



Cyber-Physical Attack Lifecycle: Hacking chemical plant

Marina Krotofil

COINS summer school on Security Applications, Lesbos, Greece

26-27.07.2019

Note



This session is based on the talk:

M. Krotofil “Rocking the Pocket Book: Hacking Chemical Plants for Competition and Extortion”, Black Hat, Las Vegas, USA, 2015.



Why to attack ICS

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



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

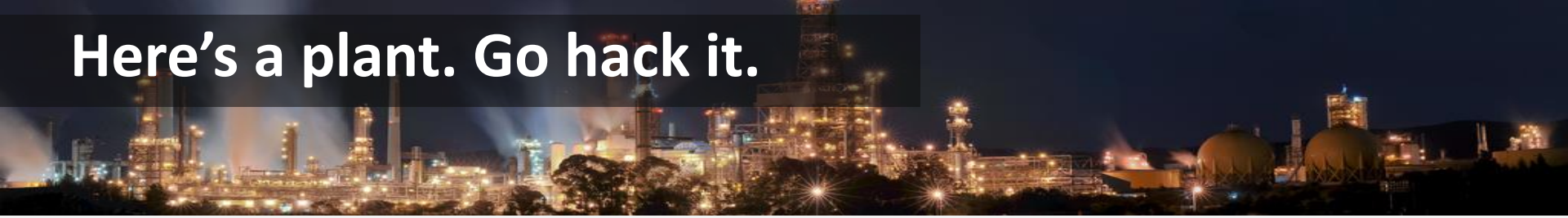
Alan Paller of SANS (2008):

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.

Here's a plant. Go hack it.



Attack scenario: persistent economic damage

What can be done to the process

Equipment damage

- Equipment overstress
- Violation of safety limits

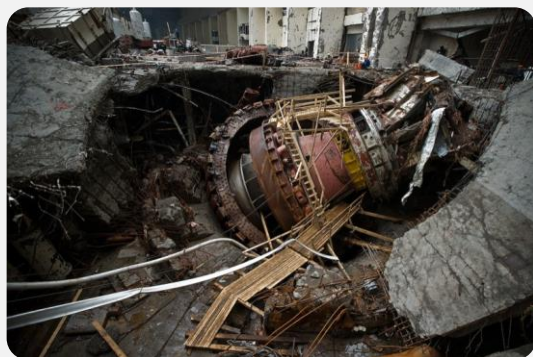
Production damage

- Product quality and product rate
- Operating costs
- Maintenance efforts

Compliance violation

- 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 ($\bar{\mp}$)
- Unclear collateral damage (-)
- May transform into compliance violation, e.g. if it kills human (-)

Equipment damage

Production damage

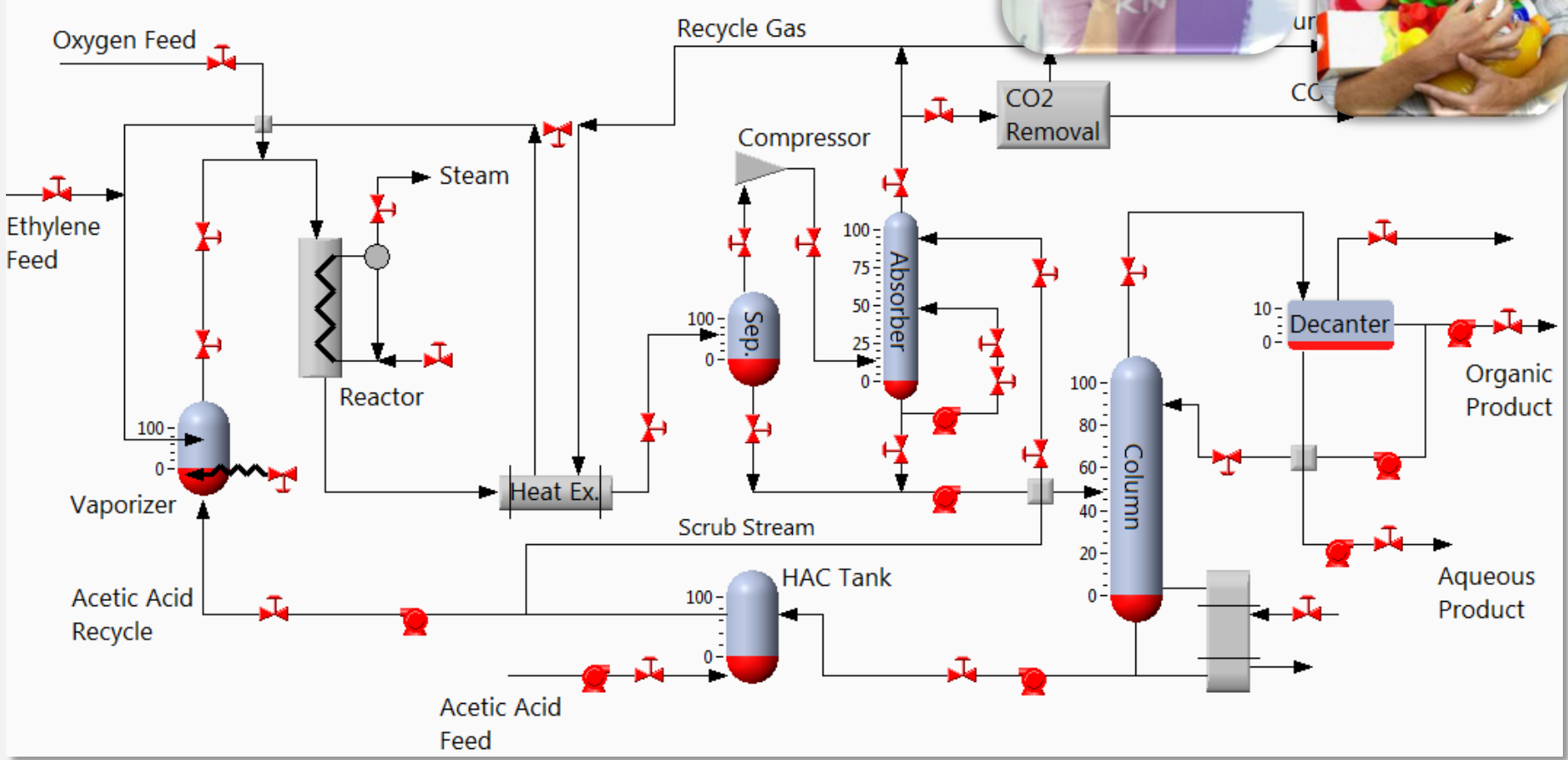
Compliance violation

Do this

❑ Compliance violation

- Compliance regulations are public knowledge (+)
- Unclear collateral damage (-)
- Must be reported to the authorities ($\bar{\mp}$)
- 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 more



More plants offers:

<http://www.usedplants.com/>

Car vs. plant hacking

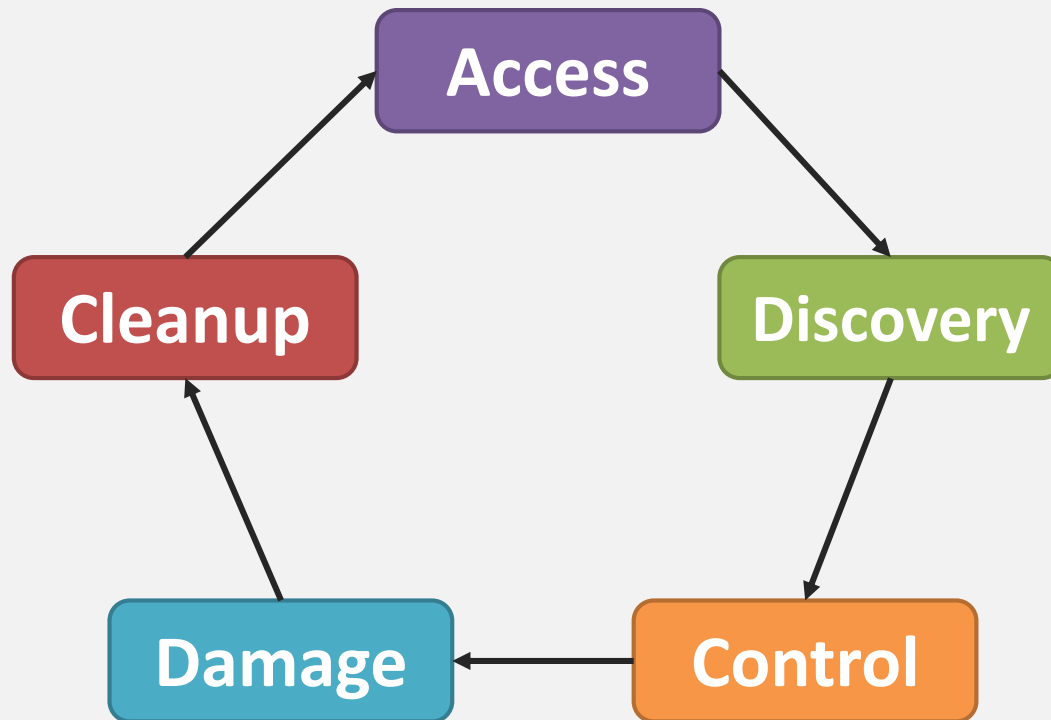


It is not about the size

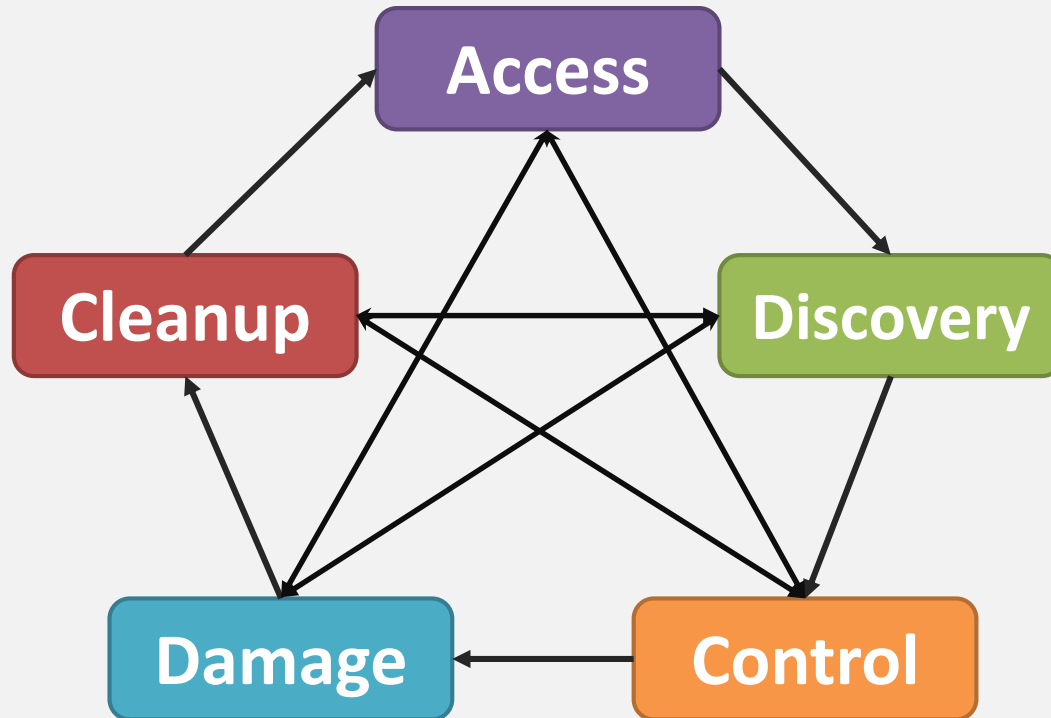


It is about MONEY
Plants are ouch! how expensive -> hence,
researching on model

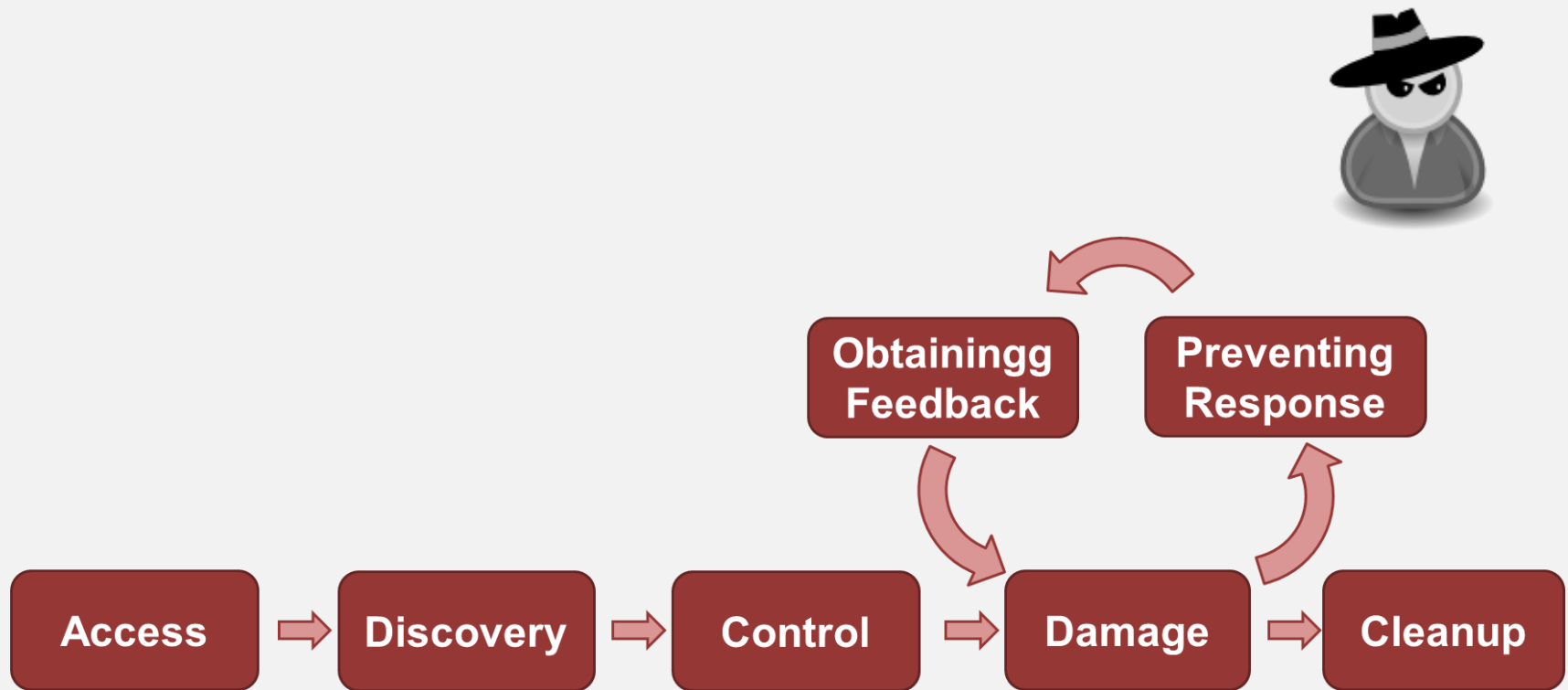
Cyber-physical attack lifecycle, version 2015



Stages of SCADA attack



Cyber-physical attack lifecycle, version 2019





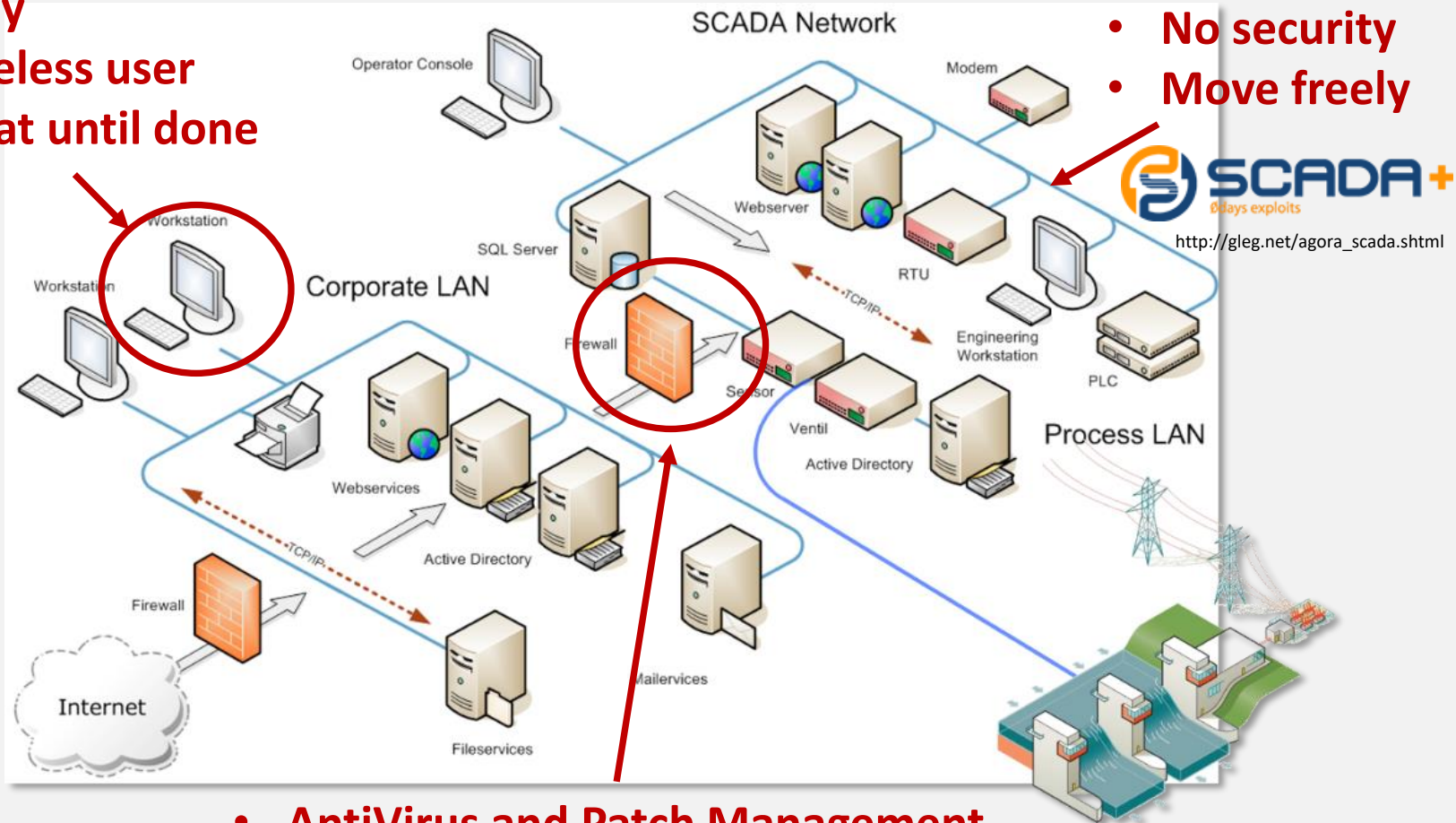
Access

**RESTRICTED
— AREA —**

**NO ENTRY
UNLESS AUTHORIZED**

Traditional IT hacking

- 1 Oday
- 1 Clueless user
- Repeat until done



- No security
- Move freely

SCADA+
Bdays exploits
http://gleg.net/agora_scada.shtml

- AntiVirus and Patch Management
- Database links
- Backup systems

Plants modernization



❑ 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”)



**Old generation
temperature sensor**



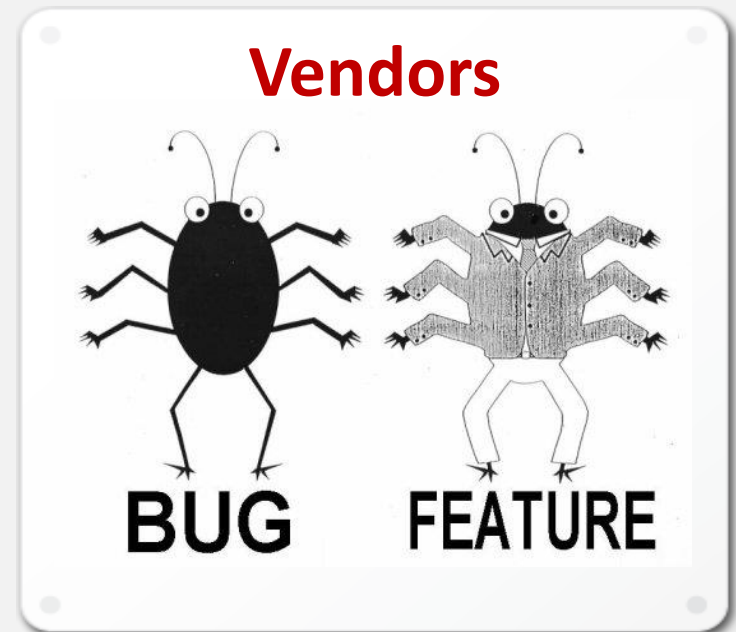
Sensor

**Computational
element**

Instrumentation of the future

Promise from the vendors:

Expect instruments of the future to have multiple communication channels, each one with built-in security (LOL), much like a present-day Ethernet switch. These channels will be managed with IP addressing and server technology, allowing the instrument to become a true data server

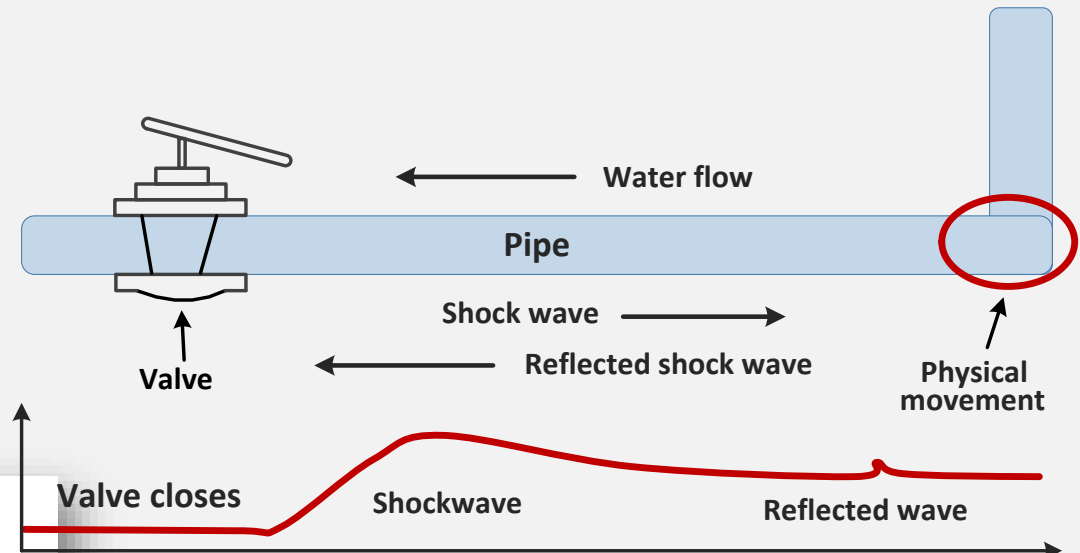
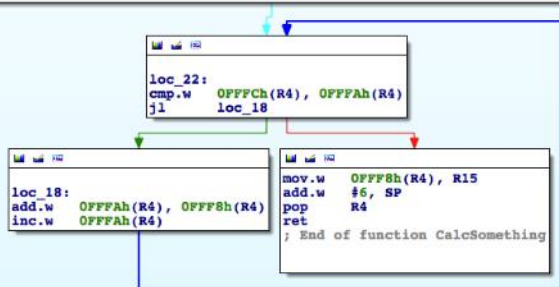


Invading field devices

❑ Inserting rootkit into sensor's firmware



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



Attack scenario: pipe damage with water hammer effect



Discovery



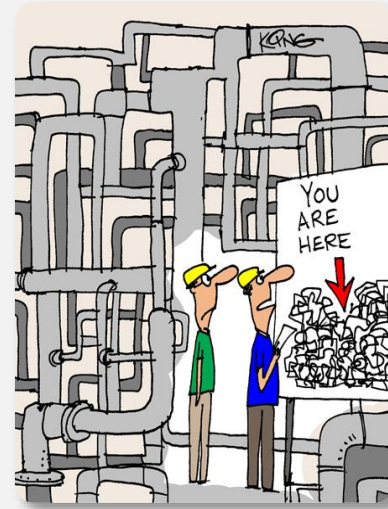
Process discovery



What and how the process is producing



How it is controlled



How it is build and wired



Operating and safety constraints

Espionage, reconnaissance
Target plant and third parties

Espionage

- Industrial espionage has started LONG time ago (malware samples dated as early as 2003)

Cyber Espionage comes to SCADA Security

Nitro Malware Targeted Chemical Companies
ment, and manufacture of chemicals and advanced materials. The goal of the attackers appears to be to collect intellectual property such as design documents, formulas, and manufacturing processes.

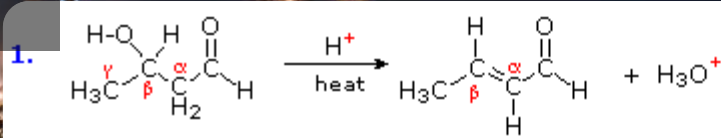
Massive 'Dragonfly' Malware Campaign Across Middle East
BY CHLOE ALBANESIJUS
Symantec
Dragonfly: West
Cyberespionage campaign stole ...
MAY 28, 2012 01:34PM EST

DragonFly/Havex/Enclave ACAD/Medre. A 10000's of AutoCAD files leaked in suspected industrial espionage
BY RICHARD ZWIENE
"VIRUSES REVEALED"
JUN 21 JUN 2012 - 04:58AM

DragonFly/Havex/Enclave Against Energy Suppliers

Nation state behind malware attacks on European ICS systems?
June 25, 2014

Process discovery



AVEVA Instrumentation Engineer

Instrument Datasheet: **PRESSURE TRANSMITTER**

1	Tag No.	01-PT-510								
2	Service	Reactor 01-R-510								
3	Fluid No.	01-220-014	01-F007-00-01							
4	Area Classification	Zone 1, GR, IC, T3								
5	Ingress Protection	IP 67								
PROCESS CONDITIONS										
Process Design Conditions										
7	Fluid	State	HC	Vapour	Process Design Conditions					
8	Pressure	Normal	Max	1200 kPa(g)	1430 kPa(g)	Design Pressure	(MeNu)	-	7	1500 kPa(g)
9	Temperature	Normal	Max	100 °C	148 °C	Design Temperature	(MeNu)	-	7	148 °C

AVEVA Instrumentation ループチェックレポート

ループ番号: 01-T-511 ループサービス: Reactor01-R-510

01-TT-511 01-JB-002 ER-01 MR-001

01-FT-900 01-F-900 Waterfron

01-FT-510 01-F-510 Reactor 0

01-FC-510 01-F-510 Reactor 0

01-FAL-510 01-F-510 Reactor 0

01-FV-510 01-F-510 Reactor 0

01-PT-510 01-P-510 Reactor 0

01-TT-511 01-T-511 Reactor 0

01-TAH-511 01-T-511 Reactor 0

01-XS-001 01-X-001 PUMP P-3

01-L-525 01-L-525 Low Pressure

01-LV-525 01-L-525 Low Pressure

01-L-525 01-L-525 Low Pressure

01-PT-500 01-P-500 Feed Surge D

01-FE-520 01-F-520 Cooling Water

01-FT-520 01-F-520 Cooling Water

08-FT-600 08-F-600 1st Stage Sep

08-FV-600 08-F-600 1st Stage Sep

01-FT-003 01-F-003

01-FALL-510

01-LG-526

01-PI-527

01-FT-500 01-F-500 Feed Surge D

01-FT-500 01-F-500 Feed Surge D

01-LV-525 01-L-525 Low Pressure

01-FT-510 01-F-510 Reactor 0

ZSRH-001

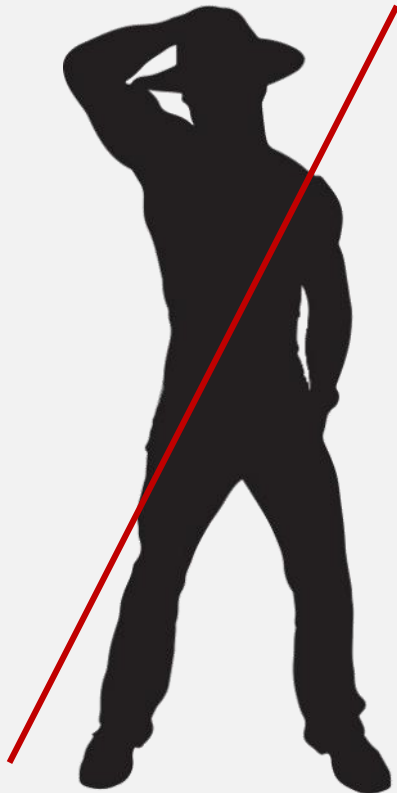
Grader
Man Basket
Other
Plow
Pressure Vessel
Pump
Quad
Rig Mats
Shacks
Threader
Tractor
Trailer

14	DS-01	DbShift 01	DSHIFT	20 Ton Picker	1D7HU18278S618229
15	E100	E100 336DL	Galaxy	Excavator	1GCHK29141E302402
16	E101	E101 325D	Galaxy	Excavator	5TFHY5F1XAX097175
17	E102	E102 325BL	Galaxy	Excavator	1D7RV1CT2AS149221
18	E103	E103 320CL	Galaxy	Excavator	3D7UT2HL5AG134976
19	E104	E104 320CL	Galaxy	Excavator	
20	Enclosed Trailer	Enclosed Trailer	RR SERVICES	Trailer	
21	FS 08	Flare Stack 08	Galaxy	Other	
22	FSH 1	Flameless Space Heater	RR SERVICES	Other	
23	G100	G100	Galaxy	Grader	
24	G101	G101	Galaxy	Grader	
25	G103	G103	Galaxy	Grader	
26	Gas Monitor	Gas Monitor	RR SERVICES	Other	
27	Generator	Generator	RR SERVICES	Generator	

Know the equipment



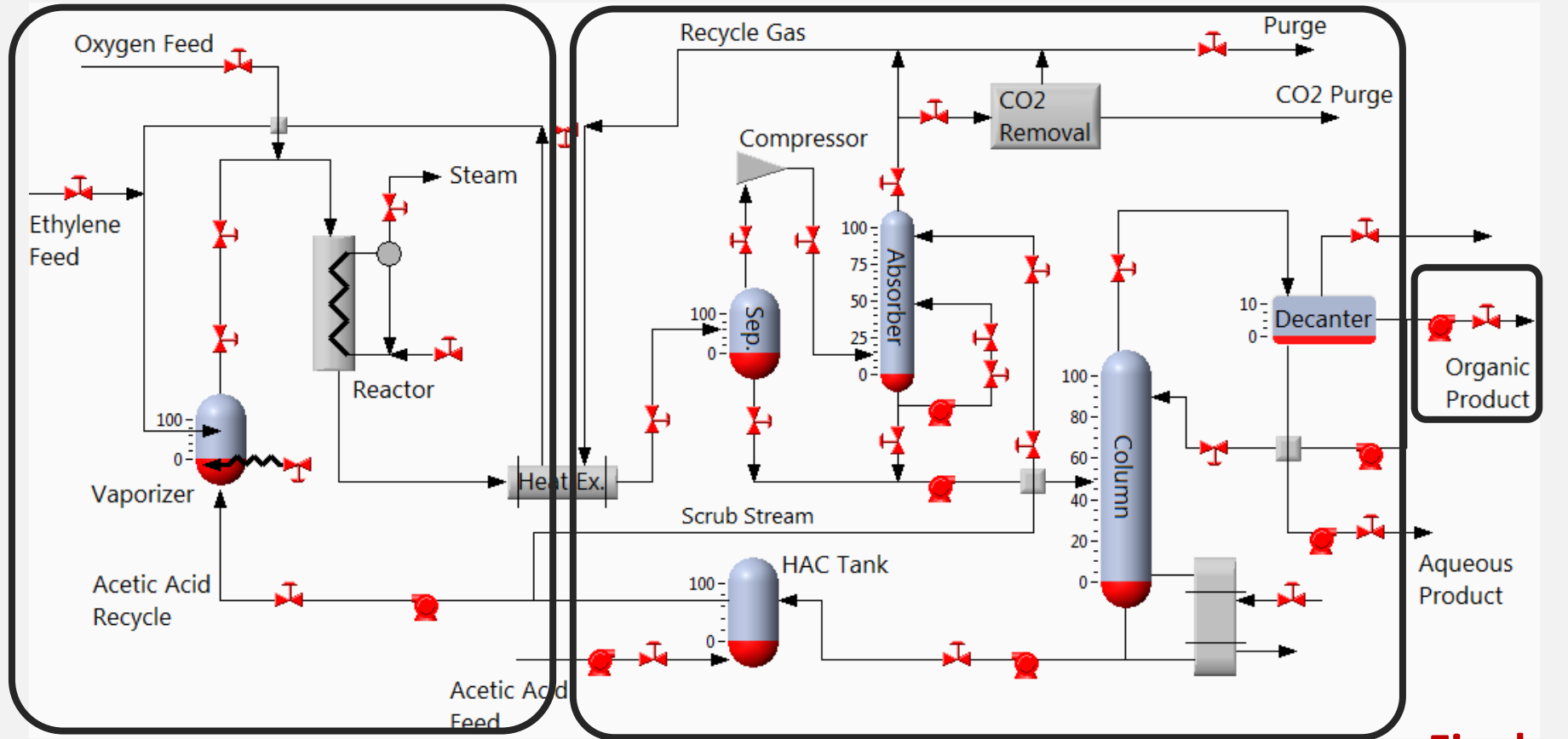
Stripper is...



Stripping column



Max economic damage?



Reaction

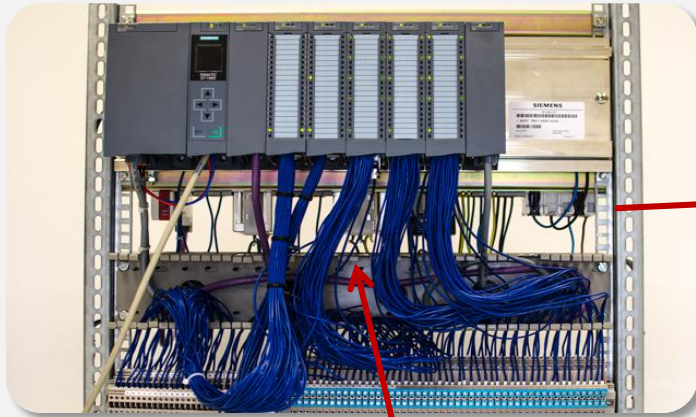
Refinement

Final product

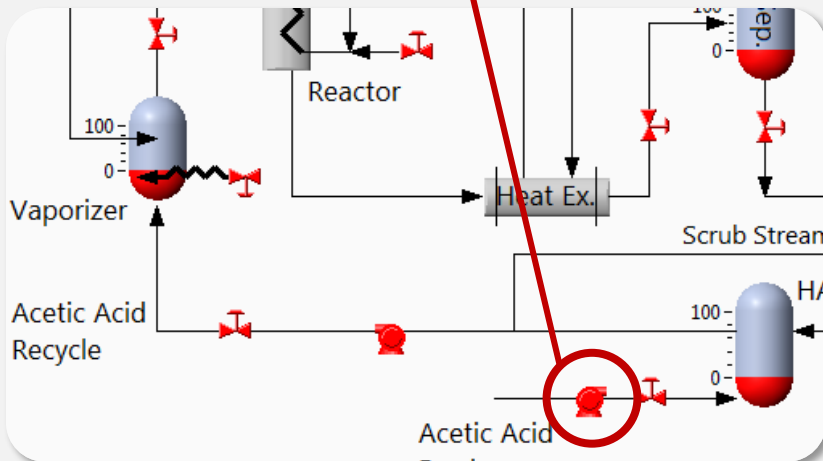
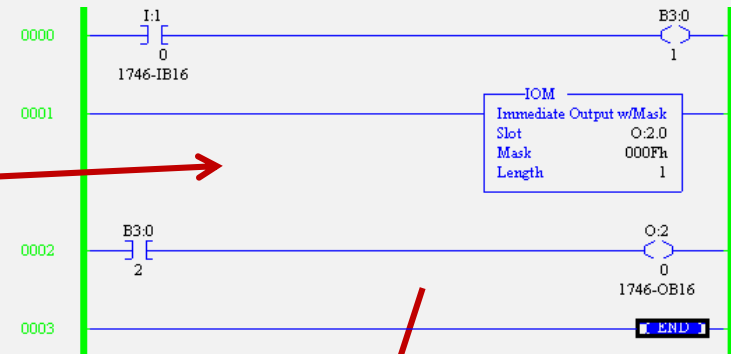
Requires input of subject matter experts

Understanding points and logic

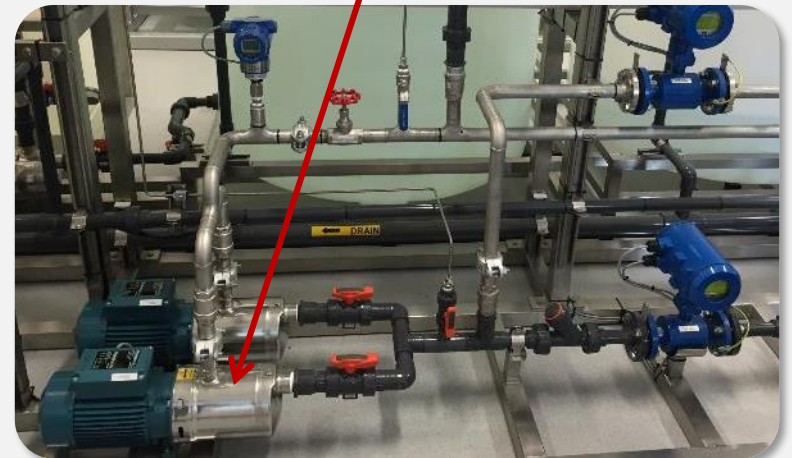
Programmable Logic Controller



Ladder logic



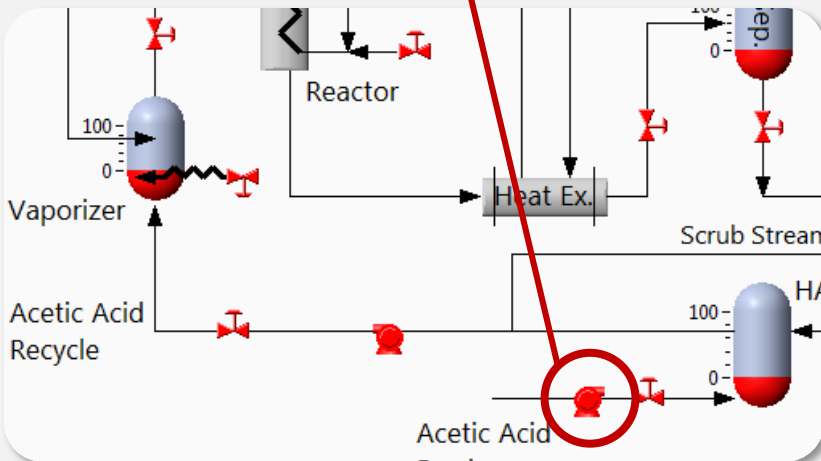
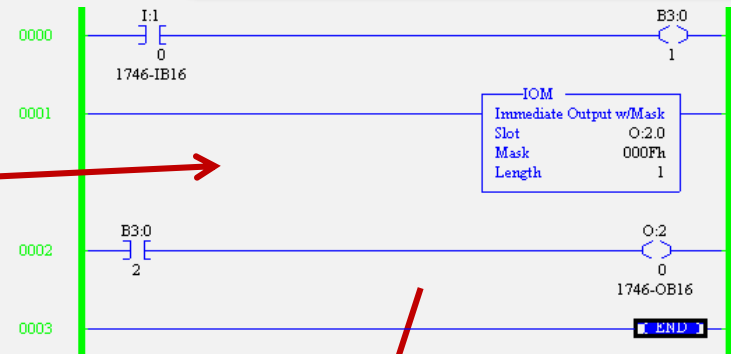
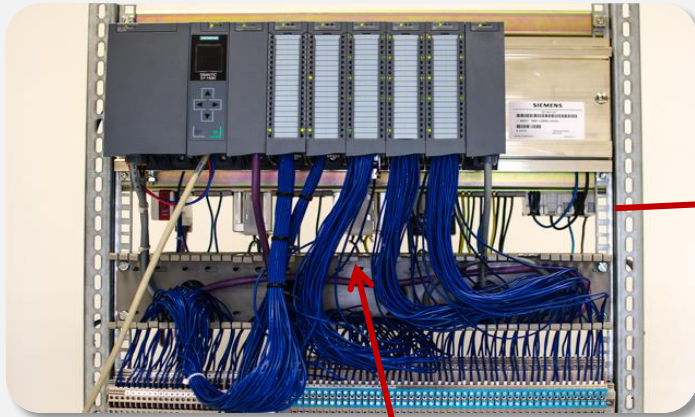
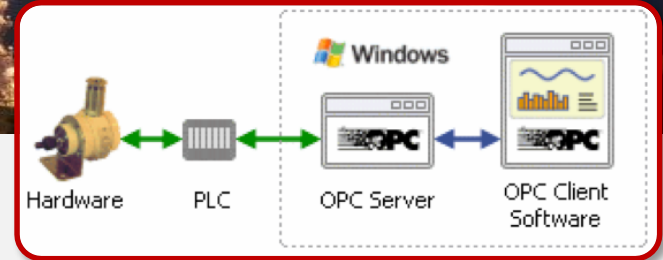
Piping and instrumentation diagram



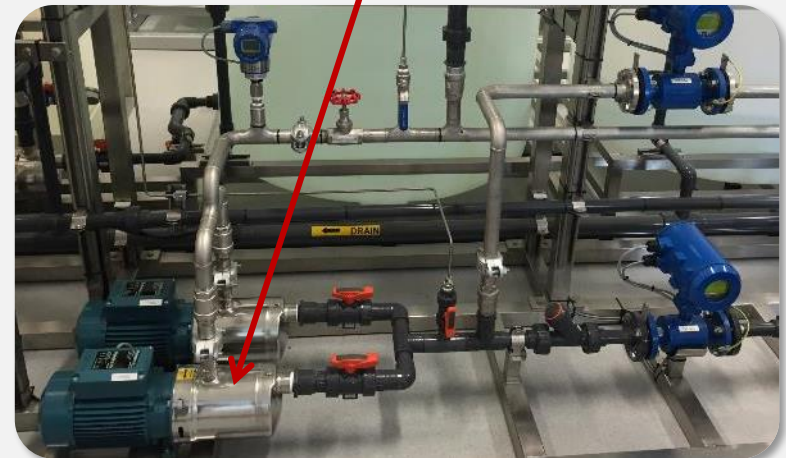
Pump in the plant

Understanding points and logic

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

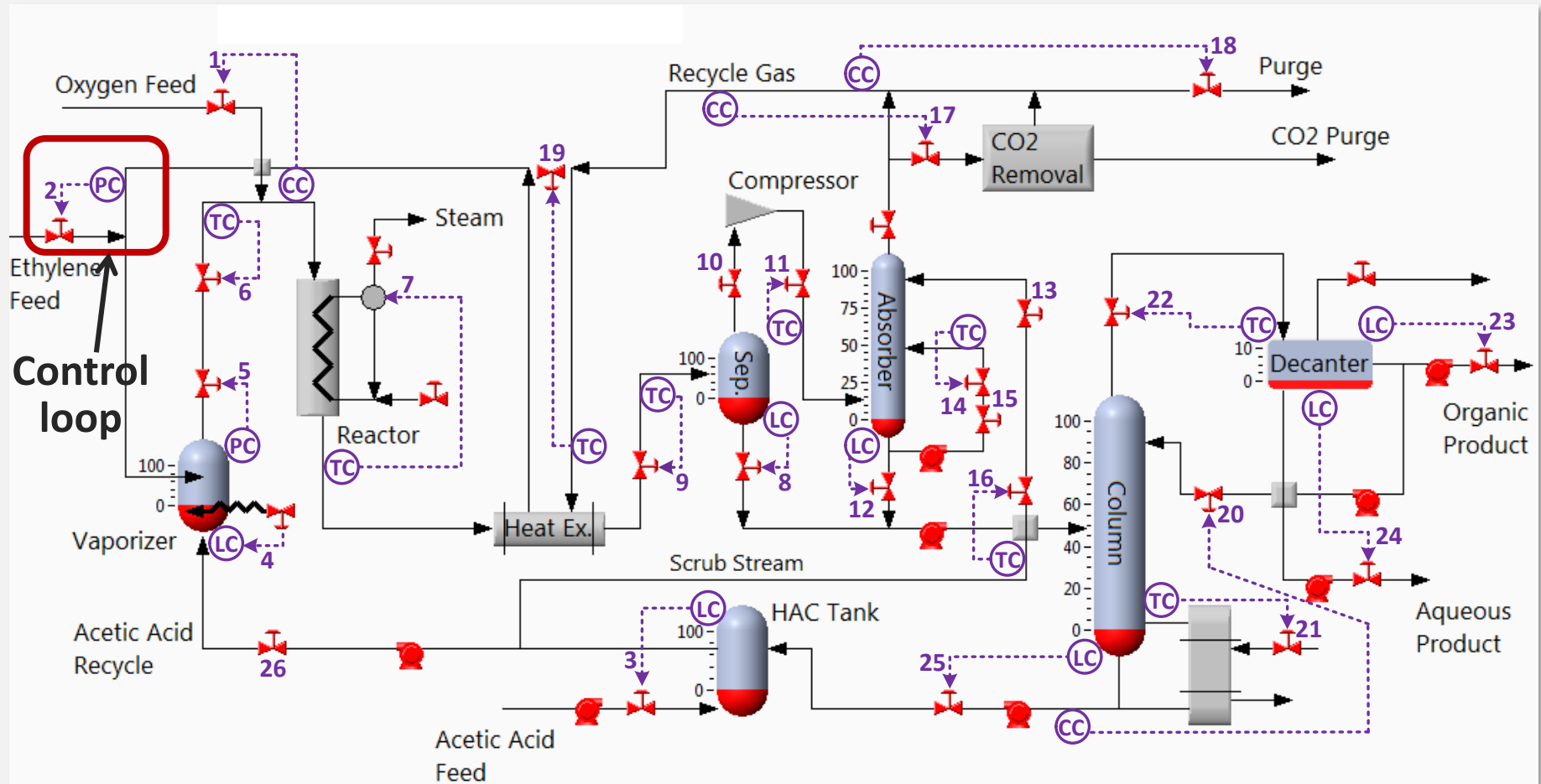


Piping and instrumentation diagram



Pump in the plant

Understanding control structure



Control loop configuration

AVEVA Instrumentation Engineer Contextual Actio...

Project Home Data Management View Instruments

Database Revisions Audit Log Claims Publish to AVEVA NET AVEVA P&ID Import AVEVA Schematic Model Import AVEVA Tags Import AVEVA Instrumentation Intelli-Link From Excel I/O Allocations Export to Excel Export to PDF Export to XPS

Changes Multi User AVEVA Integration Import Export

Instruments

Drag a column header here to group by that column.

Area	TagNo	Loop No	Loop Service	Loc	Status	Description	Instrument Service	Manufacturer	ModelNo	Assoc Equip	Size	P&ID No	DataSheetNo	LoopDwgNo	GeneralHook	Pr
01	01-FT-003	01-F-003		FLD	New	D/P Transmitter										
01	01-AE-100			FLD	Existing	Sulphur Analyser										
01	01-PT-500	01-P-500	Feed Surge Drum 01-V-500	FLD	Existing	Transmitter	Feed Surge Drum 01-V-500	Yokogawa	EJA110A	01-V-500		01-220-004	700001-2	01-P-500		
01	01-PT-510	01-P-510	Reactor 01-R-510	FLD	New	Transmitter	Reactor 01-R-510	Yokogawa	EJA110A	01-P007-80-B1		01-220-004	700001-1			
01	01-FE-510			FLD	Existing	Orifice Plate	Reactor 01-R-510 Feed			01-P007-80-B1		01-220-004		01-F-510		
01	01-FT-510	01-F-510	Reactor 01-R-510 Feed	FLD	Replace	D/P Transmitter	Reactor 01-R-510 Feed			01-P007-80-B1		01-220-004		01-F-510	00000-1	
01	01-FC-510	01-F-510	Reactor 01-R-510 Feed	DCS	New	Controller	Reactor 01-R-510 Feed							01-F-510		
01	01-FAL-510	01-F-510	Reactor 01-R-510 Feed	DCS	New	Alarm Low	Reactor 01-R-510 Feed							01-F-510		

Instrument Datasheet

700001-1

Save Copy Print Preview Issue Reset Zoom Preferences

Default Project/Process Units : Density: kg/m³ Flow: kg/hr Level: mm Mass: kg Pressure: bar Temperature: °C Viscosity: mPa.s

D582040

Instrument Datasheet

PRESSURE TRANSMITTER

1	Tag No.	01-PT-510
2	Service	Reactor 01-R-510
3	P&ID No.	01-220-004
4	Line Number	01-P007-80-B1
5	Area Classification	Zone 1, Gr IIC, T3
6	Ingress Protection	IP 67
PROCESS CONDITIONS		
7	Fluid	HC
8	State	Vapour
9	Pressure	Normal Max: 1450 KPag
10	Temperature	Normal Max: 100 °C
TRANSMITTER		
11	Instrument Range LRV / URV / Un	-0.5 / 14 / MPa
12	Calibration Range LRV / URV / Un	0 / 1700 / KPag
13	Accuracy	+/-0.075% of Span
14	Elevation	Suppression
15	LP Proc. Conn.	HP Proc. Conn.
16	Conduit Connect	Power Supply
17	Housing	Paint
ELEMENT		
20	Element Type	Element Material
21	Measurement (Gauge / Abs / Vac etc)	DP Capsule
22	Body Material	Body Rating
23	Bolts	Seals
24	Other wetted materials	Diaphragm - Hastelloy-C276, Vent Plug - SUS316
25	Fill Fluid	Silicone Oil
26	NACE Certification	MR-0175-2001 Required

Audit Manager

Tools

Find Print Refresh Close

AVEVA Application Object Type

Loop List

Process Data

Process Equipment List

Process Line List

Apply Date/Time

Occurred After: 14/05/2013 00:00

Occurred Before: 15/05/2013 00:00

Apply Limit

Max Limit to Display: 1000

Apply

Datasheet Data, Instrument List, Process Data

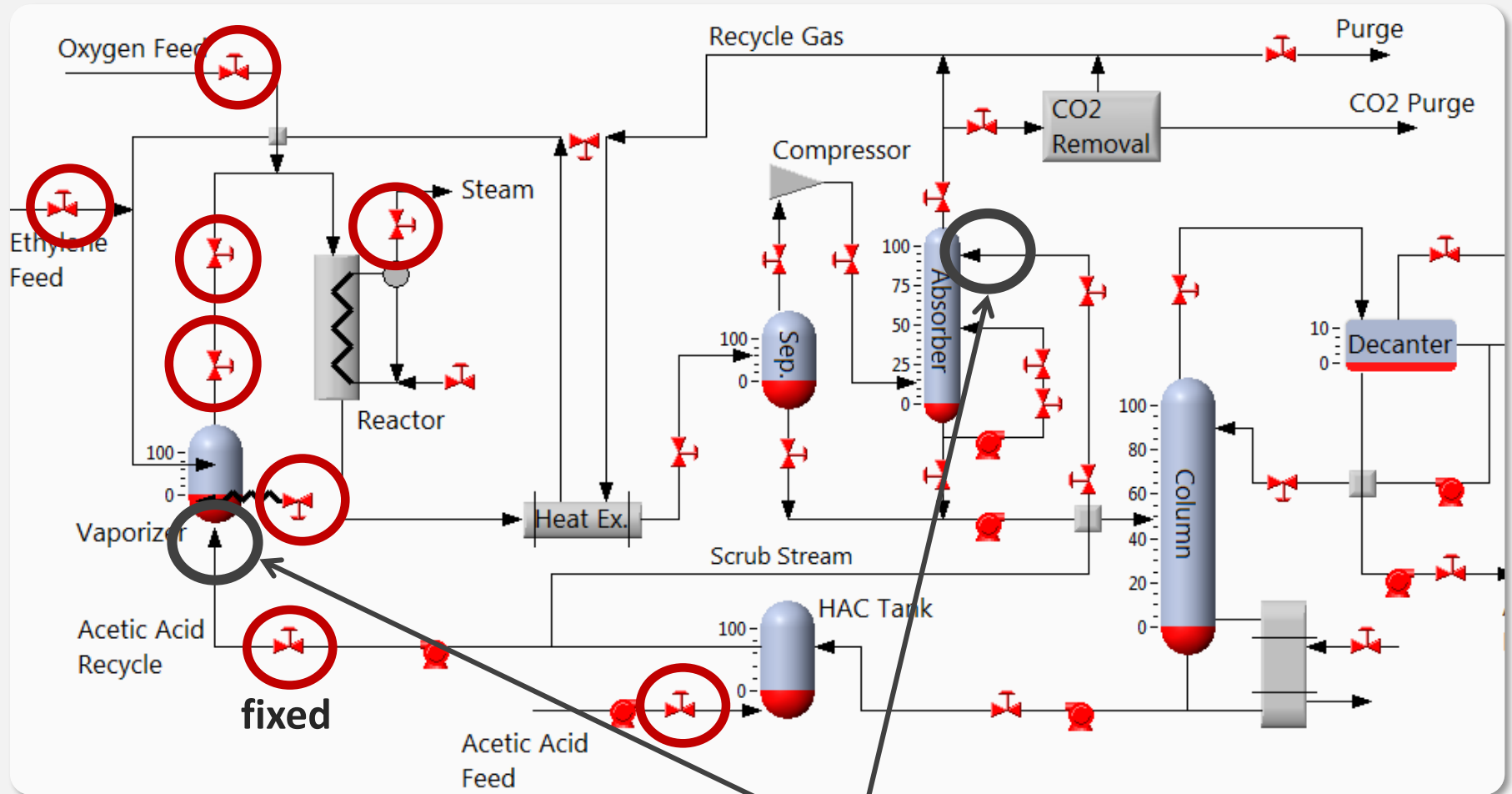
Drag a column header here to group by that column.

Type	Item Tag	Description	New Value	Old Value	User	TimeStamp
Datasheet Data	01-PT-510	Transmitter Updat	Downscale	Fail High = 21.6m	AVEVA\keith.hillier	15/05/2013 09:5
Process Data	01-PT-510	PressureMax Updat	1650	1430	AVEVA\keith.hillier	15/05/2013 09:5
Process Data	01-PT-510	PressureMaxUnits	KPag	KPag	AVEVA\keith.hillier	15/05/2013 09:5
Process Data	01-PT-510	PressureNormalUn	KPag	KPag	AVEVA\keith.hillier	15/05/2013 09:5
Process Data	01-PT-510	PressureNormal U	1450	1200	AVEVA\keith.hillier	15/05/2013 09:5
InstrumentList		Tag Deleted		01-FT-999	AVEVA\keith.hillier	15/05/2013 09:5
InstrumentList		Tag Deleted		01-FE-999	AVEVA\keith.hillier	15/05/2013 09:5
InstrumentList	01-FE-510	CalcTypeID Updat	2	1	AVEVA\keith.hillier	15/04/2013 15:0
Process Data	01-FE-510	Updated			AVEVA\keith.hillier	15/04/2013 15:0
Process Data	01-FE-510	Updated			AVEVA\keith.hillier	15/04/2013 15:0
Process Data	01-FE-510	Updated			AVEVA\keith.hillier	15/04/2013 15:0
Process Data	01-FE-510	szTemperature Up	100	100	AVEVA\keith.hillier	15/04/2013 15:0
Process Data	01-FE-510	szViscosity Update	200	200	AVEVA\keith.hillier	15/04/2013 15:0
Process Data	01-FE-510	Updated			AVEVA\keith.hillier	15/04/2013 15:0
Process Data	01-FE-510	Updated			AVEVA\keith.hillier	15/04/2013 15:0

AVEVAdefault (27 Records)

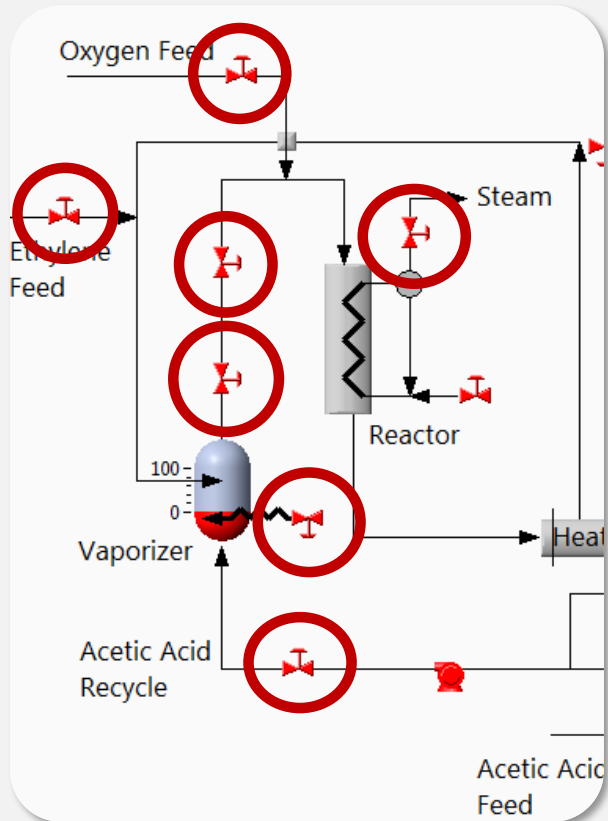
Project : AI Demo SP1 User : Keith.Hillier

Watch the flows!



HAc flows into two sections. Not good :(

Obtaining control != being in control



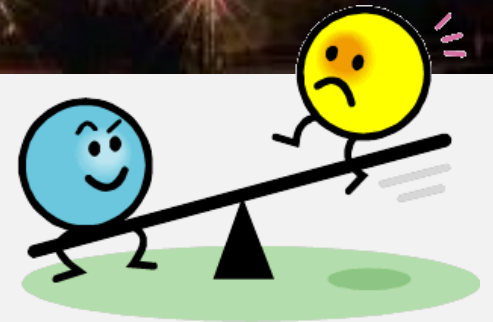
- ❑ Obtained controls might not be useful for attack goal
- ❑ How do I even speak to this thing??
K. Wilhoit, S. Hilt. The little pump gauge that could: Attacks against gas pump monitoring systems. Black Hat (2015)
- ❑ Attacker might not necessary be able to control obtained controls

Huh ???





Control



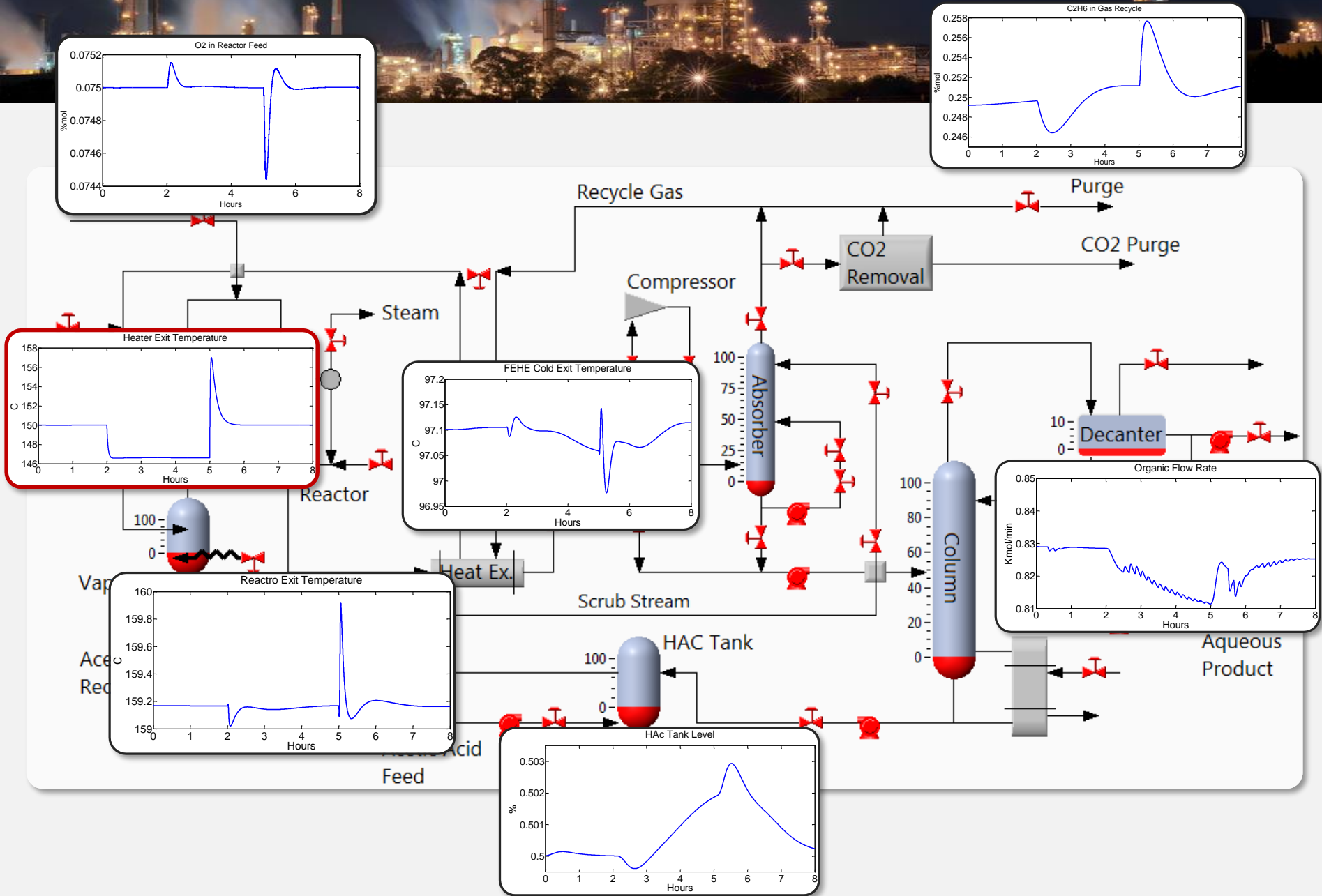
Every action has a reaction

Physics of process control

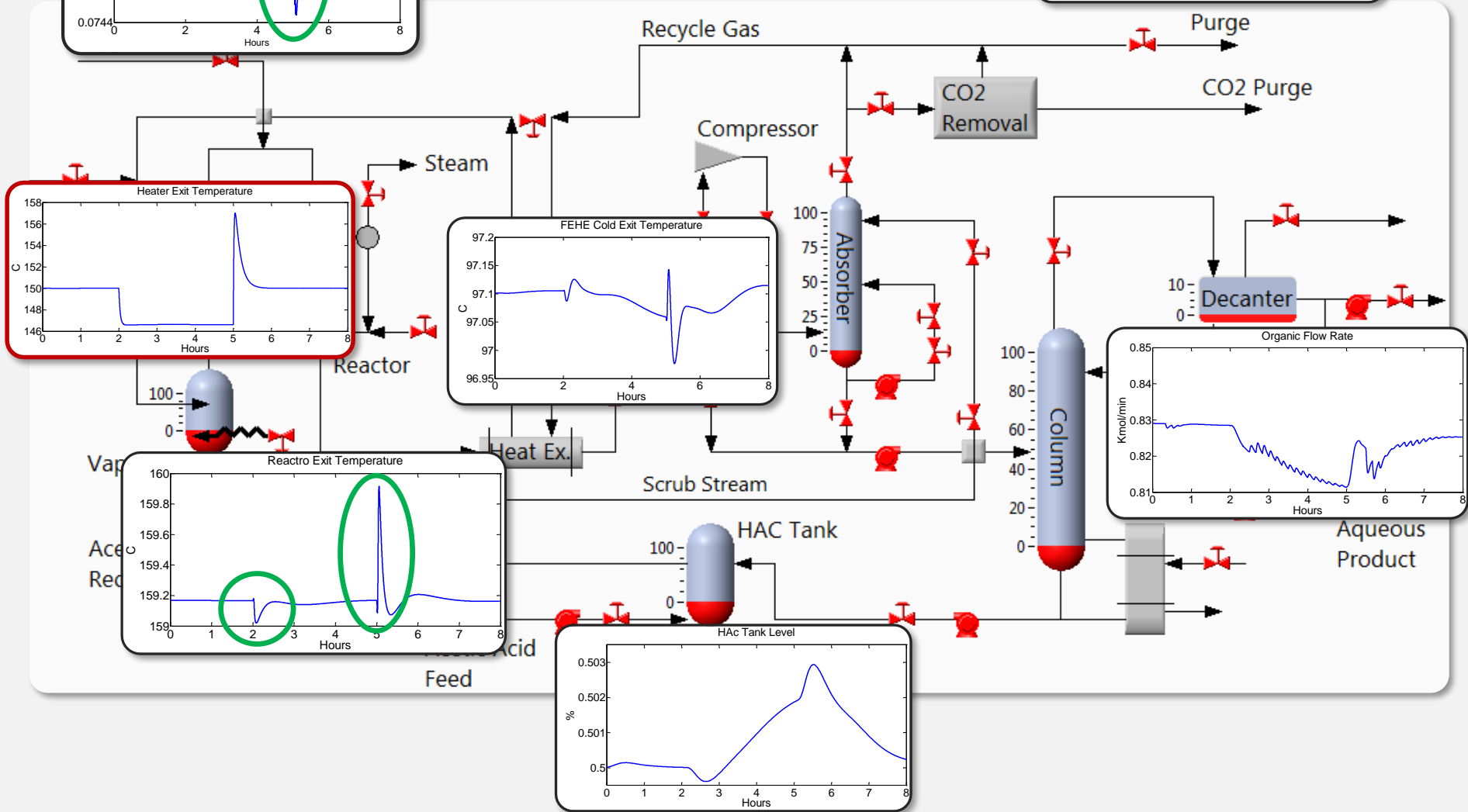
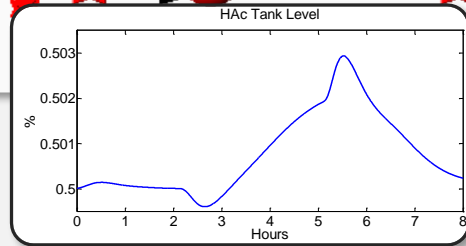
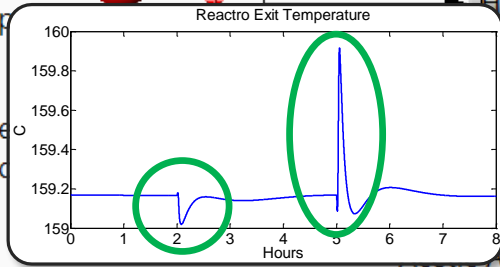
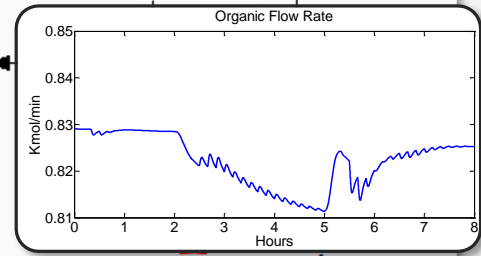
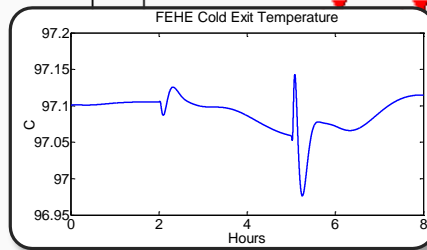
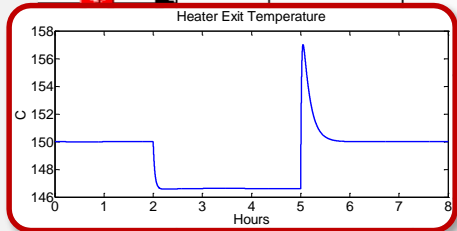
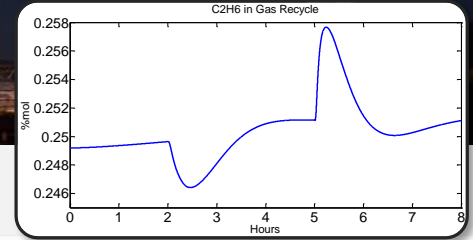
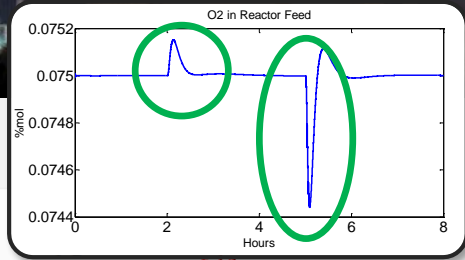
- ❑ **Once hooked up together, physical components become related to each other by the physics of the process**
- ❑ **If we adjust a valve what happens to everything else?**
 - Adjusting temperature also increases pressure and flow
 - All the downstream effects need to be taken into account (upstream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



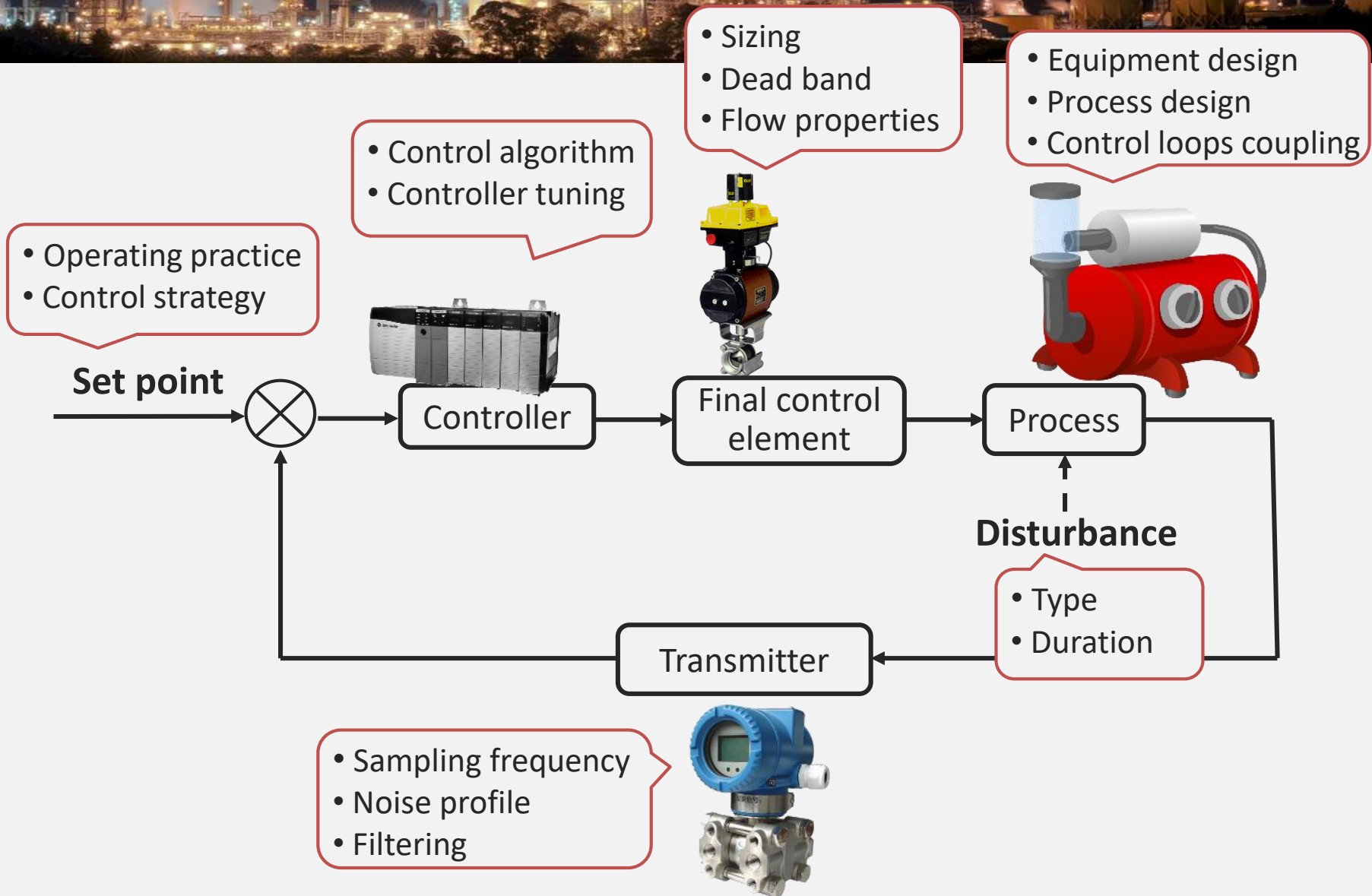
Process interdependencies



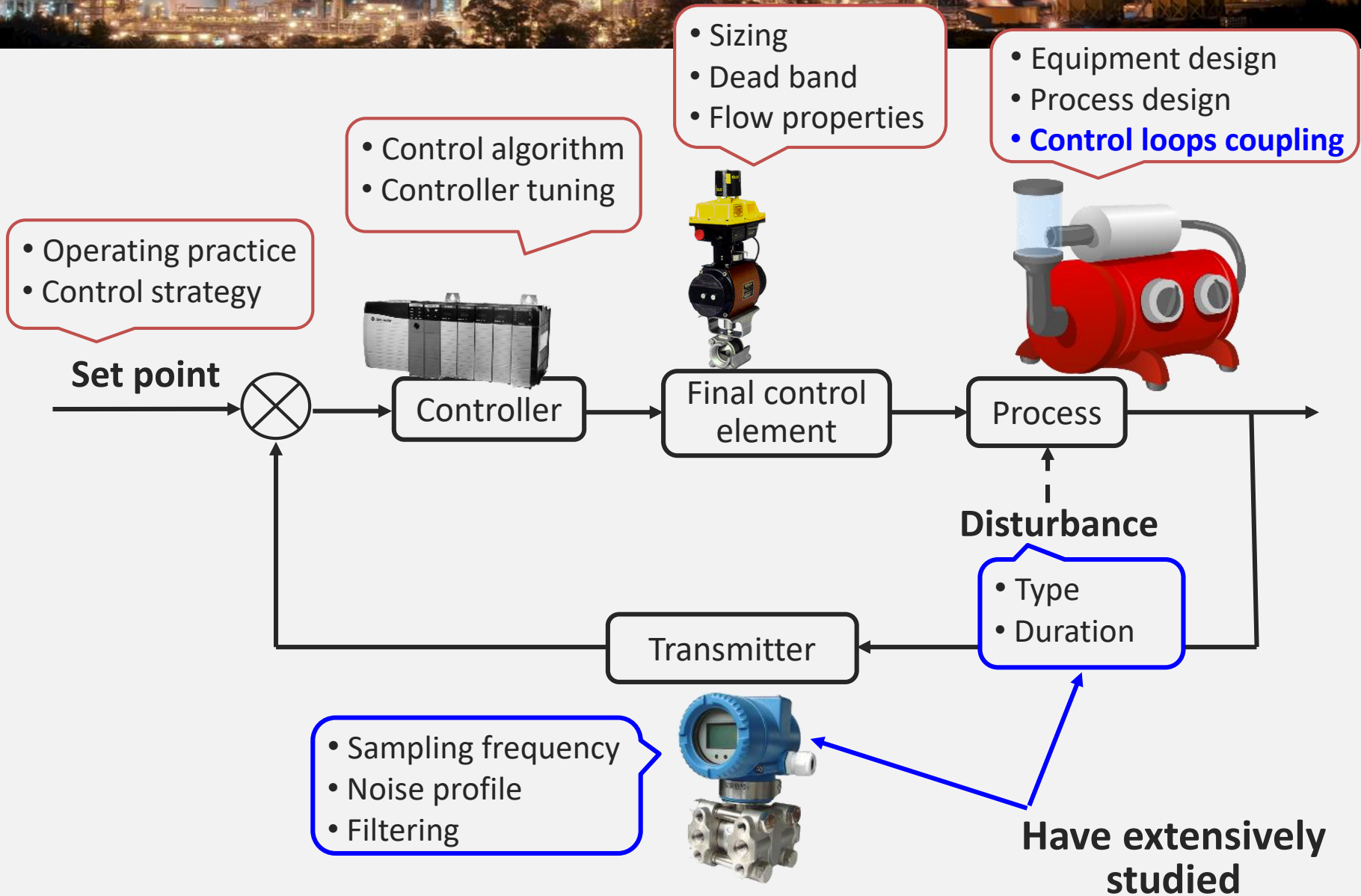
Process interdependencies



Understanding process response



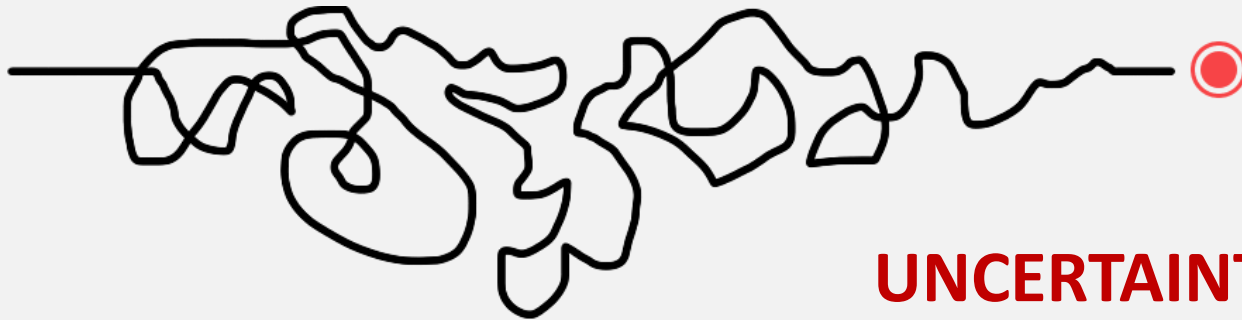
Understanding process response



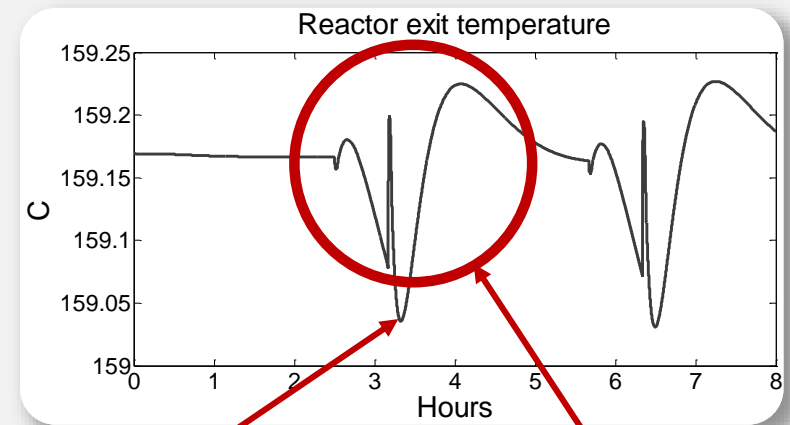
Process control challenges



- ❑ 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



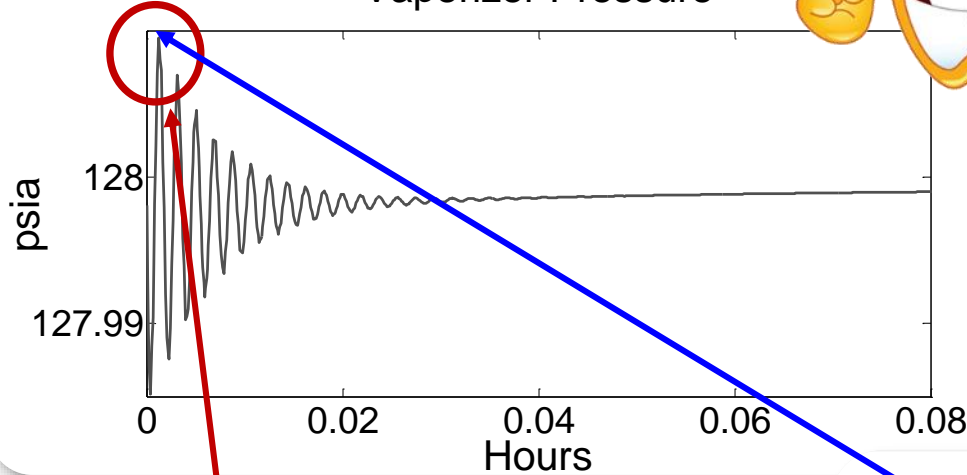
This triggers alarms

Non-linear response

Control loop ringing



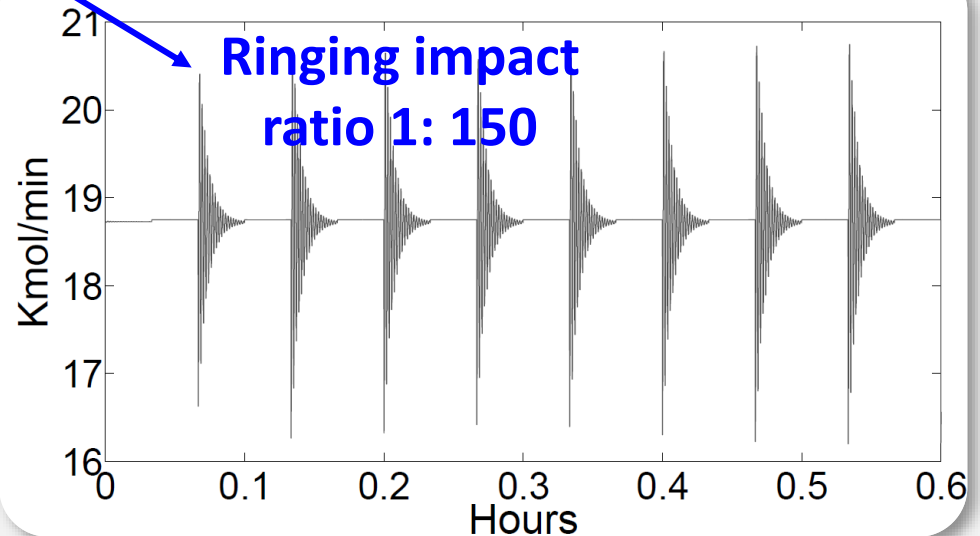
Vaporizer Pressure



Amount of chemical entering the reactor



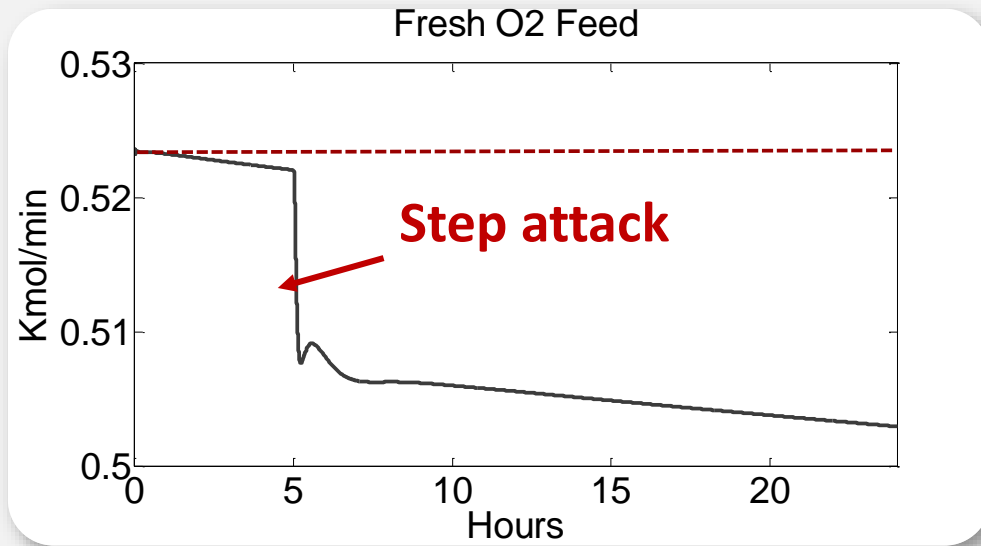
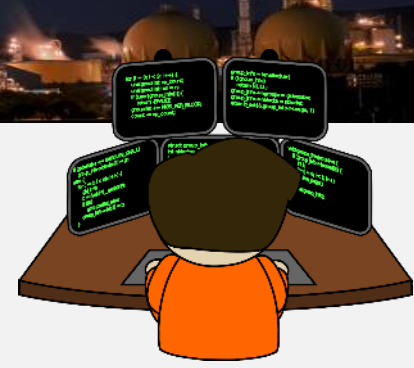
Vaporizer Exit Flow



Caused by a negative real controller poles

Makes process unstable and uncontrollable

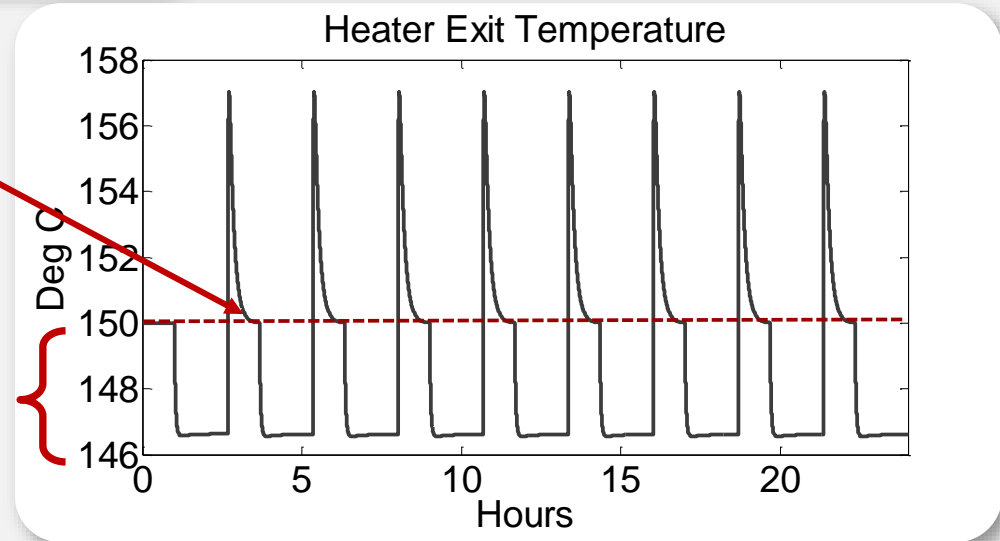
Types of attacks



Periodic attack

Recovery time

Magnitude of manipulation



Outcome of the control stage



I am 163 cm tall

We should automate this process
(work in progress)



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

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**



Damage



How to break things?

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



Hacker unfriendly process

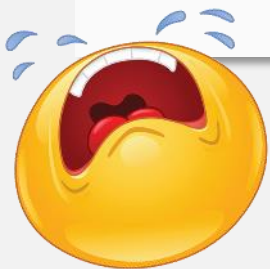
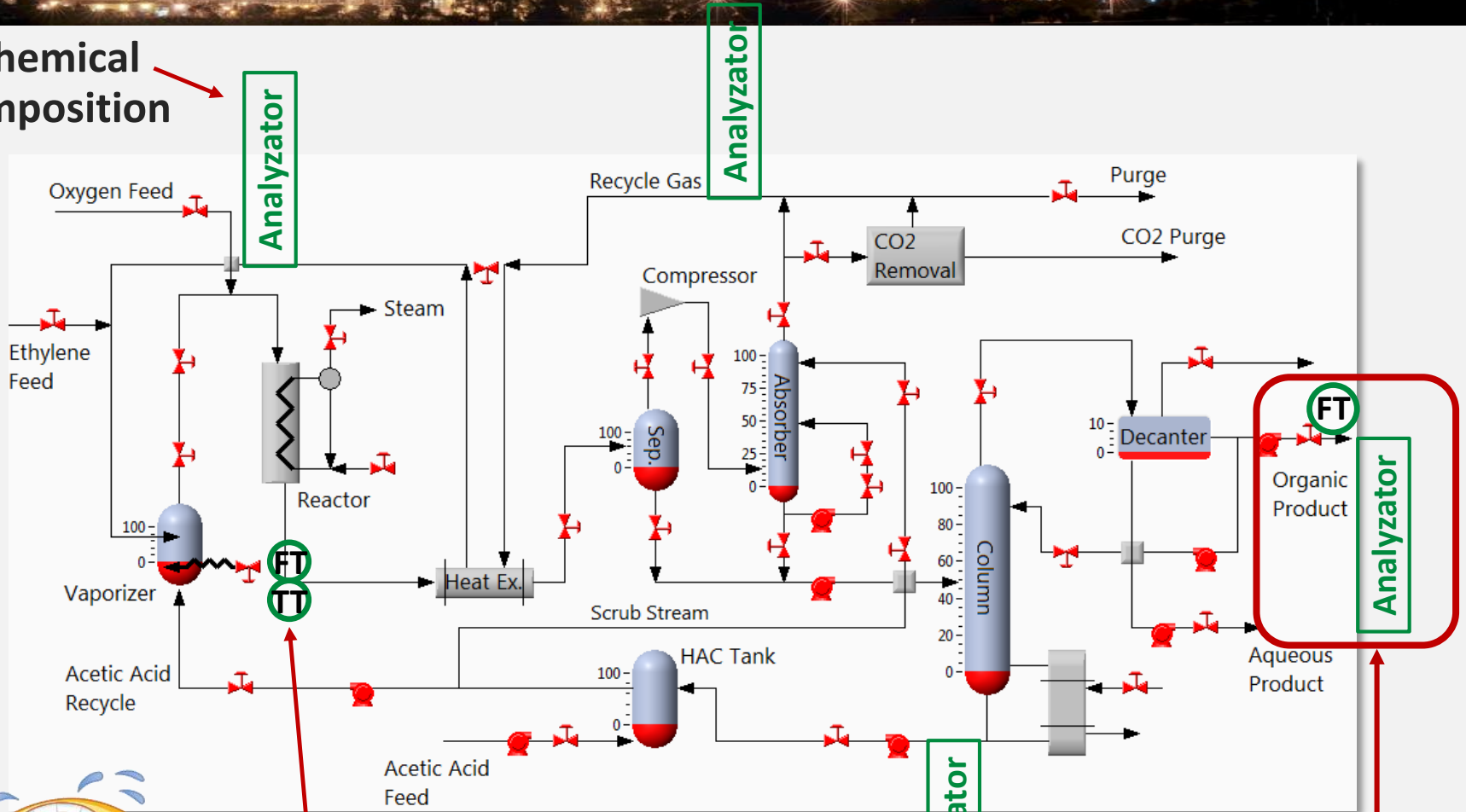


- ❑ Attacker need to obtain feedback in order to observe progress of the attack
- ❑ Target plant may not have been designed in a hacker friendly way
 - There may no sensors measuring exact values needed for the attack execution
 - The information about the process may be spread across several subsystems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



Measuring the 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



Technician vs. engineer

Technician

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

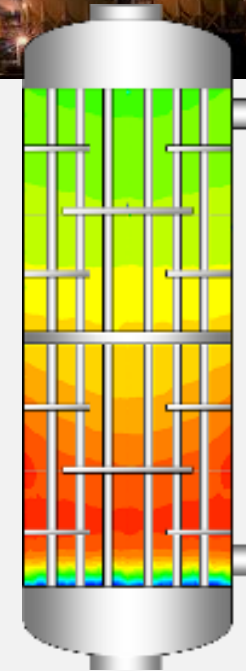
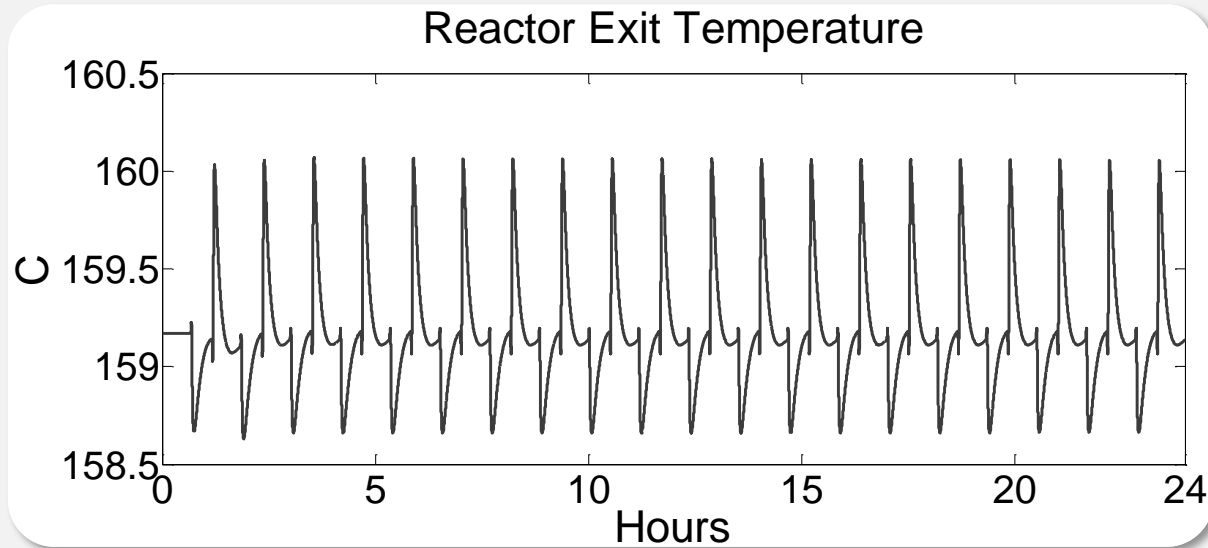


Engineer

“It will be fully drained in 20.4 seconds and 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

```
/*calculate derivatives*/
```

```
for (n=1;n<NR;n++)
```

```
{
```

```
    /*dC/dt=-delta(C*v)/deltaZ+sum(vij*ri)
```

```
    /*Use single backward
```

```
    C_O2_t[n-1]=(-(C_O2[n]*v[n]-C_O2[n-1]*v[n-1])/dz + Coefficient1[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 + Coefficient1[1]*r_all[n][0]+Coefficient2[1]*r_all[n][1])/cata_porosity;
```

```
    C_C2H4_t[n-1]=(-(C_C2H4[n]*v[n]-C_C2H4[n-1]*v[n-1])/dz + Coefficient1[2]*r_all[n][0]+Coefficient2[2]*r_all[n][1])/cata_porosity;
```

```
    C_VAc_t[n-1]=(-(C_VAc[n]*v[n]-C_VAc[n-1]*v[n-1])/dz + Coefficient1[4]*r_all[n][0]+Coefficient2[4]*r_all[n][1])/cata_porosity;
```

```
    C_H2O_t[n-1]=(-(C_H2O[n]*v[n]-C_H2O[n-1]*v[n-1])/dz + Coefficient1[5]*r_all[n][0]+Coefficient2[5]*r_all[n][1])/cata_porosity;
```

```
    C_HAc_t[n-1]=(-(C_HAc[n]*v[n]-C_HAc[n-1]*v[n-1])/dz + Coefficient1[6]*r_all[n][0]+Coefficient2[6]*r_all[n][1])/cata_porosity;
```

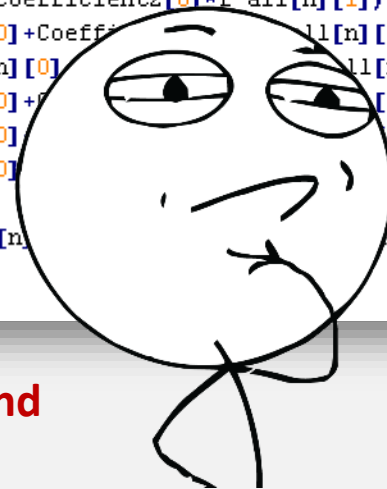
```
    Q_rct[n]= UA*(Tg[n]-Shell_T); /*kcal/min m^3*/
```

```
    Tg_t[n-1]=1/(cata_porosity*CCP[n] + cata_heatcapacity *cata_bulk_density)*(-FCP[n]*r_all[n][0]*E_r1-r_all[n][1]*E_r2-Q_rct[n]);
```

```
};
```

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

CHALLENGE CONSIDERED

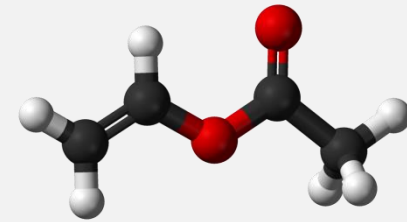
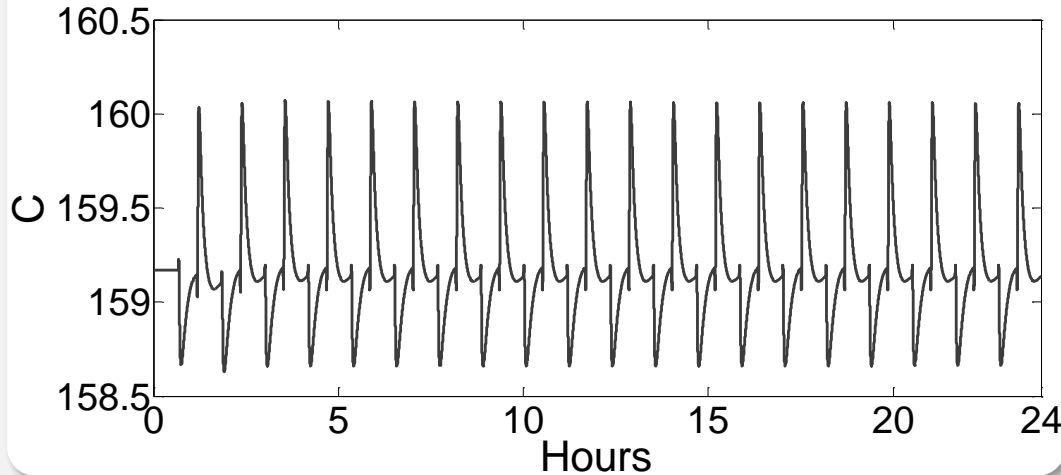


I found needed code but the numbers were very strange and did not seem being useful : 0,00073; 0,00016; 0,0007...

Engineering answer



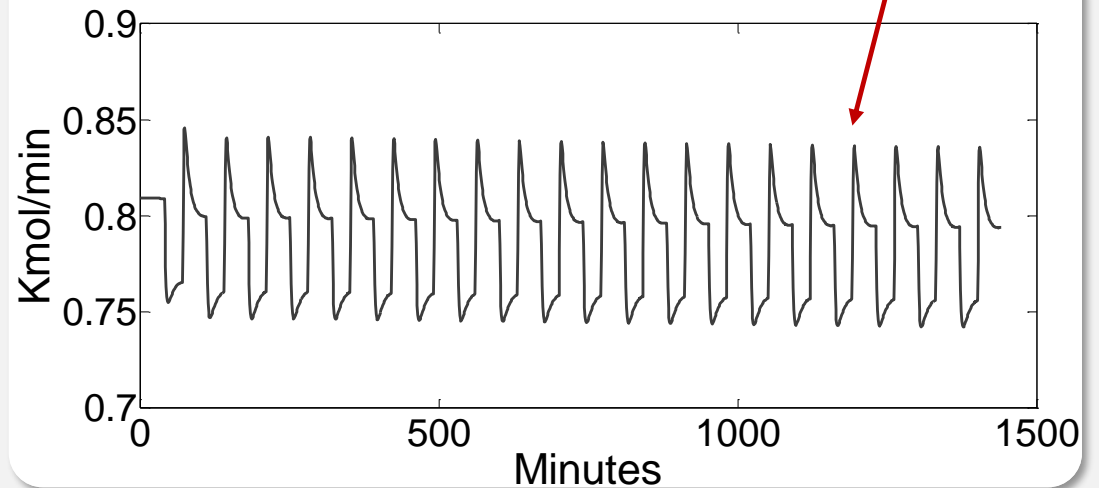
Reactor Exit Temperature



Vinyl Acetate production

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

VAC Concentration

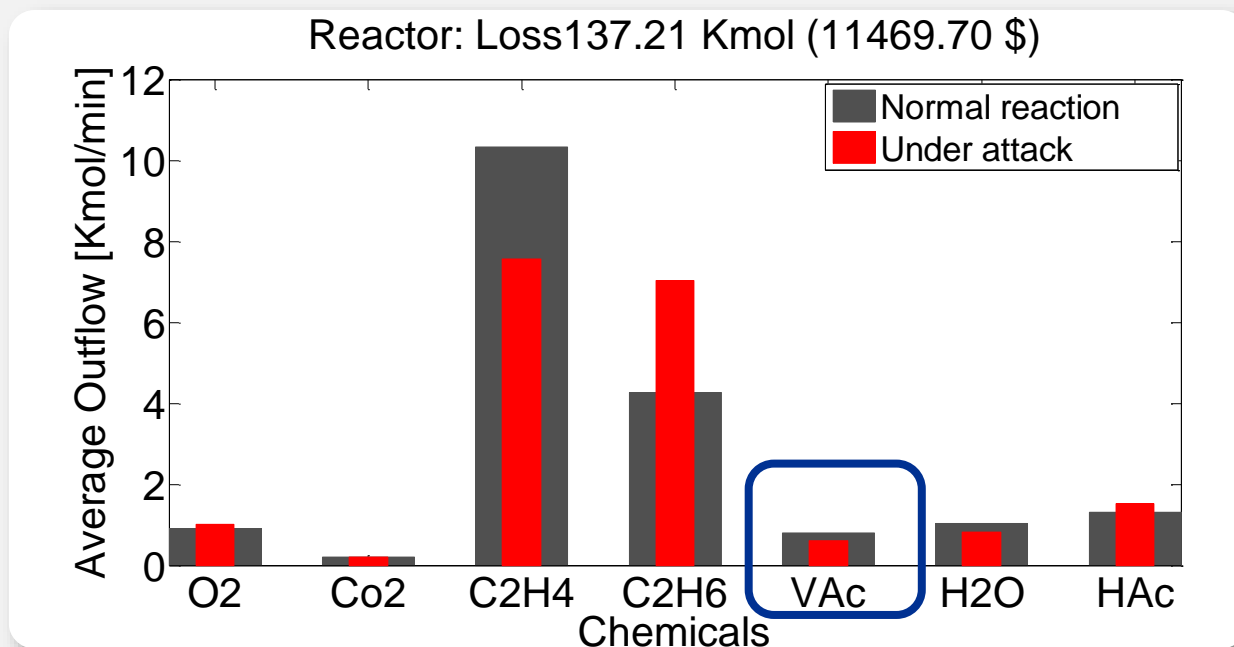


Product loss



Product per day: 96.000\$

Product loss per day: 11.469,70\$



Outcome of the damage stage

Product per day: 96.000\$

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

Still might be useful



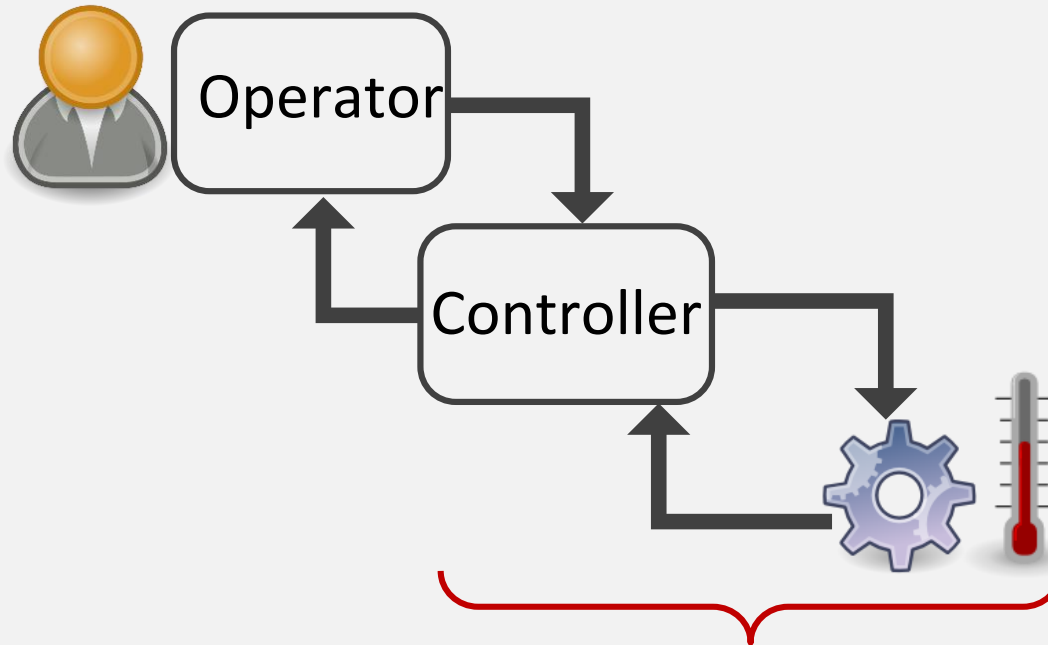
Cleanup



Socio-technical system



- Maintenance staff
- Plant engineers
- Process engineers
-



Cyber-physical system

Creating forensics 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 forensics footprint

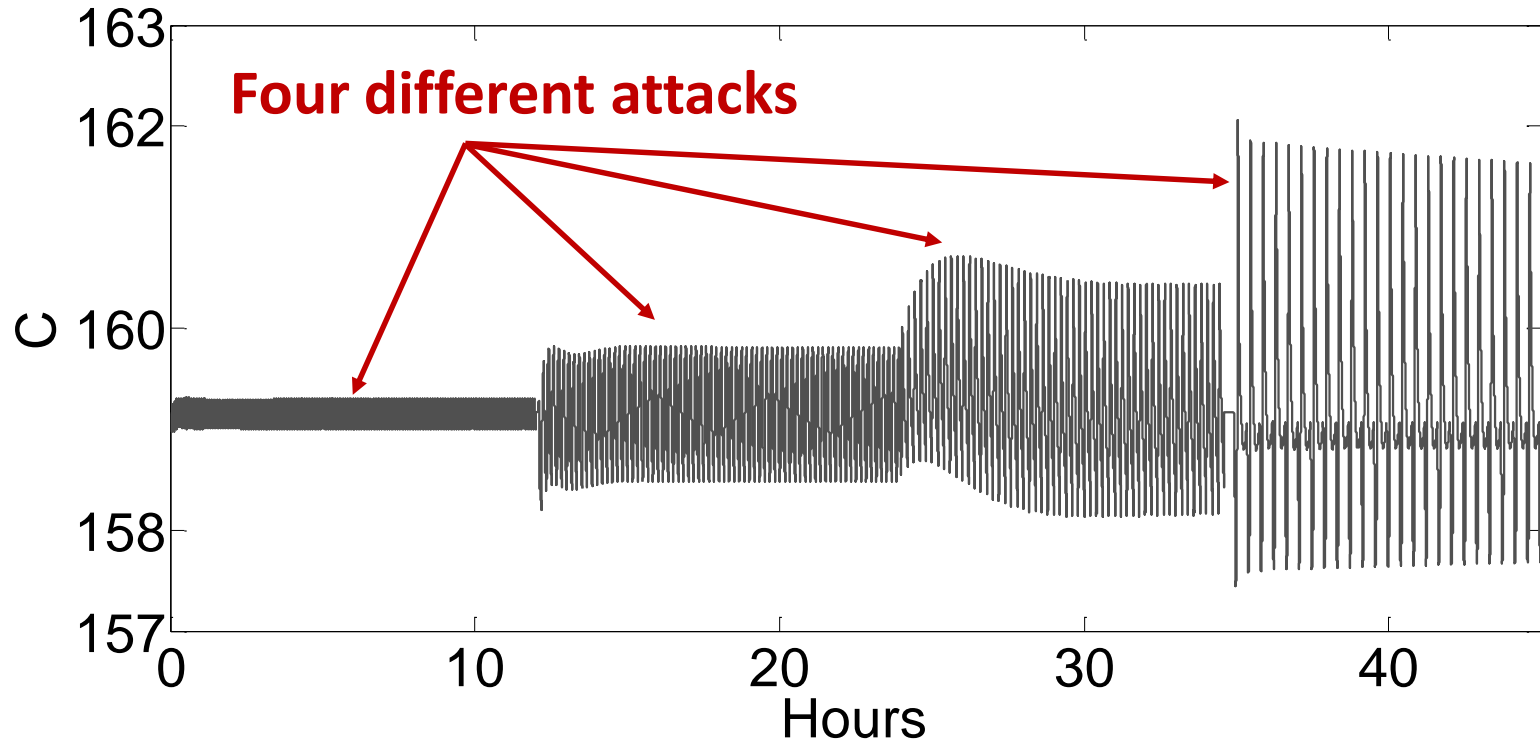
1. Pick several ways that the temperature can be increased
2. Wait for the scheduled instruments calibration
3. Perform the first attack
4. Wait for the maintenance guy being yelled at and recalibration to be repeated
5. Play next attack
6. Go to 4



Creating forensics footprint

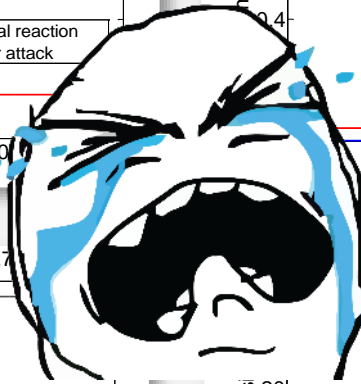
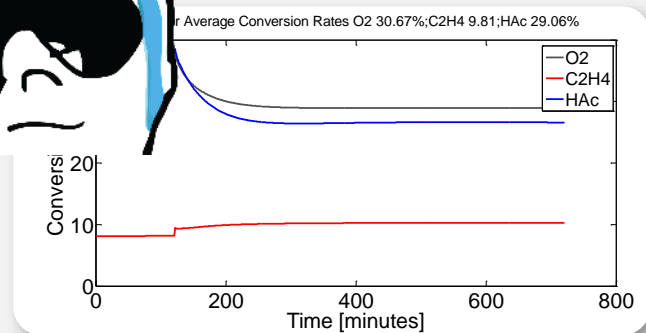
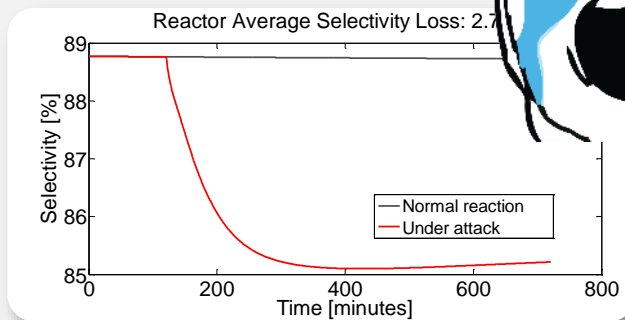
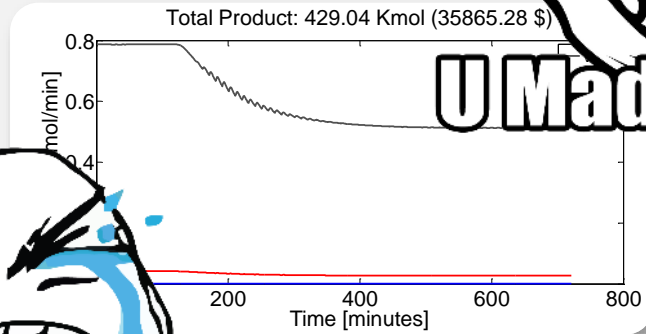
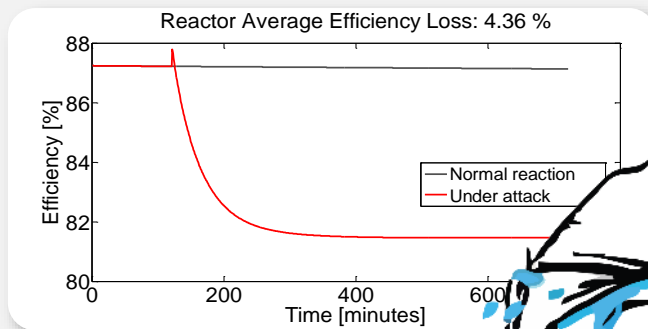
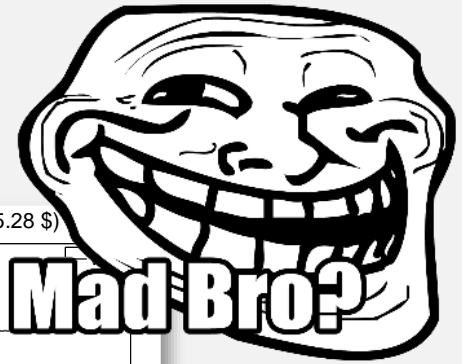


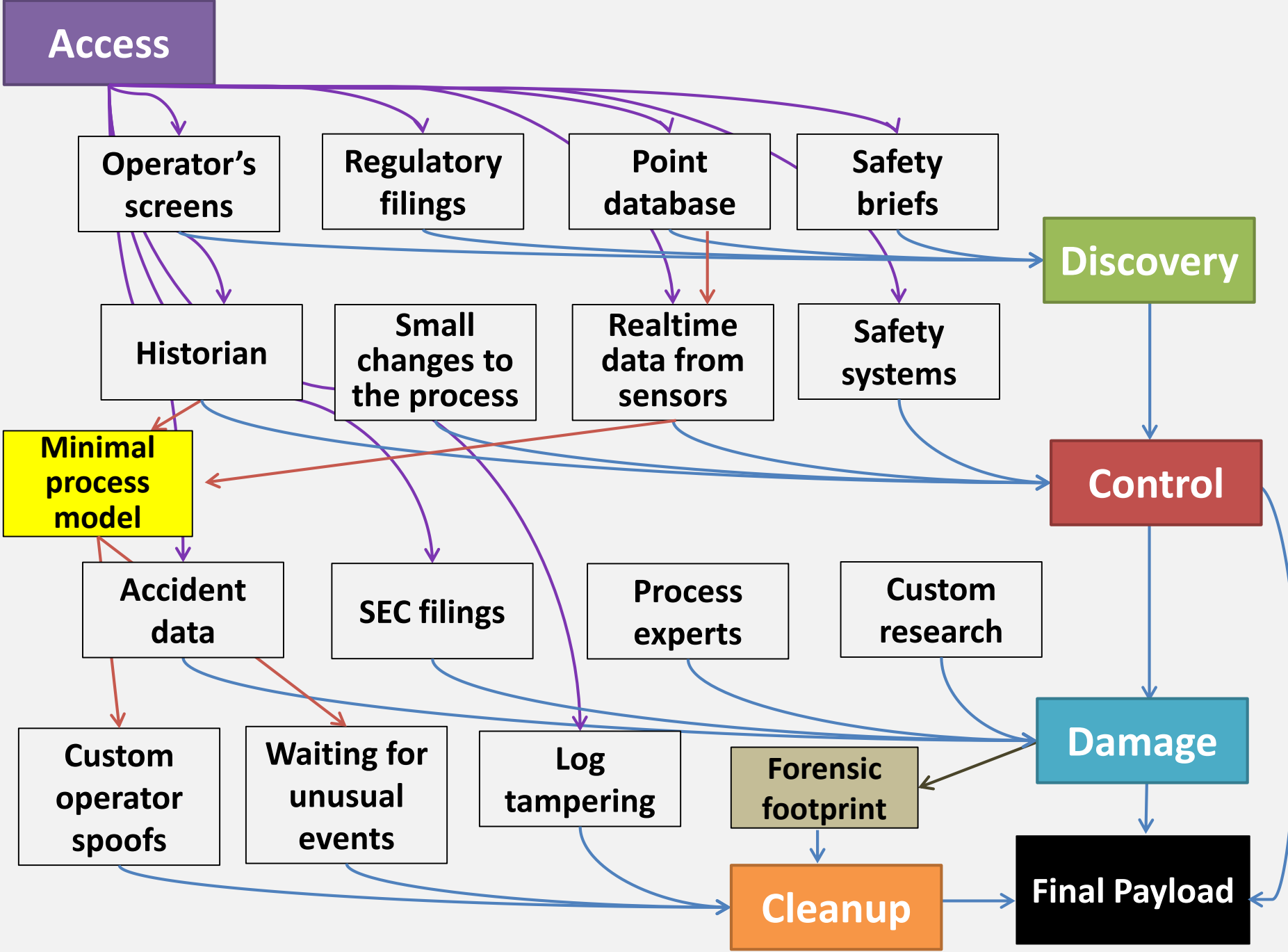
Reactor Temperature



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**





Take away



- ❑ **SCADA hacking can be more sophisticated than simply blowing, breaking and crashing**
 - Espionage attacks matter! They hurt later
- ❑ **Better understanding what the attacker needs to do and why**
 - Eliminating low hanging fruits
 - Making exploitation harder
 - Making cost of attack exceeding cost of damage
- ❑ **Look for the attacker**
 - Wait for the attacker where she has to go
 - Process control stage is done on live process



Q & A



Marina Krotofil
@marmusha
marmusha@gmail.com