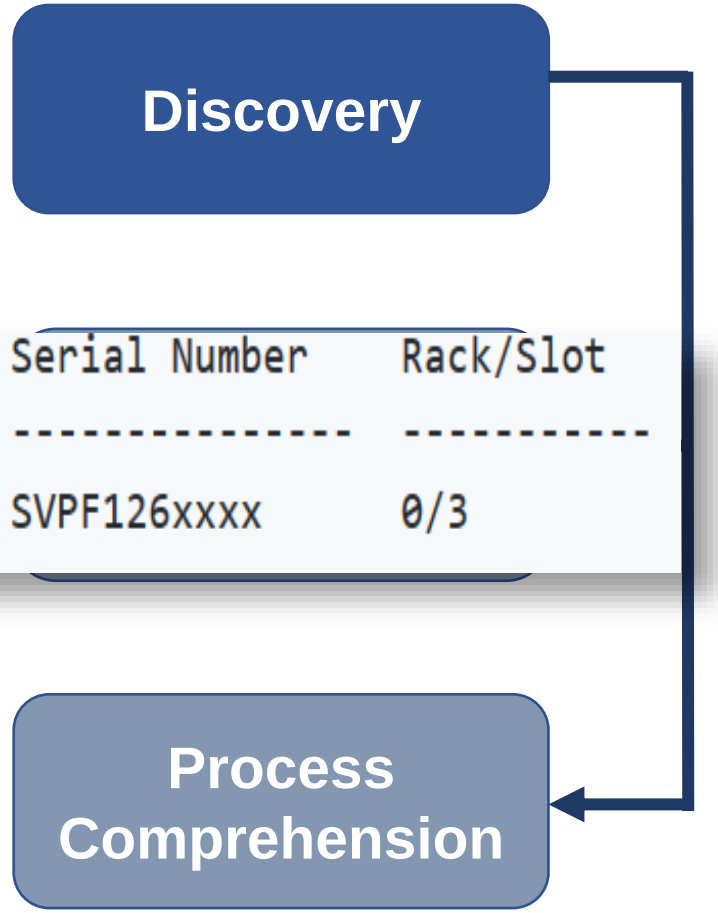
http://eprints.lancs.ac.uk/88089/1/sample_sigconf.pdf

Discovery



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





On the Significance of Process Comprehension for Conducting Targeted ICS Attacks

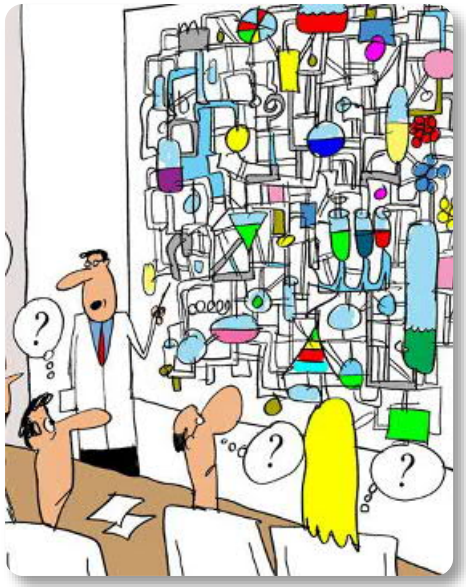
Benjamin Green
Lancaster University
Lancaster, United Kingdom
b.green2@lancaster.ac.uk

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

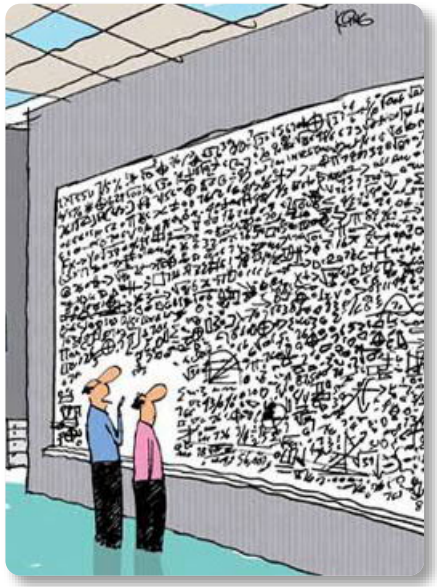
Ali Abbasi
University of Twente
Enschede, Netherlands
a.abbasi@utwente.nl

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

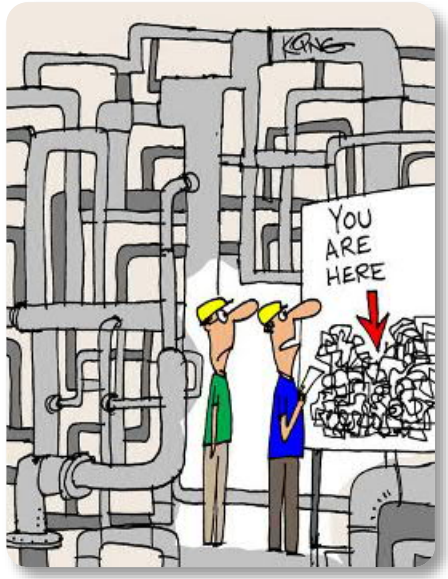
Process discovery/comprehension



What and how the process is producing



How it is controlled

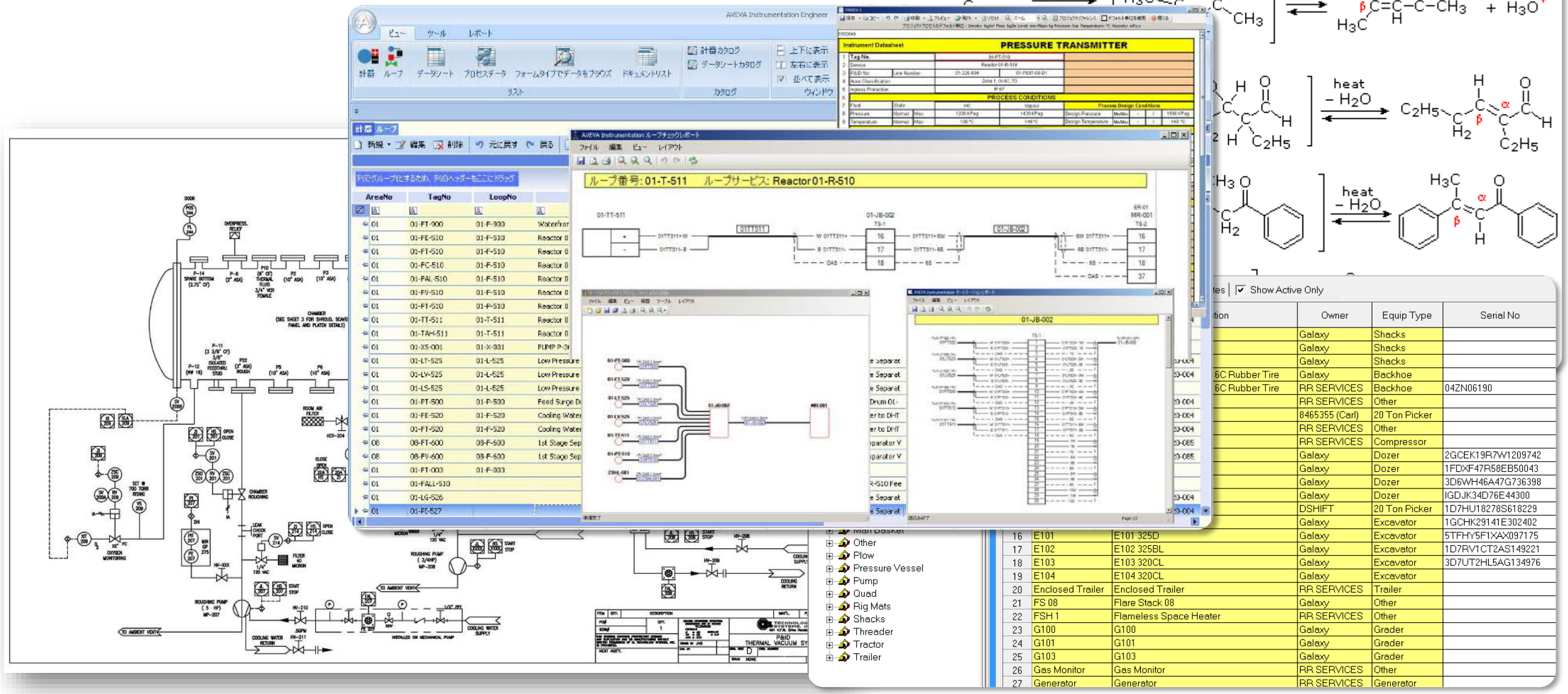


How it is build and wired

Operating & safety constraints

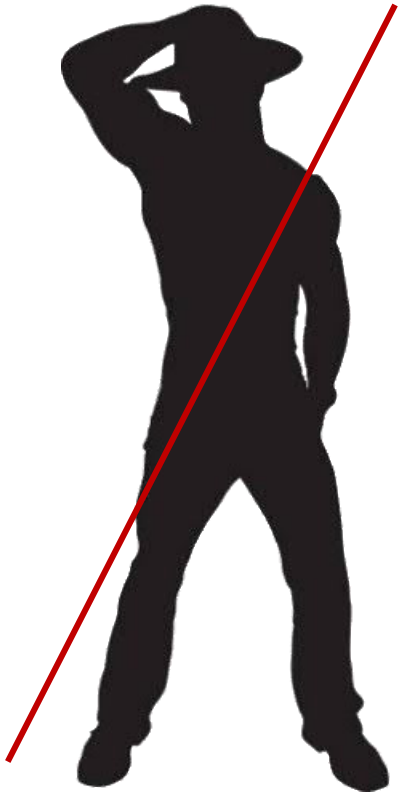
Espionage, reconnaissance
Target plant and third parties

Process Discovery



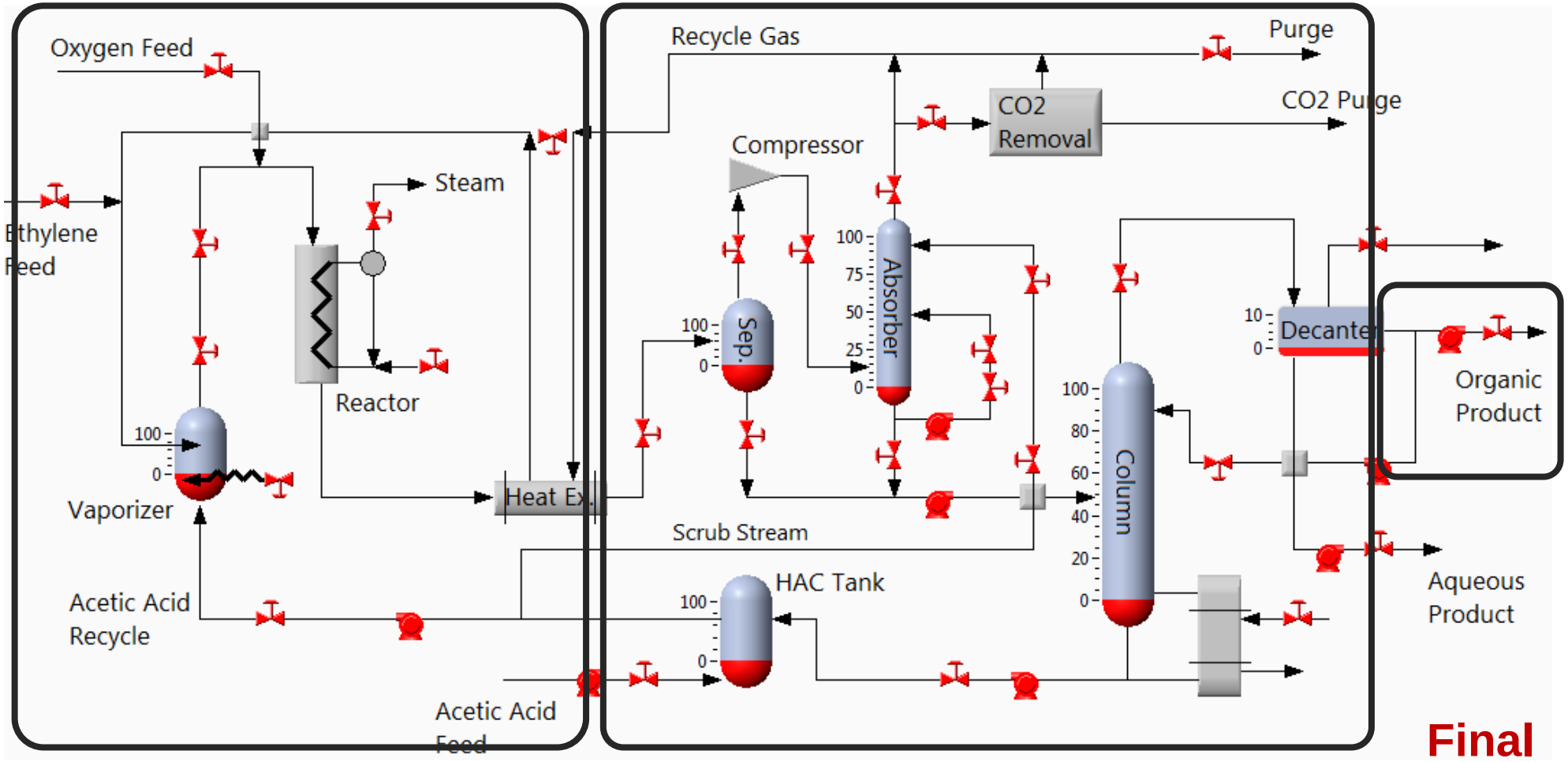
Know the equipment

Stripper is...



Stripping column

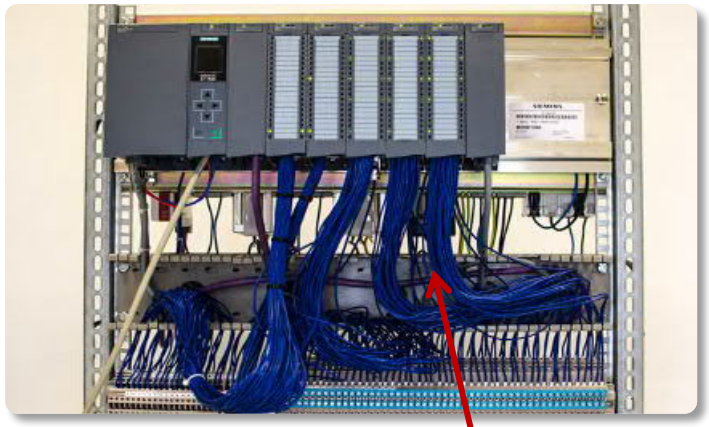
Max economic damage?



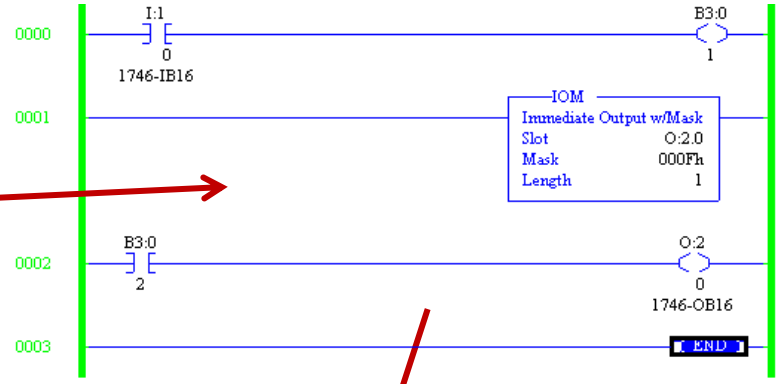
Requires input of subject matter experts

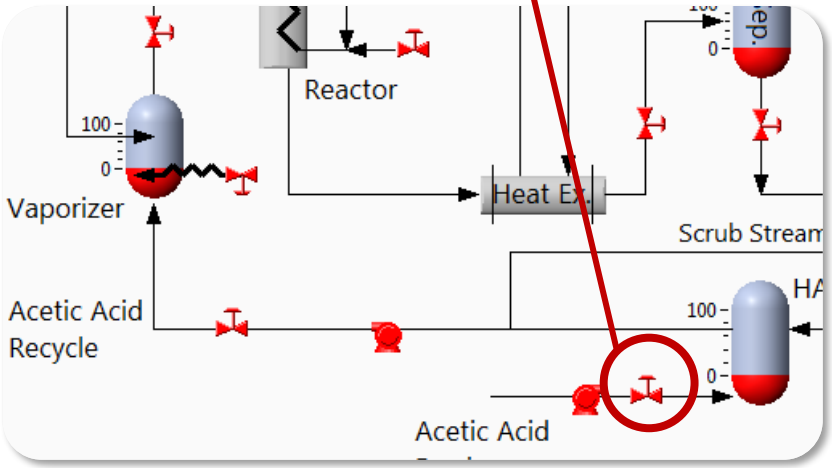
Understanding points and control logic

Programmable Logic Controller



Ladder logic



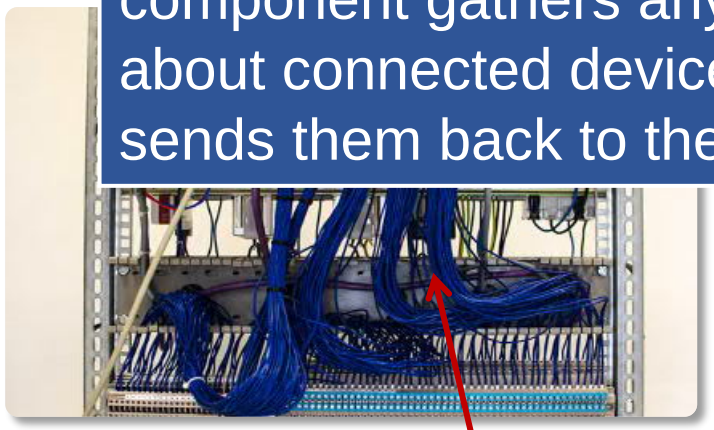


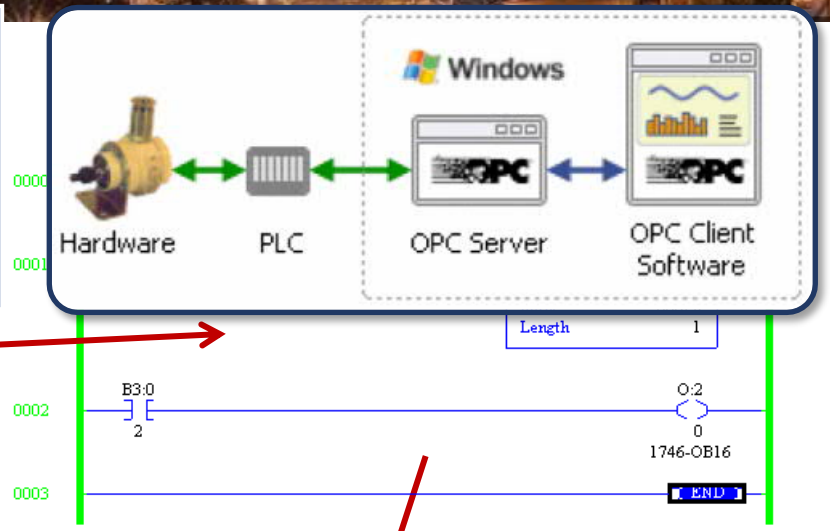
Piping and instrumentation diagram

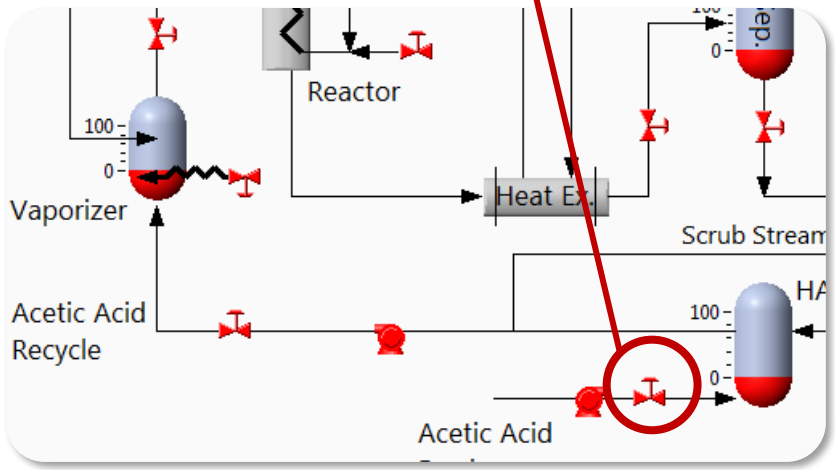
Pump in the plant

Understanding points and control logic

HAVEX: Using OPC, the malware component gathers any details about connected devices and sends them back to the C&C.



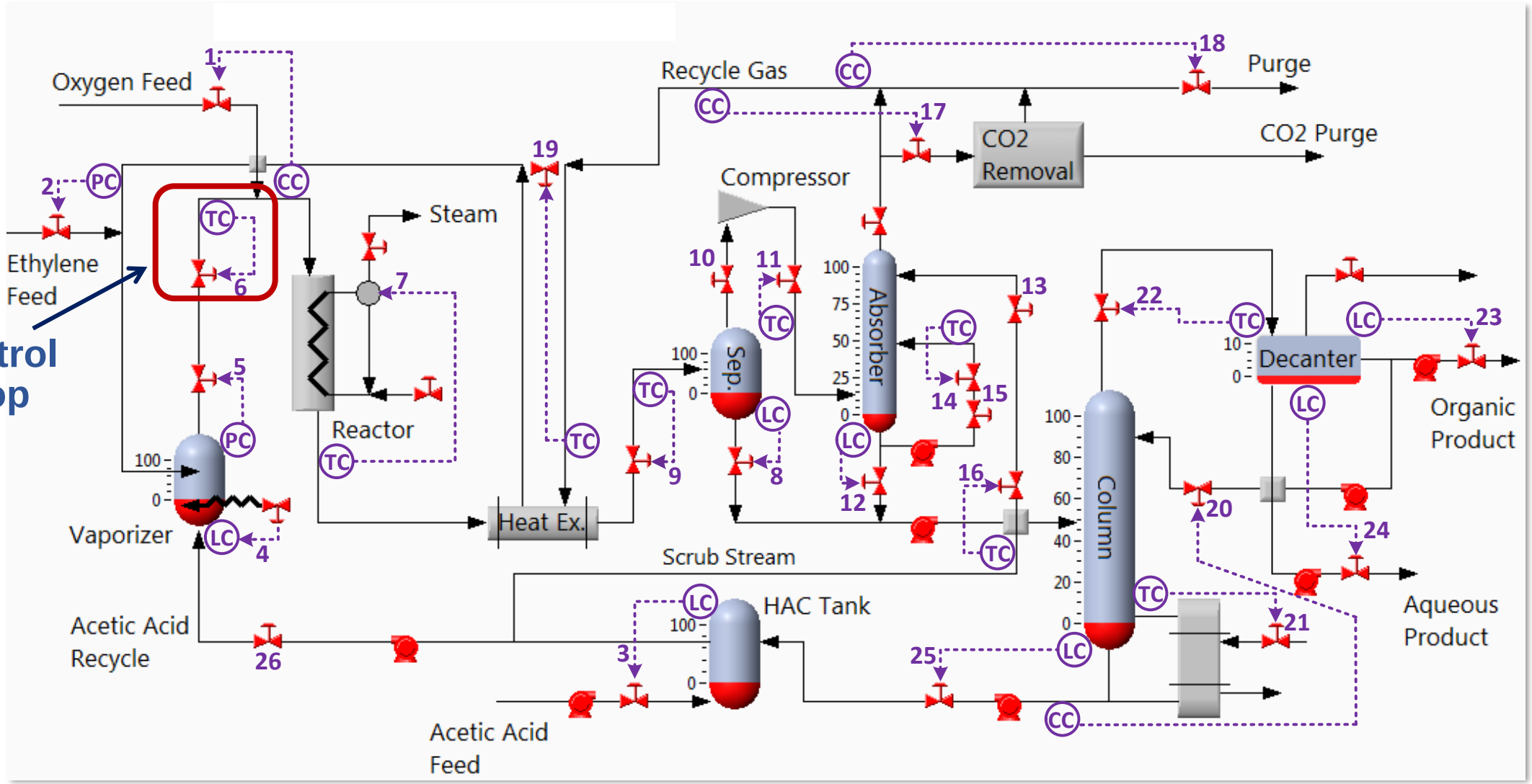




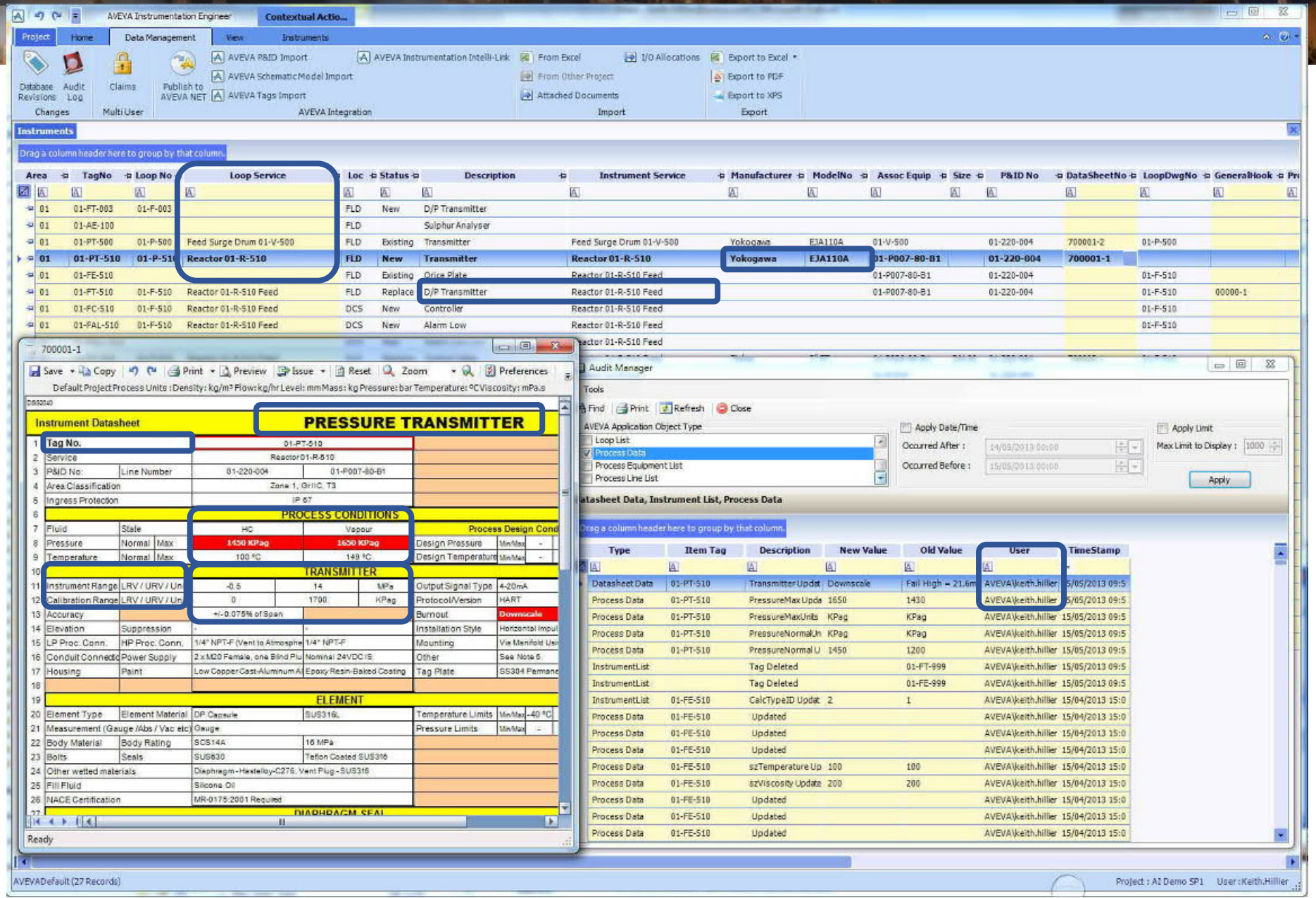
Piping and instrumentation diagram

Pump in the plant

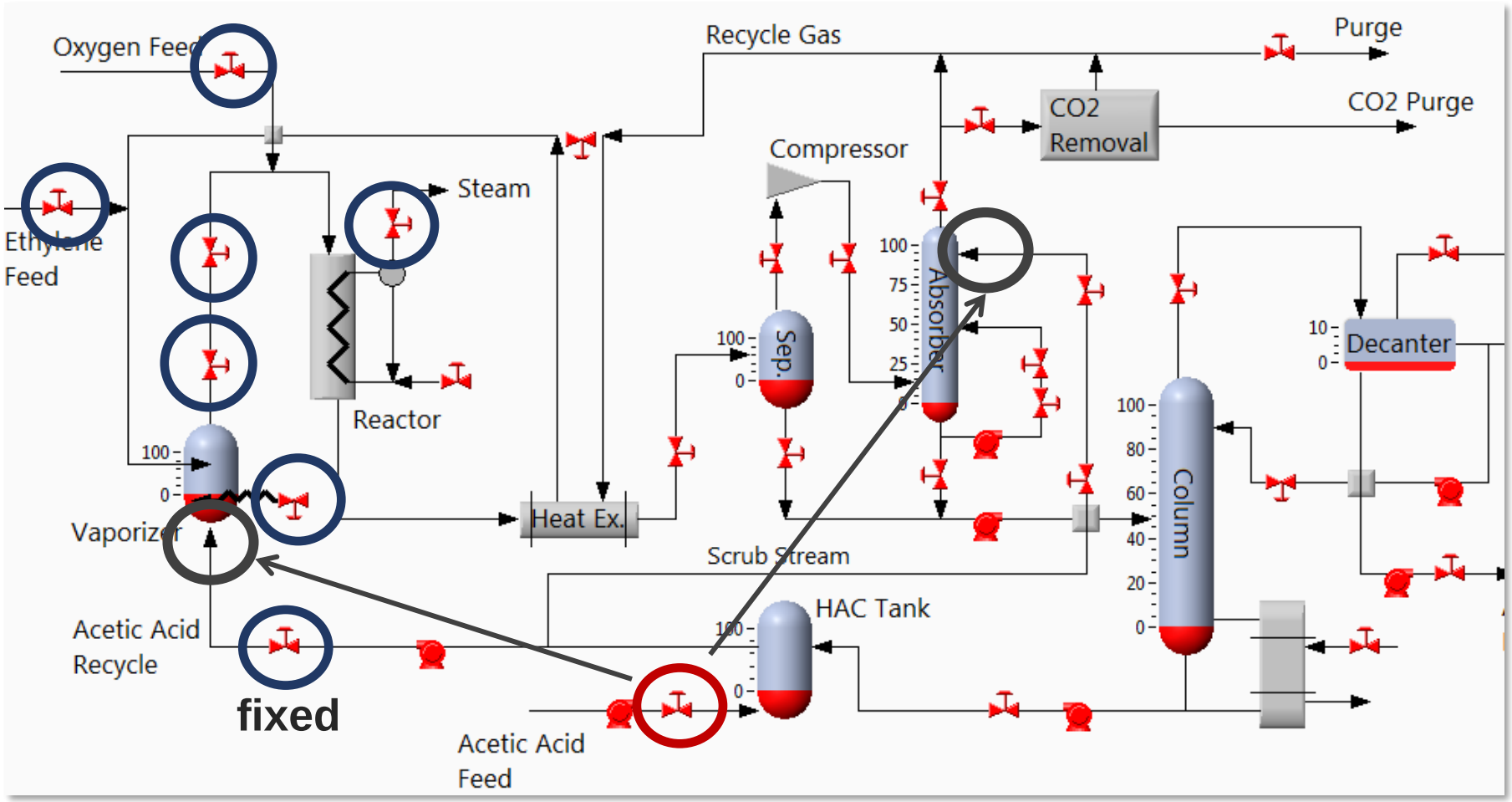
Understanding control infrastructure



Control loop configuration

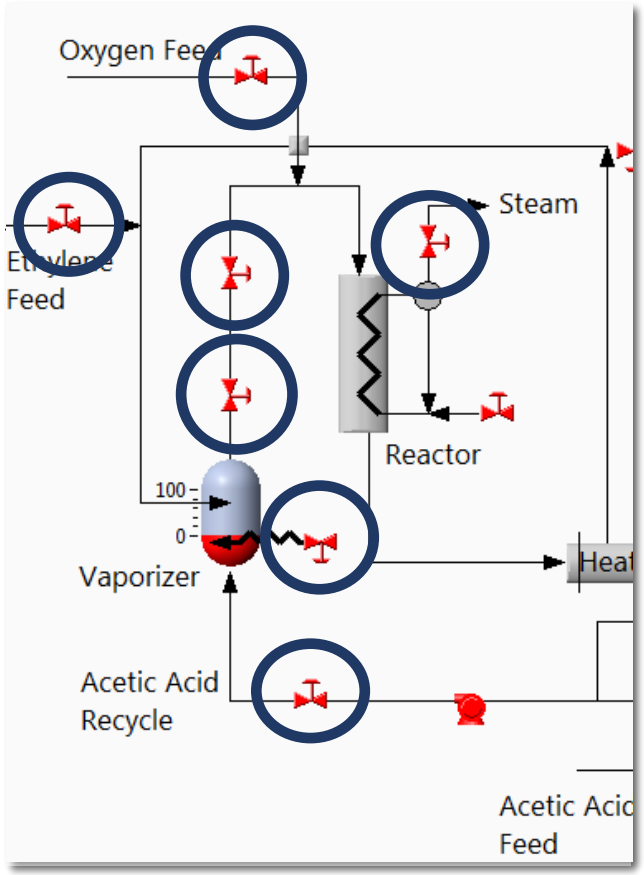


Watch the flows!



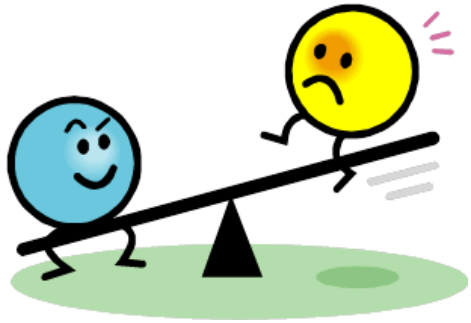
HAc flows into two sections. Not good :(

Obtaining Control != Being in control



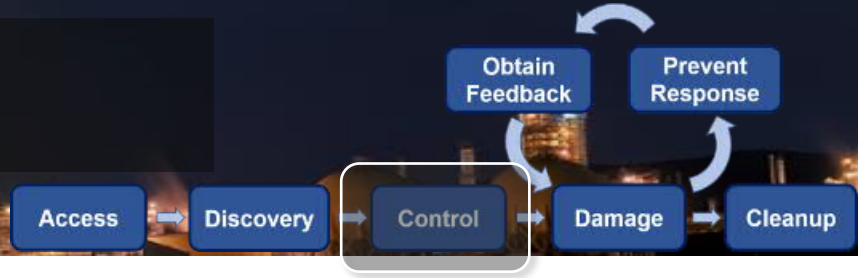
- Obtained controls might not be useful for attack goal
- How do I even speak to this thing??
- Attacker might not necessary be able to control obtained controls

Huh ???

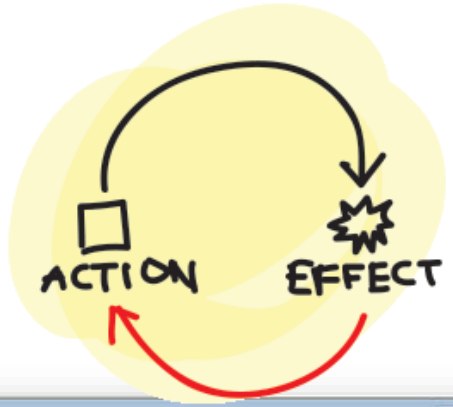


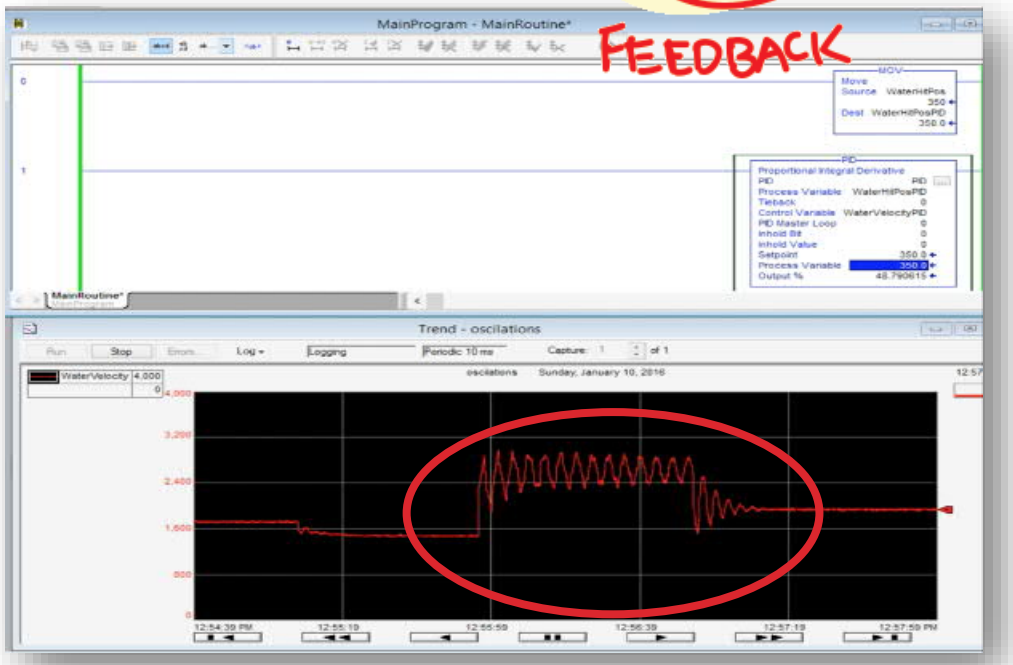
Every action has a reaction

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

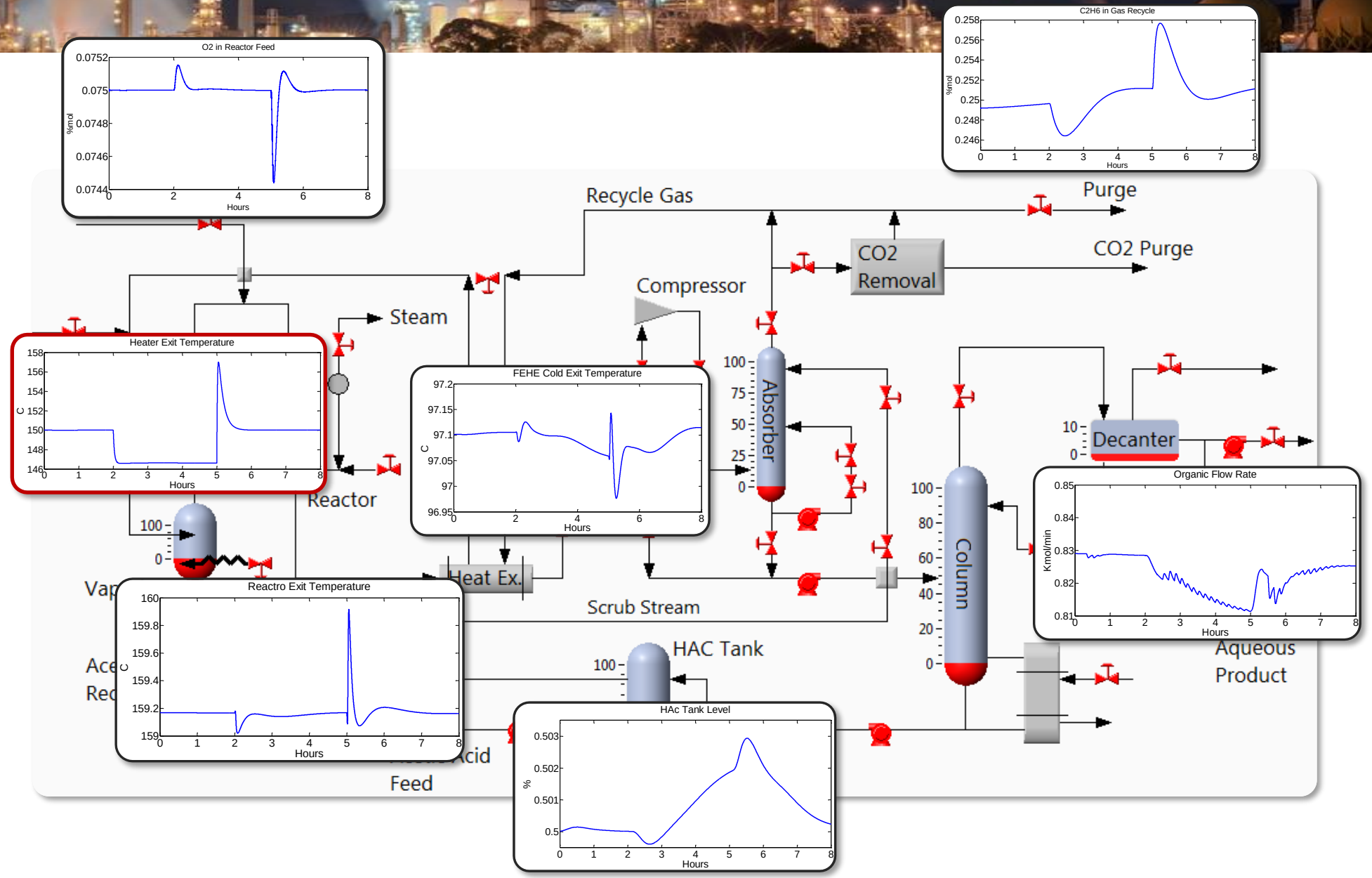
Dieter Gollmann
Hamburg University of Technology
Hamburg, Germany

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

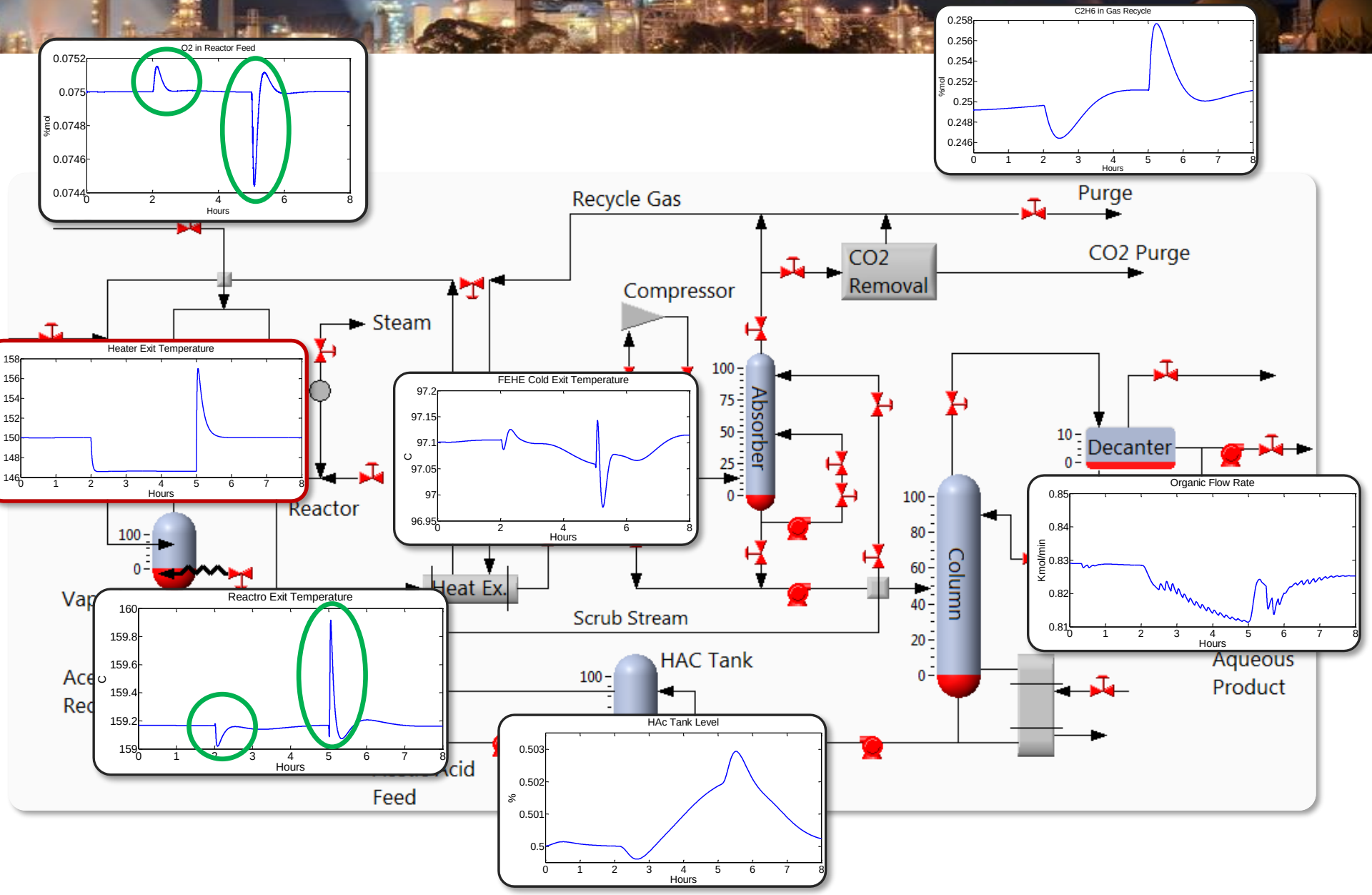
Physics of process control

- **Once connected together, physical components become related to each other by the physics of the process**
- If we adjust a valve what happens to everything else?
  - Adjusting temperature also increases pressure and flow
  - All the downstream effects need to be taken into account (upstream changes too)
- How much does the process can be changed before releasing alarms or it shutting down?

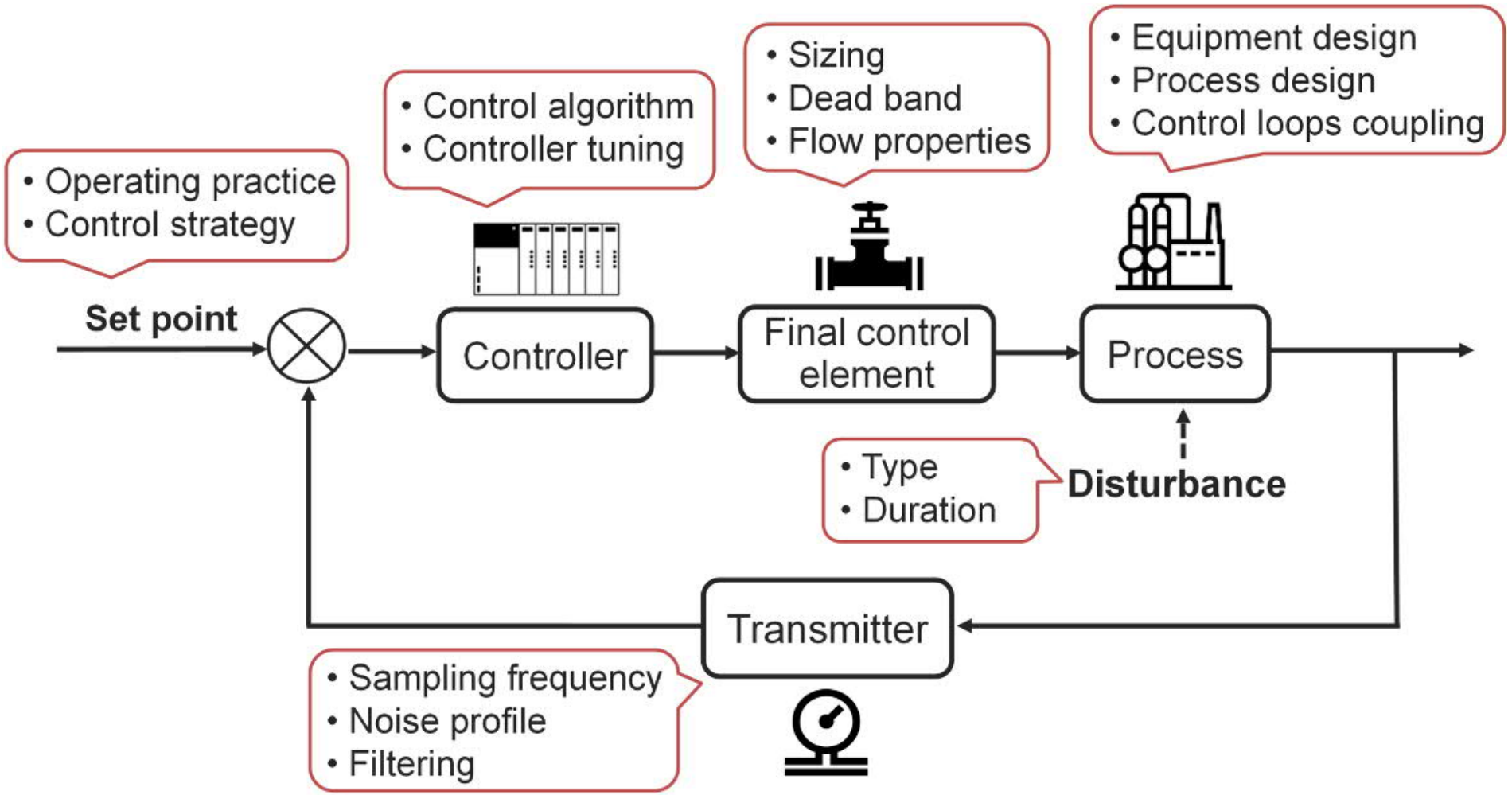
Process interdependencies



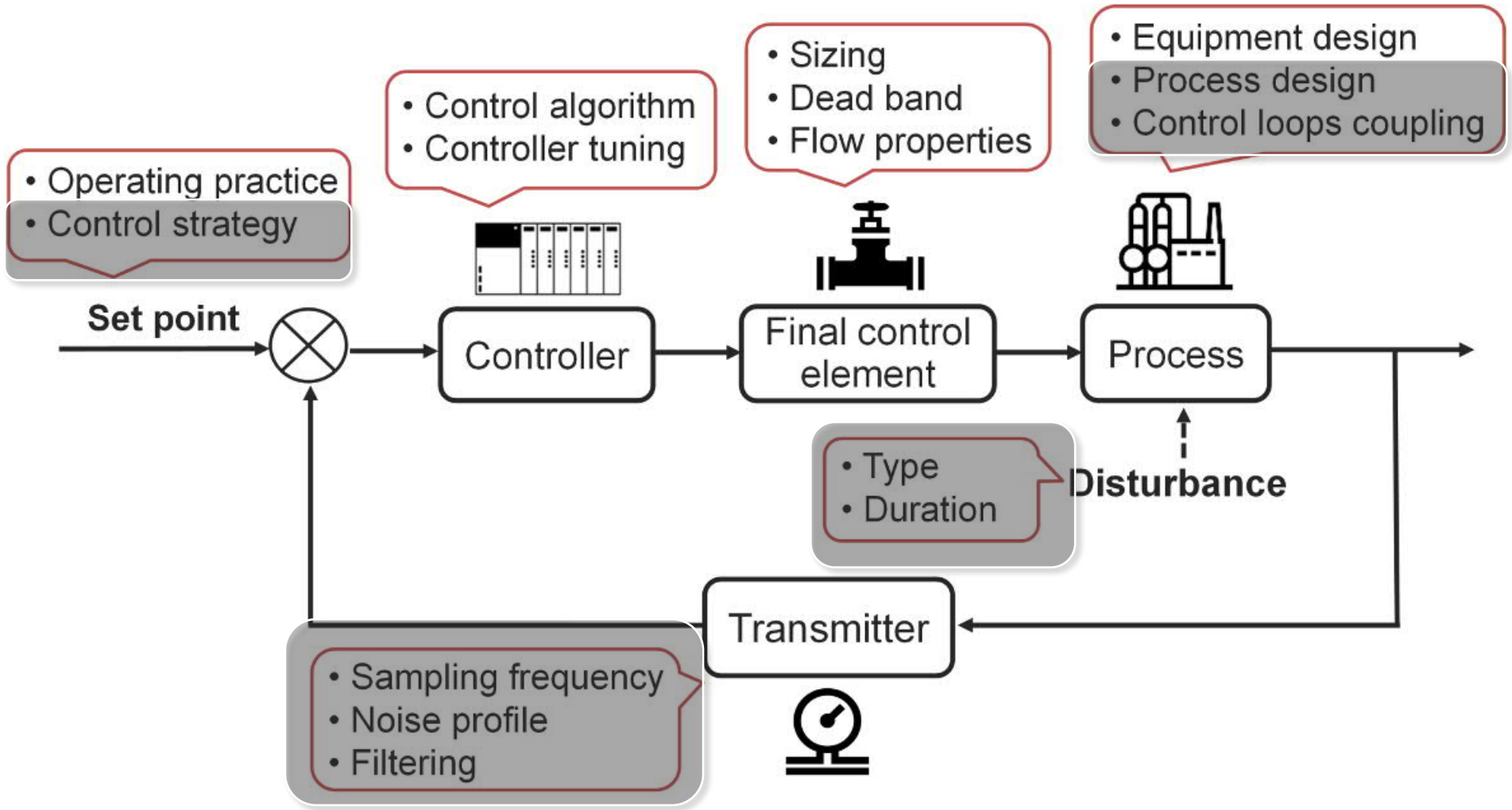
Process interdependencies



Understanding process responce

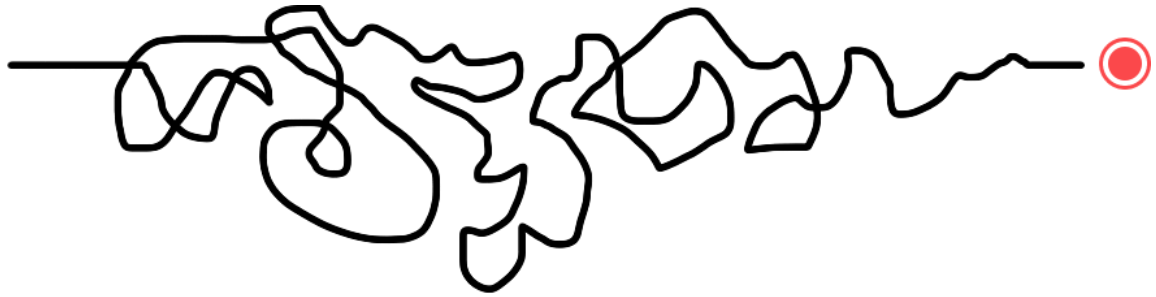


Understanding process responce



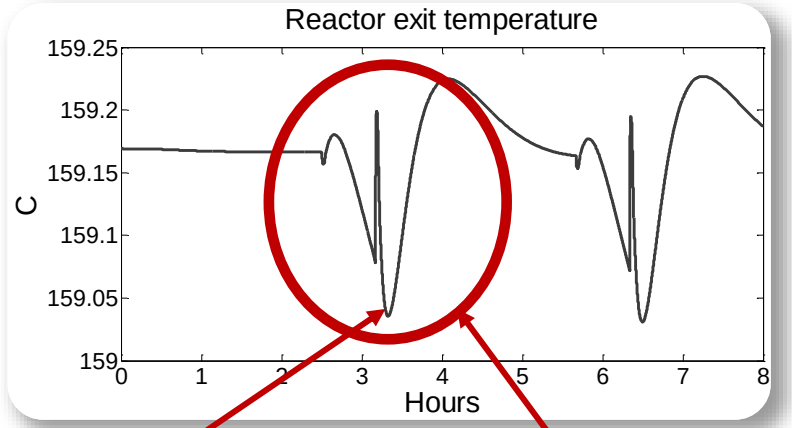
Process control challenges

- Process dynamic is highly non-linear (???)



- Behavior of the process is known to the extent of its modelling
  - So to controllers. They cannot control the process beyond their control model

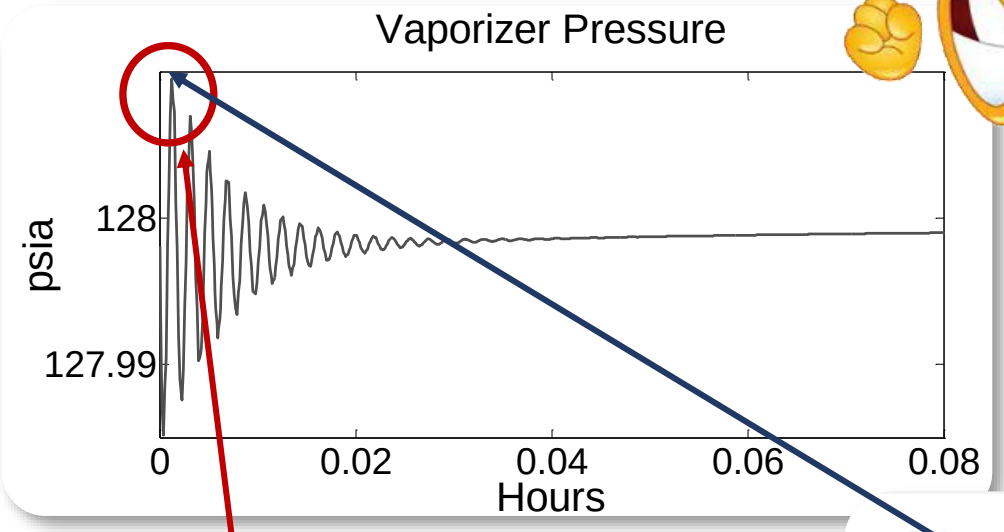
UNCERTAINTY!



This triggers alarms

Non-liner response

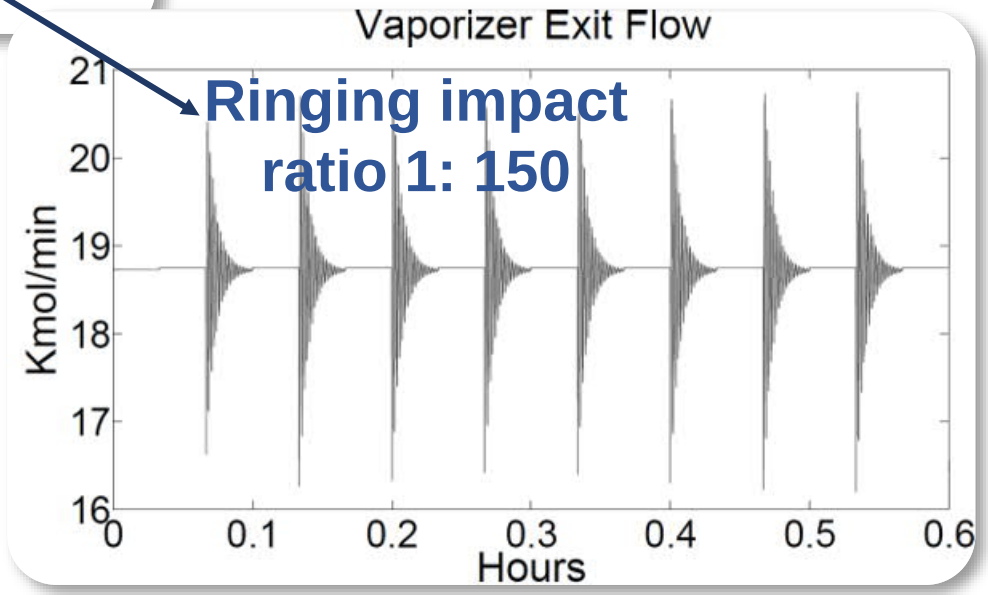
Control loop ringing



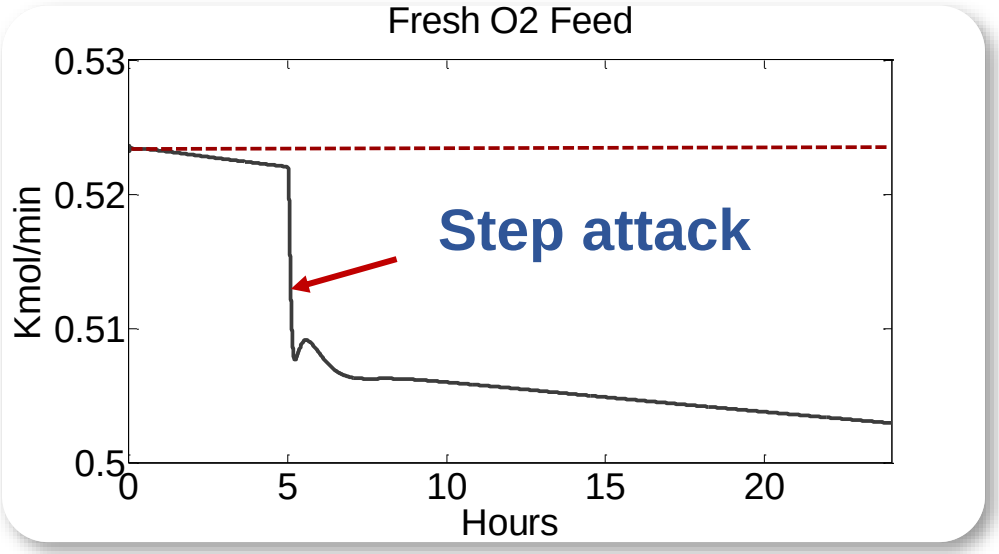
Caused by a negative real controller poles

Makes process unstable & uncontrollable

Amount of chemical entering the reactor



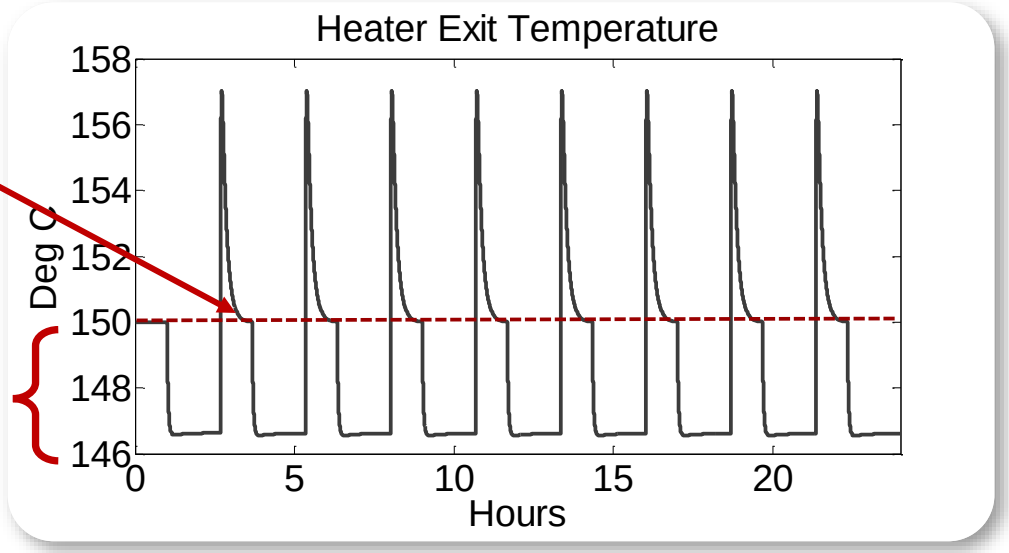
Type of attacks



Periodic attack

Recovery time

Magnitude of manipulation



Outcome of the control stage

I am 163 cm tall

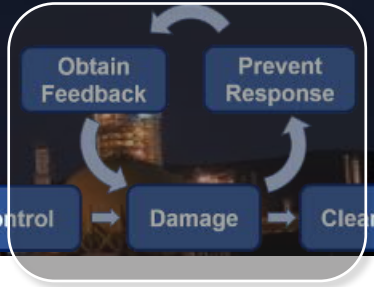
Control stage execution needs assistance with specialized tools (none available so far!)

Outcome of the control stage

Sensitivity	Magnitude of manipulation	Recovery time
High	XMV {1;5;7}	XMV {4;7}
Medium	XMV {2;4;6}	XMV {5}
Low	XMV{3}	XMV {1;2;3;6}

Reliably useful controls

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

How do we achieve needed physical impact?

Attacker needs one or more attack scenarios to deploy in final payload

- The least familiar stage to IT hackers
  - In most cases requires input of subject matter experts
- Accident data is a good starting point
  - Governmental agencies
  - Plants' own accident data bases

CSB

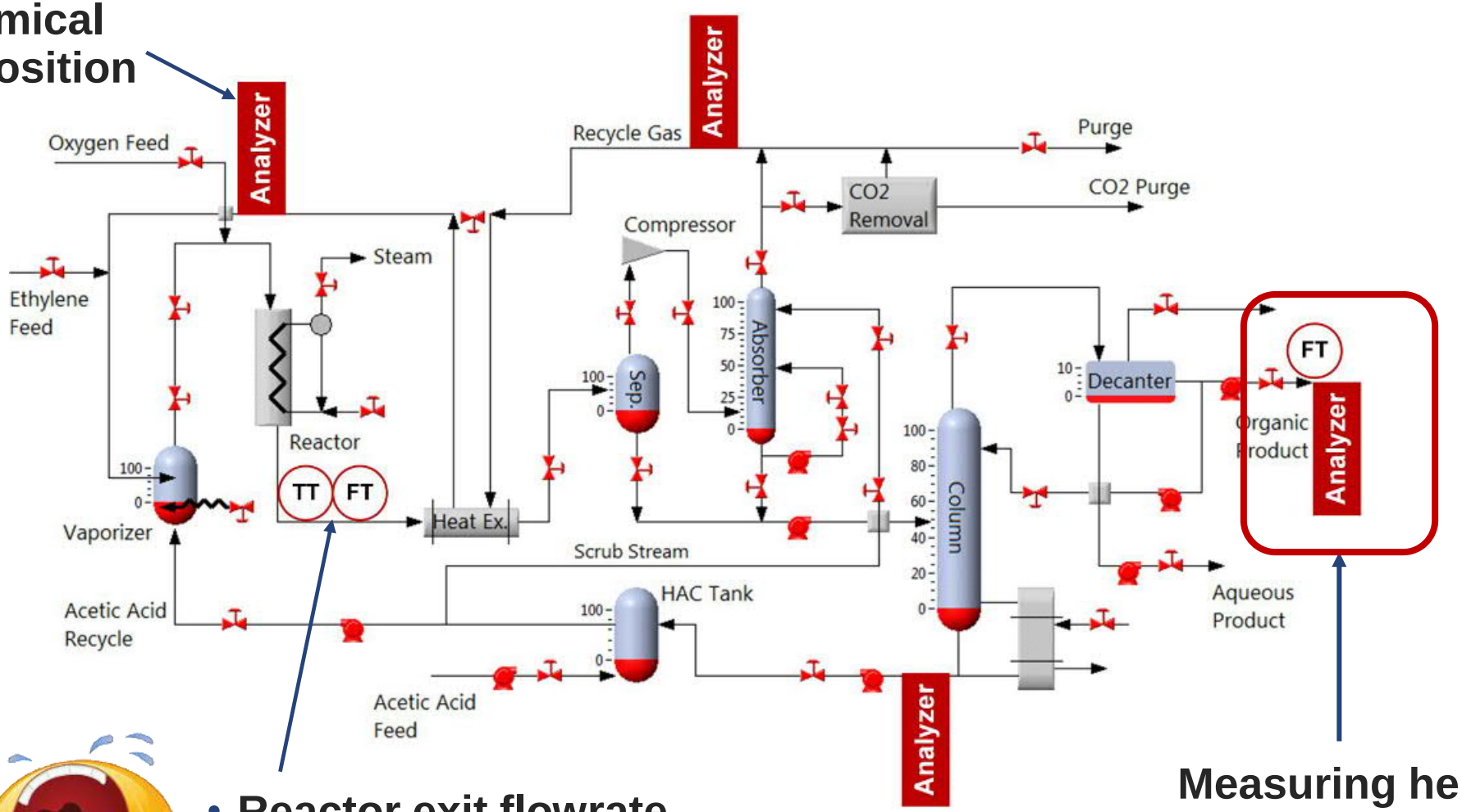
OSHA

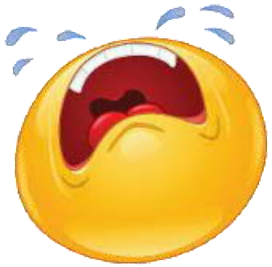
Hacker unfriendly process

- **Attacker need to obtain feedback in order to observe progress of the attack**
- Target plant may not have been designed in a hacker friendly way
  - There may no sensors measuring exact values needed for the attack execution
  - The information about the process may be spread across several subsystems forcing attacker to compromise greater number of devices
  - Control loops may be designed to control different parameters that the attacker needs to control for her goal

Obtain feedback: Measuring process

Chemical composition





- Reactor exit flowrate
- Reactor exit temperature
- No analyzer

Measuring here is too late

Measuring attack success

If you can't measure it, you can't manage it

Peter Drucker

Measurement precision

Technician

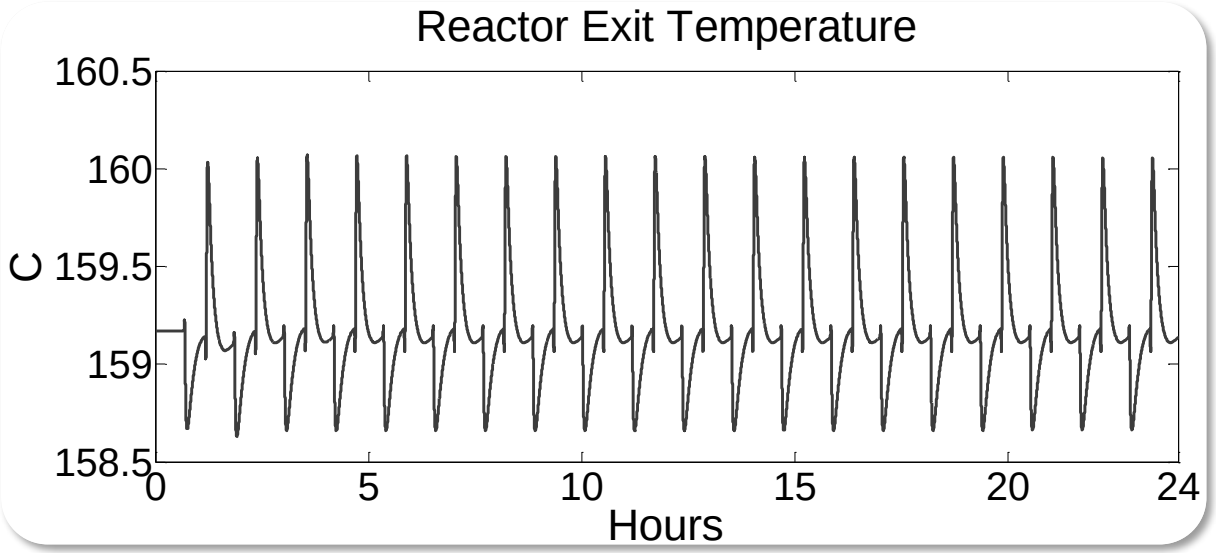
“It will eventually drain with the lowest holes loosing pressure last”

Engineer

“It will be fully drained in 20.4 seconds & the pressure curve looks like this”

“Technician” answer

Usage of proxy sensor



Reactor with cooling tubes

- Only tells us whether reaction rate increases or decreases
- Is not precise enough to compare effectiveness of different attacks

Quest for engineering answer

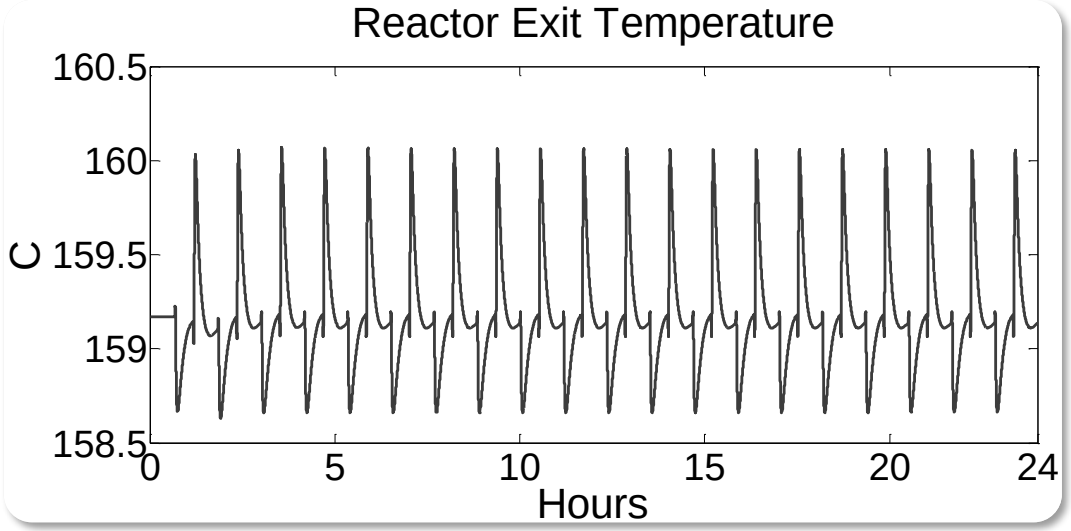
- Code in the controller
- Optimization applications
- Test process/plant

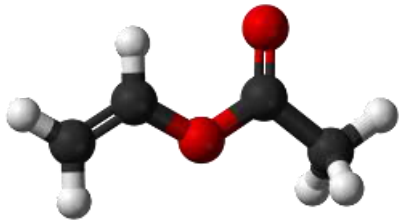
$$(\varepsilon\sum_{k=1}^{7} C_{i,k}Cp_{i,k} + \rho_b Cp_b)\frac{\partial T_i}{\partial t} = -\frac{\partial(v_i\sum_{k=1}^{7}(C_{i,k}Cp_{i,k})T_i)}{\partial z} - \phi_i\rho_b(r_{1,i}E_1 + r_{2,i}E_2) - Q_i^{RCT}$$

```
/*calculate derivatives*/
for (n=1;n<NR;n++)
{
    /*dC/dt=-delta(C*v)/deltaZ+sum(vij*rj)                    */
    /*Use single backward                                     */
    C_O2_t[n-1]=(-(C_O2[n]*v[n]-C_O2[n-1]*v[n-1])/dz + Coefficientl[0]*r_all[n][0]+Coefficient2[0]*r_all[n][1])/cata_porosity;
    C_CO2_t[n-1]=(-(C_CO2[n]*v[n]-C_CO2[n-1]*v[n-1])/dz + Coefficientl[1]*r_all[n][0]+Coeff                 ll[n][1])/cata_porosity;
    C_C2H4_t[n-1]=(-(C_C2H4[n]*v[n]-C_C2H4[n-1]*v[n-1])/dz + Coefficientl[2]*r_all[n][0]                    ll[n][1])/cata_porosity;
    C_VAc_t[n-1]=(-(C_VAc[n]*v[n]-C_VAc[n-1]*v[n-1])/dz + Coefficientl[4]*r_all[n][0]+                      [1])/cata_porosity;
    C_H2O_t[n-1]=(-(C_H2O[n]*v[n]-C_H2O[n-1]*v[n-1])/dz + Coefficientl[5]*r_all[n][0]                       1])/cata_porosity;
    C_HAc_t[n-1]=(-(C_HAc[n]*v[n]-C_HAc[n-1]*v[n-1])/dz + Coefficientl[6]*r_all[n][0]                       ])/cata_porosity;
    Q_rct[n]= UA*(Tg[n]-Shell_T); /*kcal/min m^3*/
    Tg_t[n-1]=1/(cata_porosity*CCP[n] + cata_heatcapacity *cata_bulk_density)*(-FCP[n                       ll[n][0]*E_r1-r_all[
    n][1]*E_r2-Q_rct[n]);
};
```

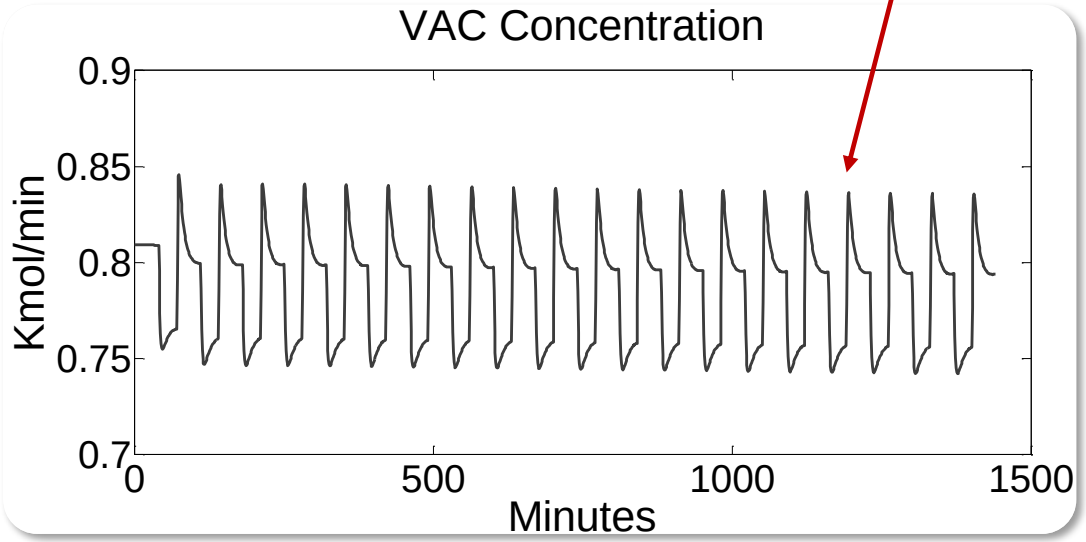
I found needed code but the numbers were very strange and did not seem being useful : 0,00073; 0,00016; 0,0007…

Bingo! Engineering answer obtained





Vinyl acetate production

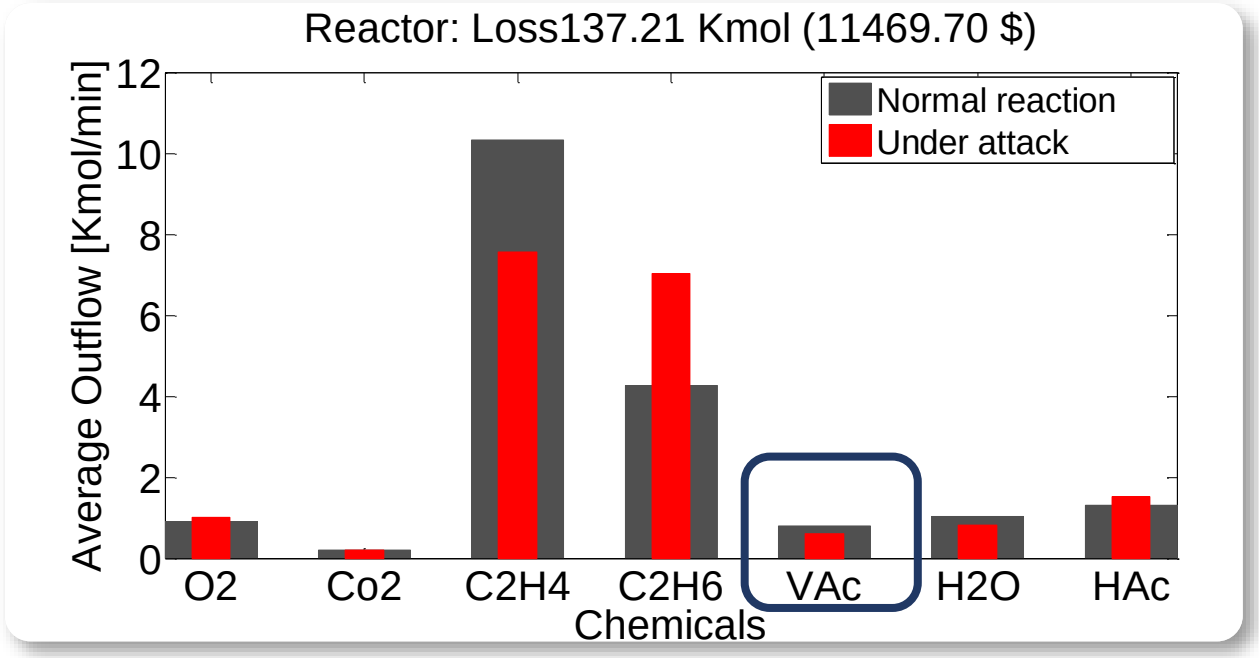


After two weeks of research and calculations, I finally got the numbers (YES!!)

Product loss

Product per day: 96.000$

Product loss per day: 11.469,70$



Prevent responce: Alarm propagation

Alarm	Steady state attacks	Periodic attacks
Gas loop 02	XMV {1}	XMV {1}
Reactor feed T	XMV {6}	XMV {6}
Rector T	XMV{7}	XMV{7}
FEHE effluent	XMV{7}	XMV{7}
Gas loop P	XMV{2;3;6}	XMV{2;3;6}
HAc in decanter	XMV{2;3;7}	XMV{3}

The attacker needs to figure out the marginal attack parameters which (do not) trigger alarms – to prevent response

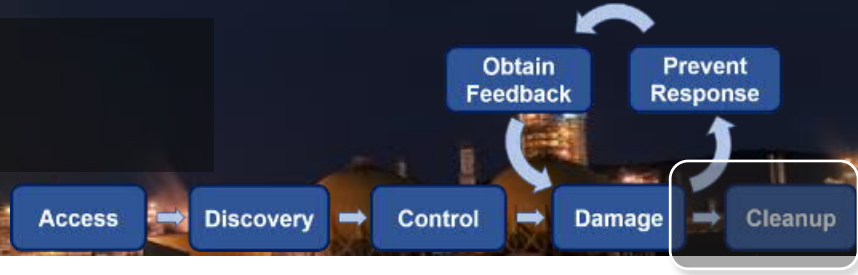
Outcome of the damage stage

Product per day: 96.000$

Product loss, 24 hours	Steady-state attacks	Periodic attacks
High, ≥ 10.000$	XMV {2}	XMV {4;6}
Medium, 5.000$ - 10.000$	XMV {6;7}	XMV {5;7}
Low, 2.000$ - 5.000$	-	XMV {2}
Negligible, ≤ 2.000$	XMV {1;3}	XMV {1;2}

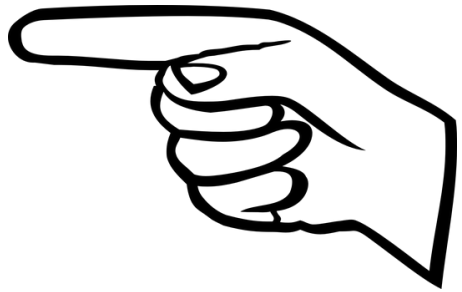
Still might be useful

Cleanup



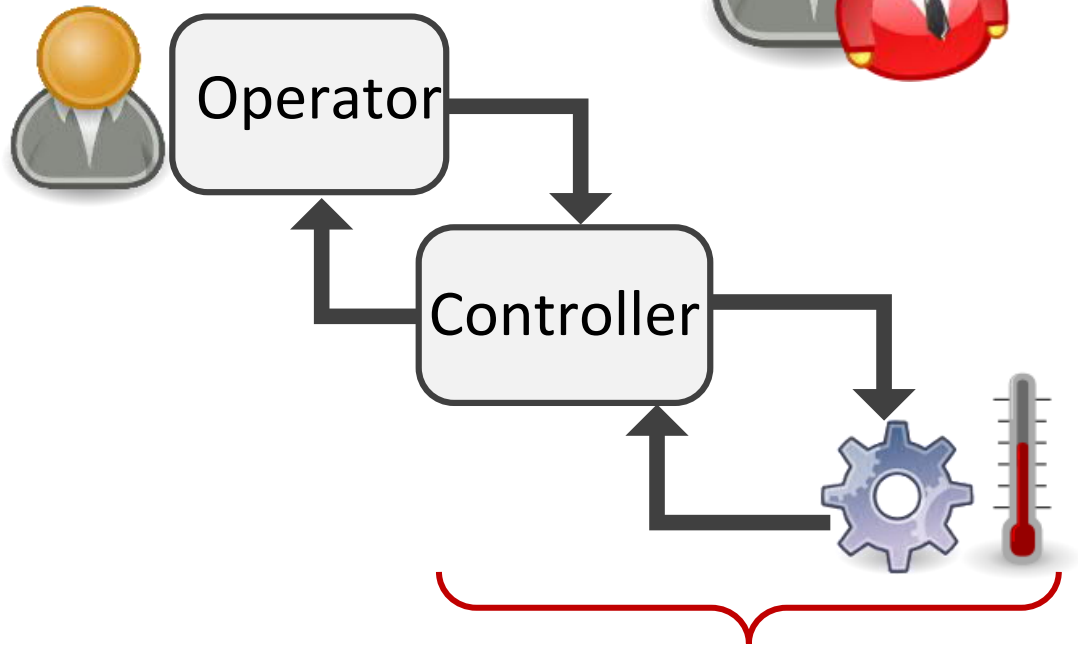
- In traditional (IT systems) hacking the goal is to stay undetected. In cyber-physical exploitation it is not an option because of physical effect:
  - Changes things in physical world which cannot hidden by e.g. “erasing logs”
  - Visible to observers

- **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



Socio-technical system

- Maintenance stuff
- Plant engineers
- Process engineers
- ….



Cyber-physical system

Creating forensic footprint

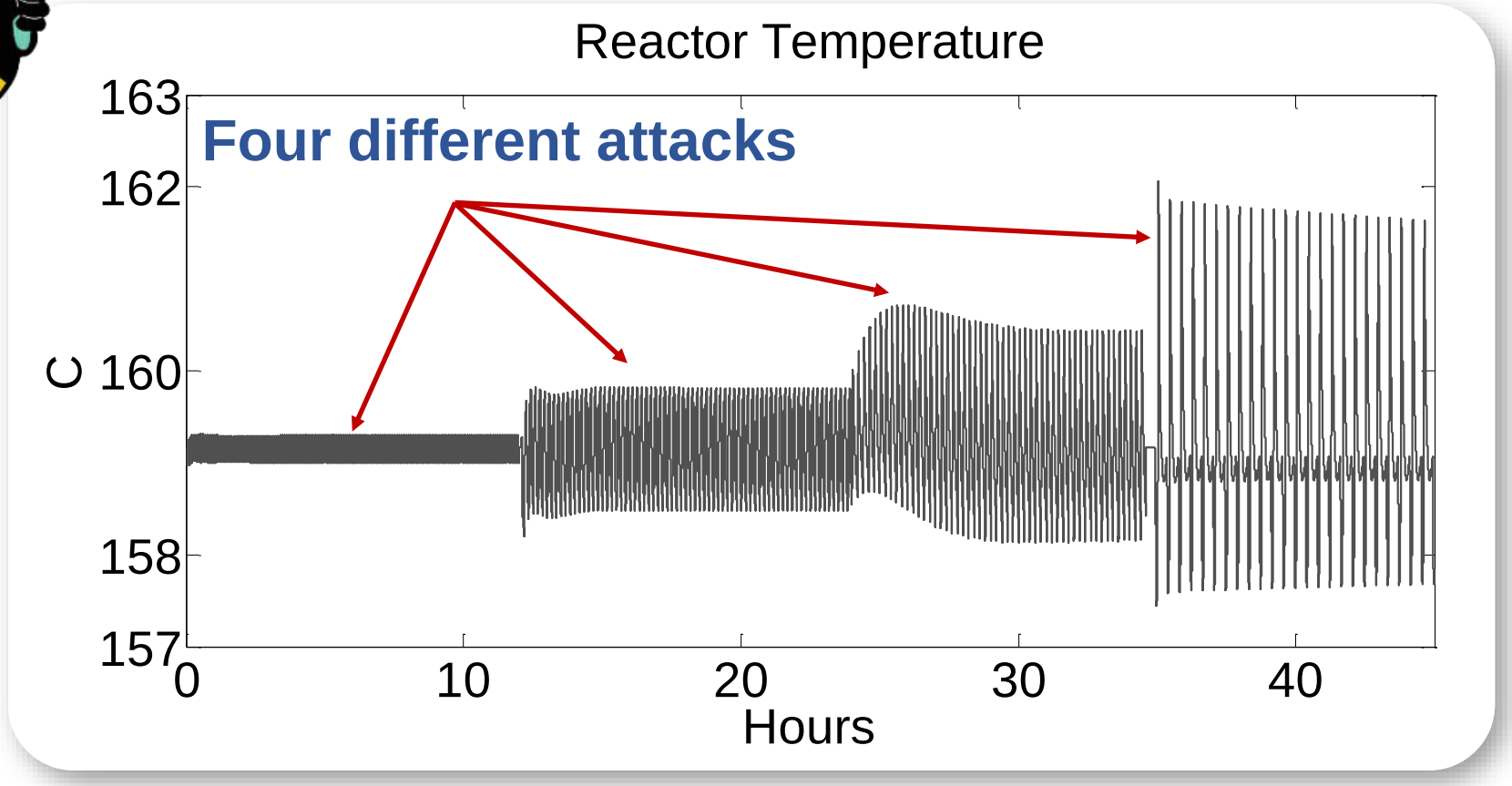
- Process operators may get concerned after noticing persistent decrease in production and may try to fix the problem
  - What do you want operators to think is causing process upset?
- If attacks are timed to a particular employee shift or maintenance work, plant employee will be investigated rather than the process

Creating forensic footprint

1. Pick several ways that the temperature can be increased
2. Wait for the scheduled instruments calibration
3. Perform the first attack
4. Wait for the maintenance guy being yelled at and recalibration to be repeated
5. Play next attack
6. Go to **4**

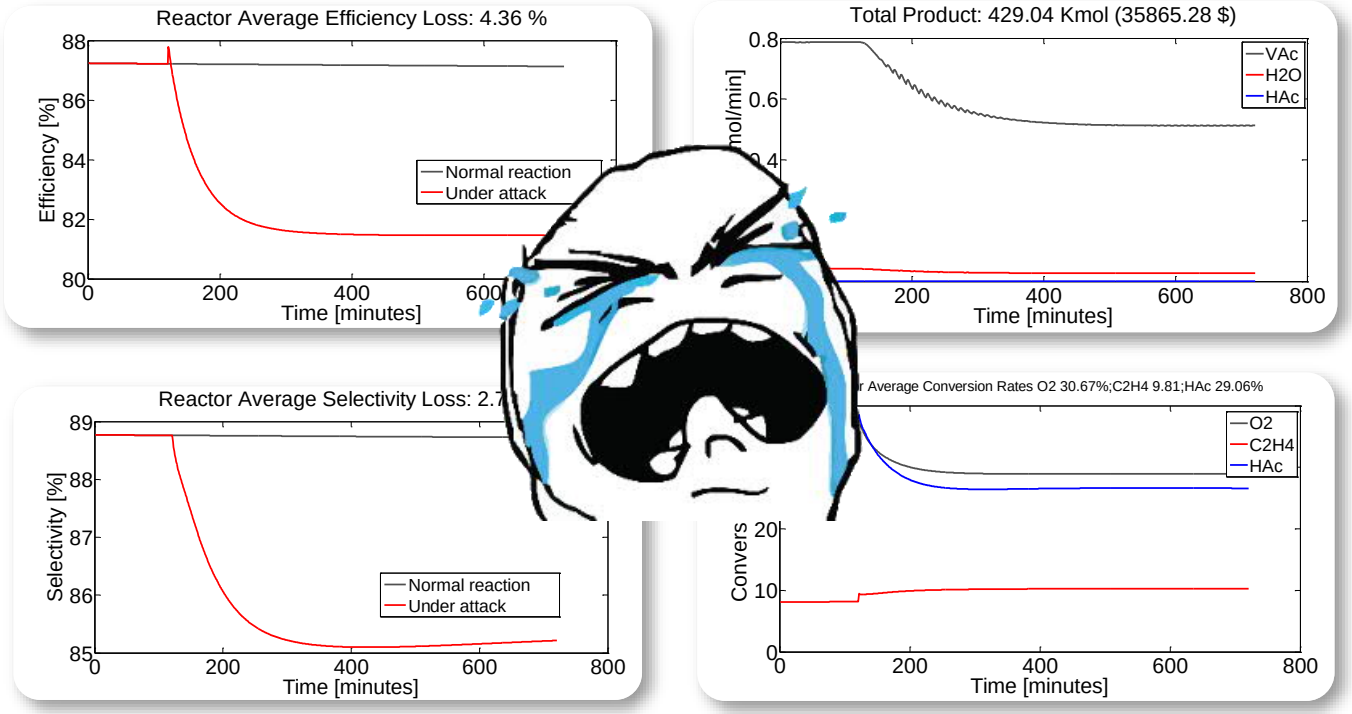
Creating forensic footprint

Creating forensics footprint



Defeating chemical forensics

- If reactor doubted, chemical forensics guys will be asked to assist
- Know metrics and methods of chemical investigators
- **Change attack patterns according to debugging efforts of plant personnel**



Conclusions

Security is not a fundamental science

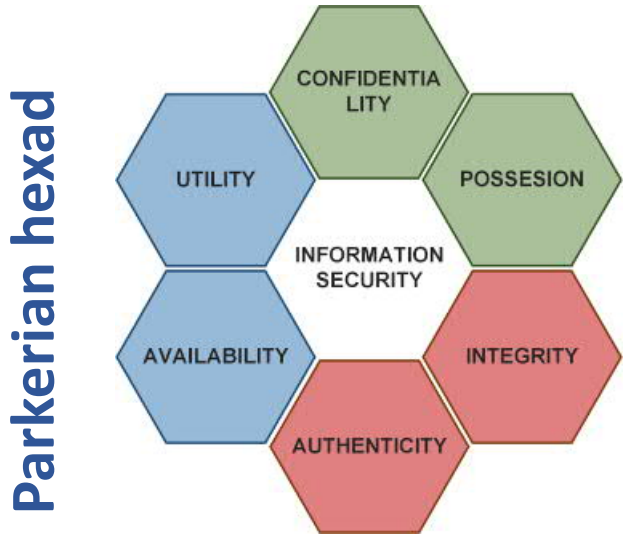
It is application driven

Security solutions exist in the context of the application

Early adopter: eCommerse

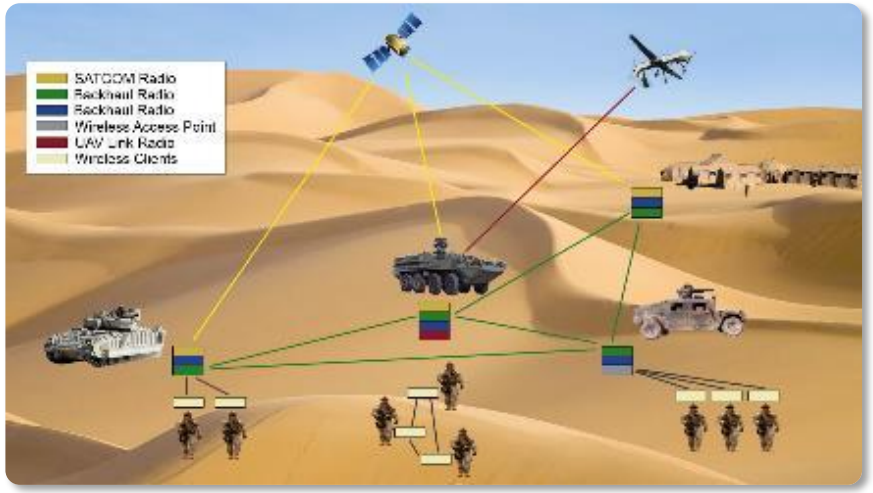
- **Security influences design decisions**
  - Attackers (mis)use functionality of web browsers
  - Novel approaches to designing web applications
  - Novel security controls in browsers

- **Application dictates security properties**
  - Information-theoretic security properties
  - CIA triad --> Parkerian hexad



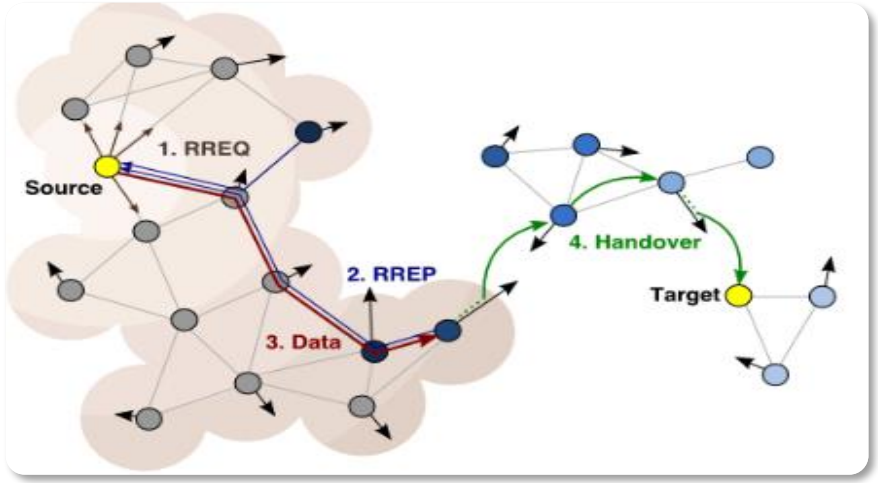
Failed to adopt

- **Wireless sensor networks: Big hope**
  - A big hype for about a decade
  - Conferences, solutions, promising applications
  - Remained a “promising” technology with limited deployment



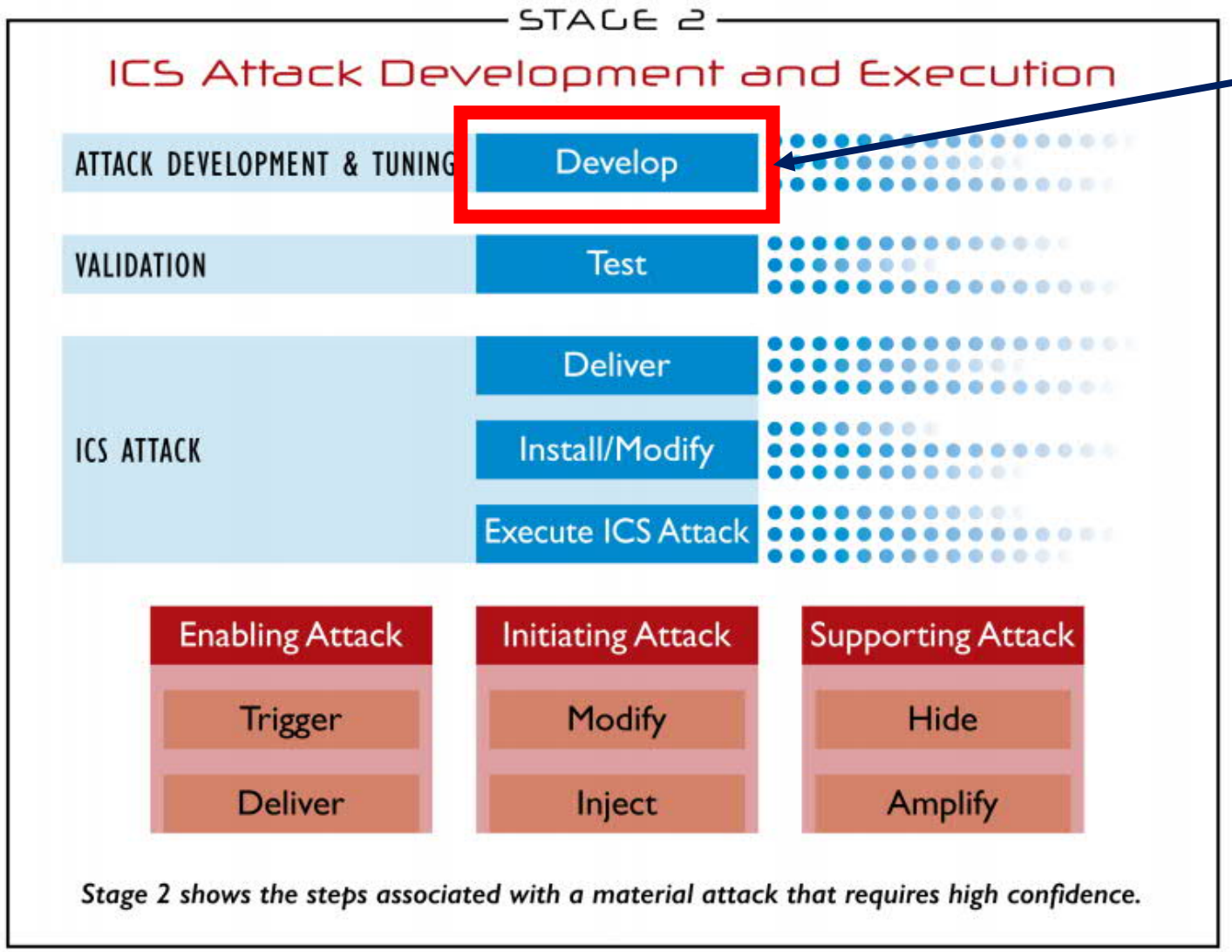
https://www.elprocus.com/wp-content/uploads/2014/12/Military-applications-based-on-wireless-sensor-networks.jpg

- **Wireless sensor networks: Big flop**
  - Deficiencies in the attacker models and security requirements
  - Unrealistic assumptions about physics of wireless communication



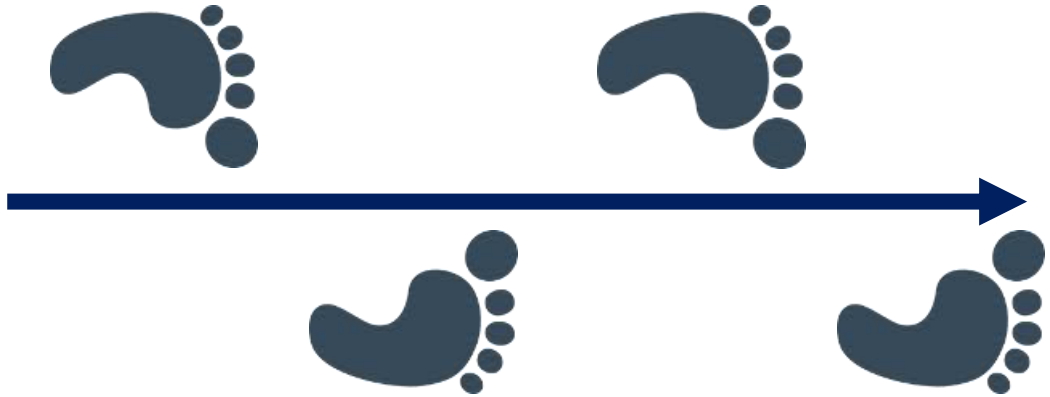
D. Gollmann, M. Krotofil, H. Sauff. Rescuing Wireless Sensor Networks Security from Science Fiction (WCNS’11)

SANS: ICS cyber-kill chain



WHAT HAPPENS HERE?

Designing cyber-physical payload

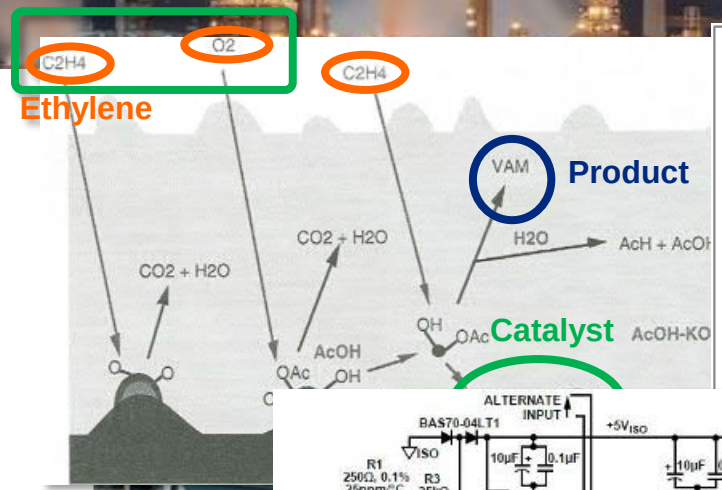


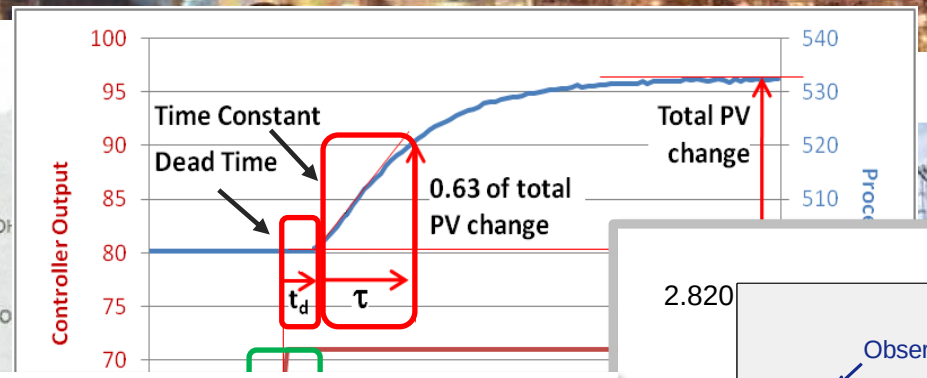
https://bloximages.newyork1.vip.townnews.com/hannapub.com/content/tncms/assets/v3/editorial/e/00/e00b6032-b883-11e9-863f-3f8704327902/5d49dabf0e770.image.jpg

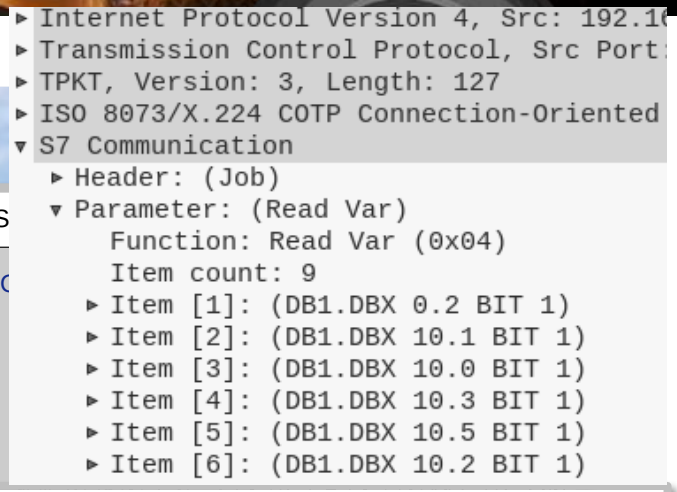
Evil Motivation

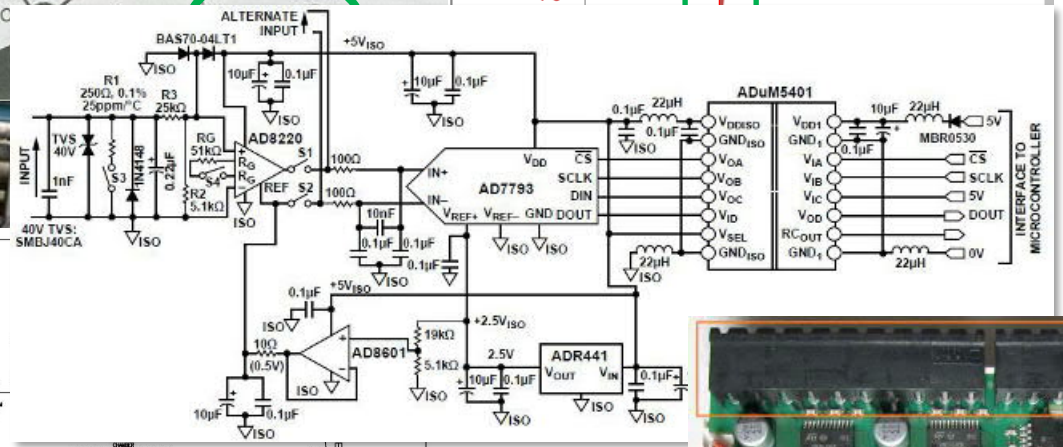
Cyber-physical Payload

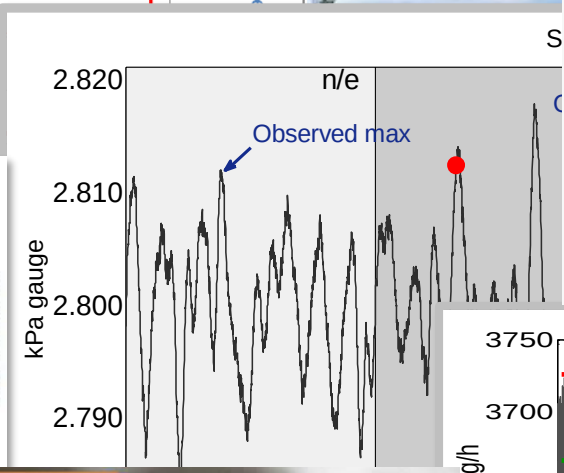
Knoweldge involved into exploit development

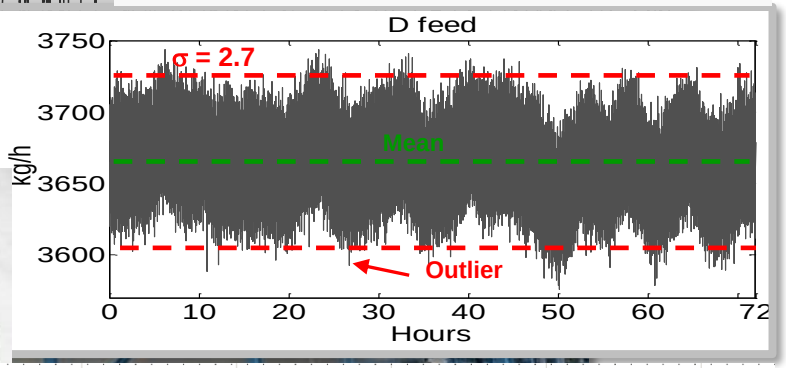


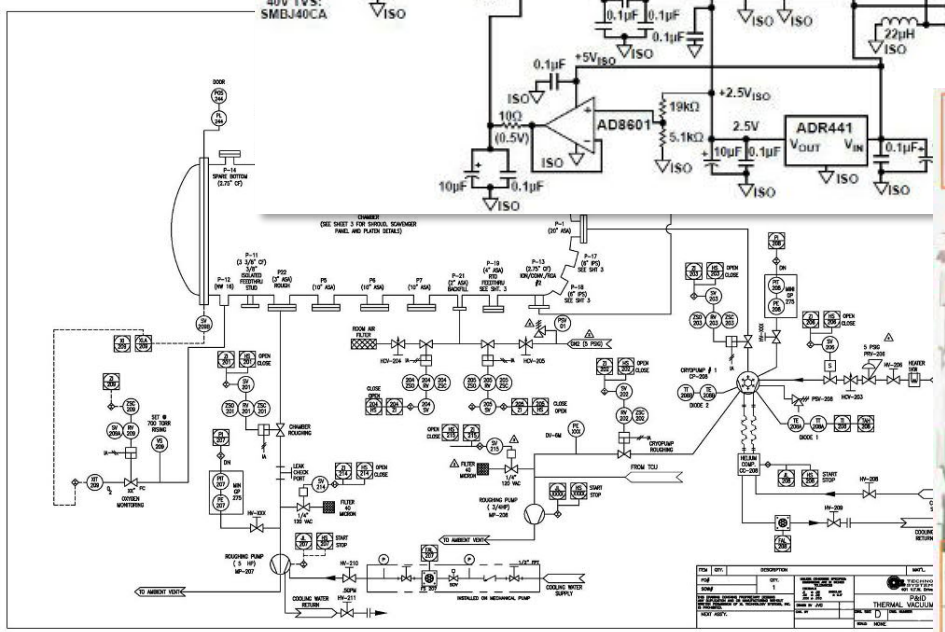


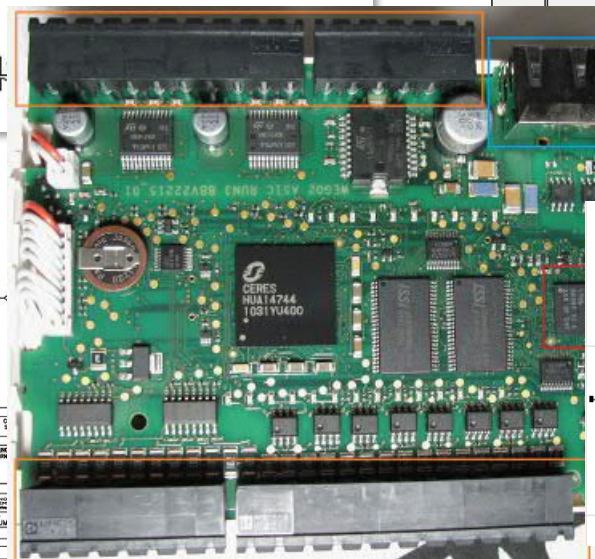


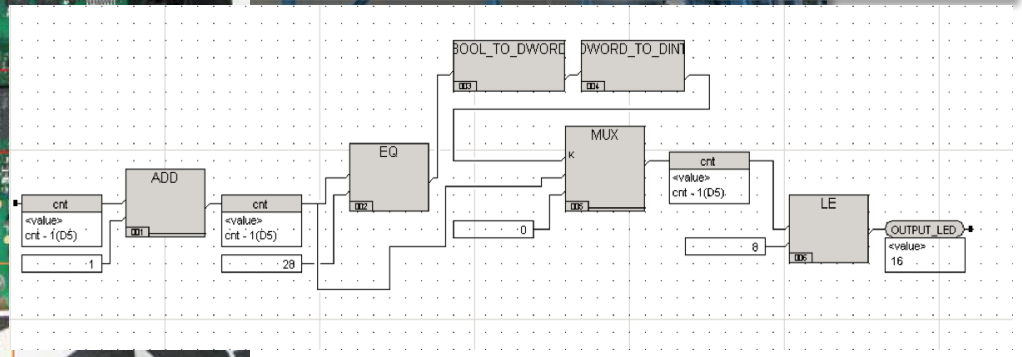




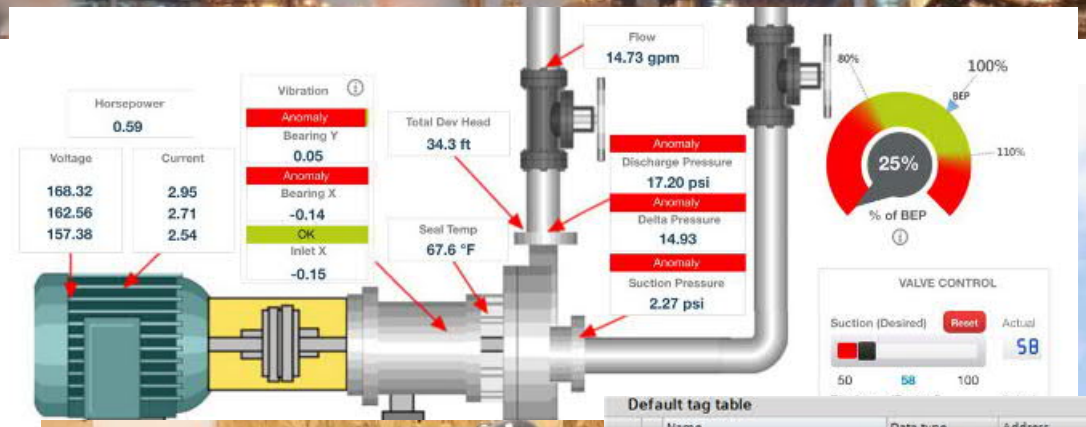








Knoweldge involved into exploit development



Algorithm 1 Runs Analysis

```
procedure EXPLORE                                   ▷ 1: analyse phase
    signal ← signal to analyse

    while not an end of signal do
        while moving up do
            runs++                                  ▷ count positives moves
            value = sum(changes)                    ▷ positive steps change
            if direction change then                ▷ save results
                positivesruns(runs)++
                positivesvalues(runs) = value
        while moving down do
            runs++                                  ▷ count negatives moves
            value = sum(changes)                    ▷ negative steps change
            if direction change then                ▷ save results
                negativesruns(runs)++
                negativesvalues(runs) = value
        if no change then
            nils++                                  ▷ count nils
                                                    es,nils
```

Default tag table

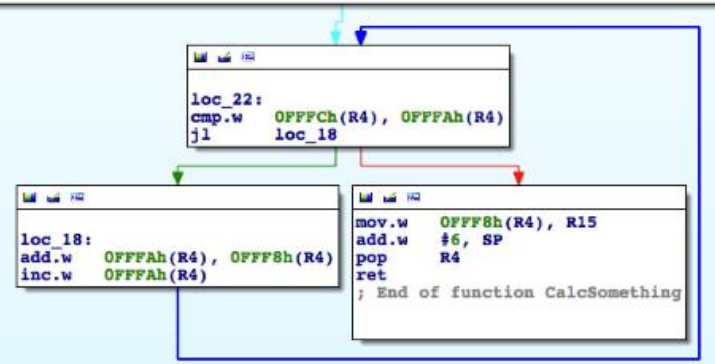
	Name	Data type	Address	Retain	Visible..	Acces...	Comment
1	Emerg-OFF	Bool	%I1.0		☑	☑	Emergency-OFF (nc contact)
2	S3	Bool	%M0.3		☑	☑	pushbutton START S3 (no contact)
3	B1	Bool	%I0.1		☑	☑	sensor safety fence closed (no contact)
4	B2	Bool	%I0.2		☑	☑	sensor cylinder A moved out (no contact)
5	M0	Bool	%Q0.0		☑	☑	move out cylinder A
6	S1	Bool	%M0.1		☑	☑	pushbutton manual mode S1 (no contact)
7	S2	Bool	%M0.2		☑	☑	pushbutton automatic mode S2 (no conta...
8	S4	Bool	%M0.5		☑	☑	pushbutton ON S4 (no contact)
9	S5	Bool	%I0.5		☑	☑	pushbutton OFF S5 (no contact)
10	Motor1	Bool	%Q0.2		☑	☑	motor conveyor belt M01
11	B0	Bool	%I0.3		☑	☑	sensor bottle counting
12	S6	Bool	%I0.6		☑	☑	reset counter / new box

Algorithm 2 Triangles

```
procedure EXPLORE
    signal ← signal to analyse
    window ← learning window
    noiselvl ← noise parameter

    step = window * 10
    topslope = −999.99
    bottomslope = 999.99
    while not an end of signal do
        if first elements then
            current = value
            index = 1
        while index < window do                     ▷ learning phase of i − th bucket
            upperslope = (current − (last + noiselvl))/index
            lowerslope = (current − (last − noiselvl))/index
            if upperslope > topslope then
                topslope = upperslope
            if lowerslope < bottomslope then
```

```
.def CalcSomething
CalcSomething:
push.w  R4
mov.w   SP, R4
incd.w  R4
add.w   #0FFFAh, SP
mov.w   R15, 0FFFCh(R4)
clr.w   0FFF8h(R4)
clr.w   0FFFAh(R4)
jmp     loc_22
```



Process-aware proactive & reactive security

- Many exploitation scenarios require (prolonged) access to the target environment
- Know data sources vital to communication infrastructure recon and process comprehension
  - Be careful with public announcements and data exposure via trusted 3rd parties
  - Lock down or monitor access to critical data sources (in all!! their locations)
  - Monitor process behavior for anomalies

Inability to collect required information & interact with the process significantly limits attack scenarios achievable by threat actors

Q & A

Marina Krotofil
@marmusha
marmusha@gmail.com