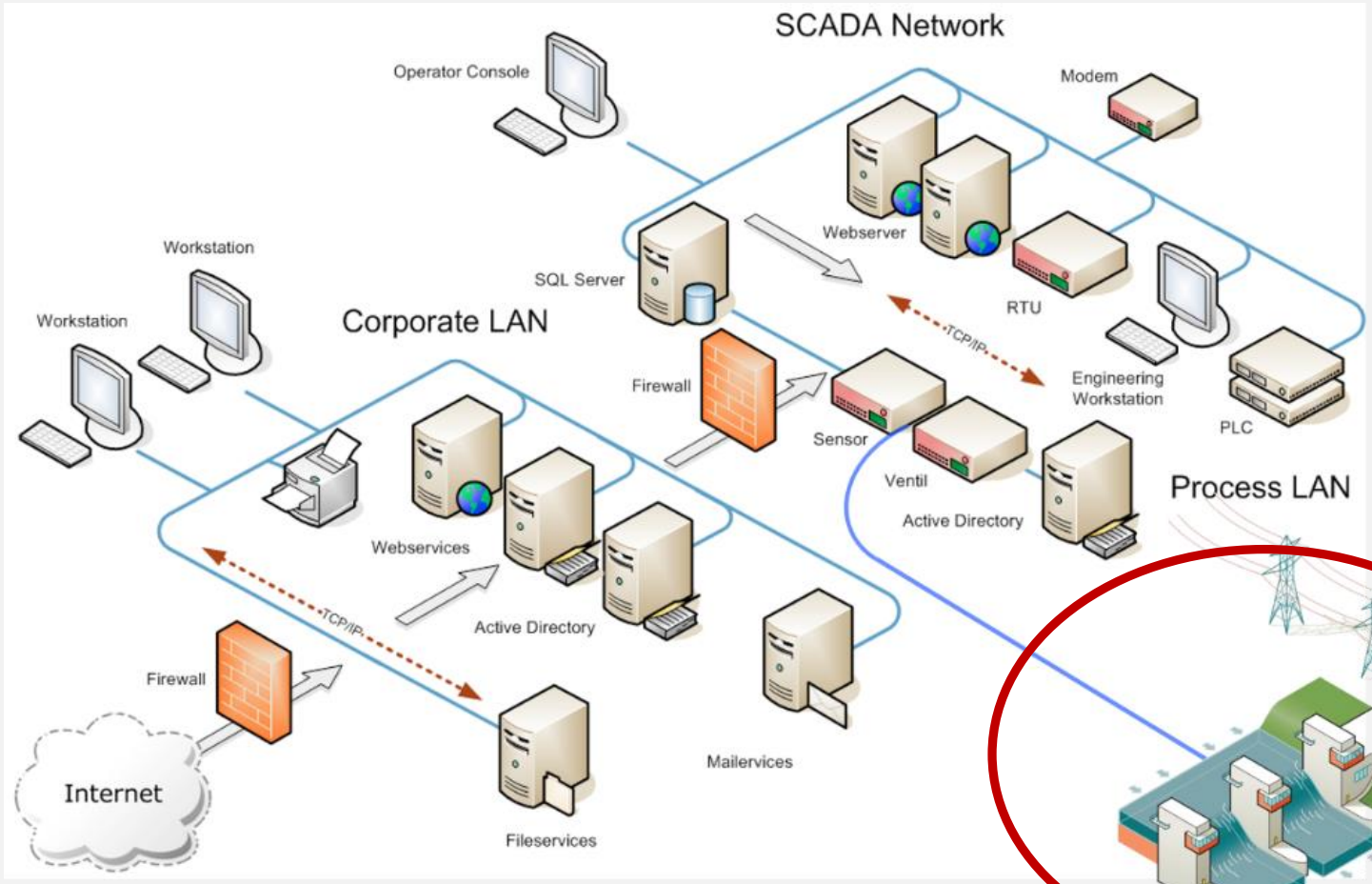
Rocking the Pocket Book: Hacking Chemical Plants for Competition and Extortion

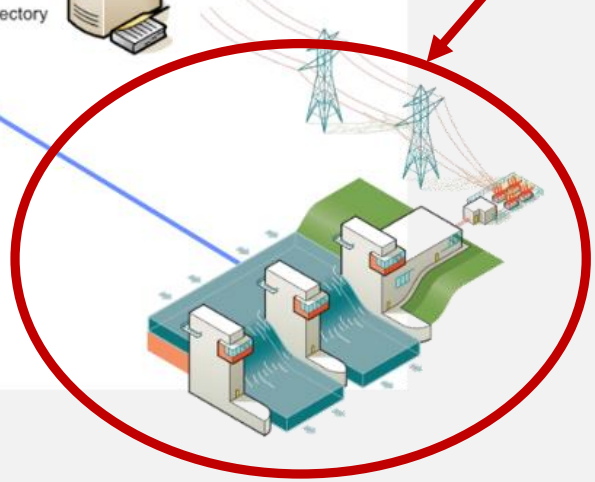
Marina Krotofil

Black Hat, Las Vegas, USA
06.08.2015

Industrial Control Systems (aka SCADA)



Physical application



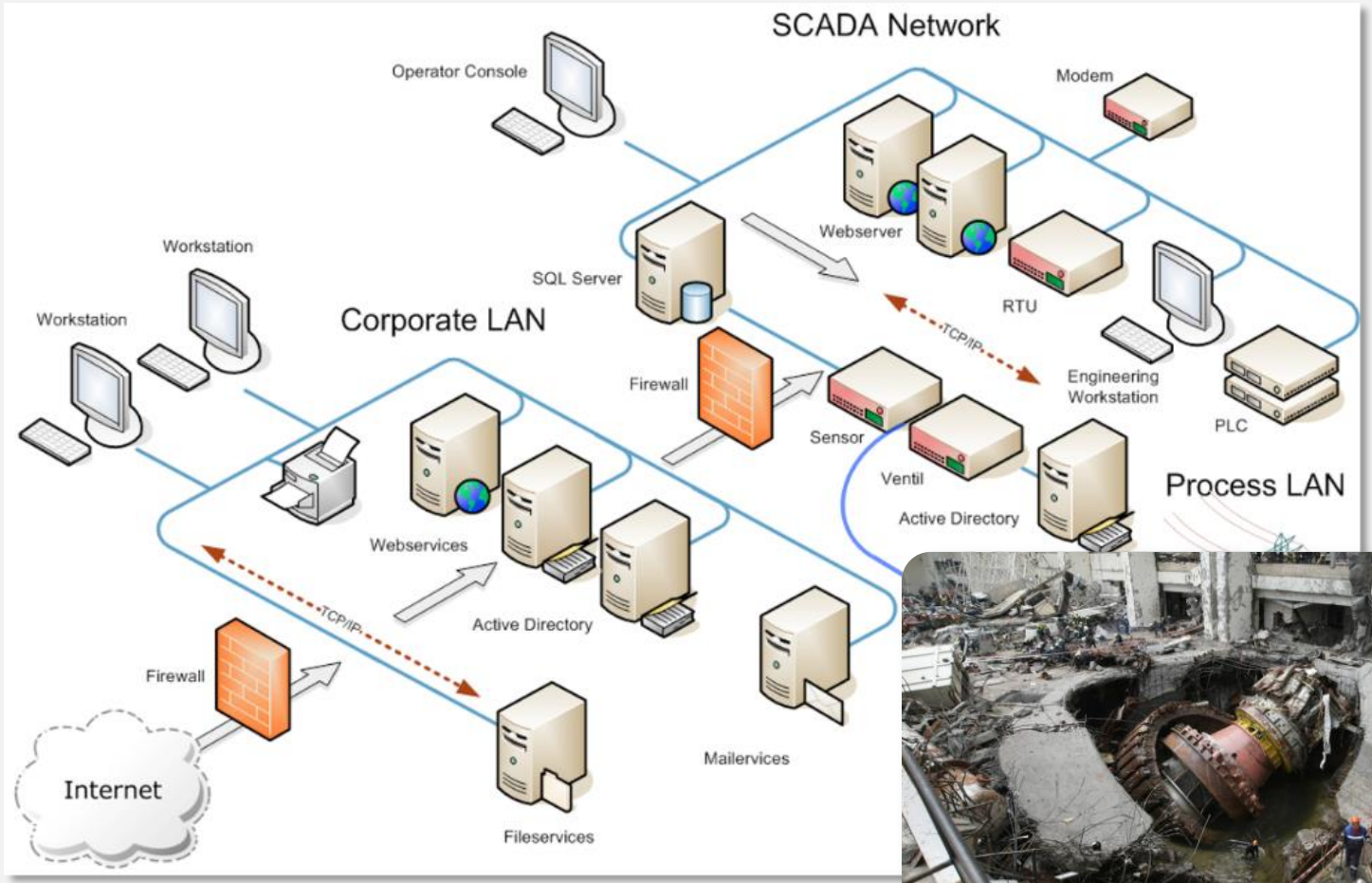
Curtesy: Compass Security Germany GmbH

Cyber-physical systems

Cyber-physical systems are IT systems “embedded” in an application in the physical world

Interest of the attacker is in the physical world

Industrial Control Systems



Control systems security

Ralph Langner: “The pro’s don’t bother with vulnerabilities; they use features to compromise the ICS”

My research focus

- Complex continuous processes (e.g. chemical plants)
- Non-opportunistic attacker
- I do not research into (but consider) cyber vulnerabilities in communication protocols and control equipment

- What the attacker can do to the process?
- What she needs to do and why?
- What needs to be programmed into a final payload?
- Are traditional cyber-security measures adequate?

Security science

Security is not a fundamental science

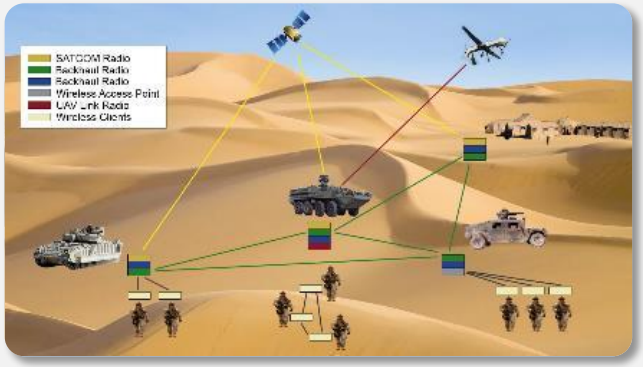
It is application driven

Security solutions exist in the context of the application

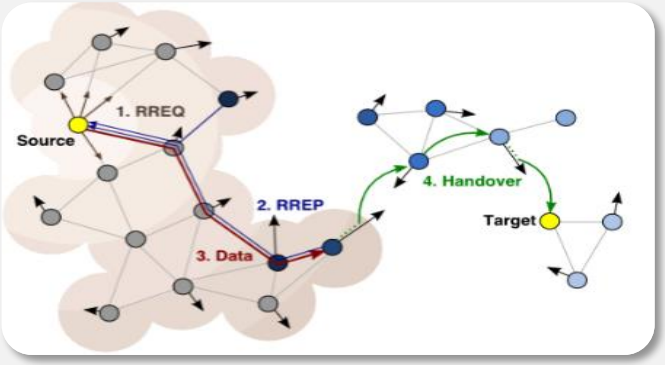
Early adopter: E-commerce

- **Security influences design decisions**
  - Attackers (mis)use functionality of web browsers
  - Novel approaches to designing web applications
  - Novel security controls in browsers
- **Application dictates security properties**
  - Information-theoretic security properties
  - CIA triad → Parkerian hexad

Failed to adopt

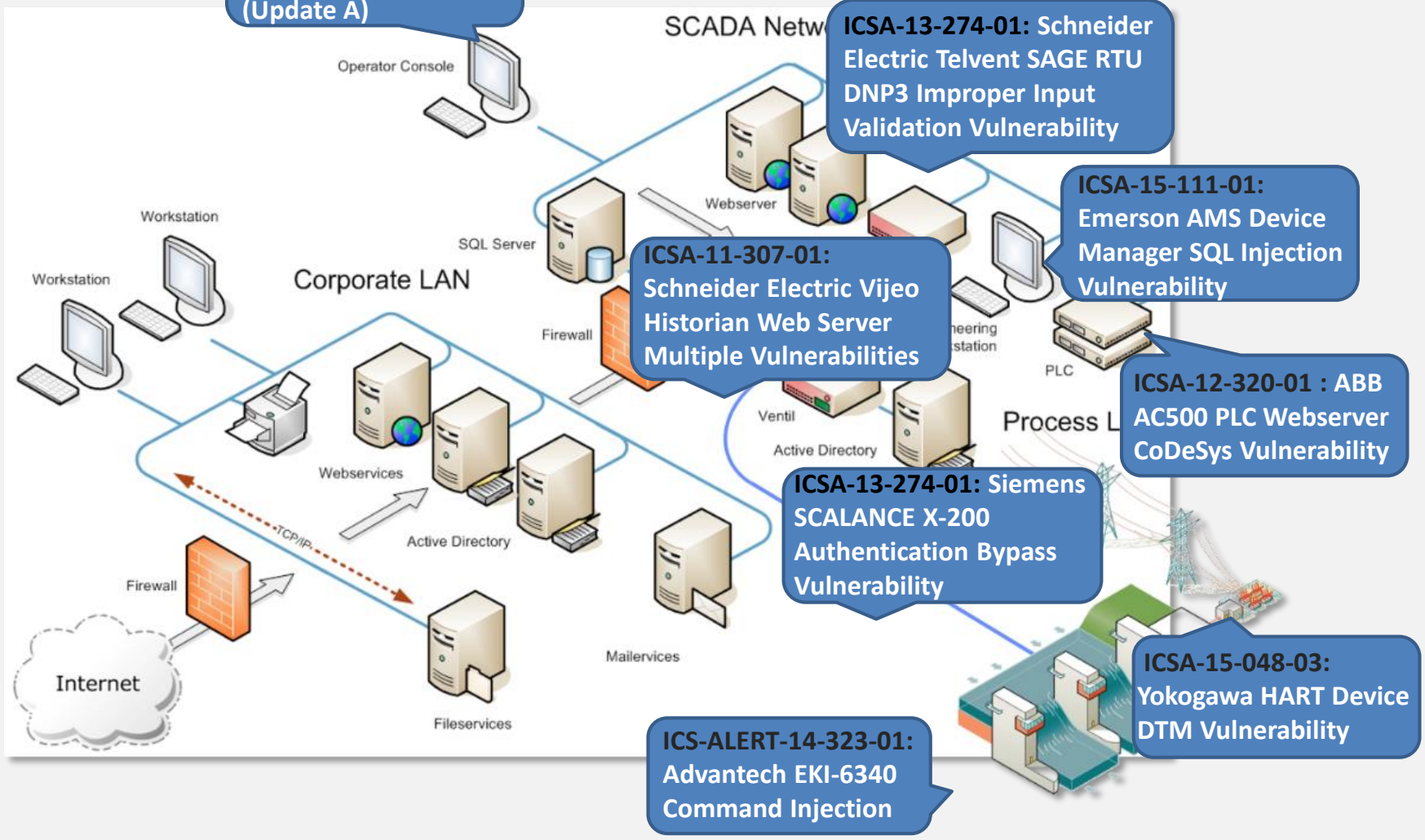


- **Wireless sensor networks**
  - A big hype for about a decade
  - Conferences, solutions, promising applications
  - Remained a “promising” technology with limited deployment
- **Downfall reasons**
  - Deficiencies in the attacker models and security requirements
  - Unrealistic assumptions about physics of wireless communication



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

Control equipment vulnerabilities



ICS-CERT recommendation

ICSA-13-274-01: Siemens SCALANCE X-200 Authentication Bypass Vulnerability

IMPACT

Successful exploitation of this vulnerability may allow attackers to perform administrative operations over the network without authentication.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

Impact evaluation

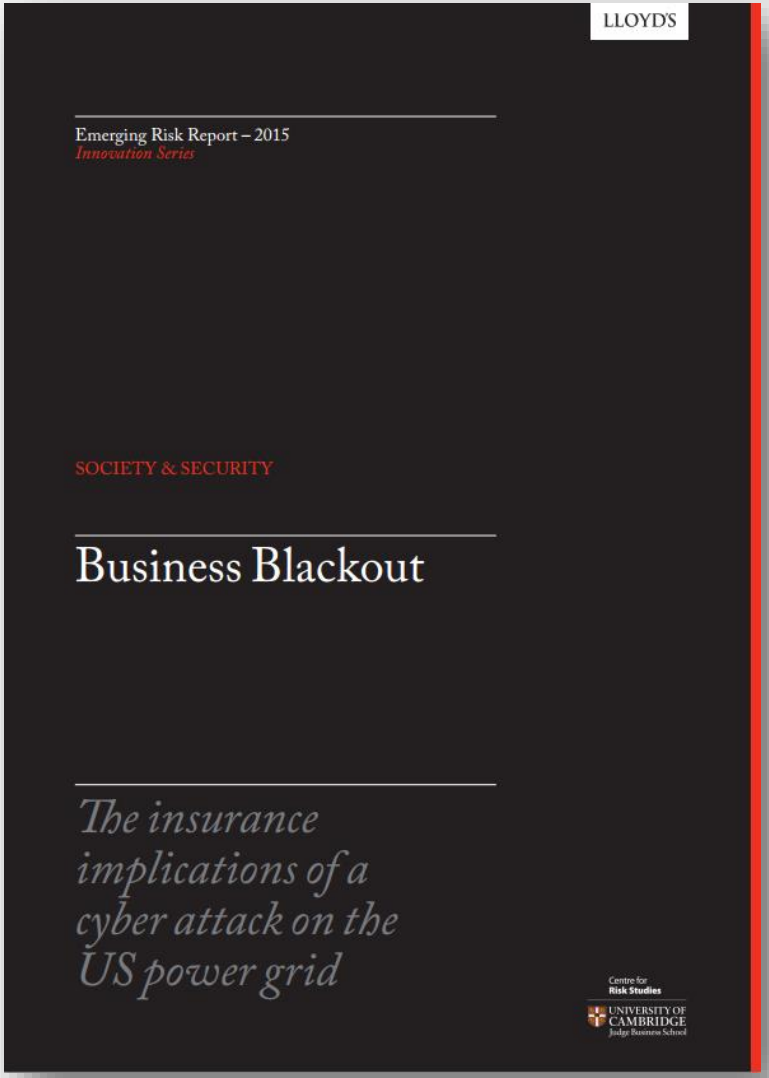
- What exactly the attacker can do with the vulnerability?
- Any further necessary conditions required?
- How severe the potential physical impact?

Answering these questions requires understanding how the attacker interacts with the control system and the process

Incident data unavailability

- Due to various schemes for reputation management and data sharing laws, the majority of Operational Technology attacks over the last 20 years have not been made public, making even a catalogue of recent reference events difficult to assemble.
- A key requirement for an insurance response to cyber risks will be to enhance the quality of data available and to continue the development of probabilistic modelling.

We can and should conduct own research on cyber-physical exploitation



Control systems security

Control system design flaw

1 **Industrial systems can be controlled without modifying the contents of the messages**

- This can be effective even if the traffic is signed or even encrypted

Overlooked data security property

2 **Process data can be spoofed to make it look like everything is normal**

- This can be done despite all traditional communication security put in place

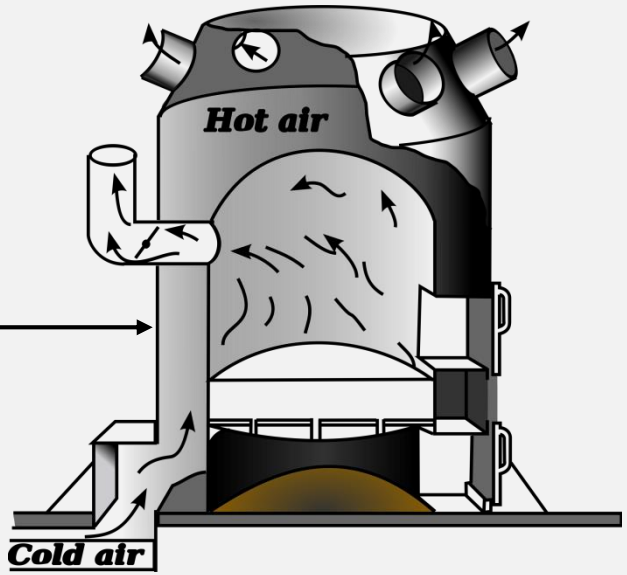
M. Krotofil, J. Larsen. What You Always Wanted and Now Can: Hacking Chemical Processes. Hack in the Box, Amsterdam (2015)

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

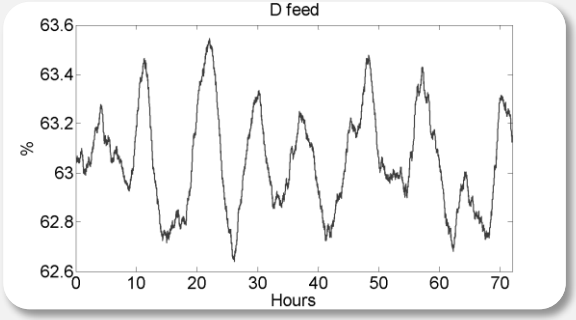
Adjust themselves to influence process behavior

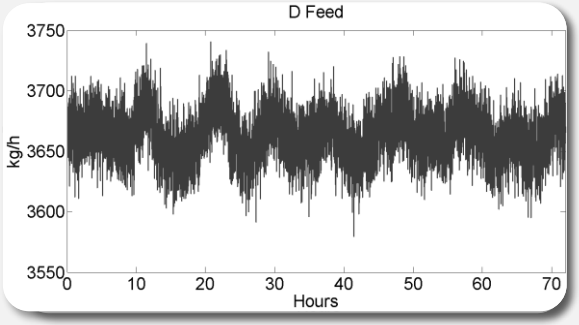
Sensors

Measure process state

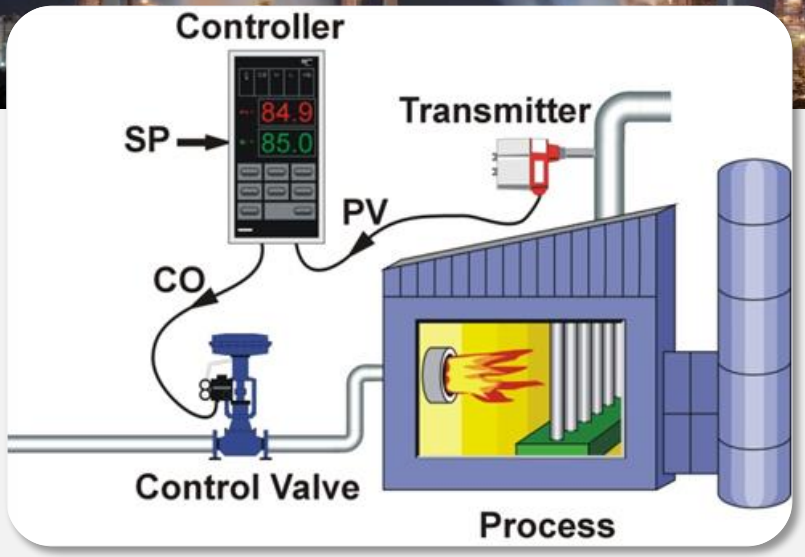
Control system

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

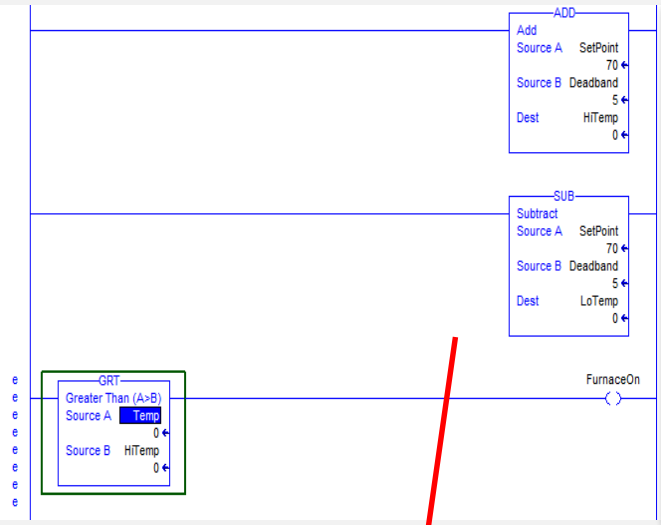
- In large –scale operations control logic gets more complex than a thermostat
- One would need something bigger than a thermostat to handle it
- Most of the time this is a programmable logic controller (PLC)

PLC internals

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

Sensors

Inputs

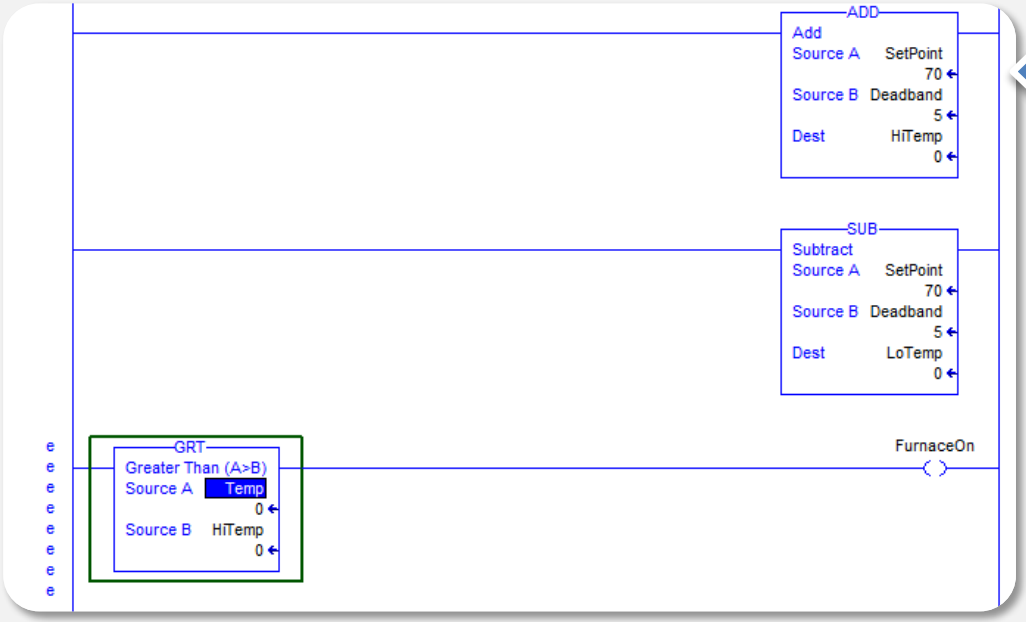


Outputs

Actuators

Control logic

- It is programmed graphically most of the time

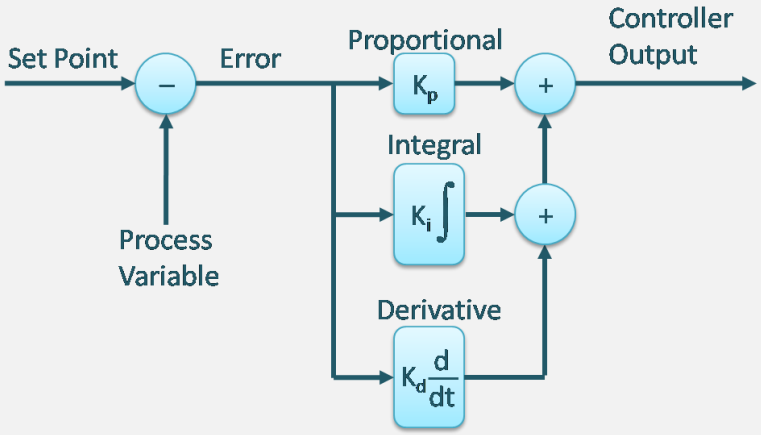


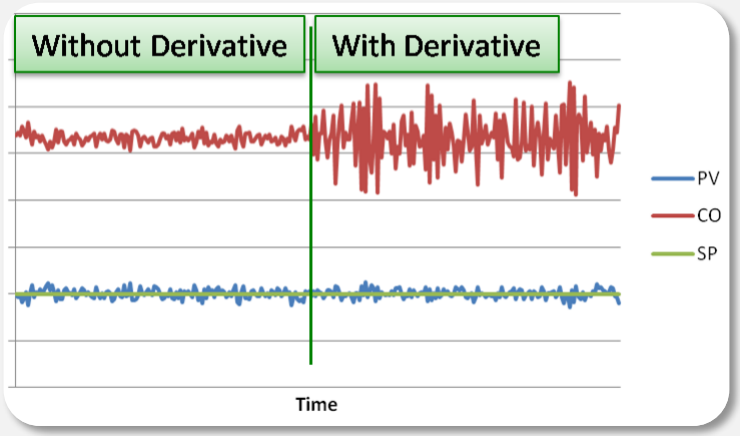
Note to the control guys: logic and given examples do not match, they picked randomly. Thank you for noticing ;-)

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
- Full PID control is mostly used for tight control (e.g. temperature in the reactor)

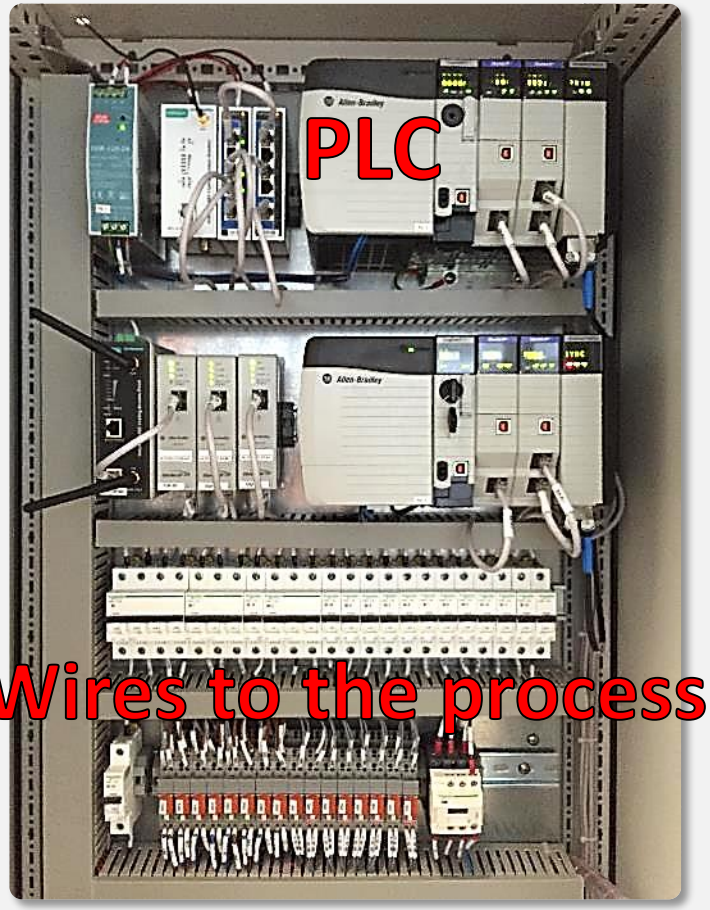
Jacques Smuts „Process Control for Practitioners“

Field communication

Communication media

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

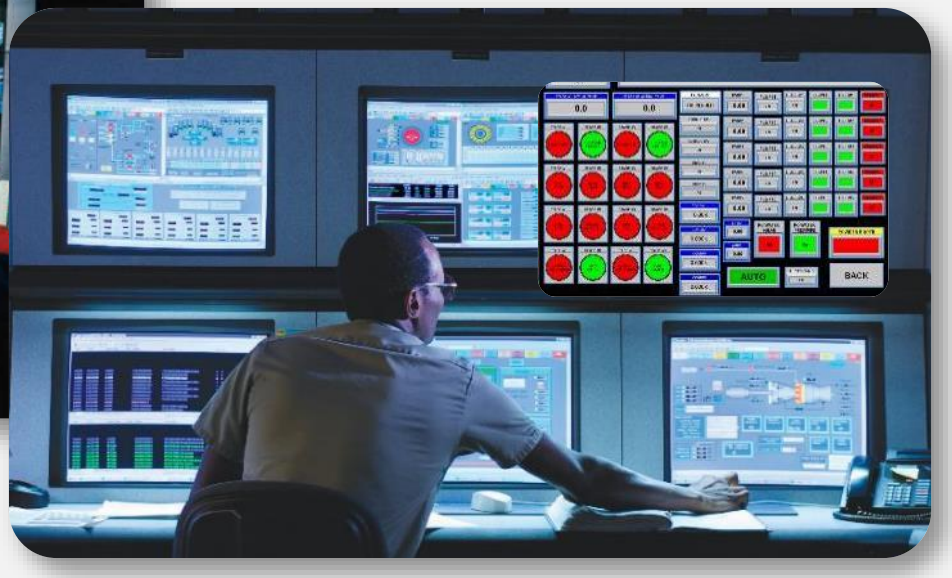
Usually process values are scaled into meaningful data in the PLC



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 crucial task: resolution of alarms**



SCADA hacking

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.**

Why to attack ICS

Source: simentari.com

Attack goal: persistent economic damage

Here's a plant. Go hack it.

What can be done to the process

Equipment damage

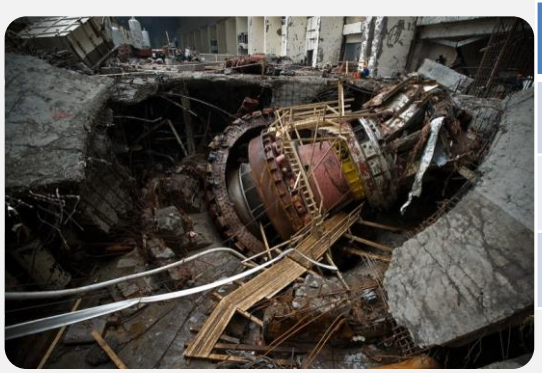
- Equipment overstress
- Violation of safety limits

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

- **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 (-)

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

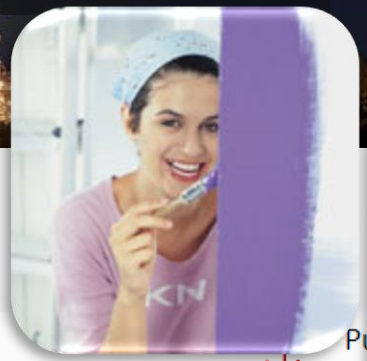
More plants offers:
http://www.usedplants.com/

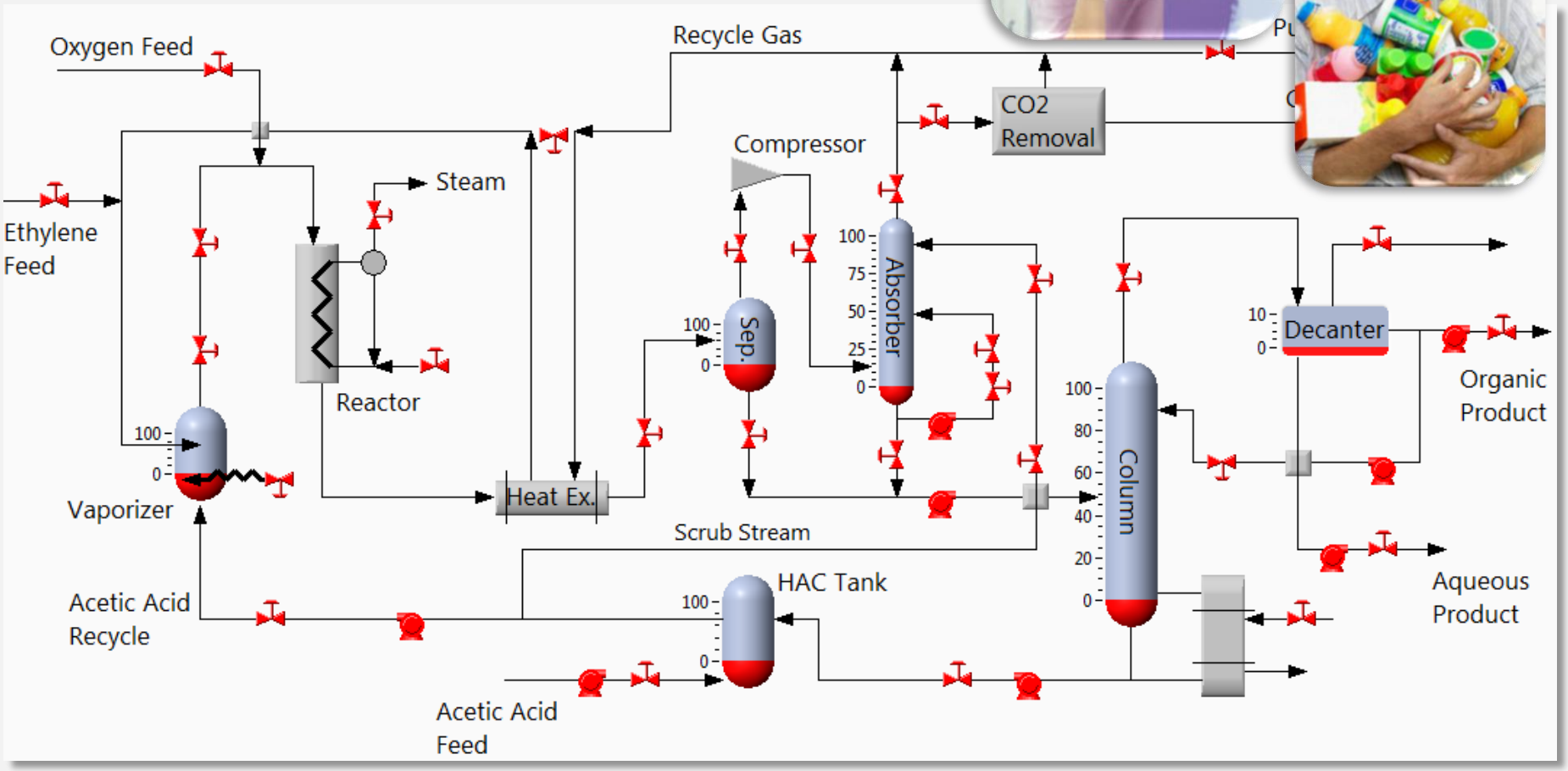
Car vs. plant hacking

It is not about the size

It is about MONEY
Plants are ouch! how expensive

Vinyl Acetate Monomer plant (model)



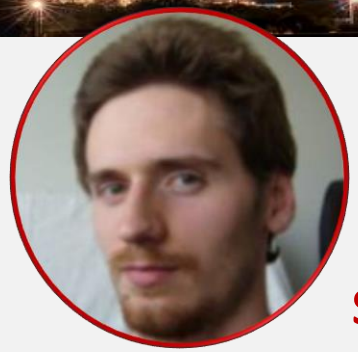


Acknowledgement

Behind great woman is a great man

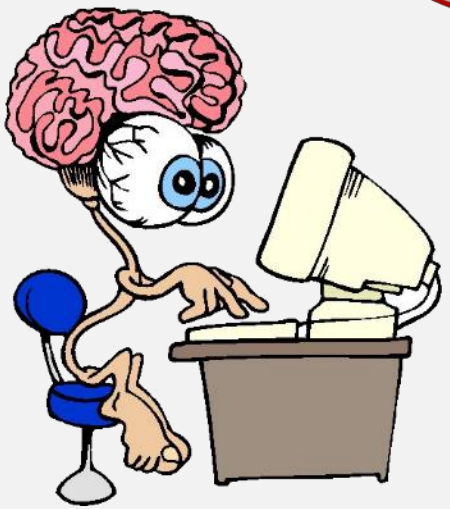
Acknowledgement

Process Automation Consultant



Student

Cyber-physical hacker



Chemical Engineer

Professor

Programmer

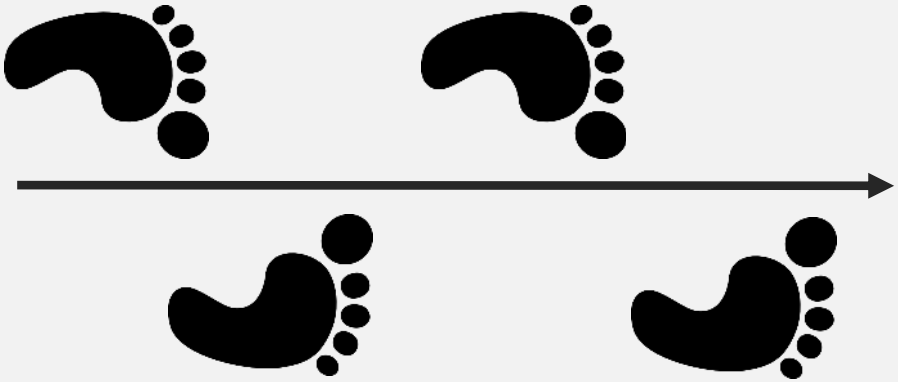
Acknowledgement

- Alexander Isakov – awesome programmer
- Alexander Winnicki – very good student
- Dieter Gollmann – most supportive professor
- Jason Larsen – cyber-physical hacking guru
- Pavel Gurikov – chemical engineer who believes in hackers
- William Horner – experienced automation expert

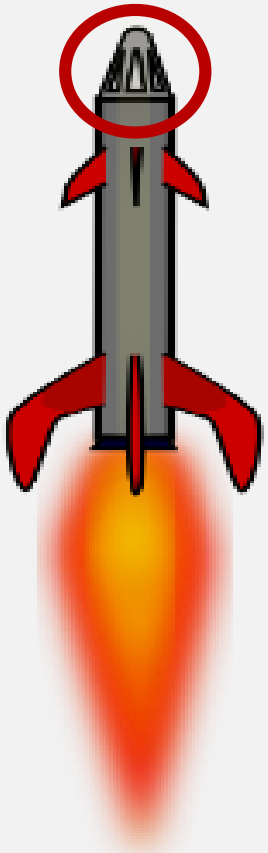
Stages of cyber-physical attacks

Attack payload

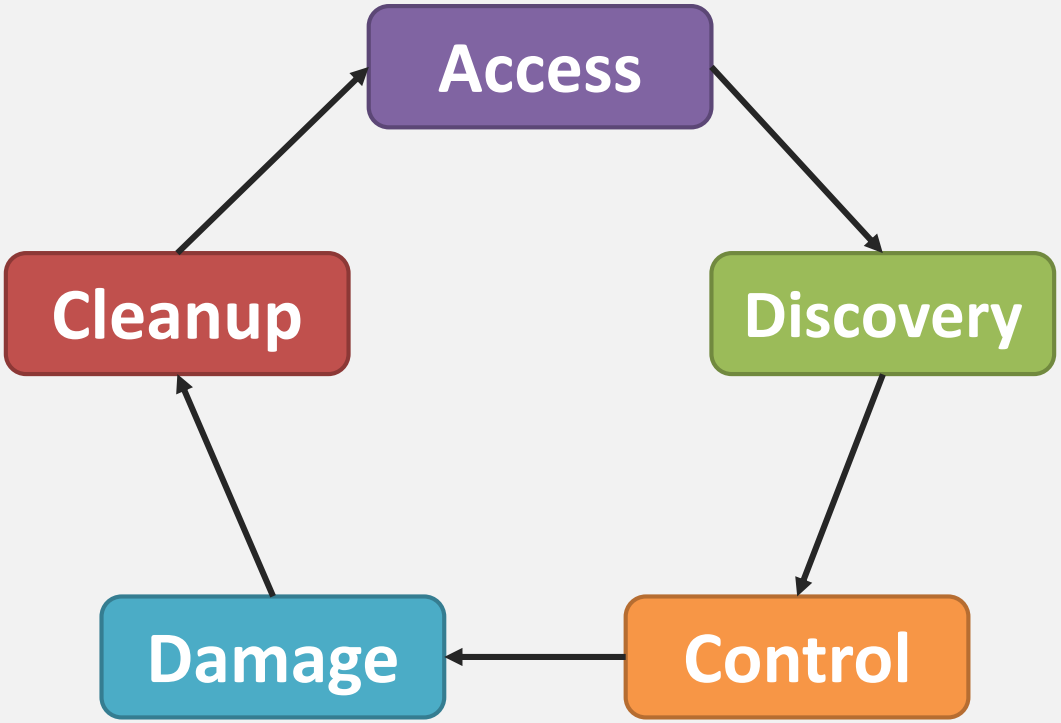
Attack objective



Cyber-physical payload

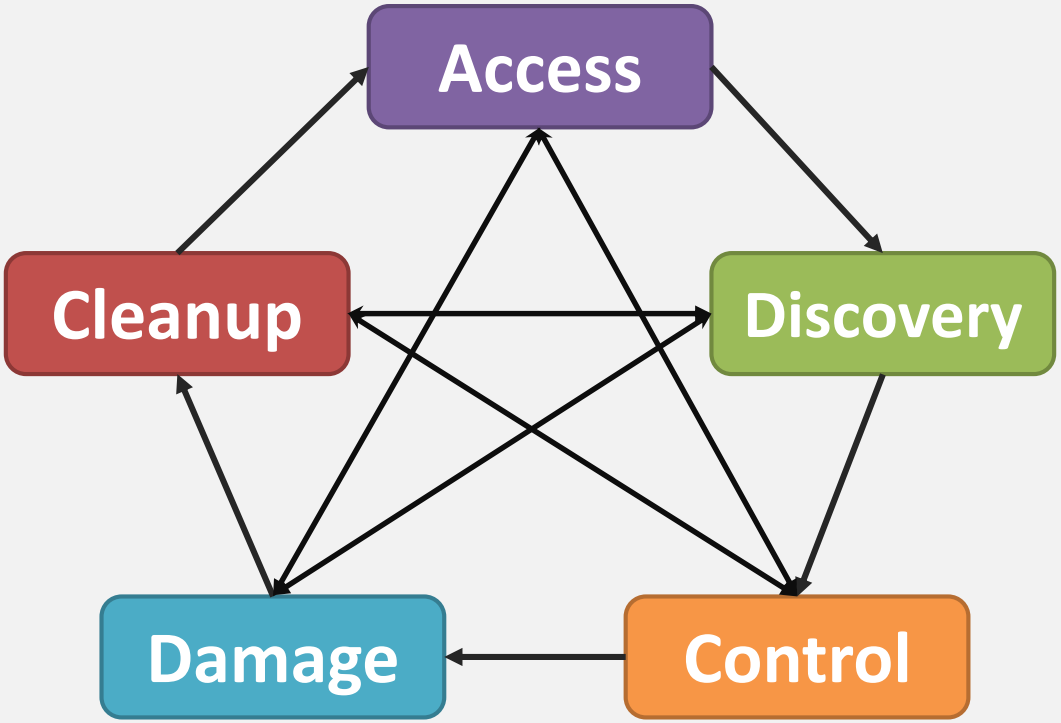


Stages of SCADA attack

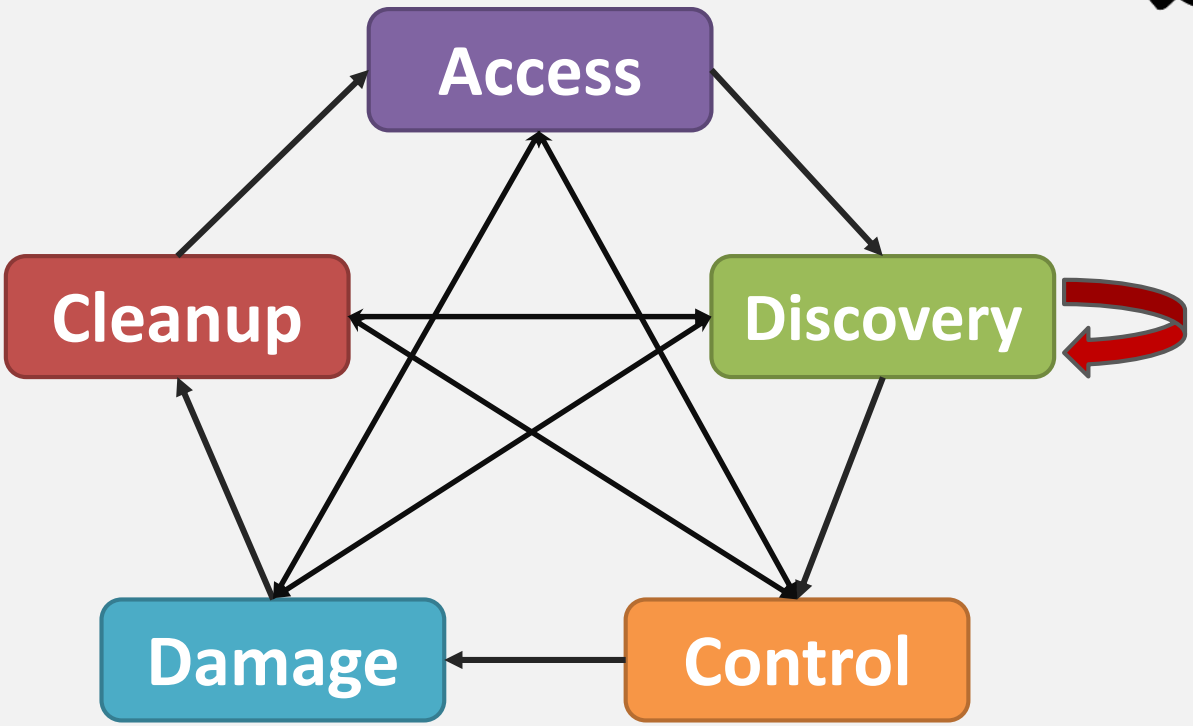


J. Larsen. Breakage. Black Hat Federal (2007)

Stages of SCADA attack



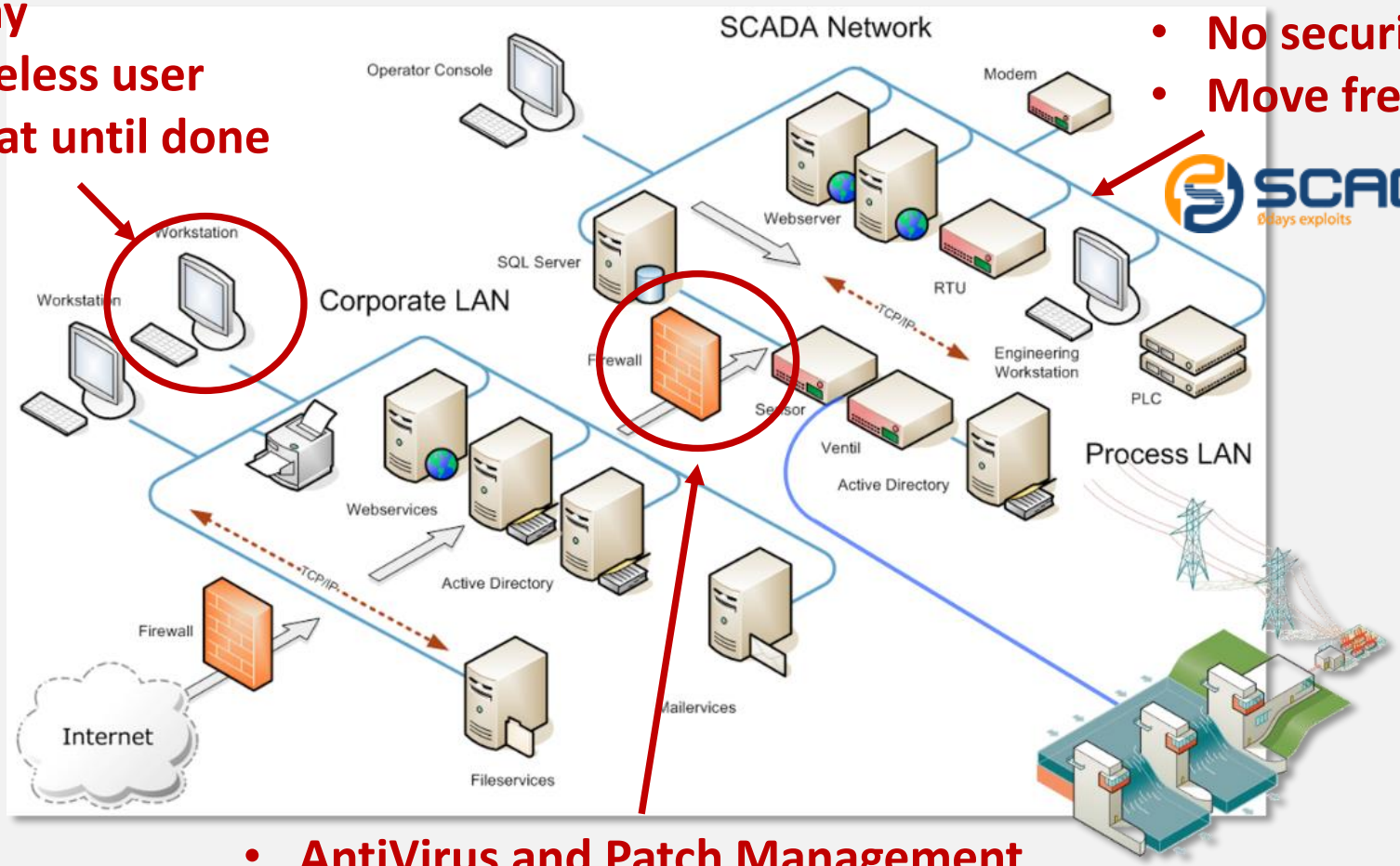
Stages of SCADA attack



Access

Traditional IT hacking

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



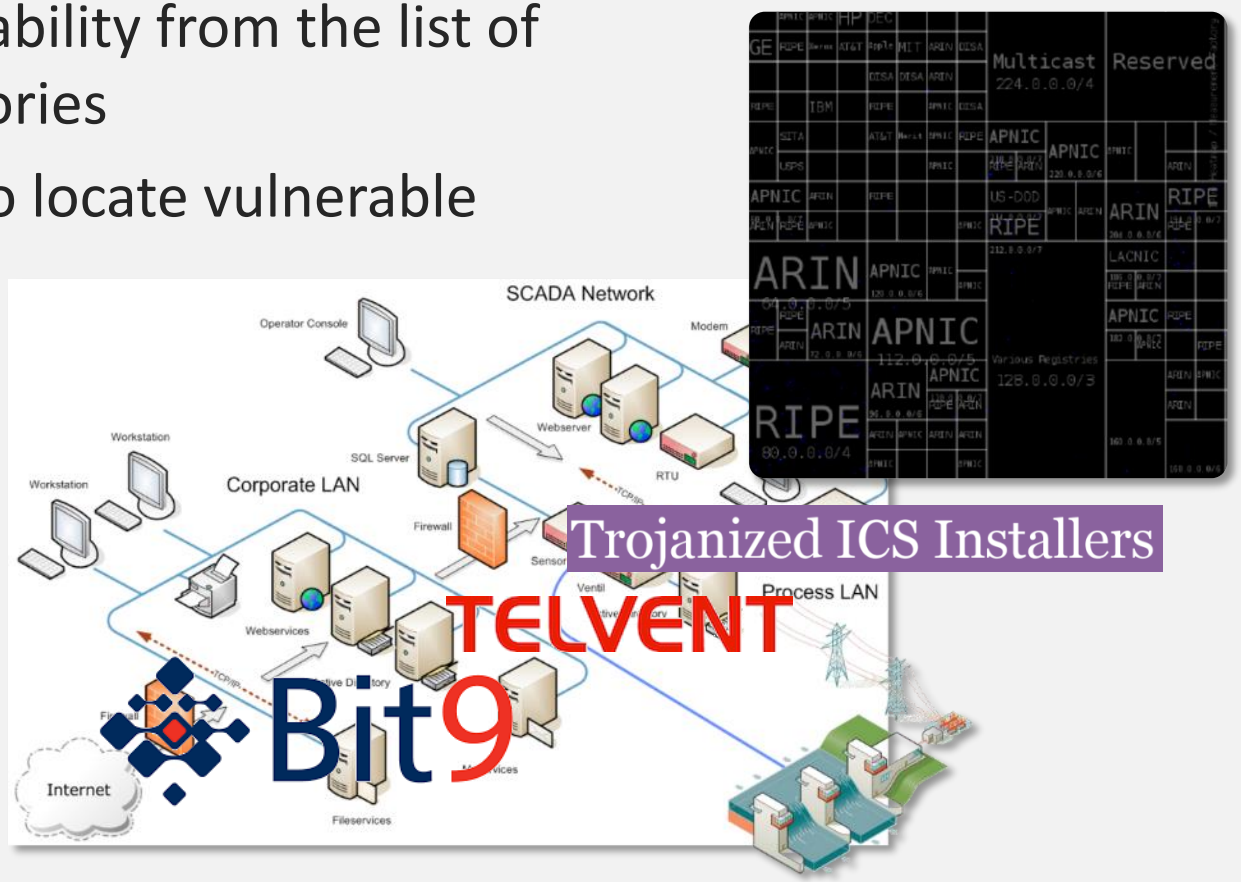
- No security
- Move freely

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)

Plants modernization

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

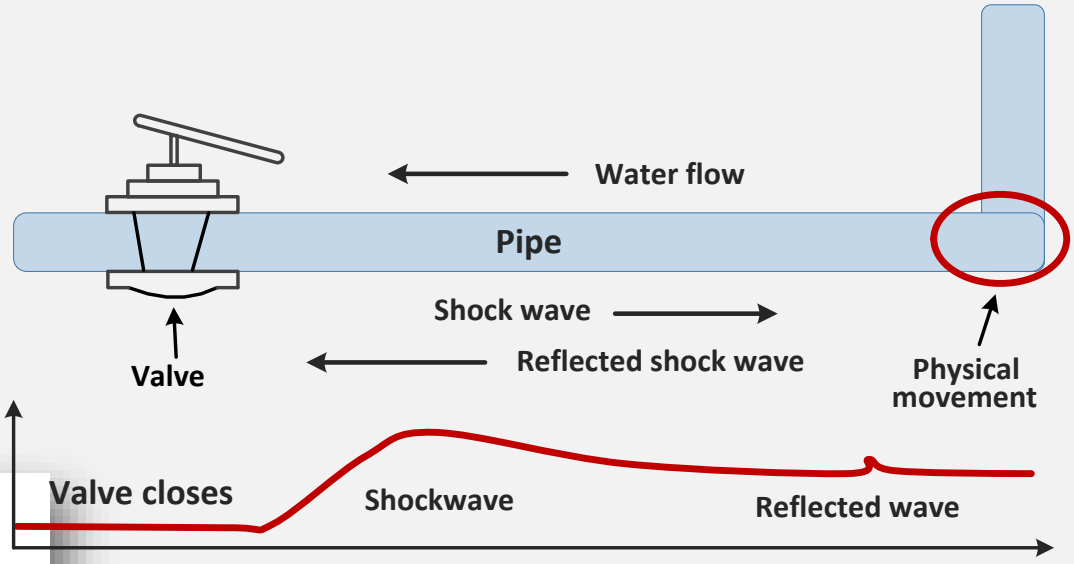
Old generation temperature sensor

Sensor

Computational element

Invading field devices

- 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, 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
```

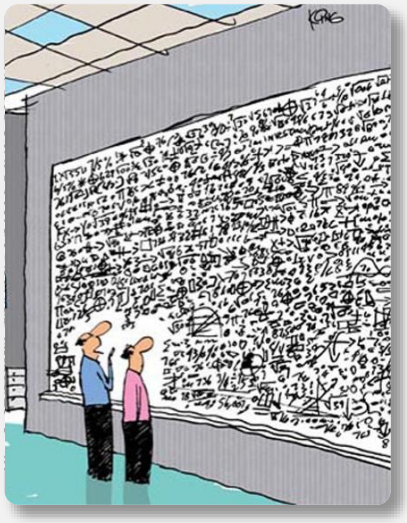
Attack scenario: pipe damage with water hammer effect

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

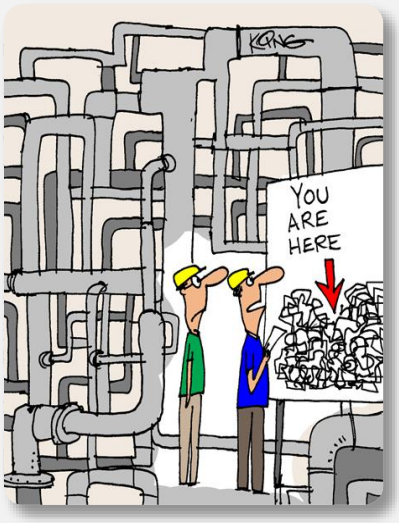
Discovery

Process discovery

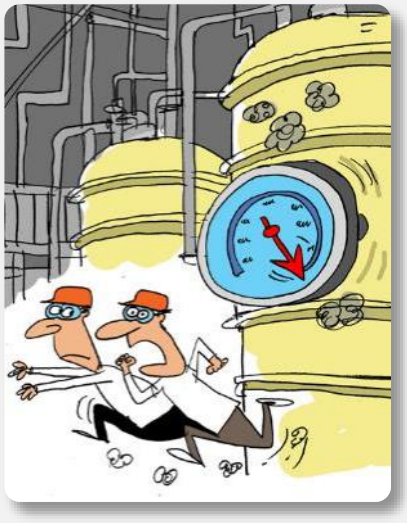
What and how the process is producing



How it is controlled



How it is build and wired



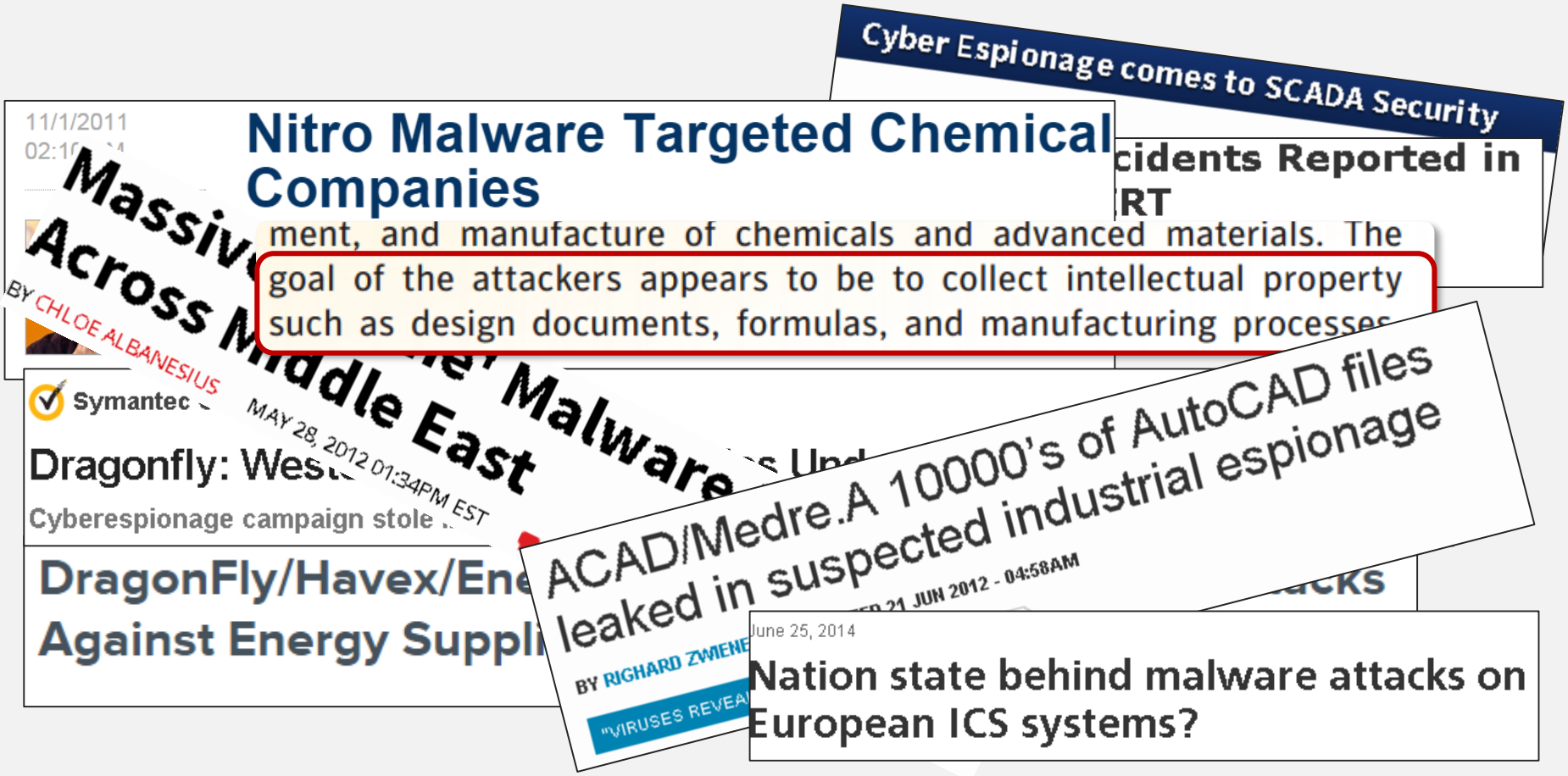
Operating and safety constraints

Espionage, reconnaissance

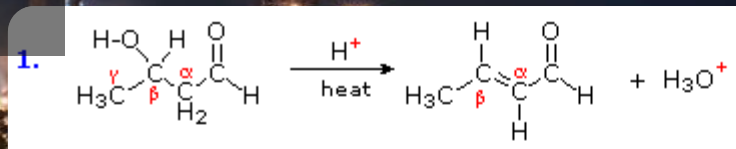
Target plant and third parties

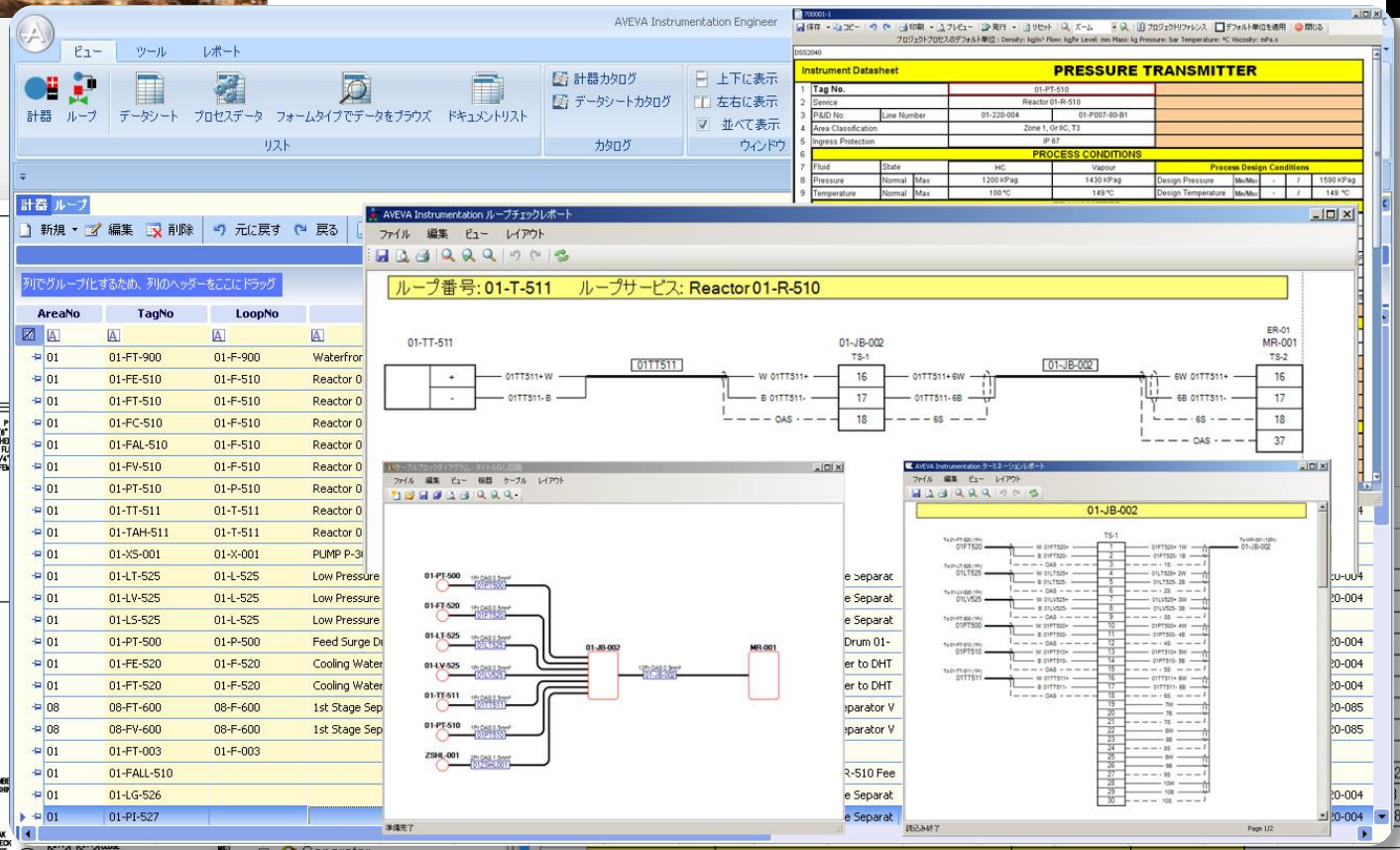
Espionage

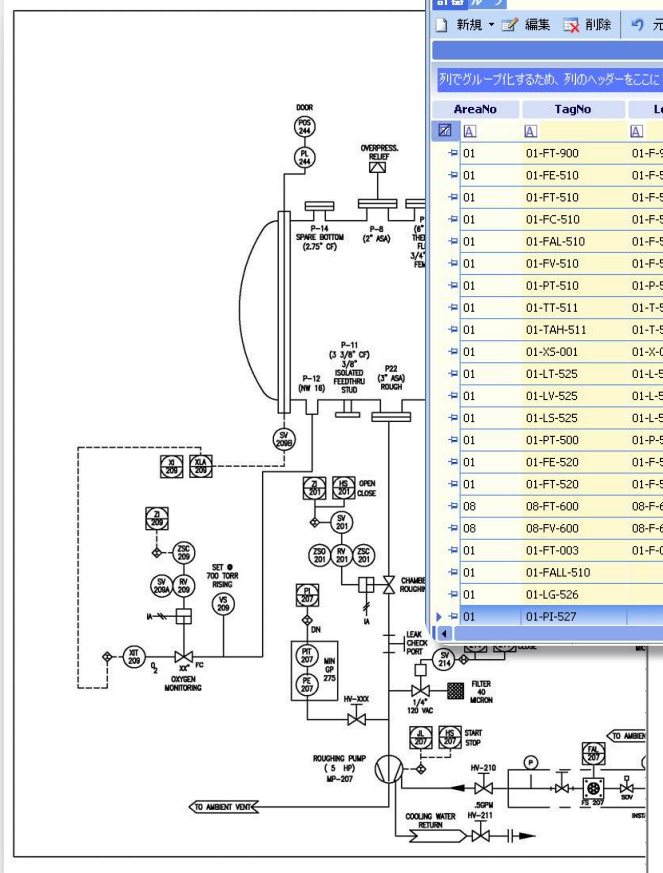
- Industrial espionage has started LONG time ago (malware samples dated as early as 2003)



Process discovery





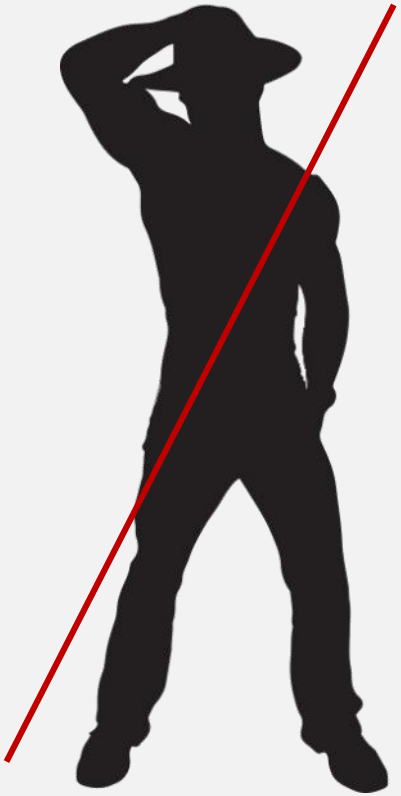


- Generator
- Grader
- Man Basket
- Other
- Plow
- Pressure Vessel
- Pump
- Quad
- Rig Mats
- Shacks
- Threader
- Tractor
- Trailer

14	DS-01	DblShift 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	

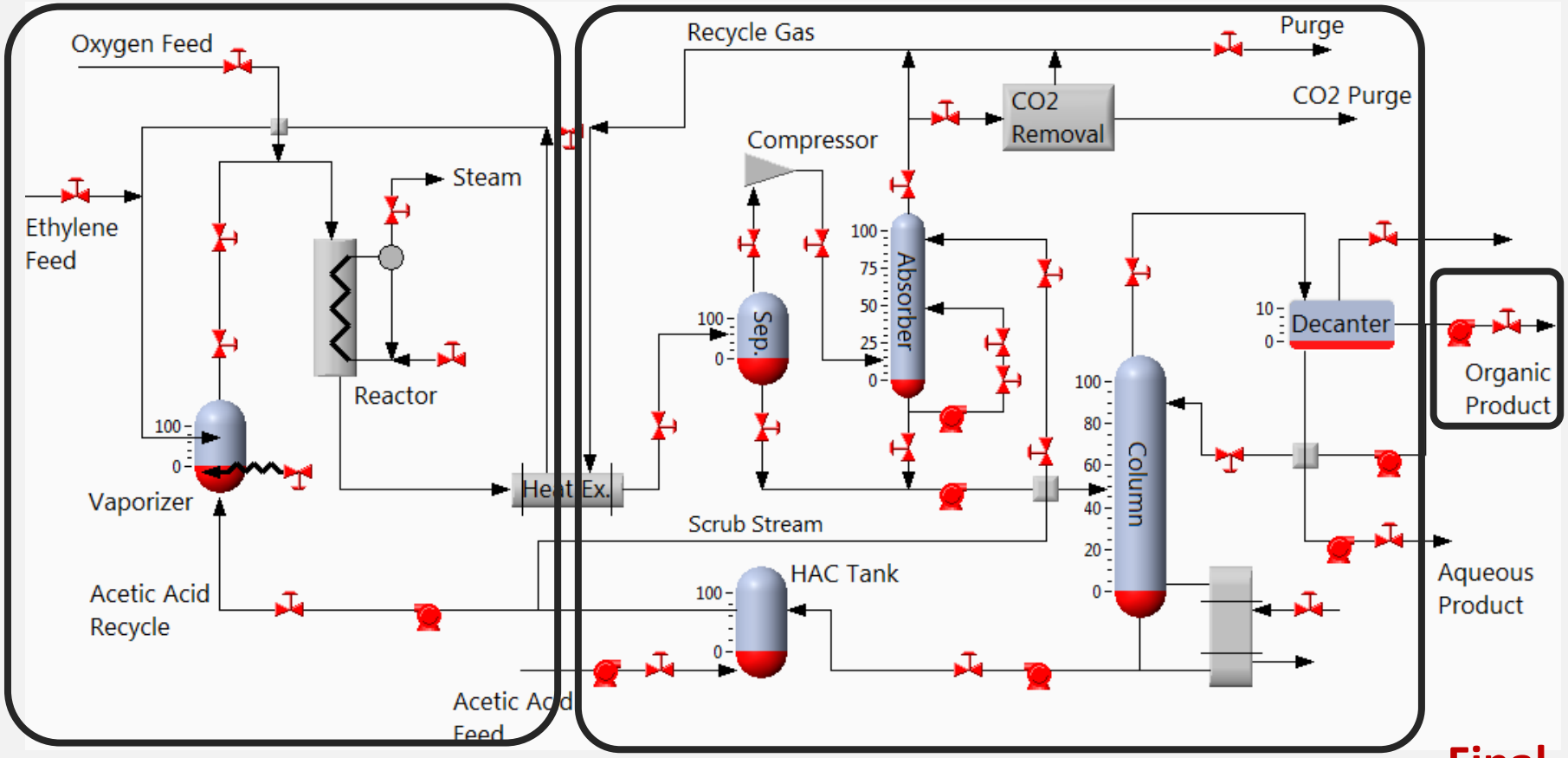
Know the equipment

Stripper is...



Stripping column

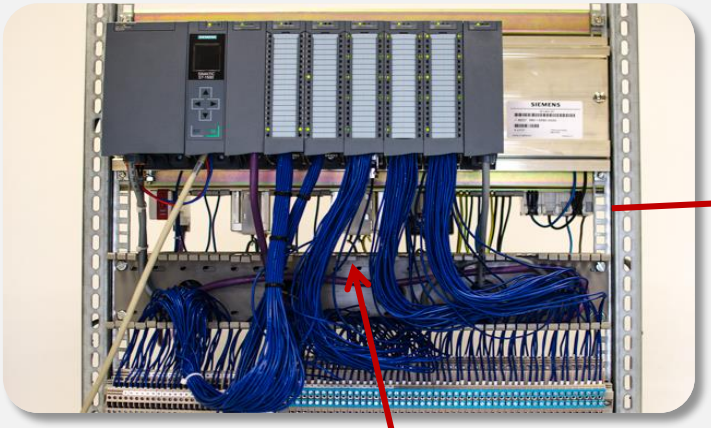
Max economic damage?



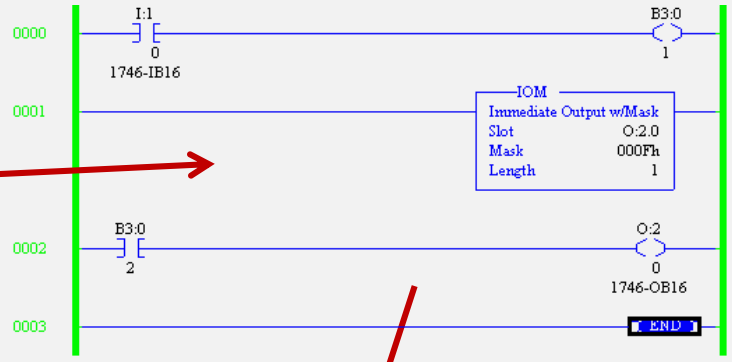
Requires input of subject matter experts

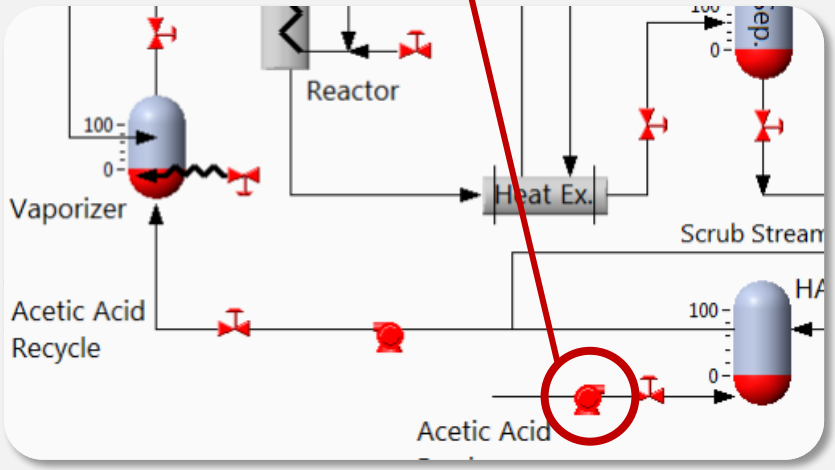
Understanding points and logic

Programmable Logic Controller

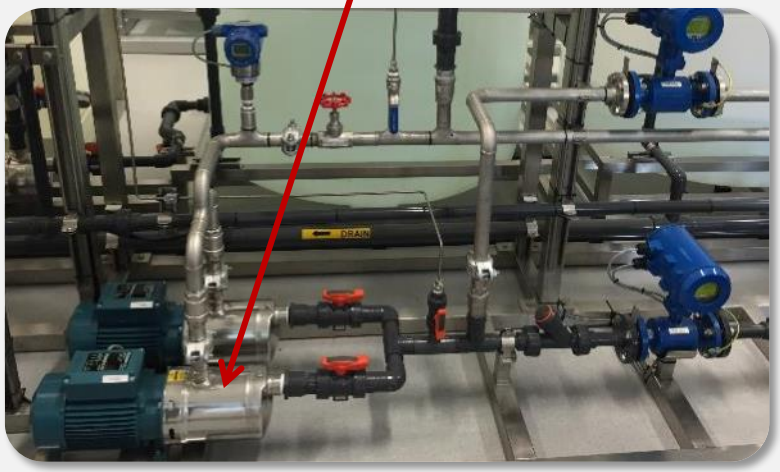


Ladder logic





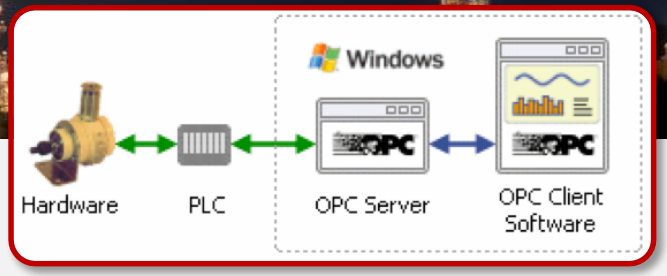
Piping and instrumentation diagram

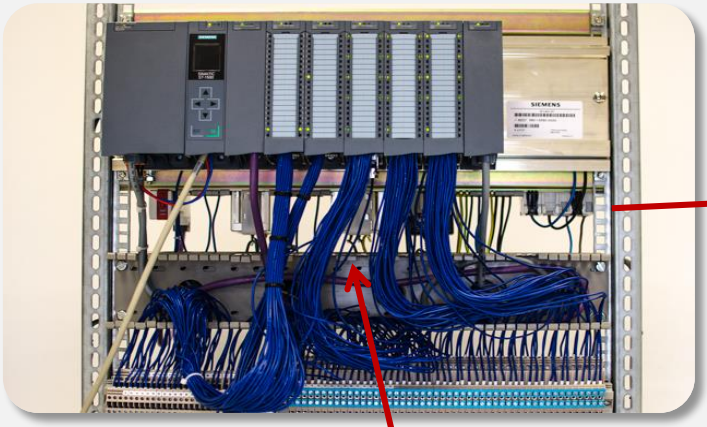


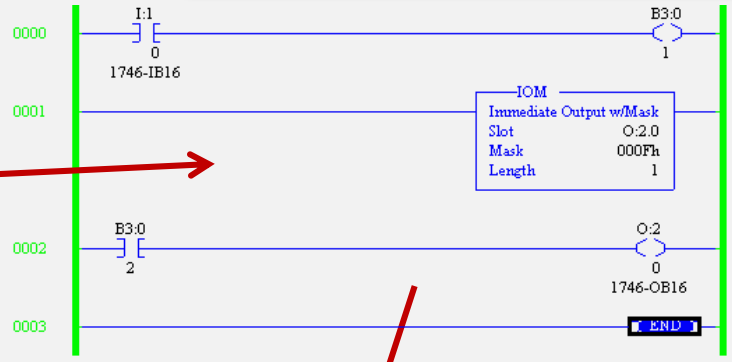
Pump in the plant

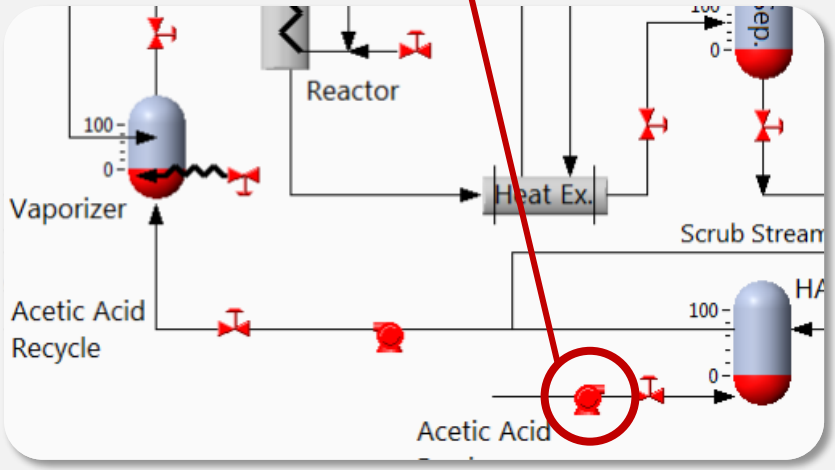
Understanding points and logic

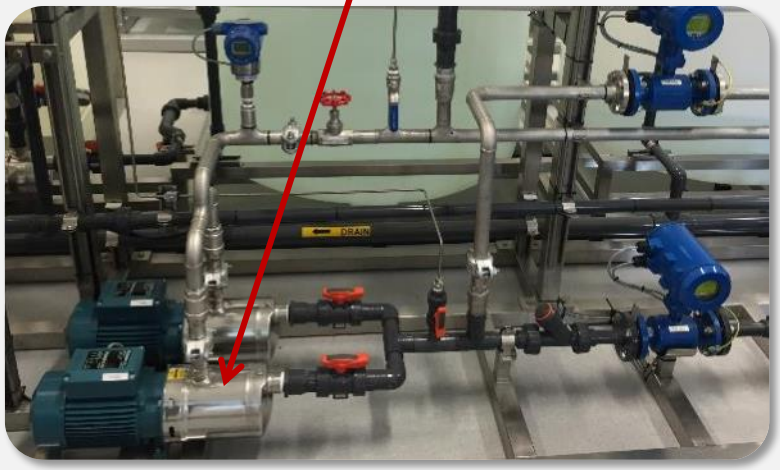
HAVEX: Using OPC, the malware component gathers any details about connected devices and sends them back to the C&C.







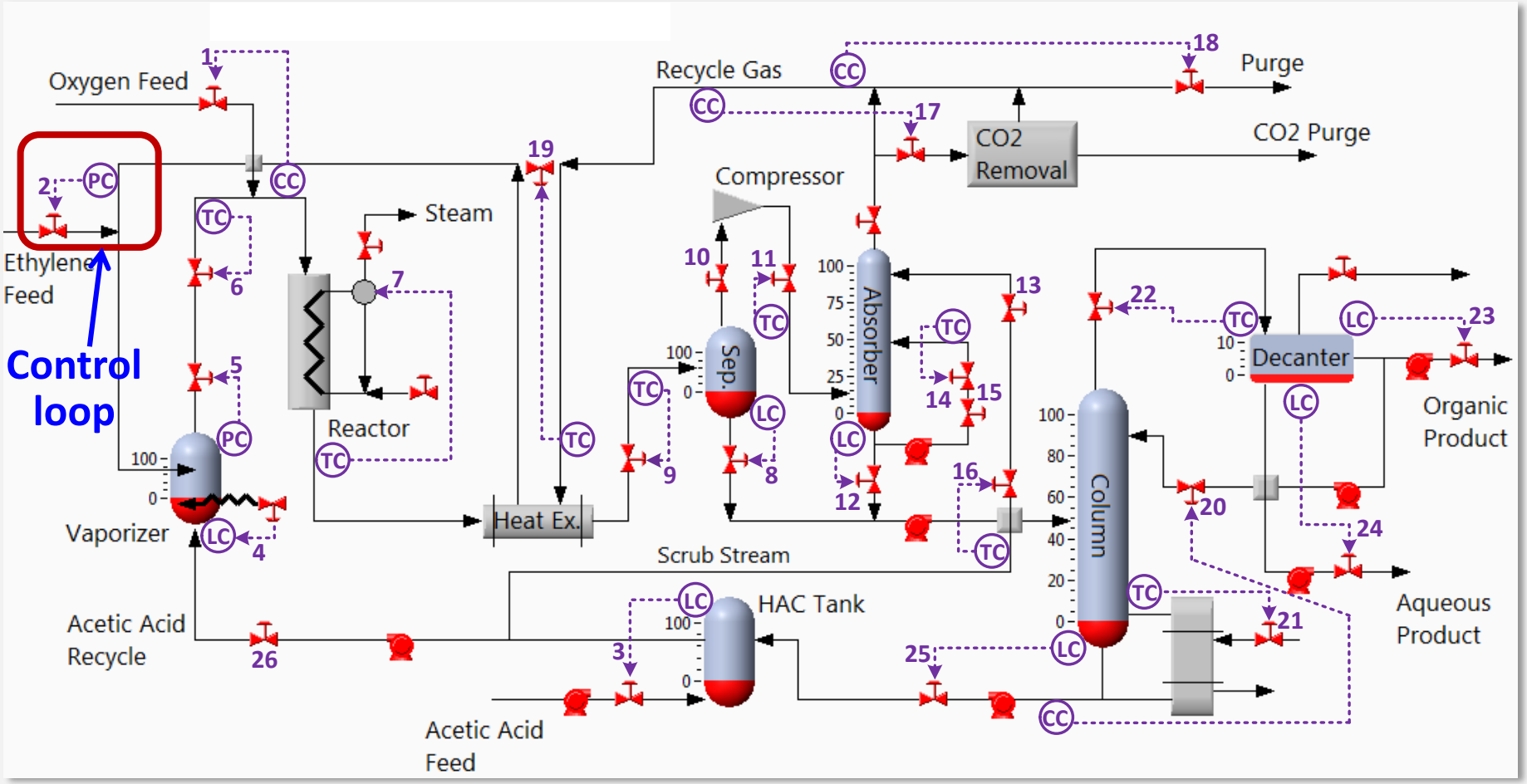




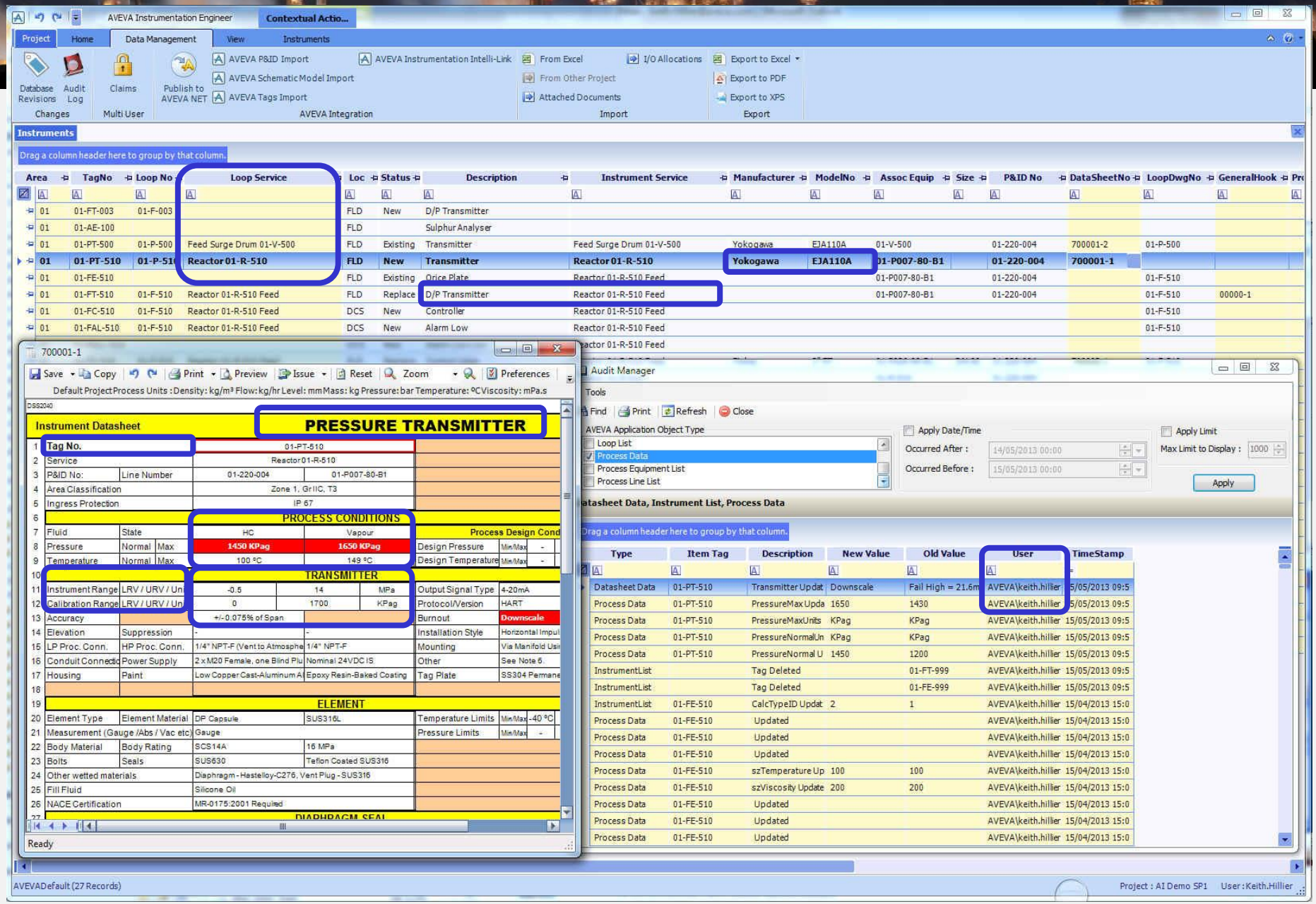
Piping and instrumentation diagram

Pump in the plant

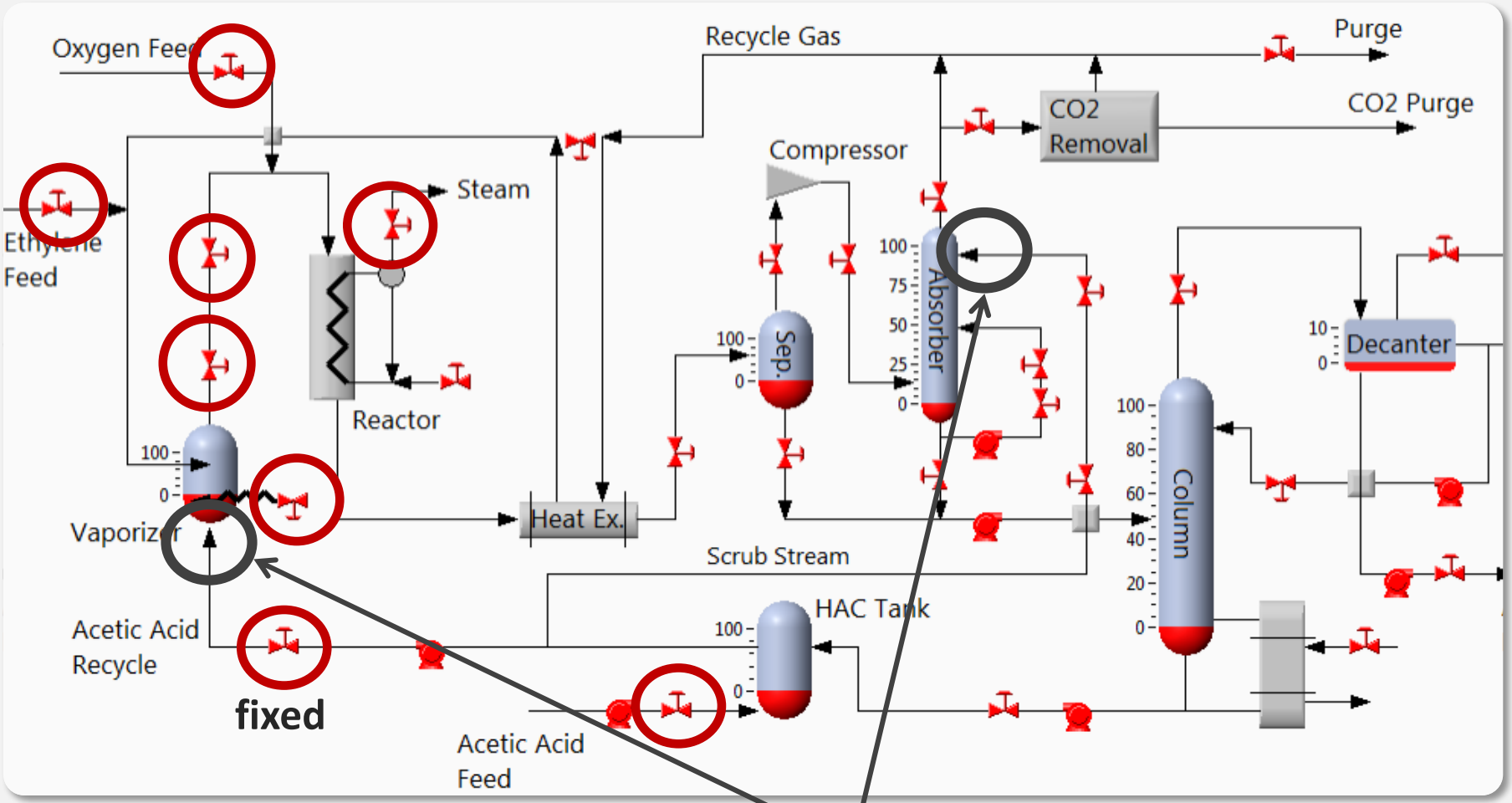
Understanding control structure



Control loop configuration

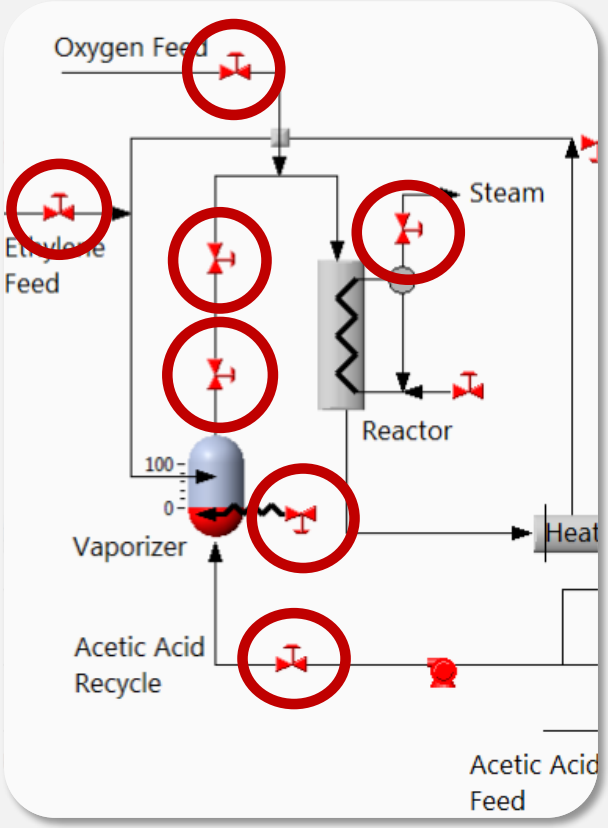


Watch the flows!



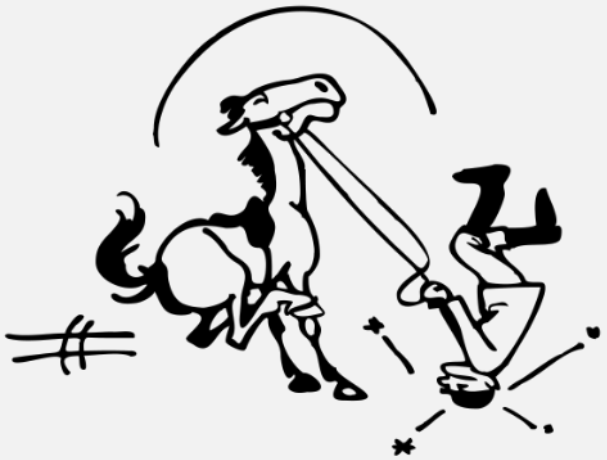
HAc flows into two sections. Not good :(

Obtaining control != being in control

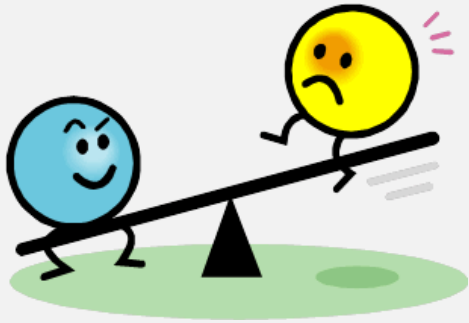


- Obtained controls might not be useful for attack goal
- Attacker might not necessary be able to control obtained controls

Huh ???



Control

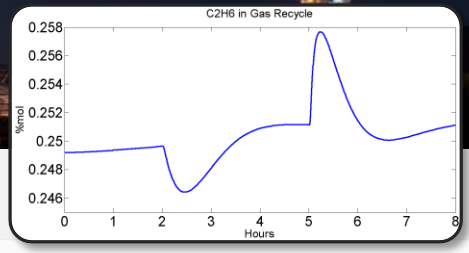


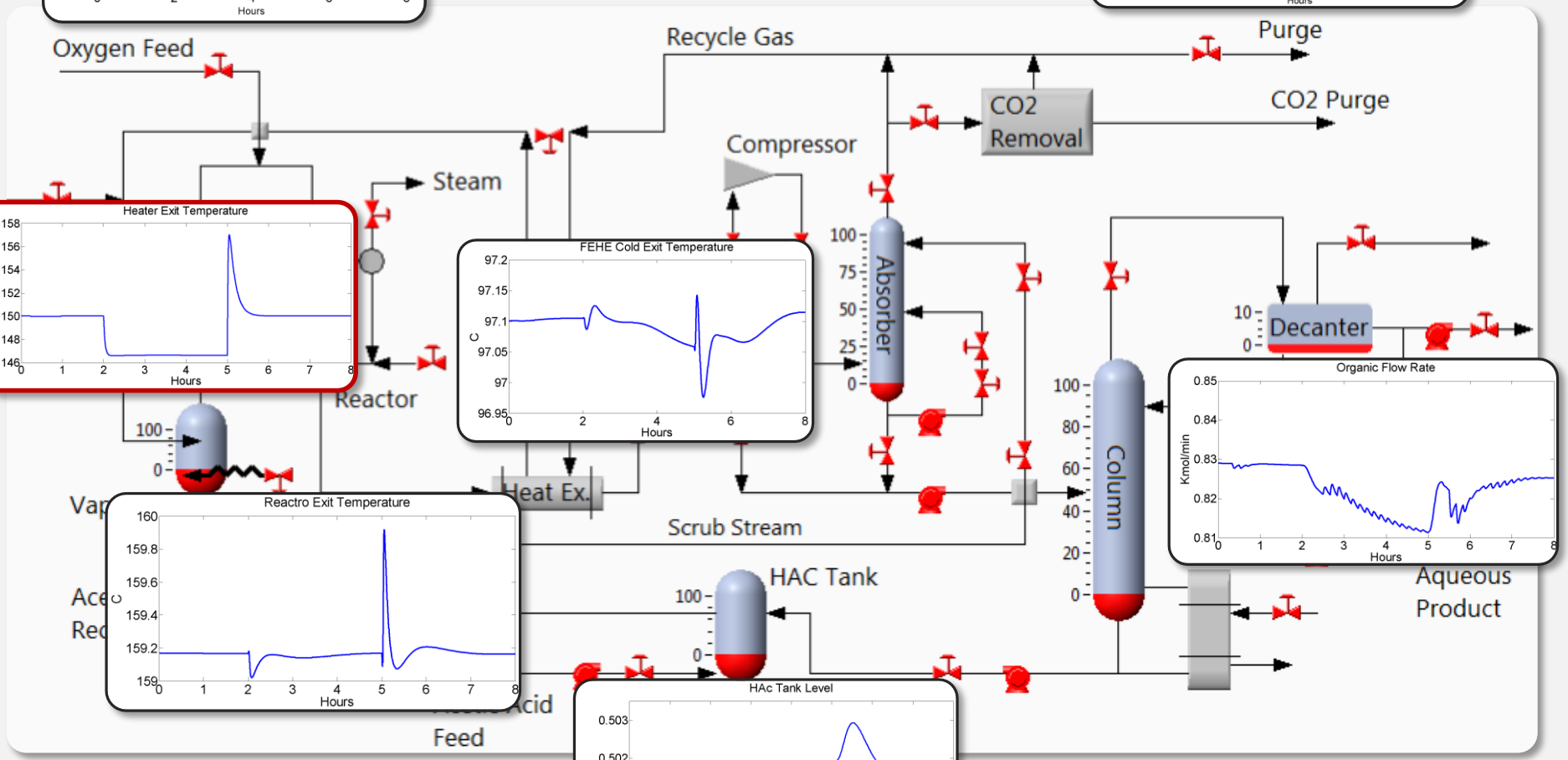
Every action has a reaction

Physics of process control

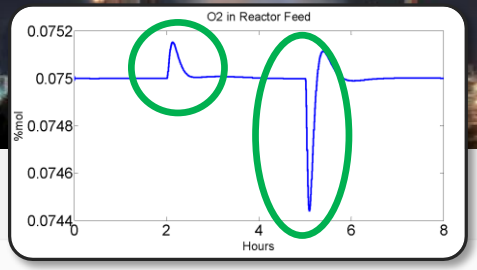
- **Once hooked up together, physical components become related to each other by the physics of the process**
- If we adjust a valve what happens to everything else?
  - Adjusting temperature also increases pressure and flow
  - All the downstream effects need to be taken into account
- How much does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

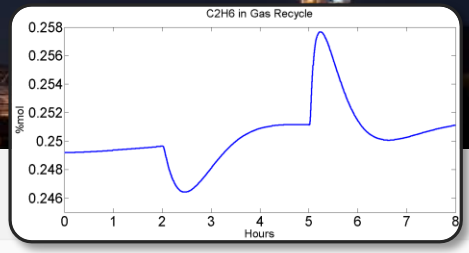
Process interdependencies





Process interdependencies





Oxygen Feed

Recycle Gas

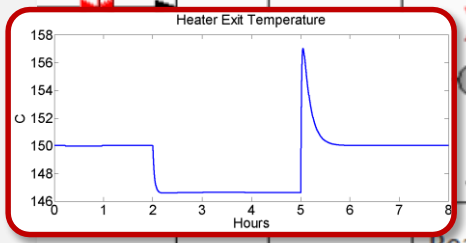
Purge

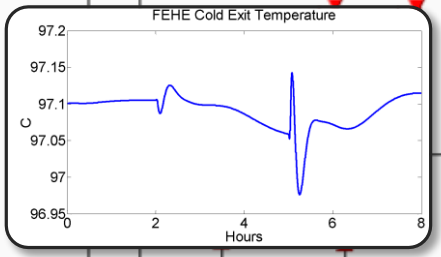
CO2 Removal

CO2 Purge

Compressor

Steam



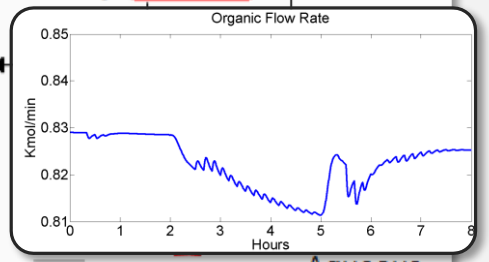


Absorber

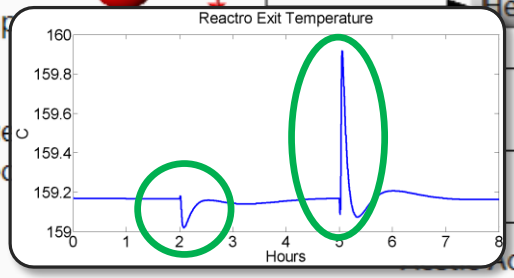
Reactor

Heat Ex.

Decanter



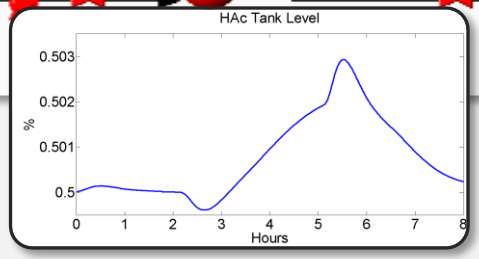
Column



Scrub Stream

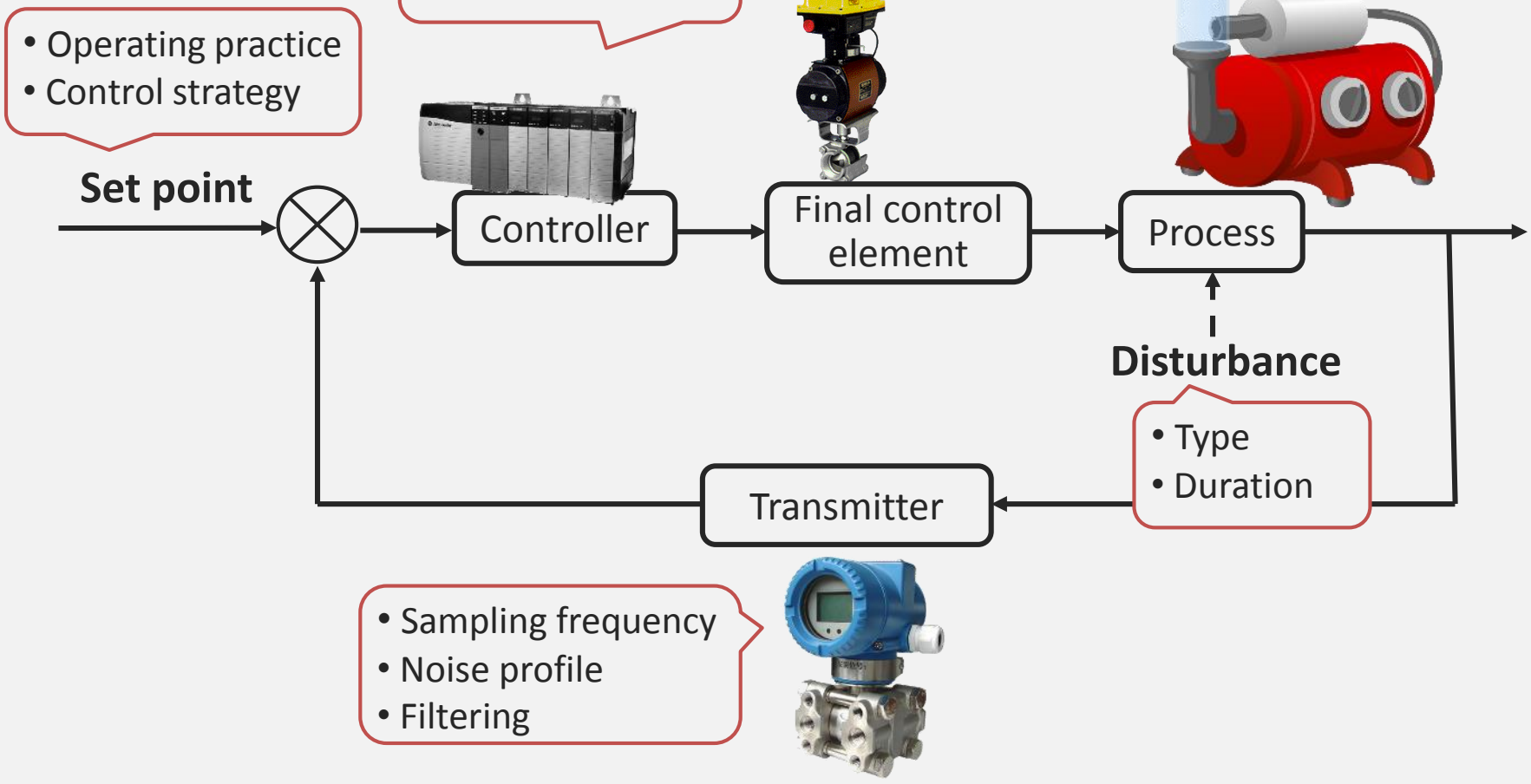
HAC Tank

Aqueous Product



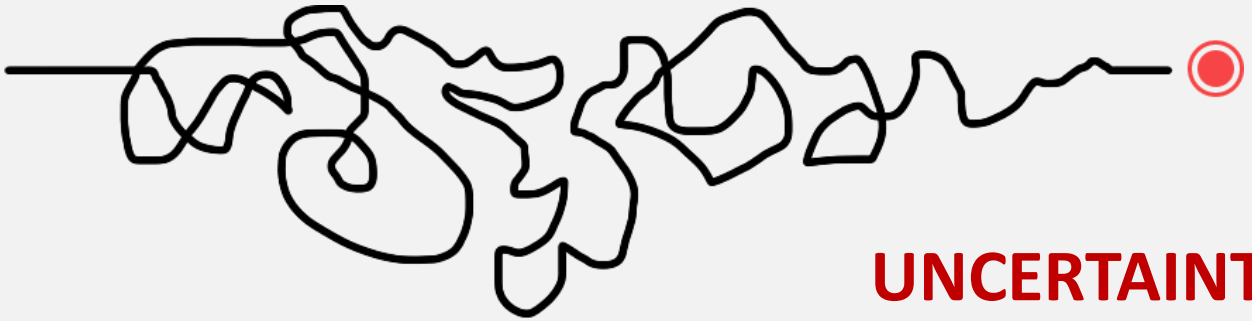
Feed

Understanding process response



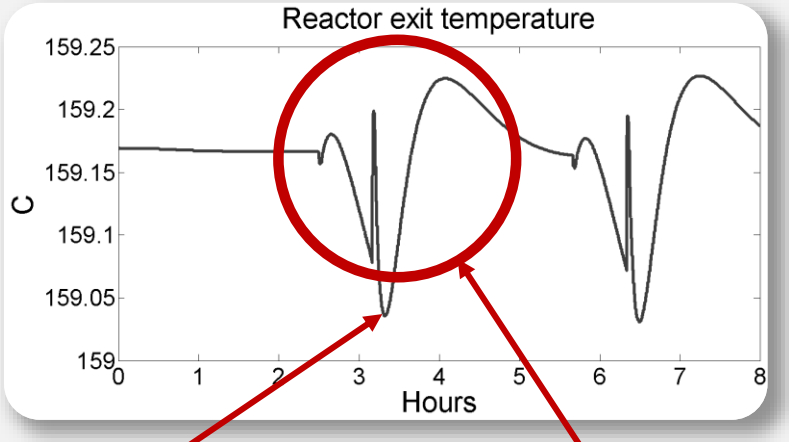
Process control challenges

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



UNCERTAINTY!

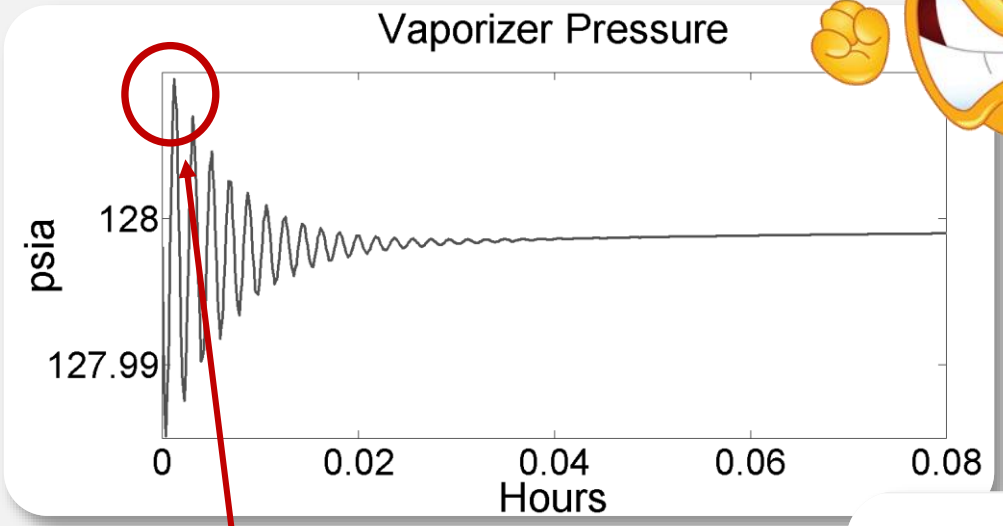
- Behavior of the process is known to the extent of its modelling
  - So to controllers. They cannot control the process beyond their control model



This triggers alarms

Non-liner response

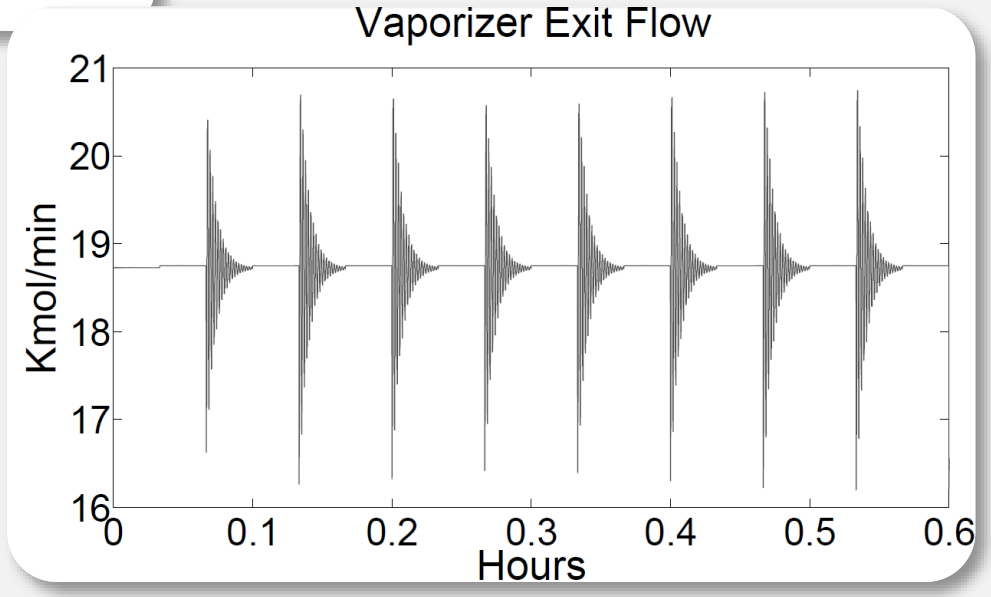
Control loop ringing



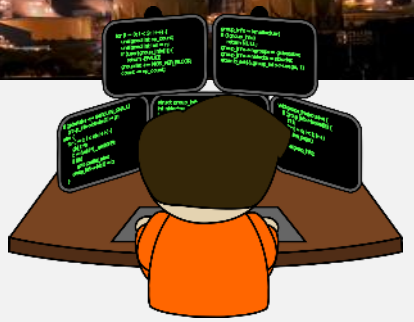
Caused by a negative real controller poles

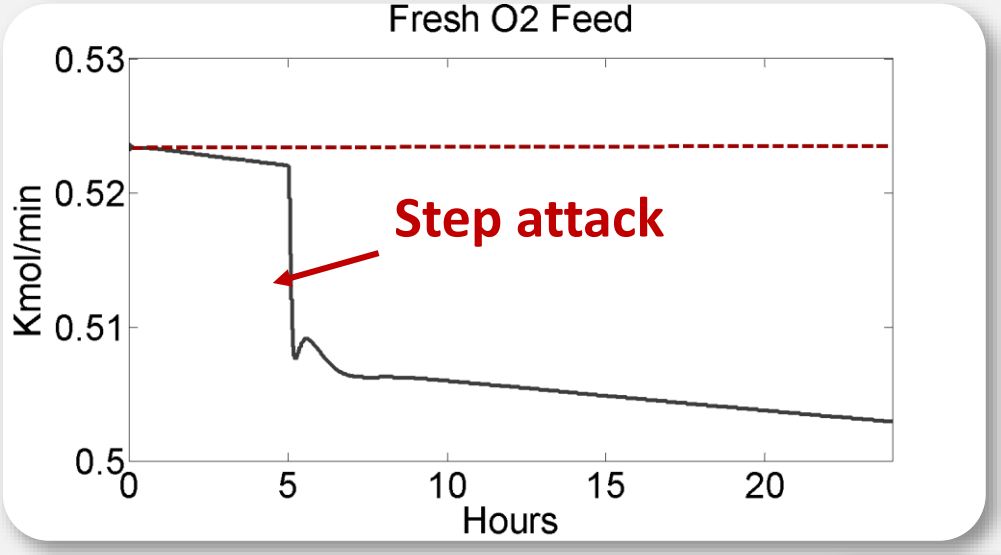
Makes process unstable and uncontrollable

Amount of chemical entering the reactor



Types of attacks

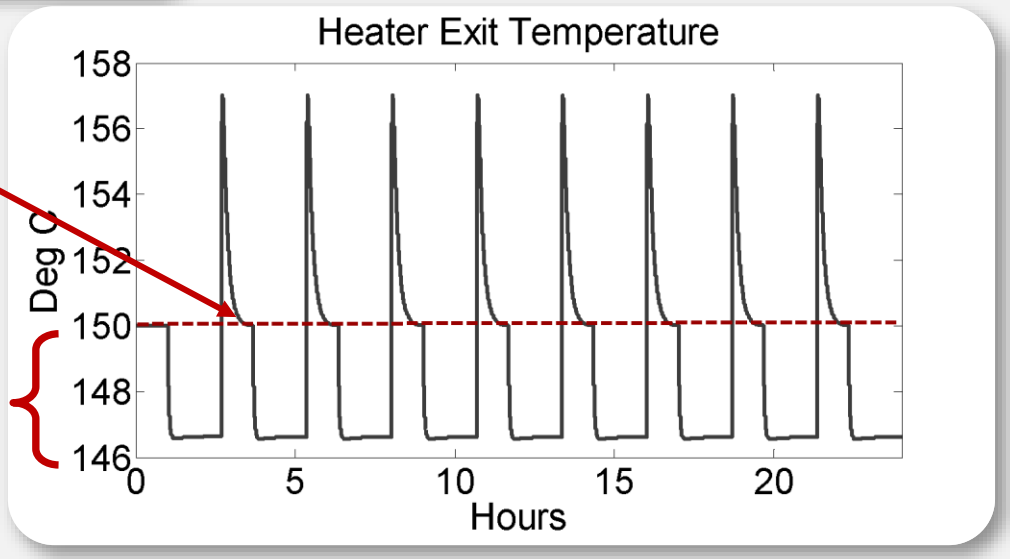




Periodic attack

Recovery time

Magnitude of manipulation



Outcome of the control stage

I am 5’3’’ tall

We probably 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

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

CSB

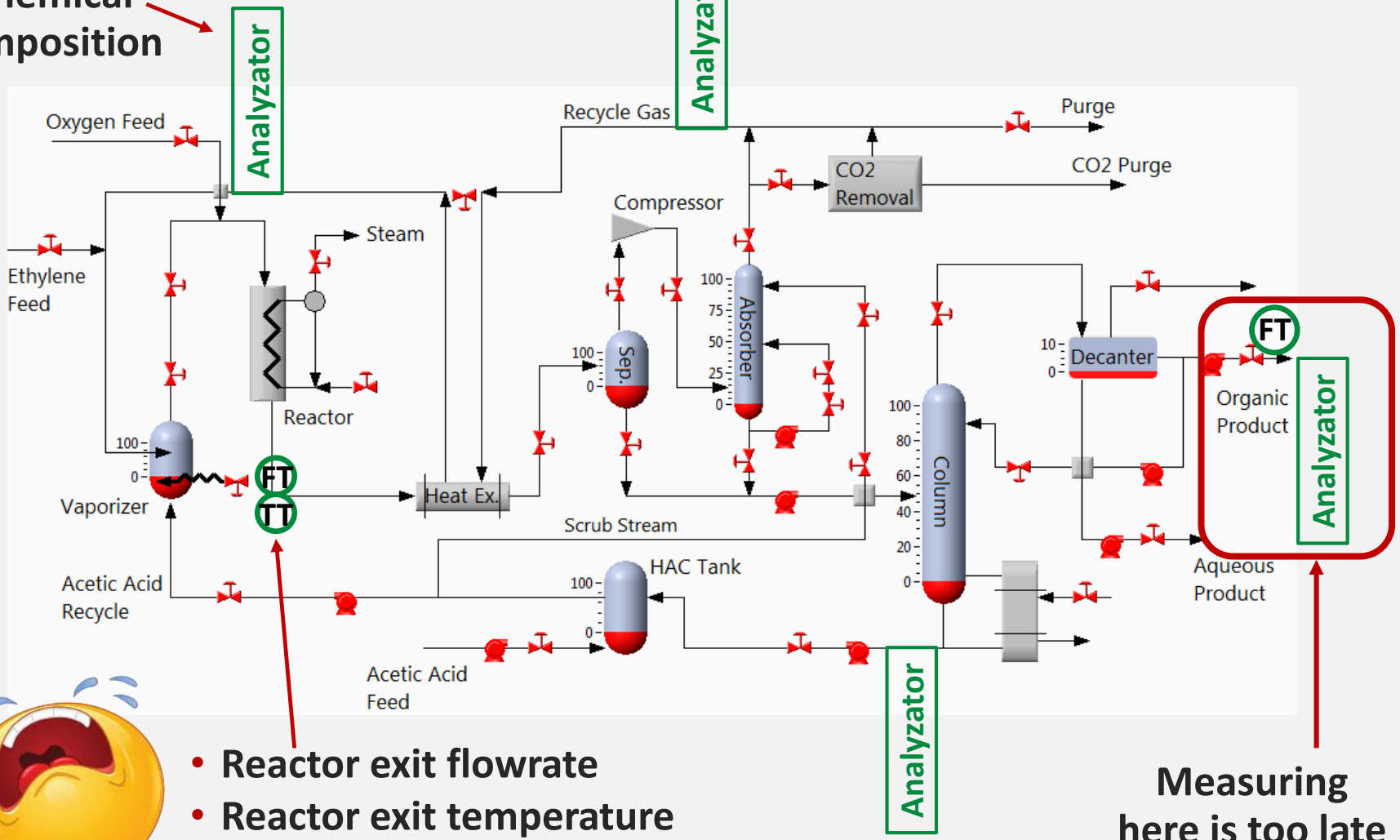
OSHA

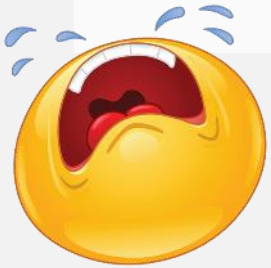
Hacker unfriendly process

- **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 spread across several subsystems making hacker invading more 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"

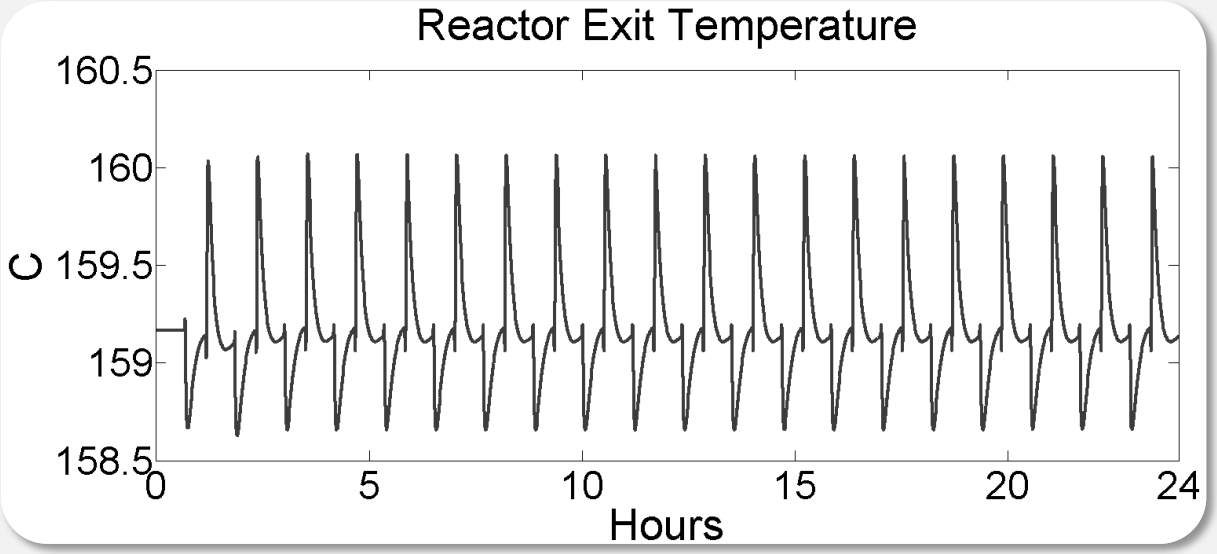
Engineer

"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

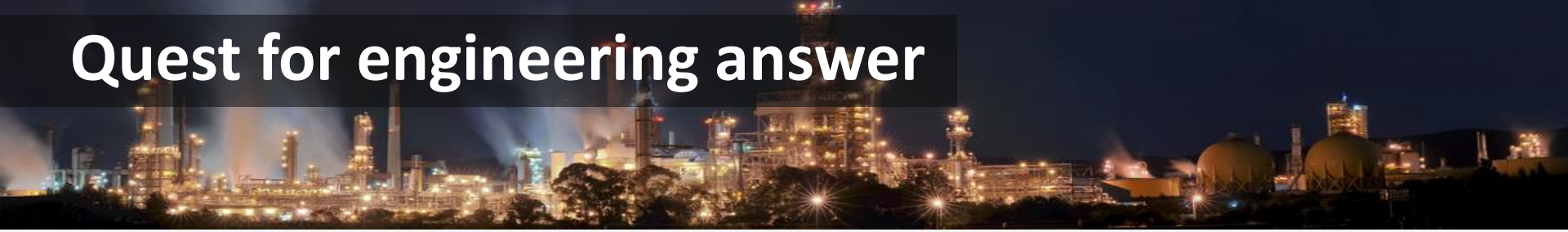
Usage of proxy sensor



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

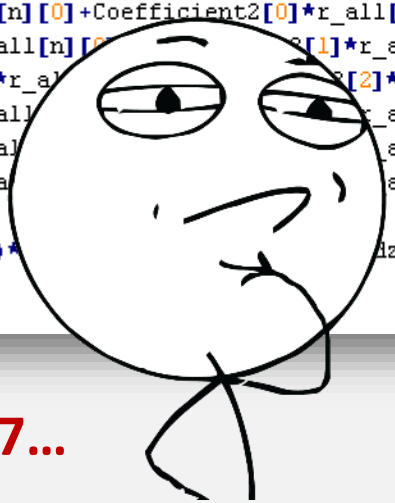


- Code in the controller
- Optimization applications
- Test process/plant

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

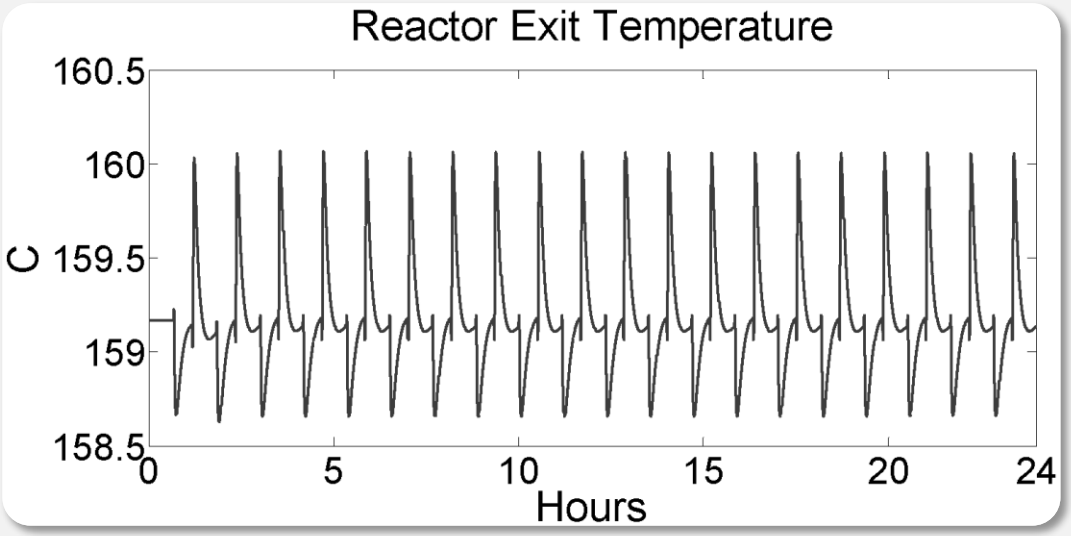
```
/*calculate derivatives*/
for (n=1;n<NR;n++)
{
    /*dC/dt=-delta(C*v)/deltaZ+sum(vij*rj)
    /*Use single backward                                    */
    C_O2_t[n-1]=(-(C_O2[n]*v[n]-C_O2[n-1]*v[n-1])/dz + Coefficient1[0]*r_all[n][0]+Coefficient2[0]*r_all[n][1])/cata_porosity;
    C_CO2_t[n-1]=(-(C_CO2[n]*v[n]-C_CO2[n-1]*v[n-1])/dz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

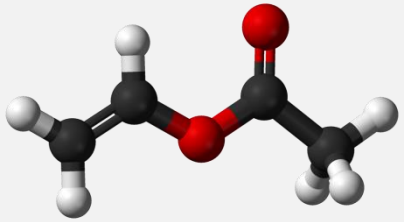
CHALLENGE CONSIDERED



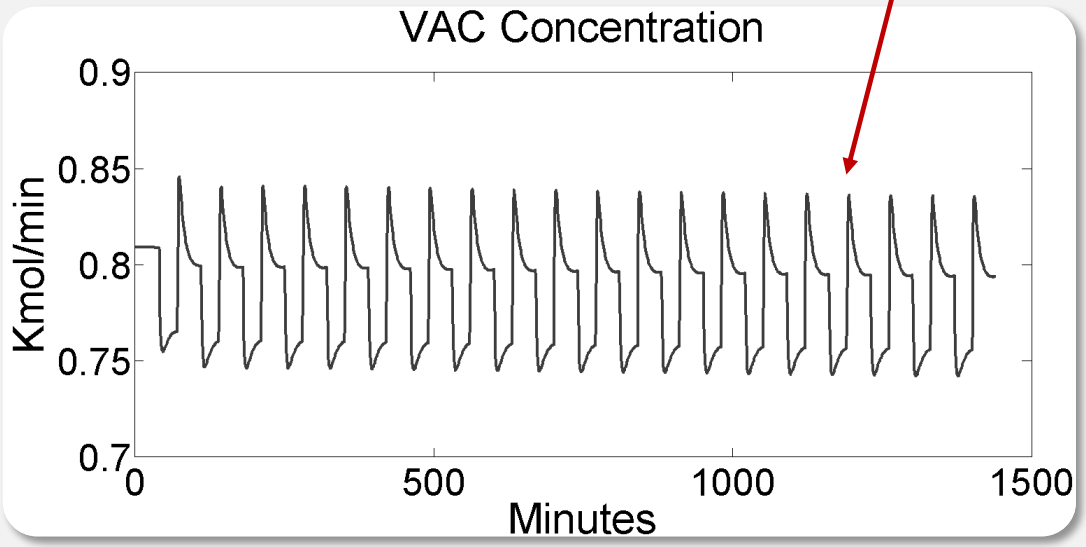
0,00073; 0,00016; 0,0007…

Engineering answer





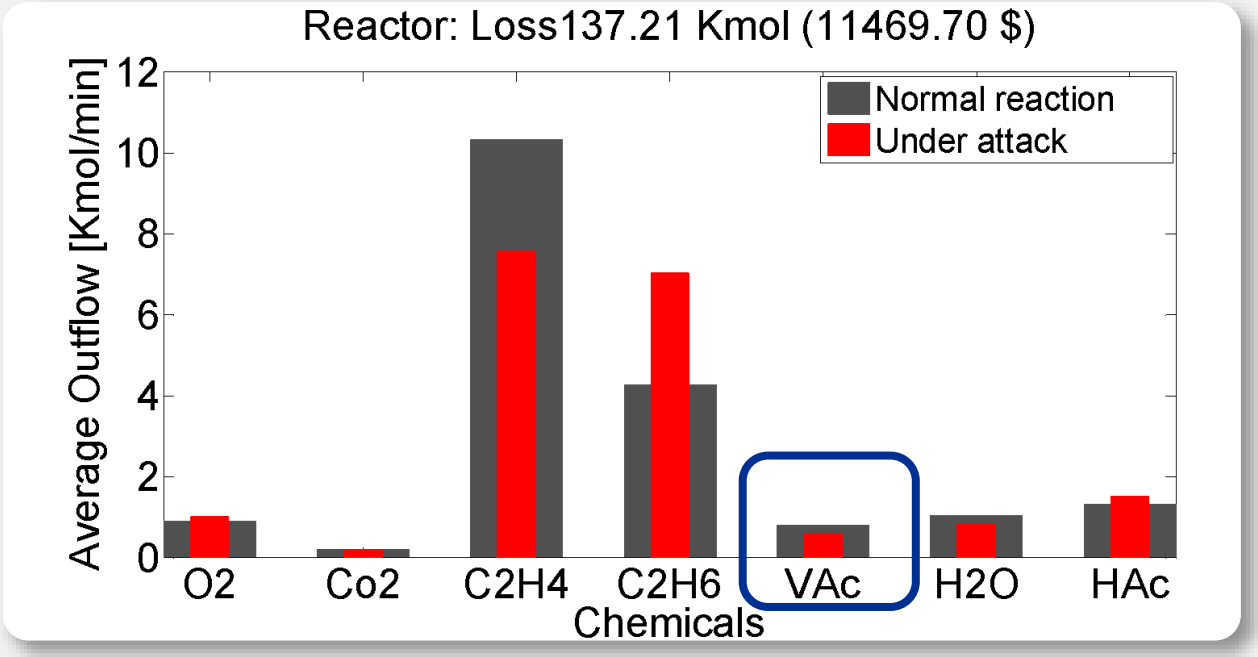
Vinyl Acetate production



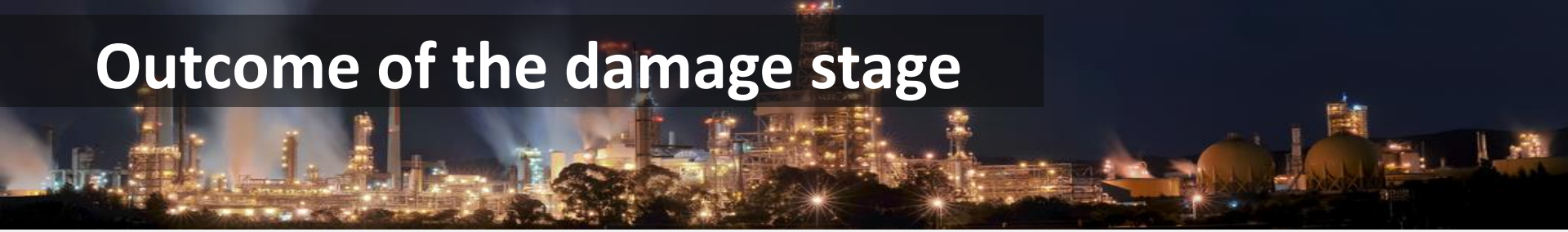
Product loss

Product per day: 96.000$

Product loss per day: 11.469,70$



Outcome of the damage stage



Product per day: 96.000$

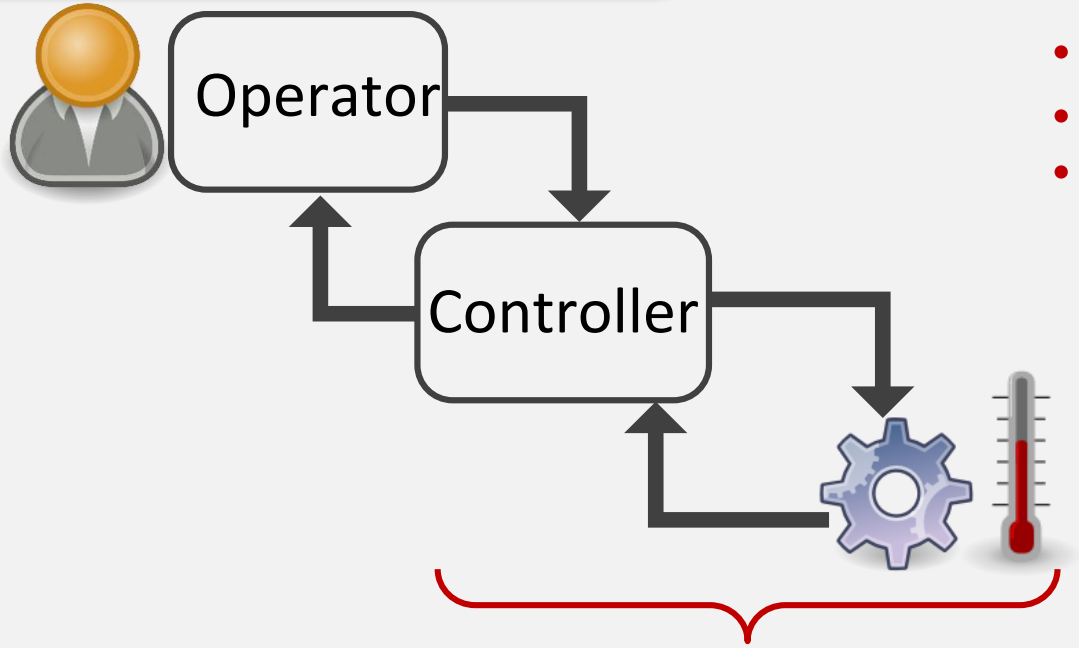
Product loss, 24 hours	Steady-state attacks	Periodic attacks
High, ≥ 10.000$	XMV {2}	XMV {4;6}
Medium, 5.000$ - 10.000$	XMV {6;7}	XMV {5;7}
Low, 2.000$ - 5.000$	-	XMV {2}
Negligible, ≤ 2.000$	XMV {1;3}	XMV {1;2}

Still might be useful

Clean-up

Socio-technical system

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



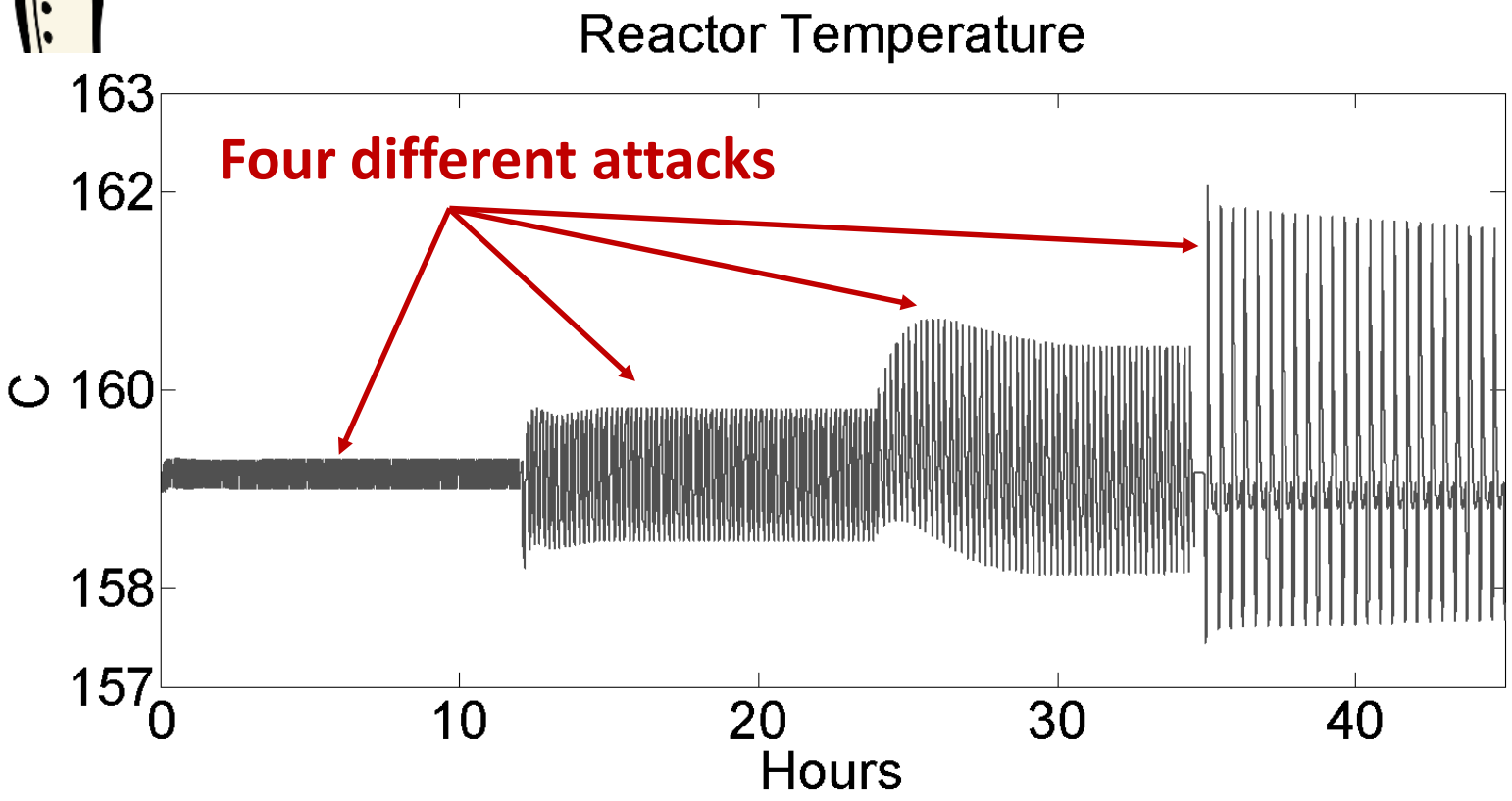
Creating forensics footprint

- 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

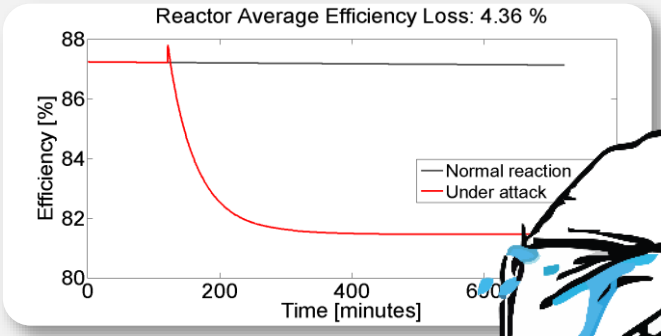
1. Pick several ways that the temperature can be increased
2. Wait for the scheduled instruments calibration
3. Perform the first attack
4. Wait for the maintenance guy being yelled at and recalibration to be repeated
5. Play next attack
6. Go to 4

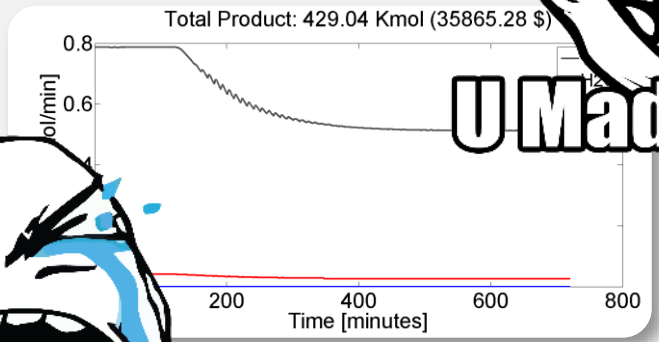
Creating forensics footprint

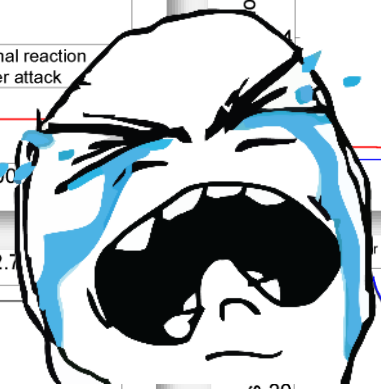


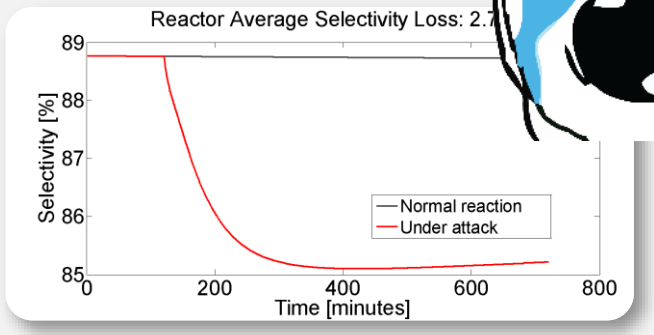
Defeating chemical forensics

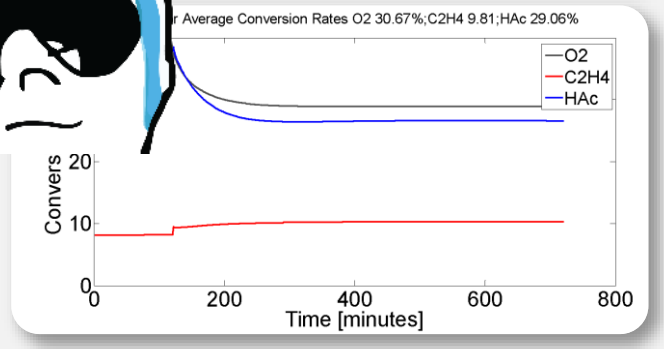
- If reactor doubted, chemical forensics guys will be asked to assist
- Know metrics and methods of chemical investigators
- **Change attack patterns according to debugging efforts of plant personnel**

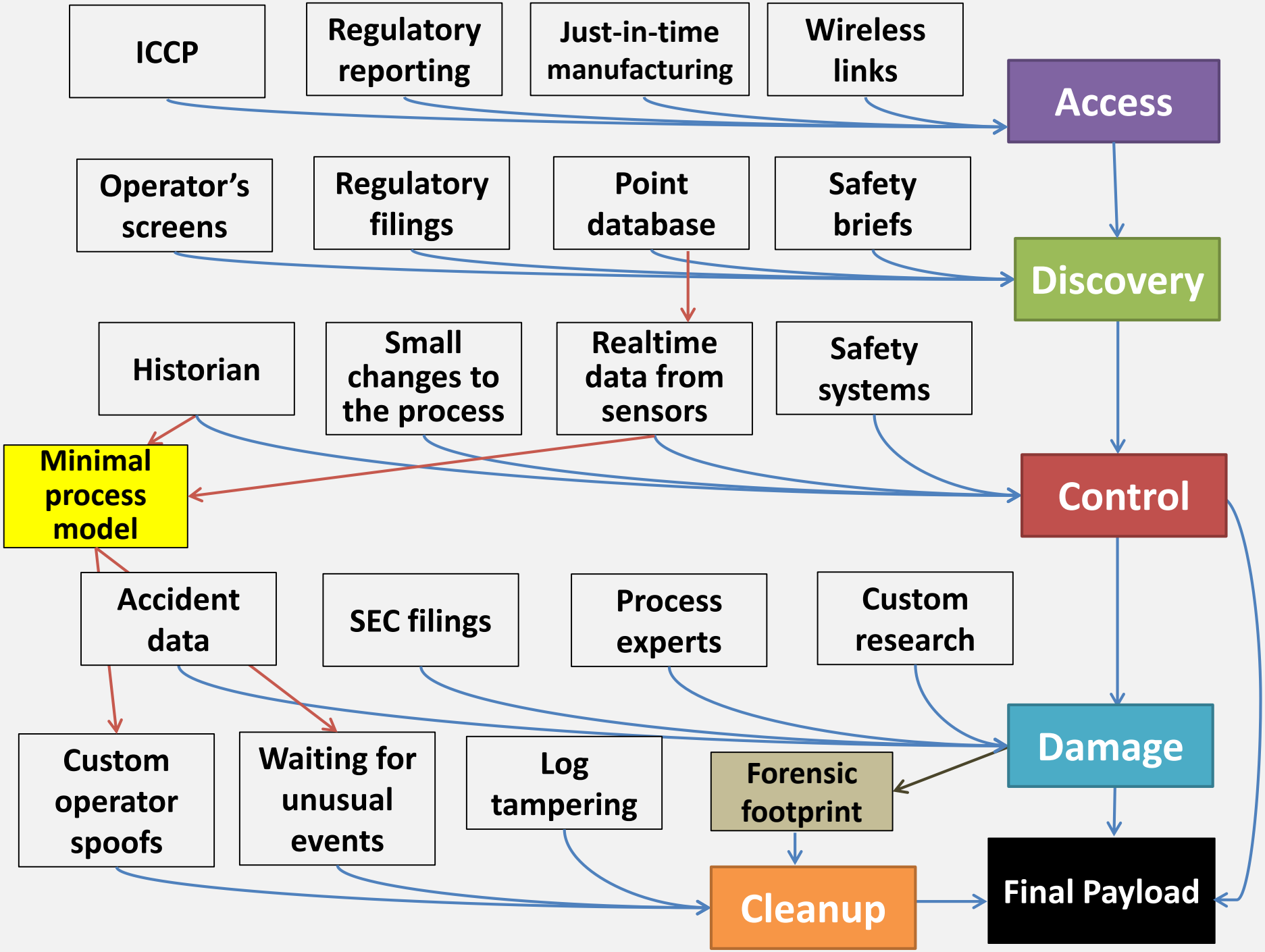






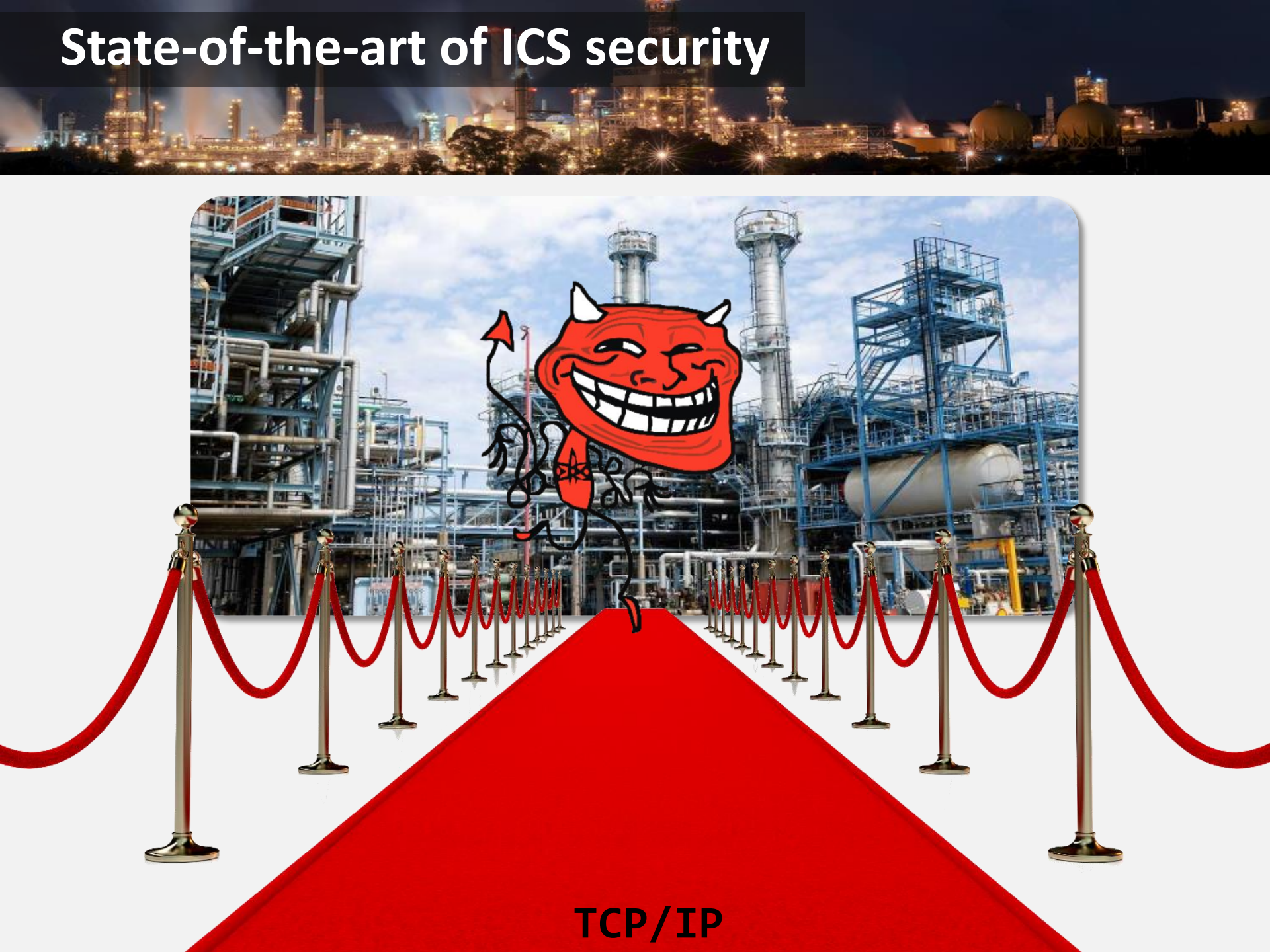





ICCP
Regulatory reporting
Just-in-time manufacturing
Wireless links
Access
Operator's screens
Regulatory filings
Point database
Safety briefs
Discovery
Historian
Small changes to the process
Realtime data from sensors
Safety systems
Minimal process model
Control
Accident data
SEC filings
Process experts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

Postamble

State-of-the-art of ICS security



What to do?

People respond to incentives.

A fundamental principle of economic analysis

Cyber-insurance

Premium drives compliance

1. "Base line" security
2. Compliance audit

Compliant?

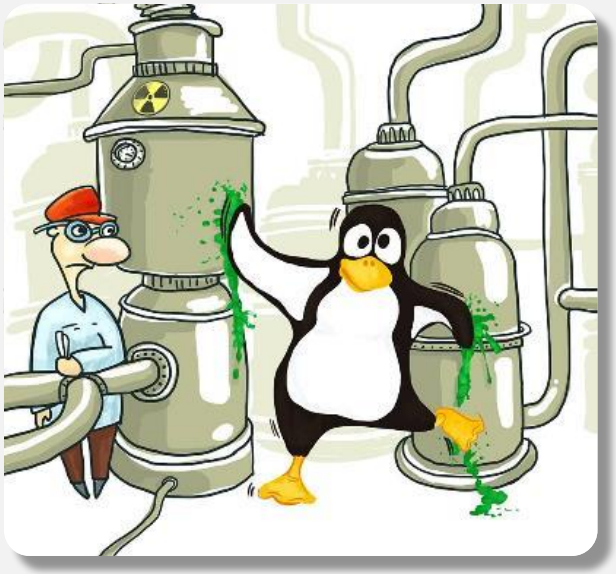
3. Residual risk assessment: setting Premium
4. Cyber-physical forensics: damage liabilities
5. Approved monitoring solution

Determine

Take away

- **Better understanding what the attacker needs to do and why**
  - Eliminating low hanging fruits
  - Making exploitation harder
- **Look for the attacker**
  - Eliminating low hanging fruits
  - Making exploitation harder
- Building attack-resilient processes

Research on cyber-physical exploitation is useful for…..



Thank you

Marina Krotofil
marina.krotofil@tuhh.de

Damn Vulnerable Chemical Process

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