

Rocking the Pocket Book: Hacking Chemical Plants for Competition and Extortion

Marina Krotofil, Jason Larsen



DefCon 23, Las Vegas, USA
07.08.2015

Who we are





(Ex)Academic

Got hooked on cyber-physical hacking



Hacker

Dragged into academic world against own will

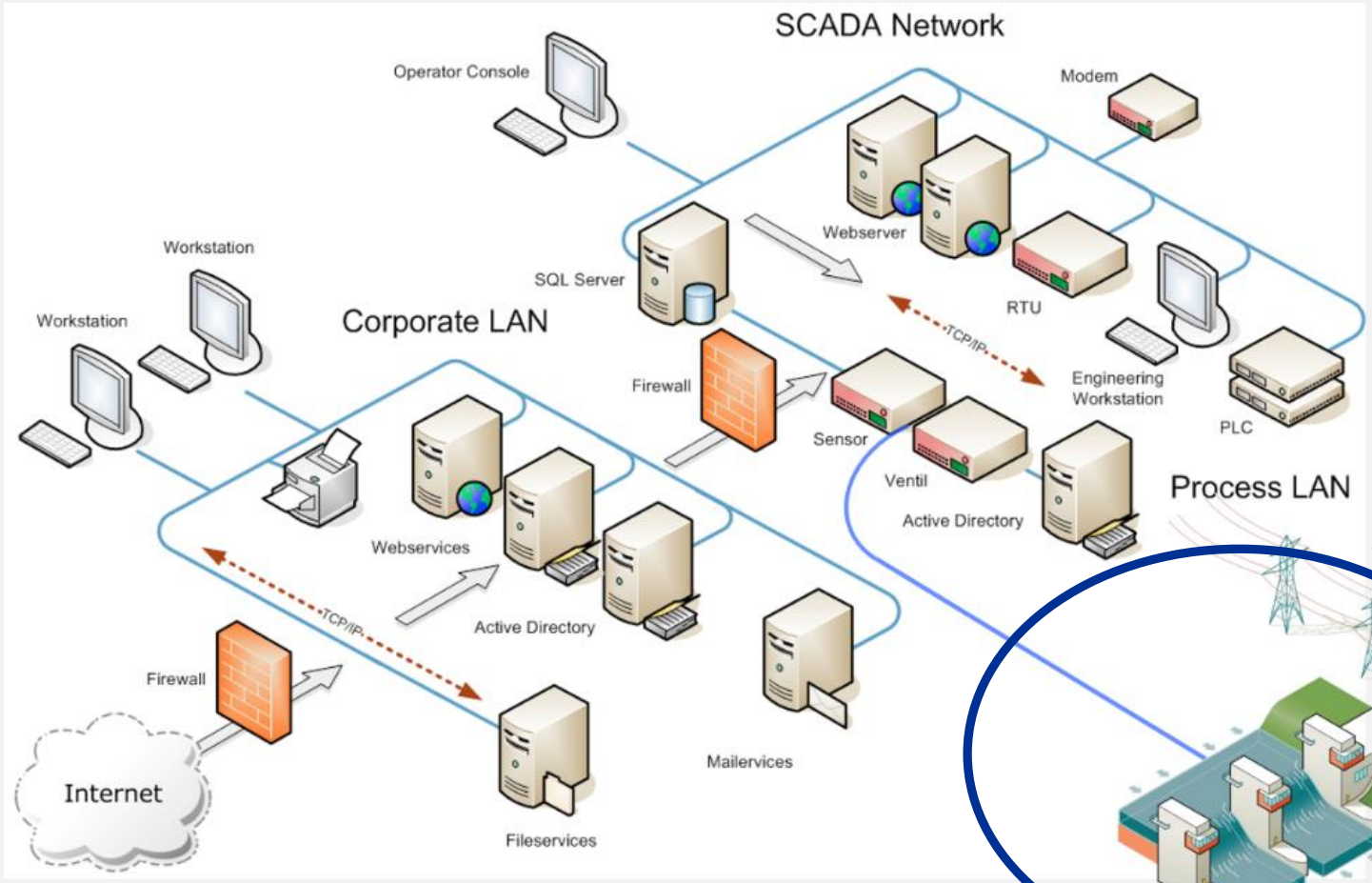
Motivation





Industrial Control Systems

Industrial Control Systems aka SCADA



Physical application

Curtesy: Compass Security Germany GmbH

Industrial Control Systems

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



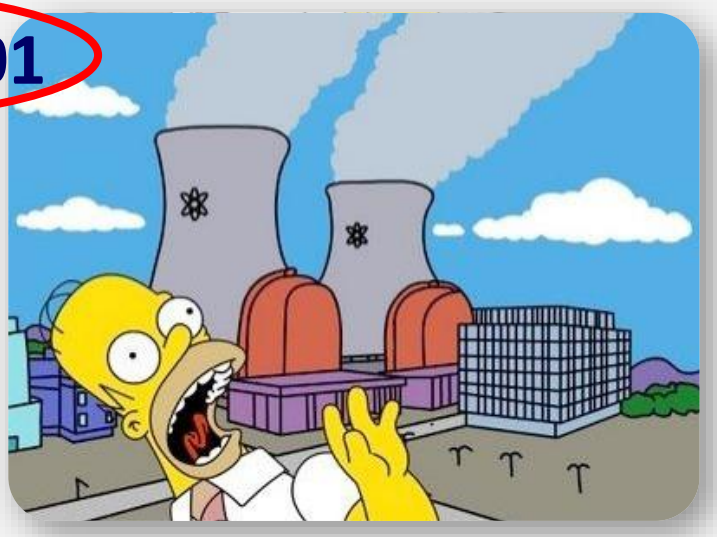
How do we do it??



0100110110111101

Missing piece of knowledge

Some horrible physical consequences



Typical understanding of SCADA hacking

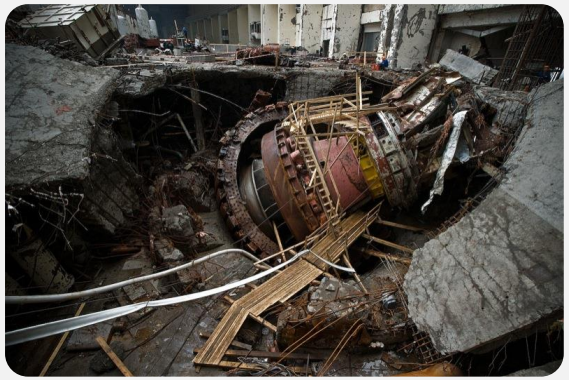


Source: simentari.com

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 (occupational, environment)
- Pollution (environment)
- Contractual agreements



Attack considerations



Equipment damage

Production damage

Compliance violation

- **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 (-)

Here's a plant. What is the plan?



Attack goal: persistent economic damage

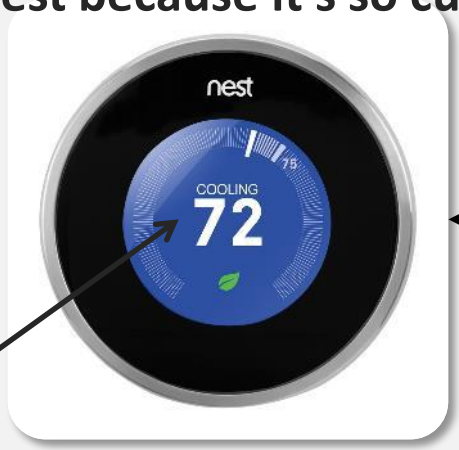


Process control

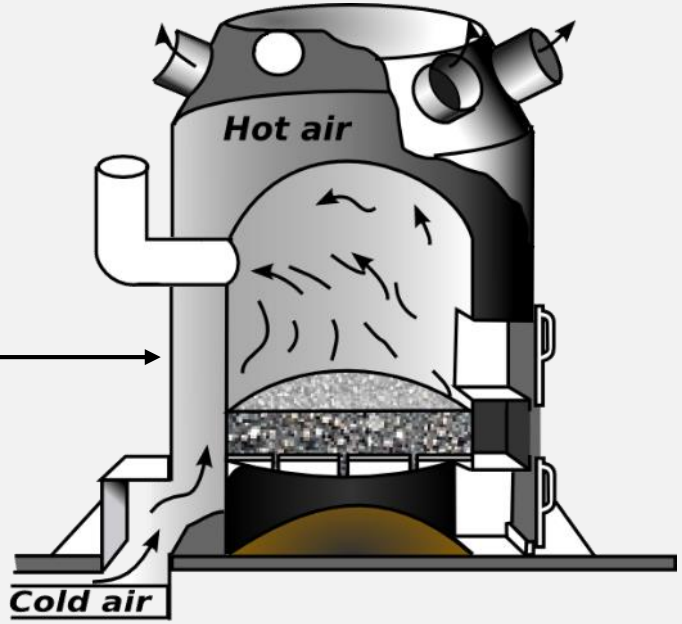
Process control automation



(Nest because it's so cute!)

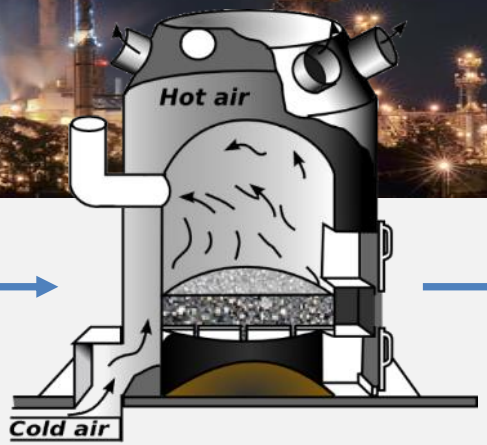


Set point



Running upstairs to turn on your furnace every time it gets cold gets tiring after a while so you automate it with a thermostat

Control loop



Physical process



Actuators

Adjust themselves to influence process behavior

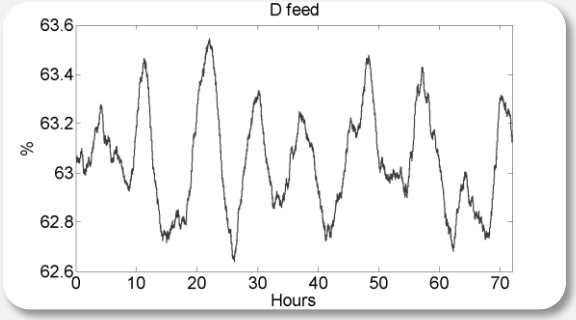
Sensors

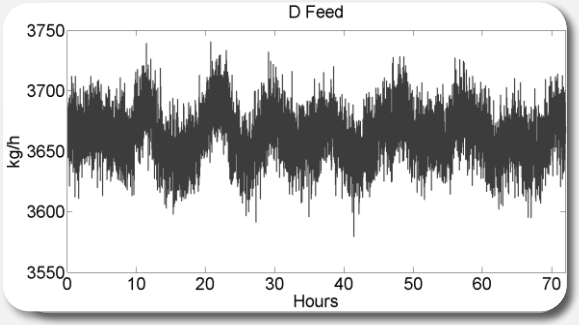


Measure process state

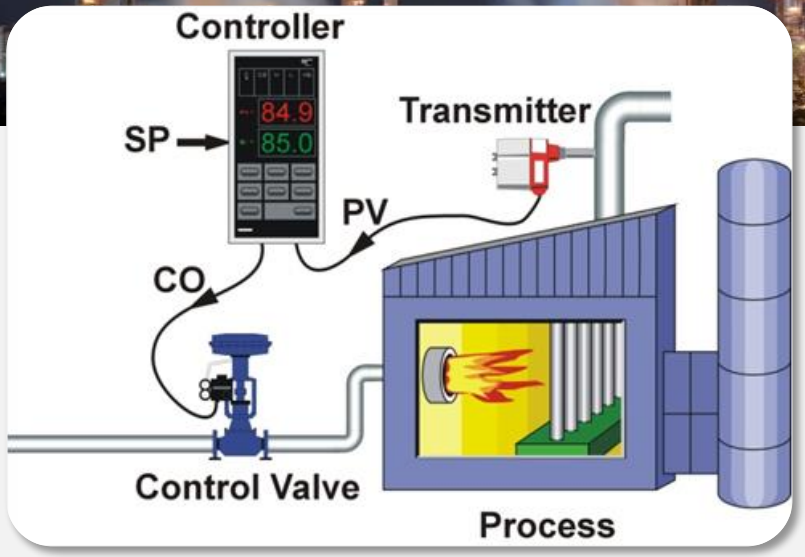
Control system

Computes control commands for actuators





Control system







Error in desired temperature **e(t) = SP - PV**

Controller output, **CO** Signal to actuator (valve)

Adjusted fuel flow to furnace

Set point (SP)

Desired temp

\+

\-

Termostat controller

Furnace fuel valve

House heating system

Heat into house

Measured temp

(Process variable, PV)

Temperature sensor

Heat loss

(e.g. through windows)

Jacques Smuts „Process Control for Practitioners“

Control equipment

- In large –scale operations control logic gets more complex than a thermostat
- One would need something bigger than a thermostat to handle it
- Most of the time this is a programmable logic controller (PLC)





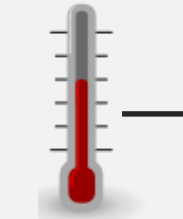
PLC internals



1. Copy data from inputs to temporary storage
2. Run the logic
3. Copy from temporary storage to outputs

Sensors

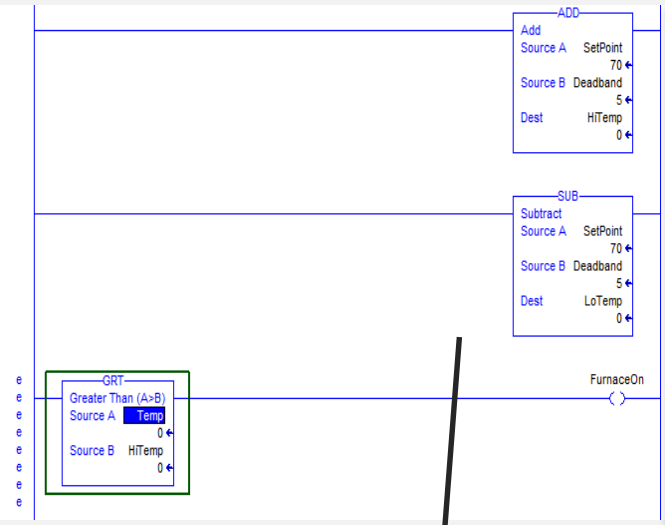
Actuators







Inputs



Outputs





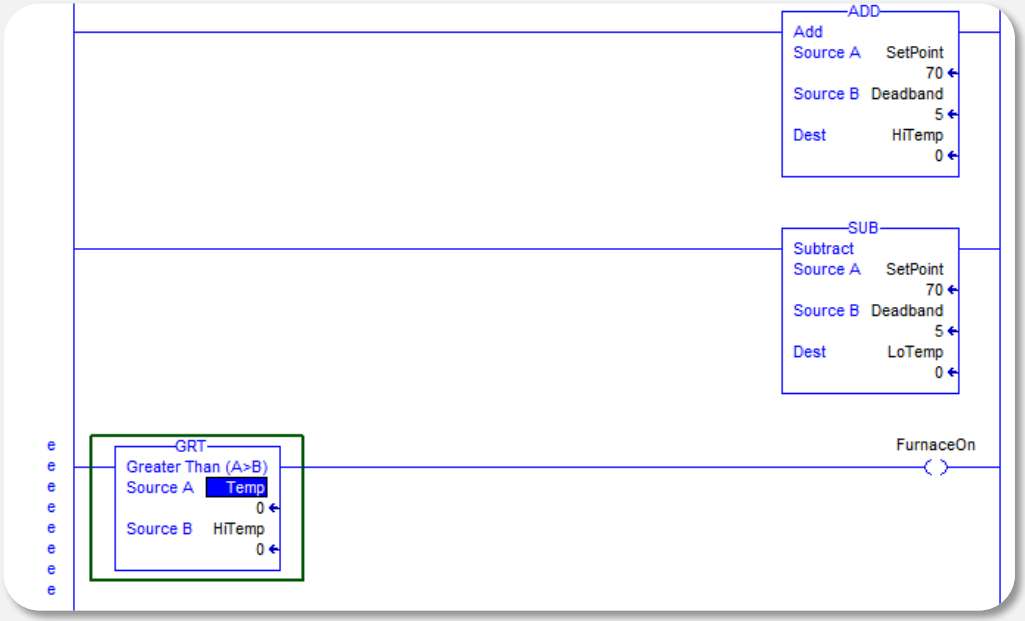




Control logic

- It is programmed graphically most of the time

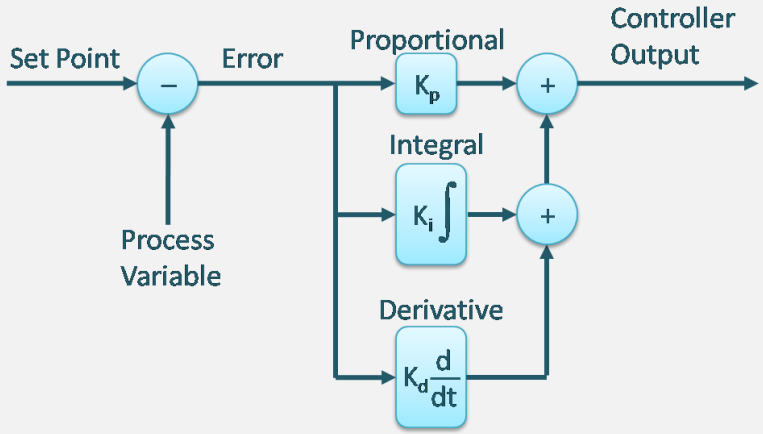
(We hear you screaming: Noooo!!!!
Just give me a real language!)

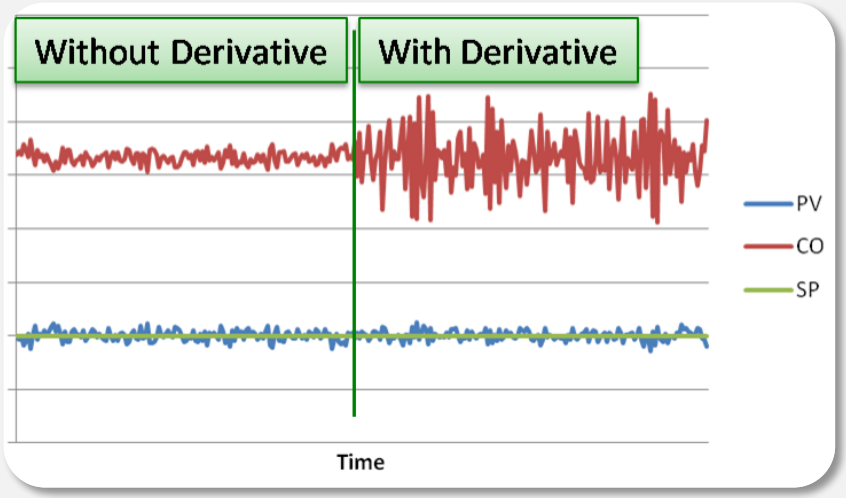


If Input 1 and (Input 4 or Input 11) then Output 6

If tank pressure in PLC 1 > 1800 reduce inflow in PLC 3

PID control





$$u(t) = K\left(e(t) + \frac{1}{T_i}\int_0^t e(\tau)d\tau + T_d\frac{de(t)}{dt}\right)$$

- **PID: proportional, integral, derivative –** most widely used control algorithm on the planet
- The sum of 3 components makes the final control signal
- PI controllers are most often used

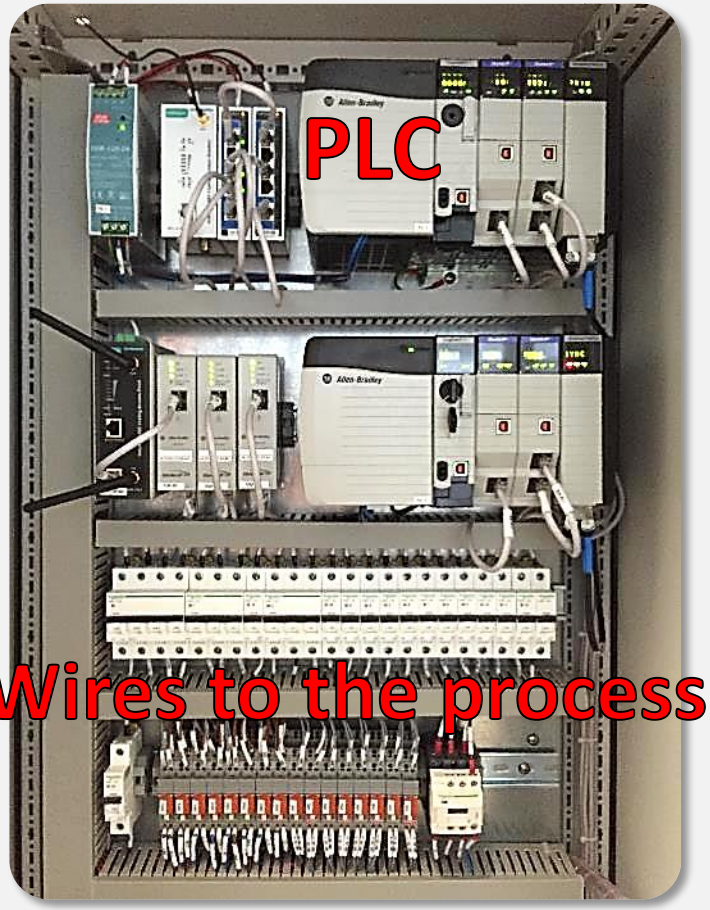
Jacques Smuts „Process Control for Practitioners“

Field communication

Communication media

- 4-20 mA
- 0-10 v
- Air pressure

Usually process values are scaled into meaningful data in the PLC



Wires are run from sensors and actuators into wiring cabinets

PLC cannot do it alone

- PLC does not have the complete picture and time trends
- Human operators watch the process 7/24
- **Most important task: resolving of alarms**

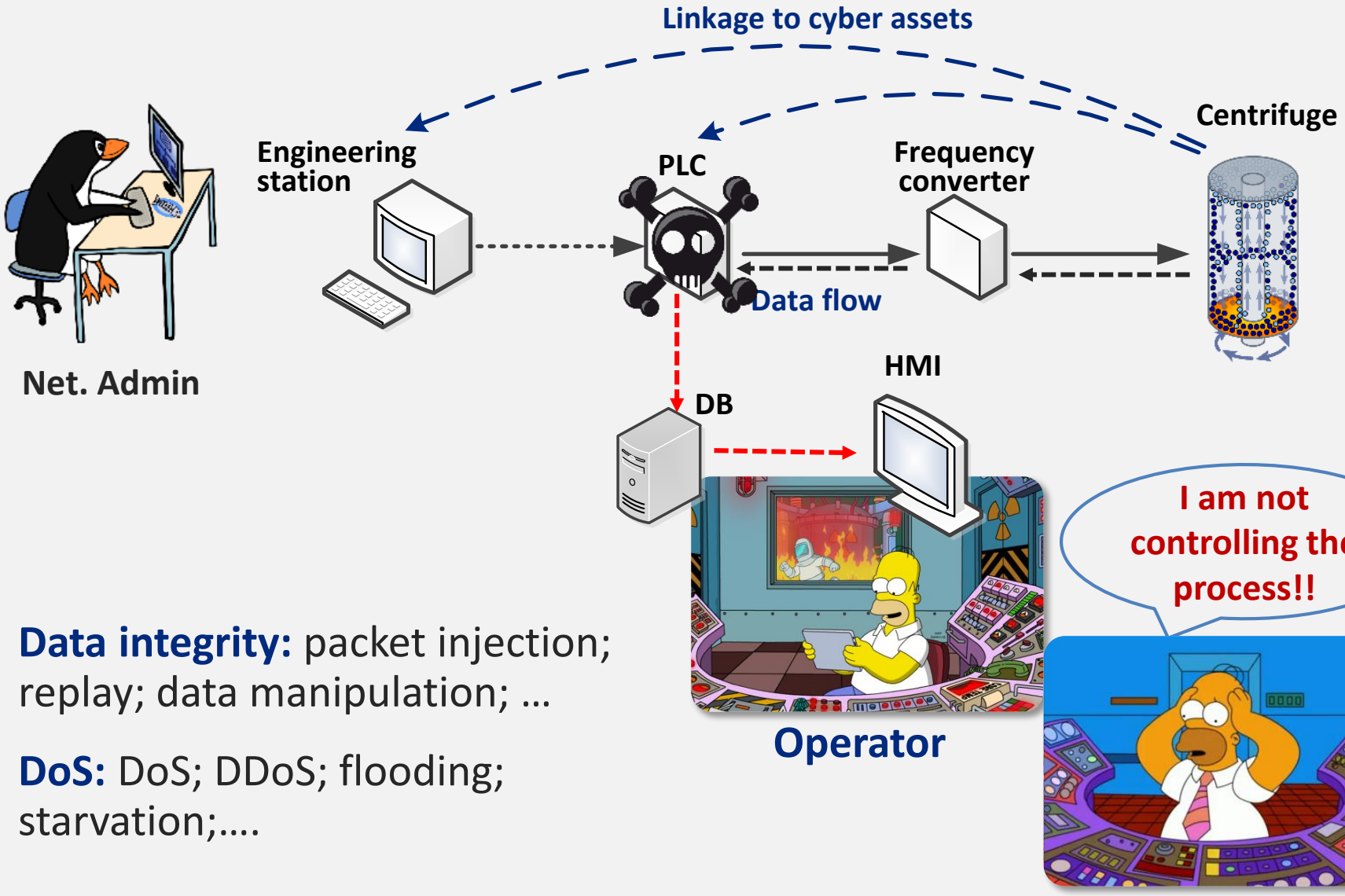






IT hacking vs. OT hacking

Example: attack on process data flow



Data integrity: packet injection; replay; data manipulation; …

DoS: DoS; DDoS; flooding; starvation;….

OT security



Controllability





Observability

OT hacking



- An attacker with an objective beyond simple mayhem will want to reliably manipulate the process
- This is achieved by obtaining and remaining in control of the process
- To remain in control you need to apply control theory fu. (not sql-injections, no XSS or ROP)

Process operator and hacker rival for control over the process



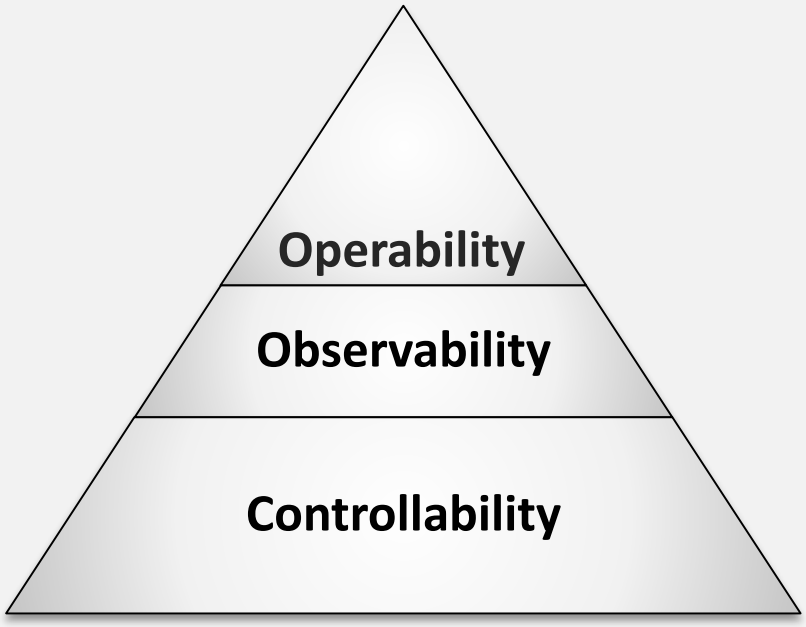
Process-related security properties



HOLY TRINITY



IT domain



Process control

Process-related security properties

HOLY TRINITY





CIA

Information security

CO2

Process control security

Haters gonna hate…



Approaches to attacker control

1. Reliably control the process throughout the attack
2. Control the process until failure is guaranteed and then let it run out of control
3. Make the process unusable by messing with the controls



Consider a car and a driver

- Attacker has control of the brakes
- Attacker applies the left front brake
- Diver steers right eventually coming back into a straight line
- Attacker applies the left brake
- Driver responds by steering to the right until the car is straight again



Consider a car and a driver

- The attacker responds by swapping brakes whenever the driver starts to compensate
- Eventually the attacker will win since a computer is faster than a human



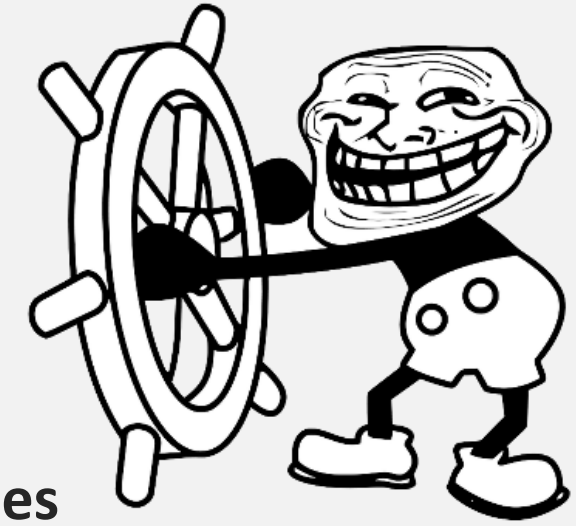
Multi-adaptive

- In the example above, the human is the “hidden actor” in the process that can’t be modeled or predicted
- Any subset of a process can be modeled as a “hidden actor” and potentially destabilized
- We call the algorithms that counter the feedback loops in the process “multi-adaptive” algorithms



Controlled uncontrollability

- Multi-Adaptive algorithms work just like process control automatic tuning programs except **they try to maximize the error instead of minimizing it**
- The algorithm learns the behavior of the hidden actor and then compensates for it
- **Everything the control loop does makes things worse**



- **A single algorithm can be used as a payload to disrupt many types of processes**
  - Crash a car or overpressure a loop



Get the party started!

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

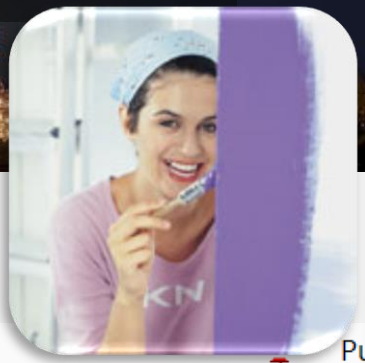




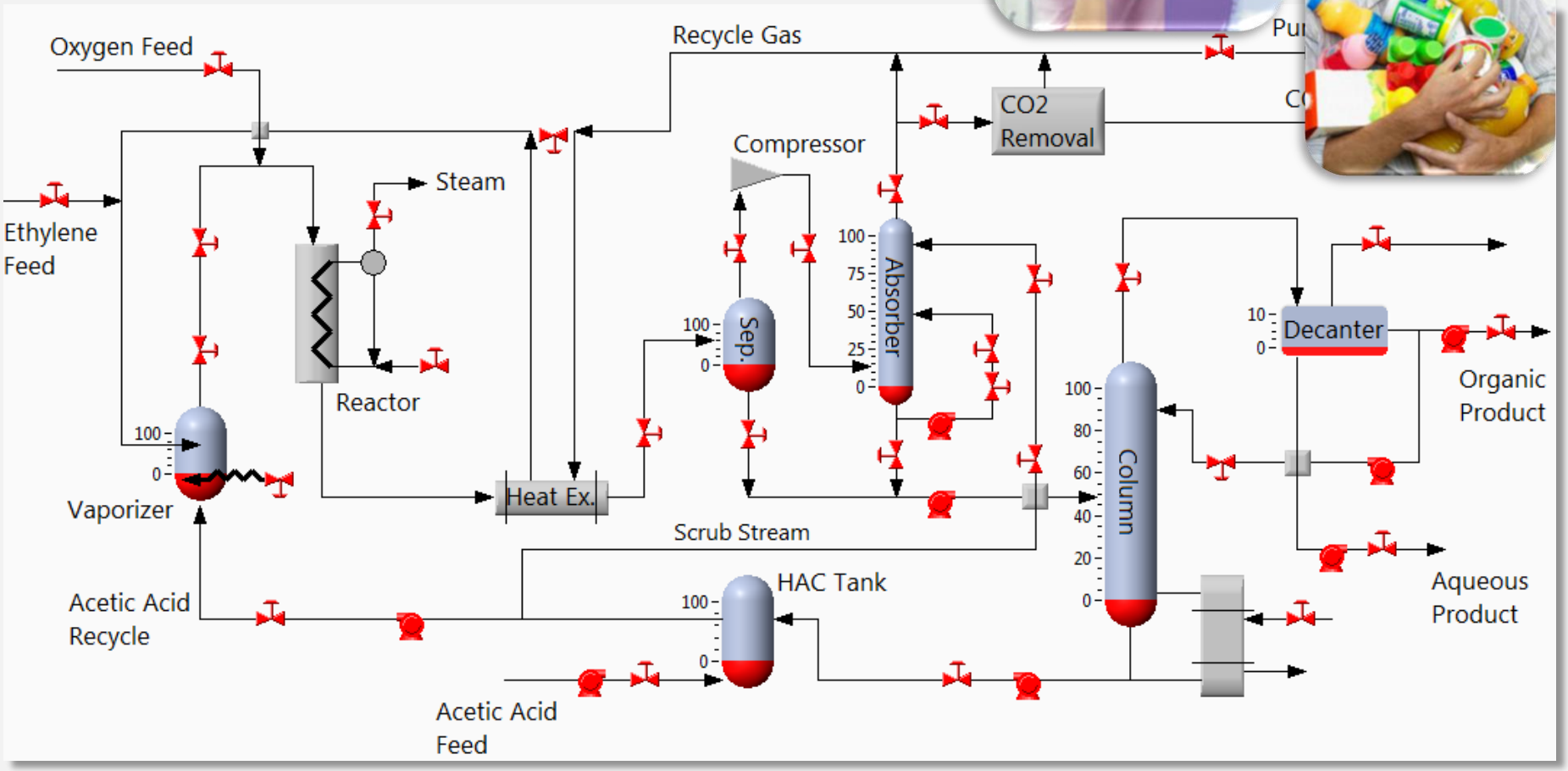
It is about MONEY

Plants are ouch! how expensive

Vinyl Acetate Monomer plant (model)









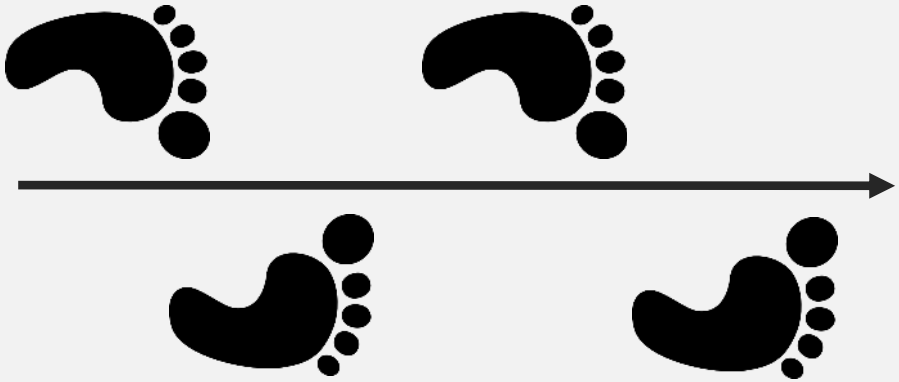
Stages of cyber-physical attacks

Attack payload

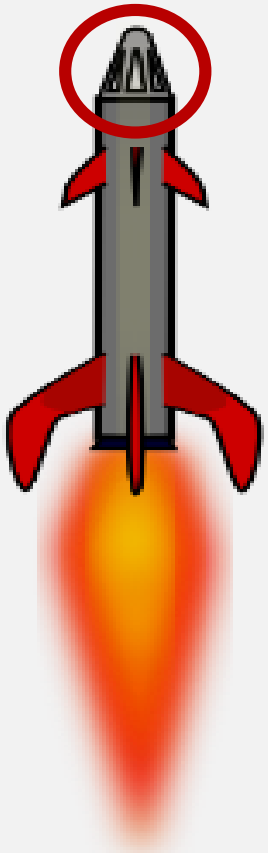


Attack objective





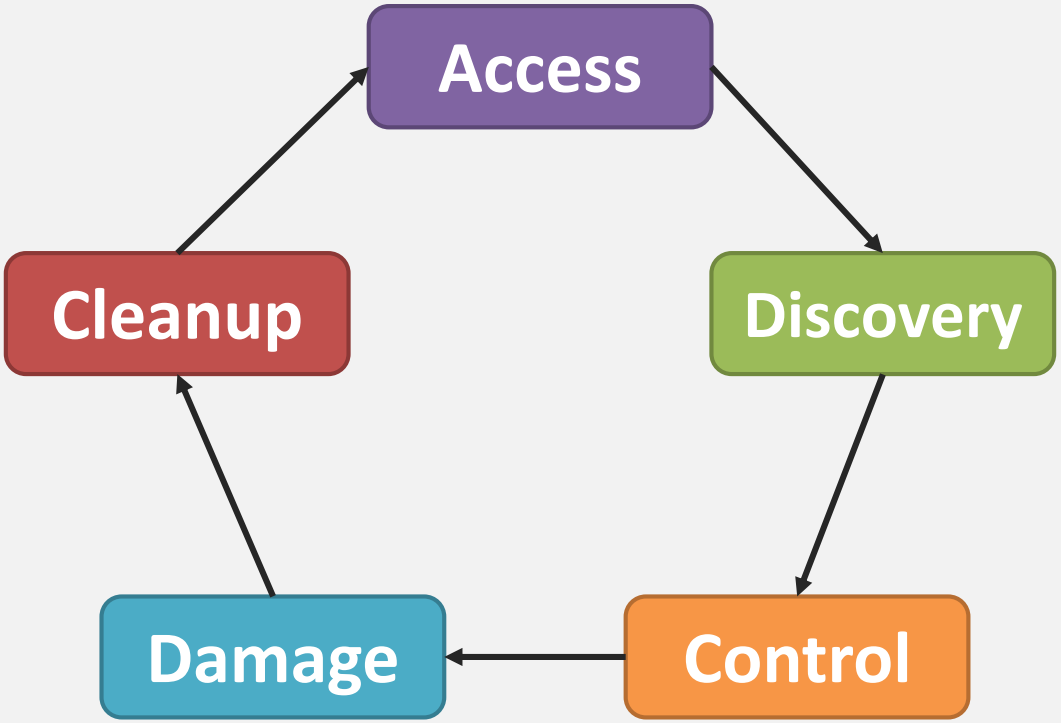
Cyber-physical payload



Stages of SCADA attack

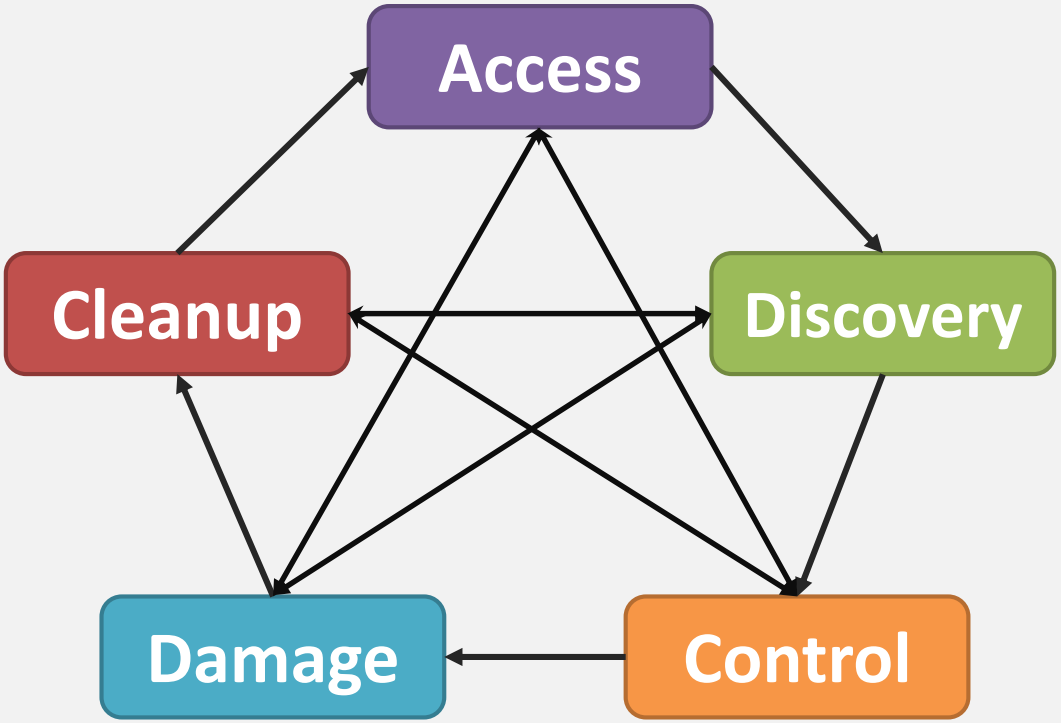






Stages of SCADA attack

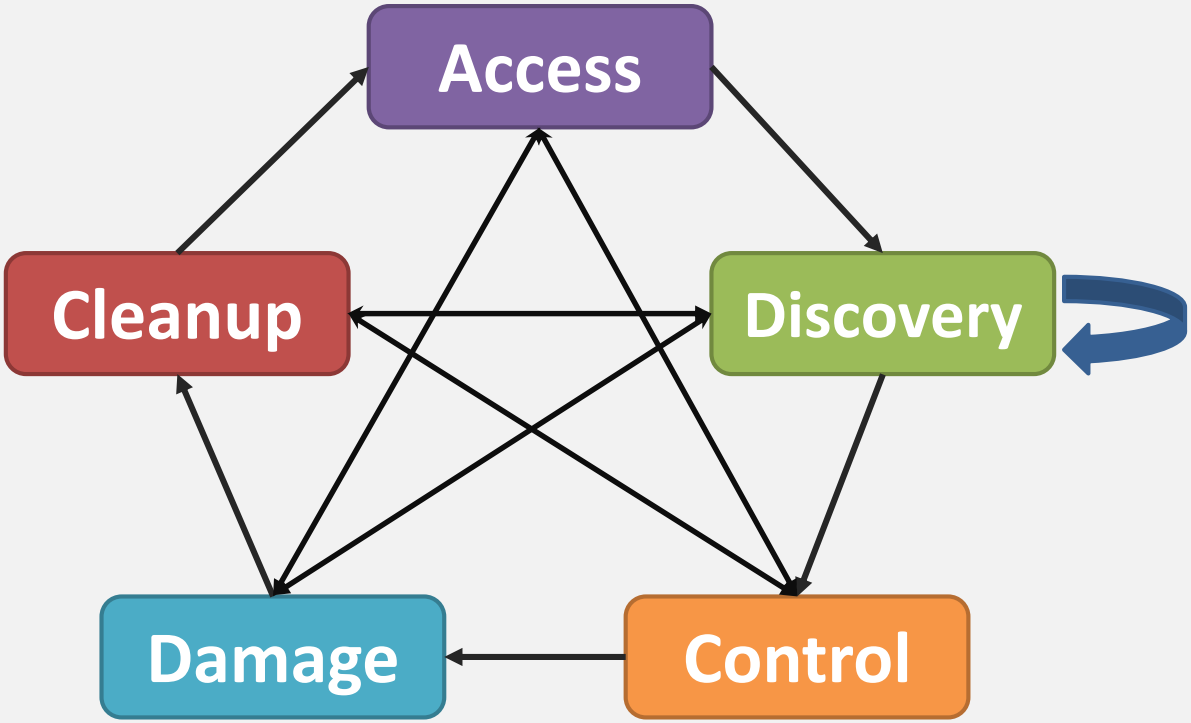




Stages of SCADA attack







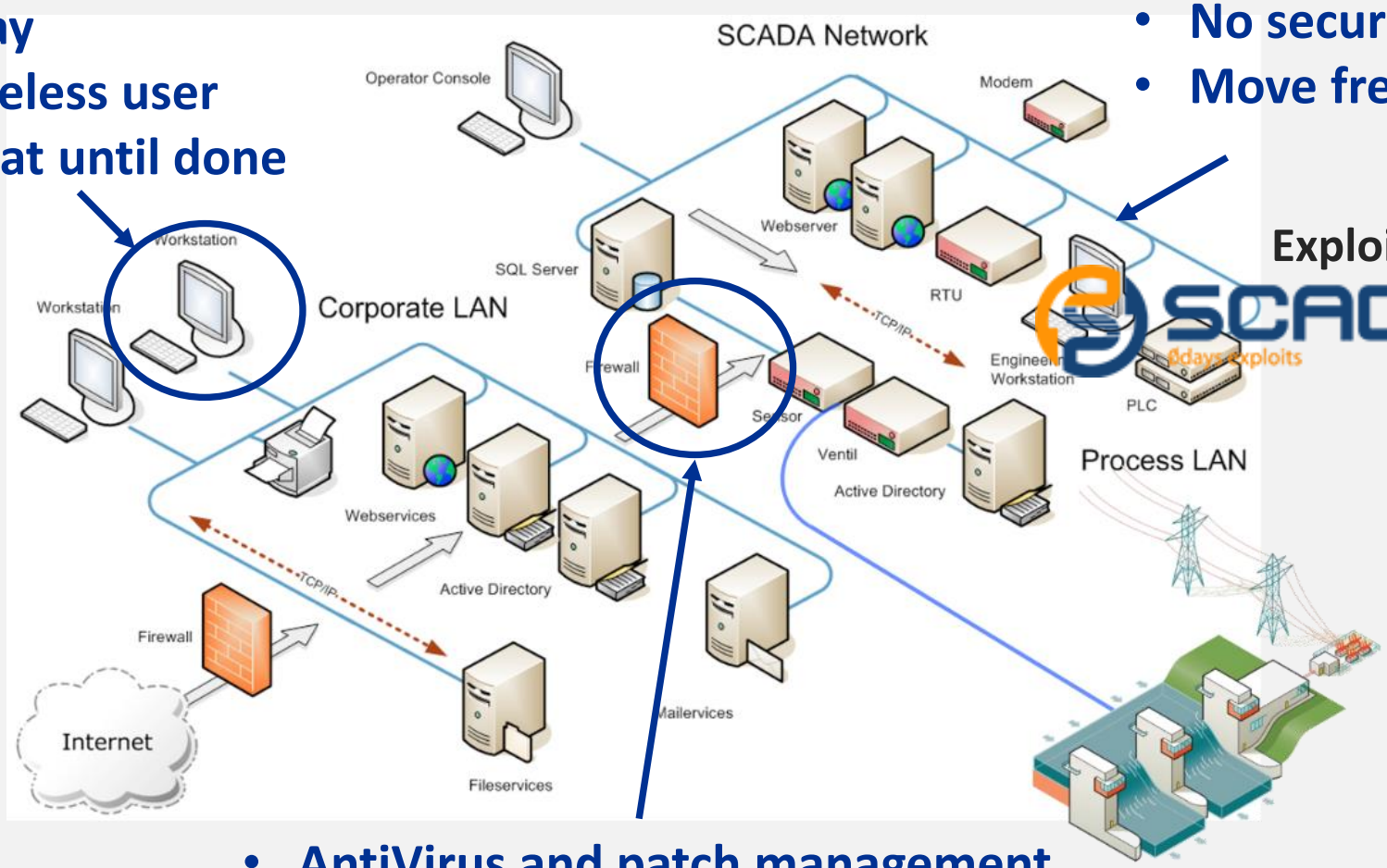


Access



Traditional IT hacking

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



- No security
- Move freely

Exploit kit

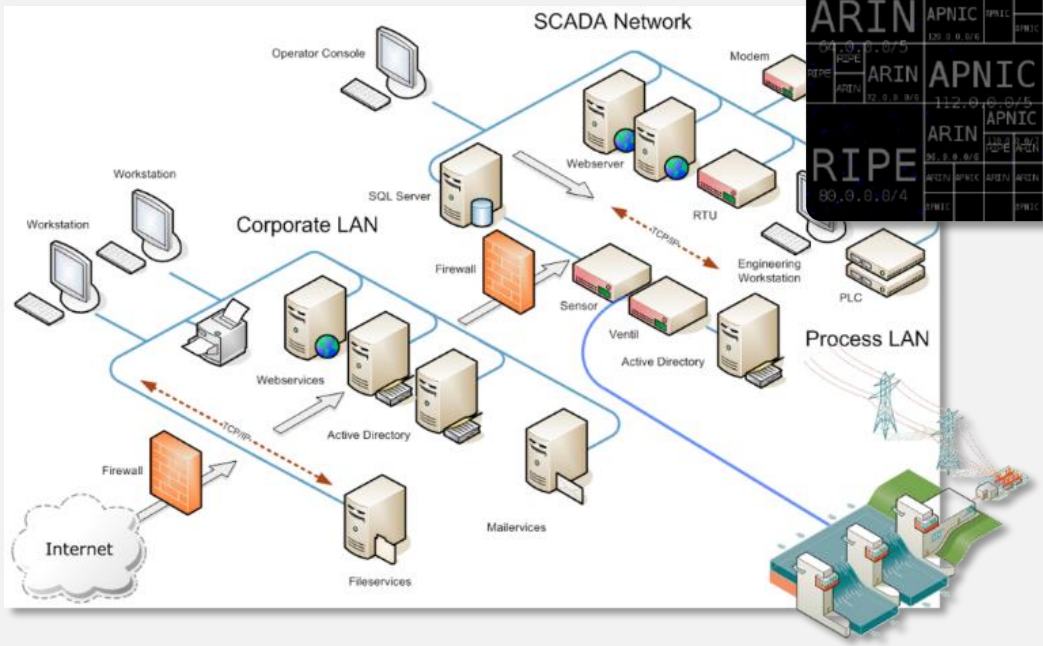
SCADA+ 0days Exploits

- 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)

Smart instrumentation

- Converts analog signal into digital
- Sensors pre-process the measurements
- IP-enabled (part of the “Internet-of-Things”)



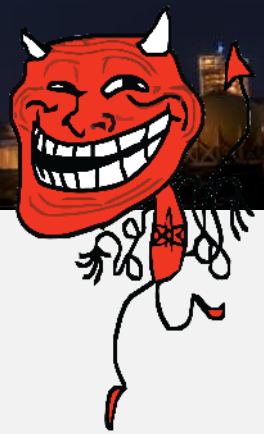
Old generation temperature sensor



Sensor

Computational element

Invading field devices



- Jason Larsen at Black Hat'15 "Miniaturization"
  - Inserting rootkit into firmware

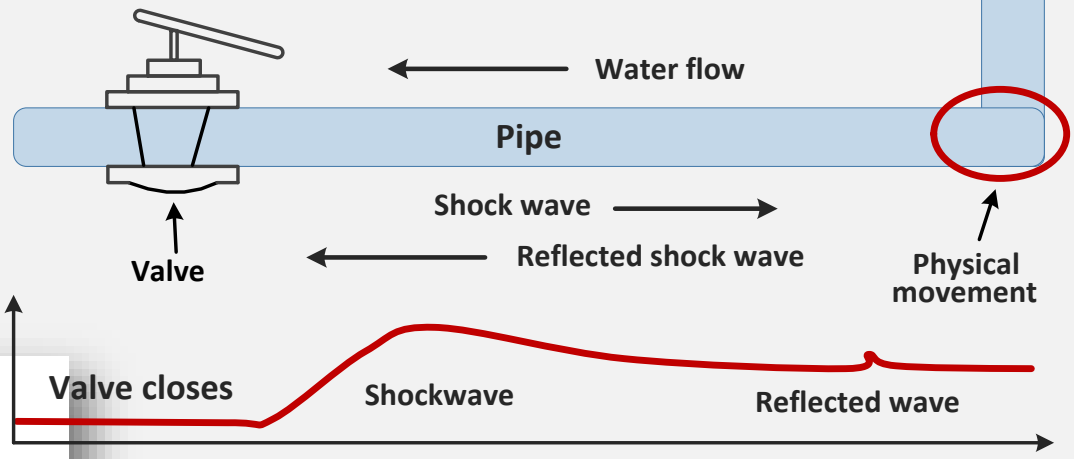


```
.def CalcSomething
CalcSomething:
push.w   R4
mov.w    SP, R4
incd.w   R4
add.w    #0FFFAh, SP
mov.w    R15, 0FFFCh(R4)
clr.w    0FFF8h(R4)
clr.w    0FFFAh(R4)
jmp      loc_22
```

```
loc_22:
cmp.w    0FFFCh(R4), 0FFFAh(R4)
jl       loc_18
```

```
loc_18:
add.w    0FFFAh(R4), 0FFF8h(R4)
inc.w    0FFFAh(R4)
```

```
mov.w    0FFF8h(R4), R15
add.w    #6, SP
pop      R4
ret
; End of function CalcSomething
```



Attack scenario: pipe damage with water hammer



Discovery

Stripper is...



Know the equipment

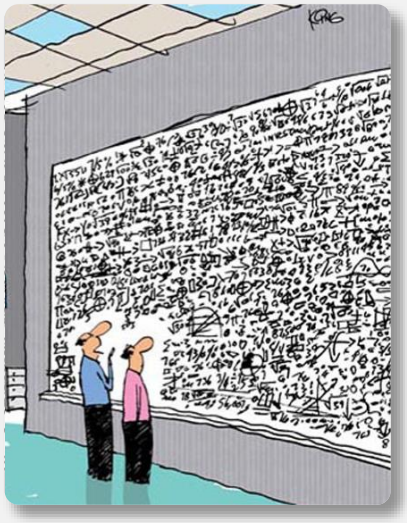
Stripping column



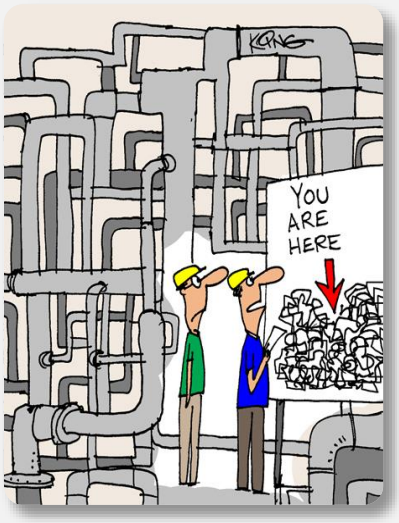
Process discovery



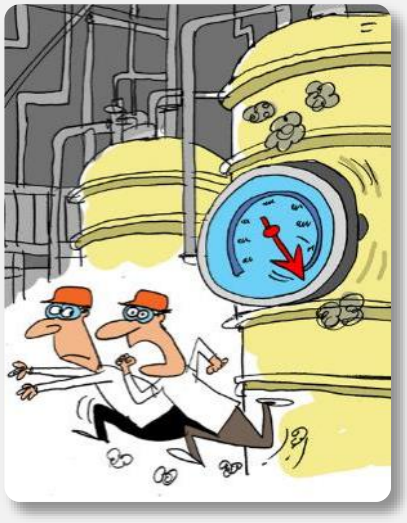
What and how the process is producing



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

Over Half of ICS Security Incidents Reported in 201[illegible] Involved APTs: ICS-CERT

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

Dragonfly: Weste[illegible]

Cyberespionage campaign stole in[illegible]

DragonFly/Havex/Ene[illegible]

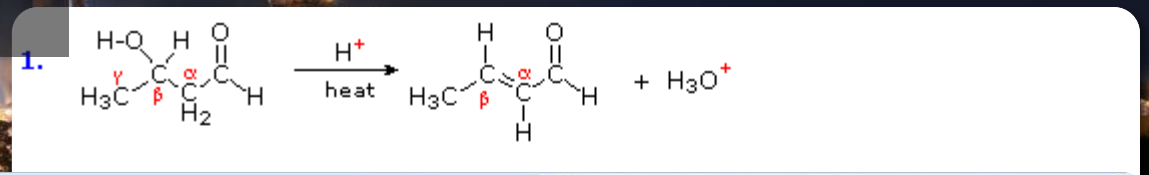
Against Energy Suppl[illegible]

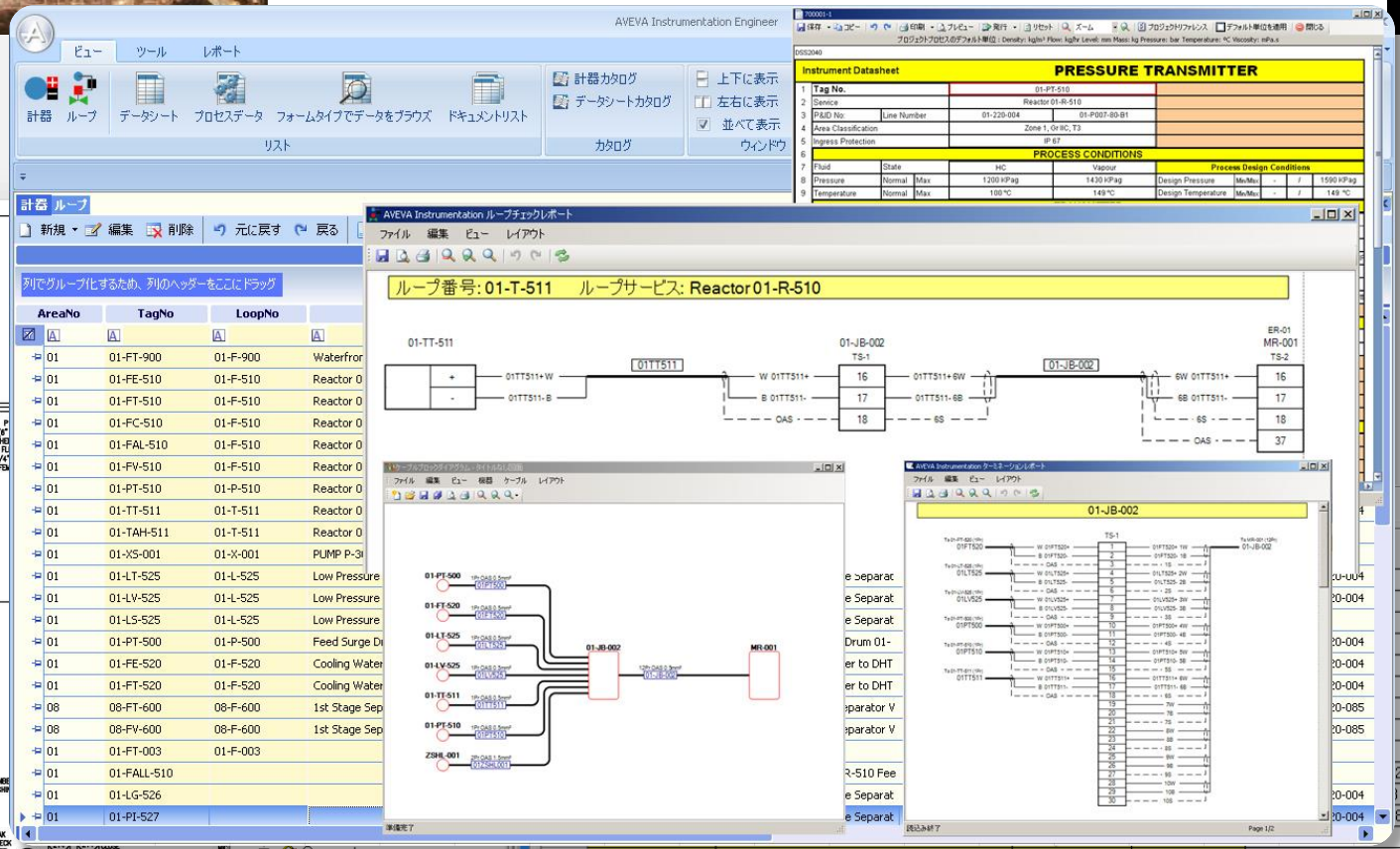
ACAD/Medre.A 10000's of AutoCAD files leaked in suspected industrial espionage

June 25, 2014

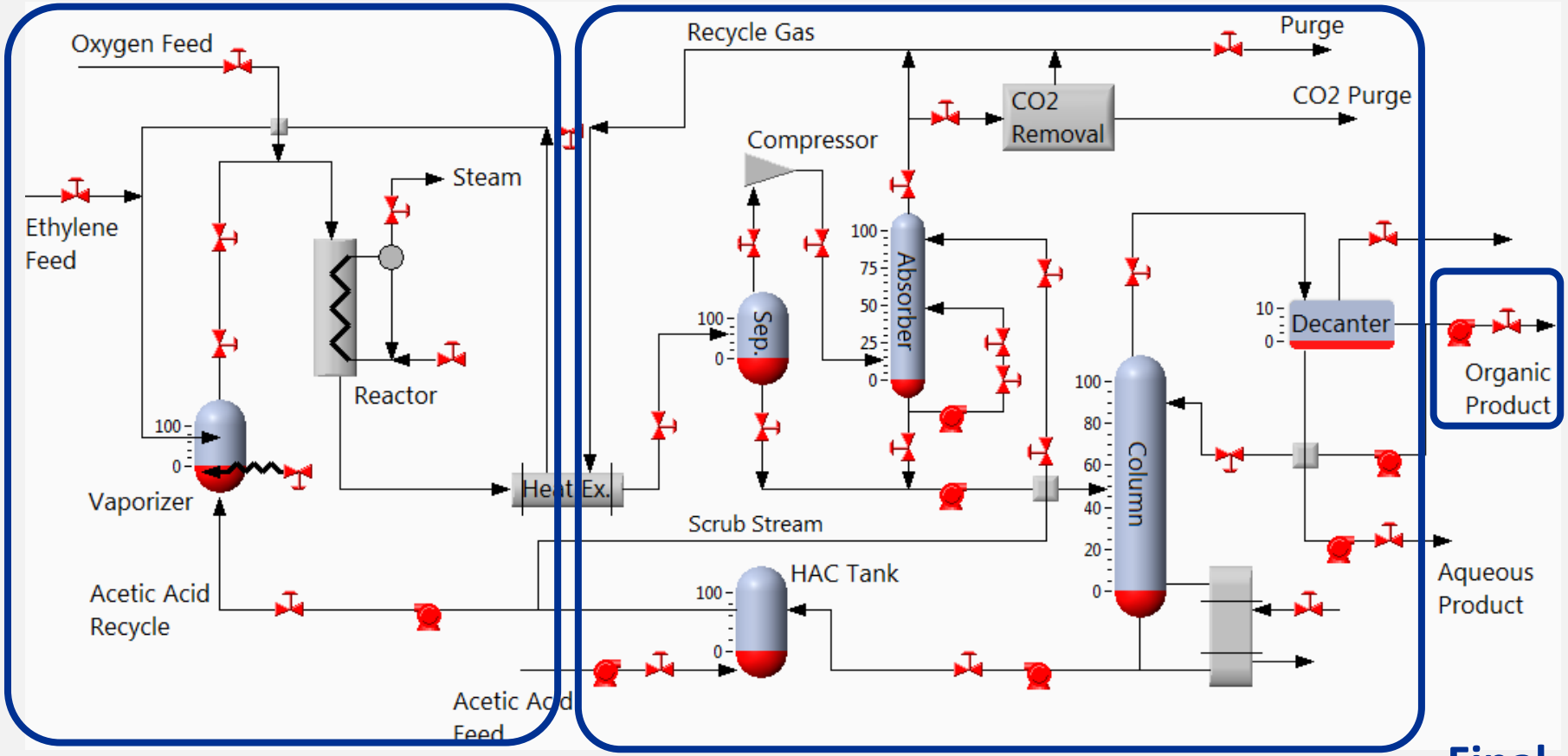
Nation state behind malware attacks on European ICS systems?

Process discovery





Max economic damage?



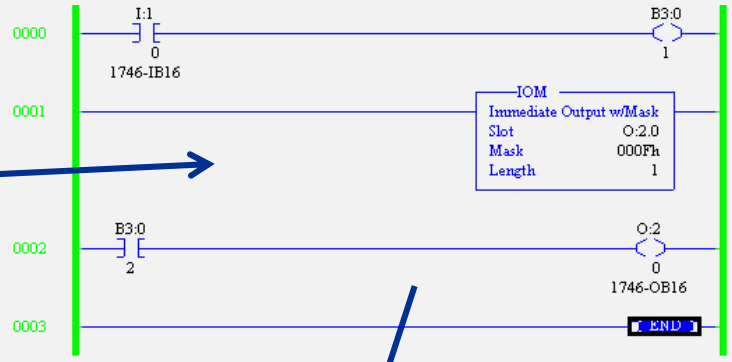
Requires input of subject matter experts

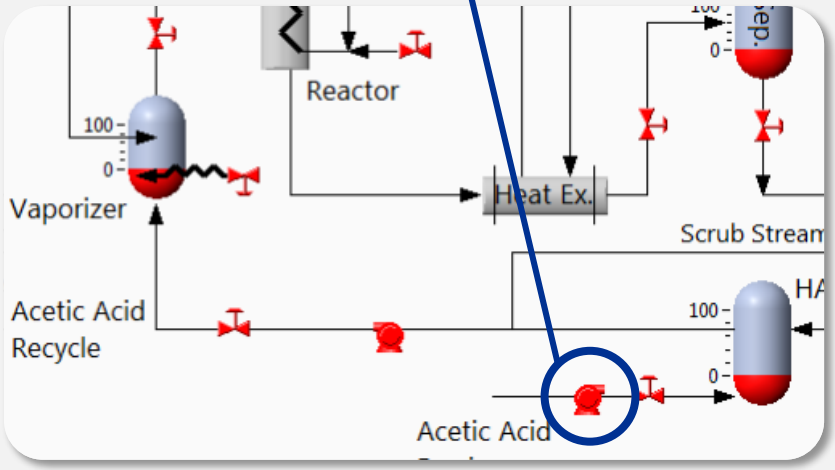
Understanding points and logic

Programmable Logic Controller

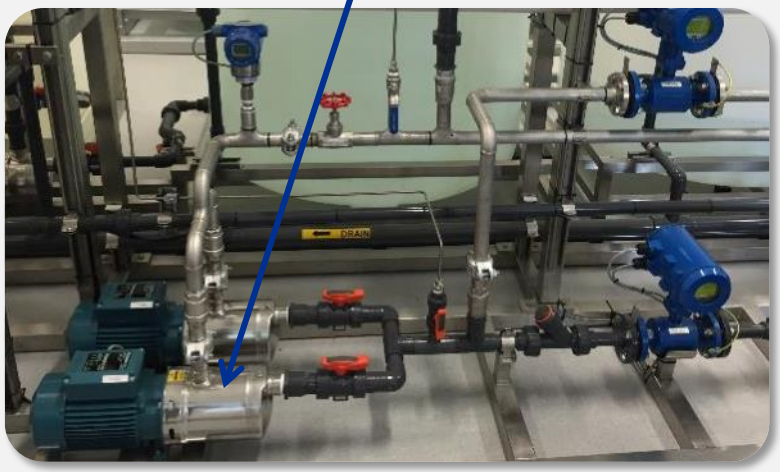


Ladder logic





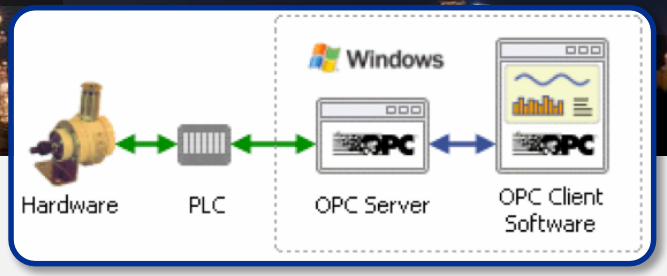
Piping and instrumentation diagram



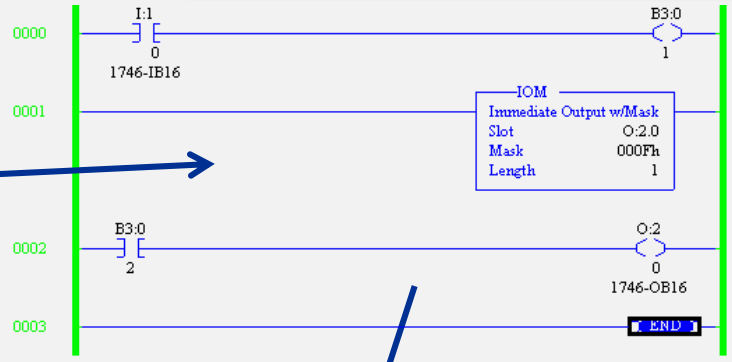
Pump in the plant

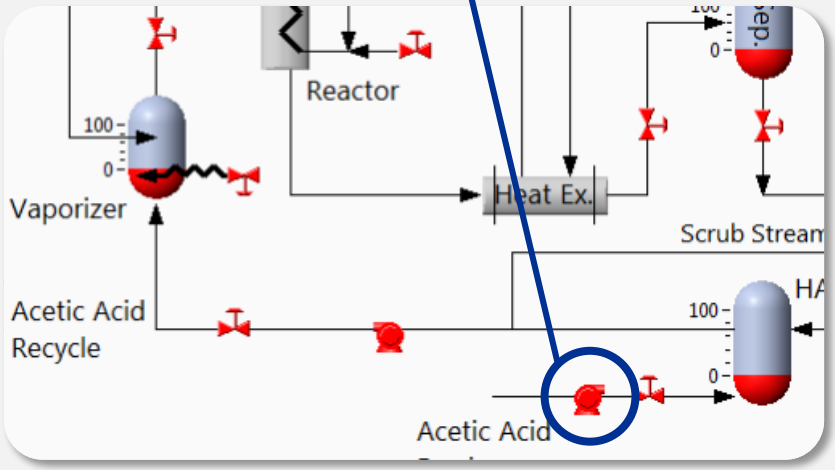
Understanding points and logic

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

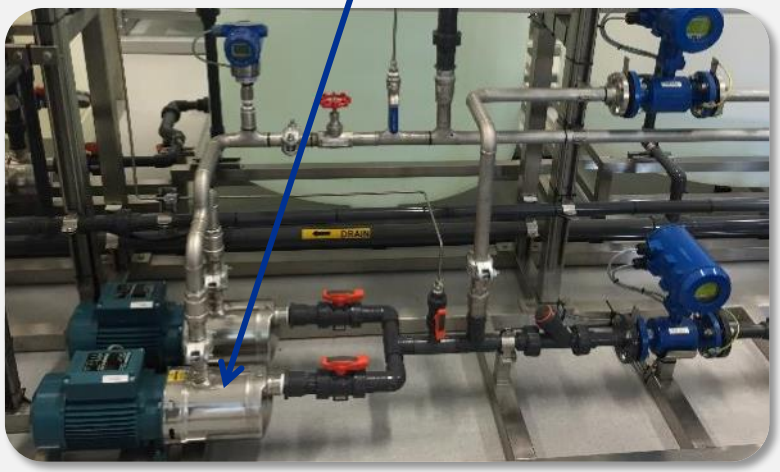






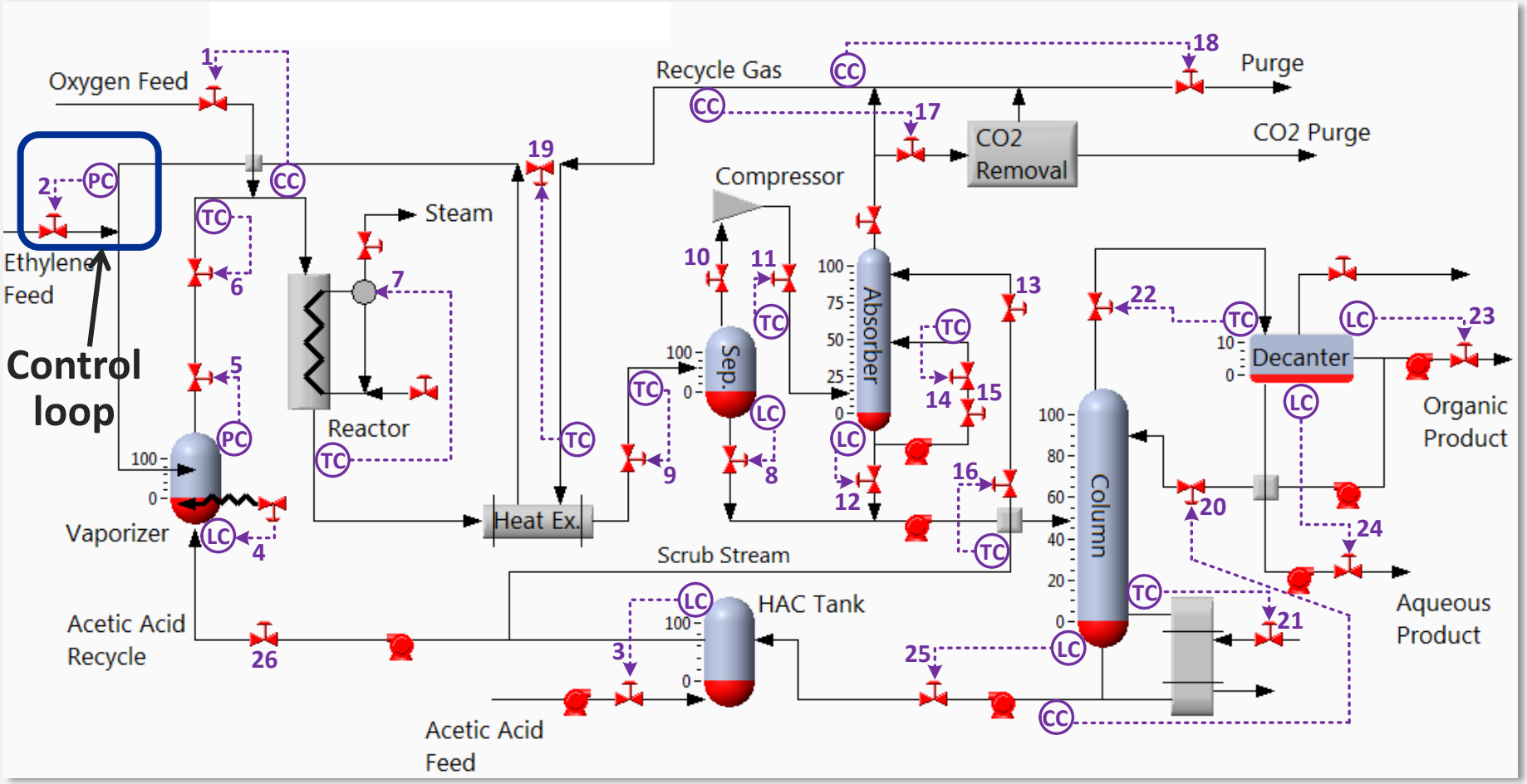


Piping and instrumentation diagram

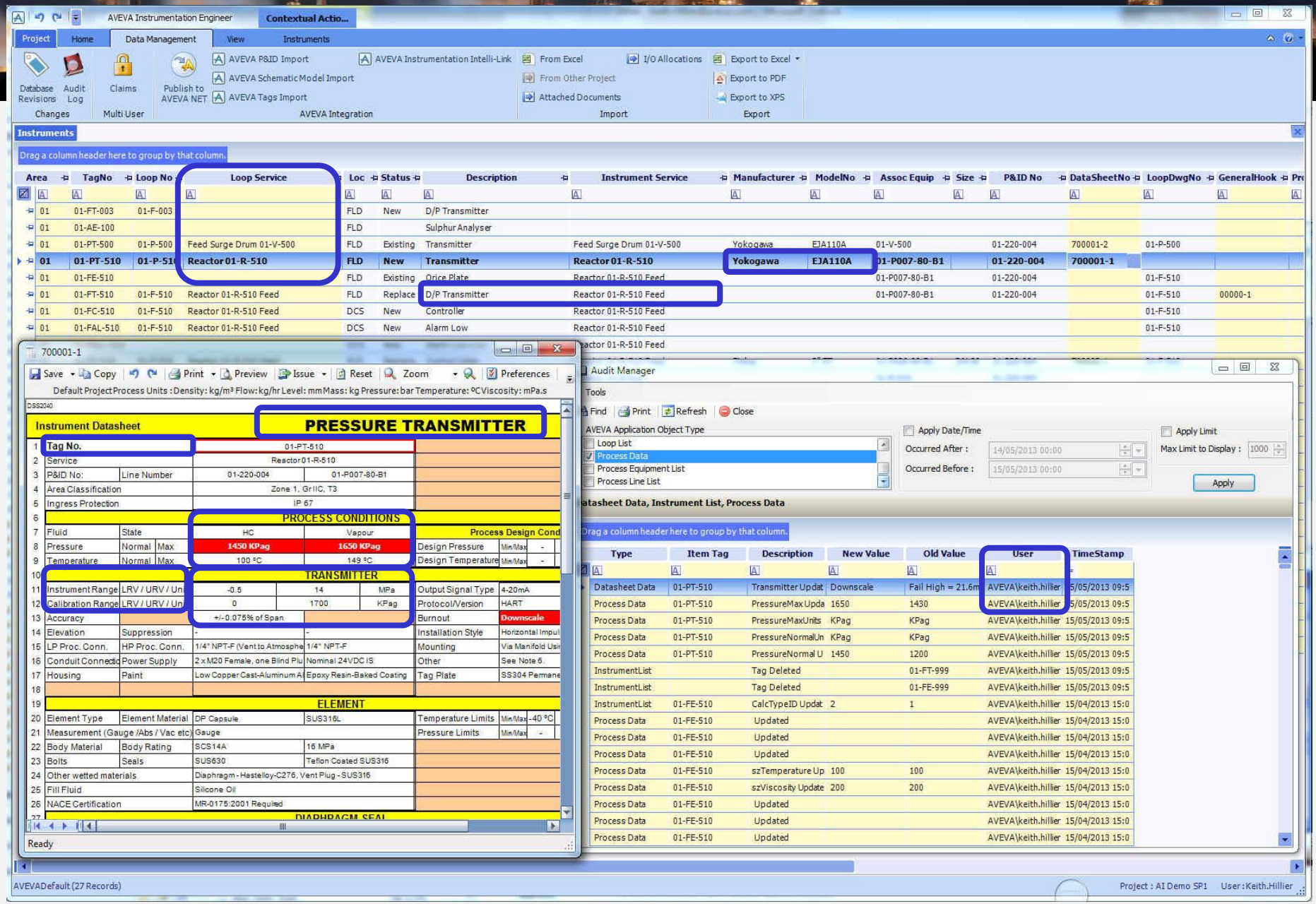


Pump in the plant

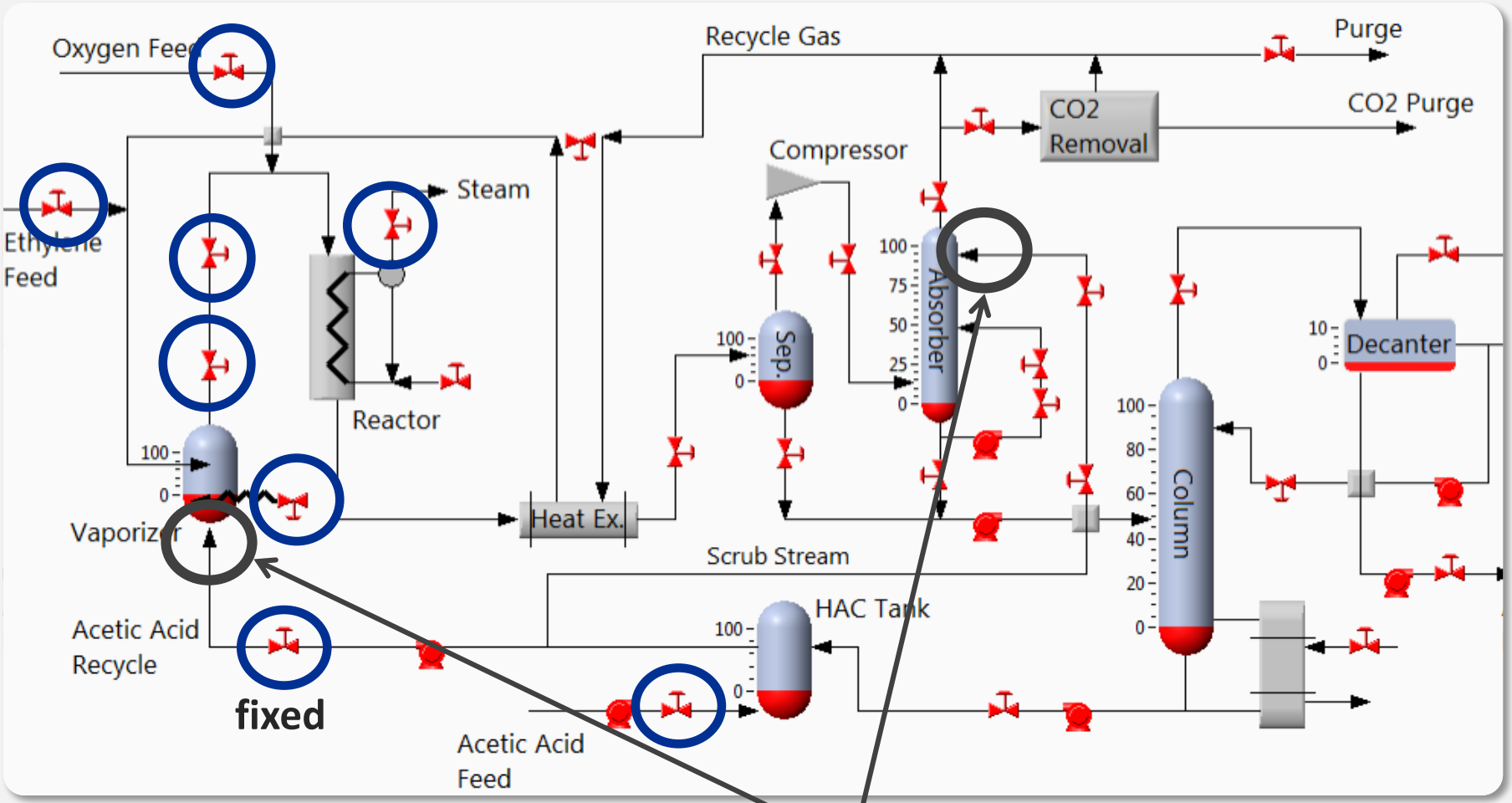
Understanding control structure



Control loop configuration

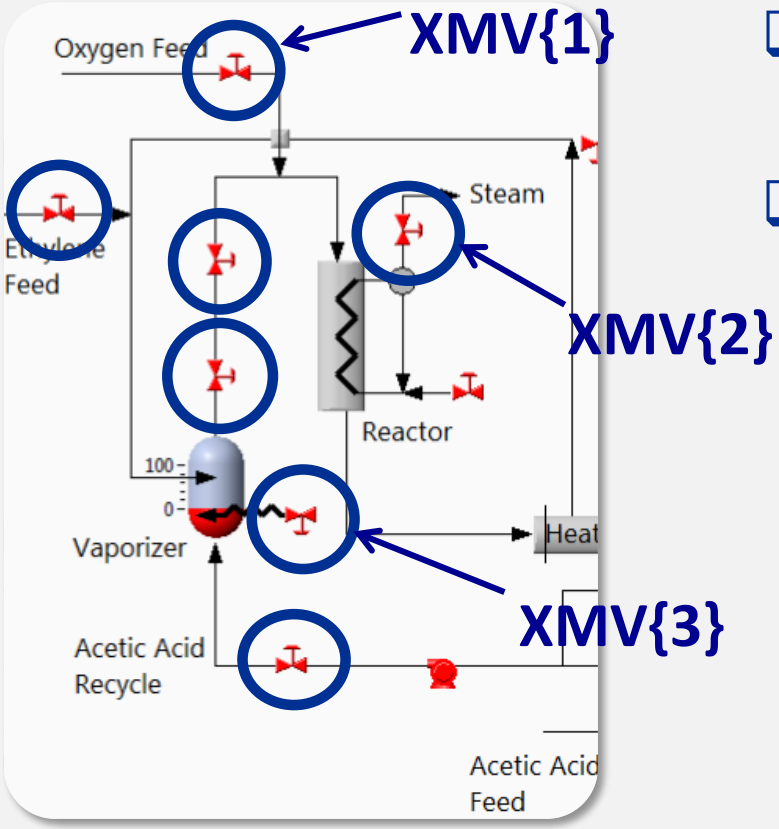


Watch the flows!



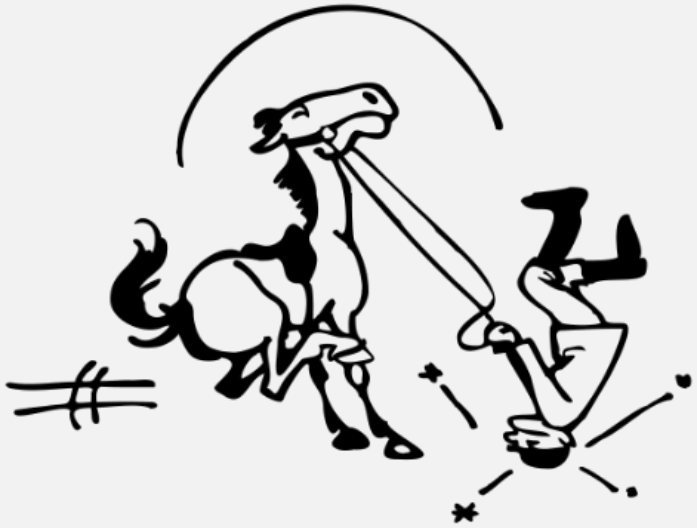
HAc flows into two sections. Not good :(

Obtaining control != being in control



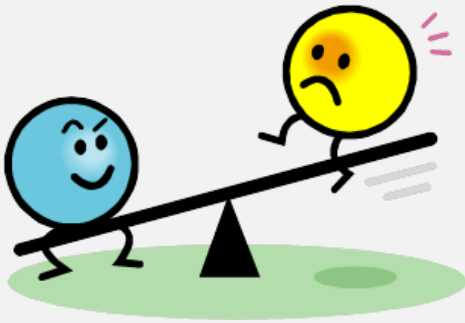
- Obtained controls might not be useful for attack goal
- Attacker might not necessary be able to control obtained controls

WTF ???





Control



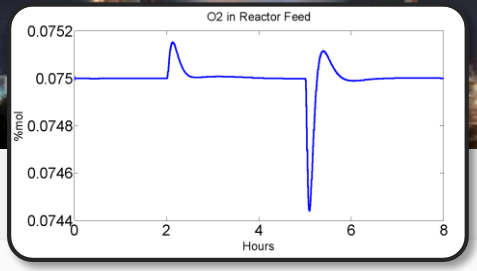
Every action has a reaction

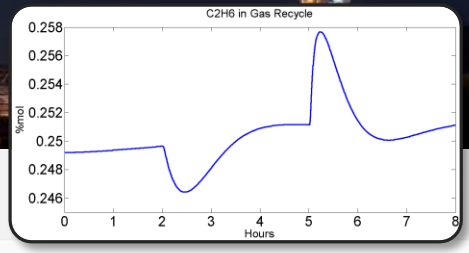
Physics of process control

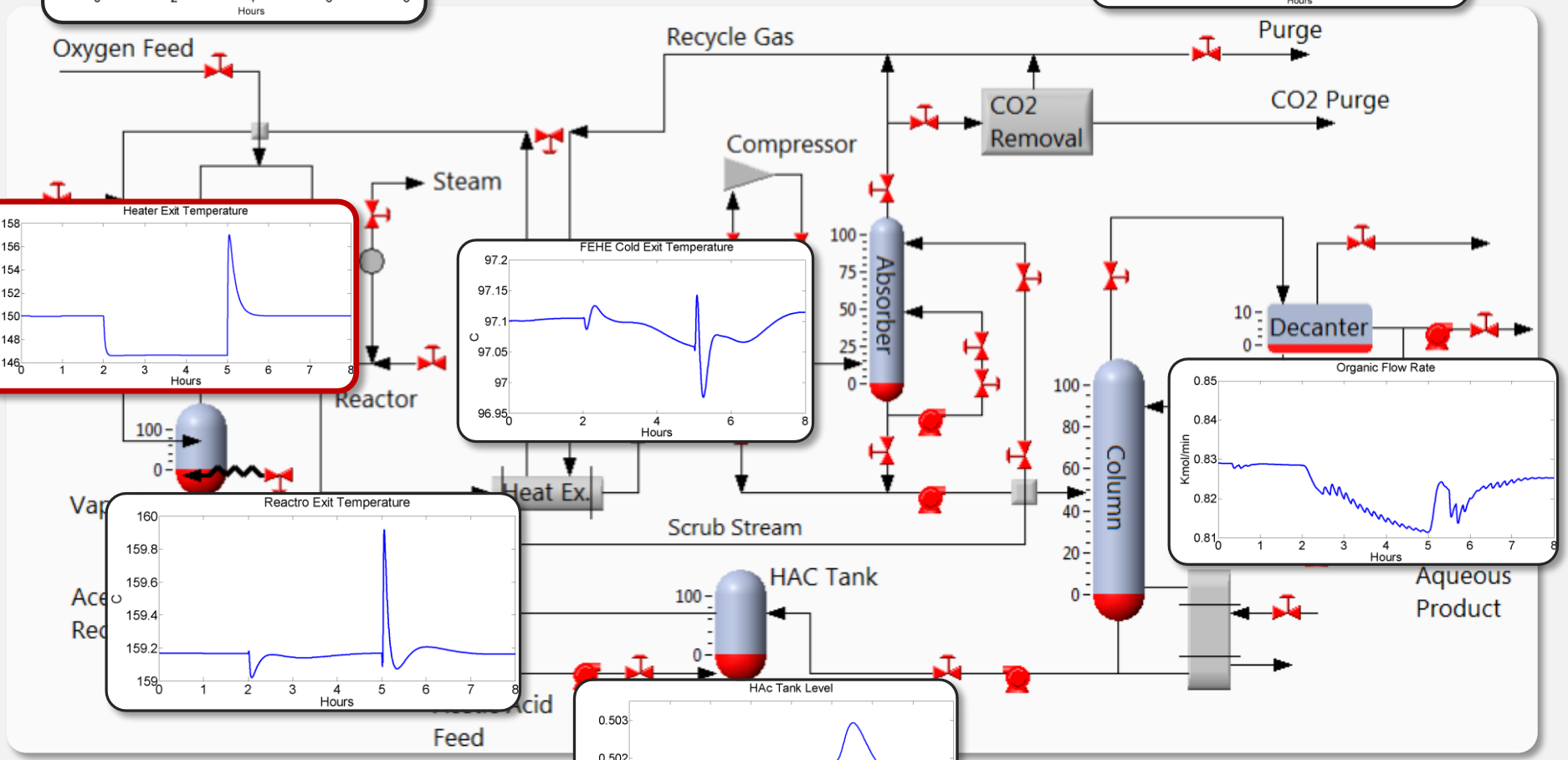


- **Once hooked up together, physical components become related to each other by the physics of the process**
- If we adjust a valve what happens to everything else?
  - Adjusting temperature also increases pressure and flow
  - All the downstream effects need to be taken into account
- How much does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

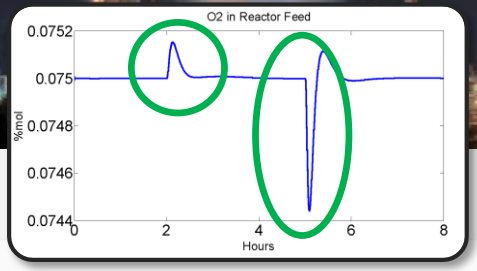
Process interdependencies

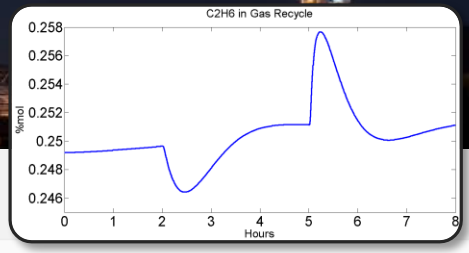


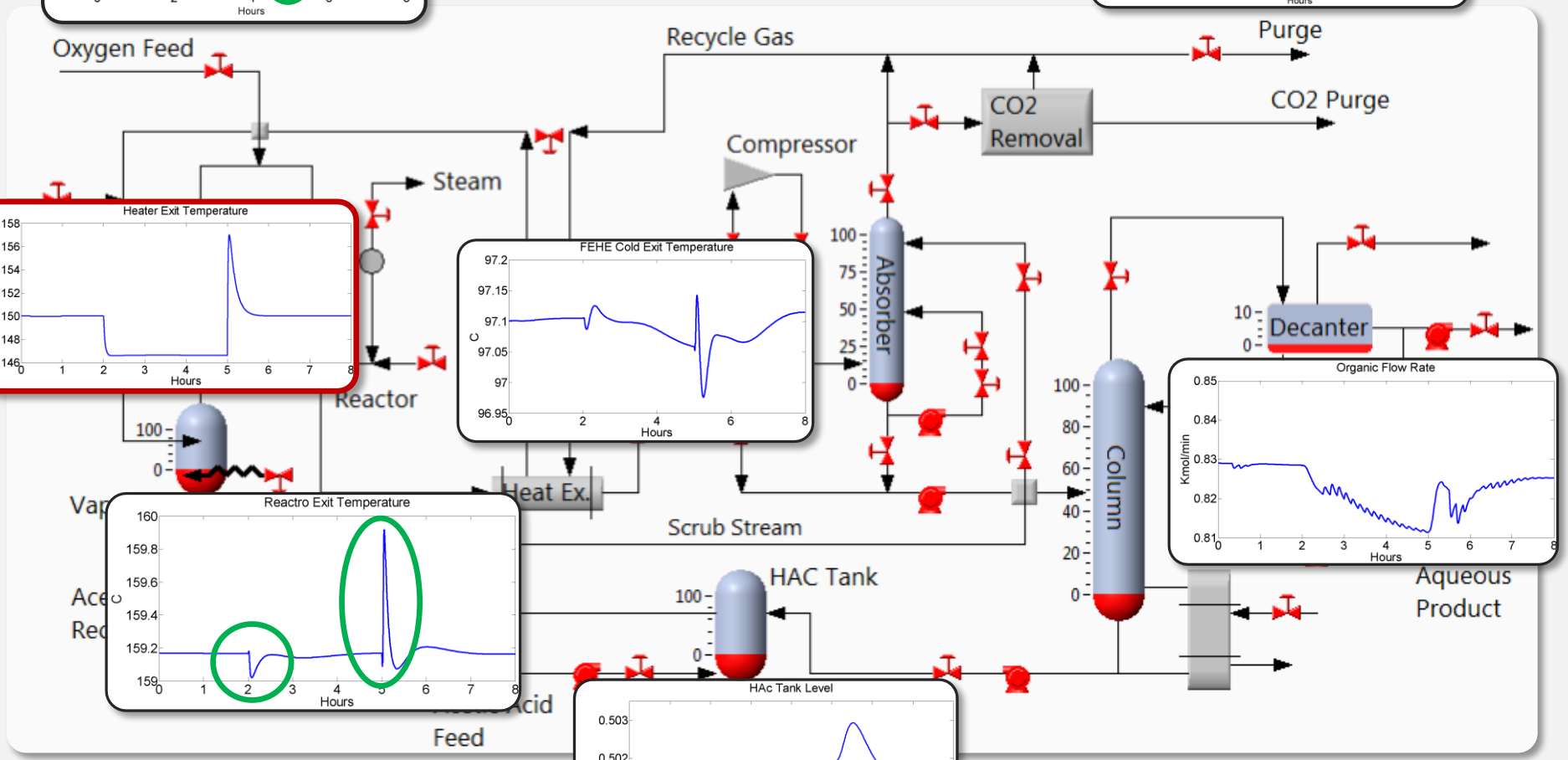




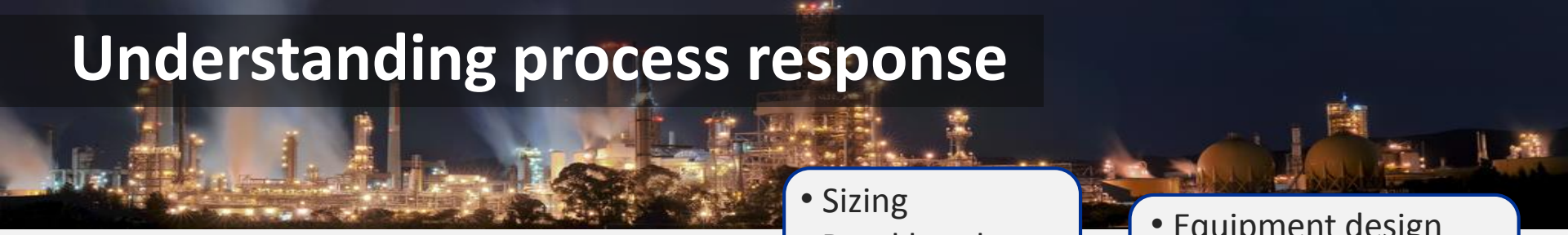
Process interdependencies







Understanding process response



- Sizing
- Dead band
- Flow properties

- Equipment design
- Process design
- Control loops coupling

- Control algorithm
- Controller tuning





- Operating practice
- Control strategy



Set point

Controller

Final control element

Process

Disturbance

- Type
- Duration

Transmitter

- Sampling frequency
- Noise profile
- Filtering



Understanding process response

- Sizing
- Dead band
- Flow properties

- Equipment design
- Process design
- **Control loops coupling**

- Control algorithm
- Controller tuning

- Operating practice
- Control strategy







Set point

Controller

Final control element

Process

Disturbance

- Type
- Duration

Transmitter

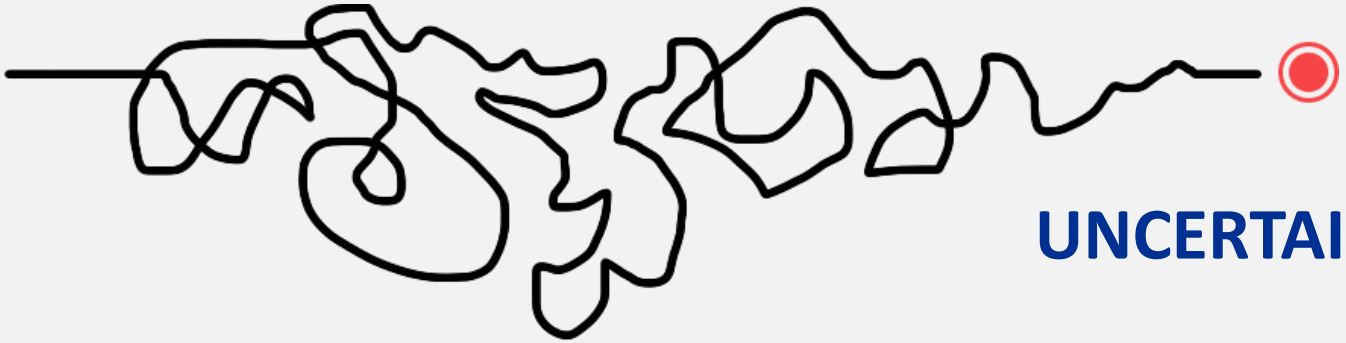
- Sampling frequency
- Noise profile
- Filtering



Have extensively studied

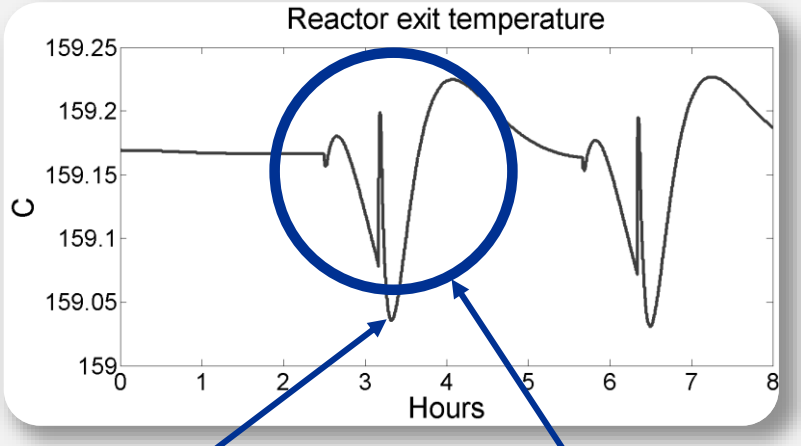
Process control challenges

- 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

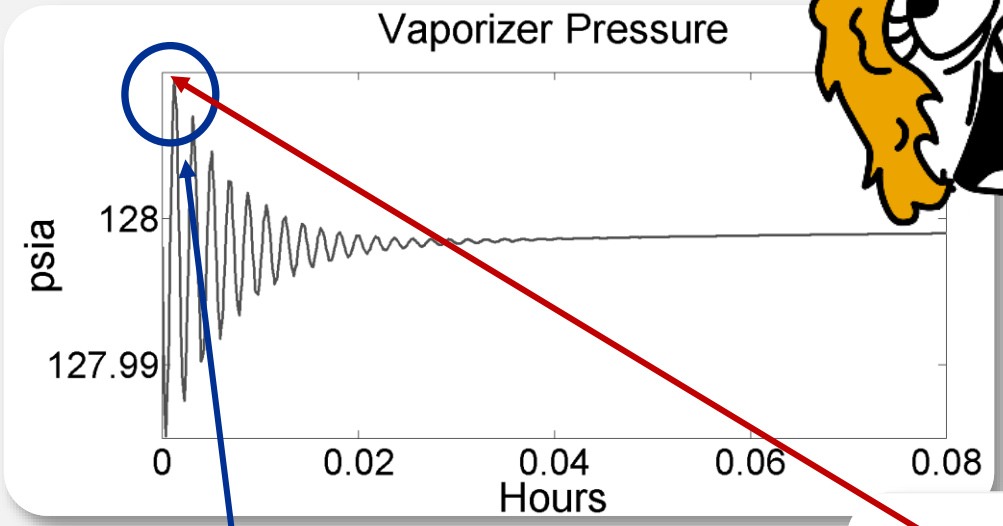


This triggers alarms

Non-liner response

Control loop ringing

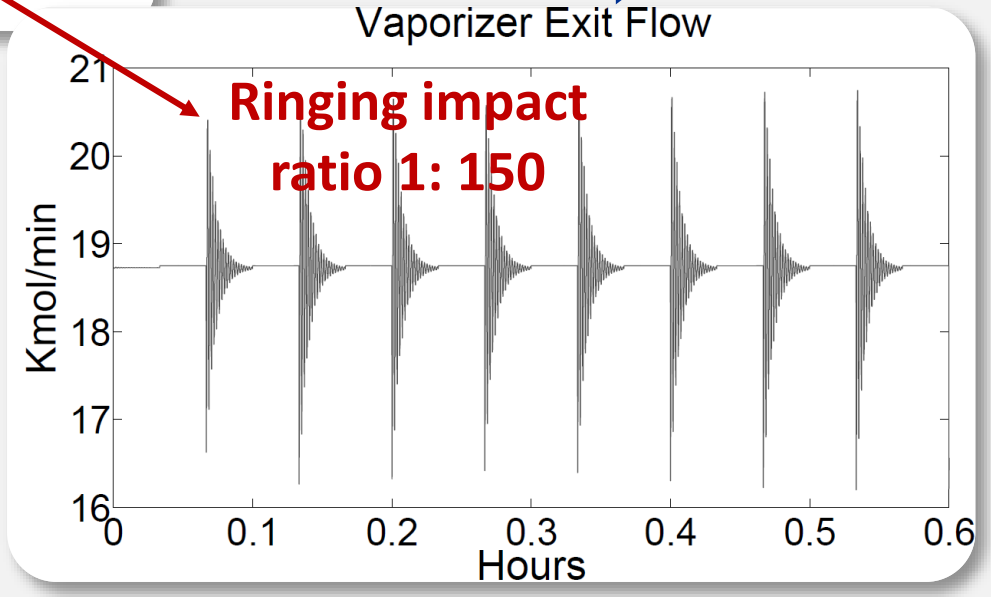




Caused by a negative real controller poles

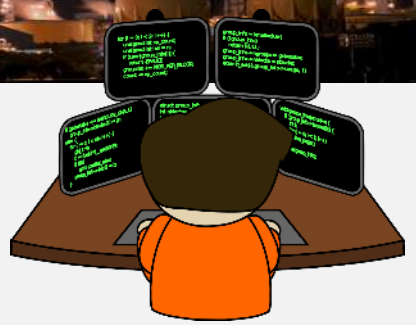
Makes process unstable and uncontrollable

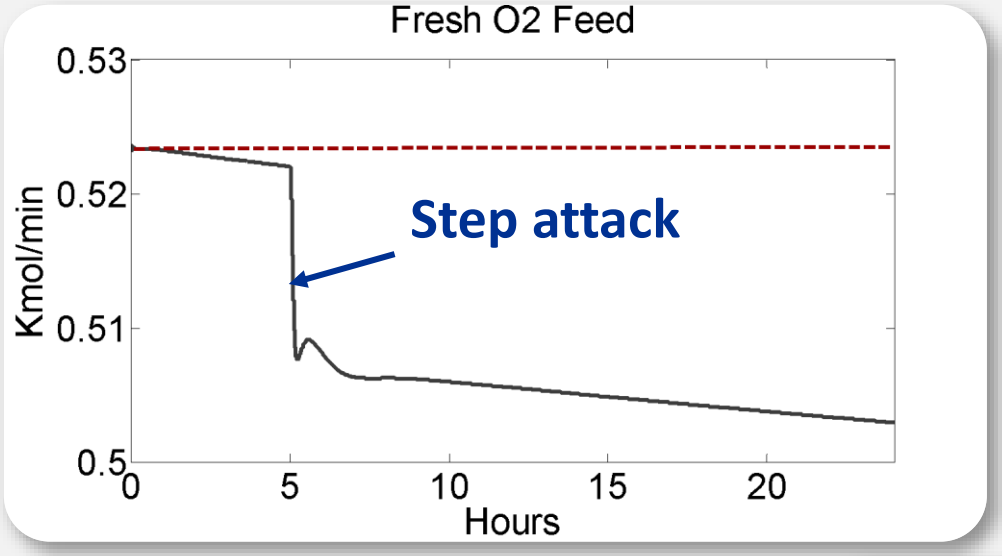
Amount of chemical entering the reactor



Types of attacks



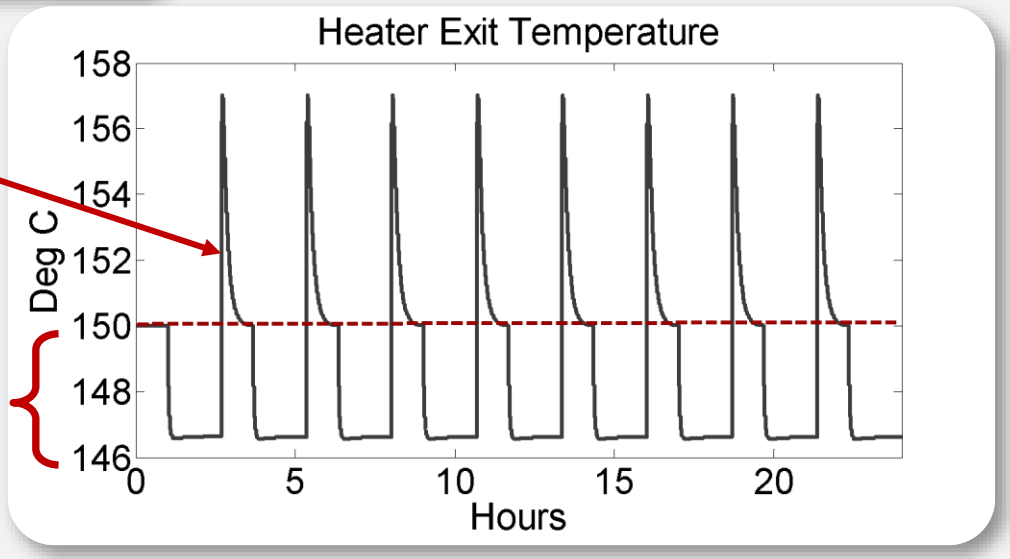




Periodic attack

Recovery time

Magnitude of manipulation



Outcome of the control stage



I am 5’3’’ 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



To persist we shall not bring about alarms

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



Damage



How to break things?



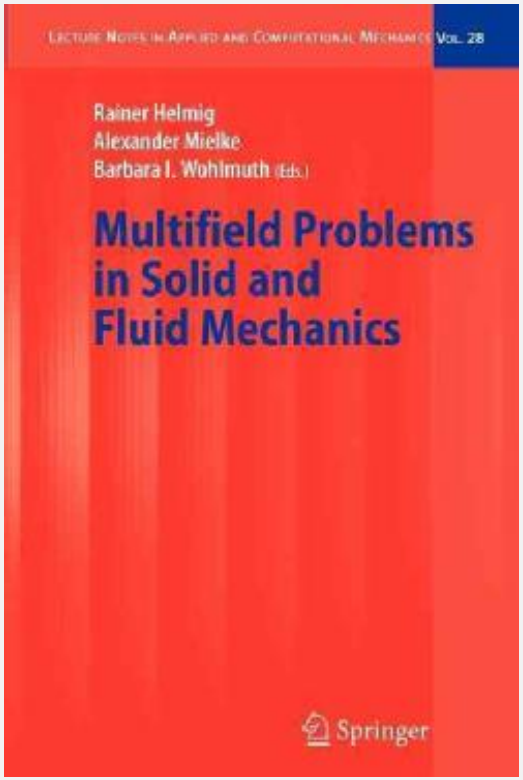
Attacker needs one or more attack scenarios to deploy in final payload

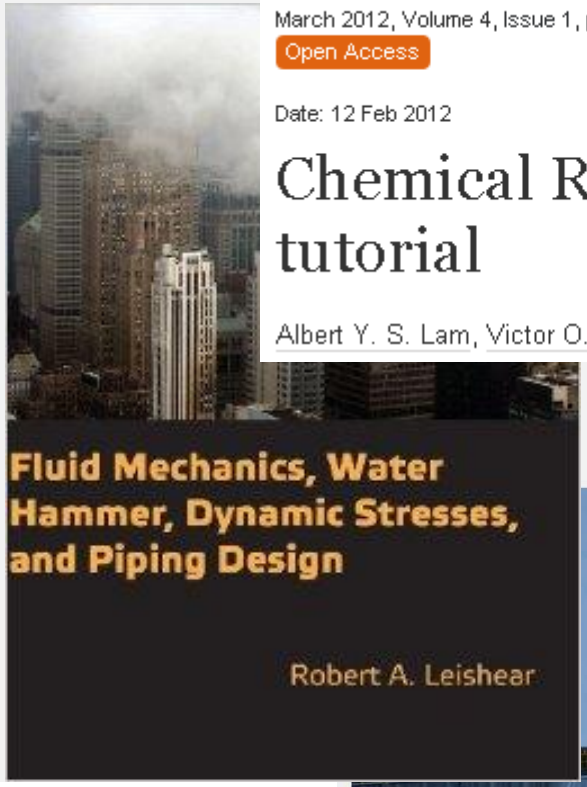
- The least familiar stage to IT hackers
  - In most cases requires input of subject matter experts
- Accident data is a good starting point
  - Governmental agencies
  - Plants' own data bases

OSHA

CSB

How to break things?



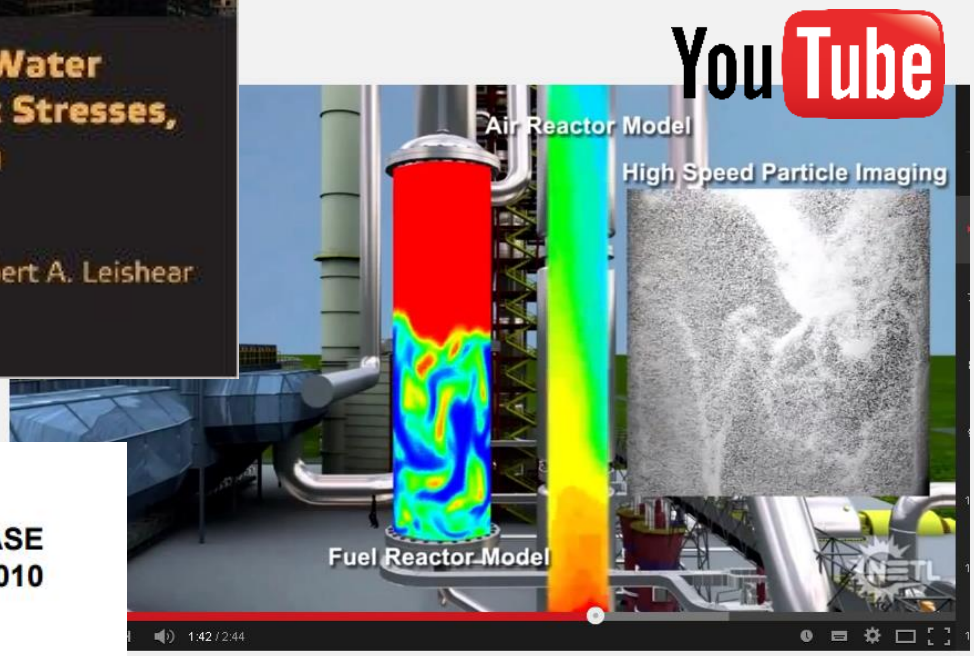


Memetic Computing
March 2012, Volume 4, Issue 1, pp 3-17,
Open Access

Date: 12 Feb 2012

Chemical Reaction Optimization: a tutorial

Albert Y. S. Lam, Victor O. K. Li



INVESTIGATION REPORT



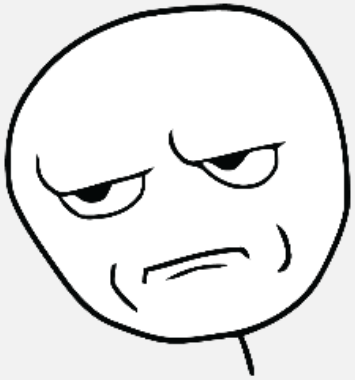
METHYL CHLORIDE RELEASE
JANUARY 22, 2010

hemical Looping Reactor

Hacker unfriendly process



ARE YOU FUCKING KIDDING ME



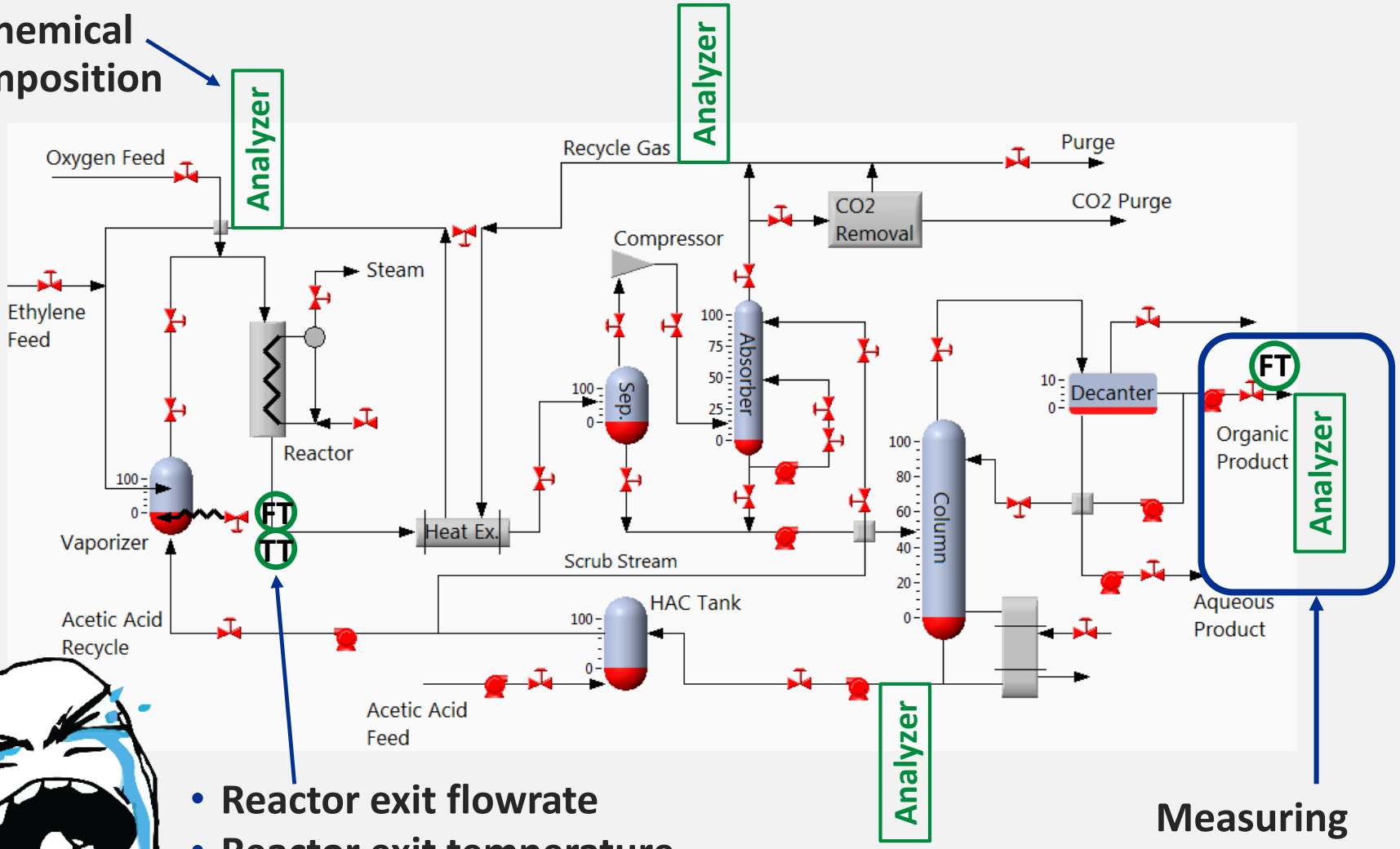
- **Target plant may not have been designed in a hacker friendly way**
  - There may no sensors measuring exact values needed for the attack execution
  - The information about the process may be spread across several subsystems making hacker invading greater number of devices
  - Control loops may be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

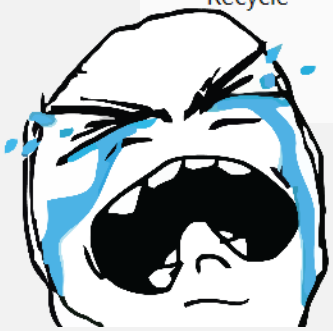


Measuring the process



Chemical composition





- Reactor exit flowrate
- Reactor exit temperature
- No analyzer

Measuring here is too late

Technician vs. engineer

Technician

"It will eventually drain with the lowest holes loosing pressure last"

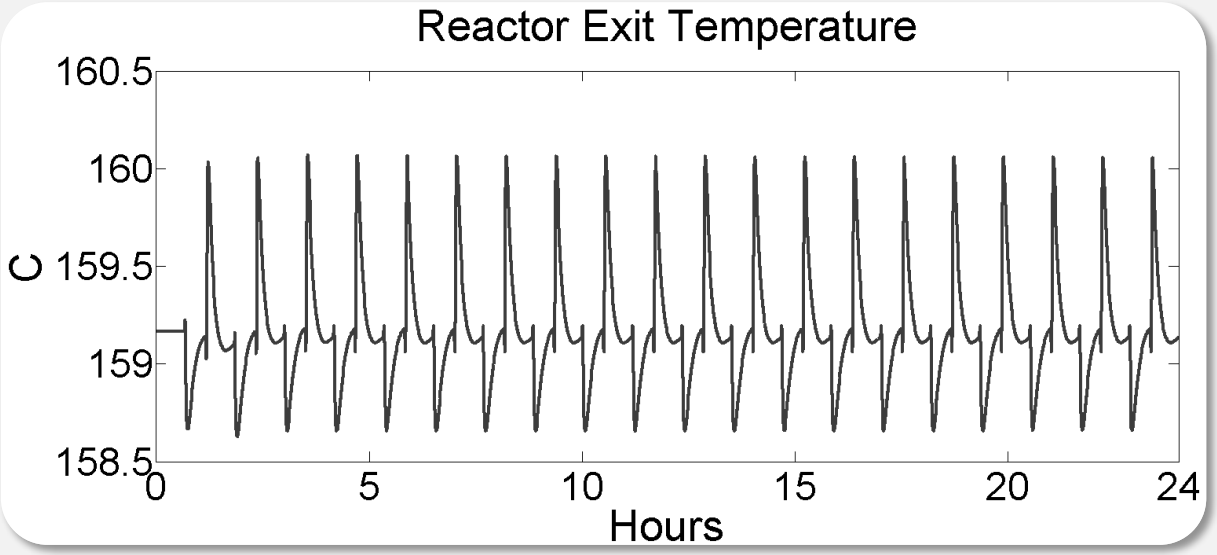


Engineer

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

Technician answer

Usage of proxy sensor





Reactor with cooling tubes

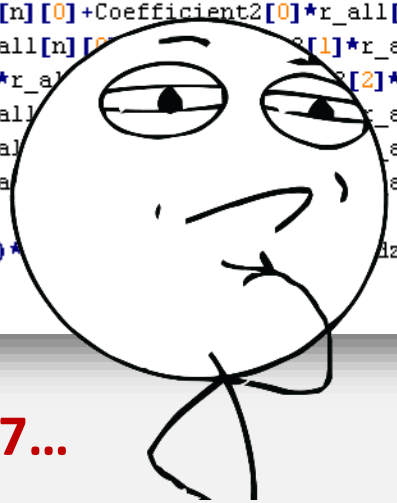
- Only tells us whether reaction rate increases or decreases
- Is not precise enough to compare effectiveness of different attacks

Quest for engineering answer

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

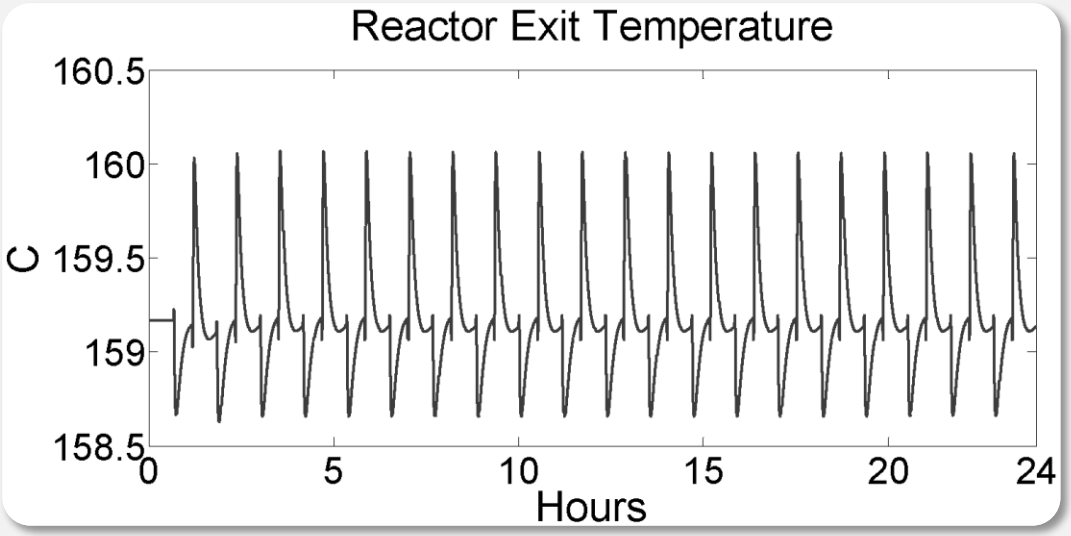
$$(\varepsilon\sum_{k=1}^{7} C_{i,k}Cp_{i,k} + \rho_b Cp_b)\frac{\partial T_i}{\partial t} = -\frac{\partial(v_i\sum_{k=1}^{7}(C_{i,k}Cp_{i,k})T_i)}{\partial z} - \phi_i\rho_b(r_{1,i}E_1 + r_{2,i}E_2) - Q_i^{RCT}$$

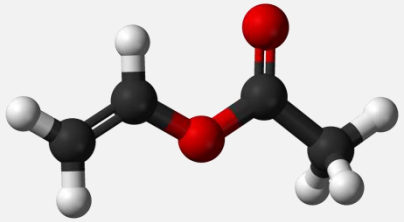
```
/*calculate derivatives*/
for (n=1;n<NR;n++)
{
    /*dC/dt=-delta(C*v)/deltaZ+sum(vij*rj)
    /*Use single backward                                    */
    C_O2_t[n-1]=(-(C_O2[n]*v[n]-C_O2[n-1]*v[n-1])/dz + Coefficient1[0]*r_all[n][0]+Coefficient2[0]*r_all[n][1])/cata_porosity;
    C_CO2_t[n-1]=(-(C_CO2[n]*v[n]-C_CO2[n-1]*v[n-1])/dz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



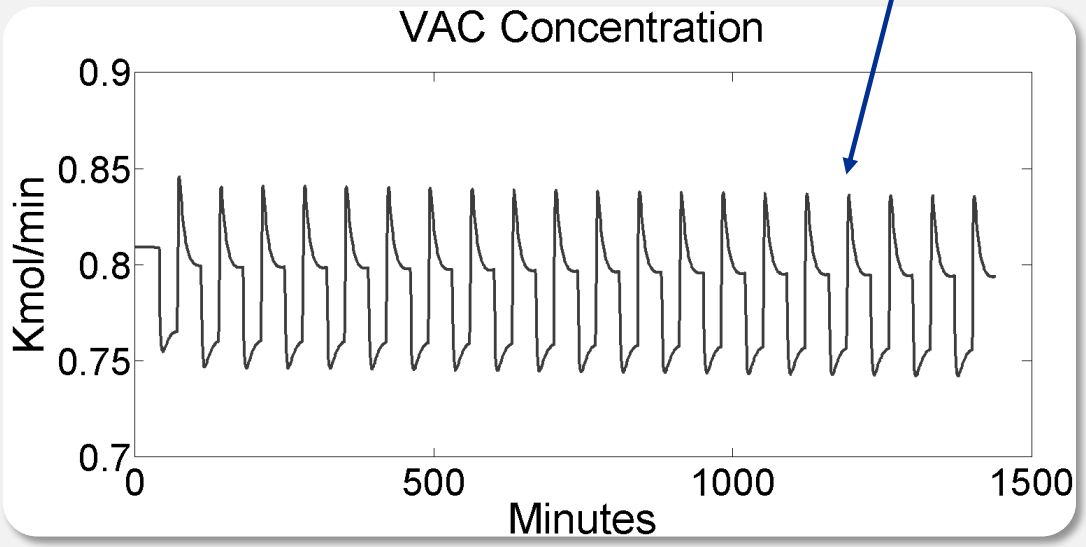
0,00073; 0,00016; 0,0007…

Engineering answer





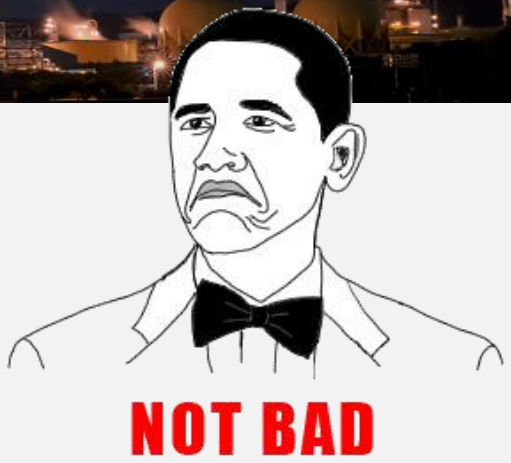
Vinyl Acetate production

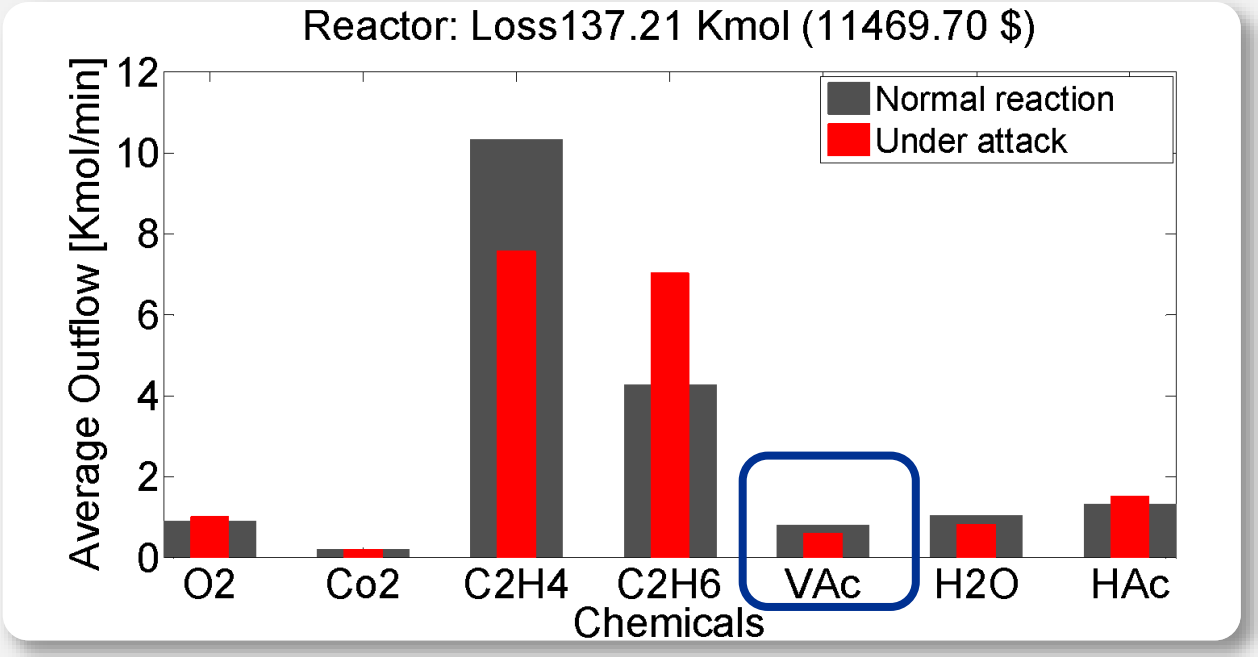


Product loss

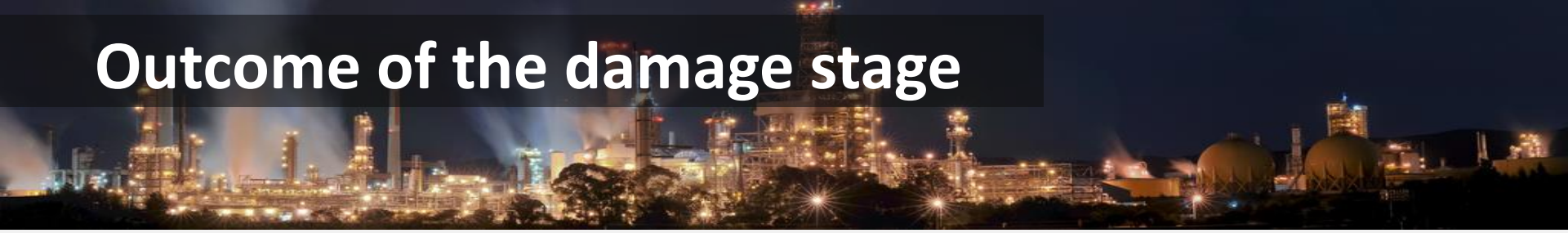
Product per day: 96.000$

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



Clean-up

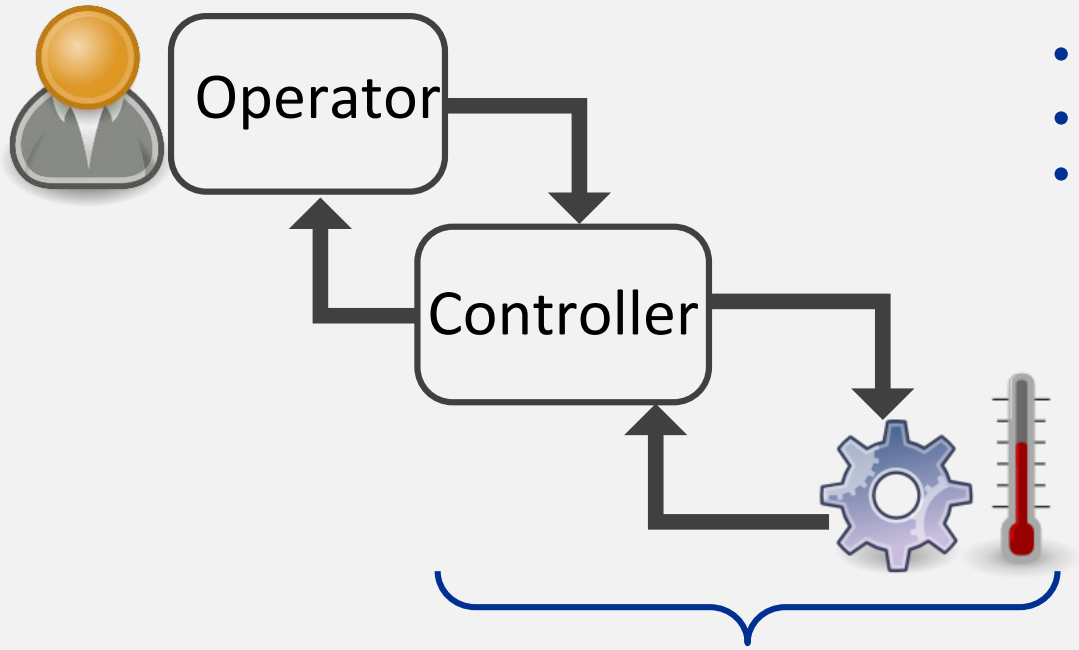


Socio-technical system





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



Creating forensics footprint

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



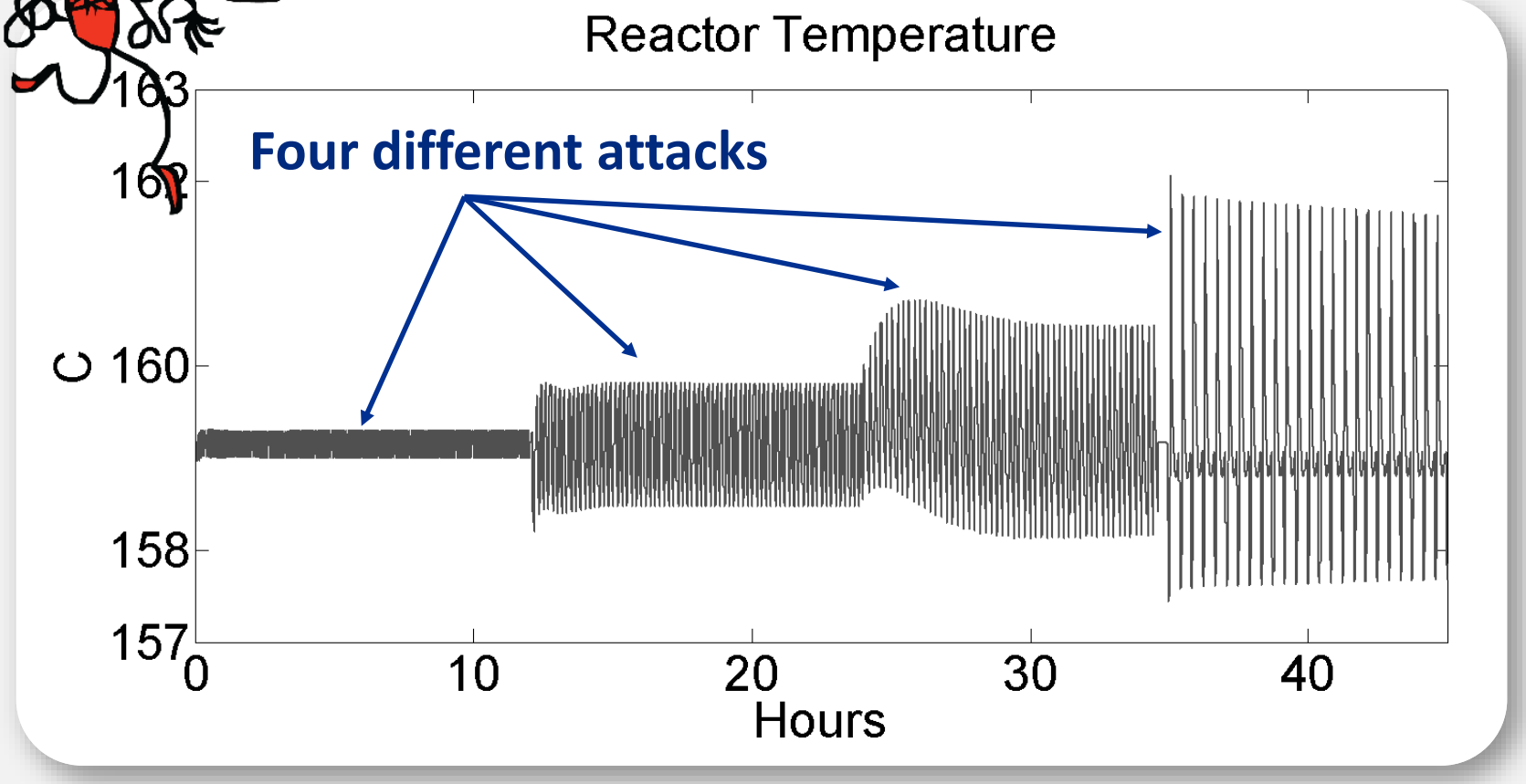
Creating forensics footprint

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

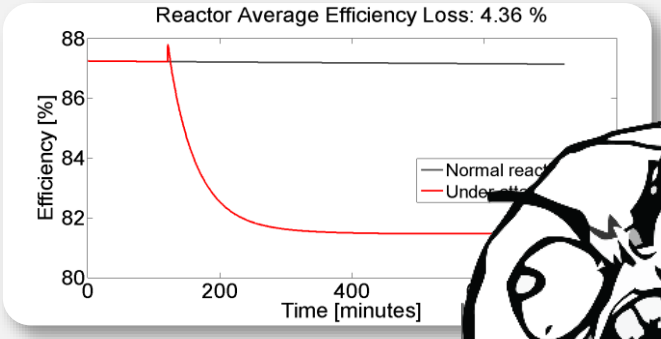


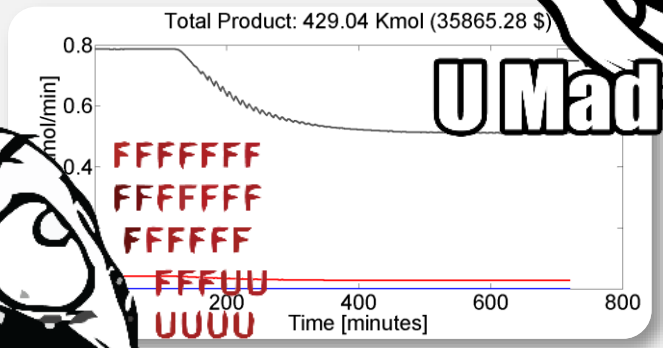


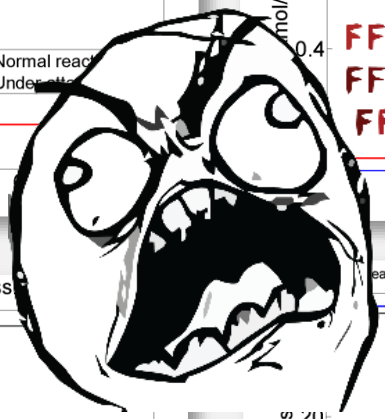
Defeating chemical forensics

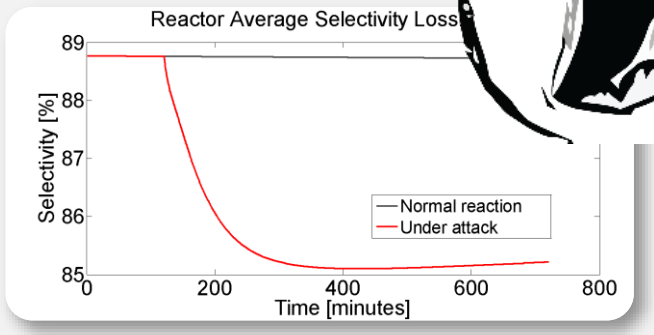
- If reactor doubted, chemical forensics guys will be asked to assist
- Know metrics and methods of chemical investigators
- **Change attack patterns according to debugging efforts of plant personnel**

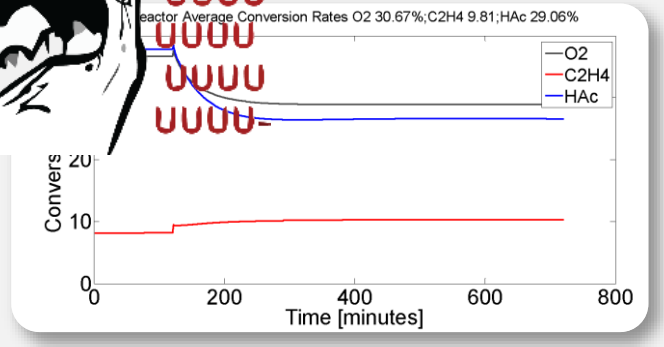


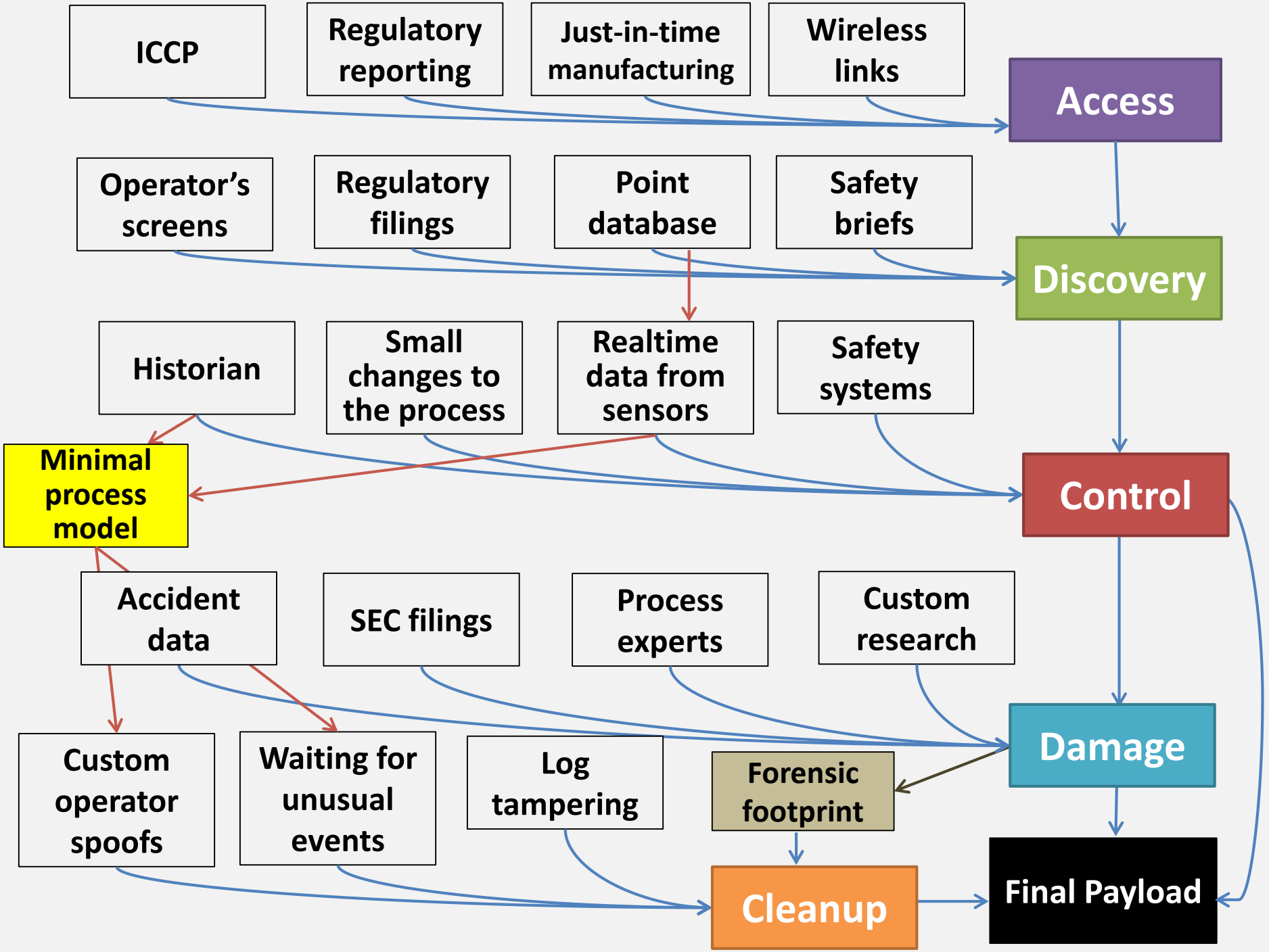








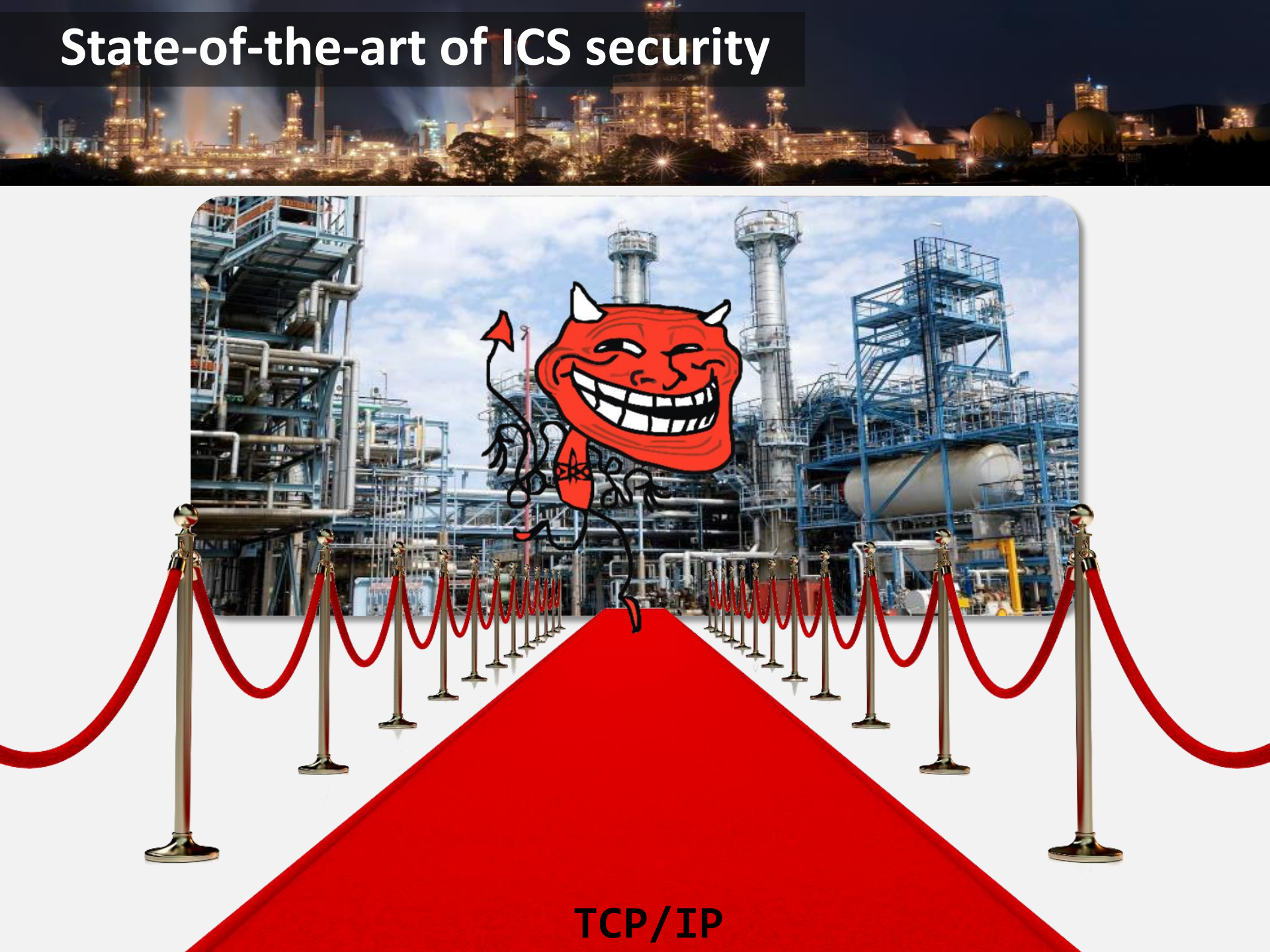



ICCP
Regulatory reporting
Just-in-time manufacturing
Wireless links
Access
Operator's screens
Regulatory filings
Point database
Safety briefs
Discovery
Historian
Small changes to the process
Realtime data from sensors
Safety systems
Minimal process model
Control
Accident data
SEC filings
Process experts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



Afterword

State-of-the-art of ICS security



Food for thought



- **Cost of attack can quickly exceed cost of damage**
  - Hacking into large number of devices
  - Suppression of alarms and process data spoofing
  - Badly behaved control loops , synchronization of actions
- **Each process is unique, but…**
  - There are instances of attacks applicable to wide range of scenarios
  - **SCADA payloads for Metasploit is just a matter of time**

Dream BIG

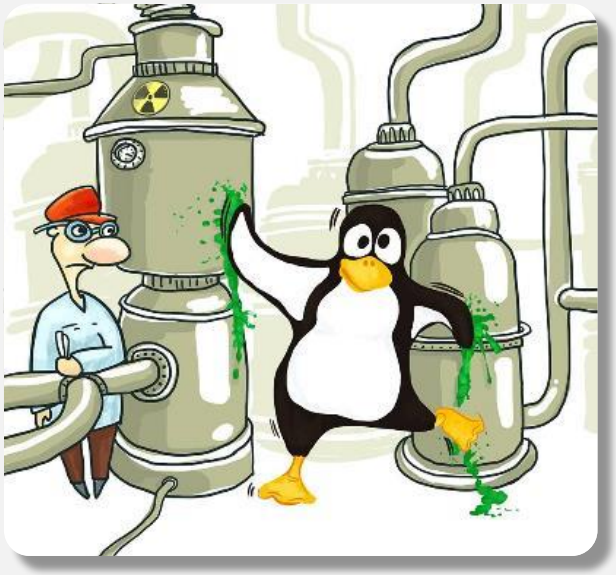


Evil villains from James Bond movies unite! Go forth and start building your evil lairs.









Thank you

marina.krotofil@tuhh.de

jason.larsen@ioactive.com

Damn Vulnerable Chemical Process

TE: http://github.com/satejnik/DVCP-TE
VAM: http://github.com/satejnik/DVCP-VAM