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.

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

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.**

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

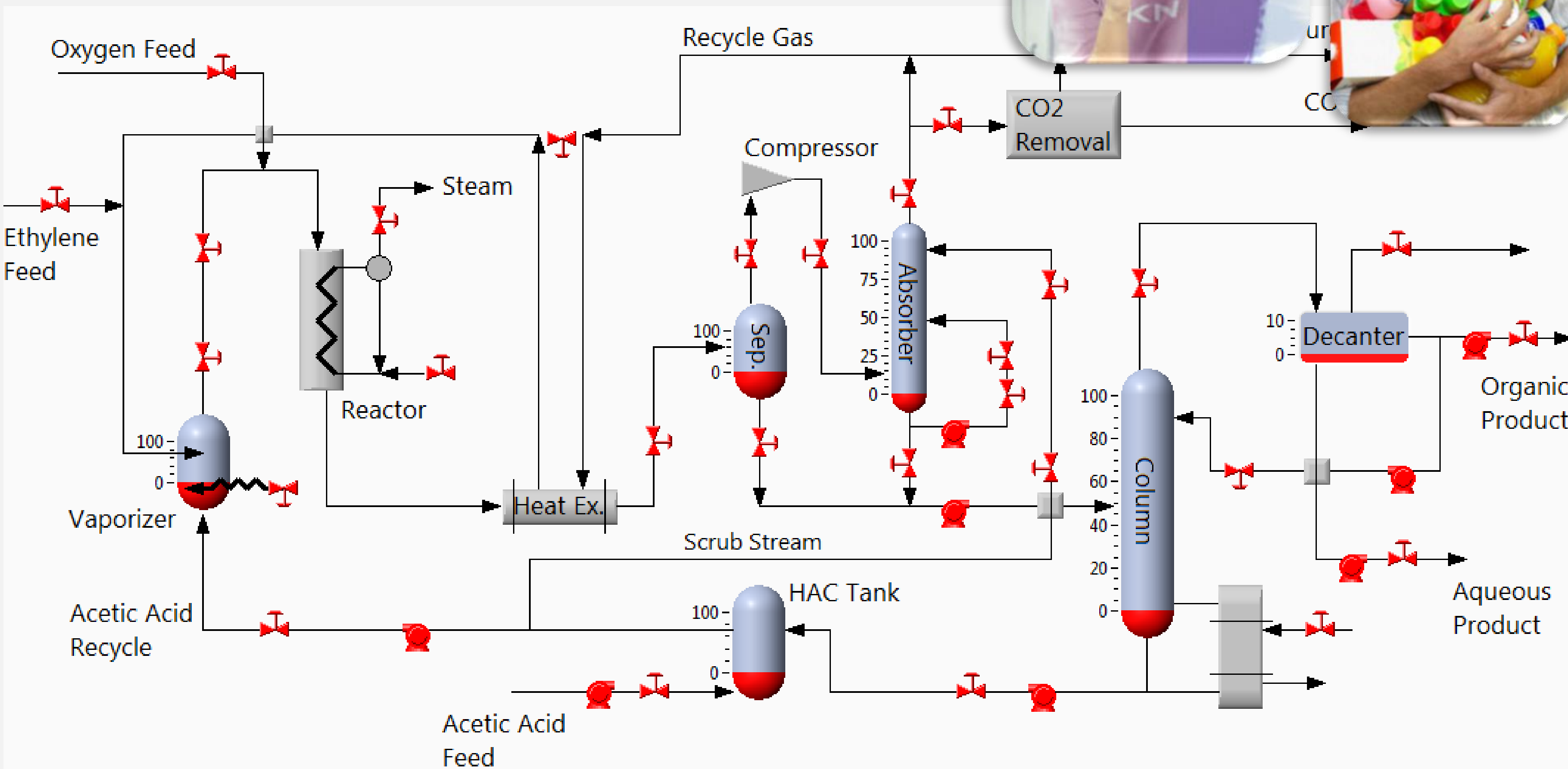
Production damage

Compliance violation

Do this

- **Equipment damage**
  - Comes first into anybody’s mind (+)
  - Irreversible ($\mp$)
  - 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 ($\mp$)
  - 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 mor

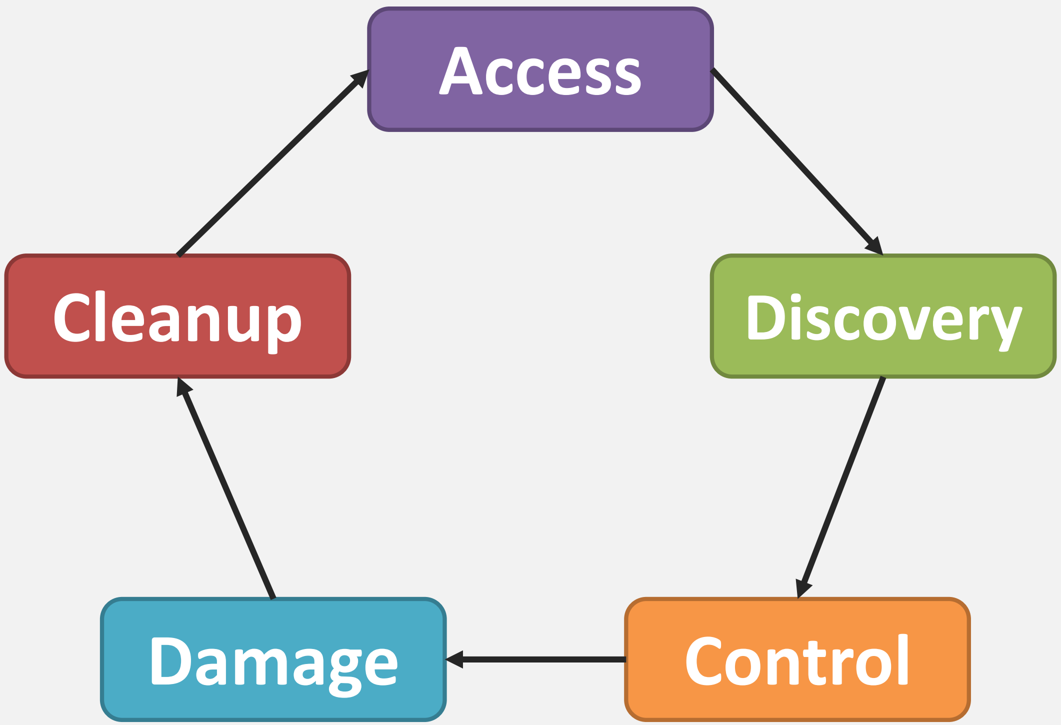
More plants offers:
http://www.usedplants.com/

Car vs. plant hacking

It is not about the size

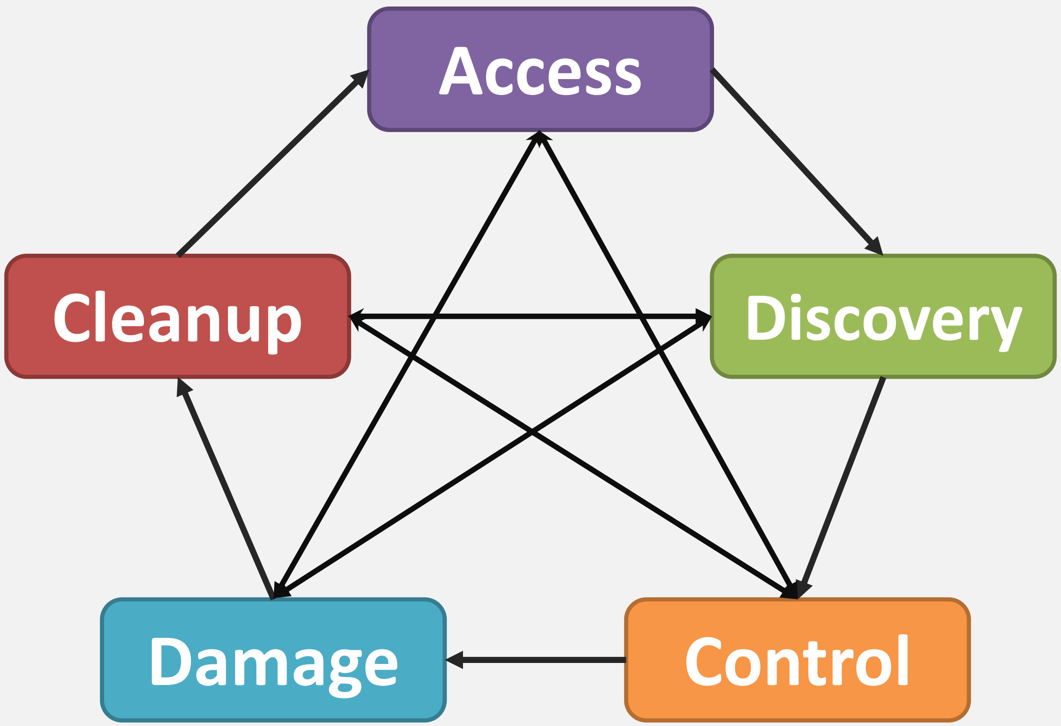
It is about MONEY
Plants are ouch! how expensive -> hence, researching on model

Cyber-physical attack lifecycle, version 2015

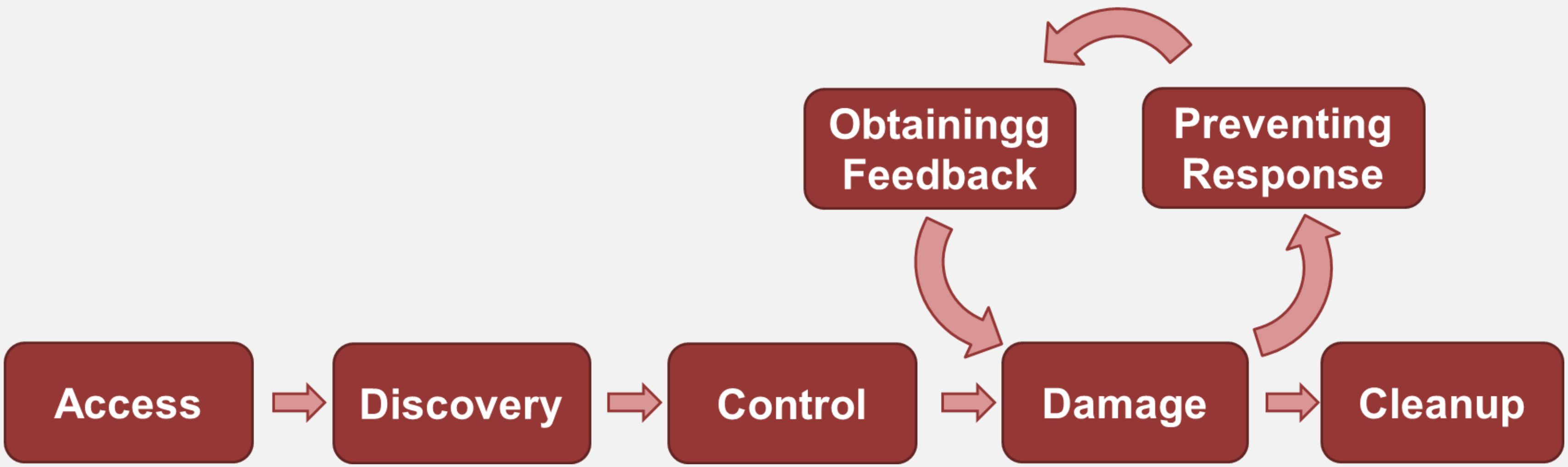


Based on work by J. Larsen. Breakage. Black Hat Federal (2007)

Stages of SCADA attack



Cyber-physical attack lifecycle, version 2019



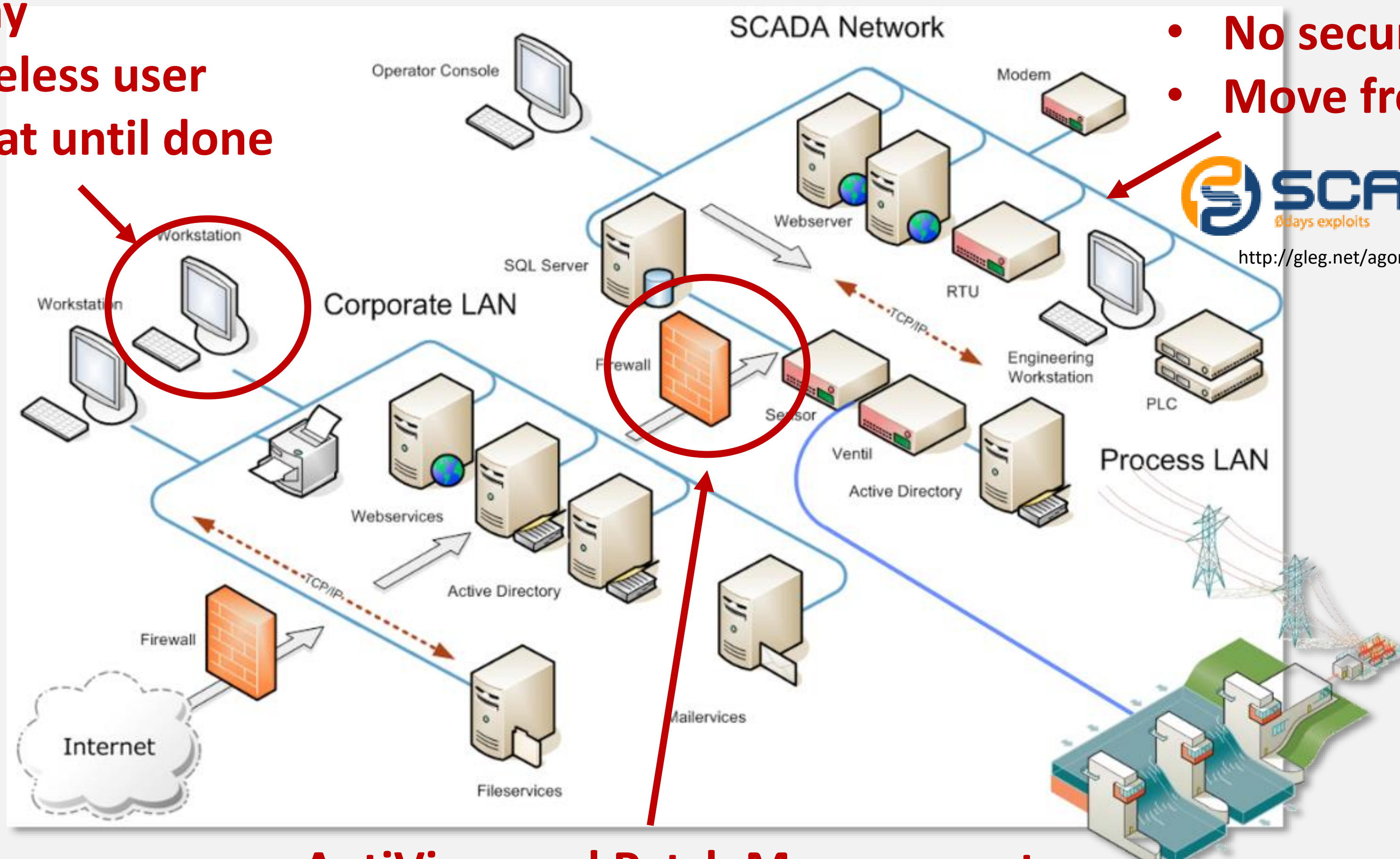
J. Wetzels, M. Krotofil “A Diet of Poisoned Fruit: Designing Implants and OT Payloads for ICS Embedded Devices”, TROOPERS, Heidelberg, Germany, 2019.

Access

Traditional IT hacking

- 1 0day
- 1 Clueless user
- Repeat until done

- No security
- Move freely

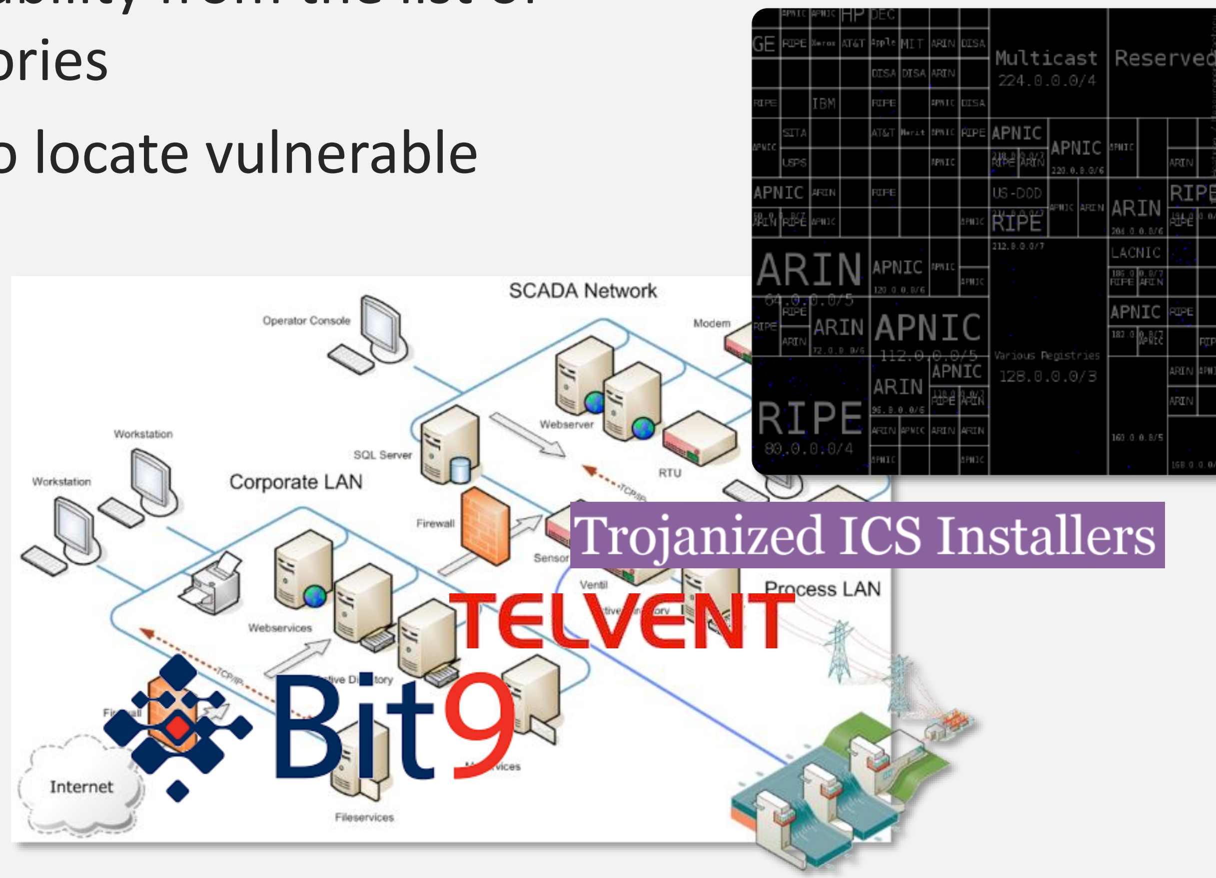


http://gleg.net/agora_scada.shtml

- AntiVirus and Patch Management
- Database links
- Backup systems

Modern IT hacking

- Select a vulnerability from the list of ICS-CERT advisories
- Scan Internet to locate vulnerable devices
- Exploit



E. Leverett, R. Wightman. Vulnerability Inheritance in Programmable Logic Controllers (GreHack‘13)
D. Beresford. Exploiting Siemens Simatic S7 PLCs . Black Hat USA (2011)

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

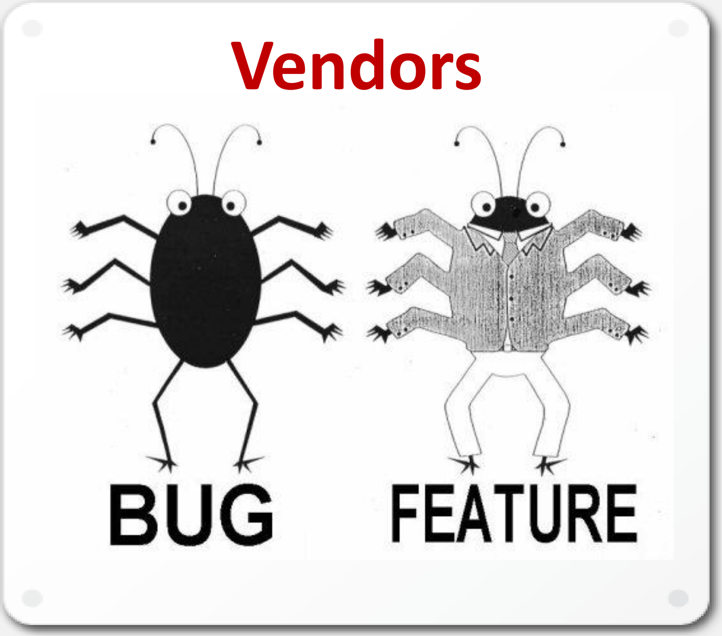
Sensor

Computational element

Instrumentation of the future

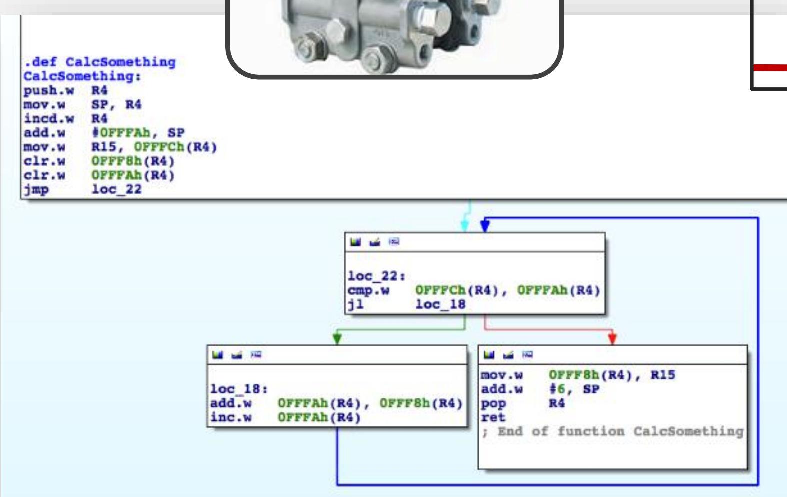
Promise from the vendors:

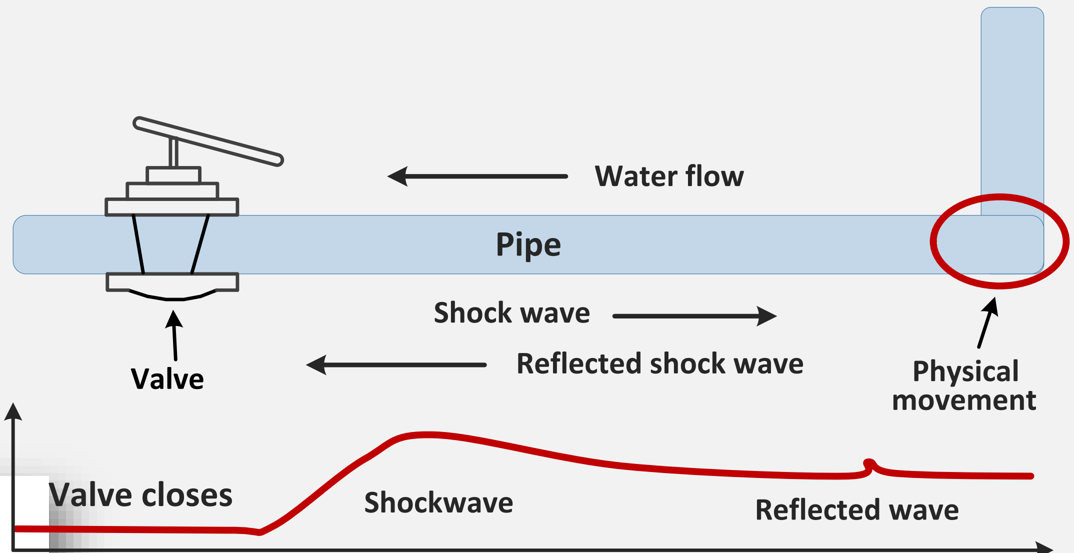
Expect instruments of the future to have multiple communication channels, each one with built-in security (LOL), much like a present-day Ethernet switch. These channels will be managed with IP adressing and server technology, **allowing the instrument to become a true data server**



Invading field devices

- Inserting rootkit into sensor's firmware





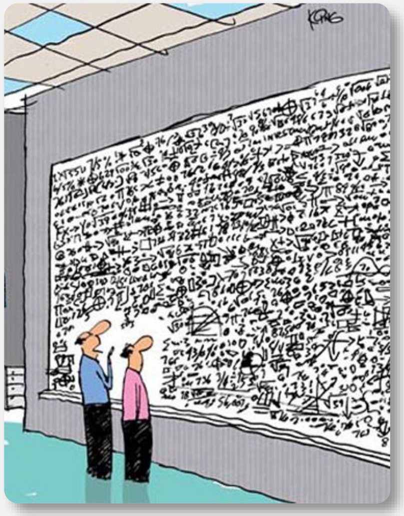
Attack scenario: pipe damage with water hammer effect

J. Larsen. Miniaturization. Black Hat USA (2014)

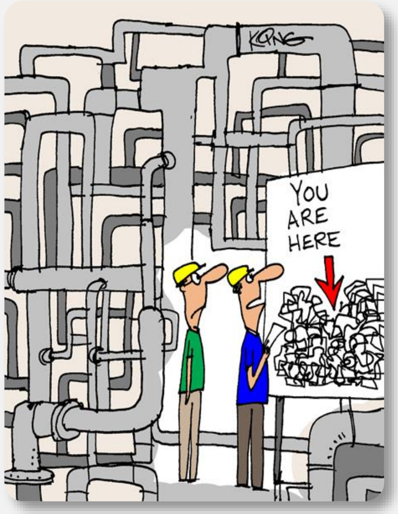
Discovery

Process discovery

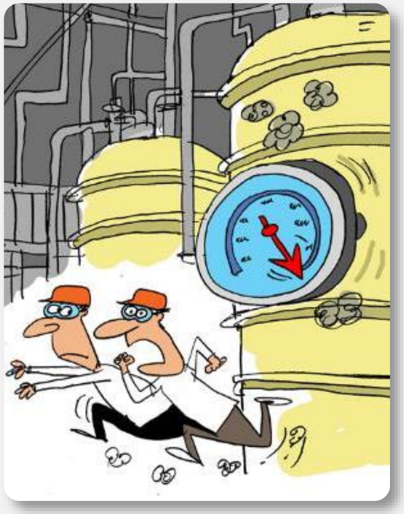
What and how the process is producing



How it is controlled



How it is build and wired



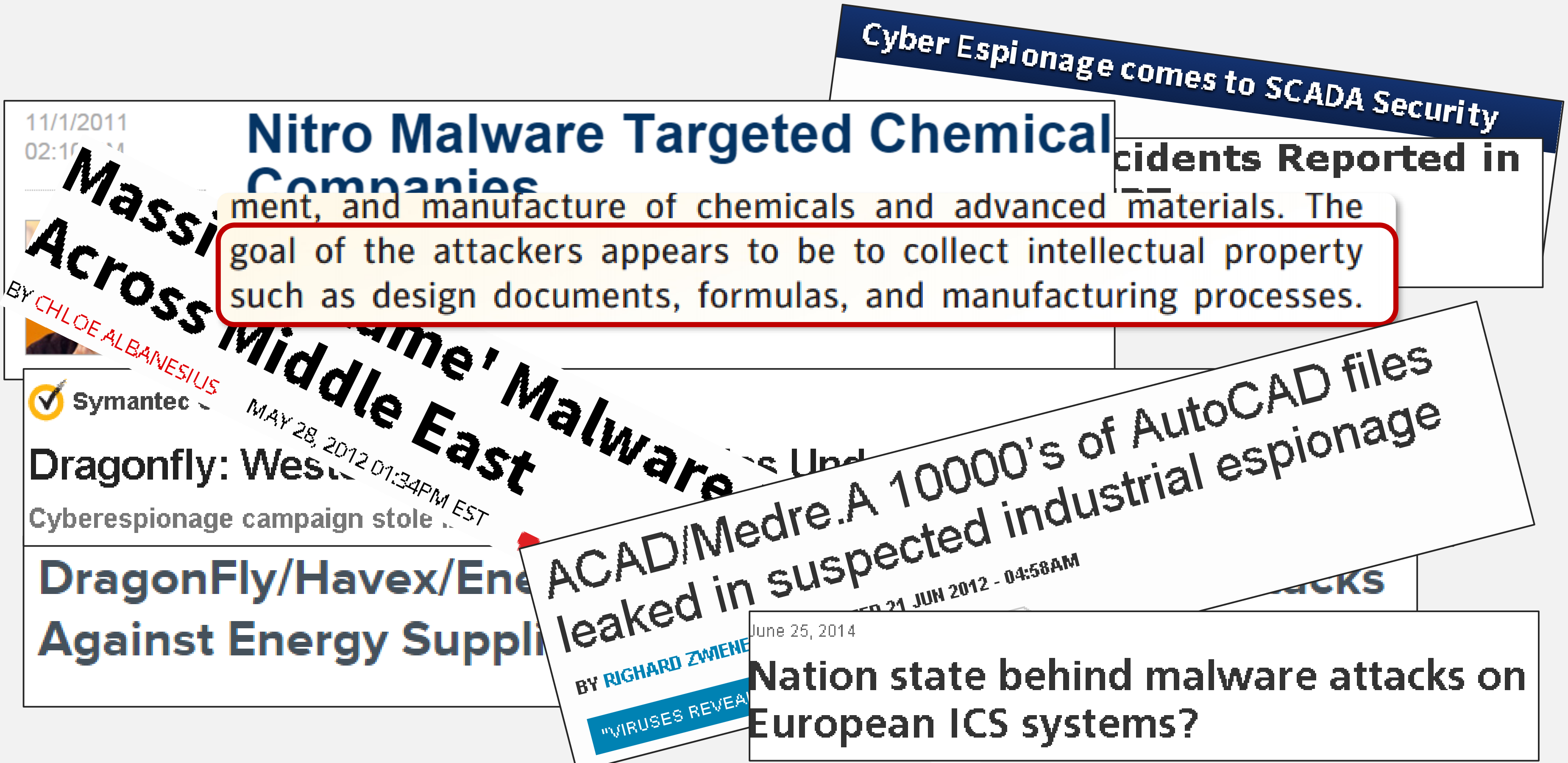
Operating and safety constraints

Espionage, reconnaissance

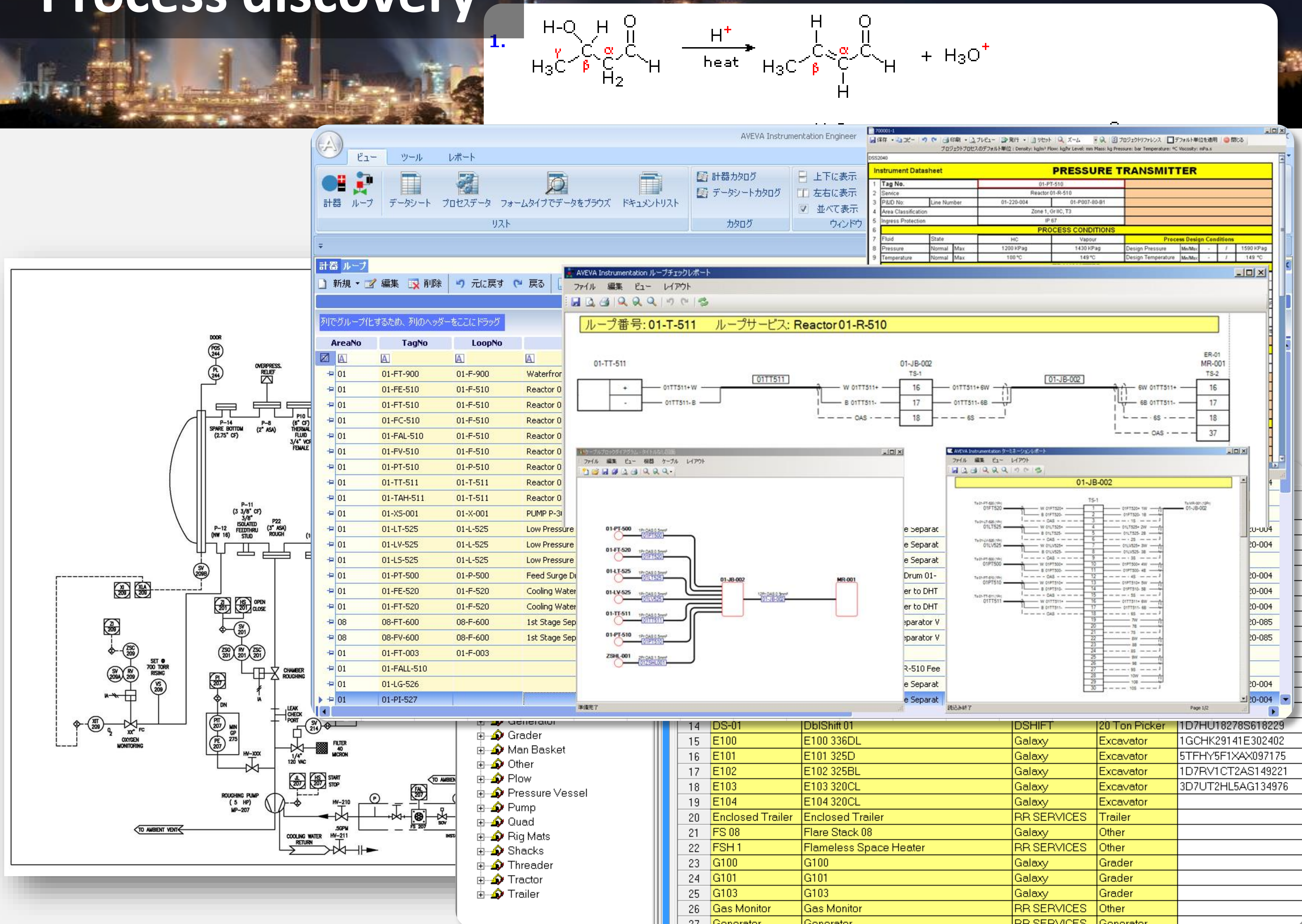
Target plant and third parties

Espionage

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

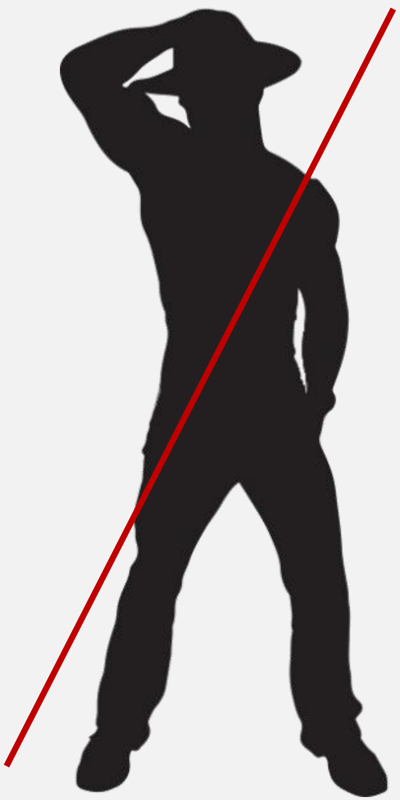


Process discovery



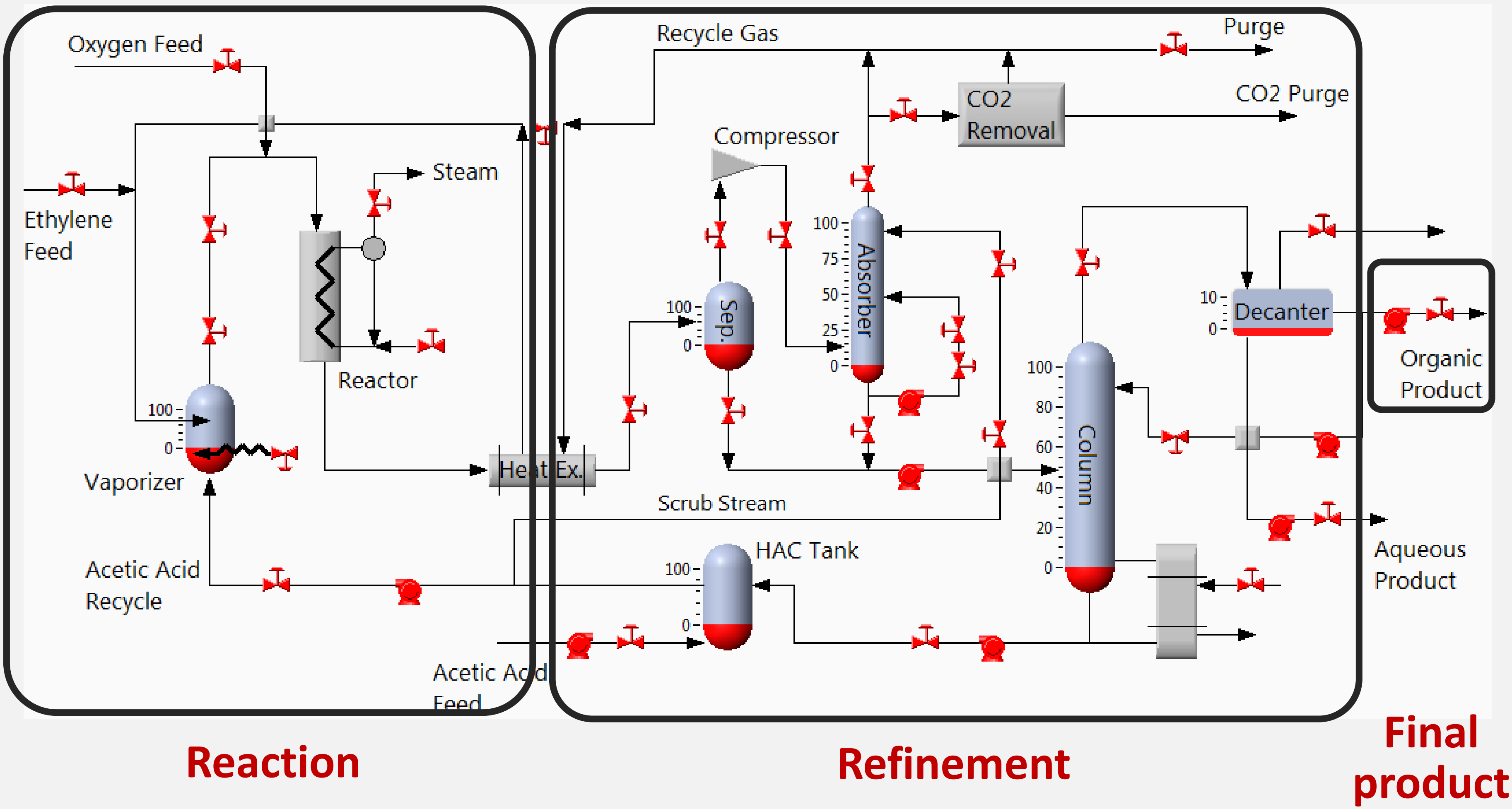
Know the equipment

Stripper is...



Stripping column

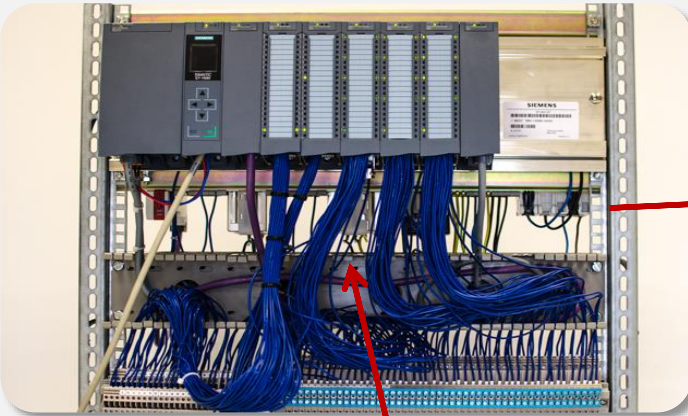
Max economic damage?



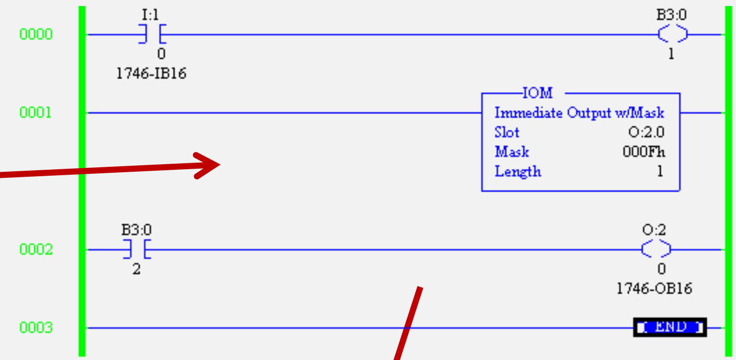
Requires input of subject matter experts

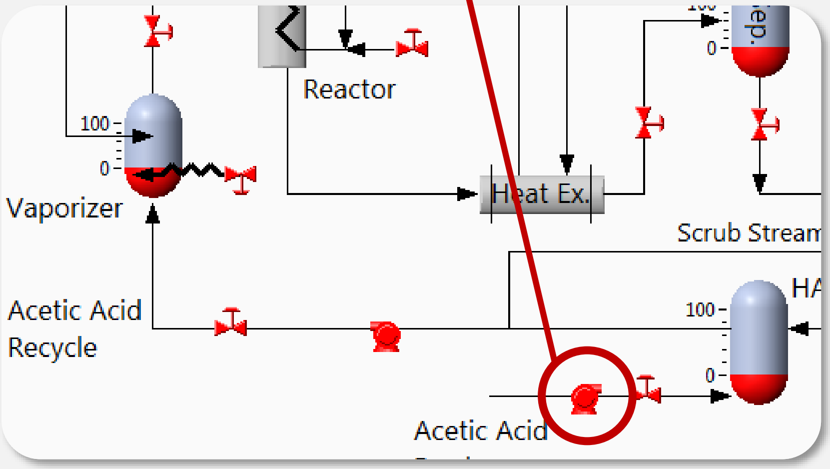
Understanding points and logic

Programmable Logic Controller

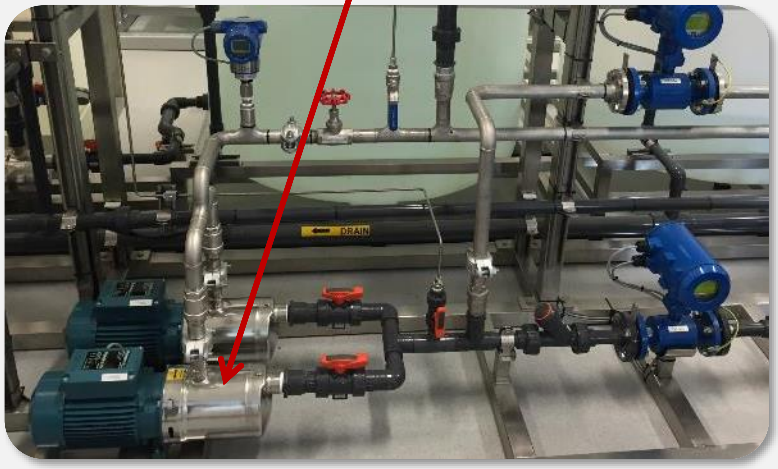


Ladder logic





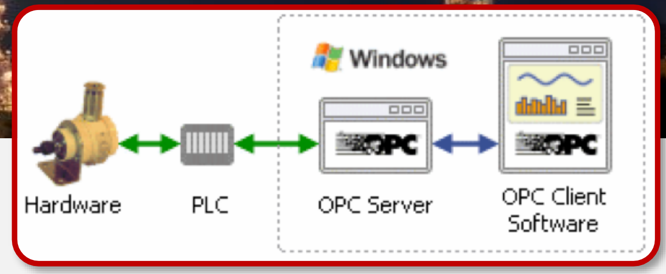
Piping and instrumentation diagram

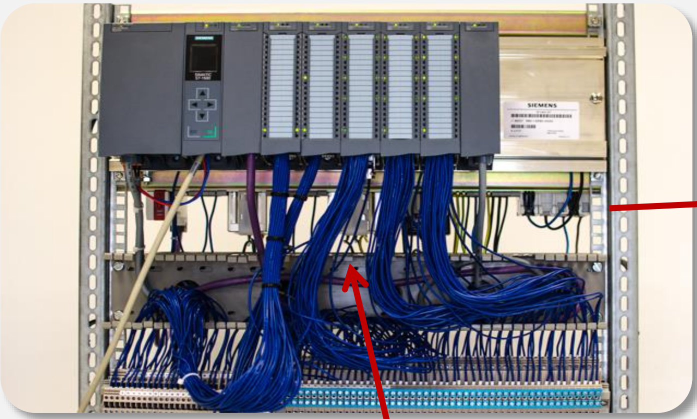


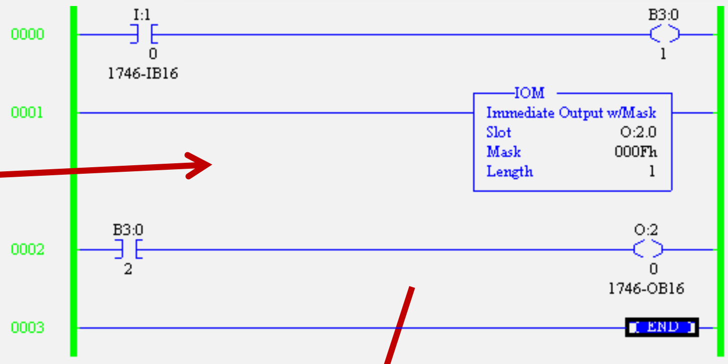
Pump in the plant

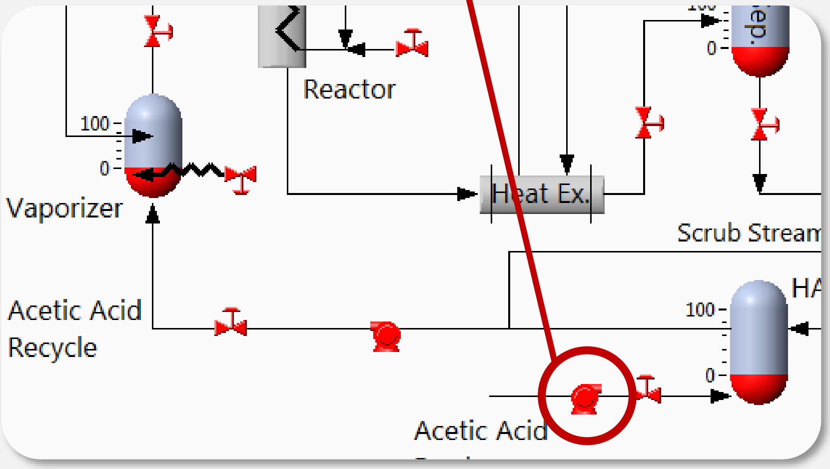
Understanding points and logic

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

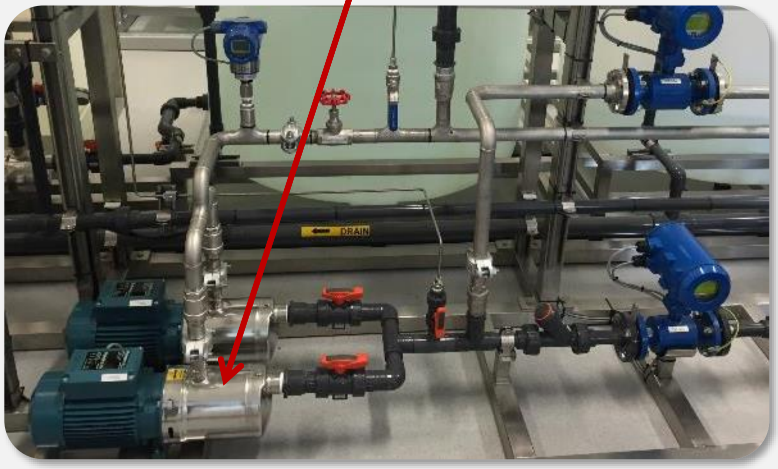






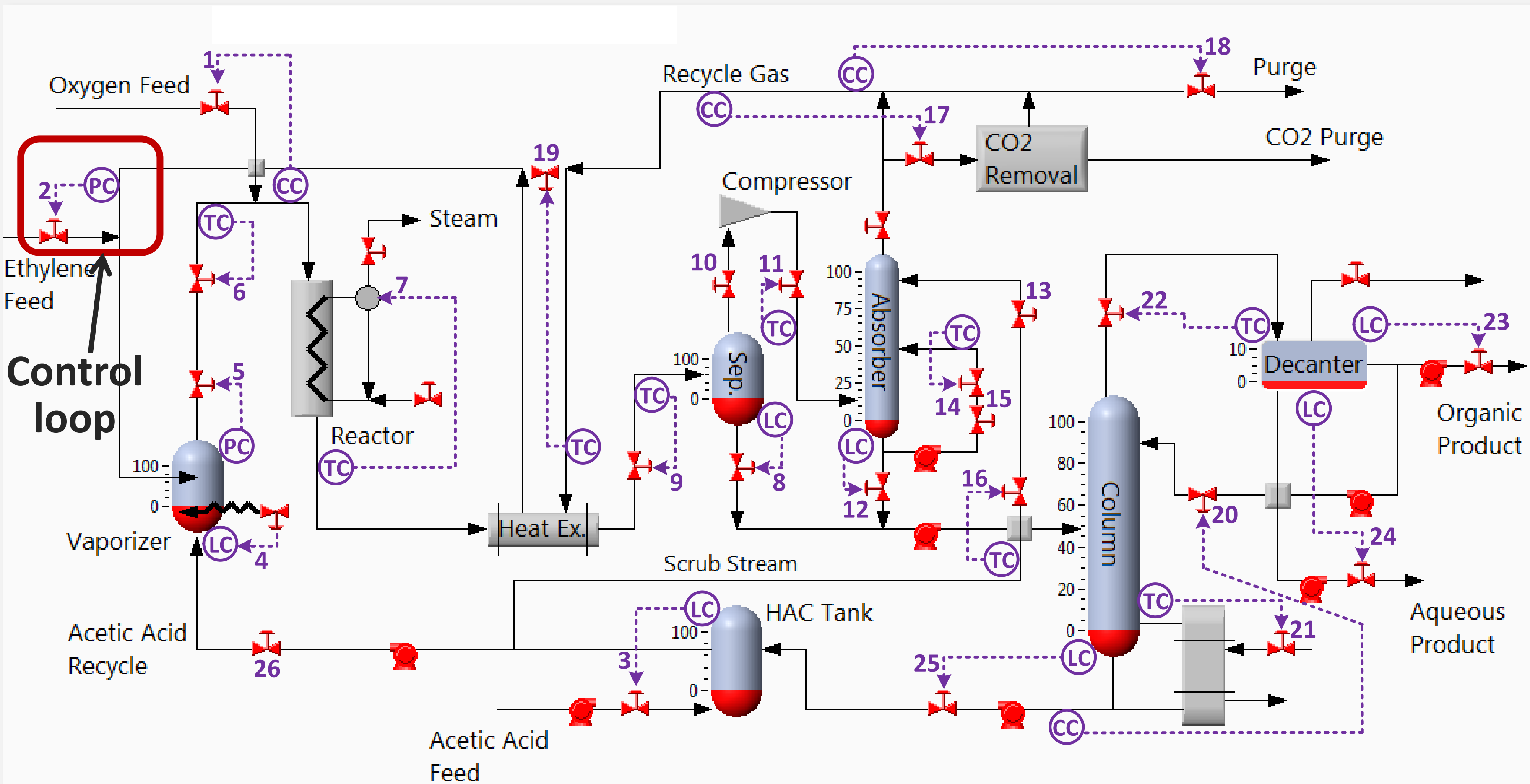


Piping and instrumentation diagram

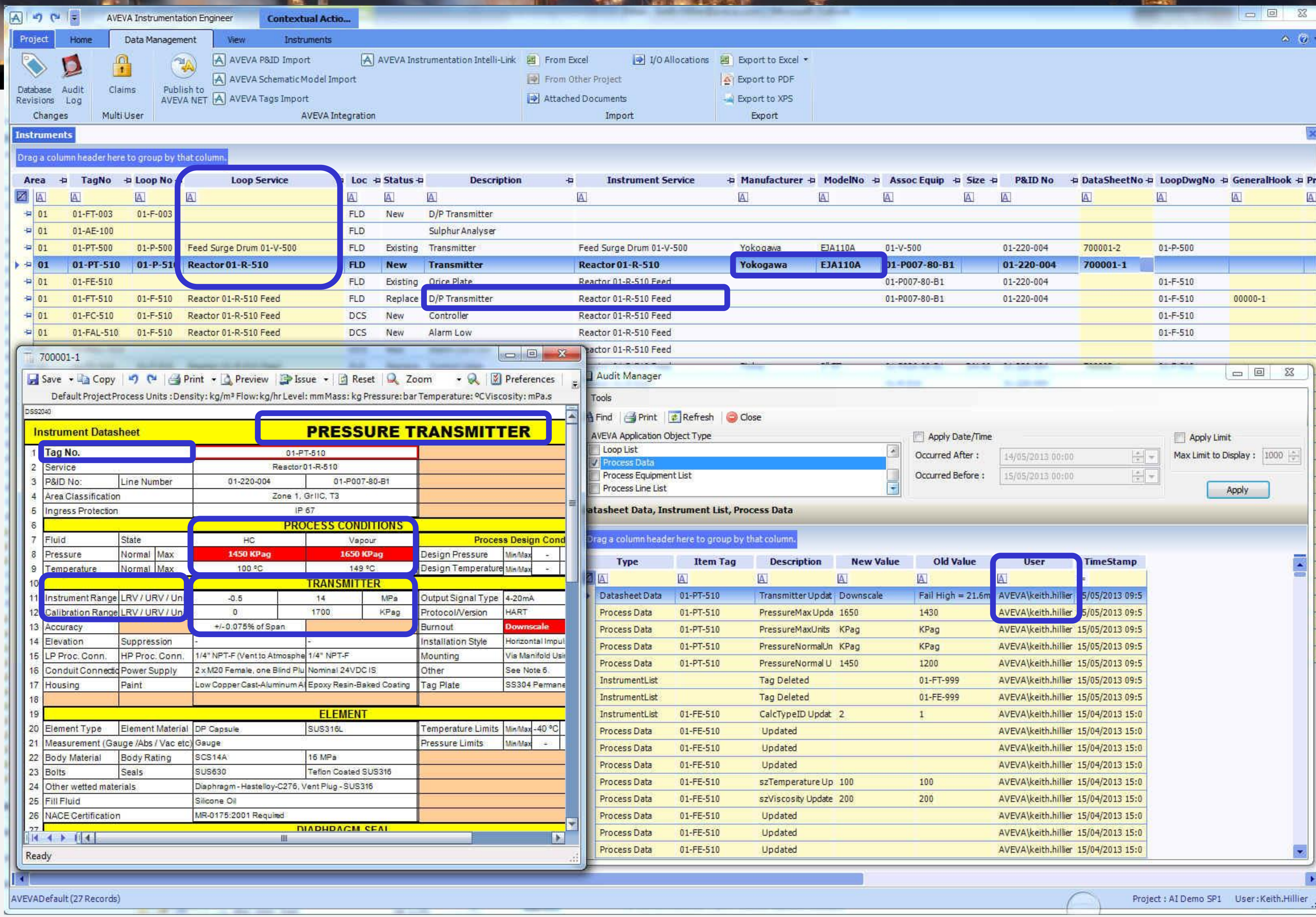


Pump in the plant

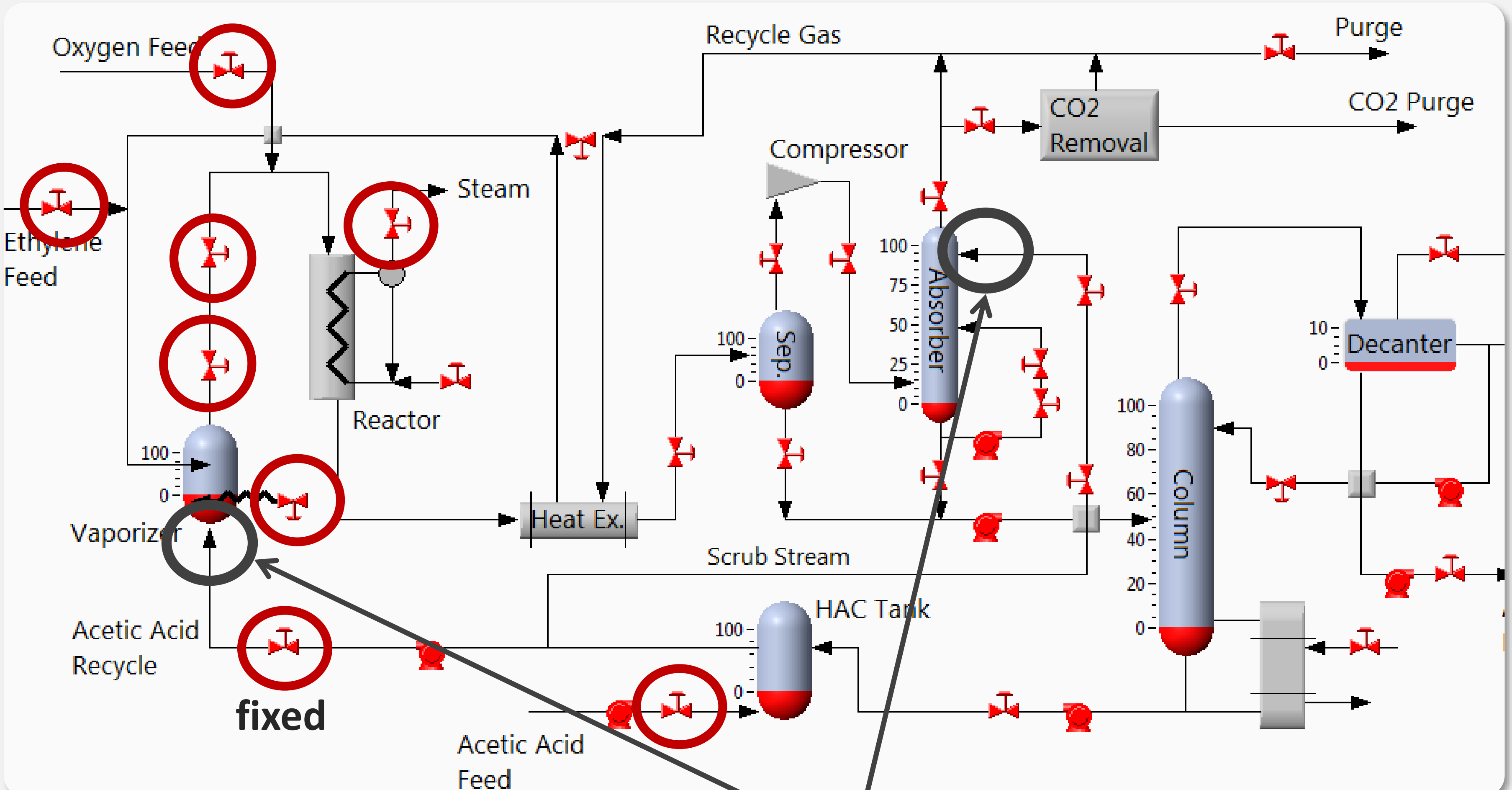
Understanding control structure



Control loop configuration

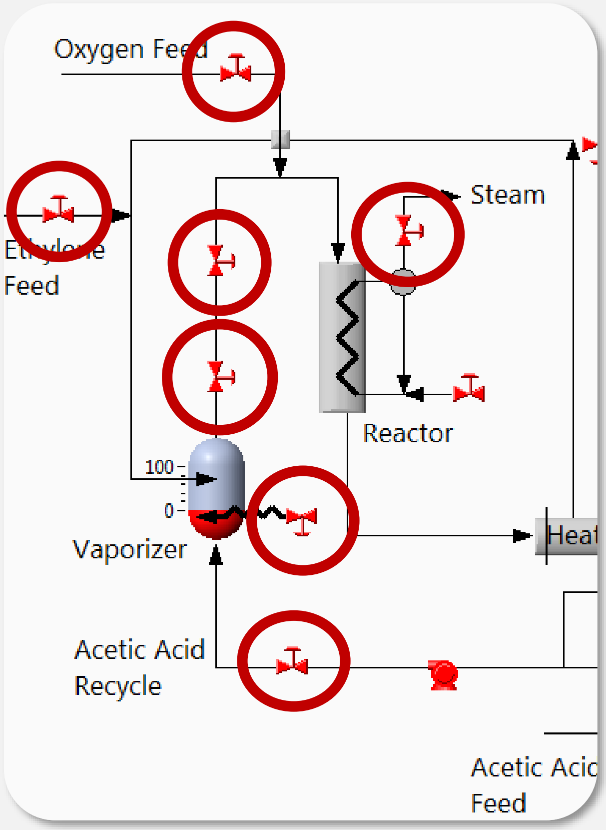


Watch the flows!



HAc flows into two sections. Not good :(

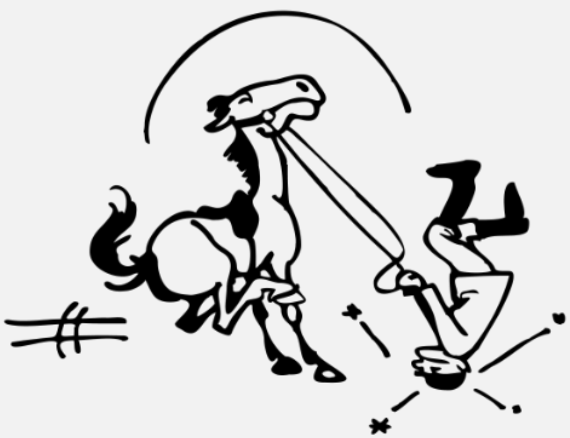
Obtaining control != being in control

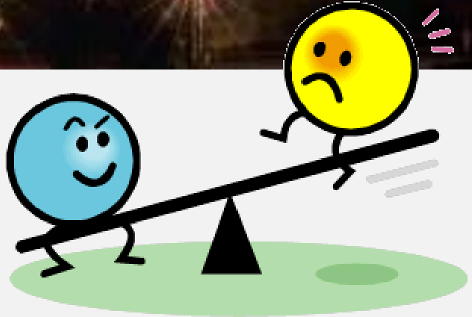


- Obtained controls might not be useful for attack goal
- How do I even speak to this thing??

  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 ???





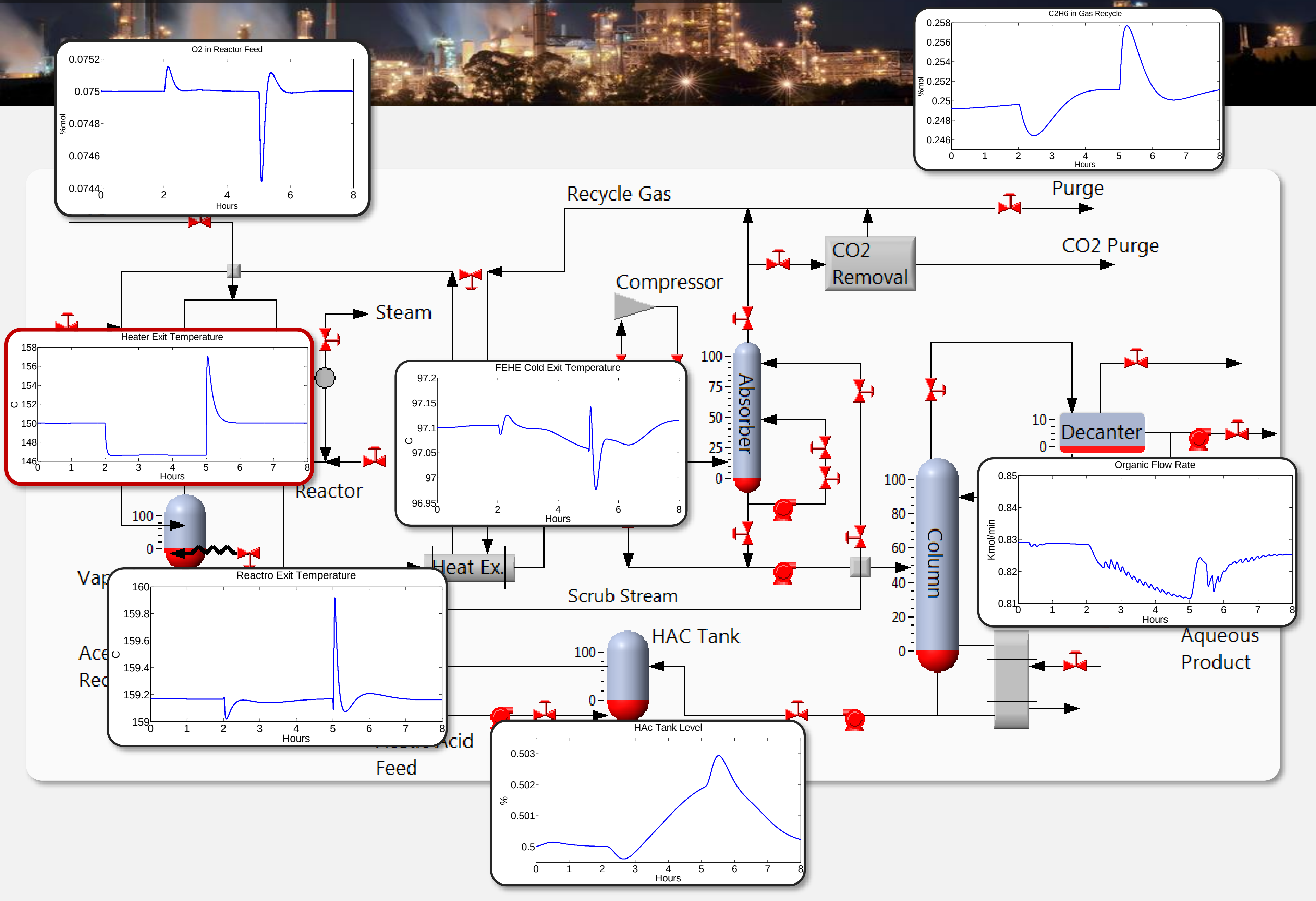
Control

Every action has a reaction

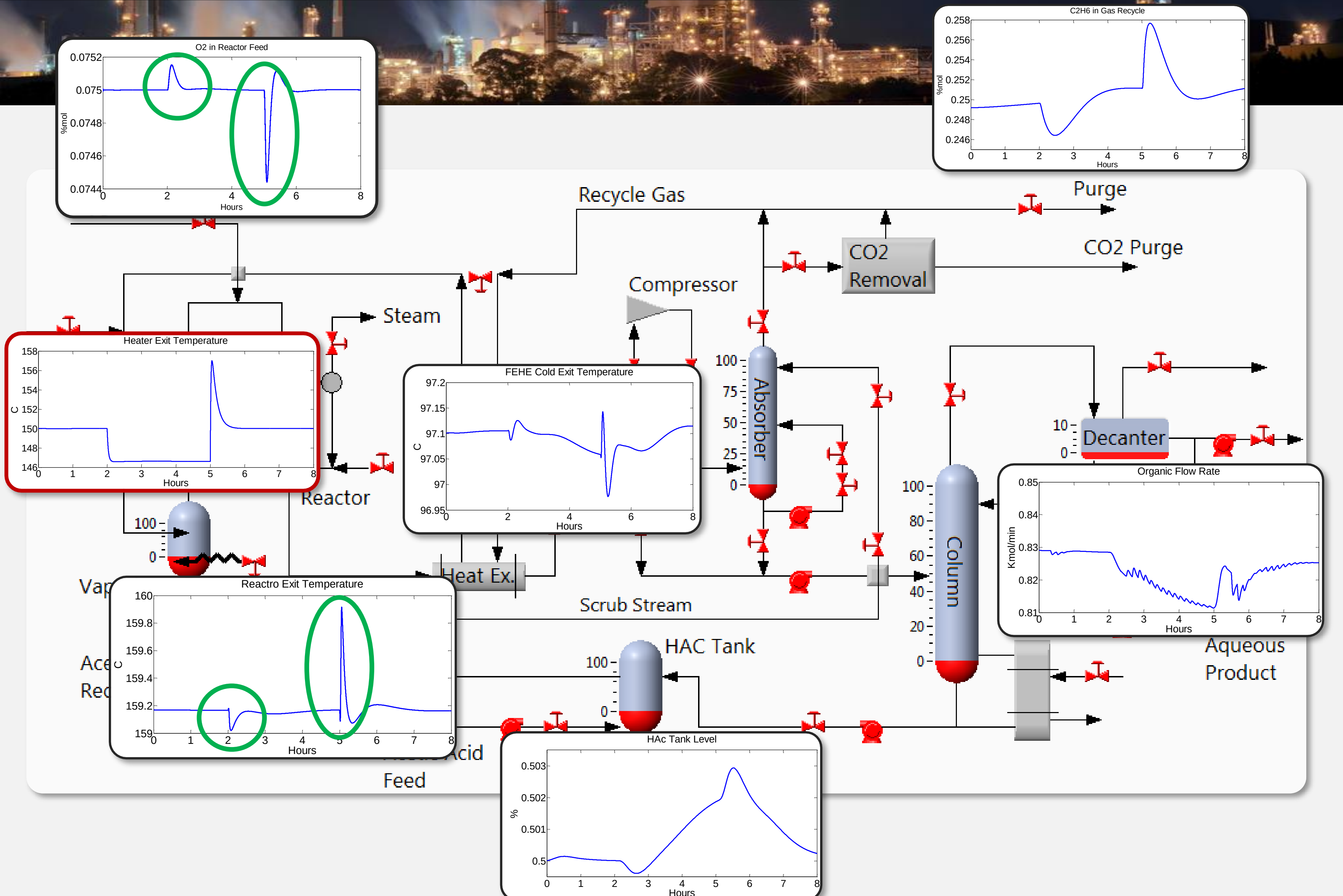
Physics of process control

- **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?

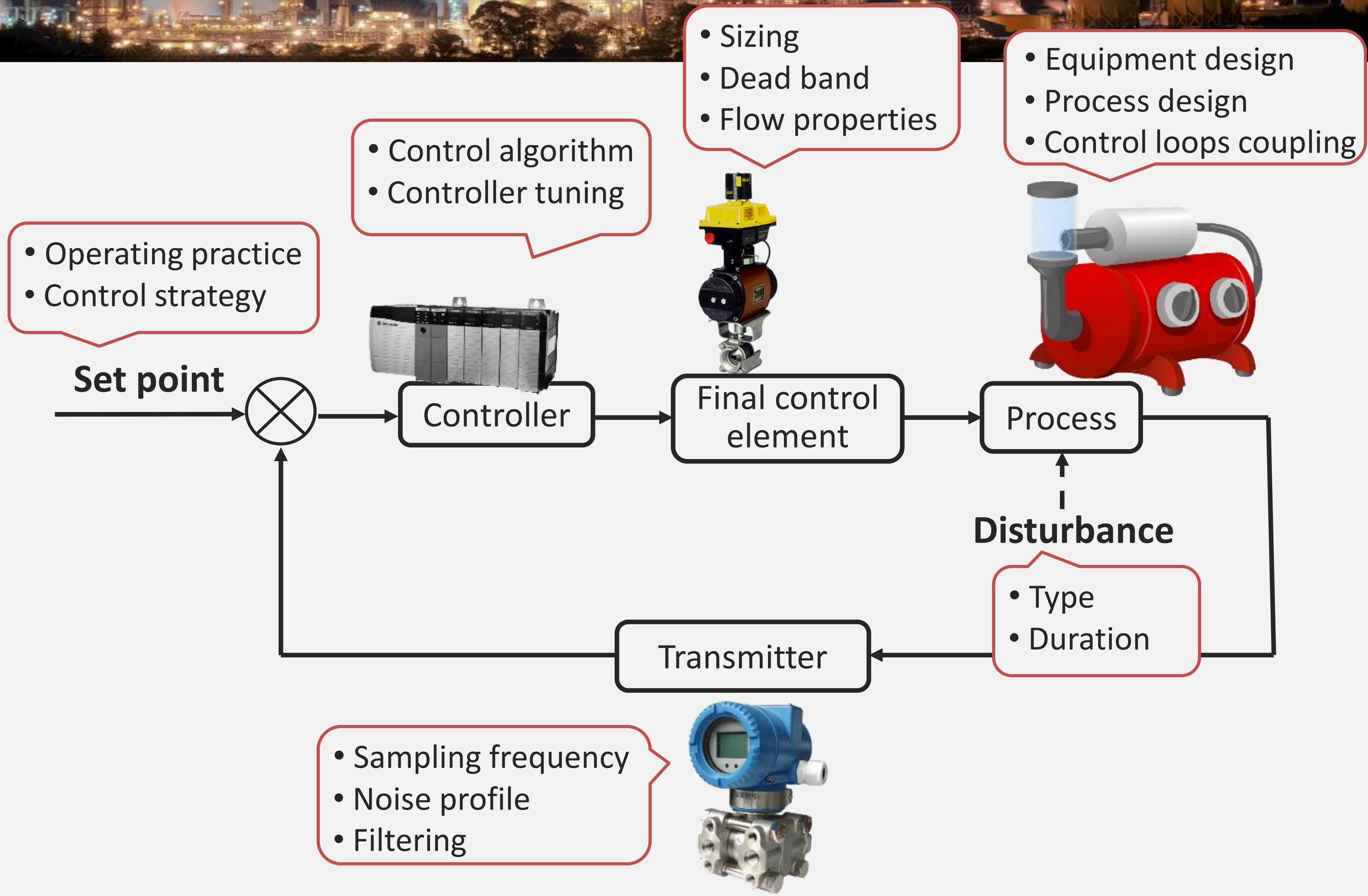
Process interdependencies



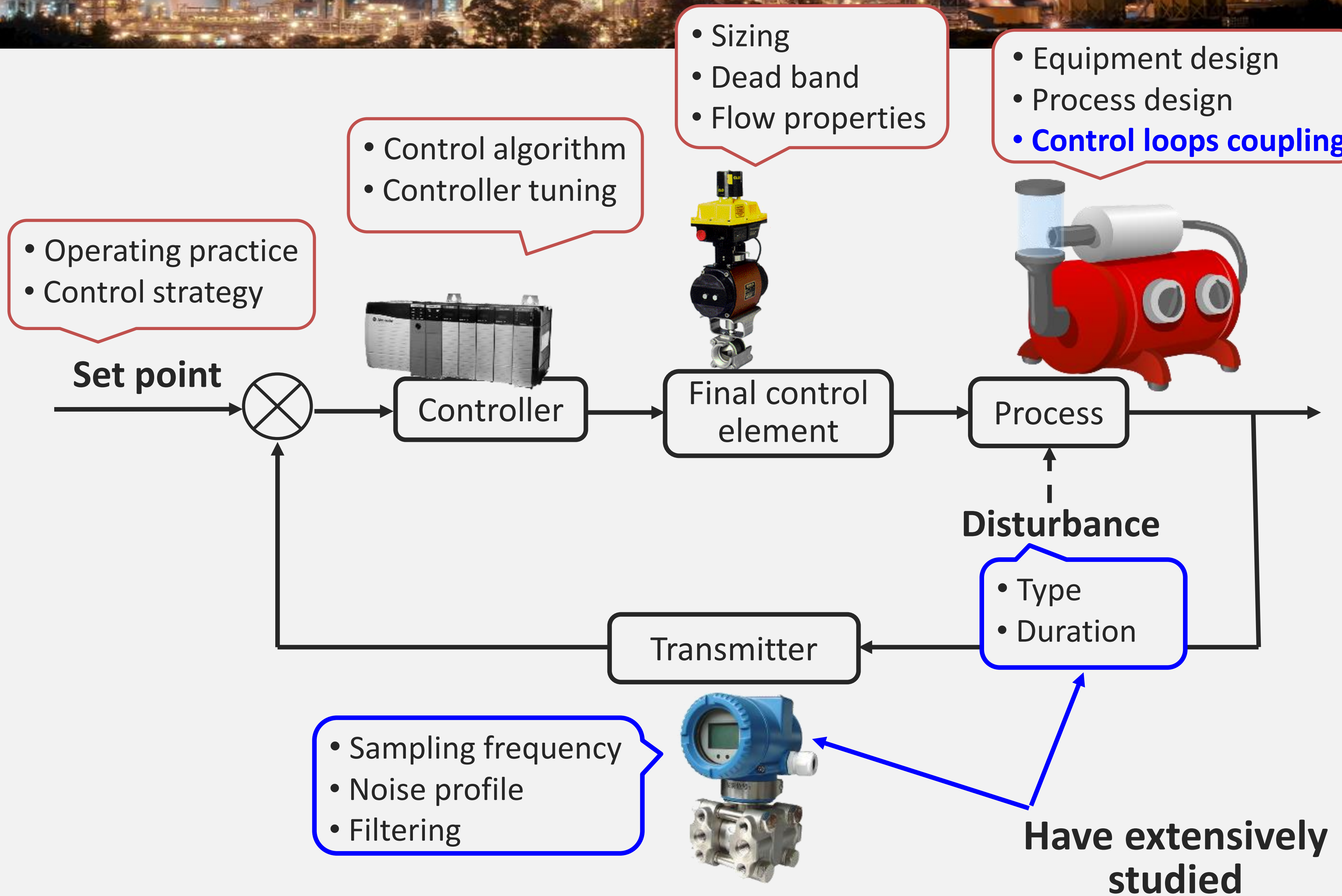
Process interdependencies



Understanding process response

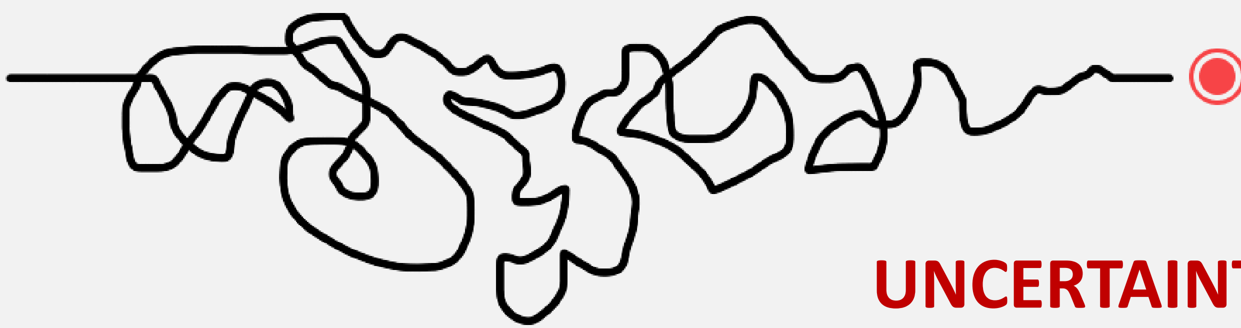


Understanding process response



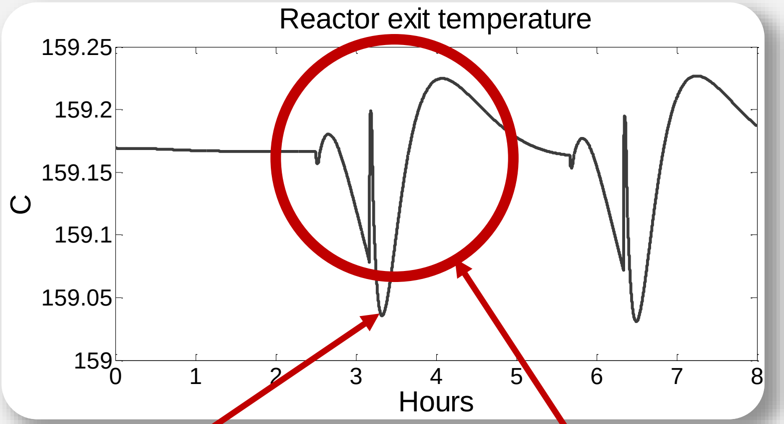
Process control challenges

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



UNCERTAINTY!

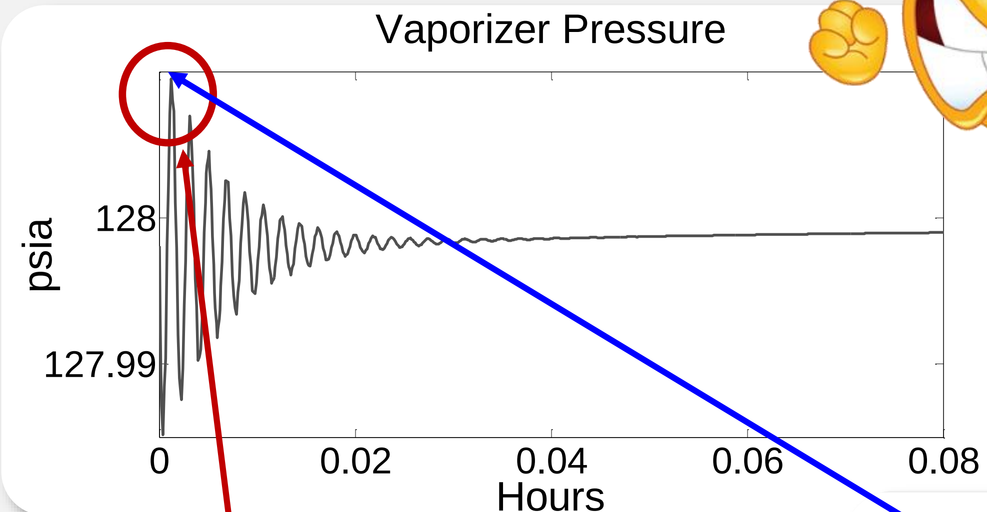
- Behavior of the process is known to the extent of its modelling
  - So to controllers. They cannot control the process beyond their control model



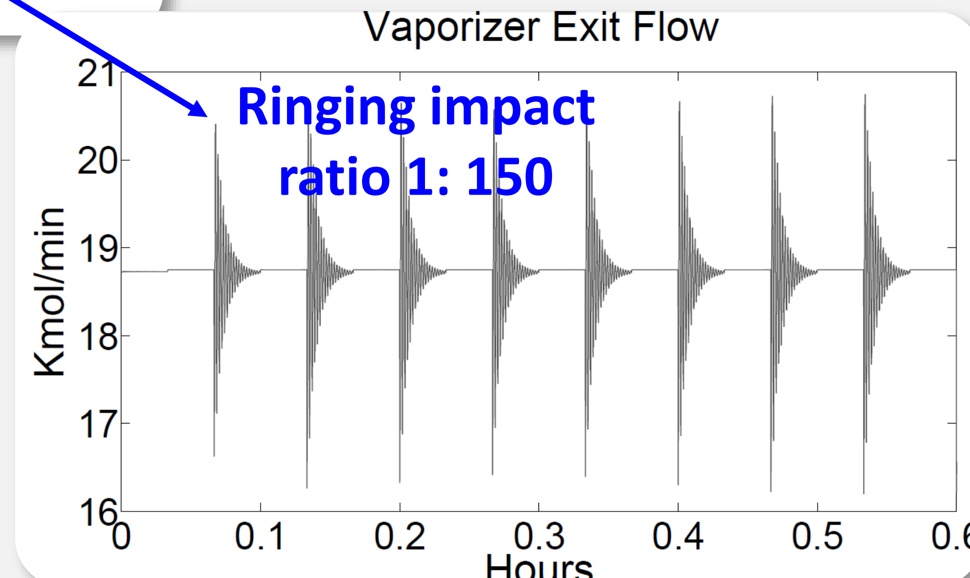
This triggers alarms

Non-liner response

Control loop ringing



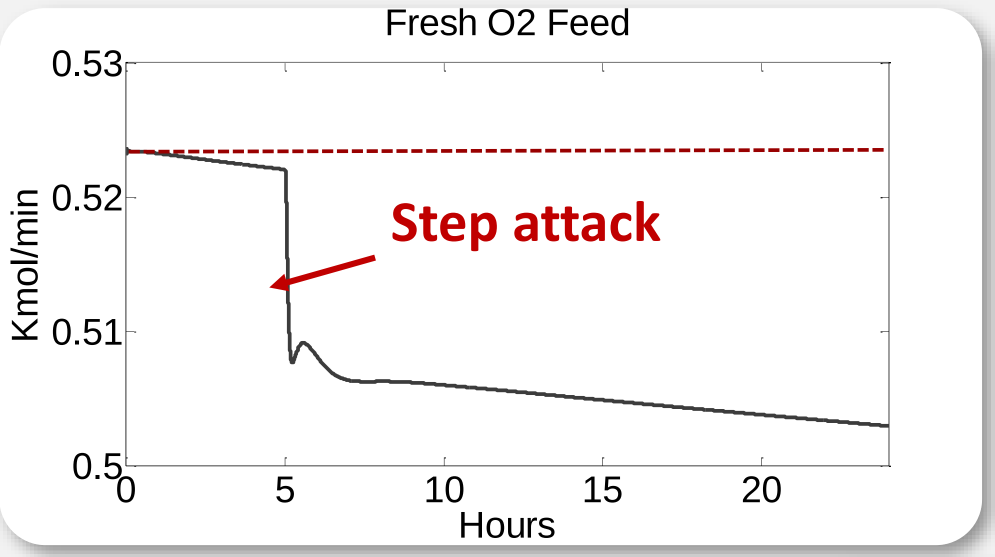
Amount of chemical entering the reactor



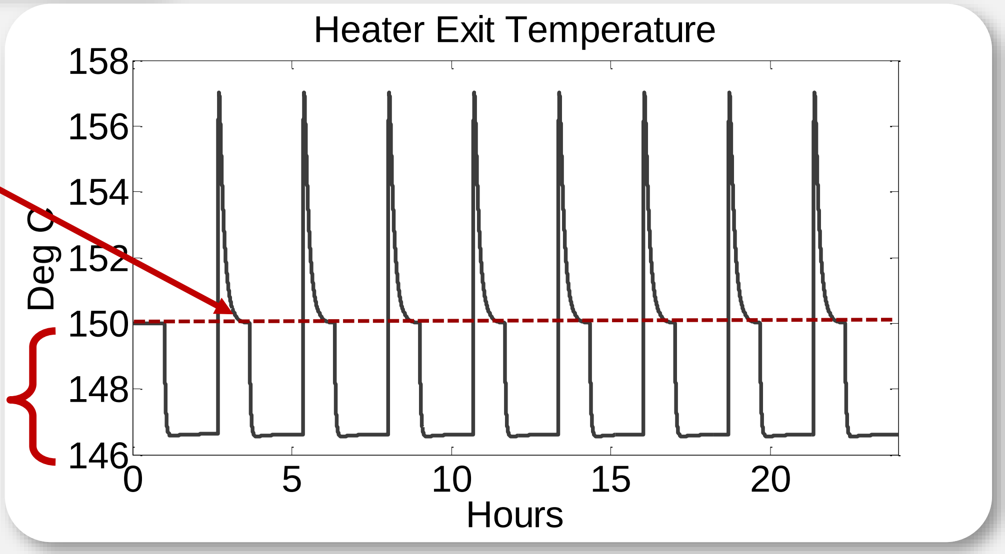
Caused by a negative real controller poles

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 <u>prevent response</u>

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

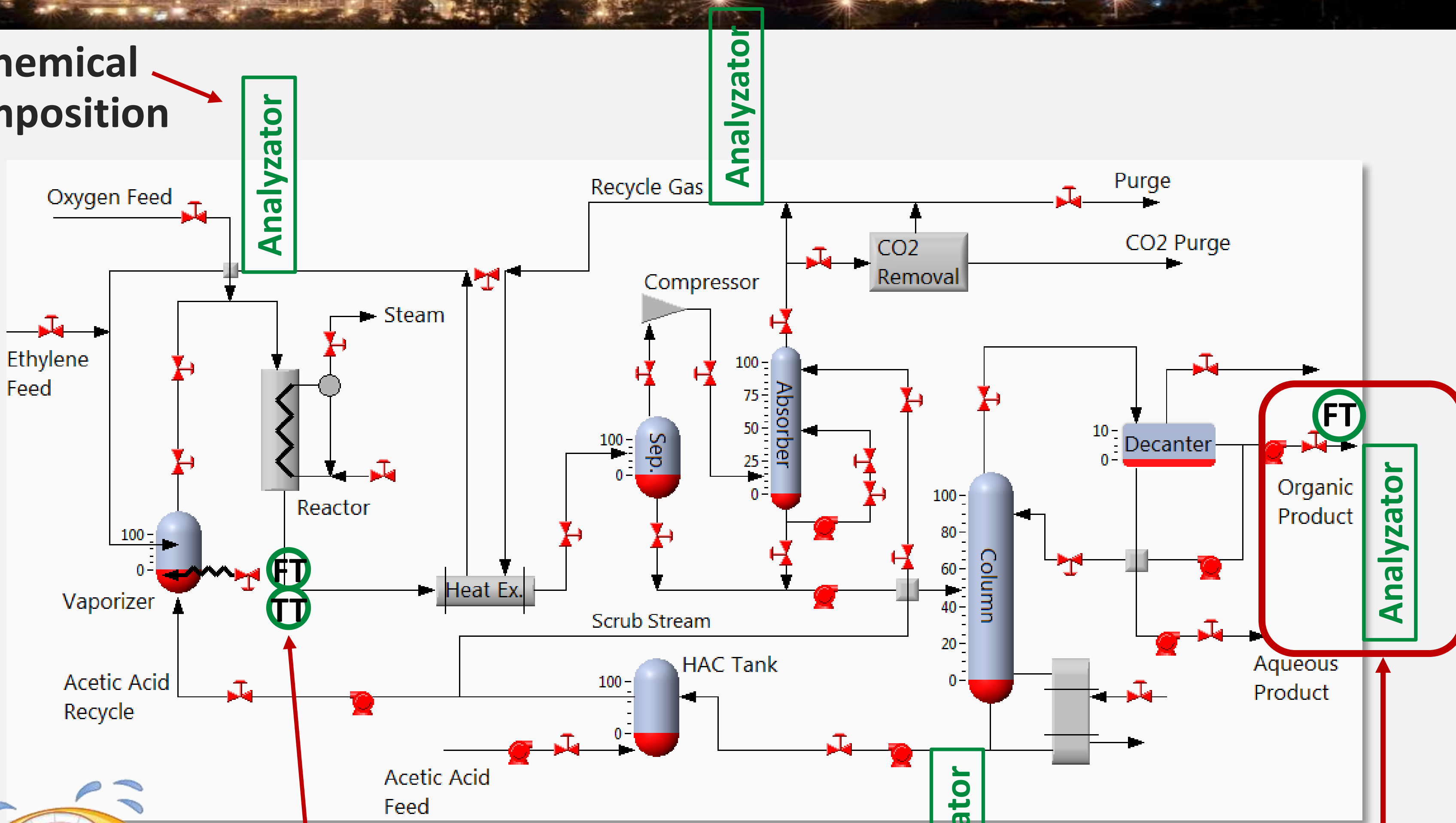
CSB OSHA

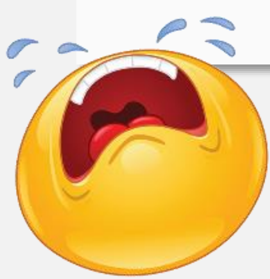
Hacker unfriendly process

- **Attacker need to <u>obtain feedback</u> 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
- <u>No analyzator</u>

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 loosing pressure last"

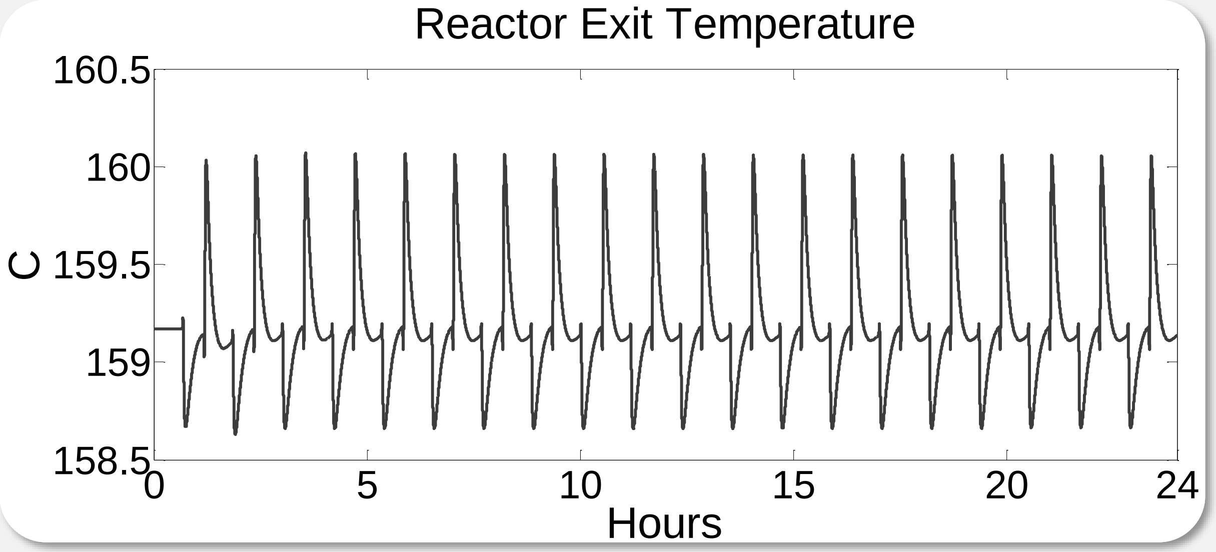
Engineer

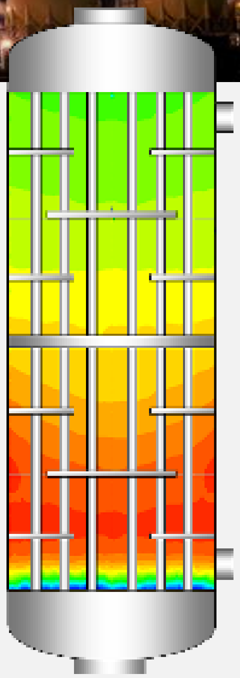
"It will be fully drained in 20.4 seconds and the pressure curve looks like this"

J. Larsen. SCADA triangles: Reloaded. S4 (2015)

Technician answer

Usage of proxy sensor

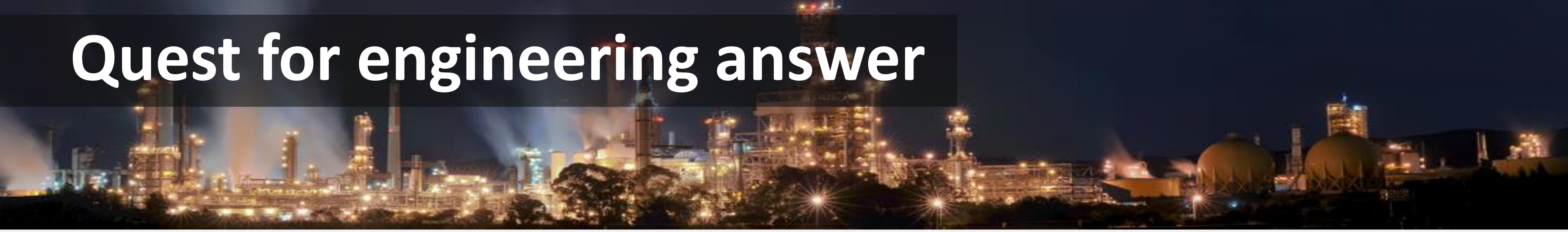




Reactor with cooling tubes

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

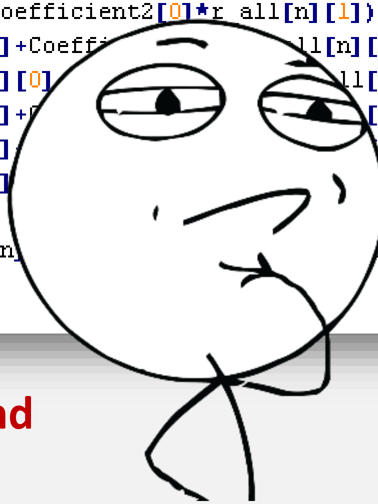
Quest for engineering answer



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

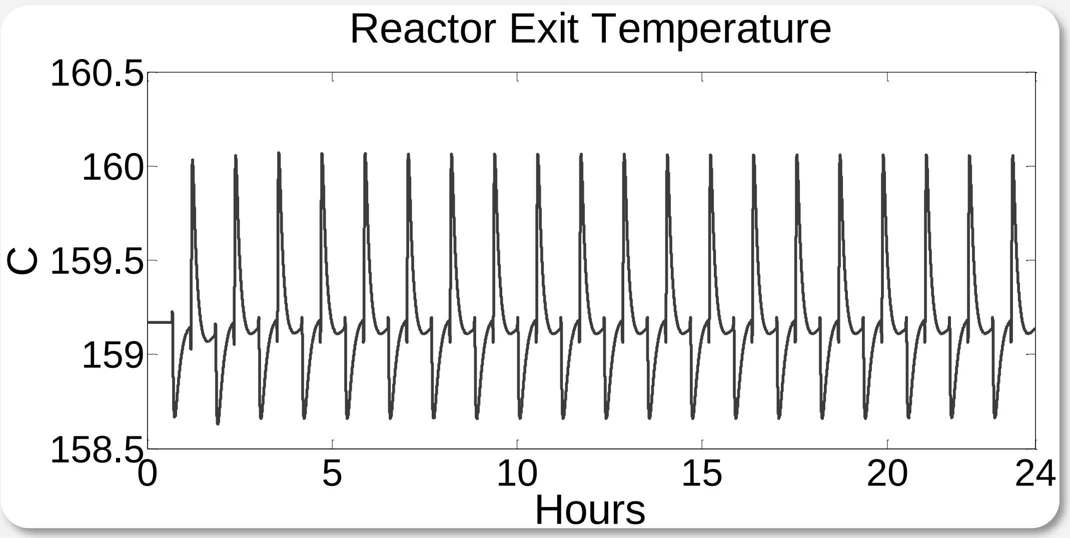
```
/*calculate derivatives*/
for (n=1;n<NR;n++)
{
    /*dC/dt=-delta(C*v)/deltaZ+sum(vij*rj)                     */
    /*Use single backward                                      */
    C_O2_t[n-1]=(-(C_O2[n]*v[n]-C_O2[n-1]*v[n-1])/dz + Coefficient1[0]*r_all[n][0]+Coefficient2[0]*r_all[n][1])/cata_porosity;
    C_CO2_t[n-1]=(-(C_CO2[n]*v[n]-C_CO2[n-1]*v[n-1])/dz + Coefficient1[1]*r_all[n][0]+Coeff   ll[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]   ll[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]+   [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]   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]   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   ll[n][0]*E_r1-r_all[
    n][1]*E_r2-Q_rct[n]);
};
```

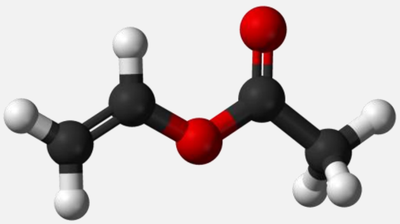
$$(\varepsilon\sum_{k=1}^{7} C_{i,k}Cp_{i,k} + \rho_b Cp_b)\frac{\partial T_i}{\partial t} = -\frac{\partial(\nu_i \sum_{k=1}^{7}(C_{i,k}Cp_{i,k})T_i)}{\partial z} - \phi_i\rho_b(r_{1,i}E_1 + r_{2,i}E_2) - Q_i^{RCT}$$



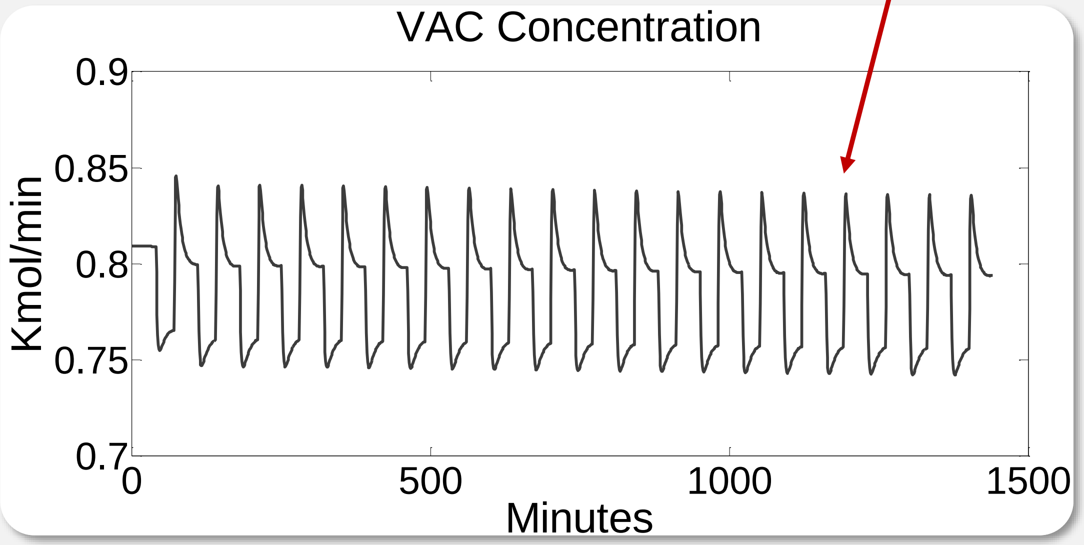
I found needed code but the numbers were very strange and did not seem being useful : 0,00073; 0,00016; 0,0007…

Engineering answer





Vinyl Acetate production

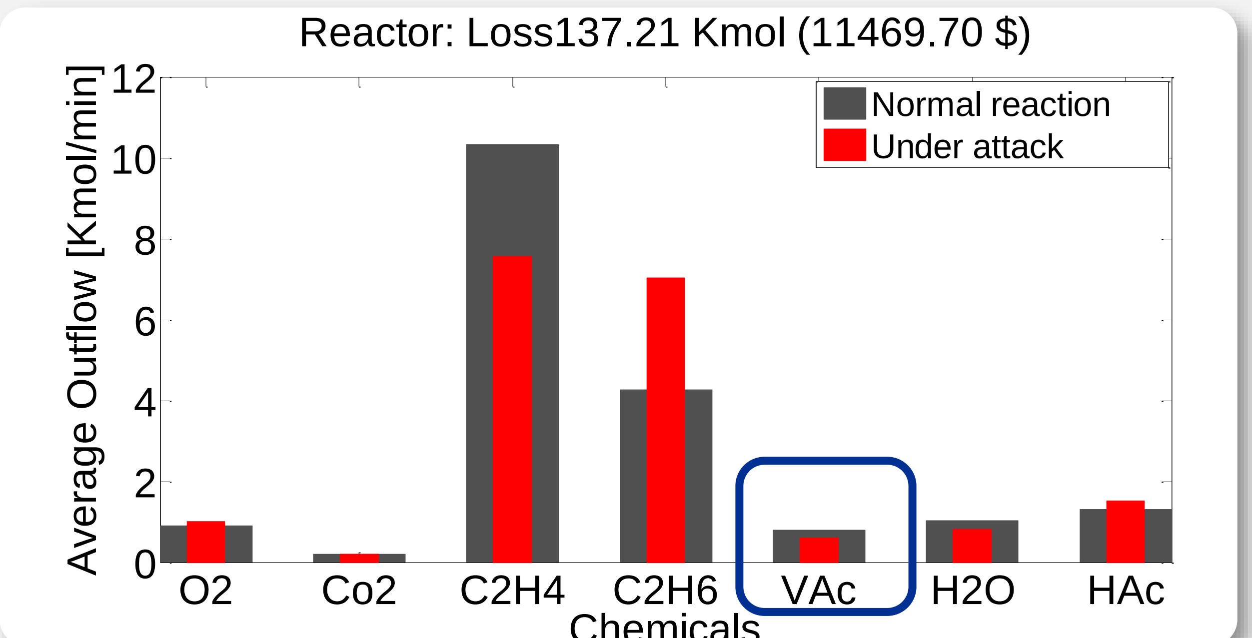


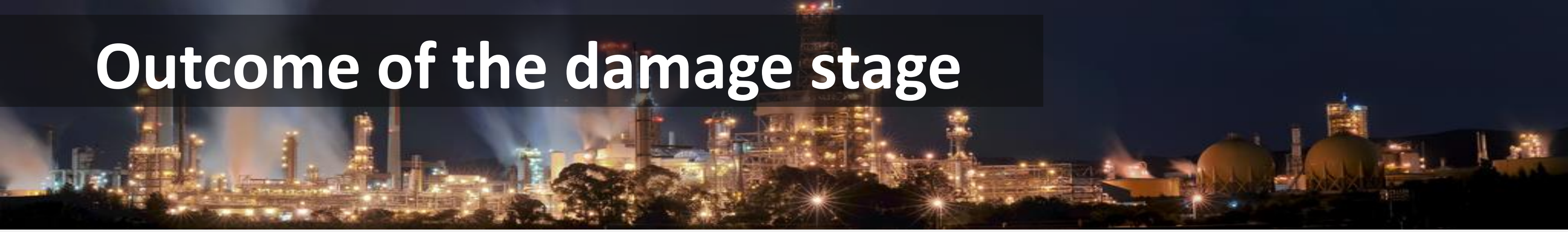
After two weeks of research and calculations, I finally got the numbers (YES!!)

Product loss

Product per day: 96.000$

Product loss per day: 11.469,70$





Outcome of the damage stage

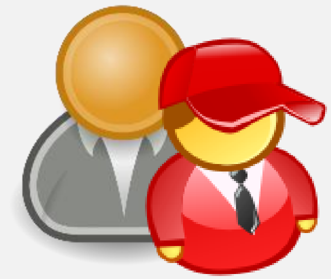
Product per day: 96.000$

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}

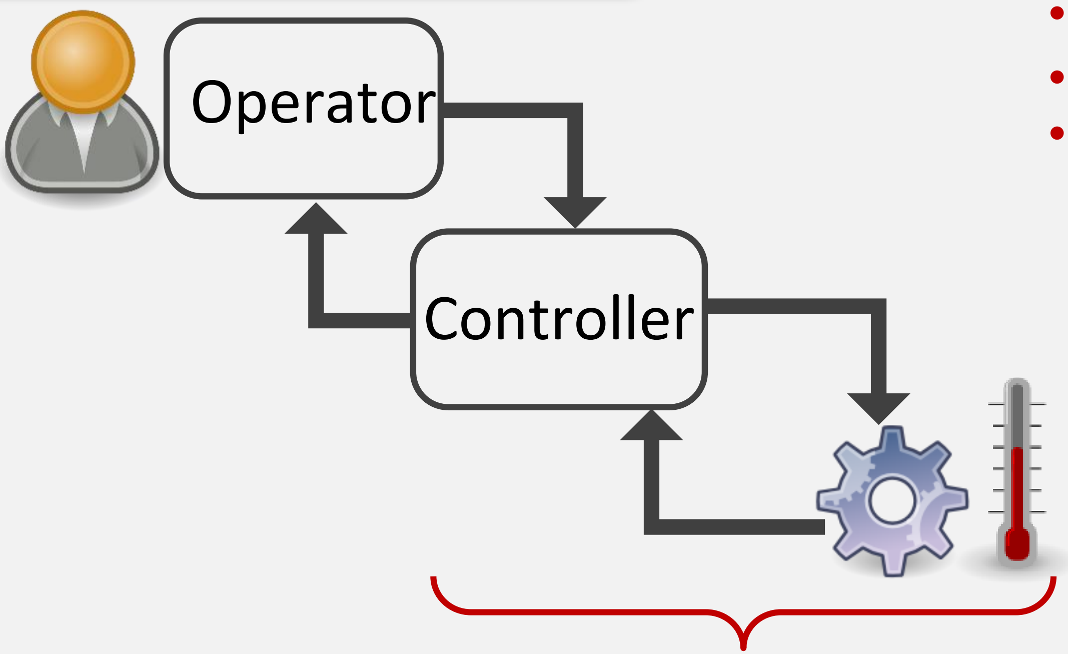
Still might be useful

Cleanup

Socio-technical system



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



Cyber-physical system

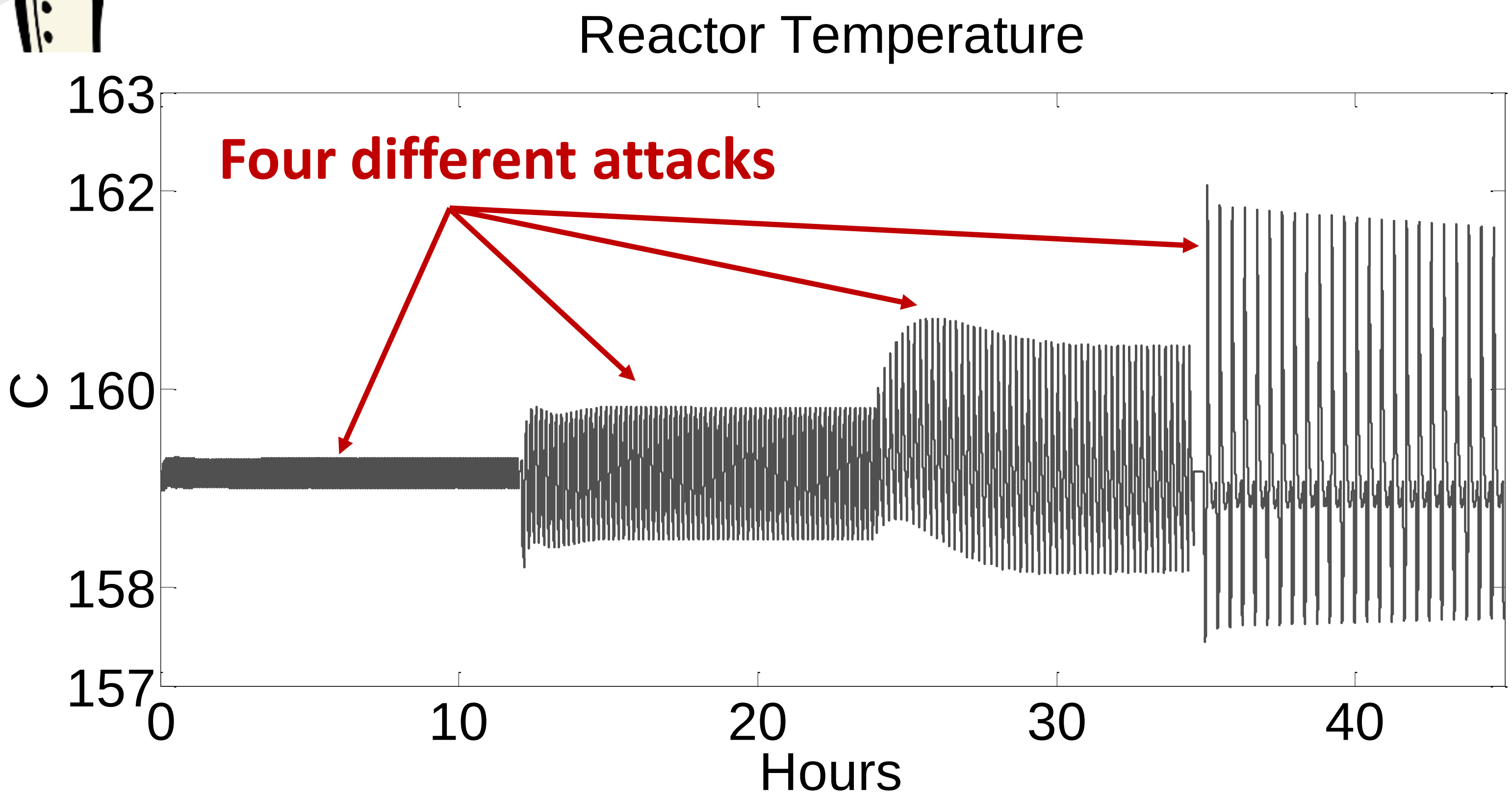
Creating forensics footprint

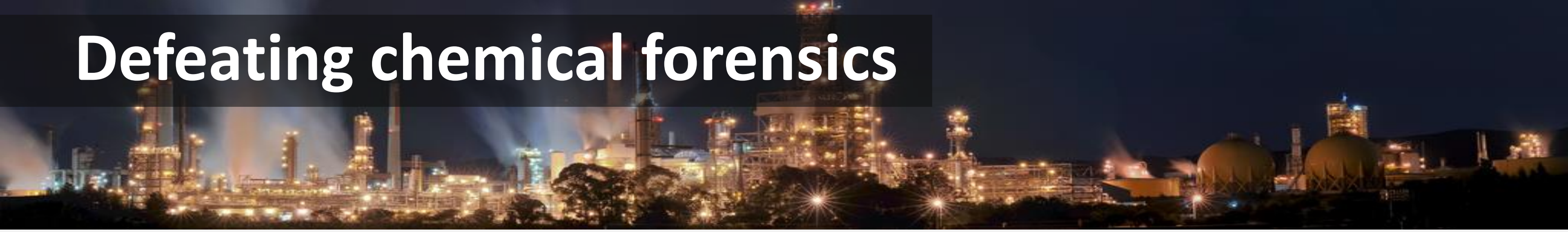
- Process operators may get concerned after noticing persistent decrease in production and may try to fix the problem
  - What do you want operators to think is causing process upset?
- If attacks are timed to a particular employee shift or maintenance work, plant employee will be investigated rather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

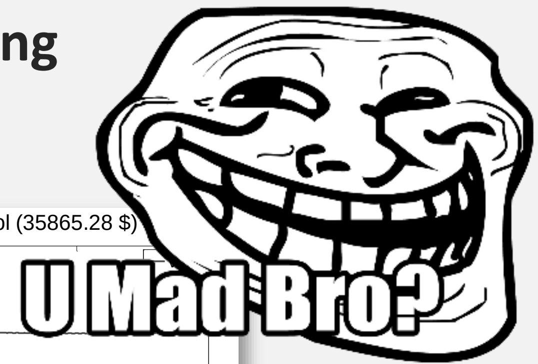
Creating forensics footprint

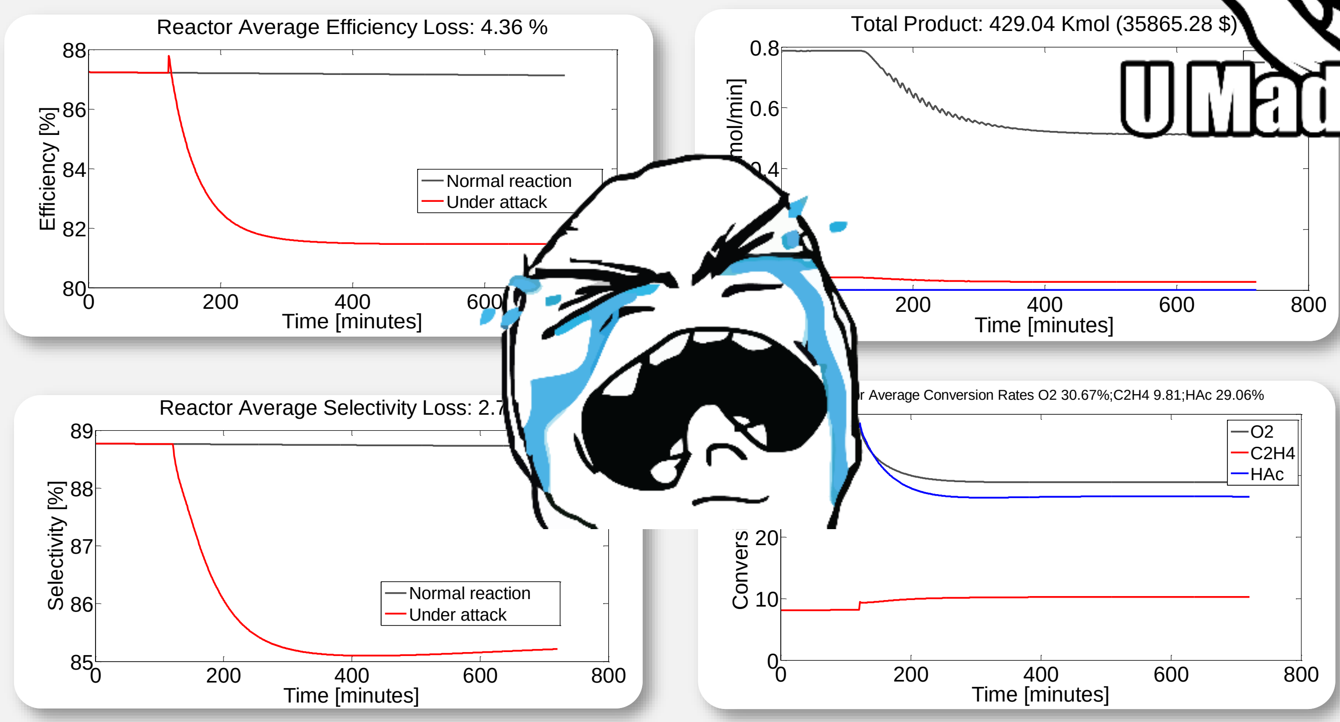


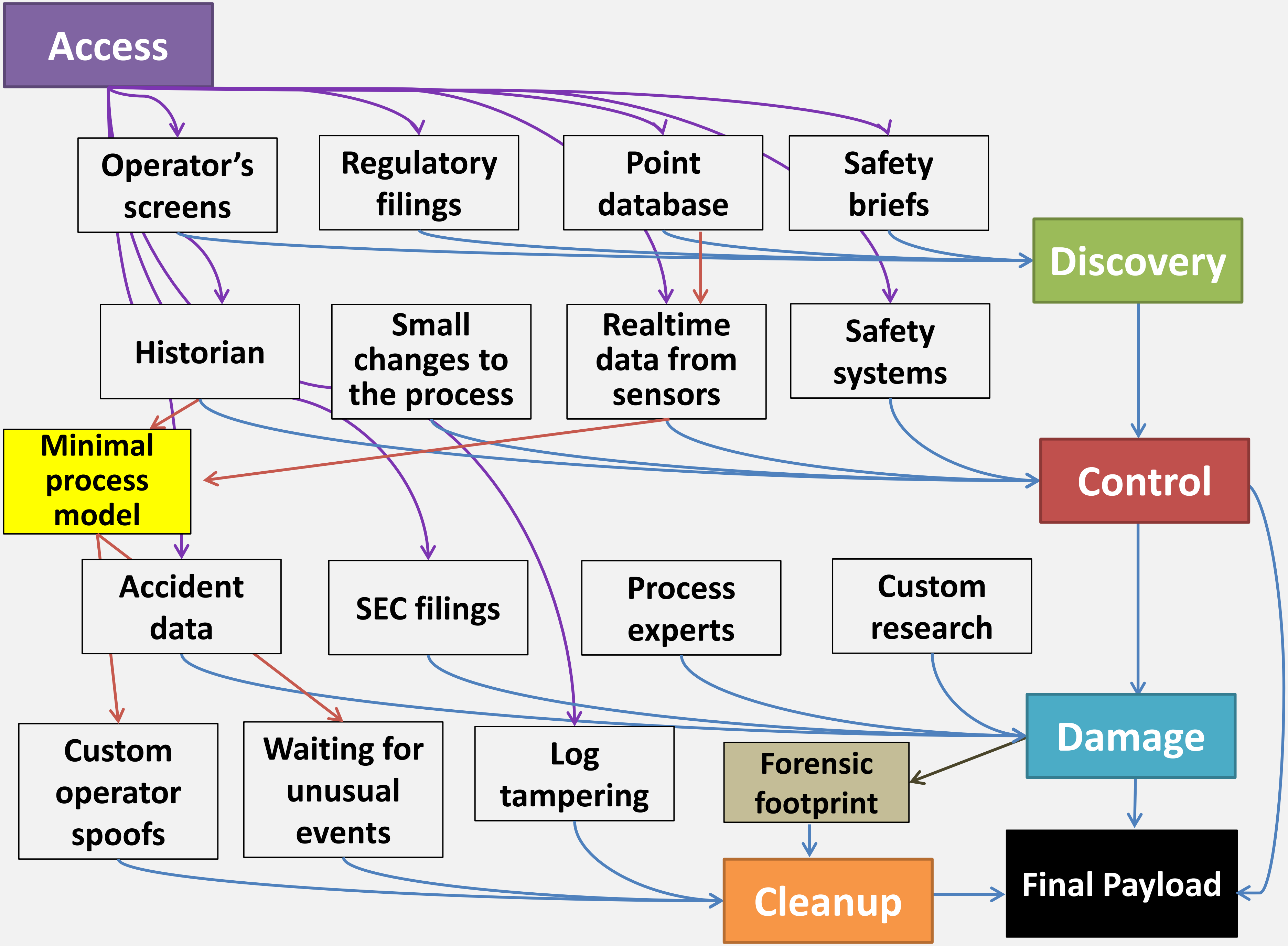


Defeating chemical forensics

- 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**







Access
Operator's screens
Regulatory filings
Point database
Safety briefs
Discovery
Historian
Small changes to the process
Realtime data from sensors
Safety systems
Minimal process model
Control
Accident data
SEC filings
Process experts
Custom research
Custom operator spoofs
Waiting for unusual events
Log tampering
Forensic footprint
Damage
Cleanup
Final Payload

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