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

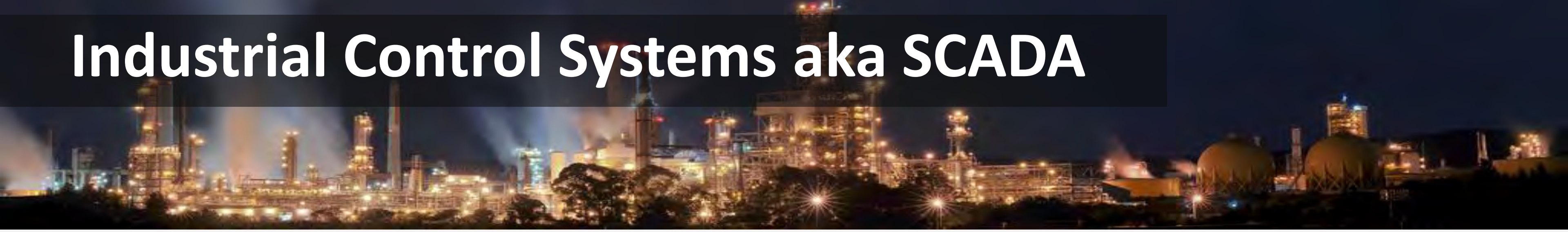
Hacker

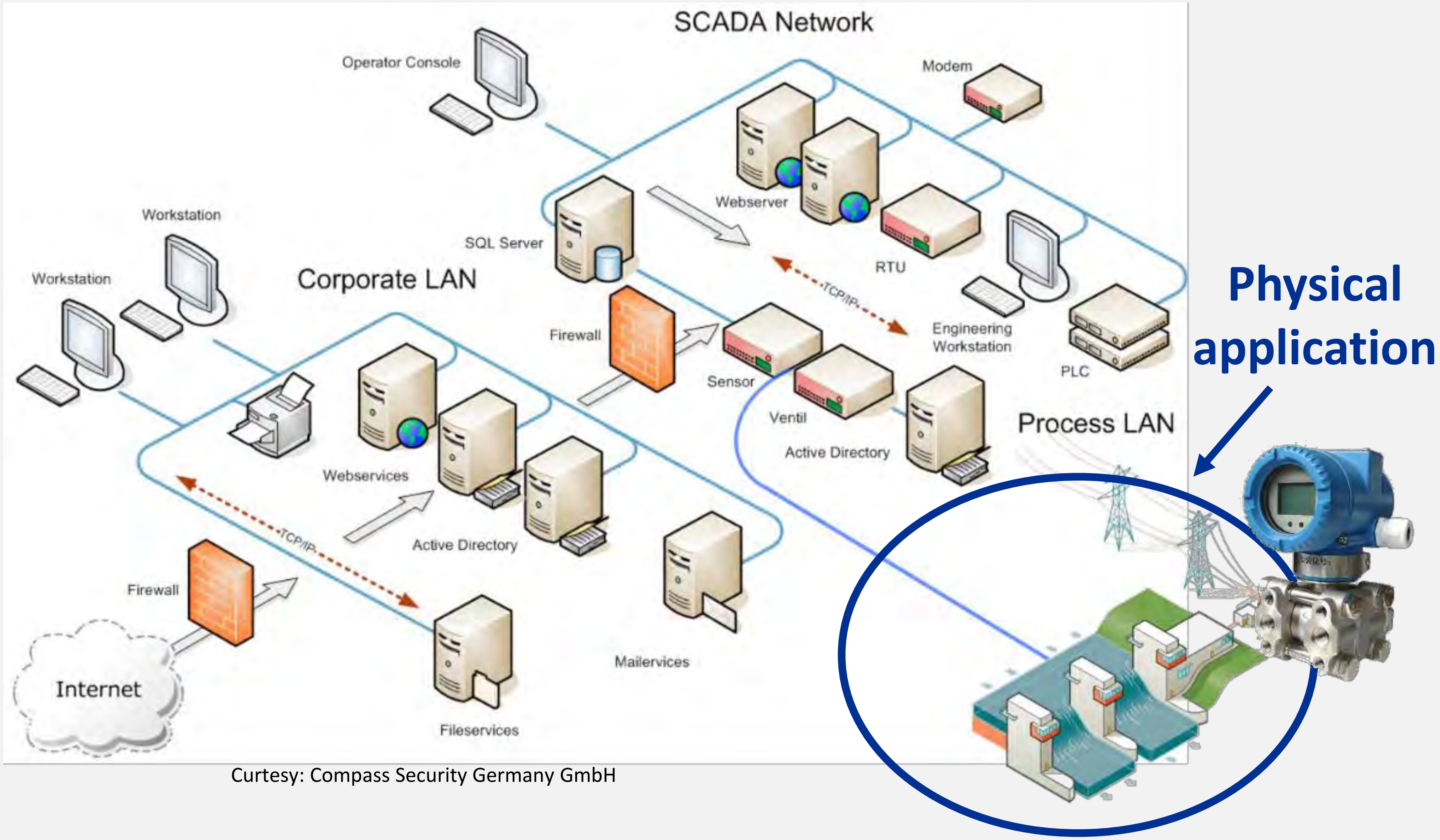
Dragged into academic world against own will

Motivation

Industrial Control Systems

Industrial Control Systems aka SCADA

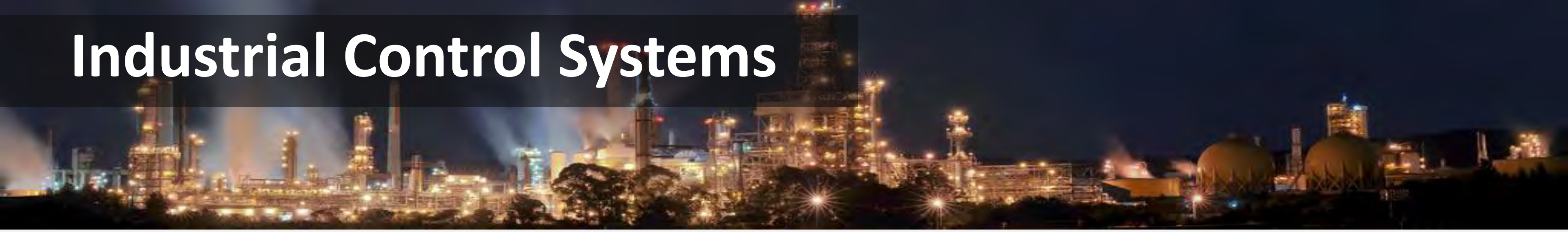




Curtesy: Compass Security Germany GmbH

Physical application

Industrial Control Systems



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

Here’s a plant. What is the plan?

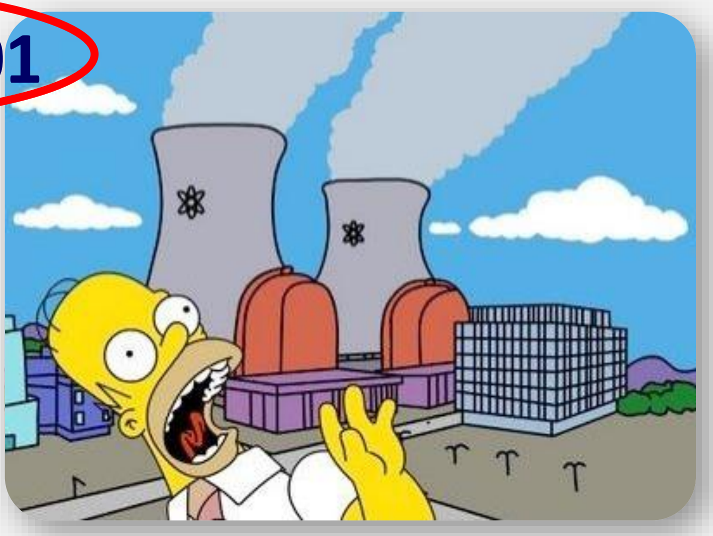
Attack scenario: persistent economic damage

How do we do it??

01001101101101

Missing piece of knowledge

Some horrible physical consequences



Typical understanding of SCADA hacking

magic button
(does not exist!)

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

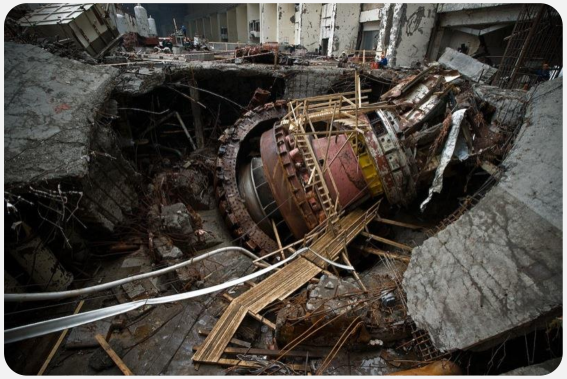
□ Maintenance efforts

Compliance violation

□ Safety (occupational, environment)

□ Pollution (environment)

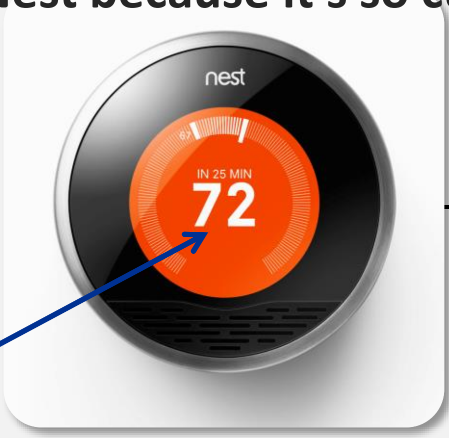
□ Contractual agreements



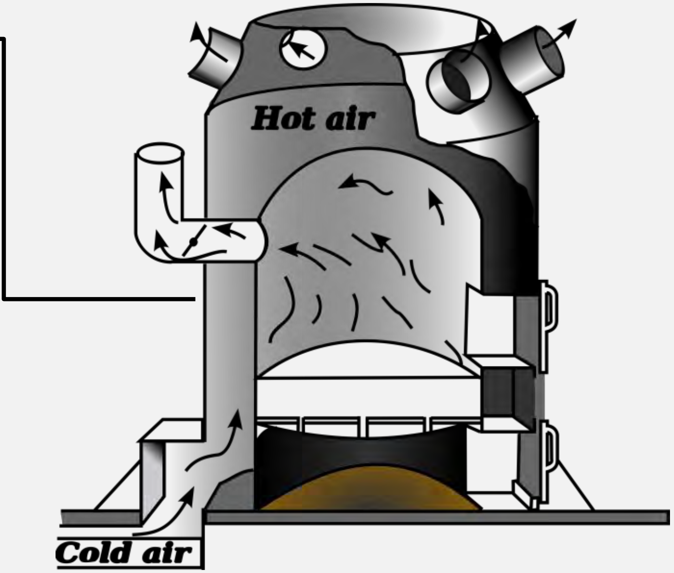
Process control

Process control automation

(Nest because it's so cute!)

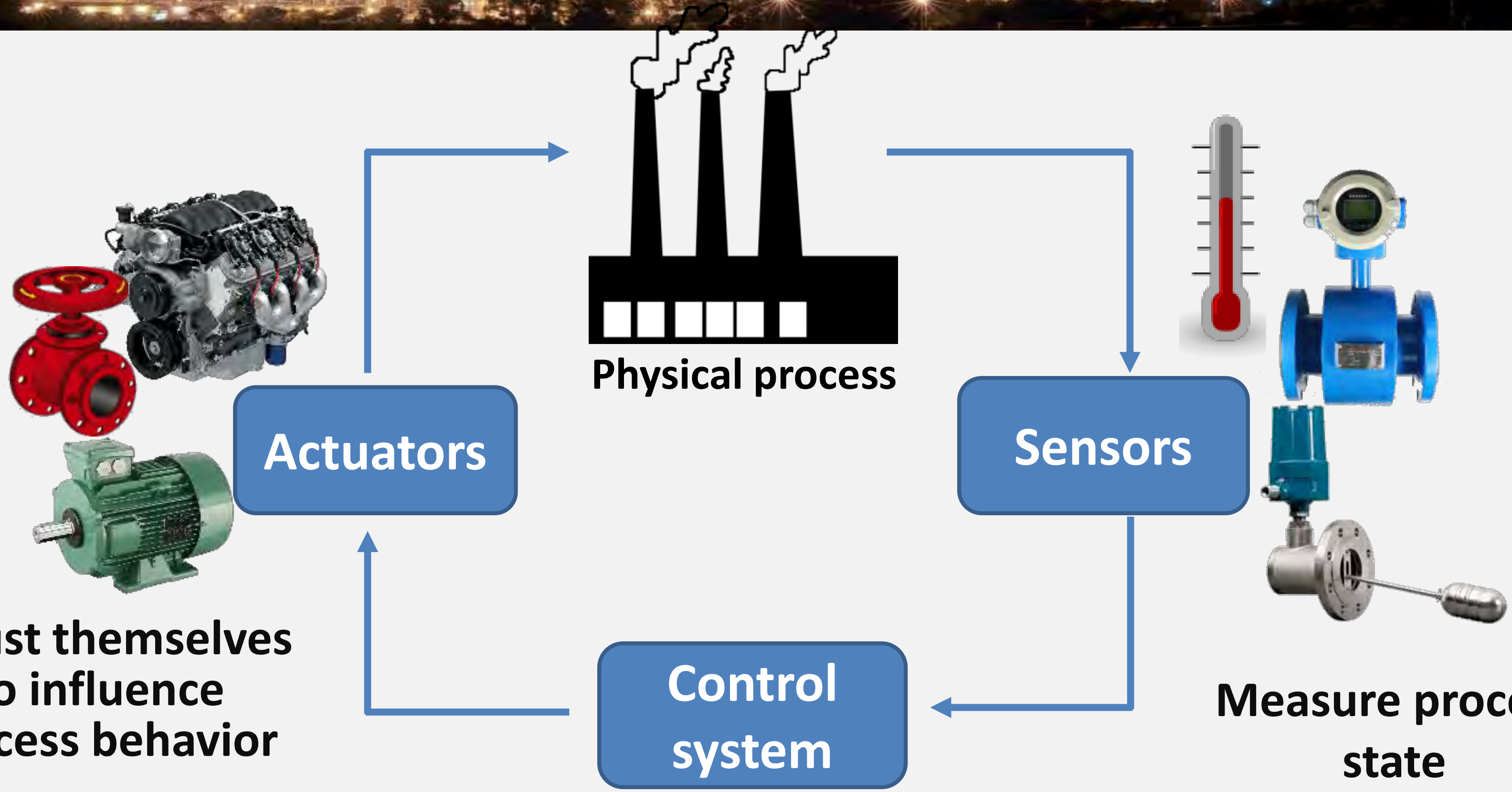


Set point



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

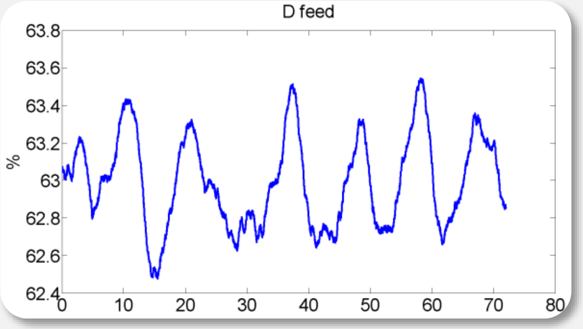
Sensors

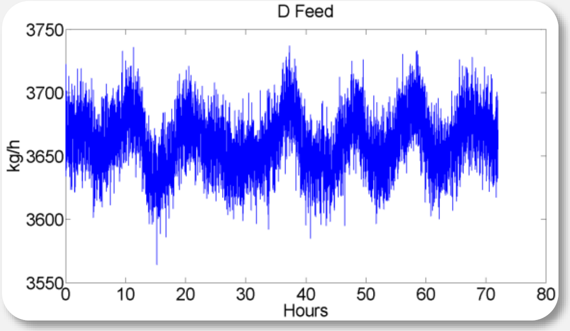
Control system

Adjust themselves to influence process behavior

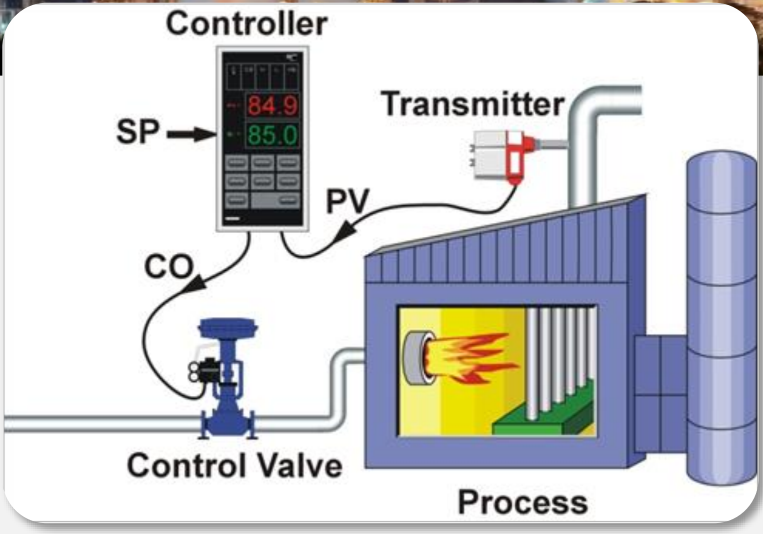
Measure process state

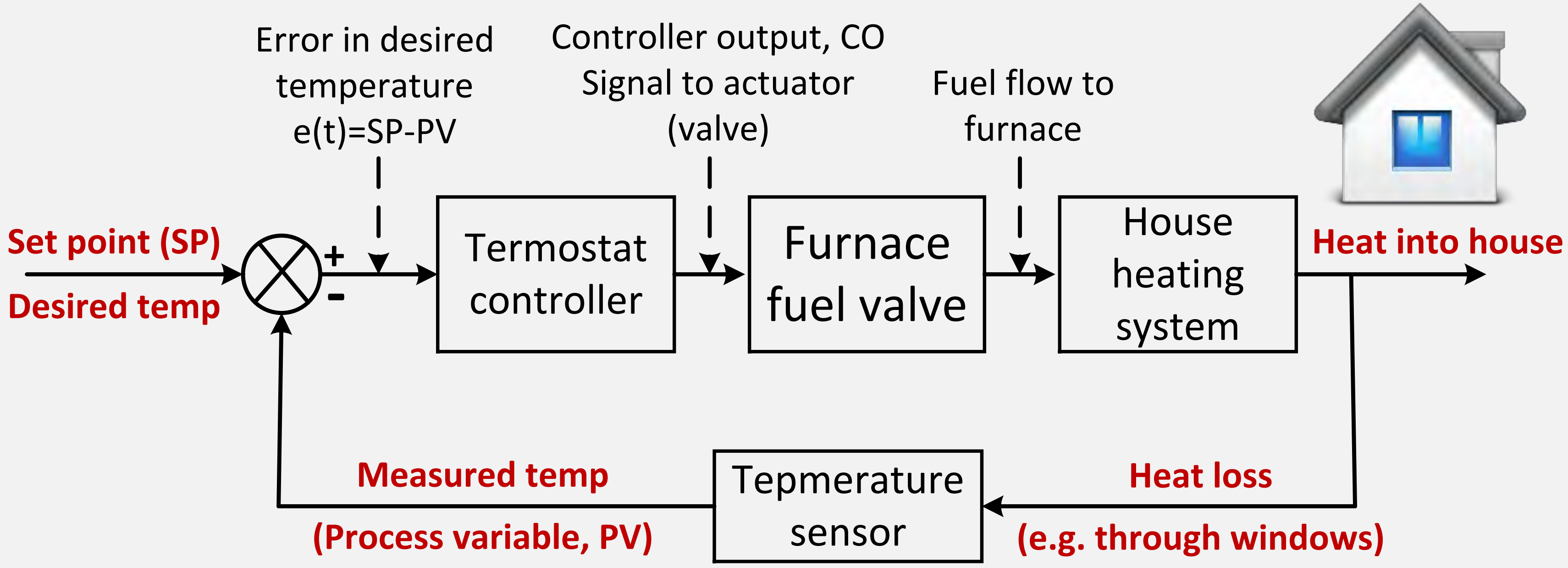
Computes control commands for actuators





Control system





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

Controller output, CO Signal to actuator (valve)

Fuel flow to furnace

Set point (SP)

Desired temp

+

-

Termostat controller

Furnace fuel valve

House heating system

Heat into house

Measured temp

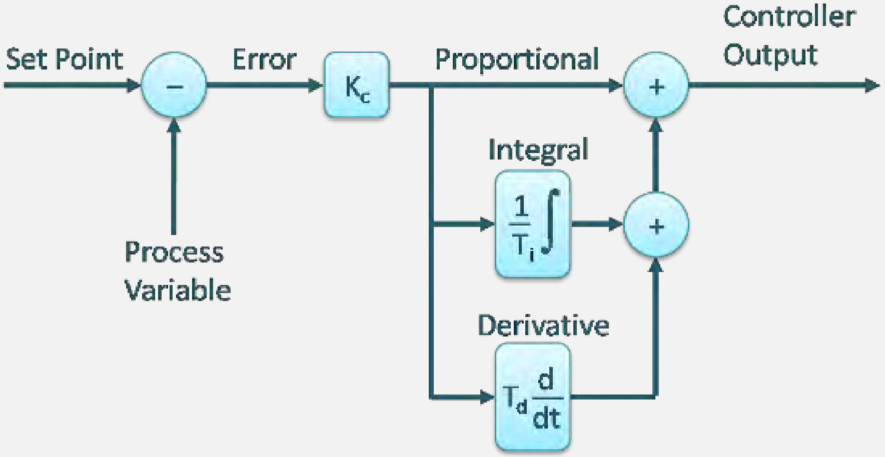
(Process variable, PV)

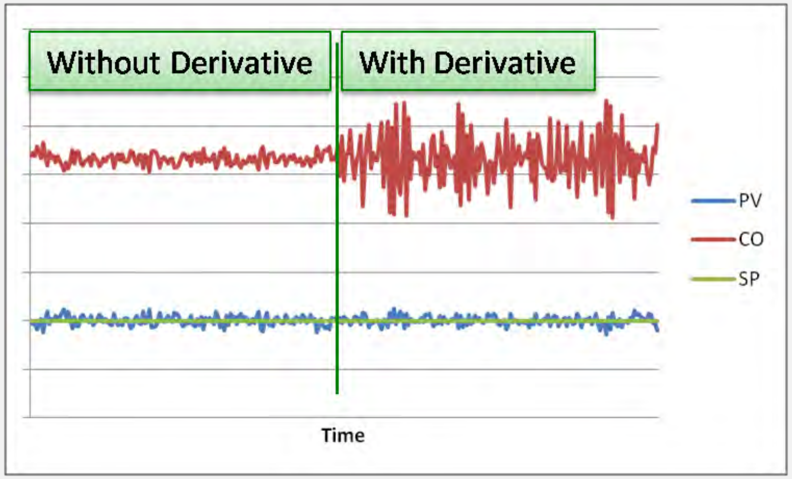
Tepmerature sensor

Heat loss

(e.g. through windows)

PID control





$$u(t) = \mathrm{MV}(t) = K_p e(t) + K_i \int_0^t e(\tau)\, d\tau + K_d \frac{d}{dt} e(t)$$

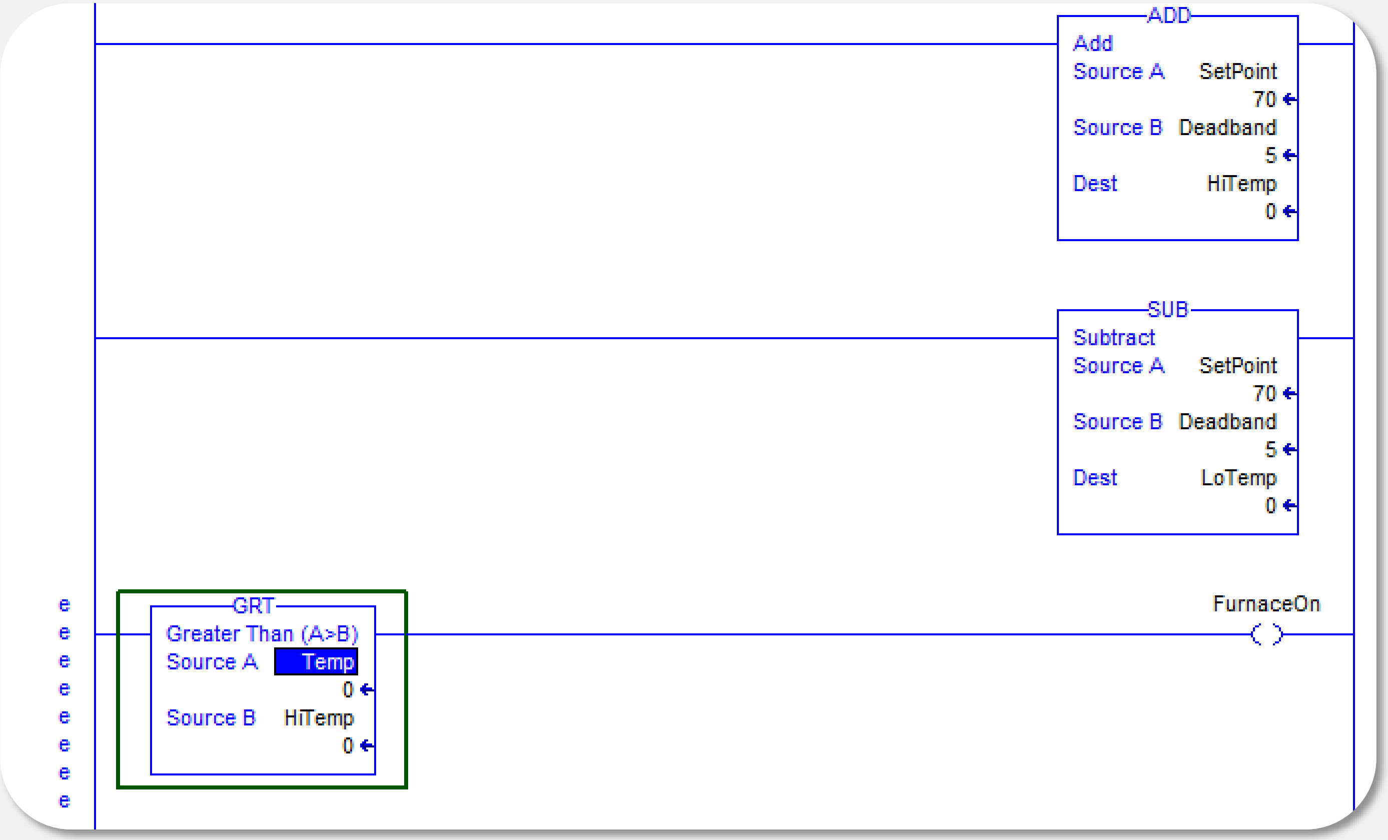
- ❑ **PID: proportional, integral, derivative –** most widely used control algorithm on the planet
- ❑ Sum of 3 components make final control signal
- ❑ Full PID control is hard(er) and used for tight control (e.g. temperature in the reactor)

Jacques Smuts „Process Control for Practitioners“

Control logic

- Obviously control logic gets more complex than a thermostat
- You’ll need something bigger than a thermostat to handle it all
- Most of the time this is a programmable logic controller (PLC)
- It is programmed graphically most of the time

Control logic



ADD
Add
Source A SetPoint
70
Source B Deadband
5
Dest HiTemp
0

SUB
Subtract
Source A SetPoint
70
Source B Deadband
5
Dest LoTemp
0

GRT
Greater Than (A>B)
Source A Temp
0
Source B HiTemp
0

FurnaceOn

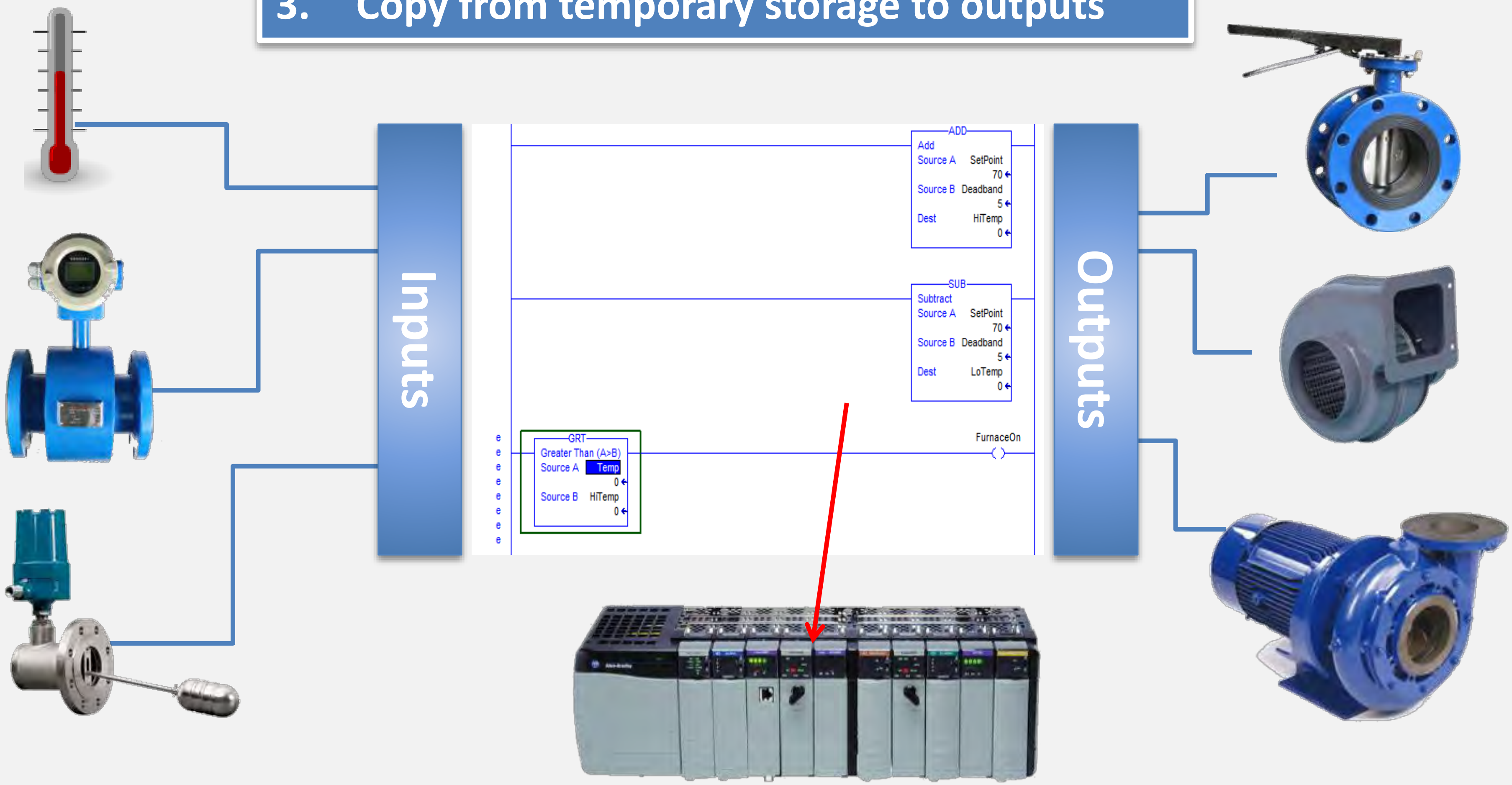
Computer scientists: Nooooooo!!!! Just give me a real language!

PLC internals

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

Sensors

Actuators



Inputs

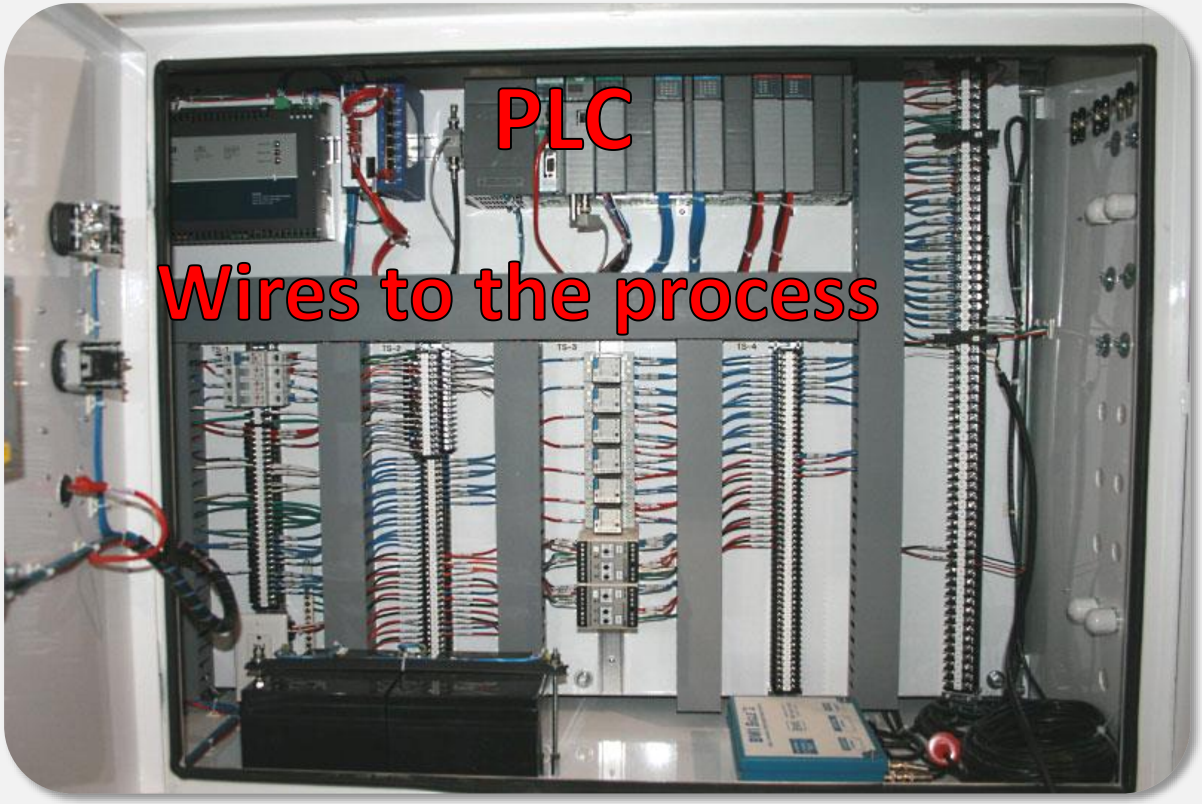
Outputs

```
ADD
Add
Source A   SetPoint
                 70
Source B   Deadband
                  5
Dest         HiTemp
                  0

SUB
Subtract
Source A   SetPoint
                 70
Source B   Deadband
                  5
Dest         LoTemp
                  0

GRT
Greater Than (A>B)
Source A   Temp
              0
Source B   HiTemp
              0

FurnaceOn
( )
```

Field communication

- 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

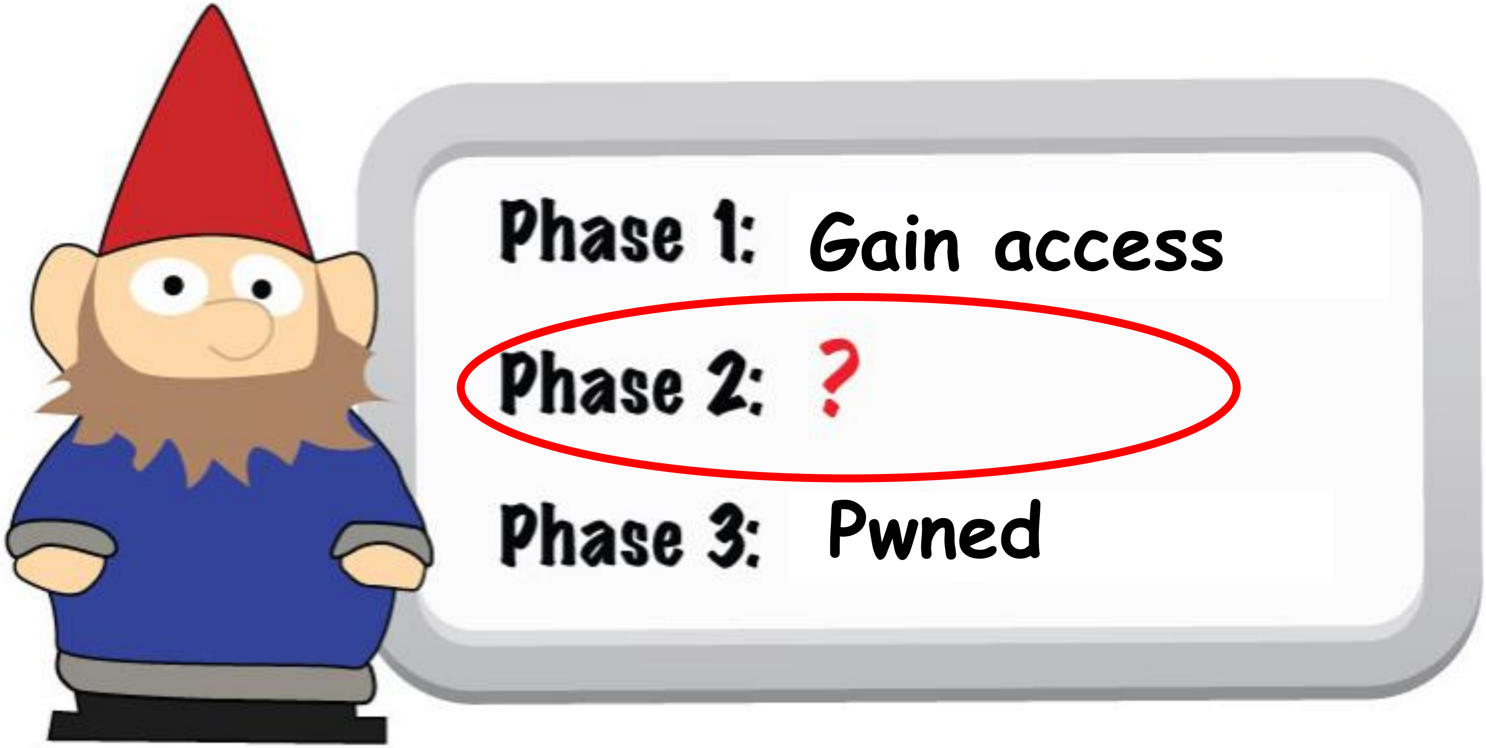
PLC cannot do it alone

□ PLC does not have the complete picture and time trends

□ Human operators watch the process 7/24

IT hacking vs. OT hacking

OT hacking



Phase 1: Gain access

Phase 2: ?

Phase 3: Pwned

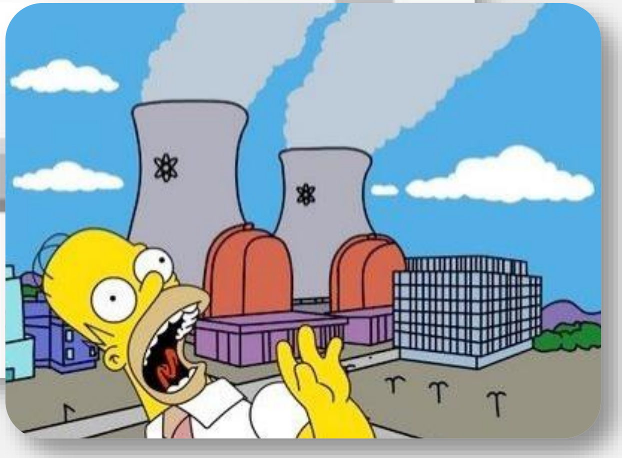
OT hacking

OT hacking

Phase 1: Gain access

Phase 2: ?

Phase 3: Pwned

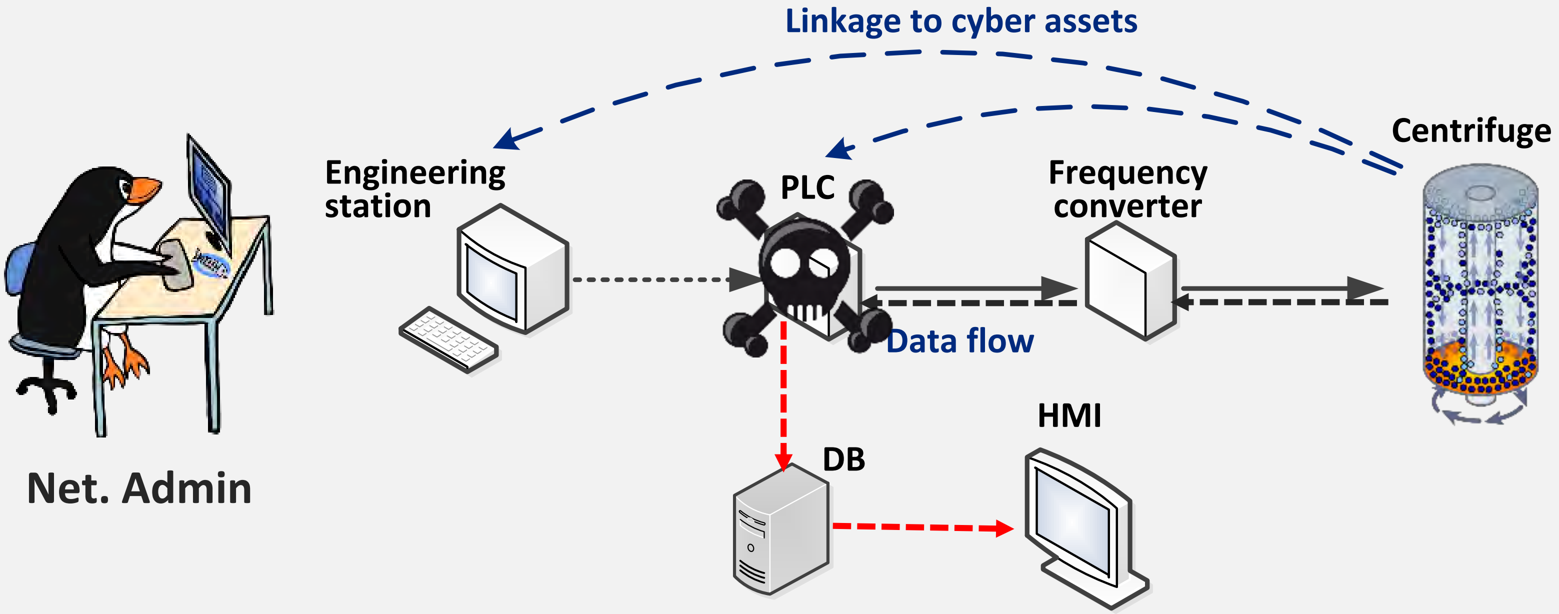


OT wizardry

> ***You can do unfocused and uncontrolled magic without a wand but to do really good spells, yes, you need a wand.***
>
> *Joanne Rowling, 2001*

- 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
- In the context of OT hacking the “focused magic” is achieved with control theory methods

Example: attack on process data flow



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

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

Operator

I am not controlling the process!!

OT hacker

Controllability

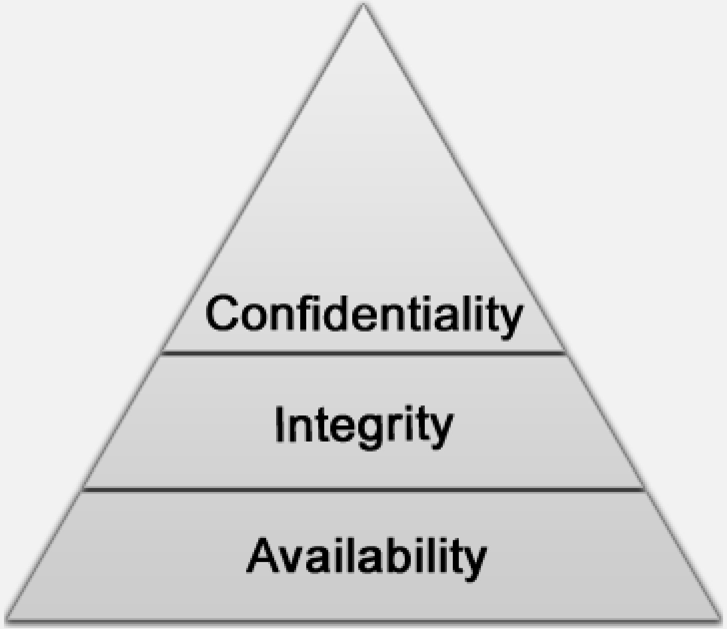
1000
800
1200
600
1400
400
1600
200
1800
0
2000

Observability

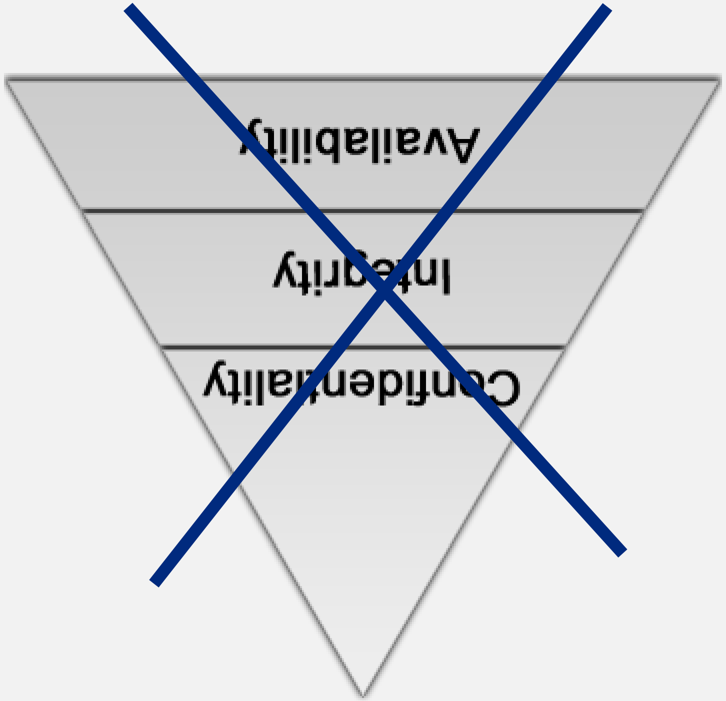
- ❑ During the attack the hacker herself must be process engineer, control engineer and process operator
- ❑ **Process operator and hacker rival for control over the process**

Process-related security properties

HOLY TRINITY



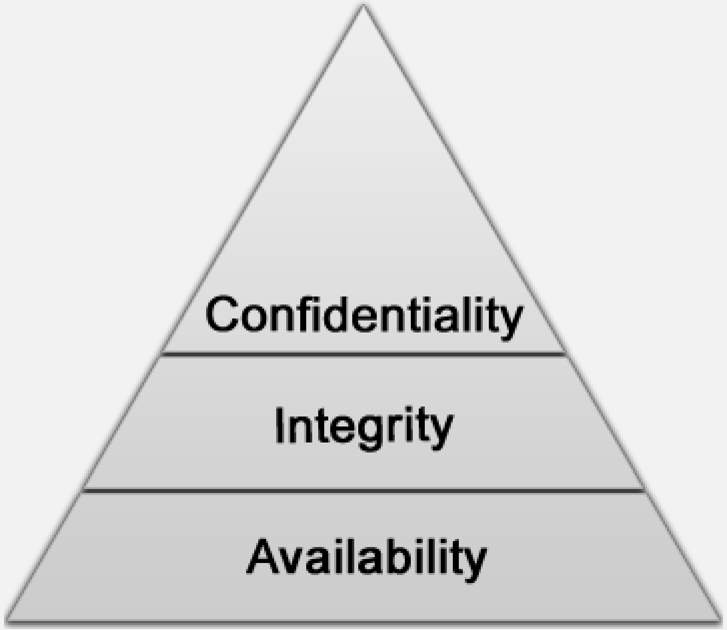
IT domain



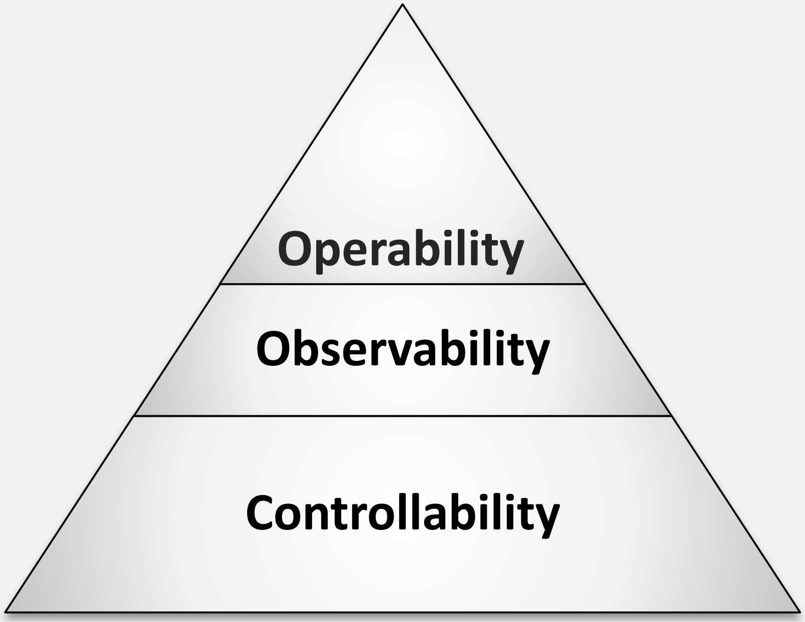
Process control

Process-related security properties

HOLY TRINITY



IT domain



Process control

Process-related security properties

HOLY TRINITY

CIA

Information security

CO2

Process control security

Haters gonna hate…

Process control challenges

- There are some things in a process that are impossible to understand or model
- All is not lost, the process can still be (controllably) destabilized

Consider a car and a driver

- The attacker wants to drive the car off the road
  - She has control of the brakes
- The attacker closes the left front brake 100% and the car pulls to the left
- The driver compensates by steering to the right eventually coming back into a straight line

Consider a car and a driver

❑ The attacker responds by letting go of the left brake and applying the right brake 100%

❑ The driver responds by steering to the right until the car is straight again

❑ The attacker responds by swapping back and forth between the brakes

❑ **The driver responds by steering back and forth to the rhythm of the brakes keeping the car more-or-less straight**

Consider a car and a driver

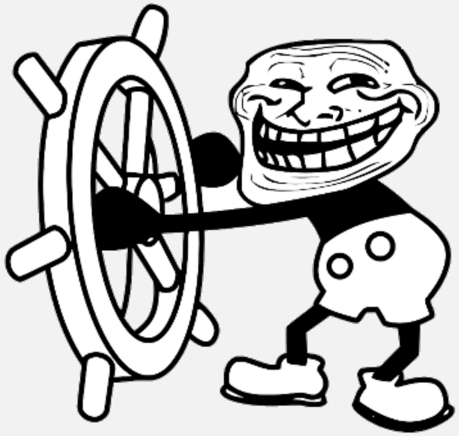
- The attacker responds by swapping brakes whenever the driver starts to compensate
- Eventually the attacker will win since a computer is faster than a human

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

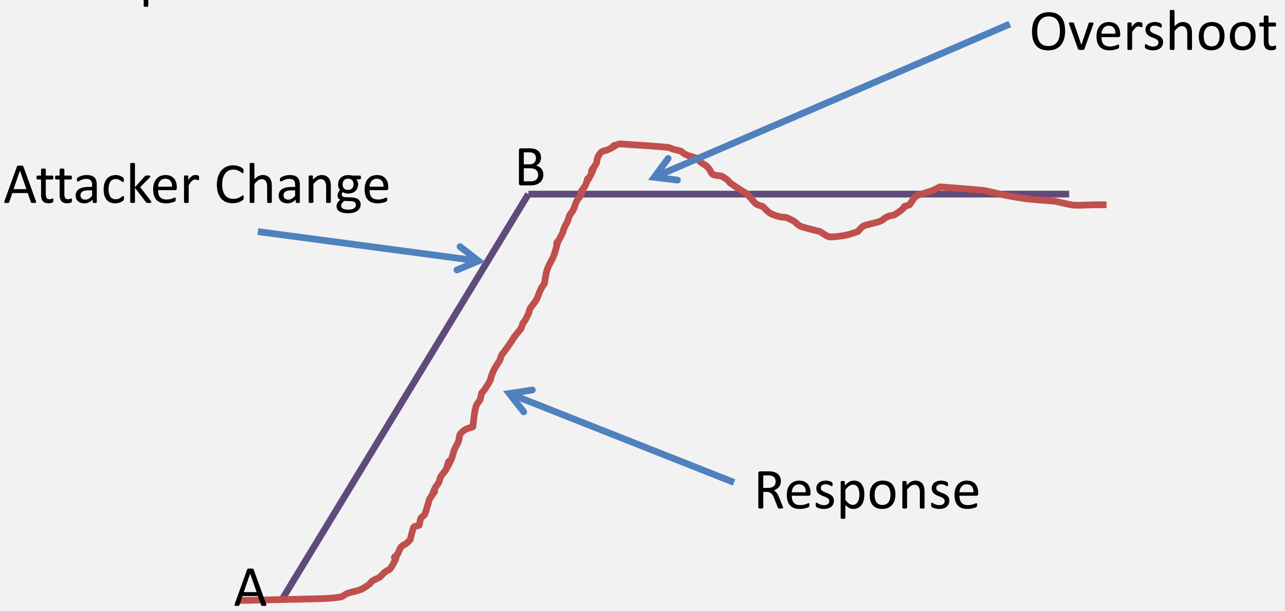
Controlled uncontrollability

- Multi-Adaptive algorithms work just like PID autotuners 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**



Proportional

$$U_p = Ke(t) + U_b$$



Overshoot

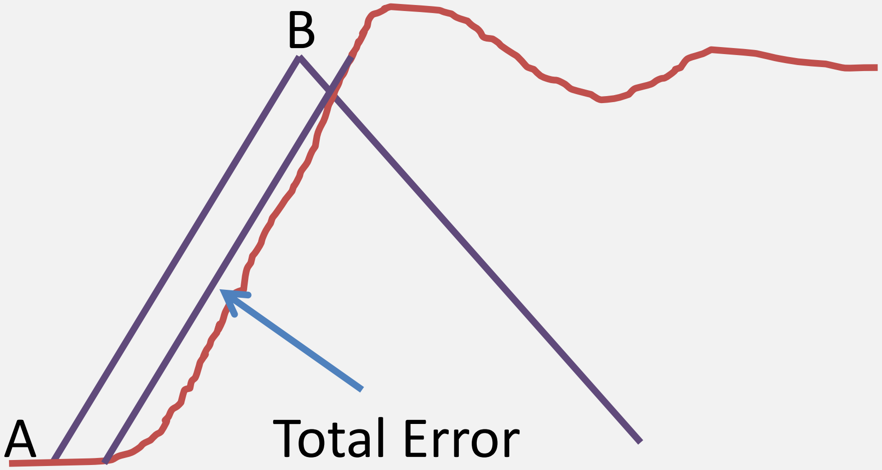
Attacker Change

Response

Adjust the slope of AB to maximize overshoot

Integral

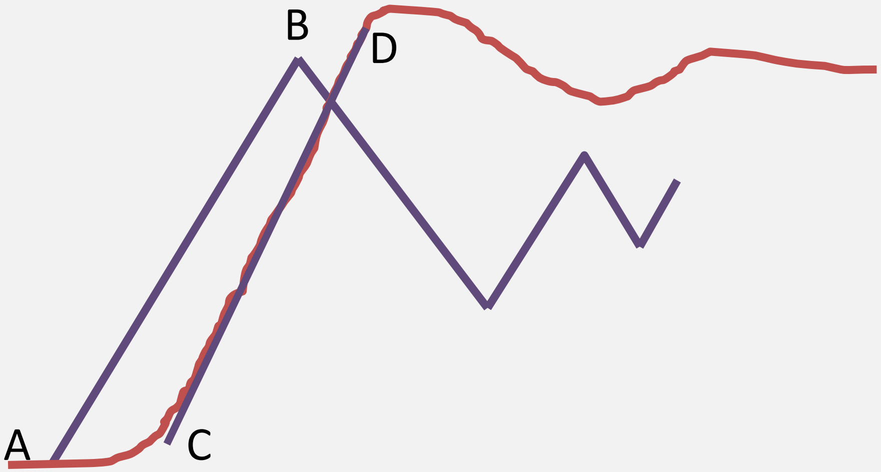
$U_I(t)=K/T_i*Sum(e(t)+u(0))$



If that fails, adjust period of AB->AB maximizing the running total error

Derivative

$$U_d(t)=KT_d*de(t)/dt$$



If that fails, adjust the rate of period change to maximize the angle between AB and CD

Demo

<Robotic arm demo here>

Multi-adaptive

- A single algorithm can be used as a payload to disrupt many types of processes
- Crash a car or overpressure a loop
- Correlation engines can be used to automatically pair actuators with sensors
- Think of this as process “fuzzing”

Get the party started!

Car vs. plant hacking

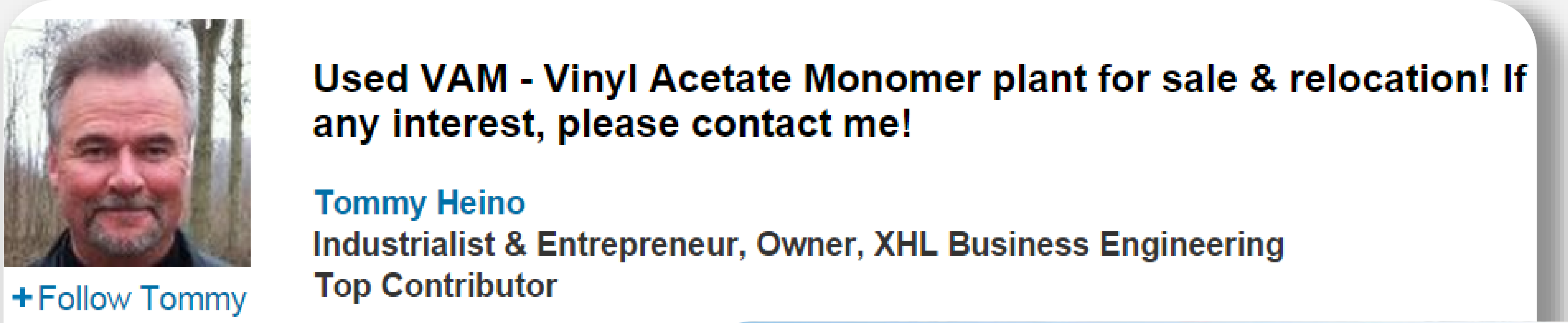
It is not about the size

It is about MONEY

Plants are ouch! how expensive

Plants for sale

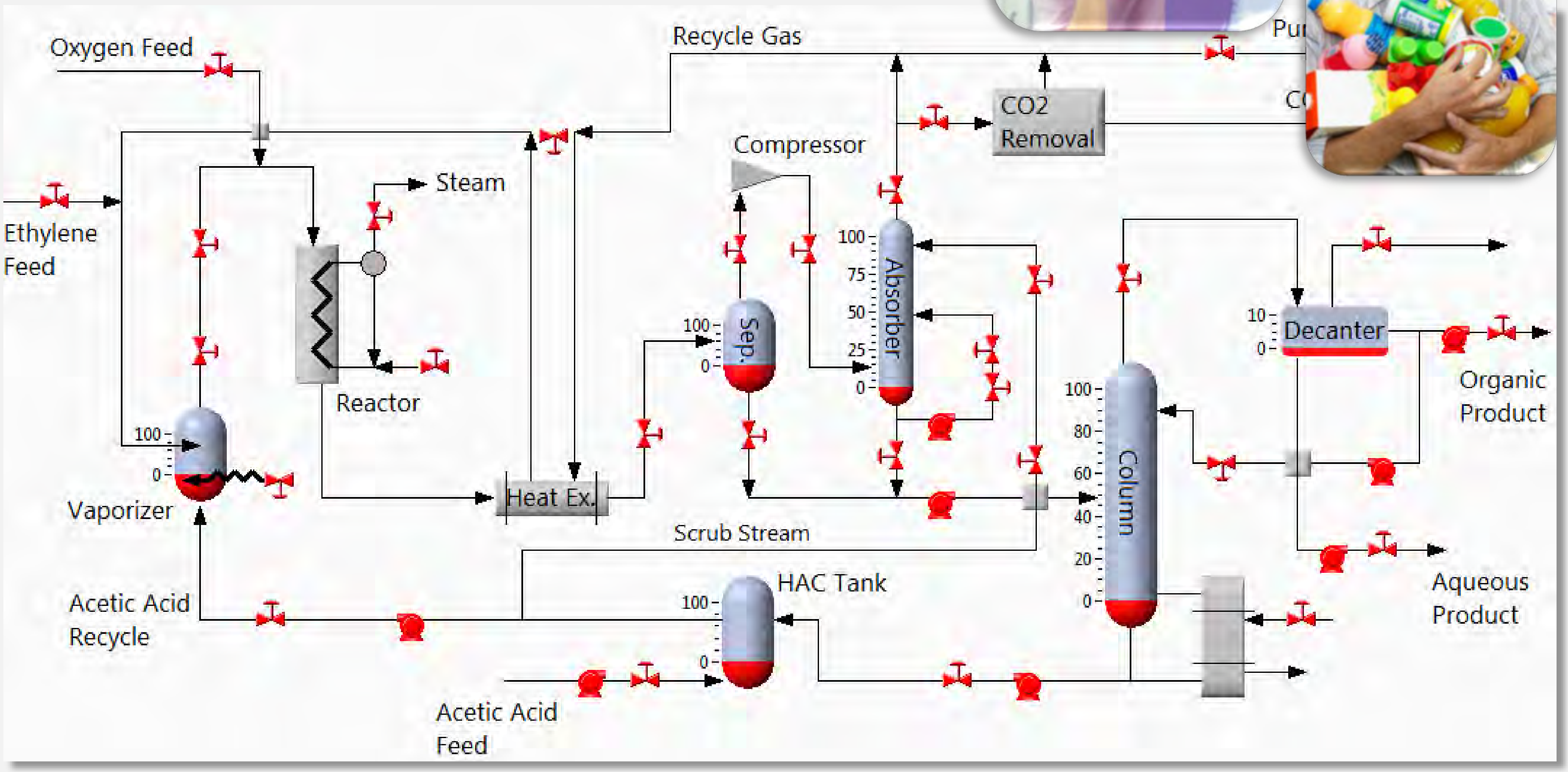
From LinkedIn, really ;-)



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

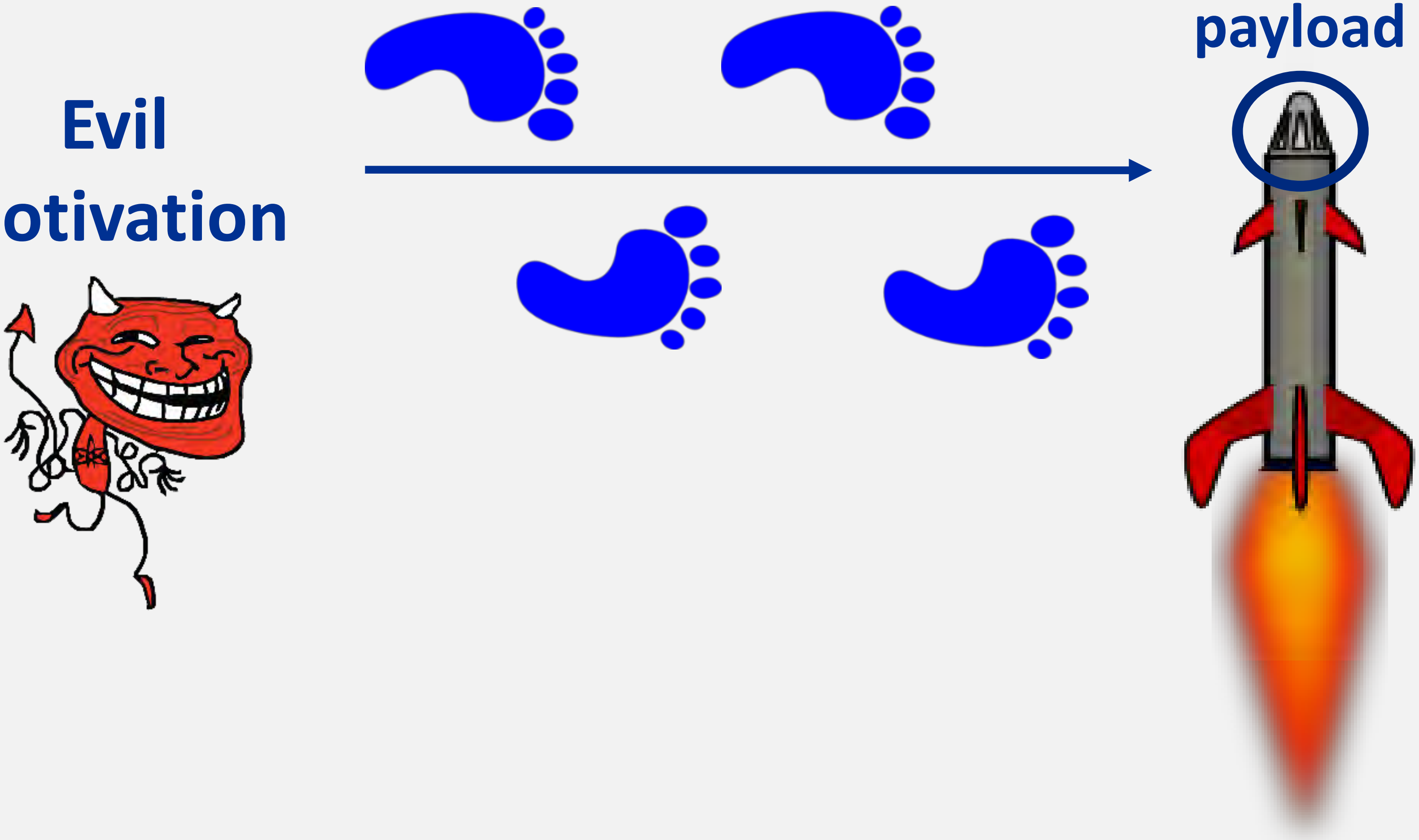
Vinyl Acetate Monomer plant (model)



Stages of cyber-physical attacks

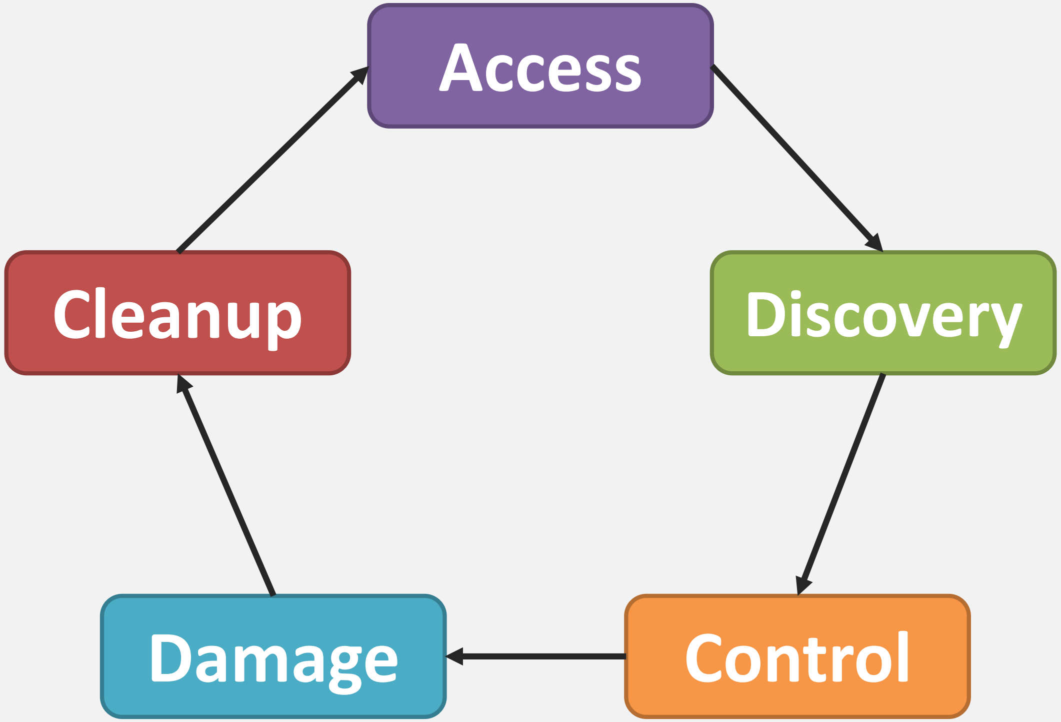
Attack objective

Evil motivation



Cyber-physical payload

Stages of SCADA attack



Access

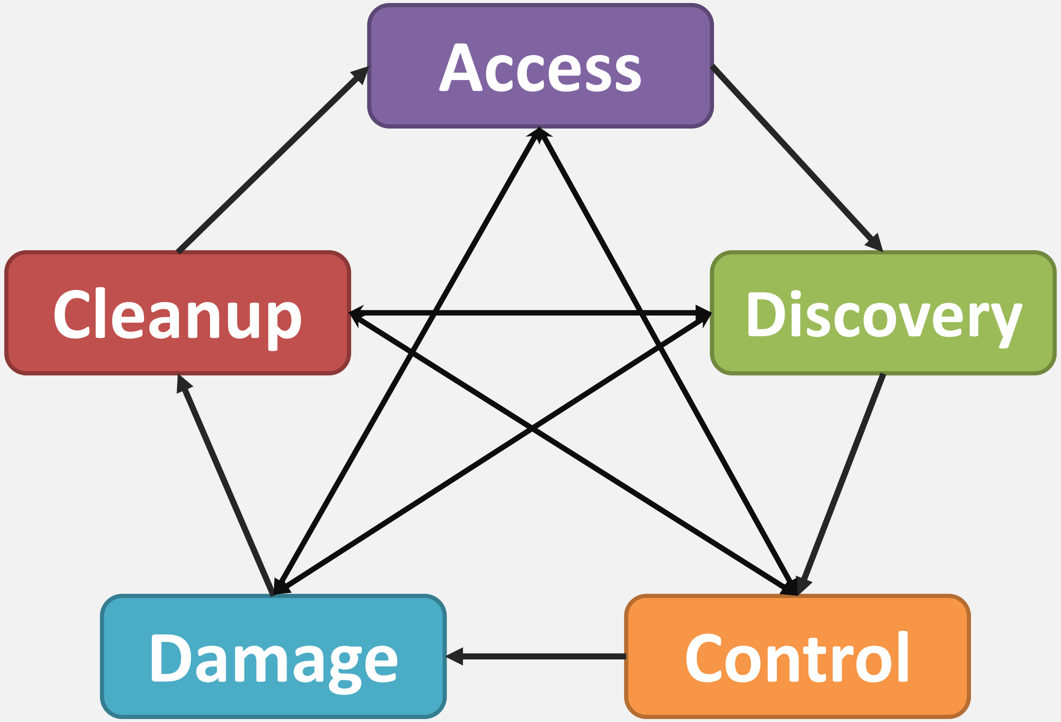
Discovery

Control

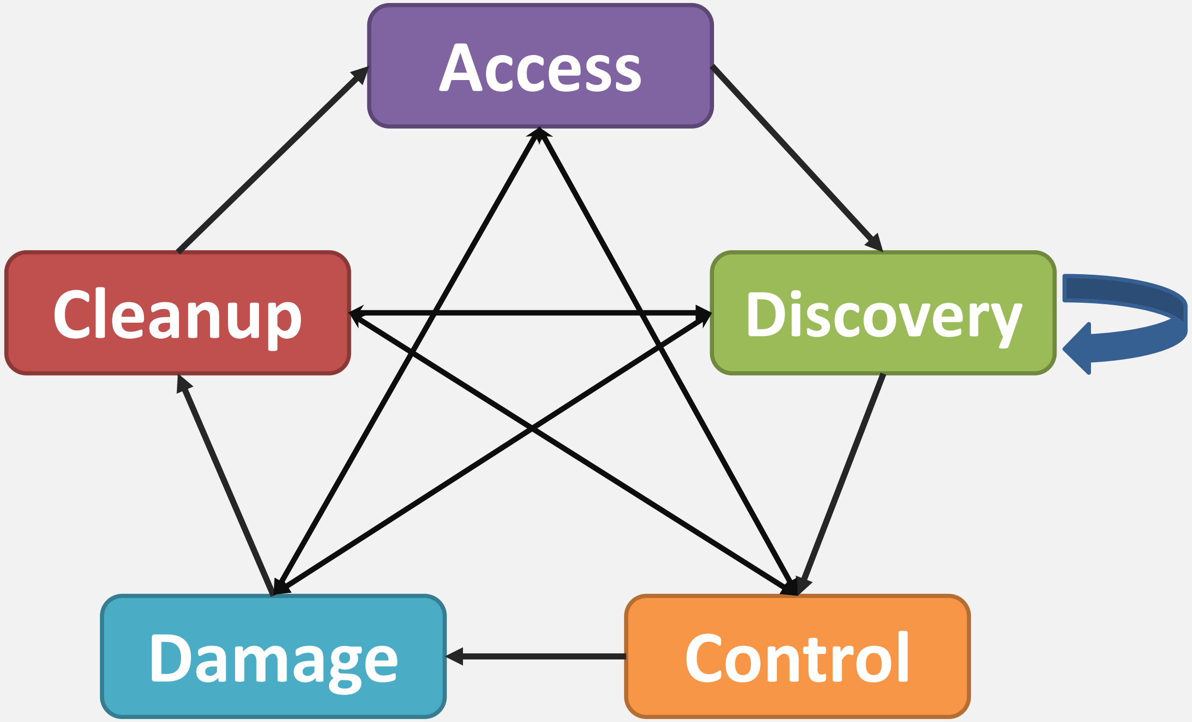
Damage

Cleanup

Stages of SCADA attack



Stages of SCADA attack



Access

Discovery

Control

Damage

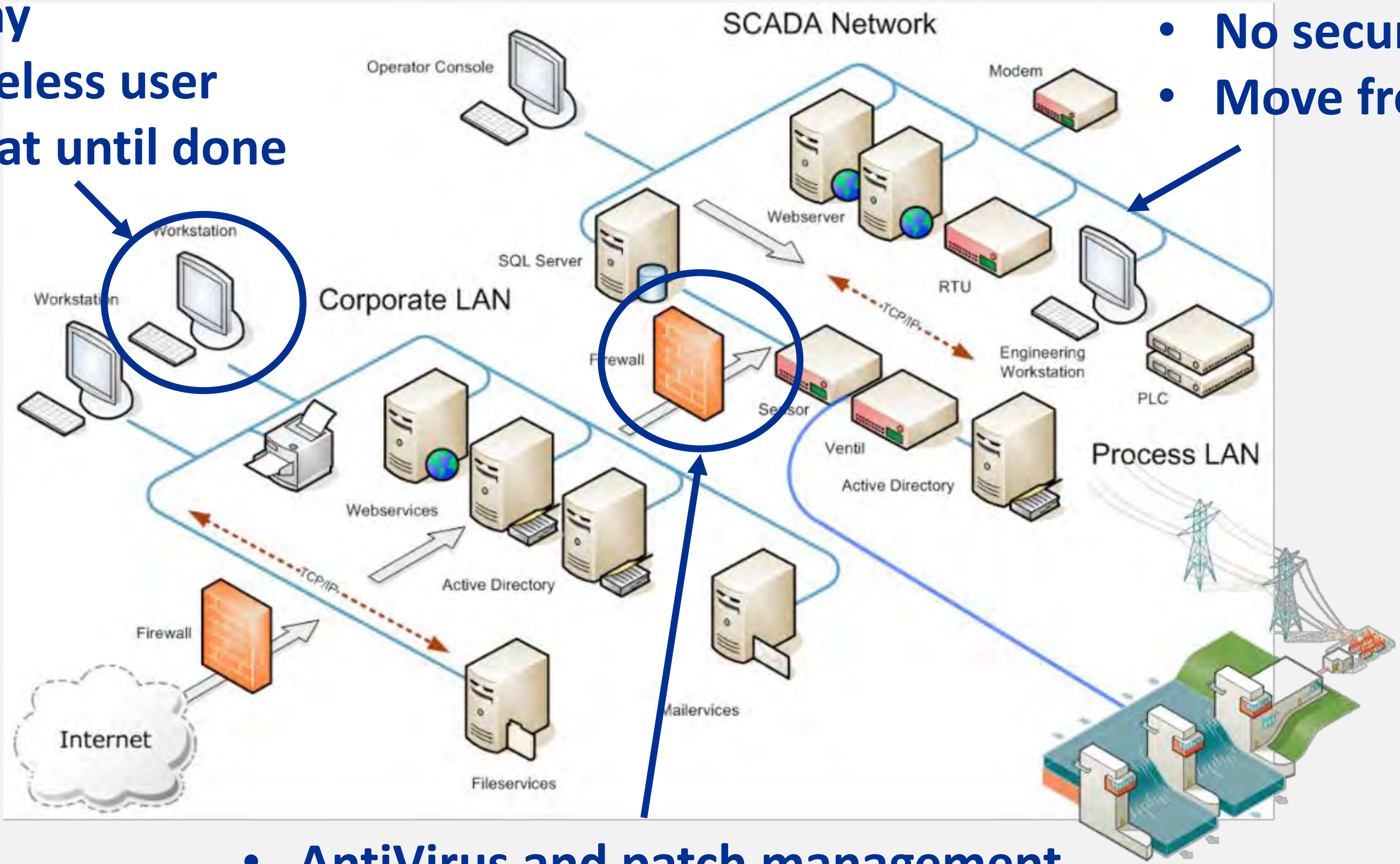
Cleanup

Access

Traditional IT hacking

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

- No security
- Move freely



- AntiVirus and patch management
- Database links
- Backup systems

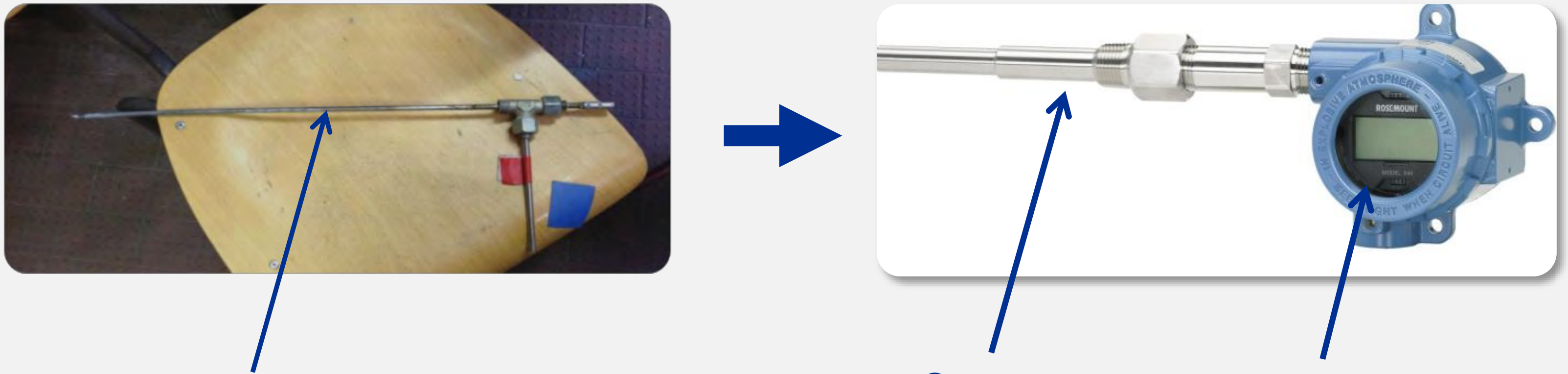
Smart instrumentation

□ Converts analog signal into digital

□ Sensors pre-process the measurements

□ May send data directly to actuators

□ IP-enabled (part of the “Internet-of-Things”)



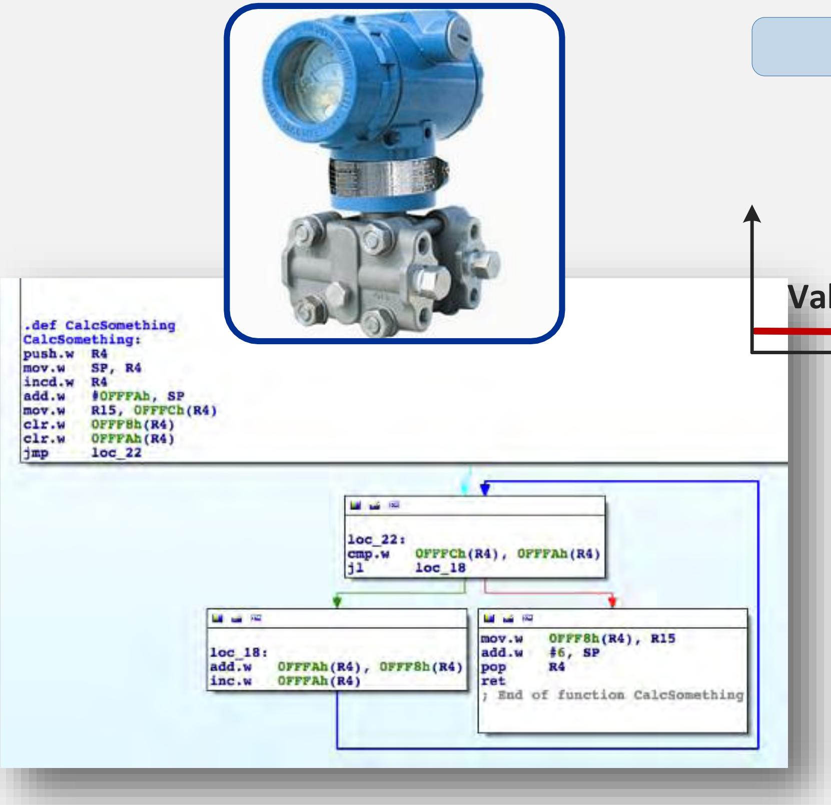
Old generation temperature sensor

Sensor

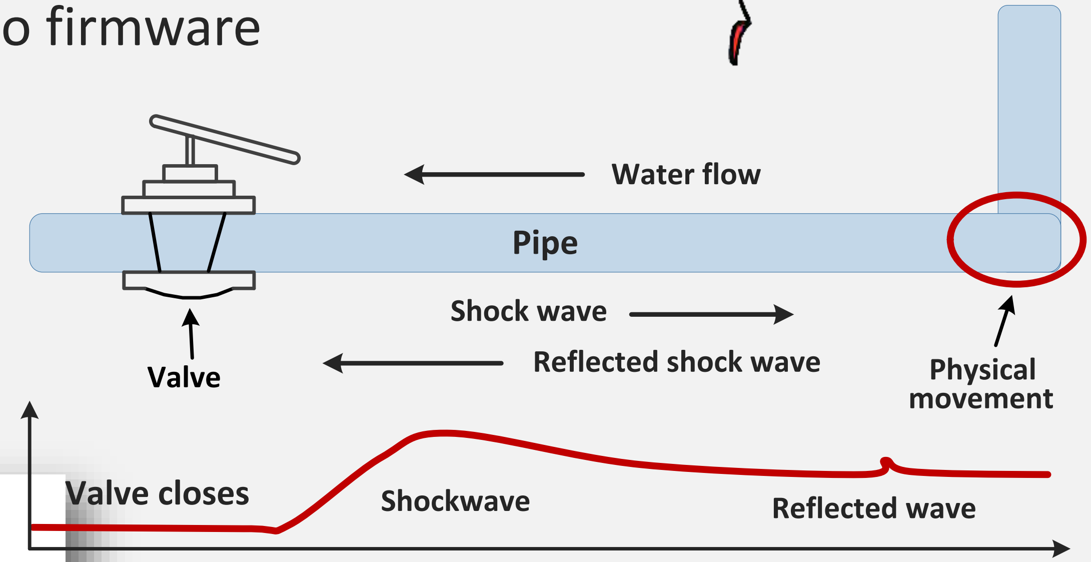
Computational element

Invading field devices

- ❑ Jason Larsen at Black Hat’15 “Miniaturization”
  - ○ Inserting rootkit into firmware



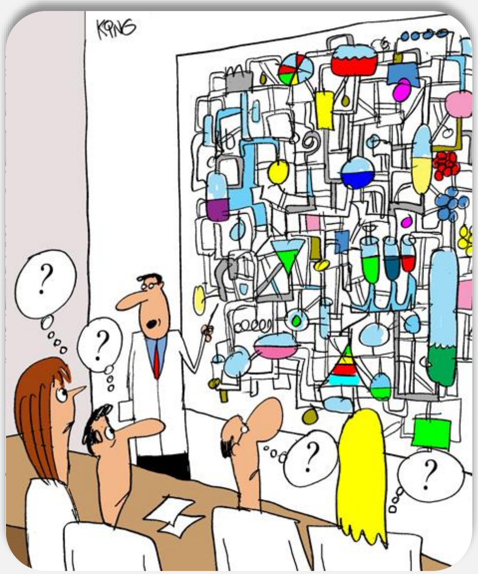
```
.def CalcSomething
CalcSomething:
push.w  R4
mov.w   SP, R4
incd.w  R4
add.w   #0FFFAh, SP
mov.w   R15, 0FFFCh(R4)
clr.w   0FFF8h(R4)
clr.w   0FFFAh(R4)
jmp     loc_22

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

Process discovery



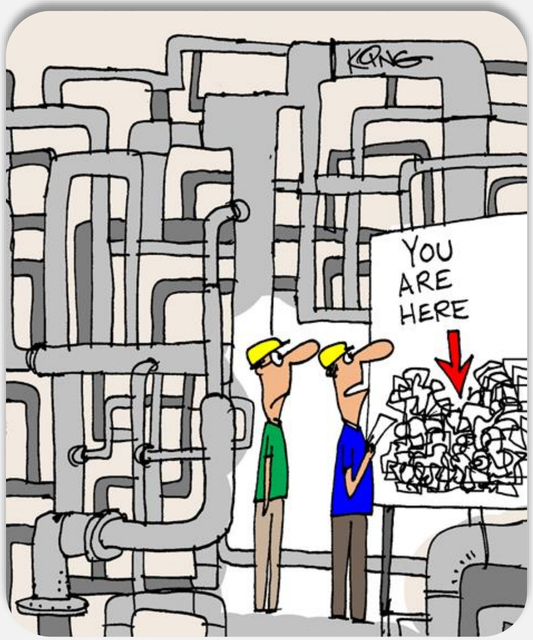
What and how the process is producing

Espionage

How it is controlled

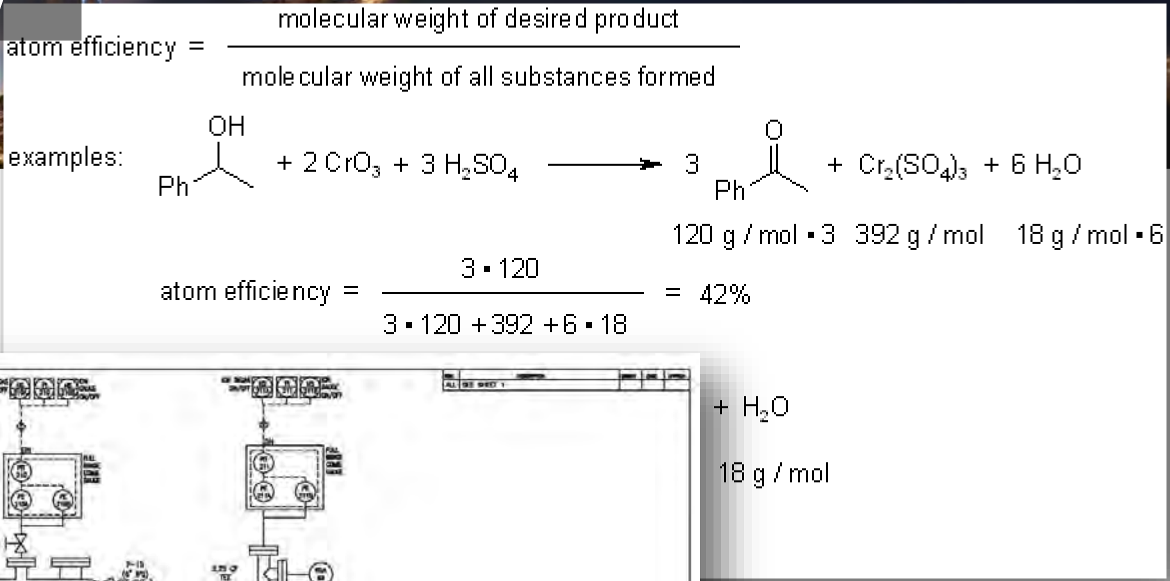
Espionage, reconnaissance

Espionage, reconnaissance



How it is build and wired

Process discovery



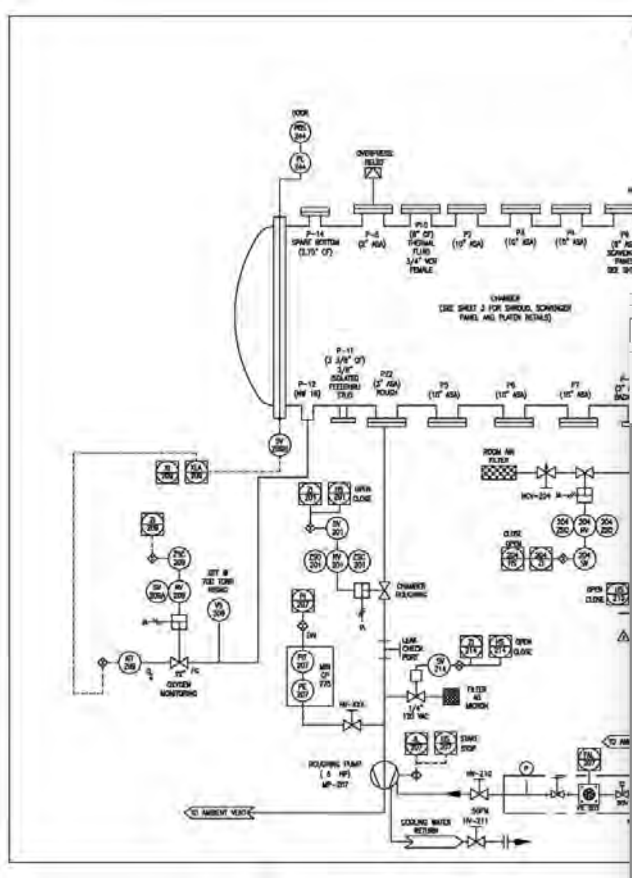
$$\text{atom efficiency} = \frac{\text{molecular weight of desired product}}{\text{molecular weight of all substances formed}}$$

examples:

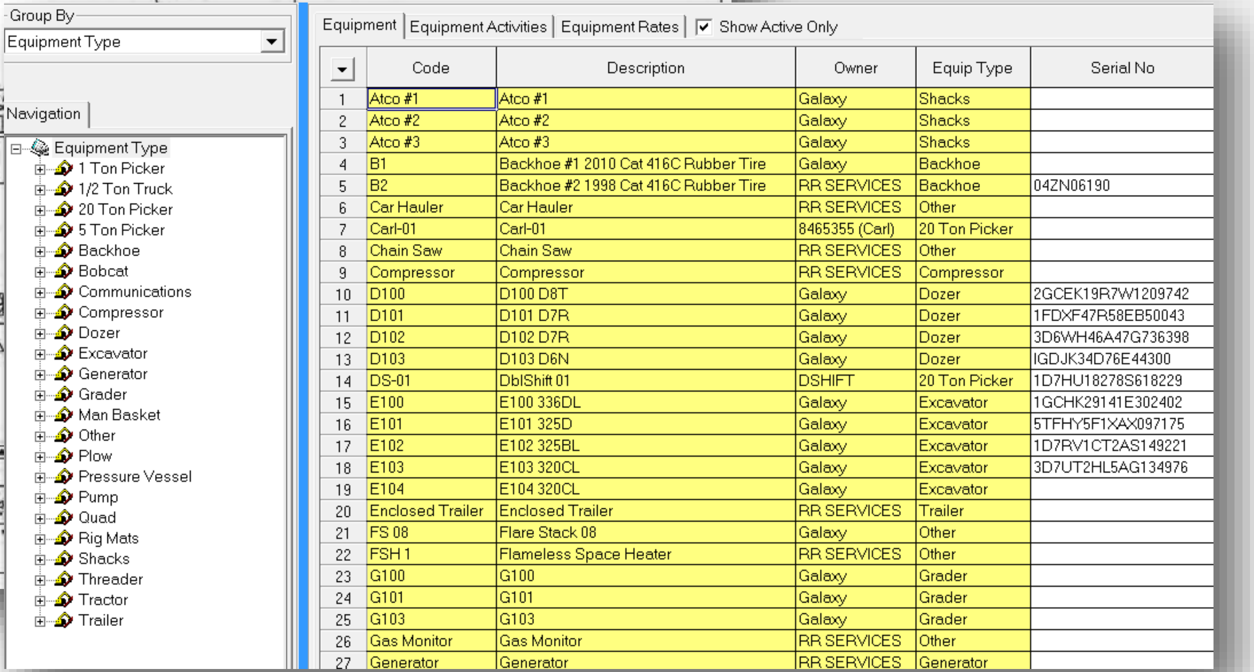
120 g / mol • 3 392 g / mol 18 g / mol • 6

$$\text{atom efficiency} = \frac{3 \cdot 120}{3 \cdot 120 + 392 + 6 \cdot 18} = 42\%$$

18 g / mol



OVERPRESS RELIEF
HCV-201
HCV-202
CHAMBER (SEE SHEET 3 FOR SHROUD, SCAVENGER PANEL AND PLATEN DETAILS)
OXYGEN MONITORING
ROUGHING PUMP (6 HP) MP-207
TO AMBIENT VENT
COOLING WATER RETURN



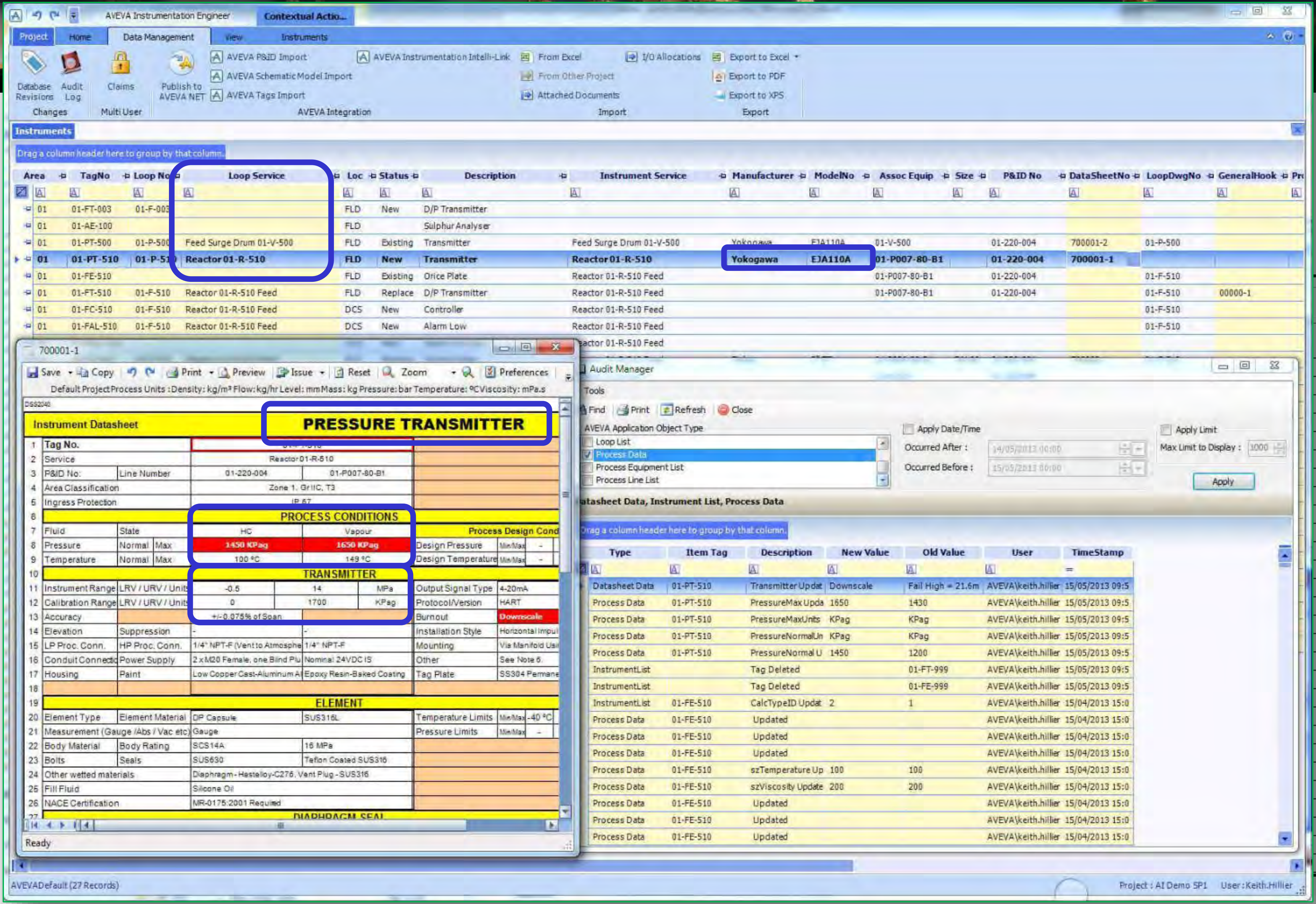
Group By
Navigation
Equipment | Equipment Activities | Equipment Rates | ☑ Show Active Only

Group By: Equipment Type

- Equipment Type
  - 1 Ton Picker
  - 1/2 Ton Truck
  - 20 Ton Picker
  - 5 Ton Picker
  - Backhoe
  - Bobcat
  - Communications
  - Compressor
  - Dozer
  - Excavator
  - Generator
  - Grader
  - Man Basket
  - Other
  - Plow
  - Pressure Vessel
  - Pump
  - Quad
  - Rig Mats
  - Shacks
  - Threader
  - Tractor
  - Trailer

	Code	Description	Owner	Equip Type	Serial No
1	Atco #1	Atco #1	Galaxy	Shacks	
2	Atco #2	Atco #2	Galaxy	Shacks	
3	Atco #3	Atco #3	Galaxy	Shacks	
4	B1	Backhoe #1 2010 Cat 416C Rubber Tire	Galaxy	Backhoe	
5	B2	Backhoe #2 1998 Cat 416C Rubber Tire	RR SERVICES	Backhoe	04ZN06190
6	Car Hauler	Car Hauler	RR SERVICES	Other	
7	Carl-01	Carl-01	8465355 (Carl)	20 Ton Picker	
8	Chain Saw	Chain Saw	RR SERVICES	Other	
9	Compressor	Compressor	RR SERVICES	Compressor	
10	D100	D100 D8T	Galaxy	Dozer	2GCEK19R7W1209742
11	D101	D101 D7R	Galaxy	Dozer	1FDXF47R58EB50043
12	D102	D102 D7R	Galaxy	Dozer	3D6WH46A47G736398
13	D103	D103 D6N	Galaxy	Dozer	IGDJK34D76E44300
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	

Process discovery



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

700001-1

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

DSS2040

Instrument Datasheet — **PRESSURE TRANSMITTER**

1	Tag No.		[illegible]				
2	Service		Reactor 01-R-510				
3	P&ID No:	Line Number	01-220-004	01-P007-80-B1			
4	Area Classification		Zone 1, Gr IIC, T3				
5	Ingress Protection		IP 67				
6	PROCESS CONDITIONS						
7	Fluid	State	HC	Vapour	Process Design Cond		
8	Pressure	Normal / Max	1450 KPag	1650 KPag	Design Pressure	Min/Max	-
9	Temperature	Normal / Max	100 °C	149 °C	Design Temperature	Min/Max	-
10	TRANSMITTER						
11	Instrument Range	LRV / URV / Units	-0.5	14 / MPa	Output Signal Type	4-20mA	
12	Calibration Range	LRV / URV / Units	0	1700 / KPag	Protocol/Version	HART	
13	Accuracy		+/-0.075% of Span		Burnout	Downscale	
14	Elevation	Suppression	-	-	Installation Style	Horizontal Impul	
15	LP Proc. Conn.	HP Proc. Conn.	1/4" NPT-F (Vent to Atmosphe	1/4" NPT-F	Mounting	Via Manifold Usi	
16	Conduit Connectio	Power Supply	2 x M20 Female, one Blind Plu	Nominal 24VDC IS	Other	See Note 6.	
17	Housing	Paint	Low Copper Cast-Aluminum Al	Epoxy Resin-Baked Coating	Tag Plate	SS304 Permane	
18							
19	ELEMENT						
20	Element Type	Element Material	DP Capsule	SUS316L	Temperature Limits	Min/Max	-40 °C
21	Measurement (Gauge /Abs / Vac etc)		Gauge		Pressure Limits	Min/Max	-
22	Body Material	Body Rating	SCS14A	16 MPa			
23	Bolts	Seals	SUS630	Teflon Coated SUS316			
24	Other wetted materials		Diaphragm - Hastelloy-C276, Vent Plug - SUS316				
25	Fill Fluid		Silicone Oil				
26	NACE Certification		MR-0175:2001 Required				
27	DIAPHRAGM SEAL						

Ready

Audit Manager

AVEVA Application Object Type

- □ Loop List
- ☑ Process Data
- □ Process Equipment List
- □ Process Line List

□ Apply Date/Time

Occurred After : 14/05/2013 00:00

Occurred Before : 15/05/2013 00:00

□ Apply Limit

Max Limit to Display : 1000

atasheet Data, Instrument List, Process Data

Drag a column header here to group by that column.

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

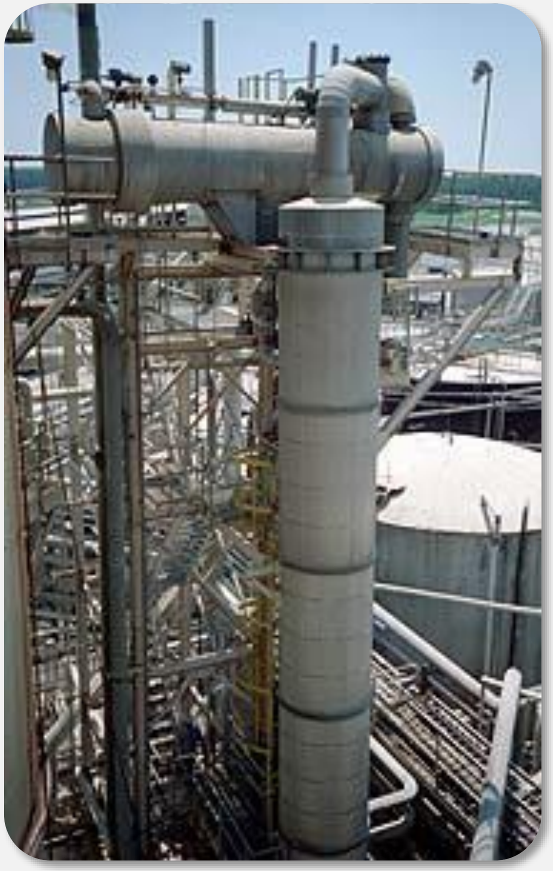
AVEVADefault (27 Records)

Project : AI Demo SP1 User : Keith.Hillier

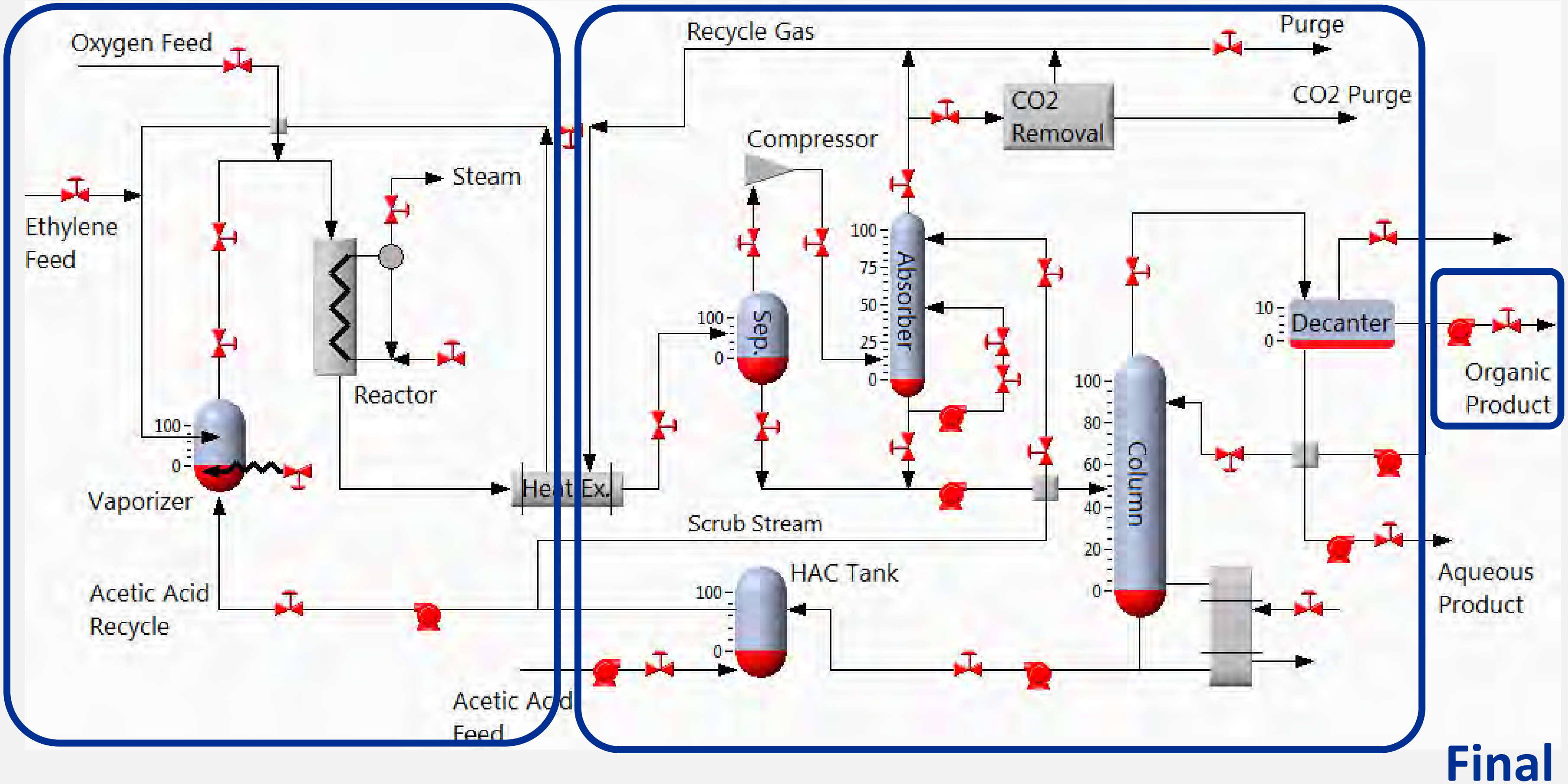
Know the equipment

Stripper is...

Stripping column



Max economic damage?

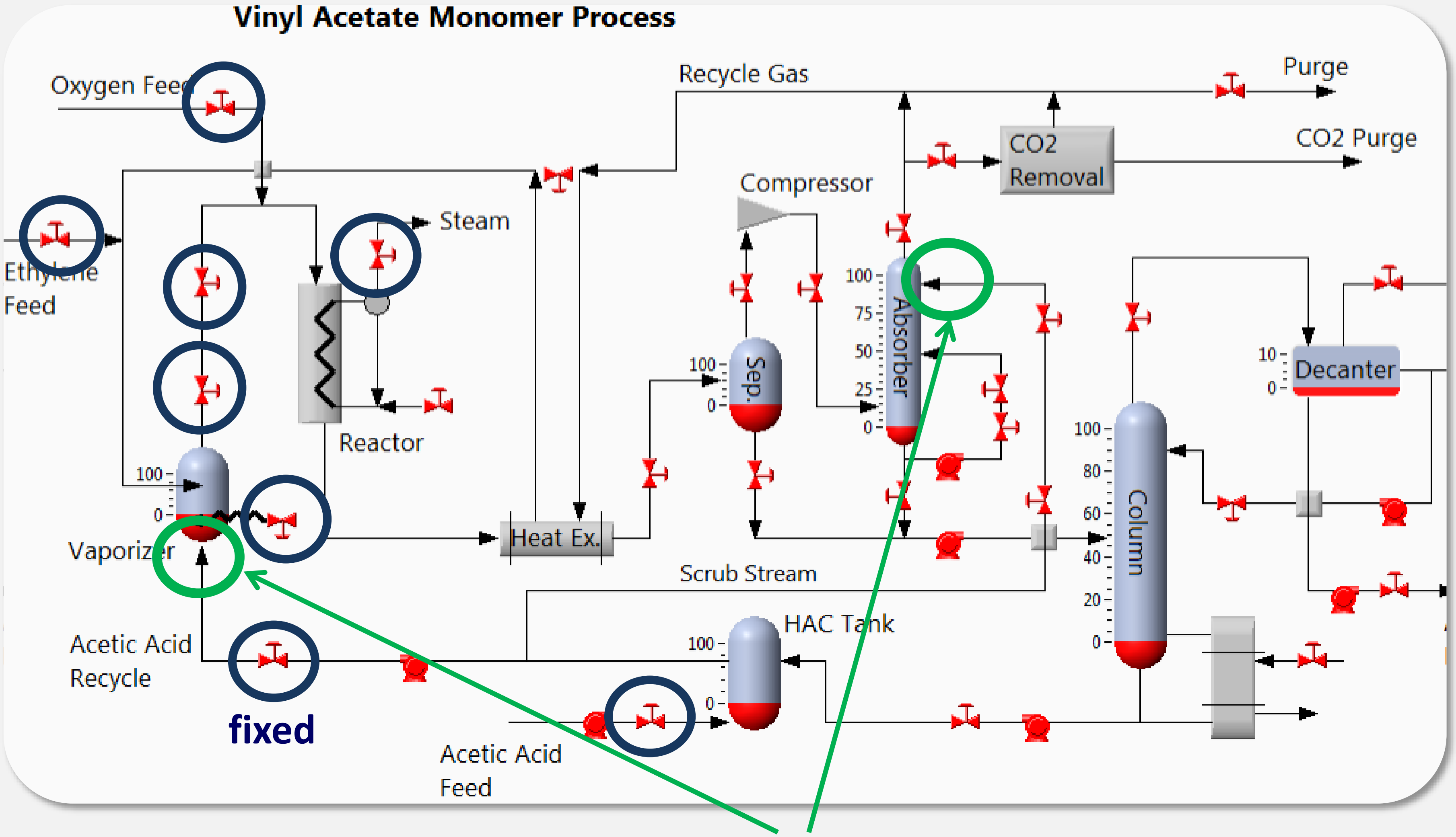


Reaction

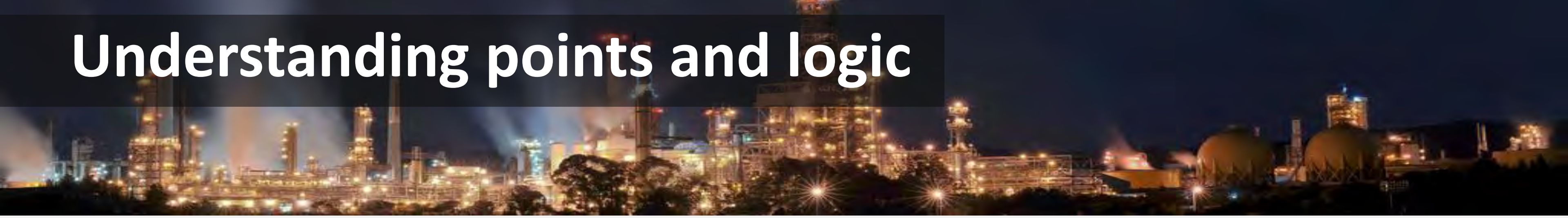
Refinement

Final product

Available controls



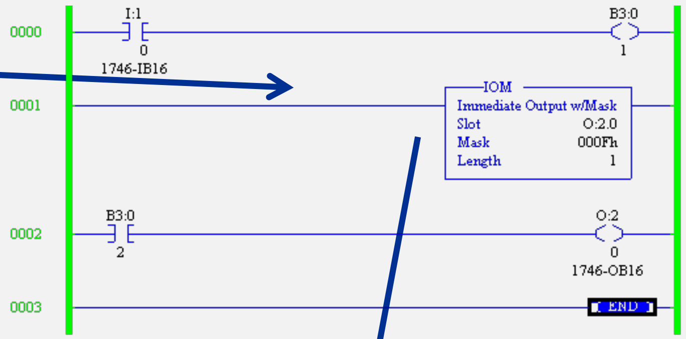
HAc flows into two sections. Not good :(

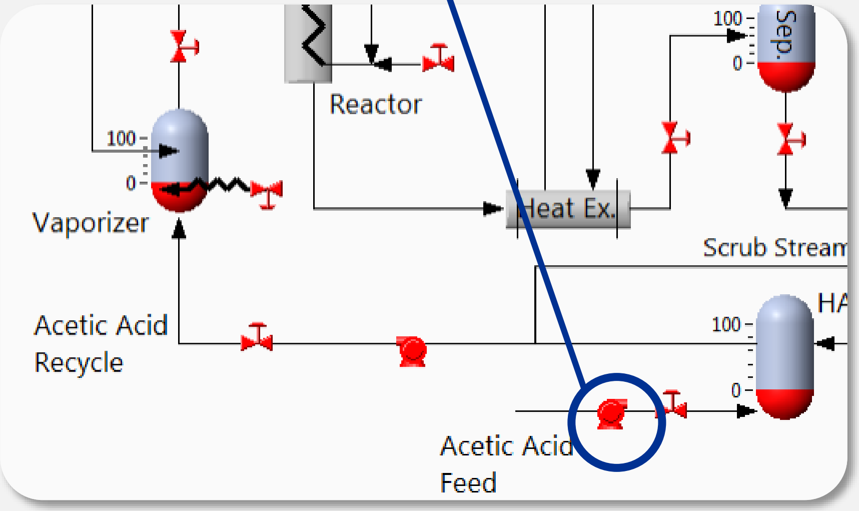


Understanding points and logic

Programmable Logic Controller

Ladder logic

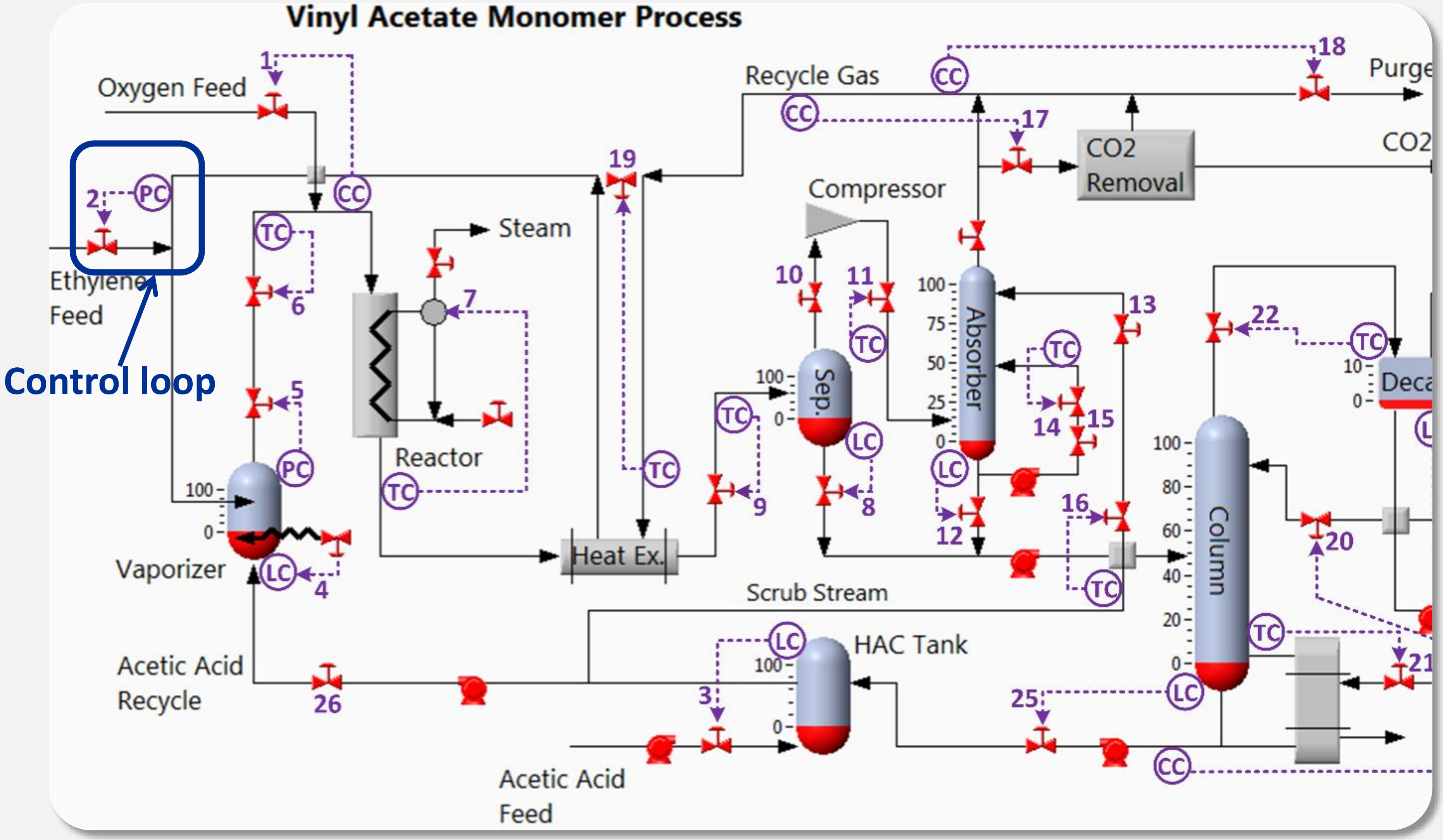




Piping and instrumentation diagram

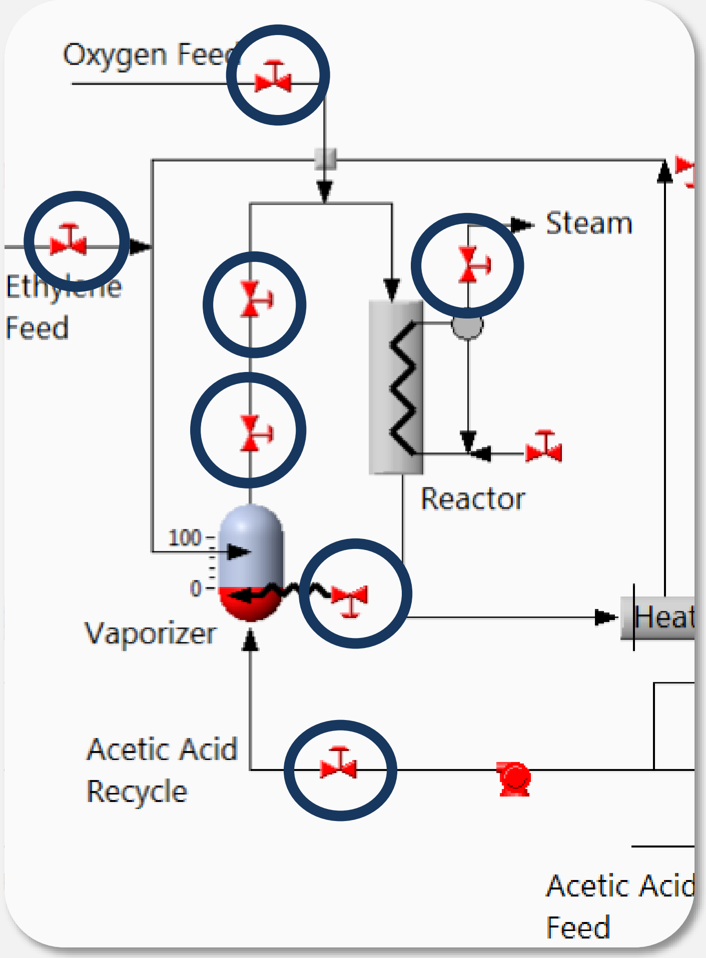
Pump on the plant

Available controls



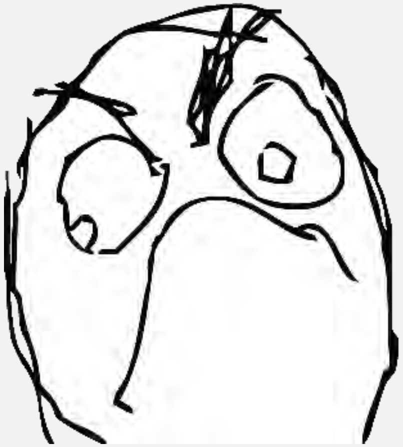
Control loop

Available controls



- ❑ **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???

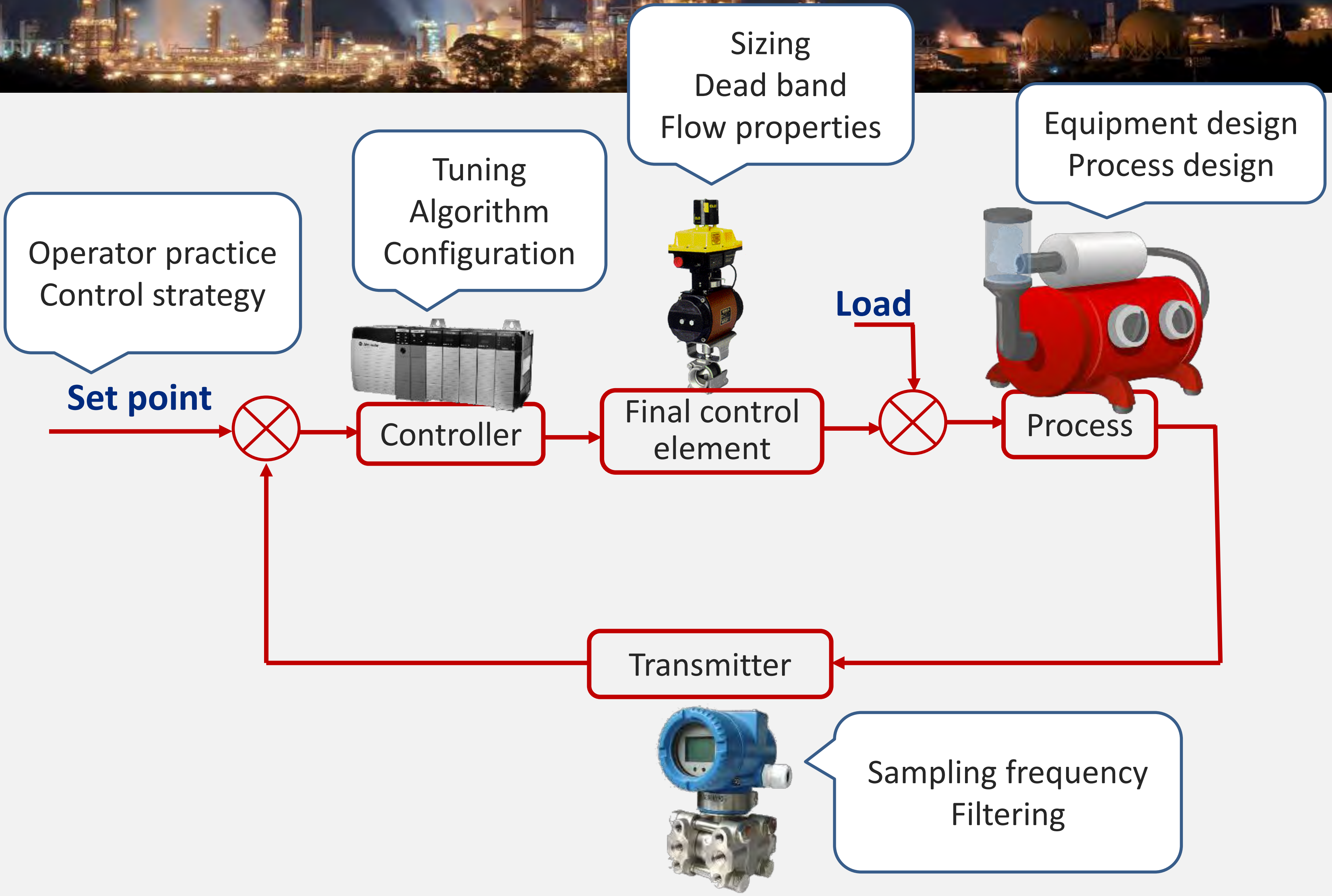


Control

Physics of process control

- Once hooked up together, physical components they become related to each other by the physics of the process
- If we adjust one 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 control challenges



Operator practice
Control strategy

Tuning
Algorithm
Configuration

Sizing
Dead band
Flow properties

Equipment design
Process design

Load

Set point

Controller

Final control element

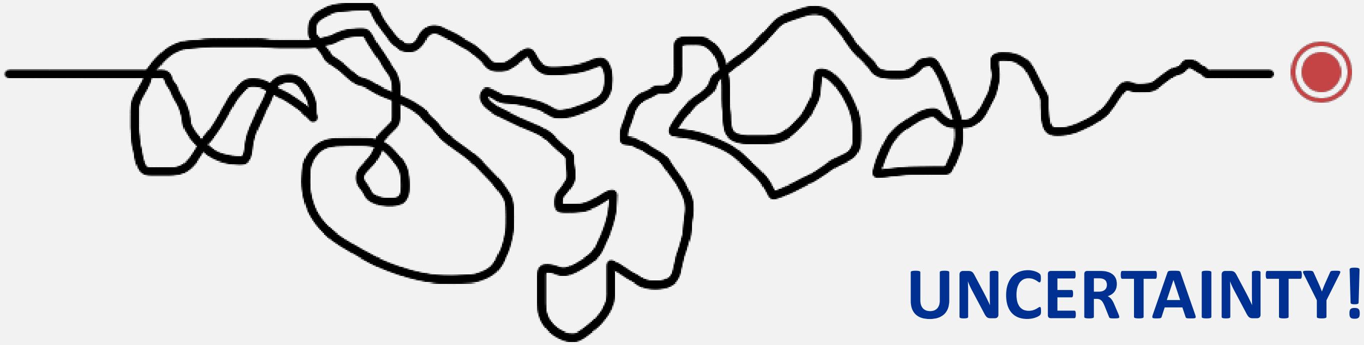
Process

Transmitter

Sampling frequency
Filtering

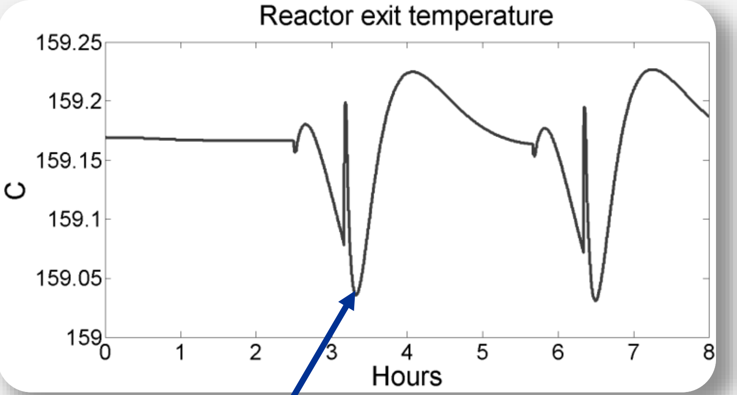
Process control challenges

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



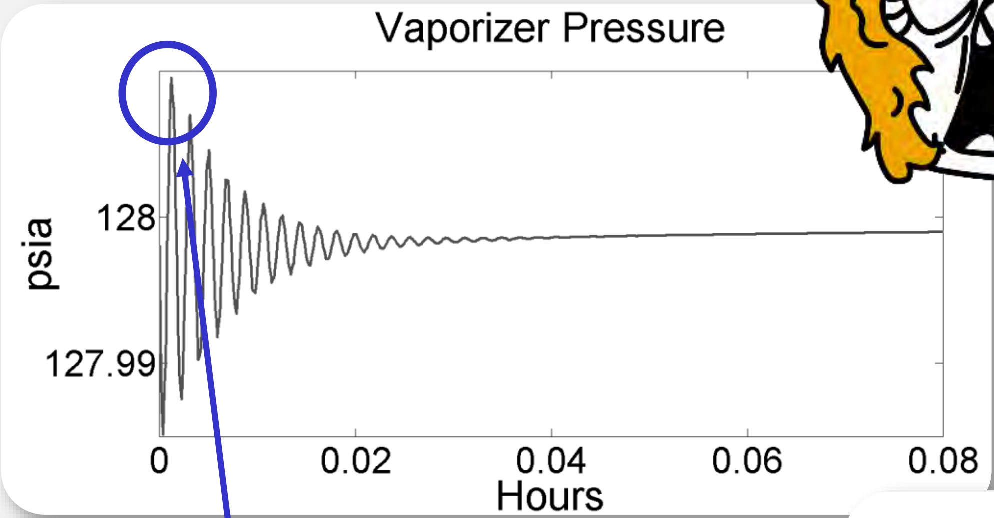
UNCERTAINTY!

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



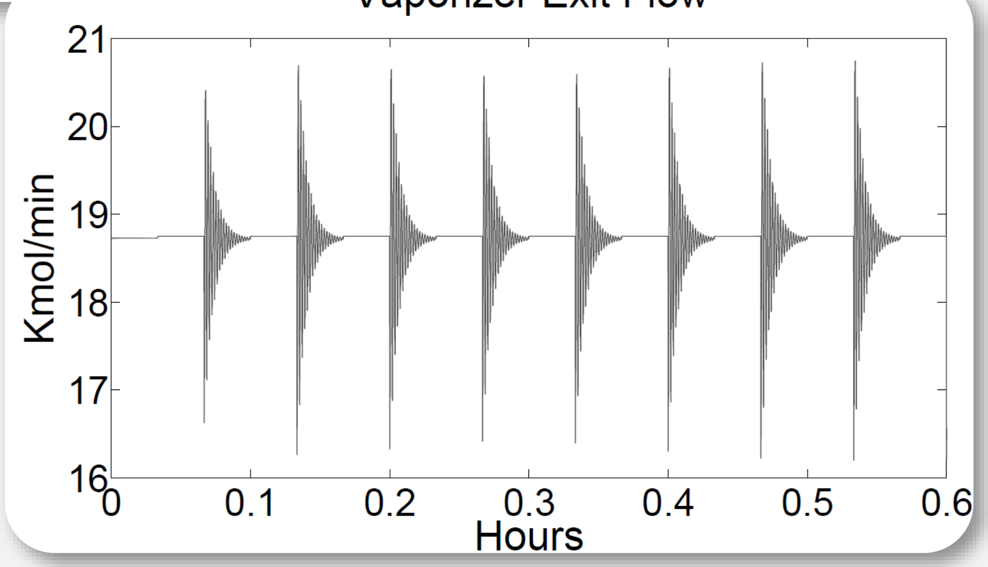
Triggers alarms

Control loop ringing

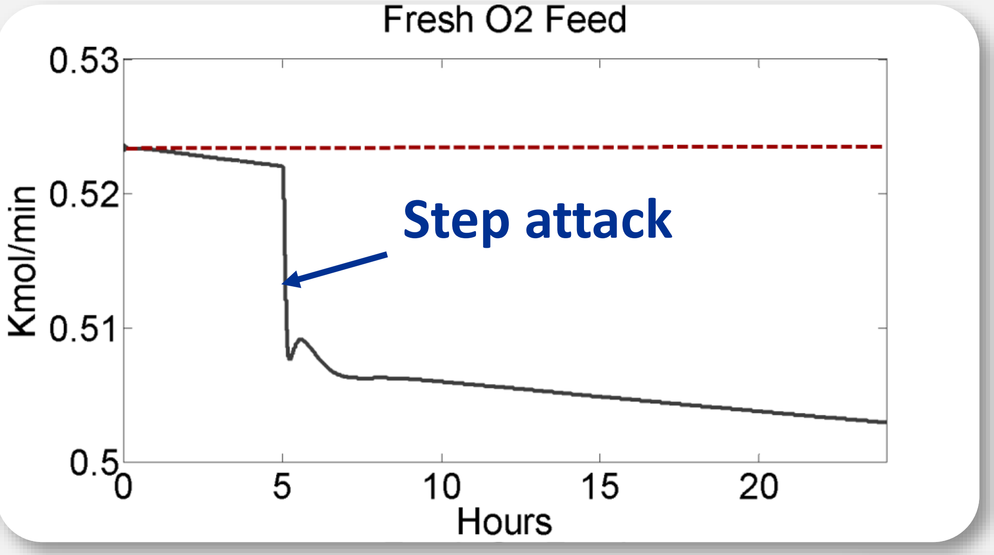


Caused by a negative real controller poles

Amount of chemicals entering the reactor

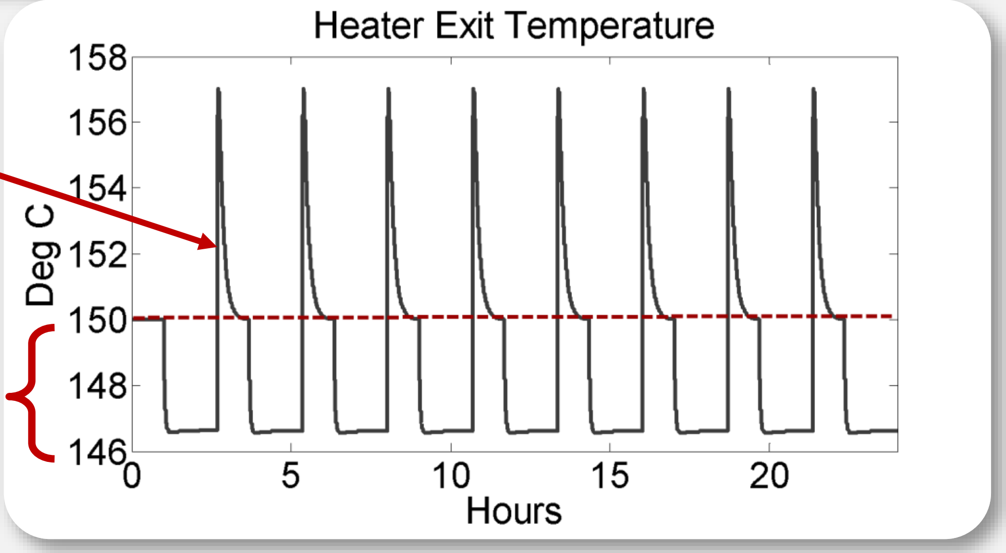


Types of attacks



Step attack

Periodic attack



Recovery time

Magnitude of manipulation

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}

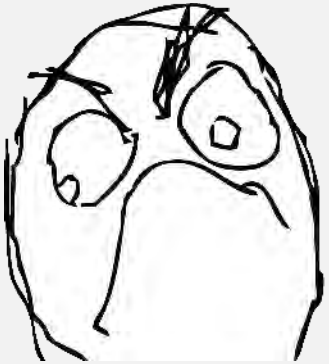
Reliably useful controls

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}

To persist we shall not bring about alarms

Outcome of the control stage



We should automate this process
(work in progress)

Damage

How to break things?

- Attacker needs one or more attacks 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
- Requires a metric/measure to compare between scenarios

OSHA®

CSB

U.S. CHEMICAL SAFETY AND HAZARD INVESTIGATION BOARD

The New York Times

Technician vs. engineer

Technician

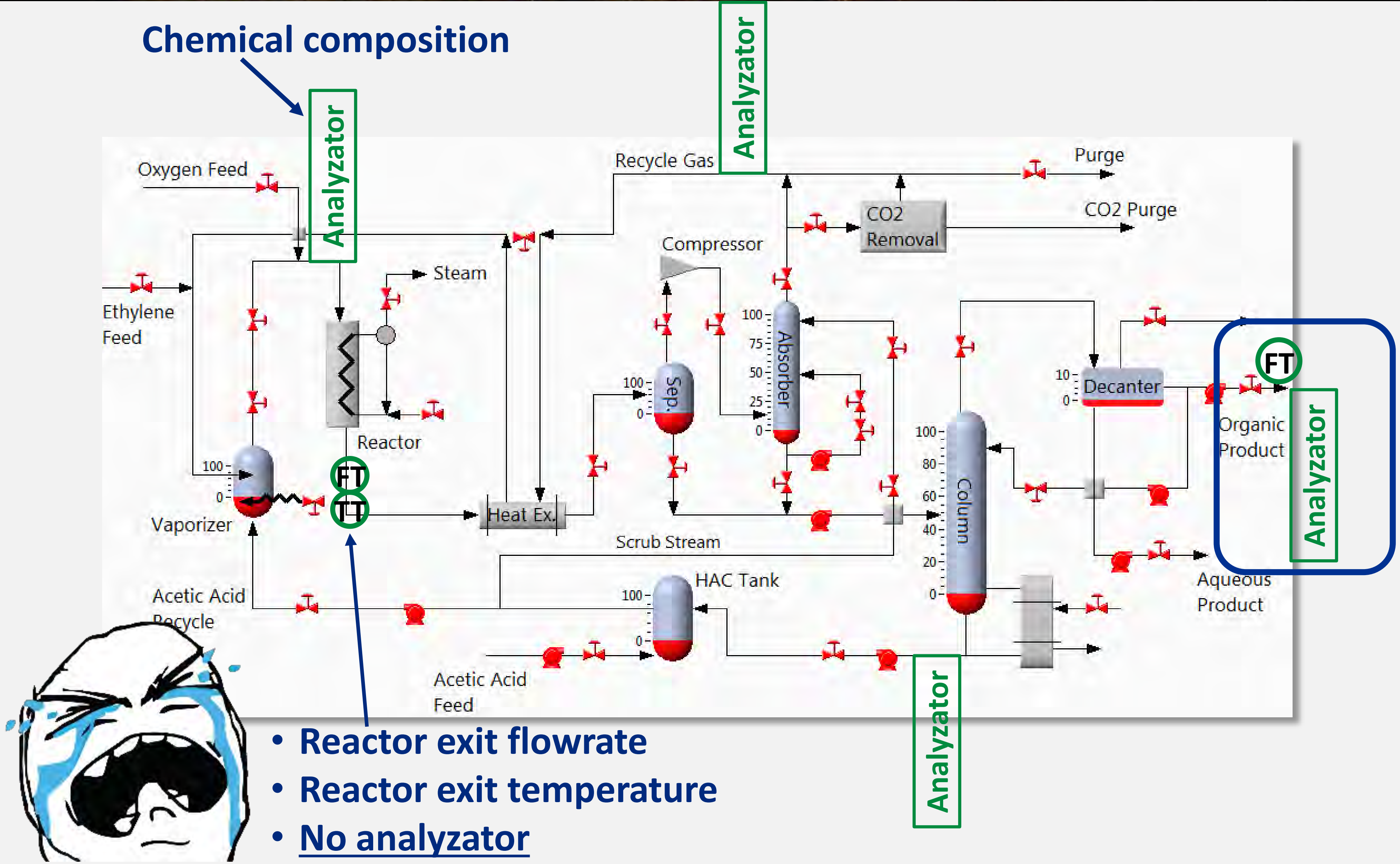
“It will eventually drain with the lowest holes loosing pressure last”

Engineer

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

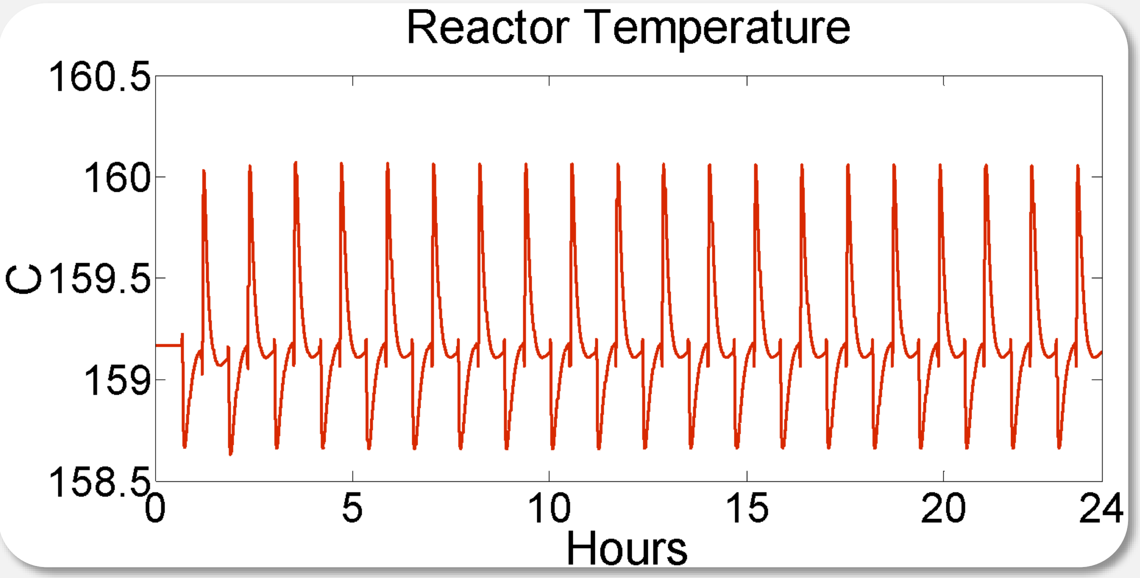
Process observation

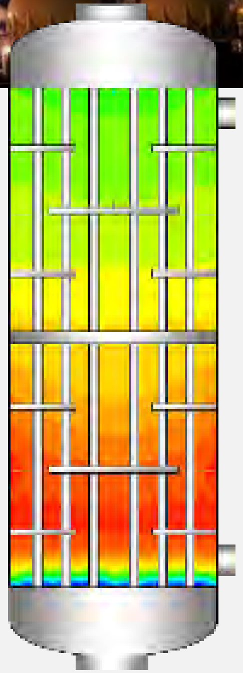
Chemical composition



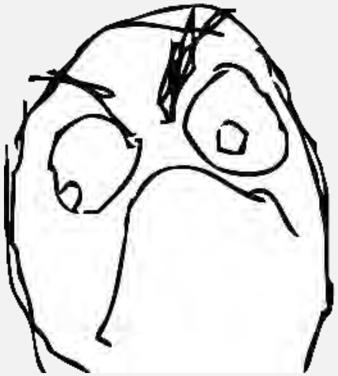
- Reactor exit flowrate
- Reactor exit temperature
- No analyzator

Technician answer





Reactor with cooling tubes

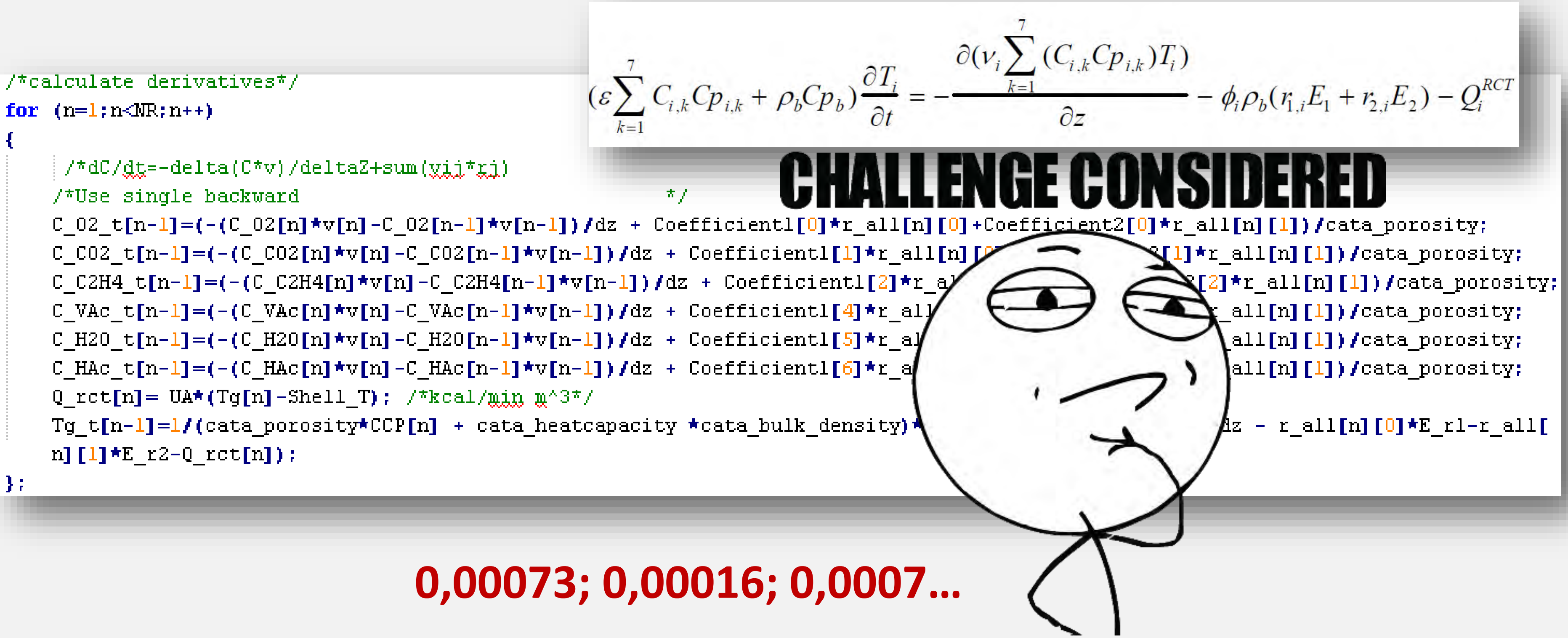


If you can't measure it, you can't manage it

Peter Drucker

Quest for engineering answer

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

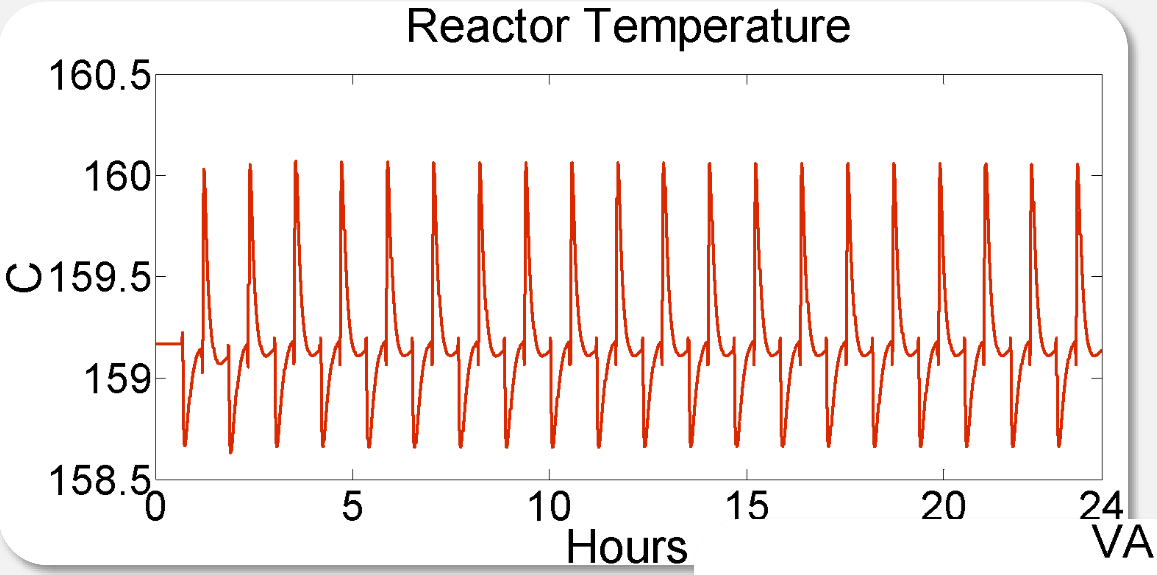


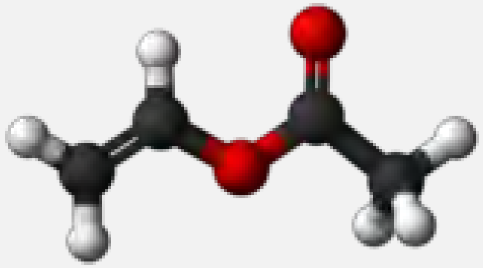
$$(\varepsilon\sum_{k=1}^{7} C_{i,k}Cp_{i,k} + \rho_b Cp_b)\frac{\partial T_i}{\partial t} = -\frac{\partial(v_i\sum_{k=1}^{7}(C_{i,k}Cp_{i,k})T_i)}{\partial z} - \phi_i\rho_b(r_{1,i}E_1 + r_{2,i}E_2) - Q_i^{RCT}$$

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

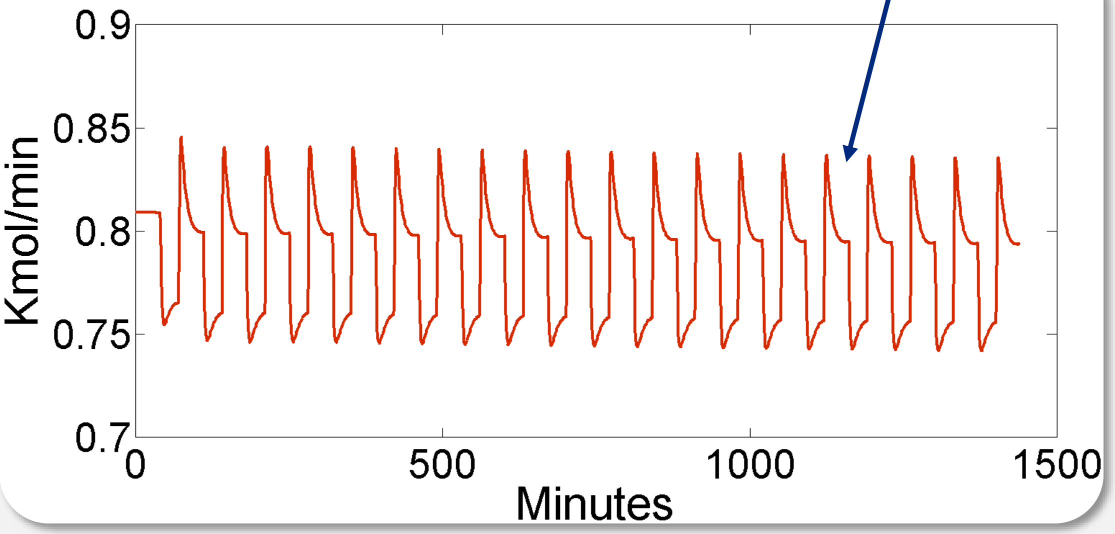
Engineering answer





Vinyl Acetate production

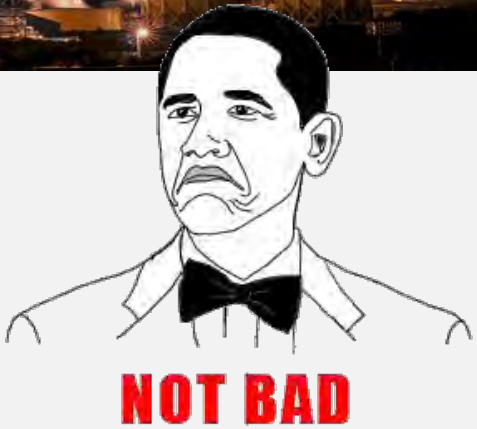
VAM Concentration

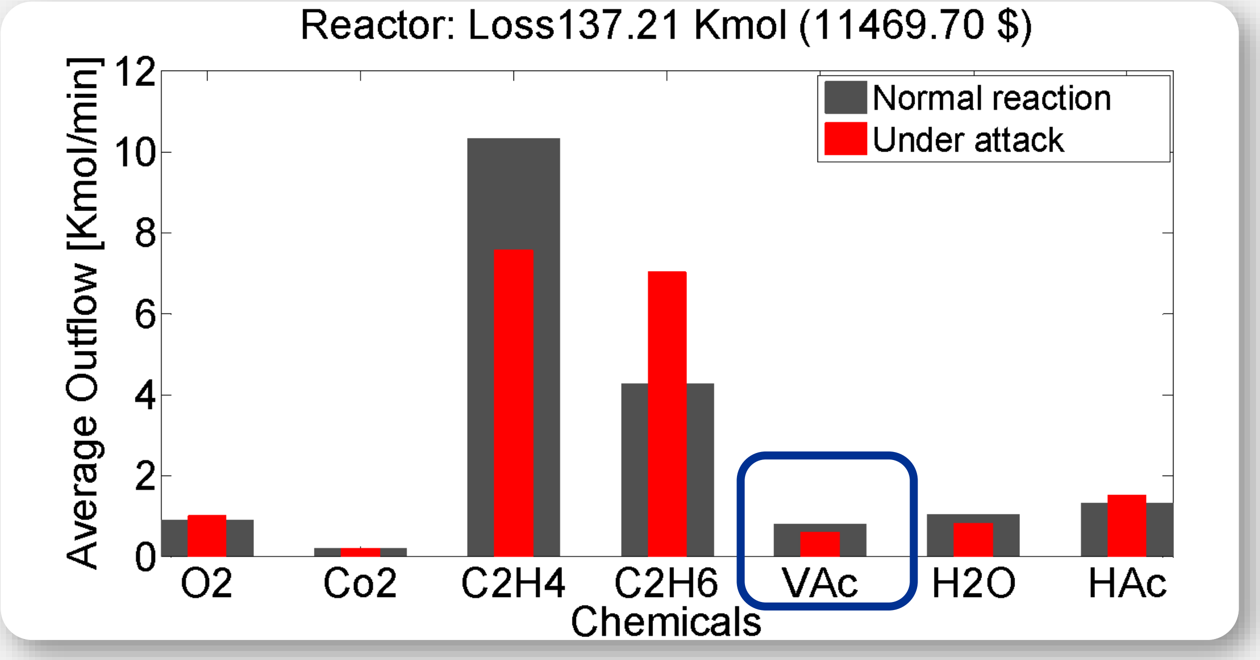


Product loss

Product per day: 96.000$

Product loss per day: 11.469,70$





Outcome of the damage stage

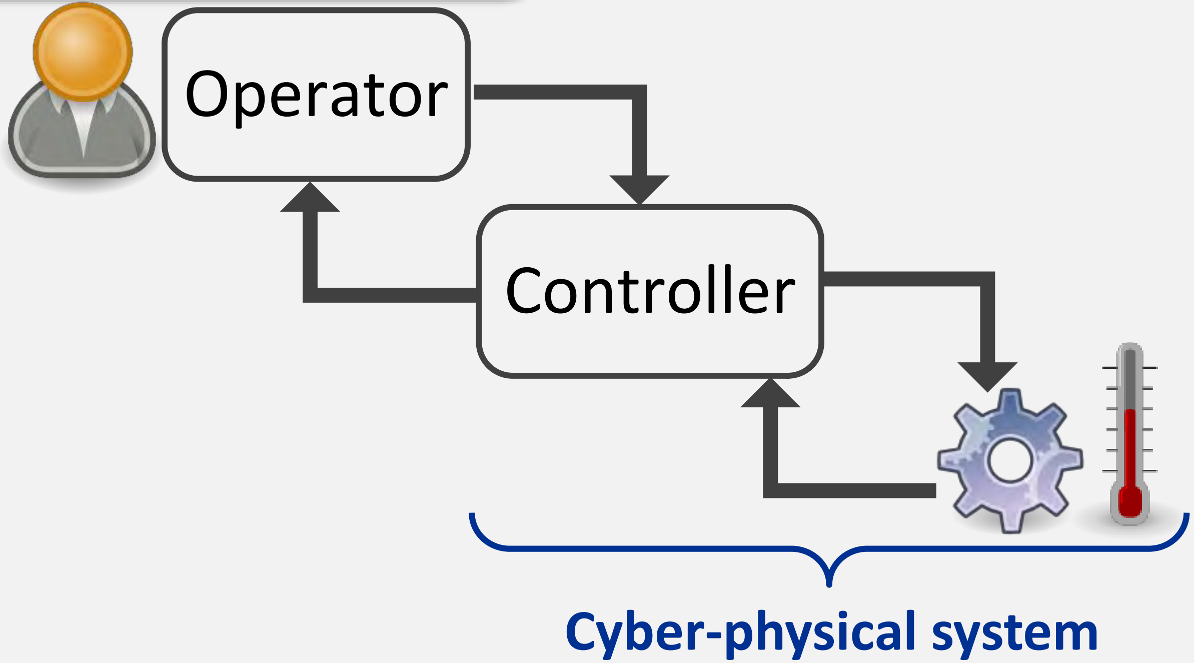
Product per day: 96.000$

Product loss, 24 hours	Steady-state attacks	Periodic attacks
High, ≥ 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
- ….

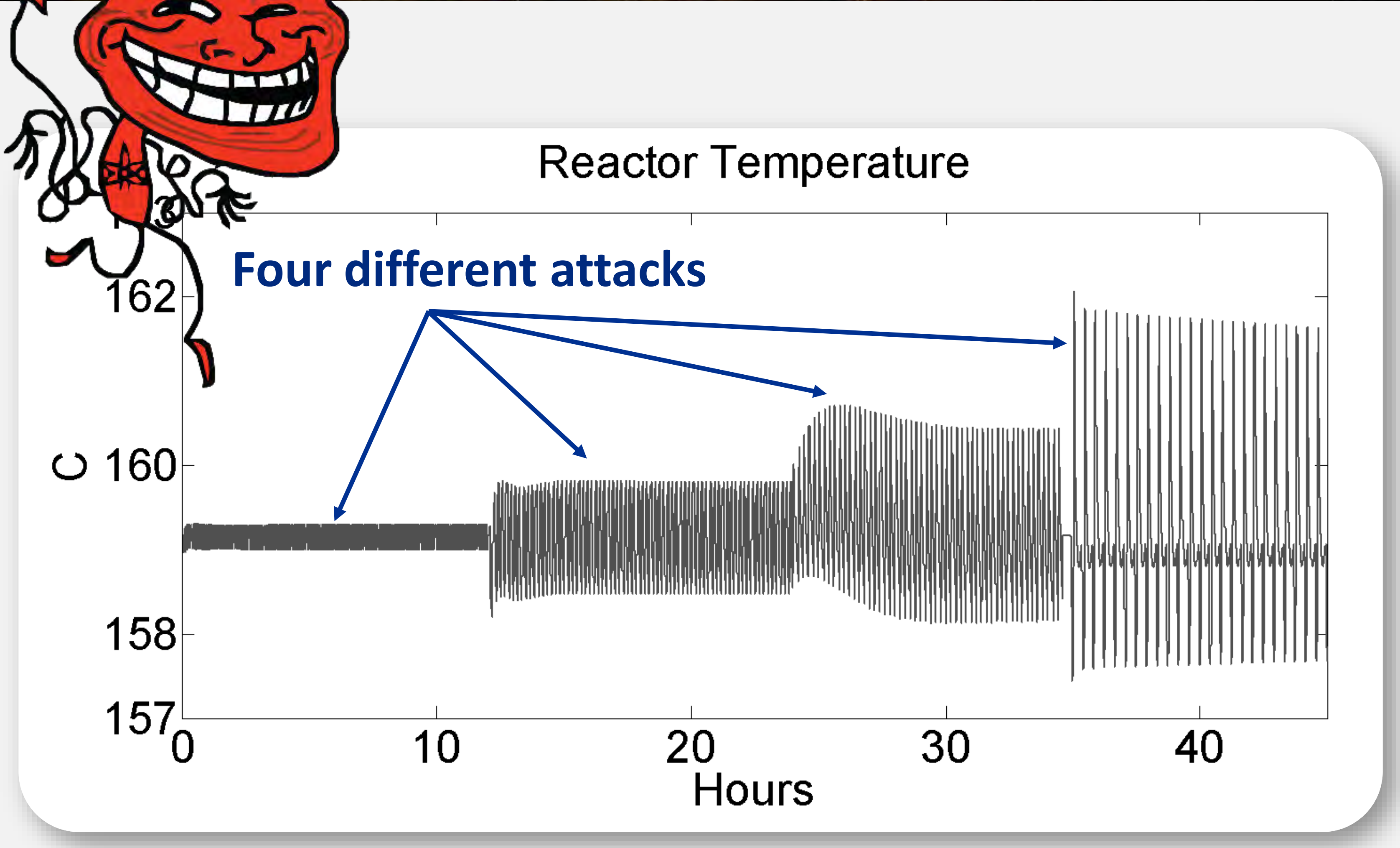
Creating forensics footprint

- 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

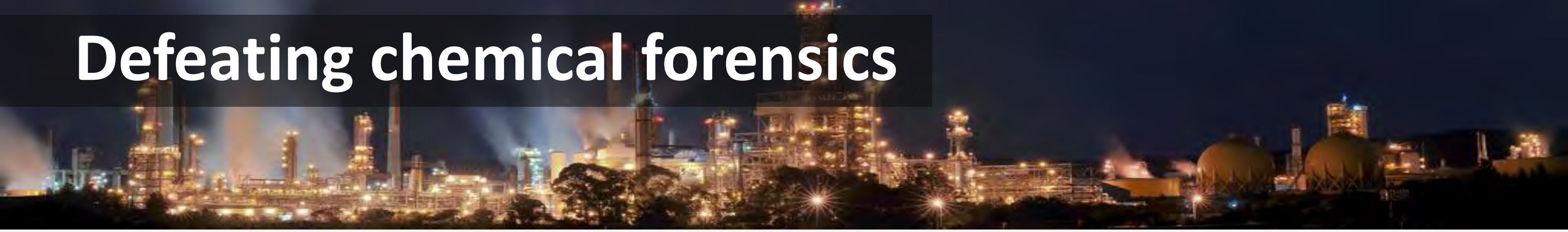
Creating forensics footprint

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

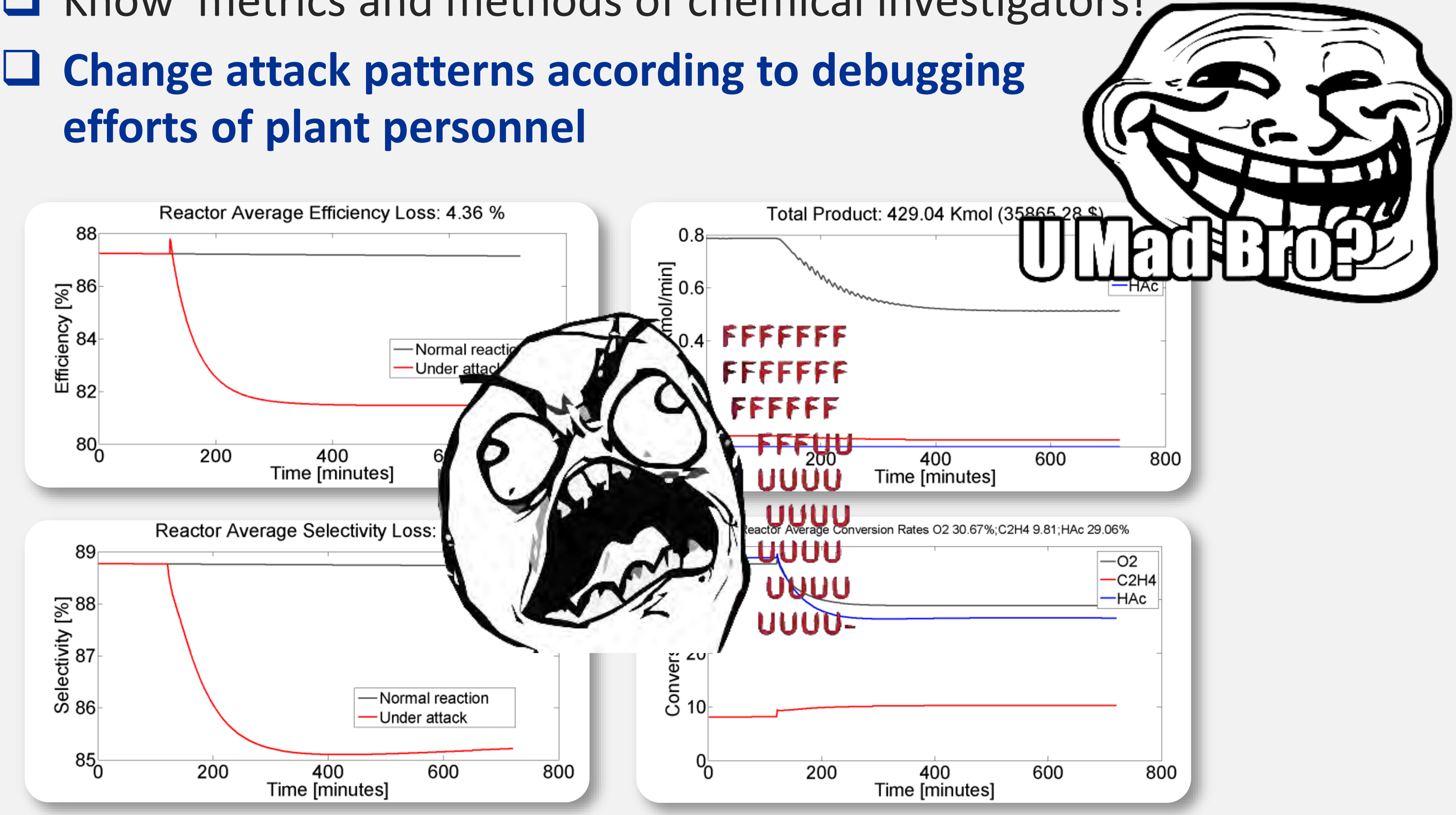


Four different attacks



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**



Afterword

Impressions

Please rate your hacking experience

Cost of attack vs. cost of damage

Medium effort

- ❑ SCADA access stage is (well) understood and facilitated by tools
  - ○ ICS-CERT and multiple public presentations
  - ○ SCADA access for sale

Medium to high effort

- ❑ Discovery stage has started long time ago and goes on
  - ○ Hackers know more about the process than process owners
  - ○ First field equipment reconnaissance malware is caught in wild

Cost of attack vs. cost of damage

High effort

- ❑ Control stage
  - ○ Requires established approaches for mapping and storing dynamic behavior of the process and interdependencies
  - ○ **Our work in progress**
- ❑ Damage stage
  - ○ Requires involvement of subject matter experts
  - ○ Several public damage attack instances
  - ○ **Our work in progress**
- ❑ Clean-up stage is understood by attackers
  - ○ Several public presentations
  - ○ The defenders are too busy setting up firewalls

Cost of attack vs. cost of damage

□ 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
- Inclusion of several attacks scenarios

□ Each process is unique, but…

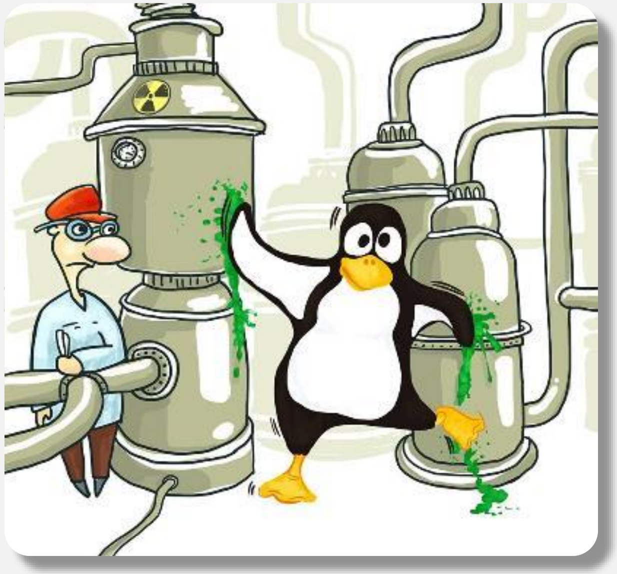
- There is a number of tasks needed to done for each process
- There is a number of issues similar to different processes
- There are instances of attacks applicable to wide range of scenarios
- **SCADA payloads for Metasploit is just a matter of time**

□ Research agenda

- Developing of light-weight real time algorithms for various tasks
- Working out breakage scenarios

Dream BIG

If you plan to improve your financial posture, is a good time (and at least next 5 year as well)



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