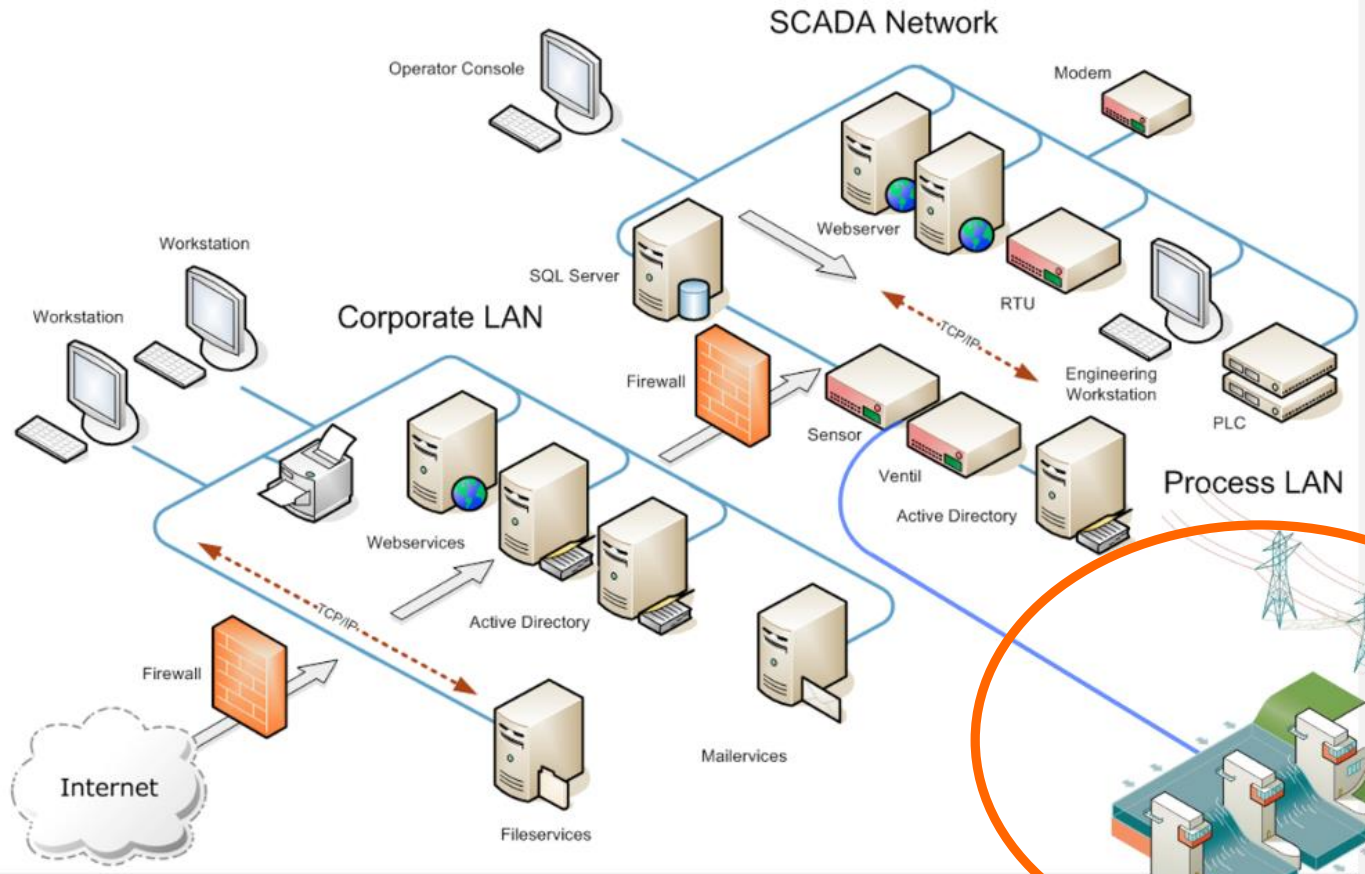
Damn Vulnerable Chemical Process

Marina Krotofil & Co

31C3, 27.12.2014

Industrial Control Systems



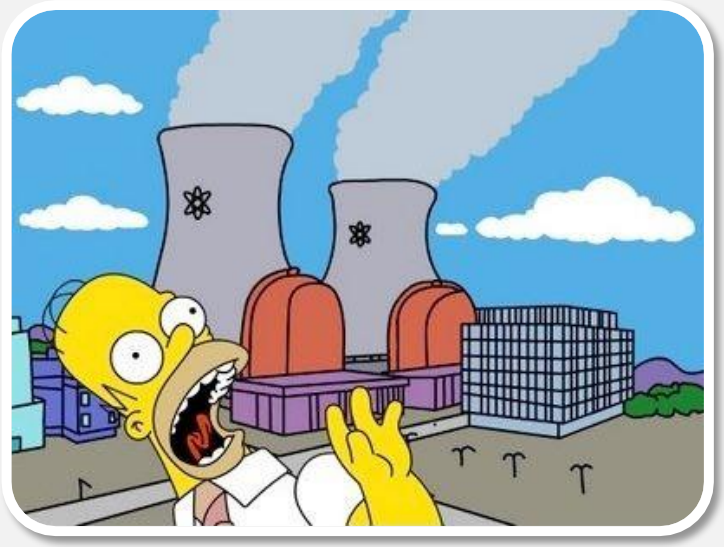
Physical application

Curtesy: Compass Security Germany GmbH

Cyber-Physical Systems

- **Cyber-physical systems are IT systems "embedded" in an application in the physical world**

- Attack goals:
  - Get the physical system in a state desired by the attacker
  - Make the physical system perform actions desired by the attacker



Wish list of ICS security practitioner

… more public disclosures about “catastrophic” ICS accidents happening in real world…

Wish came true

Iranian Cyber-Campaign
Researche Say

By Robert Lemo

ndwork for Sabotage,

nuclear plant

steel factory

Cyberattack
causes 'mas

By Loek Essers | FOLLOW
IDG News Service | December 1

ned New

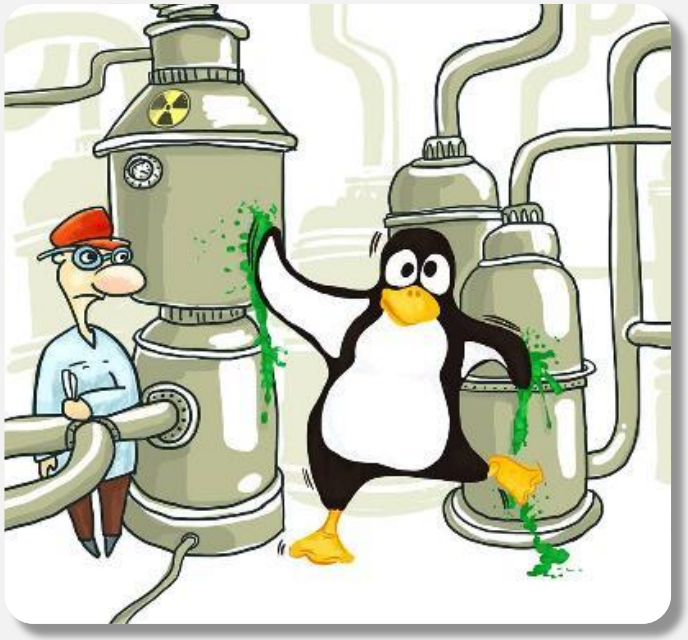
– Jordan Robertson – The eline outfitted with sensors and cameras to monitor every step of its 1,0 miles m the Caspian Sea to the

Laziness is a stimulus to progress

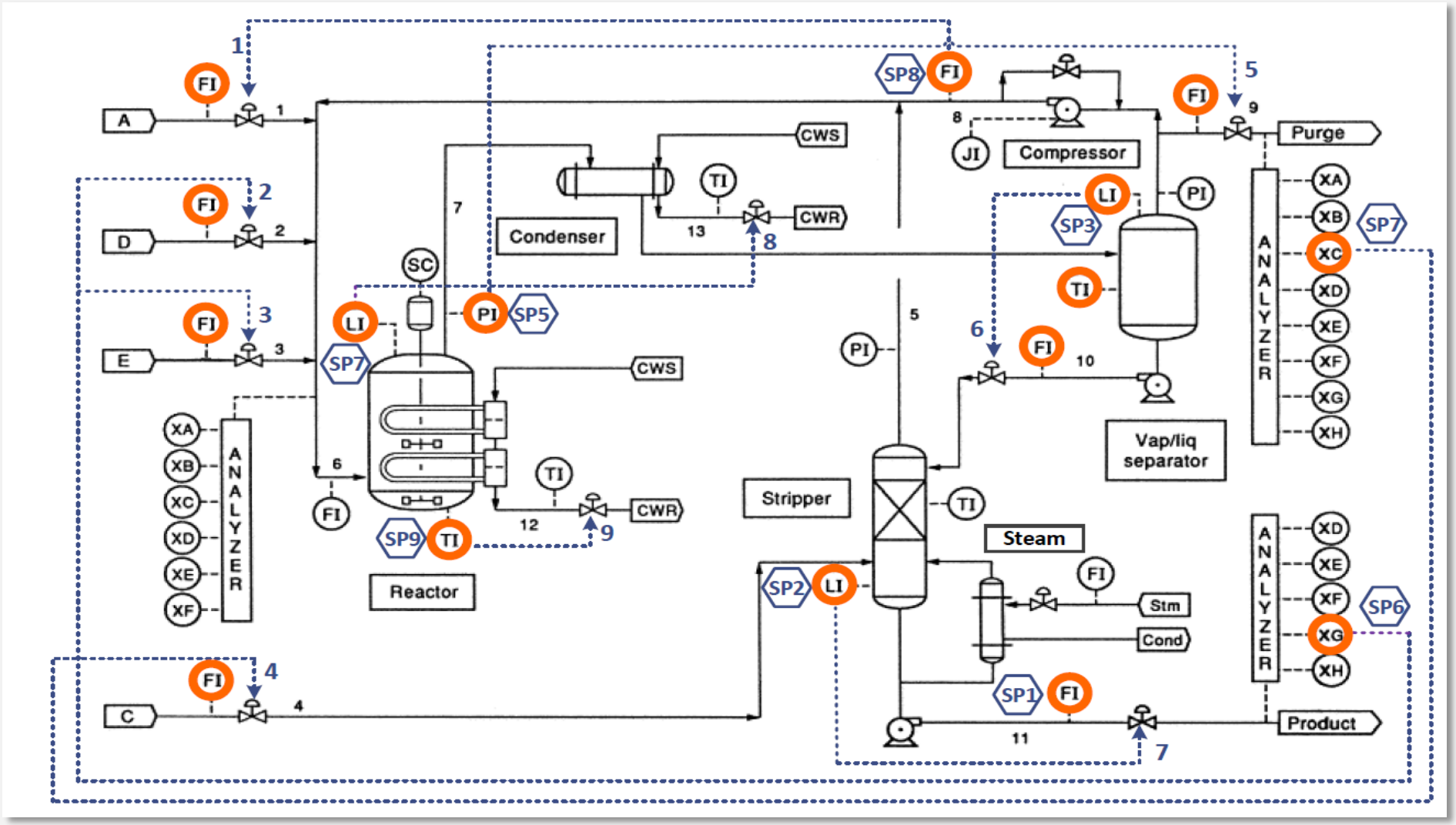
Chemical plants

Source: simentari.com

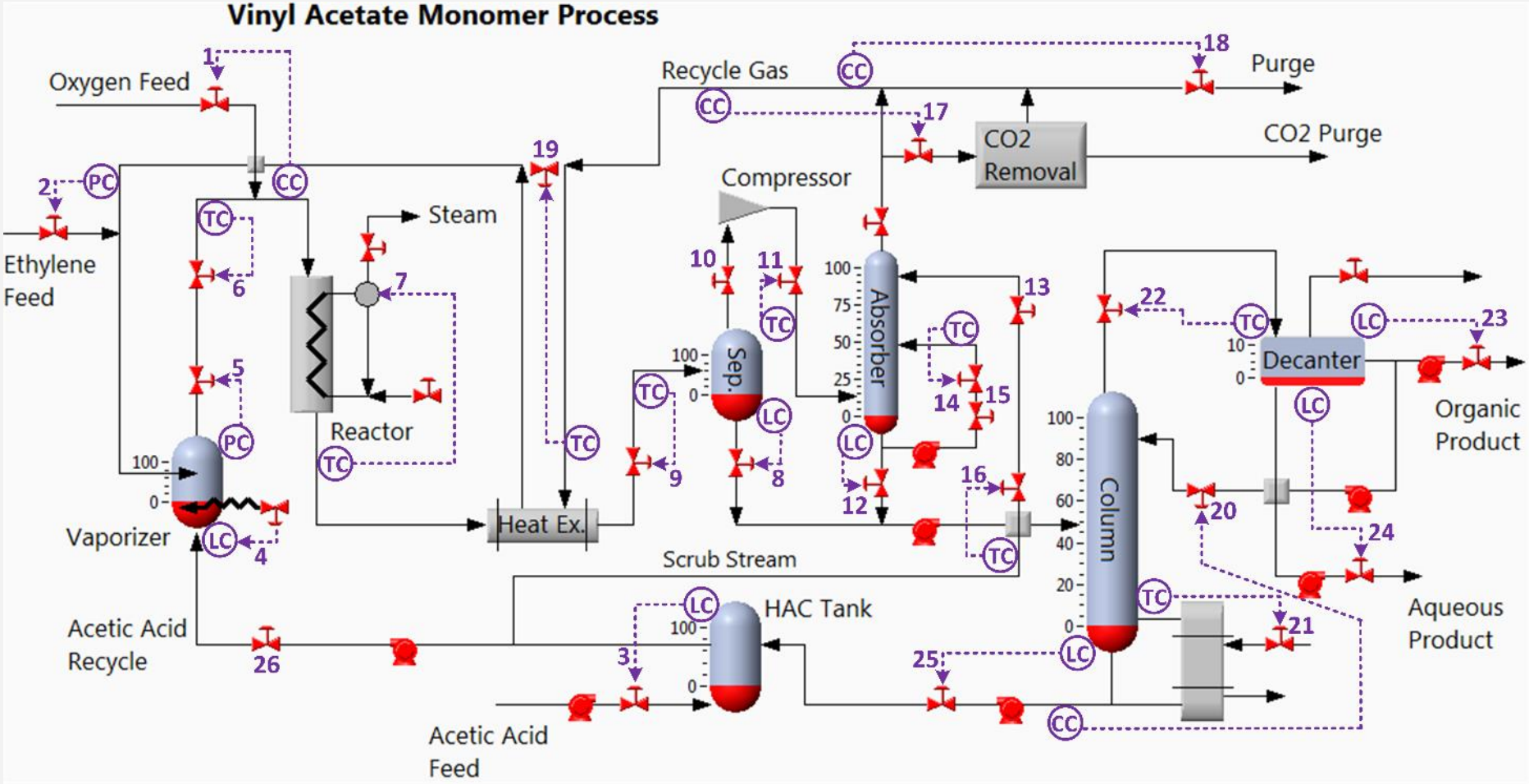
- **Damn Vulnerable Chemical Process**



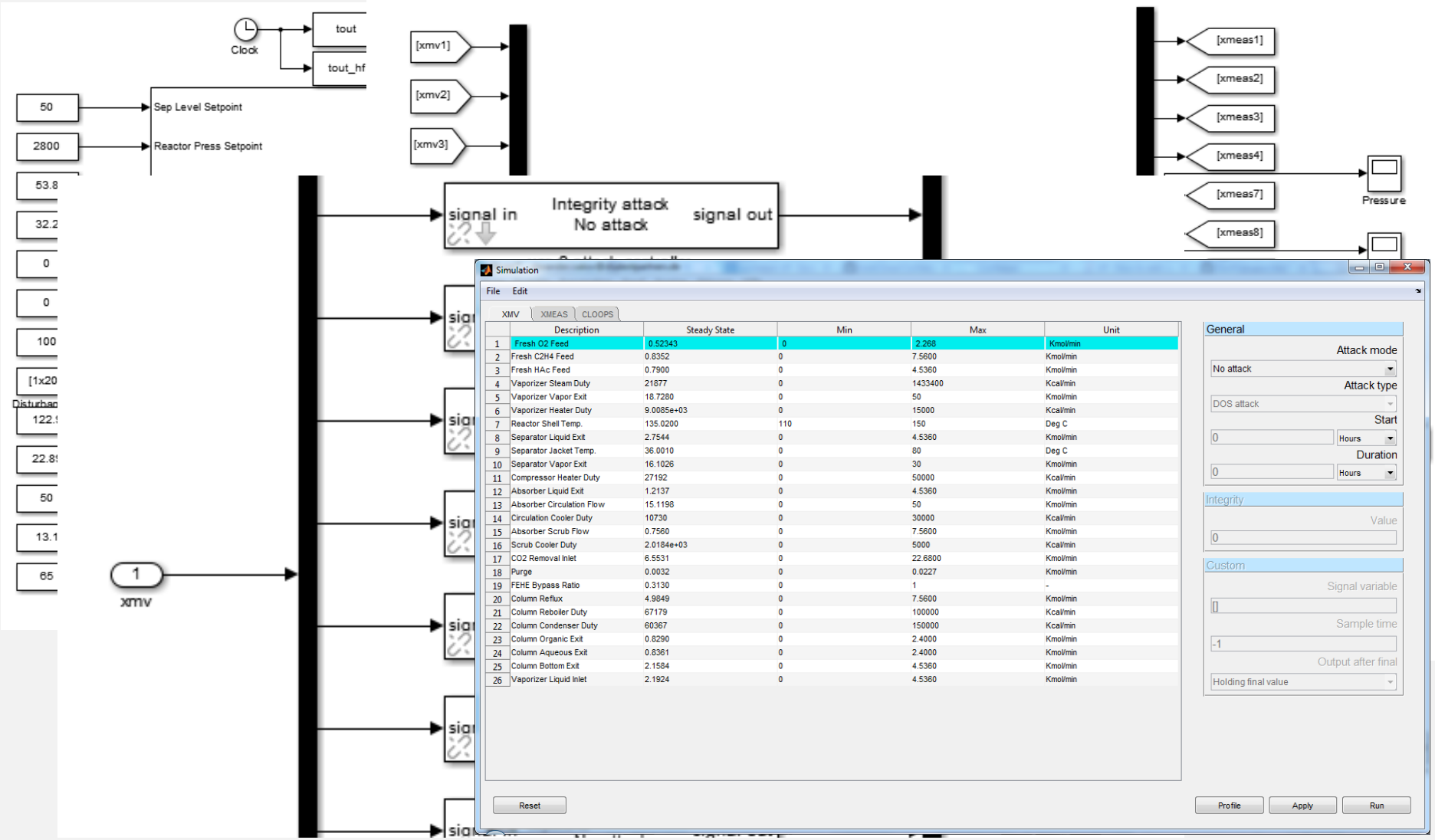
Tennessee Eastman (TE) chemical process



Vinyl Acetate Monomer (VAM) process

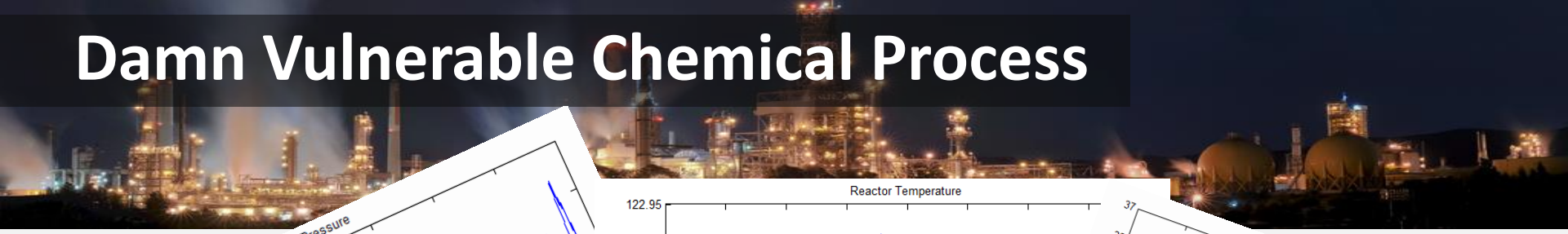


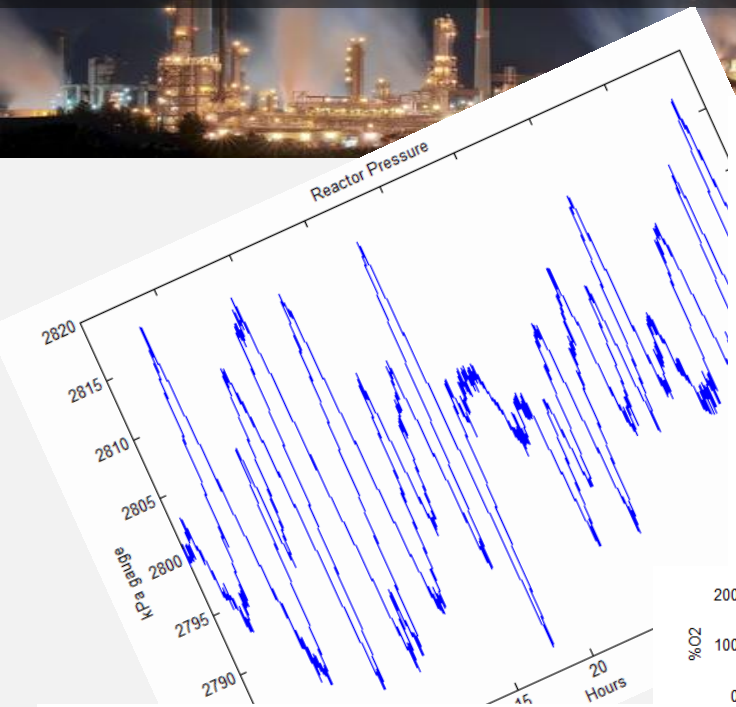
Damn Vulnerable Chemical Process

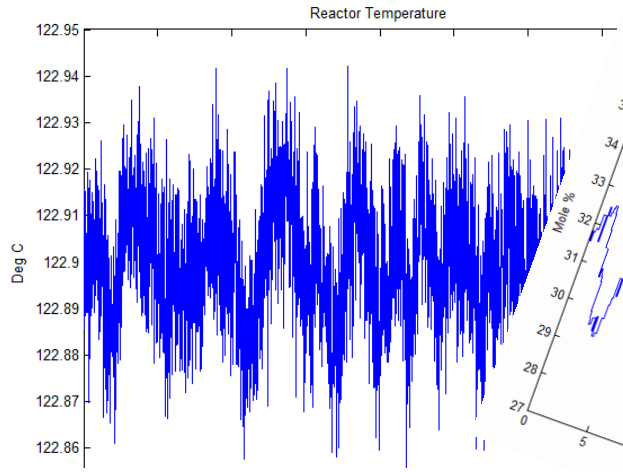


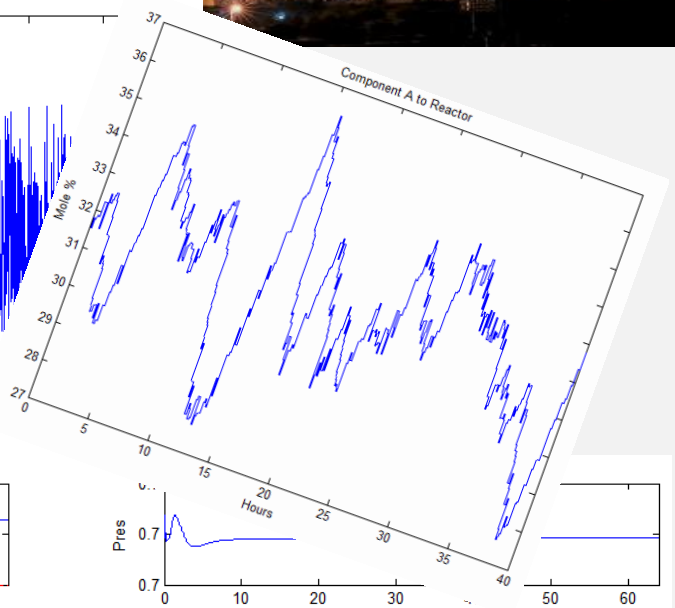
	Description	Steady State	Min	Max	Unit
1	Fresh O2 Feed	0.52343	0	2.268	Kmol/min
2	Fresh C2H4 Feed	0.8352	0	7.5600	Kmol/min
3	Fresh HAc Feed	0.7900	0	4.5360	Kmol/min
4	Vaporizer Steam Duty	21877	0	1433400	Kcal/min
5	Vaporizer Vapor Exit	18.7280	0	50	Kmol/min
6	Vaporizer Heater Duty	9.0085e+03	0	15000	Kcal/min
7	Reactor Shell Temp.	135.0200	110	150	Deg C
8	Separator Liquid Exit	2.7544	0	4.5360	Kmol/min
9	Separator Jacket Temp.	36.0010	0	80	Deg C
10	Separator Vapor Exit	16.1026	0	30	Kmol/min
11	Compressor Heater Duty	27192	0	50000	Kcal/min
12	Absorber Liquid Exit	1.2137	0	4.5360	Kmol/min
13	Absorber Circulation Flow	15.1198	0	50	Kmol/min
14	Circulation Cooler Duty	10730	0	30000	Kcal/min
15	Absorber Scrub Flow	0.7560	0	7.5600	Kmol/min
16	Scrub Cooler Duty	2.0184e+03	0	5000	Kcal/min
17	CO2 Removal Inlet	6.5531	0	22.6800	Kmol/min
18	Purge	0.0032	0	0.0227	Kmol/min
19	FEHE Bypass Ratio	0.3130	0	1	-
20	Column Reflux	4.9849	0	7.5600	Kmol/min
21	Column Reboiler Duty	67179	0	100000	Kcal/min
22	Column Condenser Duty	60367	0	150000	Kcal/min
23	Column Organic Exit	0.8290	0	2.4000	Kmol/min
24	Column Aqueous Exit	0.8361	0	2.4000	Kmol/min
25	Column Bottom Exit	2.1584	0	4.5360	Kmol/min
26	Vaporizer Liquid Inlet	2.1924	0	4.5360	Kmol/min

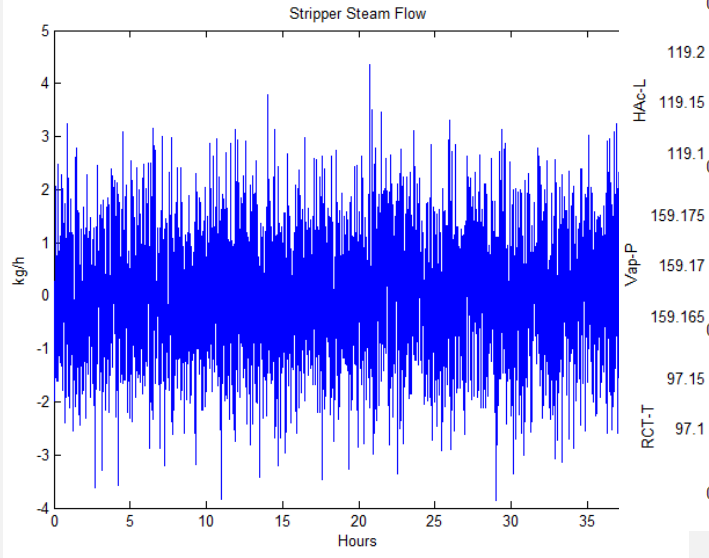
Damn Vulnerable Chemical Process

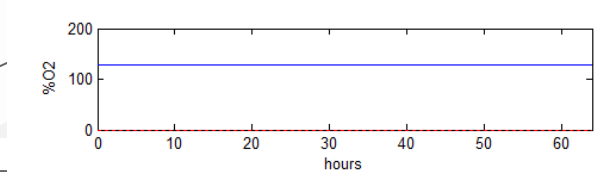


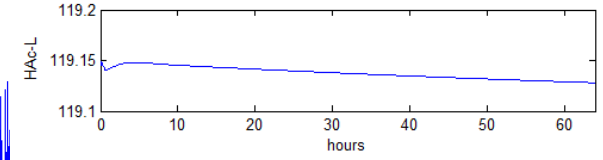


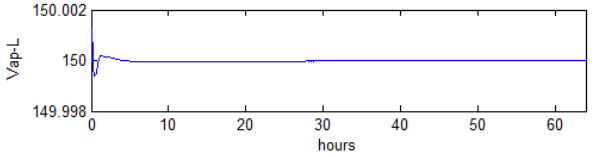


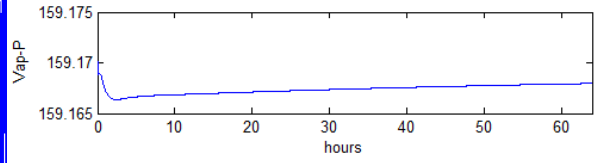


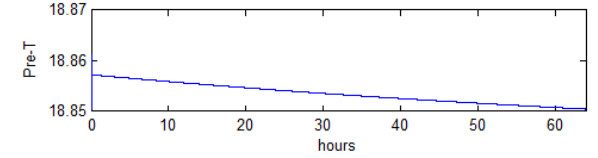


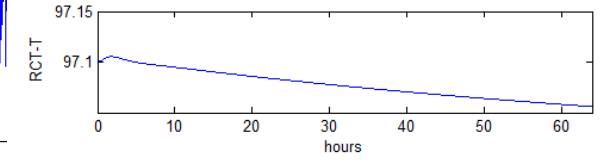


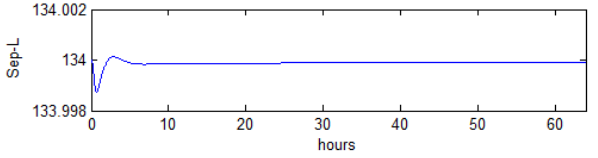












Damn Vulnerable Chemical Process

- Process in C-code
- Execution in Matlab/Simulink, still licensed…
  - Universities - free for students
  - Research institutions, industry
  - Other appropriate sources
- **Where to find**
  - Currently on GitHub
  - (Hopefully) Readme will be handy

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

- The team and cheerleaders

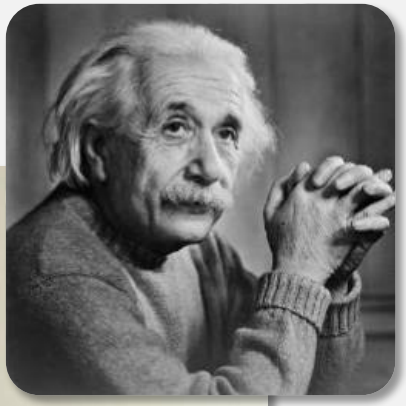
The cheerleaders

Éireann Leverett

Mona Lange

The professors

Prof. Dieter Gollmann



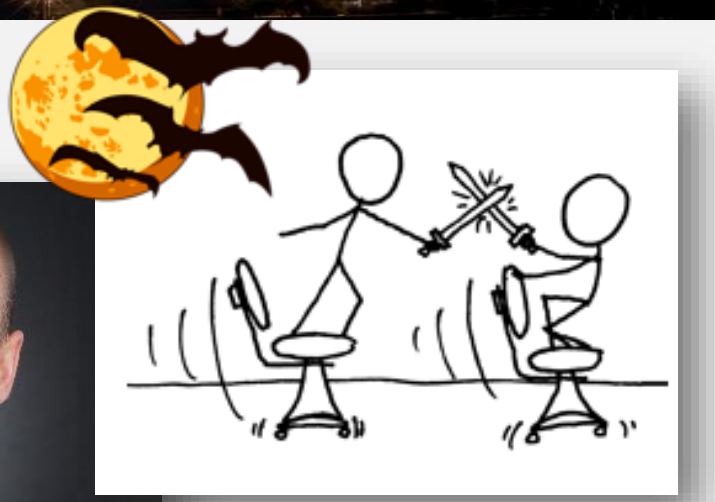
Prof. Alvaro Cardenas

The graphic designer

Ola Balakireva

The programmer

Alexander Isakov



The chemical engineer

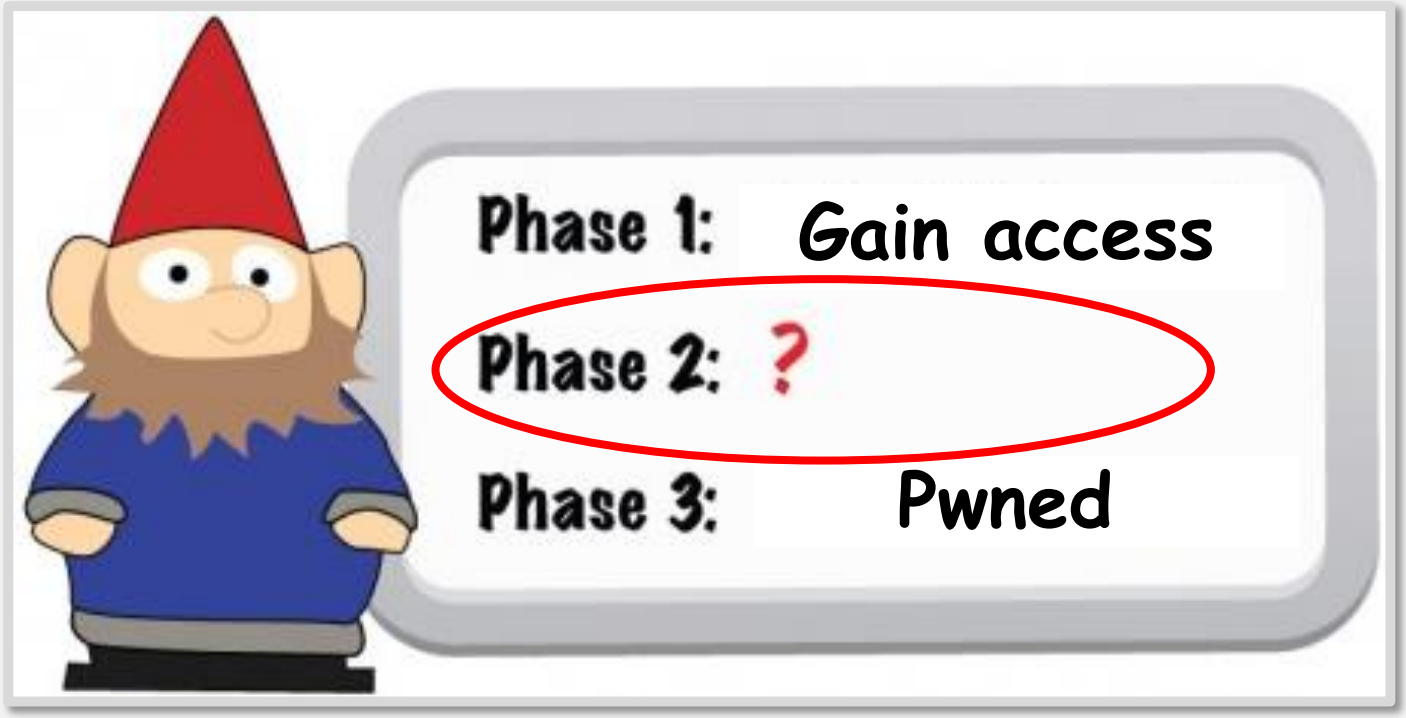
Pavel Gurikov

The GURU

Jason Larsen

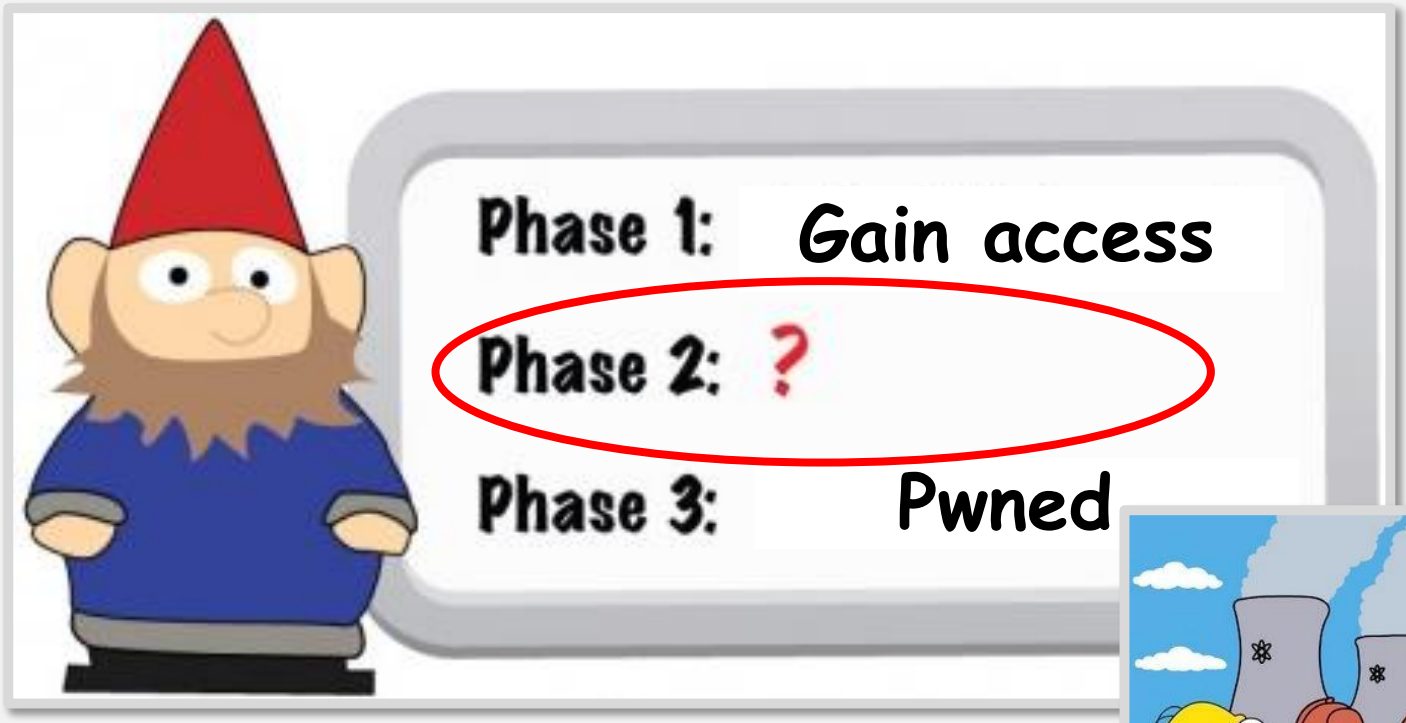
SCADA hacking

Typical understanding of SCADA hacking



Typical understanding of SCADA hacking

Typical understanding of SCADA hacking



Debunking SCADA hacking myths

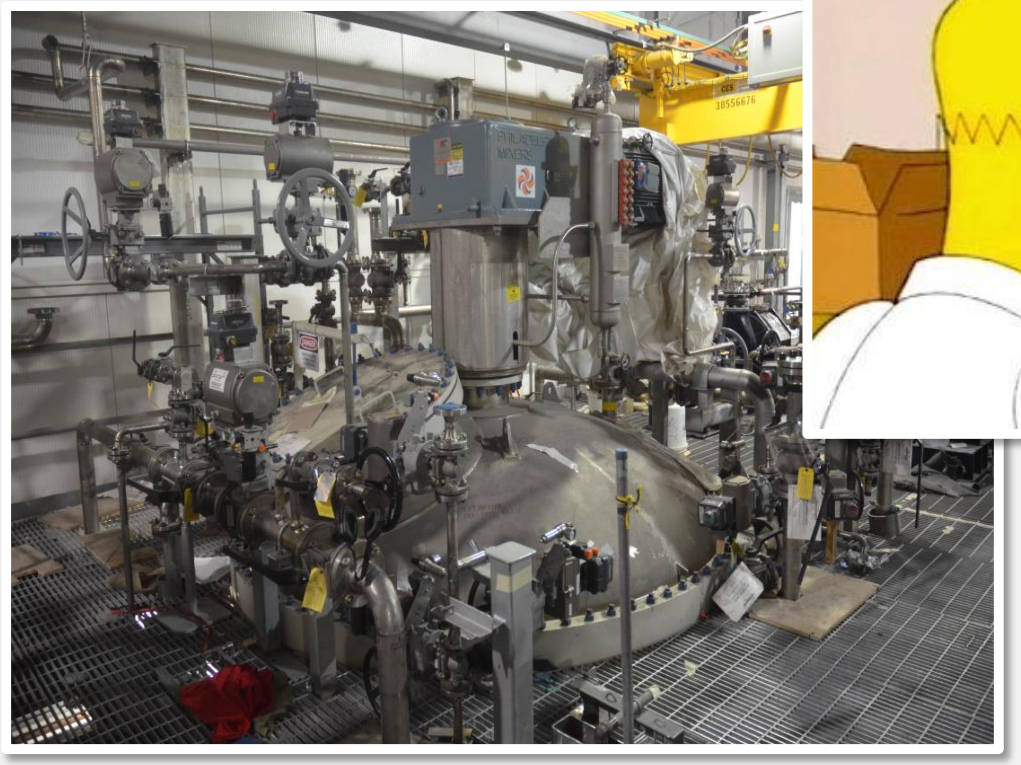
Obtaining access != Obtaining control

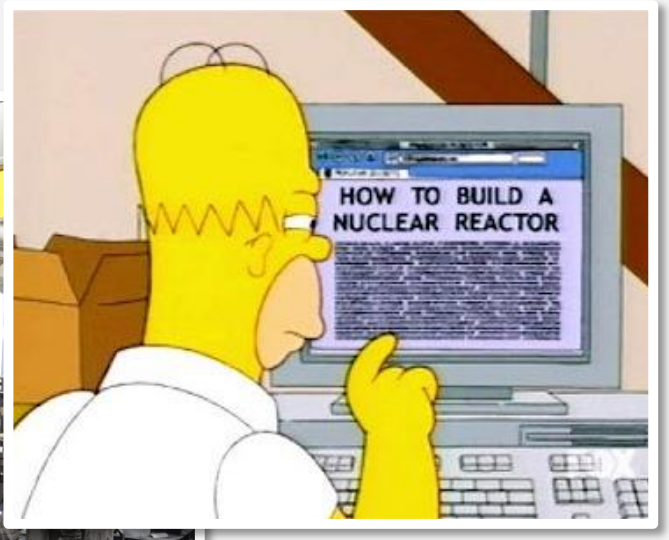
0100110110111101

Digital
Perl Harbor

Debunking SCADA hacking myths

Breaking into system != breaking the system





http://commons.wikimedia.org

Stripper is….

Stripping column

SCADA hacker

Is not who…..

- Has hacked into “something”
- Did “something”
- Achieved “something”

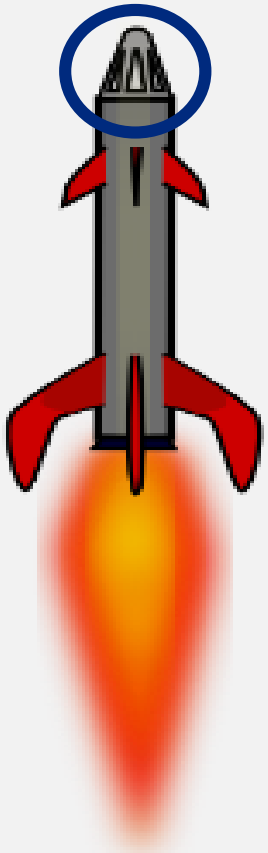
She…

- Has a defined attack objective
- Is limited by real world constraints
  - Management
  - Time, money
  - Experience…..

Attack objective

Your evil motivation

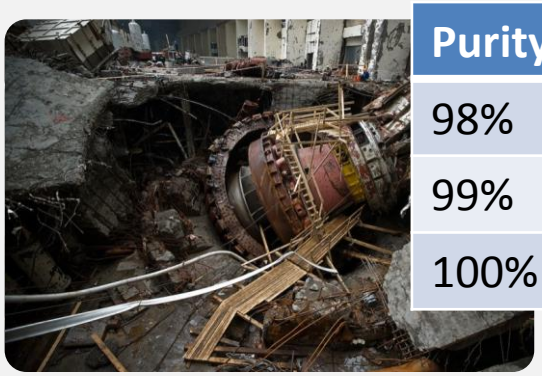
Your cyber-physical payload



Your evil motivation

Equipment damage	Production damage	Compliance violation
❑ Equipment overstress ❑ Violation of safety limits	❑ Product quality and product rate ❑ Operating costs ❑ Maintenance efforts	❑ Safety ❑ Pollution ❑ Contractual agreements

Paracetamol

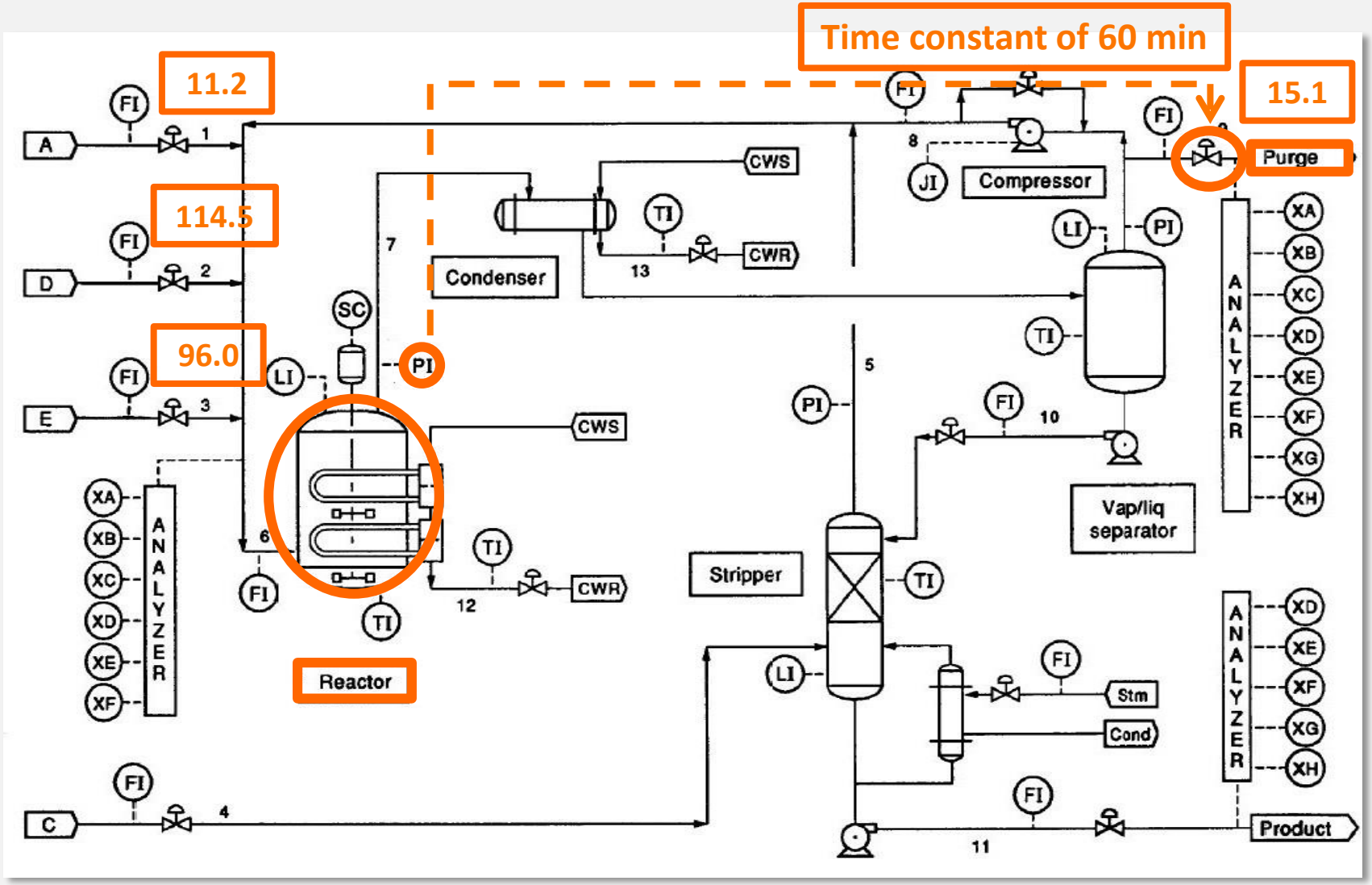


Purity	Price, EUR/kg
98%	78
99%	392
100%	640.000

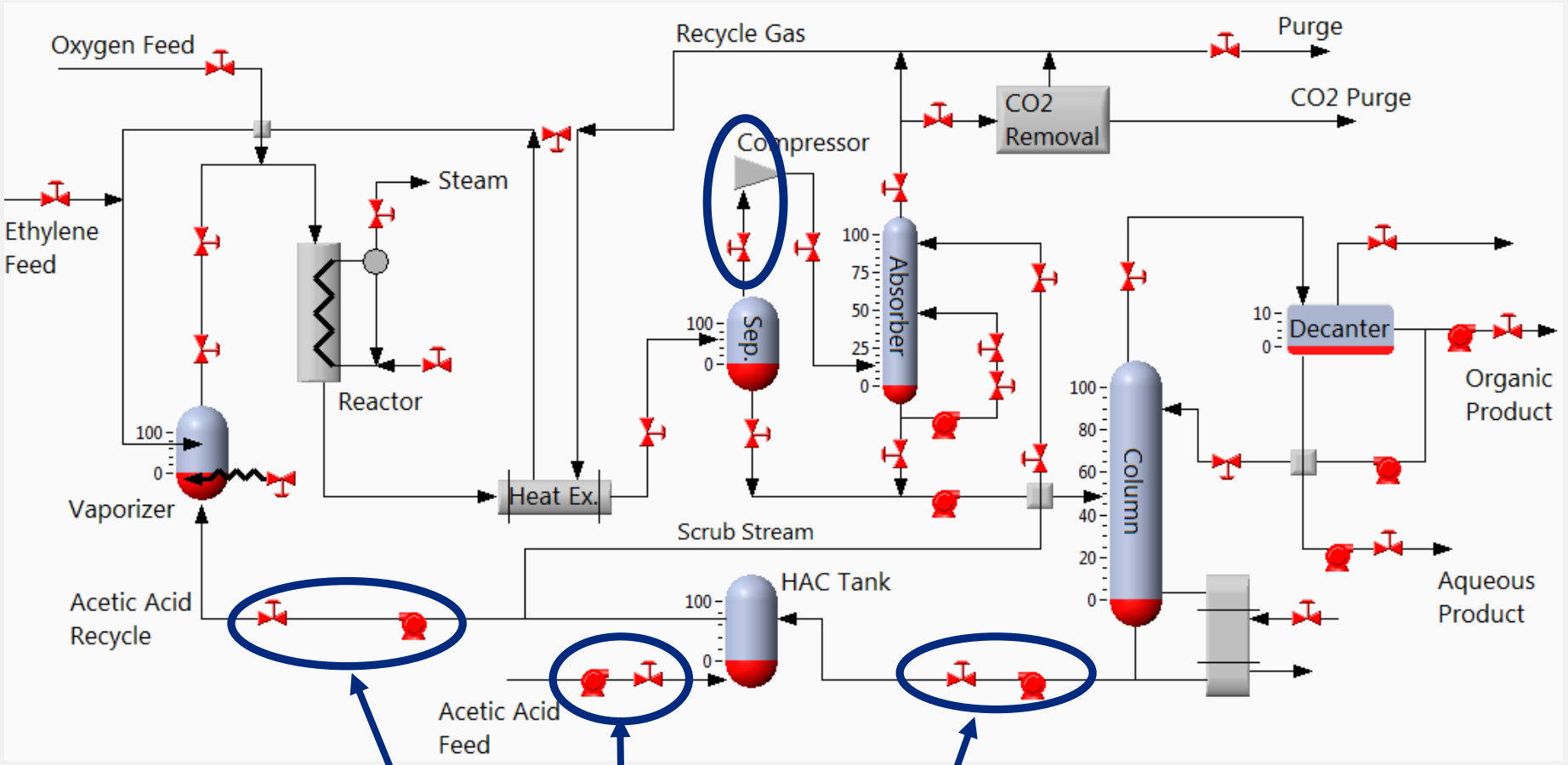
Source: http://www.sigmaaldrich.
Date: 26.12.2014

Process-related vulnerabilities

Tennessee Eastman process



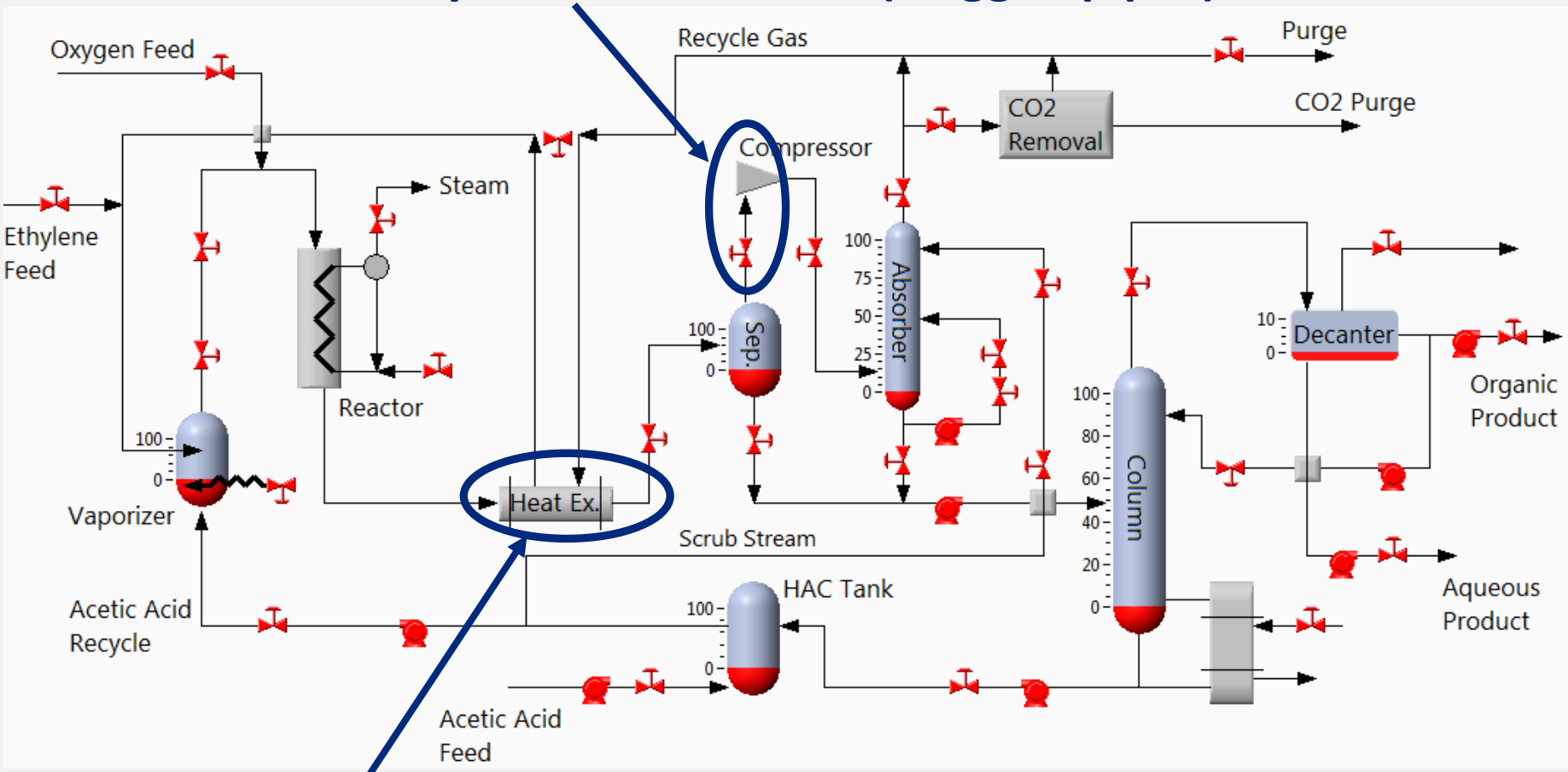
Breakage attack



Candidates for water hammer

Production damage

Polymerization threat (clogged pipes)

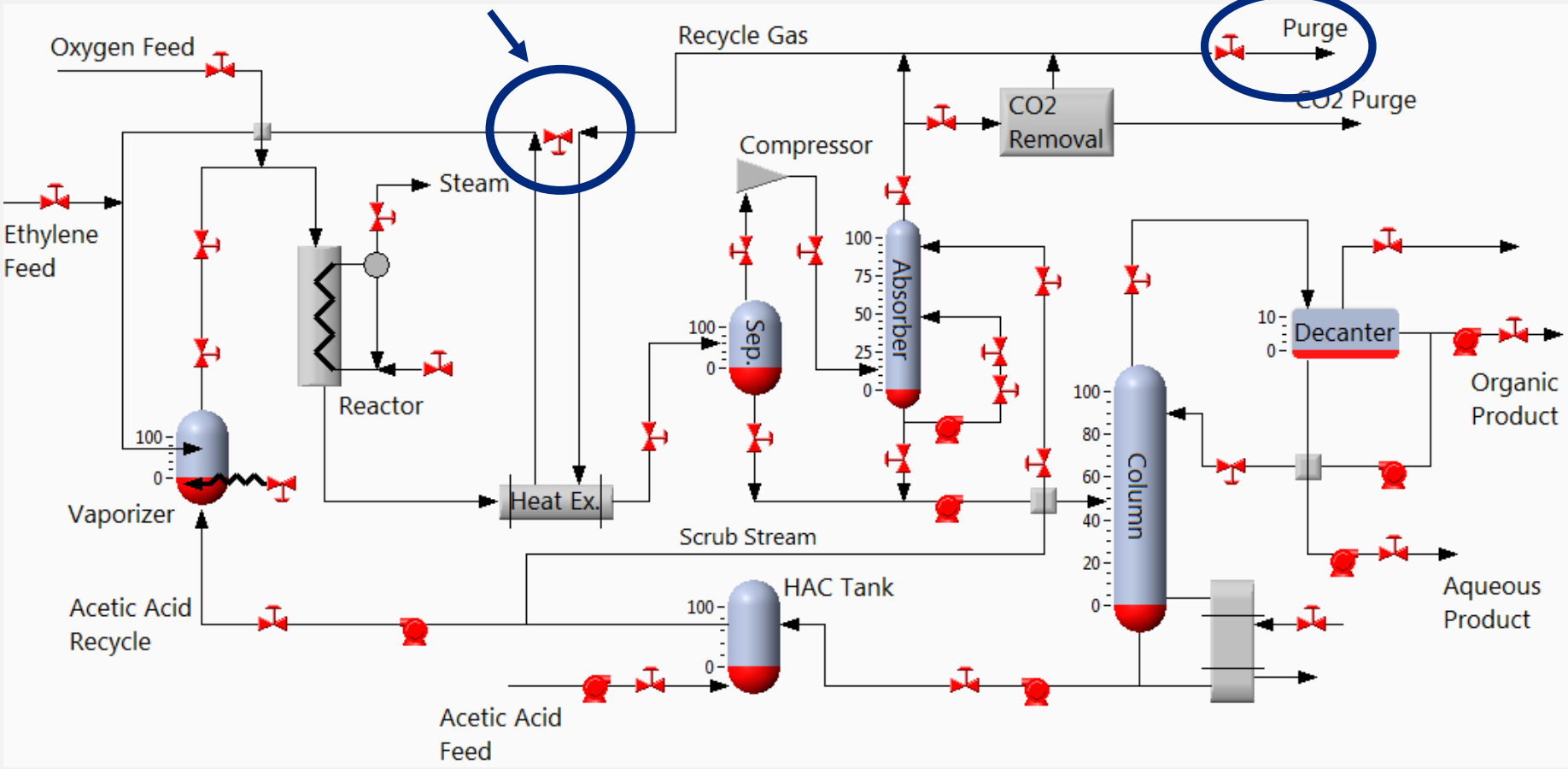


Switch off

Compliance violation

Open the valve

Strange stuff in emissions

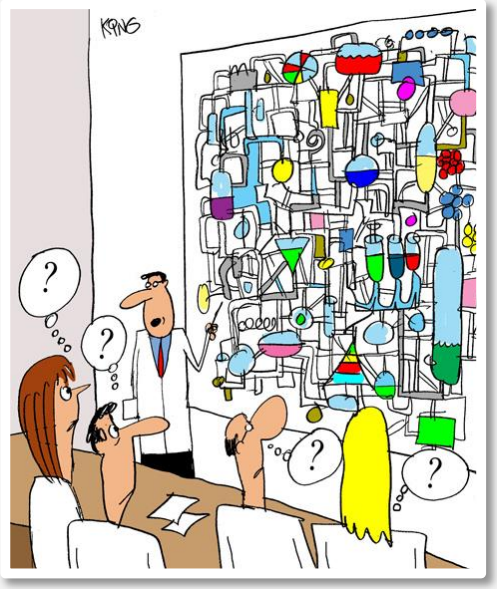


Stages of SCADA attack

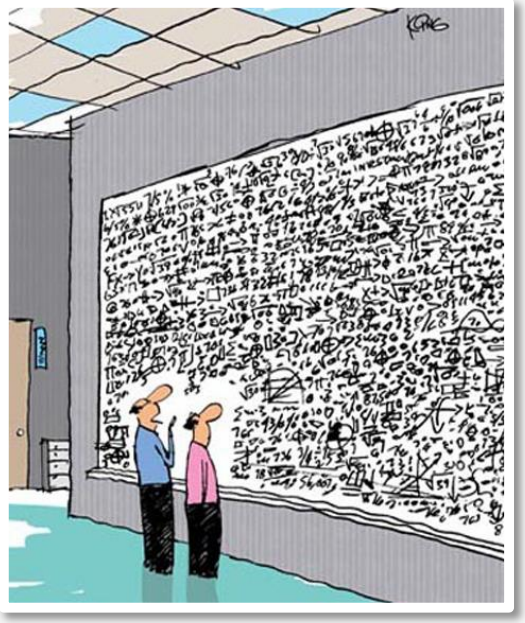
Stages of SCADA attack

Traditional hacking	**Access**
How is this place built and controlled?	**Discovery**
What can I change and how can I conceal?	**Control**
What evil things can I do?	**Damage**
What will they think happened?	**Cleanup**

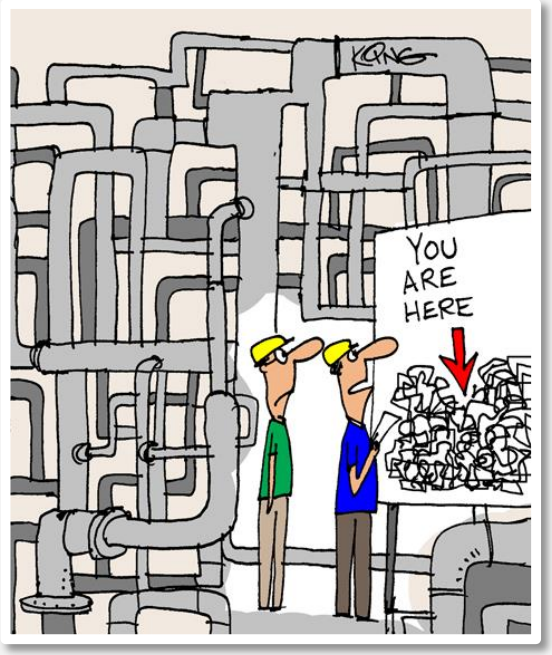
Process discovery



What and how the process is producing



How it is controlled



How it is build and wired

Espionage

11/1/2011
02:10 PM

Nitro Malware Targeted Chem… Companies

Symantec finds Trojan launched indu… chemical compound and advan…

…onage targeting European

targeted campaigns aimed at private companies to steal design documents, formulas, manufacturing processes and research materials.

Drag… …ic Bear Cyber Espionage Attacks Again… …pliers

Hide details

Dick O'Brien, Senior Threat Re…

pbe…

July 3 in AlienVault Labs: Threat Intelligence Updates

Stages of SCADA attack

Traditional hacking

How is this place built and controlled?

What can I change and how can I conceal?

What evil things can I do?

What will they think happened?

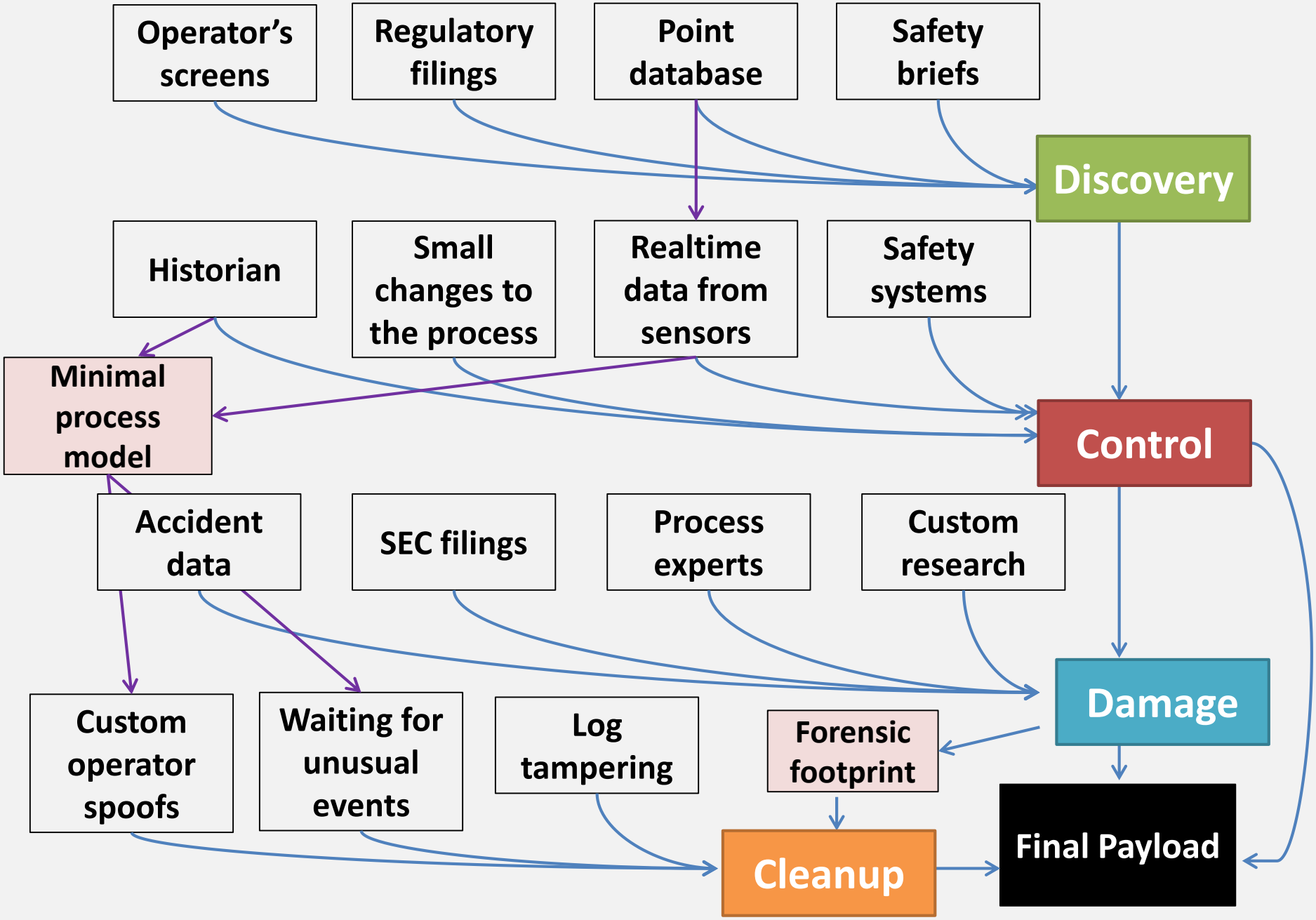
Access

Discovery

Control

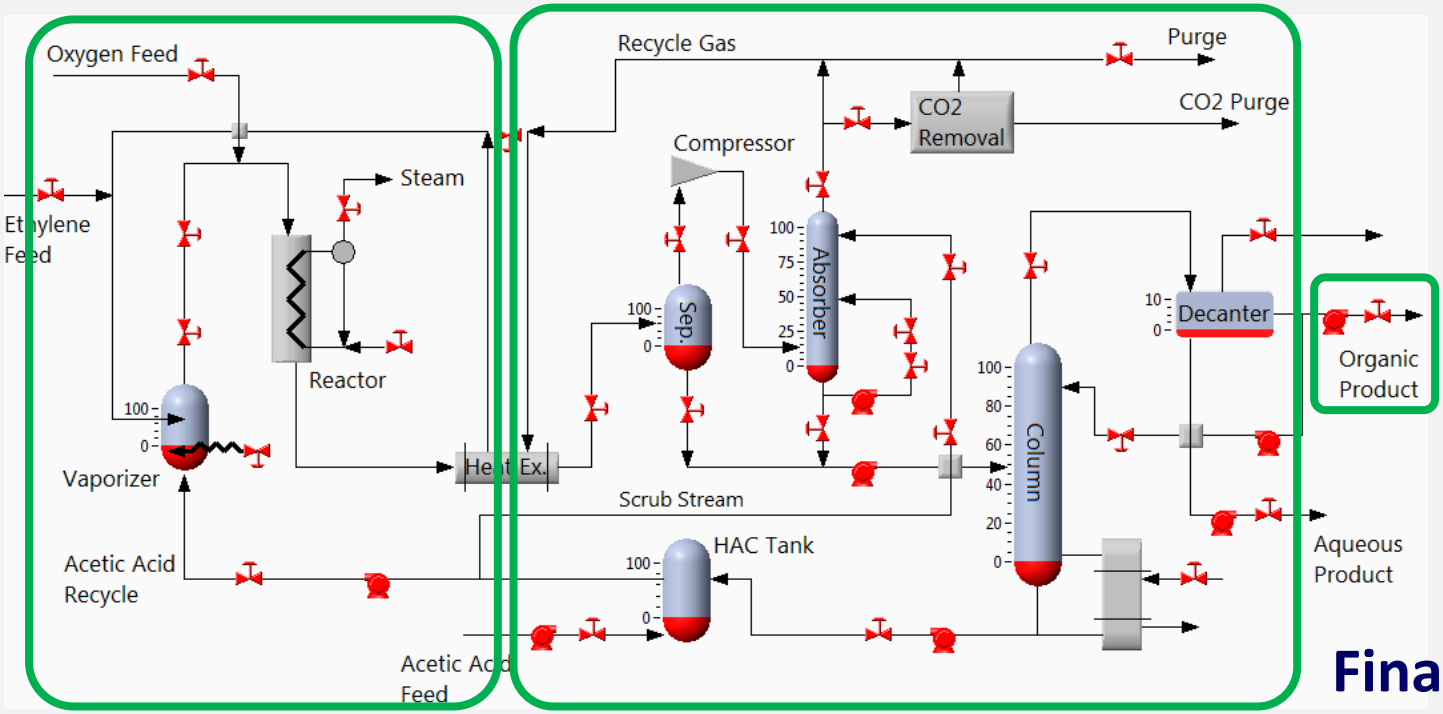
Damage

Cleanup


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

Scenario: catalyst deactivation

Max economic damage?



Product added value

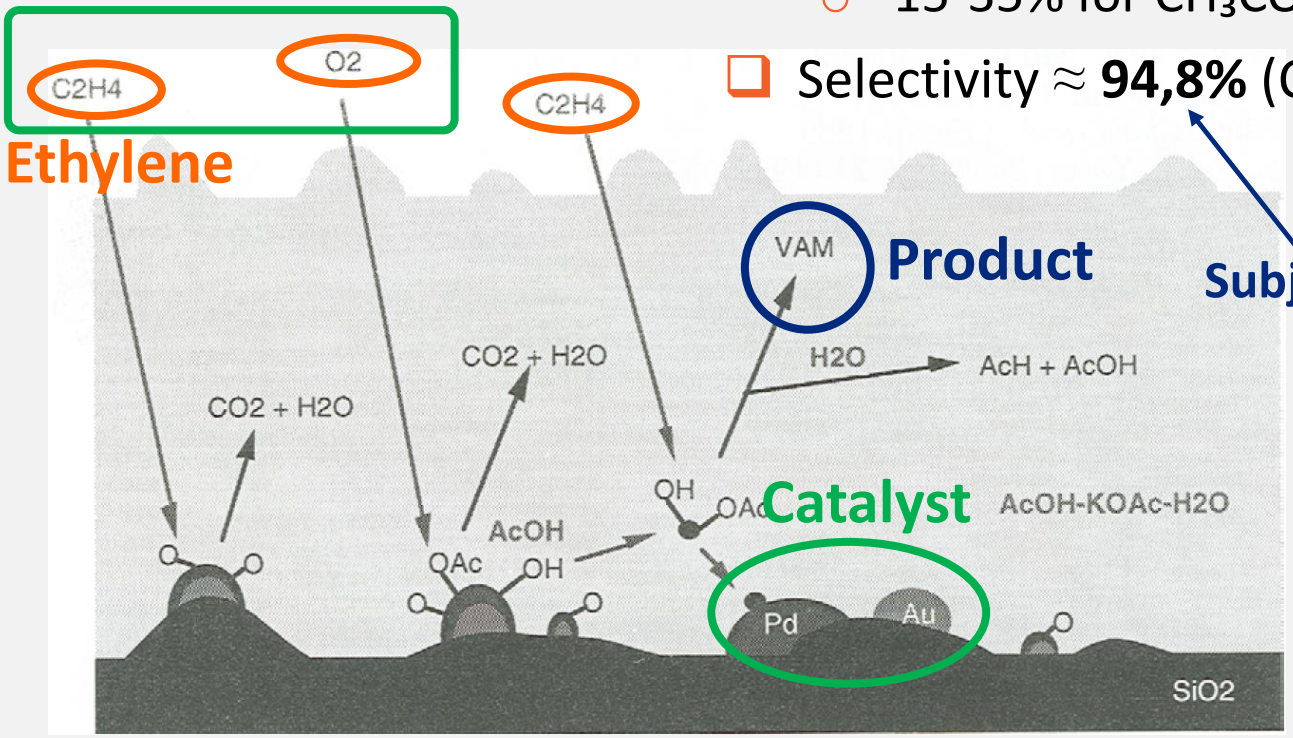
Exploitation knowledge needed

Catalyst

- Lifetime 1-2 years
- Low per-pass conversion
  - 15-35% for CH_3COOH and **8-10%** for C2H4
- Selectivity ≈ **94,8%** (C2H4)

On purpose low

Subjected to constant improvement



W. D. Provine, P. L. Mills, and J. J. Lerou. Discovering the role of Au and KOAc in the catalysis of vinyl acetate synthesis. In Proceedings of the 11th International Congress of Catalysis, volume 101, pages 191-200, 1996

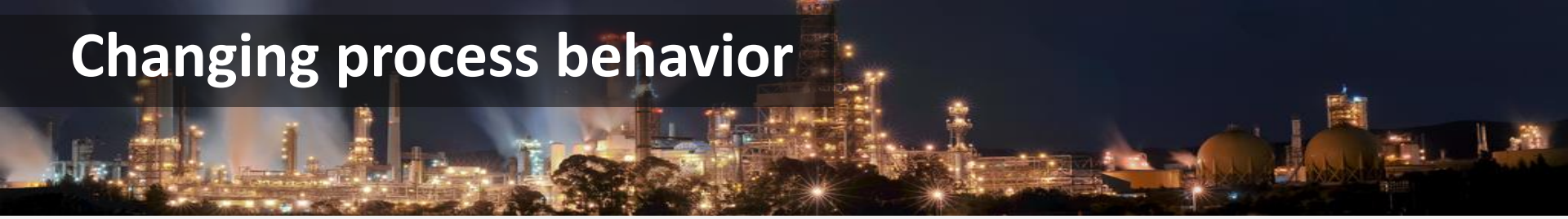
Catalyst killers

- Hot spots above 200C -> permanent deactivation
  - Lower activity at T > 180C
- Change in the reactants inflow ratio
  - More of side reactions (not main reaction)
    - Ethylene combustion
    - CO is a catalyst poison

Reactor with cooling tubes

Discovery

Changing process behavior



- Directly adjust actuators
- Deceive controller about current state of the process
  - Present false process measurements

Control loop

Operator

Controller

SP

Control algorithm

SP

Controller

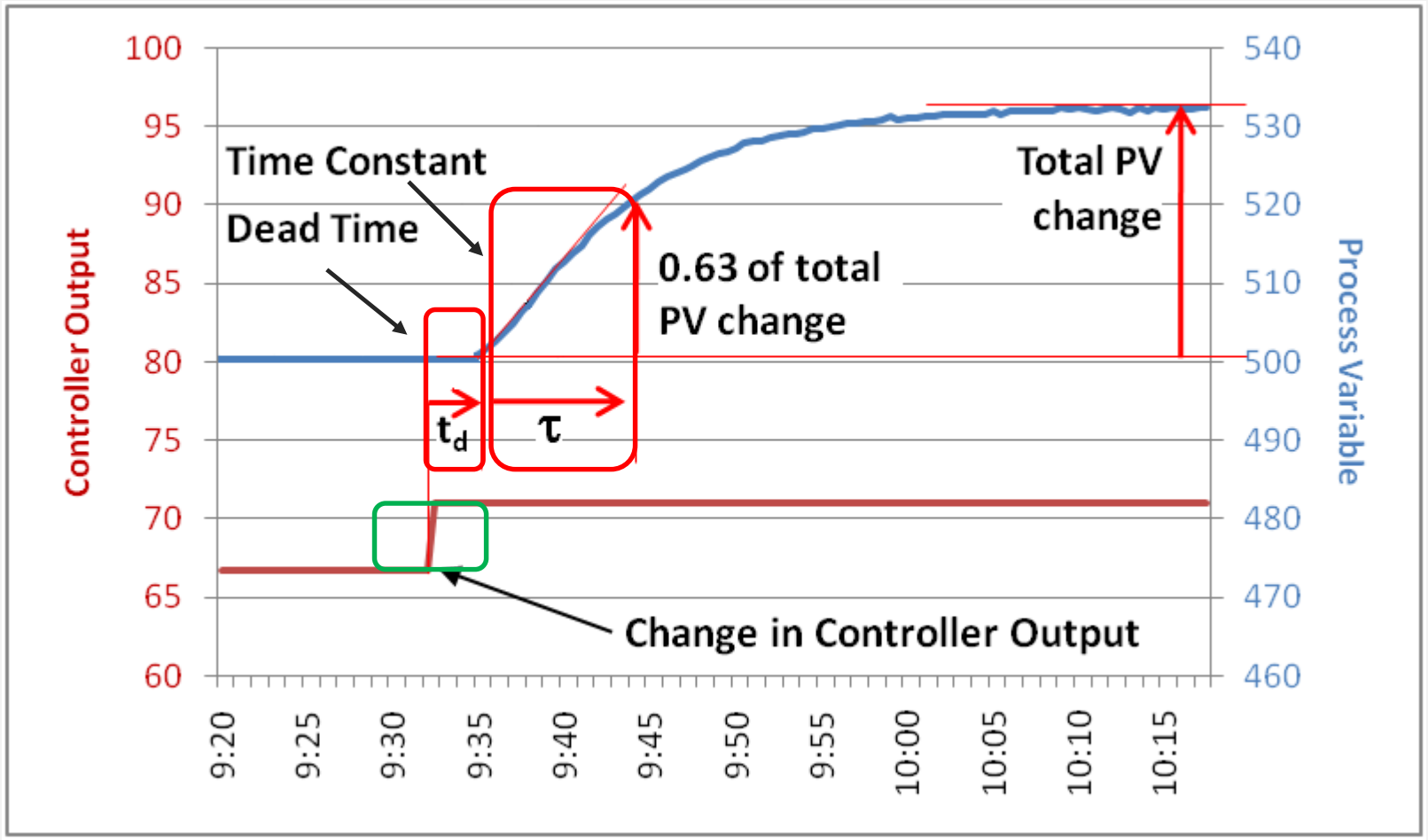
Control algorithm

Sensor

Actuator

Physical process

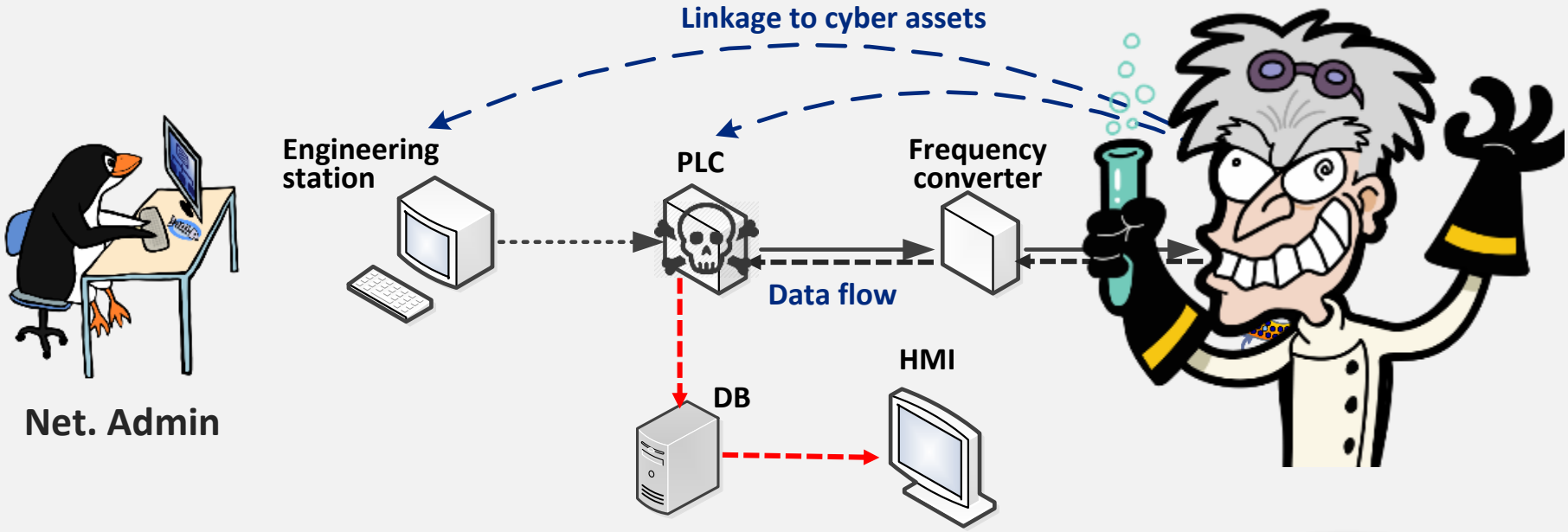
How long: Time constants



Requires local reconnaissance

Jacques Smuts „Process Control for Practitioners“

Example: attack on data flow



Operator

I am not controlling the process!!

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

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

SCADA hacker

During the attack the hacker herself is process engineer, control engineer and process operator

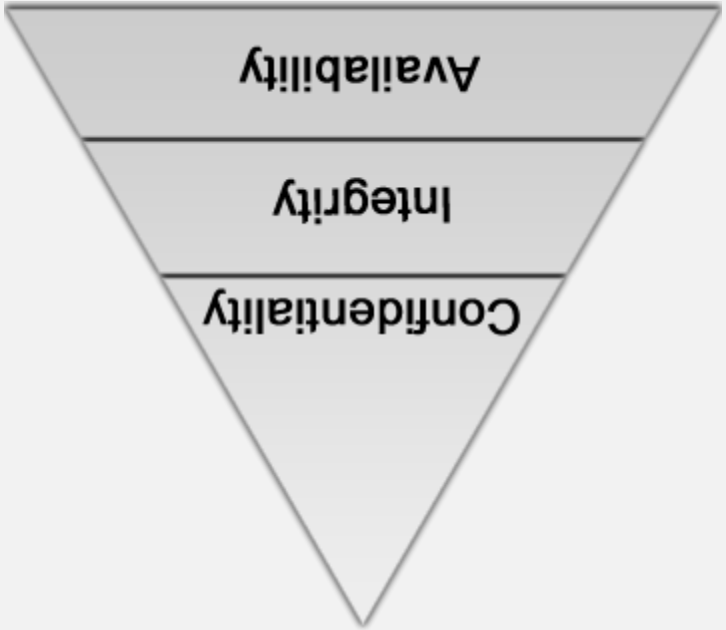
Controllability

Observability

Process-related security properties

HOLY TRINITY

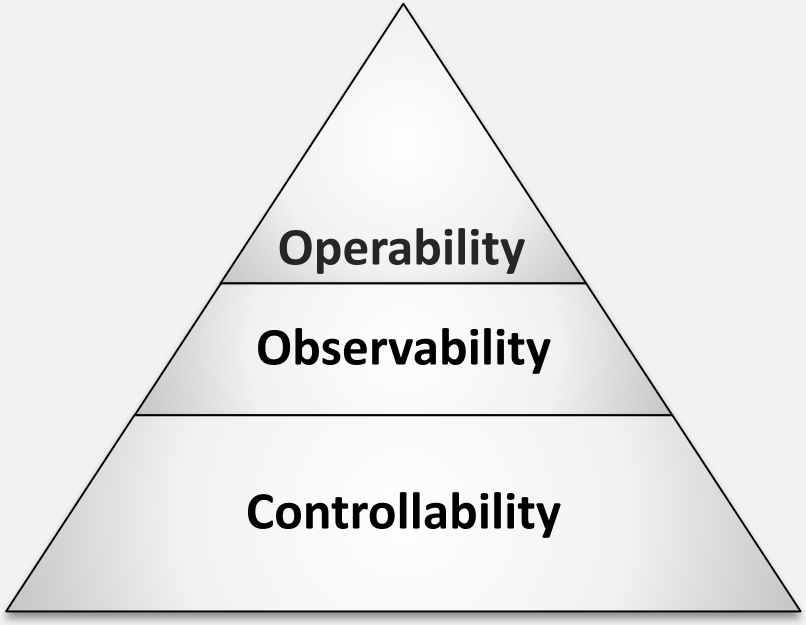
IT domain



Process control

Process-related security properties

HOLY TRINITY



IT domain

Process control

Process-related security properties

HOLY TRINITY

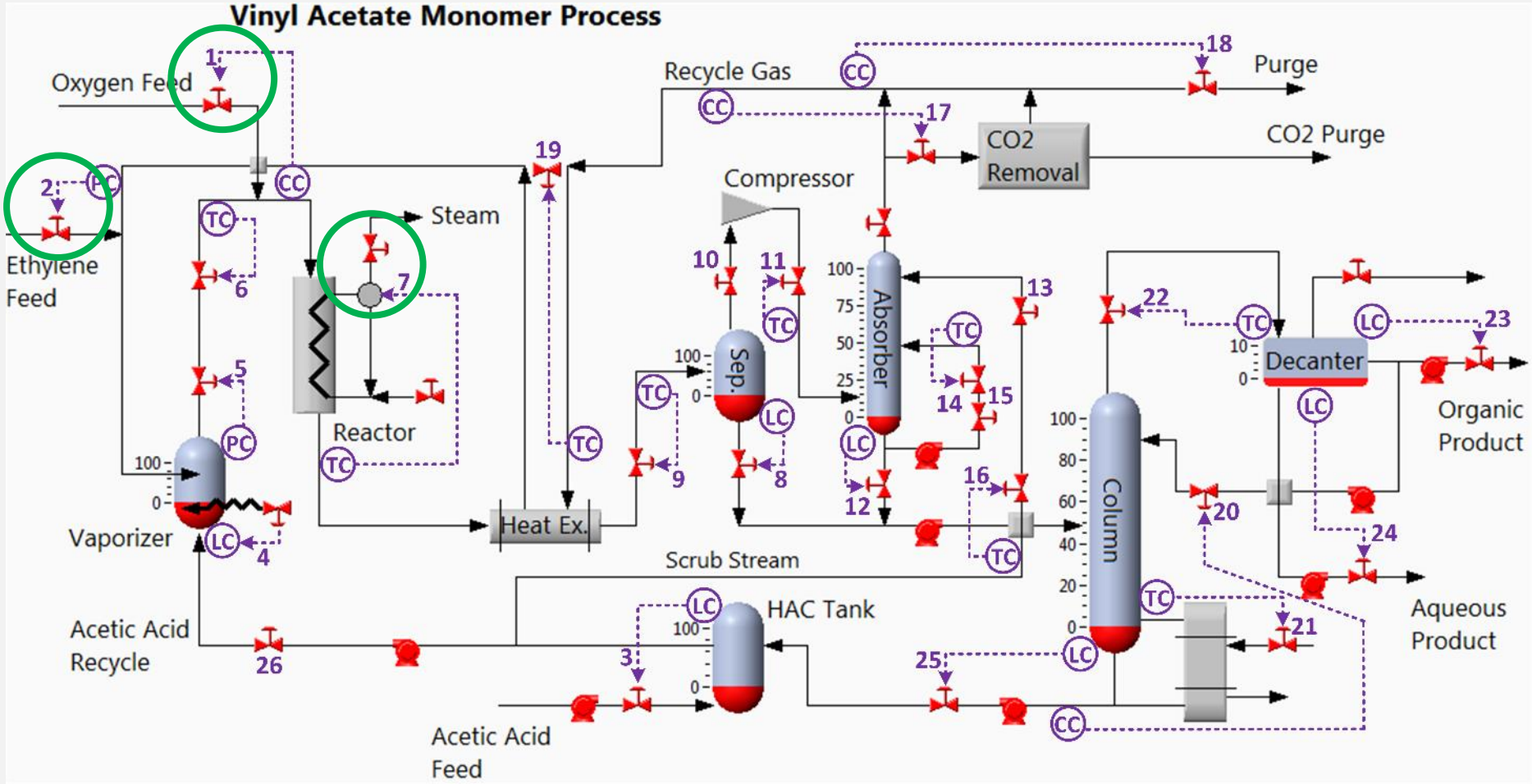
CIA

Information security

CO2

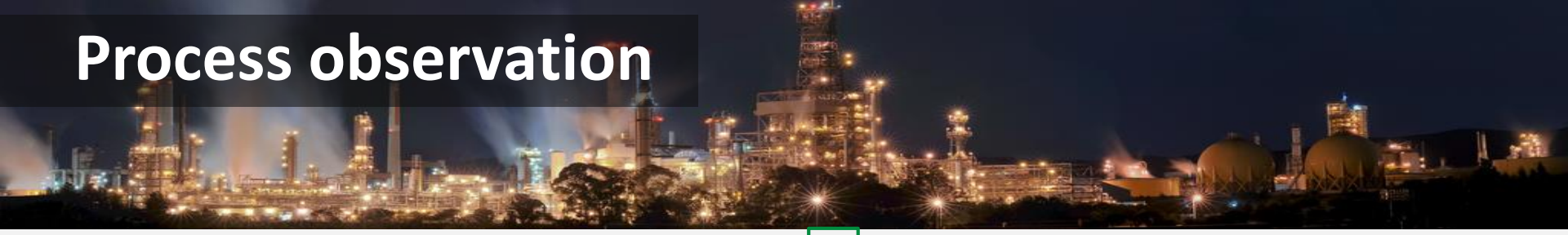
Process control security

Finding controls

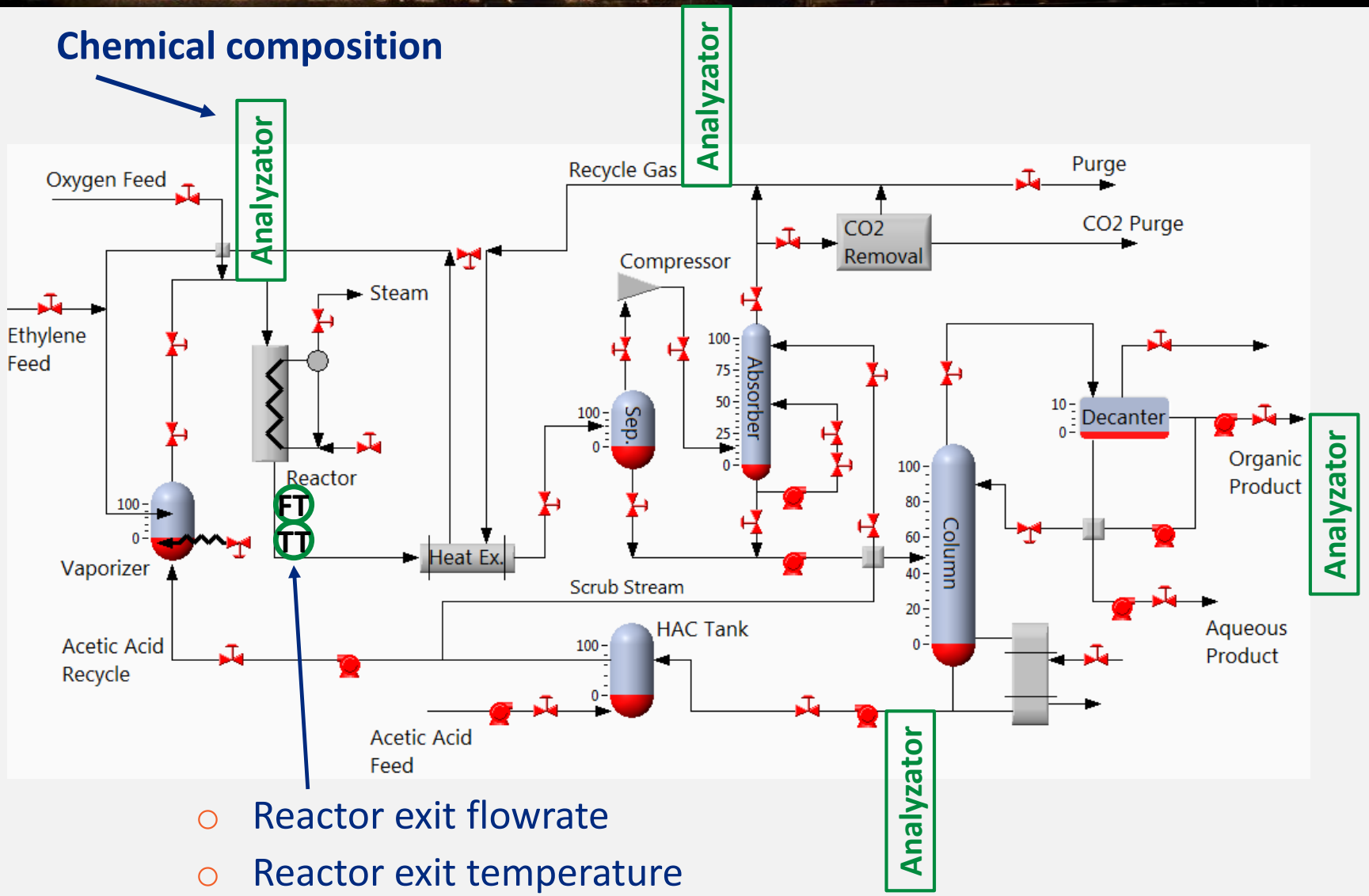


26 actuators ○ 43 measurements

Process observation



Chemical composition



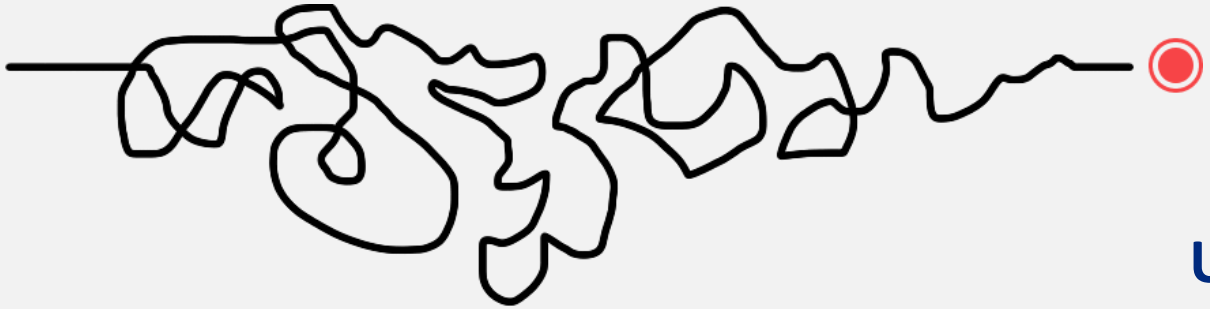
- Reactor exit flowrate
- Reactor exit temperature

Process observation challenges

- **If the required measurements are not in place**
  - Build process model to derive measurements
  - Deduce process state from related measurements
    - E. g. reduced temperature of reactor exit
  - Convert a sensor in place to measure what is needed
    - Work in progress of Mr. Jason Larsen
- **If the required sensor is not measurement capable**
  - Enable capabilities
    - E. g. supersampling for shock wave detection

Process control challenges

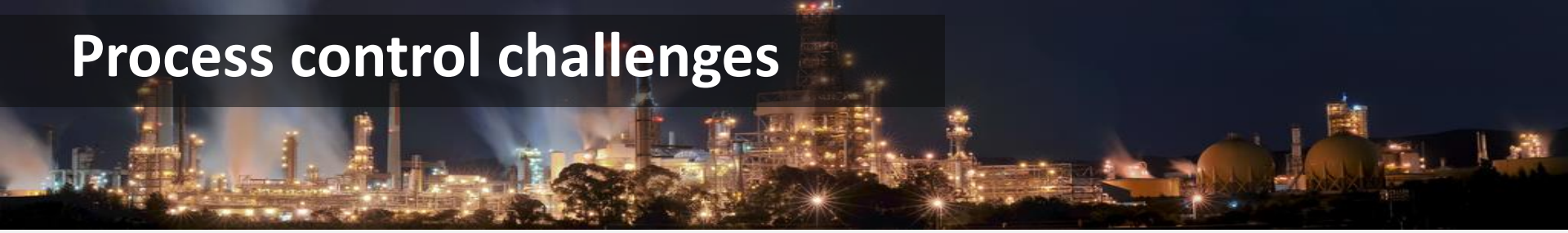
- Process dynamic is highly non-linear
  - WTF (?)



UNCERTAINTY!

- Behavior of process is known to the extent of its modelling
  - So the controllers! They cannot control the process beyond their control model
- The instruments are calibrated to measure the process within its expected operating envelope
  - Attacker will likely to push process outside of its boundaries

Process control challenges



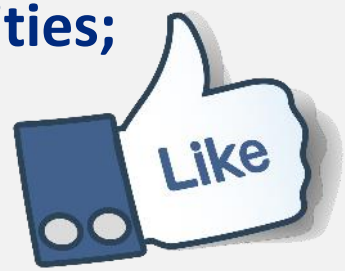
- Process dynamic is highly non-linear
  - WTF (?)

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

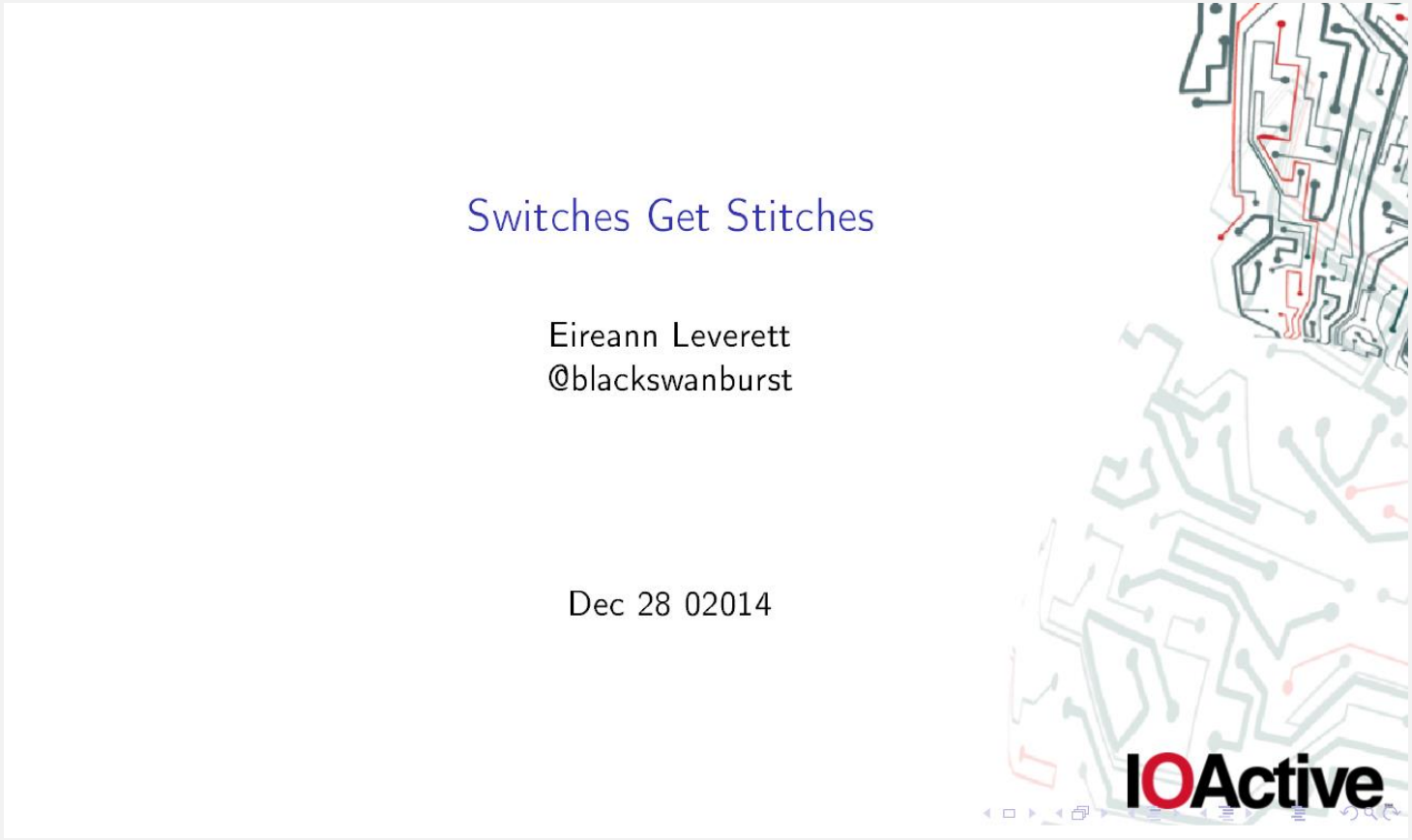
- Behavior of process is known to the extent of its modelling
  - So the controllers! They cannot control the process beyond their control model
- The instruments are calibrated to measure the process within its expected operating envelope
  - Attacker will likely to push process outside of its boundaries

❑ Manipulation of process

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

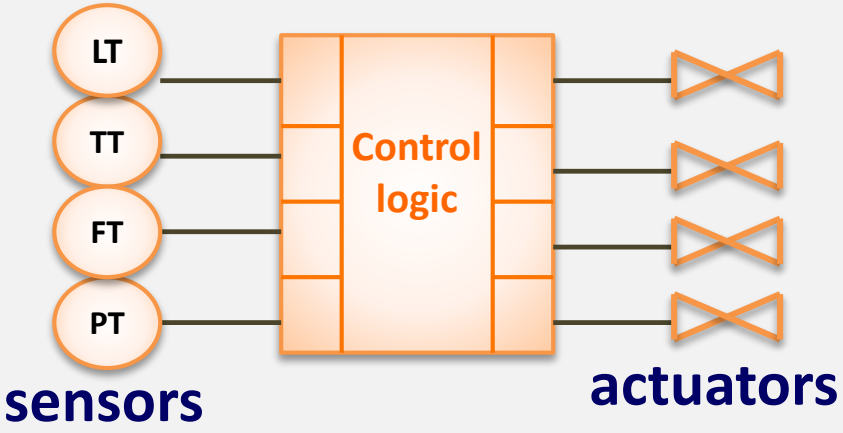


Industrial switches



If timing DoS attacks correctly the attacker can control process at will

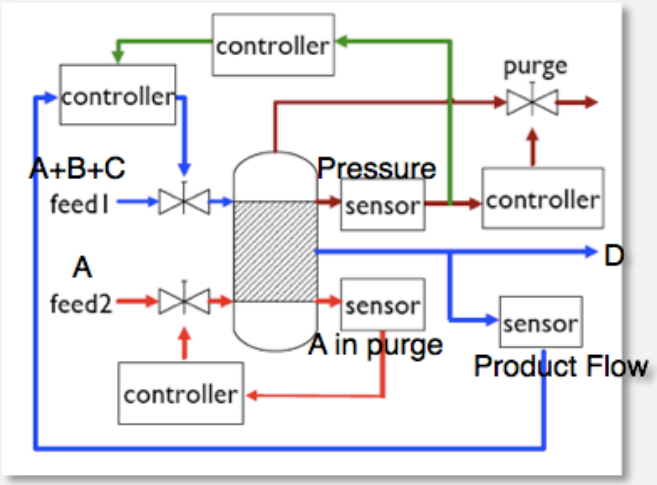
Stale Data attack

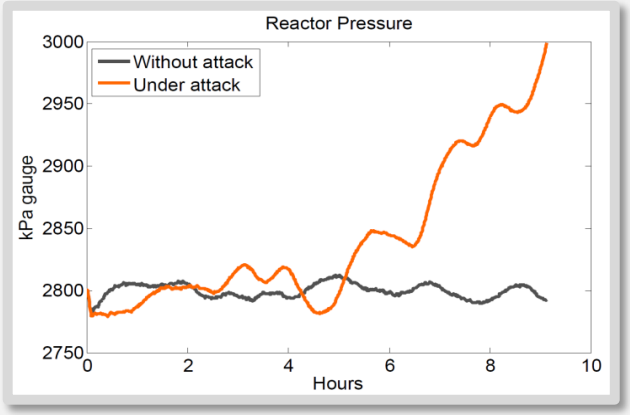


43	45	47	45	43	43	44	43	43
90	89	88	91	91	90	89	90	91
13	15	17	15	13	13	14	13	13
17	15	12	**15**	12	12	12	12	12

Attack time

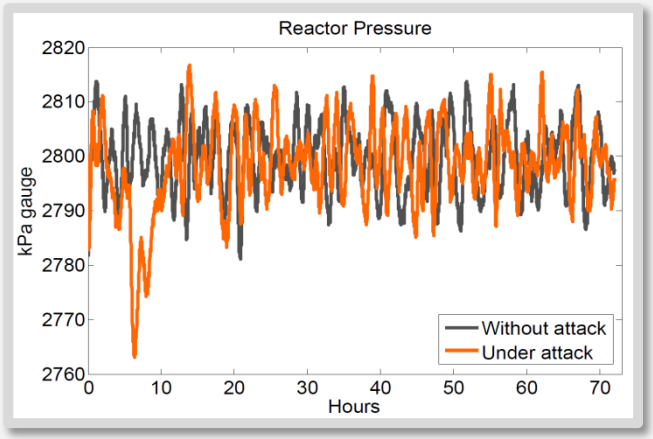
Attack duration

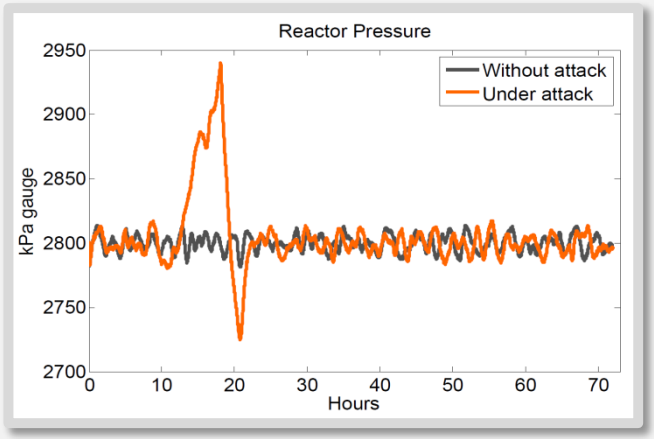


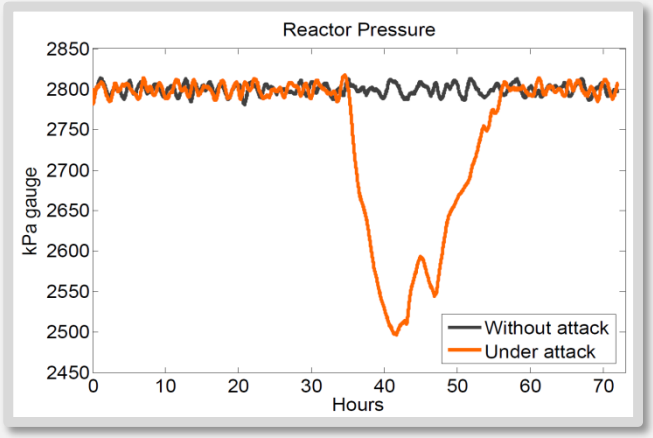


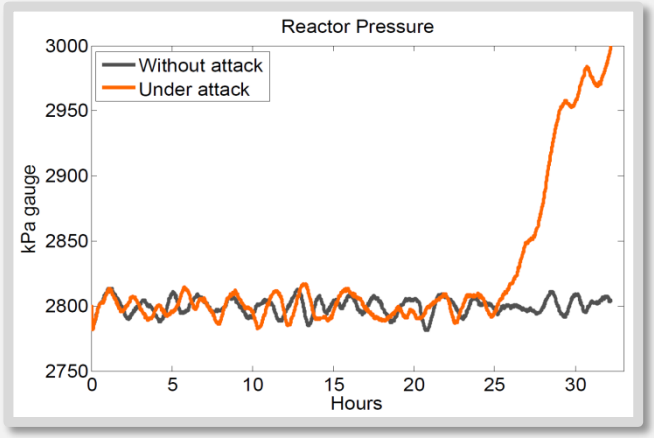
M. Krotofil, A. Cardenas, B. Manning, J. Larsen. CPS: Driving Cyber-Physical Systems to Unsafe Operating Conditions by Timing DoS Attacks on Sensor Signals. In Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC'14)

Timing of the DoS attack









Impact of 8h DoS attacks on reactor pressure sensor at random time

Attack timing

Not yet
Not yet
Not yet
Not yet
Not yet
EAT ME NOW
Too late.

– Avocados

For advanced SCADA hackers

- **Physical environment is a communication media**
- Components can influence each other even if their control loops do not communicate electronically
- **„Unseen state“** of the other component may have **„hidden impact“**

- If a chemical is transferred out of a vessel before it finishes reacting, its behavior may be unexpected – unexpected physics
  - Gaseous ammonia reacts differently than liquid ammonia

Greetings to Sergey Bratus and his „weird machines“

M. Krotofil, J. Larsen. Are you Threatening my Hazards? In Proceedings of the 9th International Workshop on Security (IWSEC‘14)

- **Attack concealment**

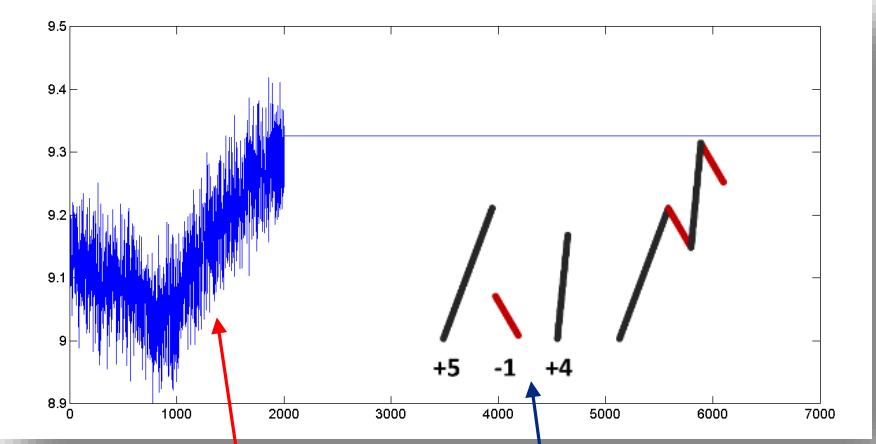
Spoof scenarios

- „Record-and-play-back“
  - Used in Stuxnet
  - Storage requirements
- Derive process model
  - Requires knowledge, CPU cycles and storage
- **Crafted sensor signals**
  - Reconstruction of sensor data features
  - Detection of spoofed signals by the mean of plausibility checks

M. Krotofil, J. Larsen, D. Gollmann. Process Matters: Ensuring Data Veracity in Cyber-Physical Systems. In Proceedings of the 10th ACM Symposium n Information, Computer and Communications Security (ASIACCS‘15)

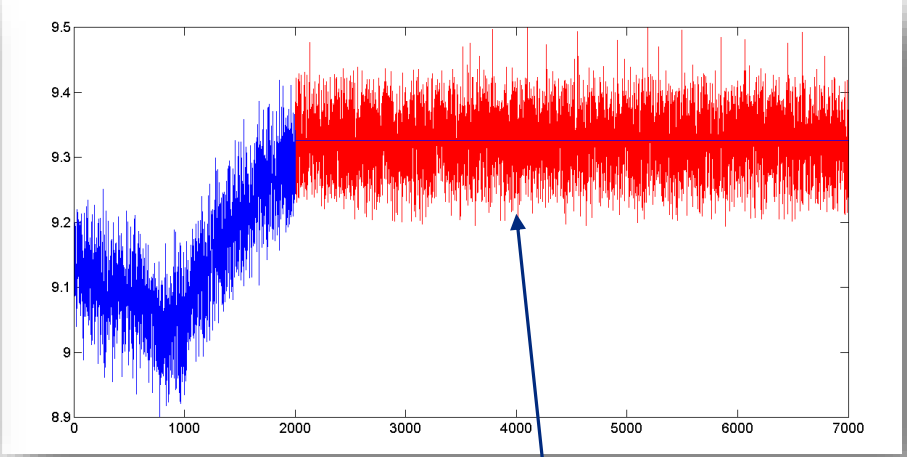
Sensor noise

- Based on Runs Test from statistics
- Treats sensors noise as a pseudo-random sequence



Learning phase

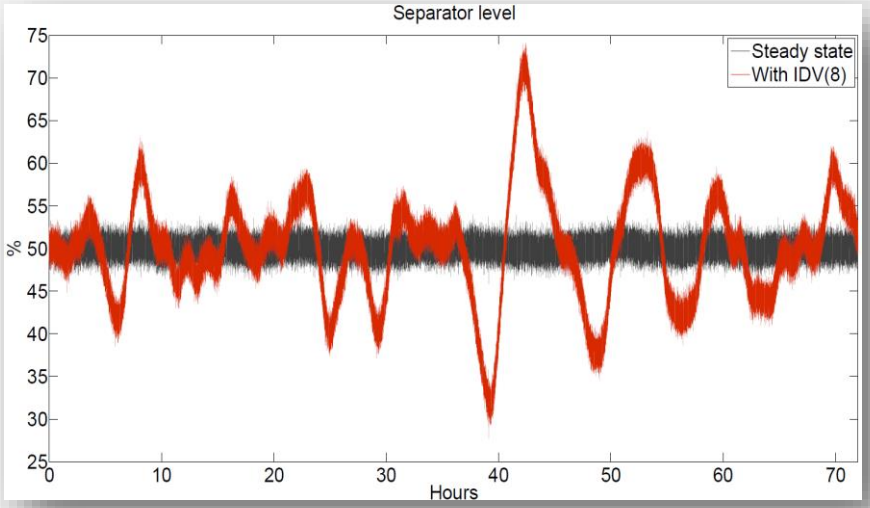
Extracted “runs”

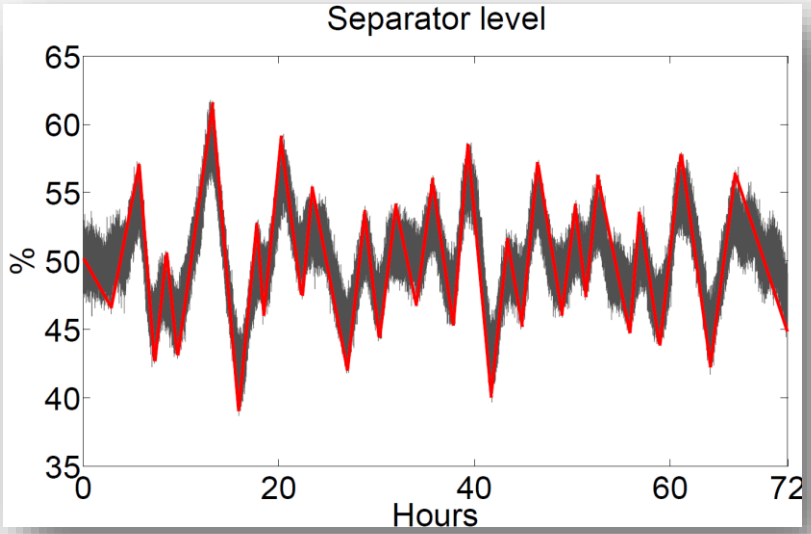


Believable noise

Sensor dynamic behavior

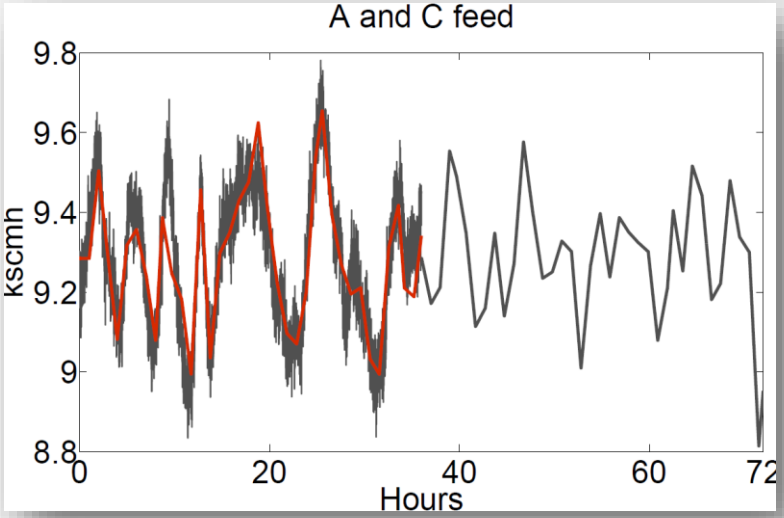
- Line segment approximation for extracting process dynamic
- Spoof: place line segments around signal mean

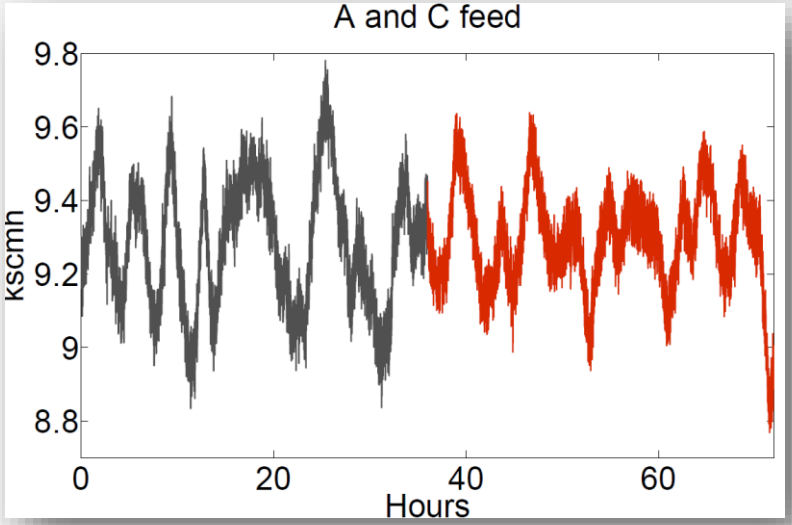




Final result

Find X differences



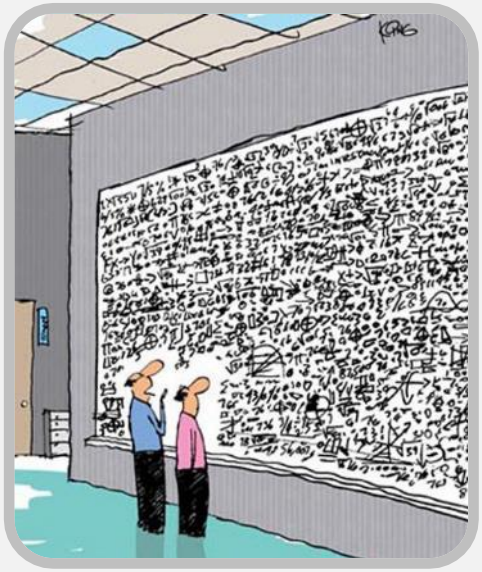


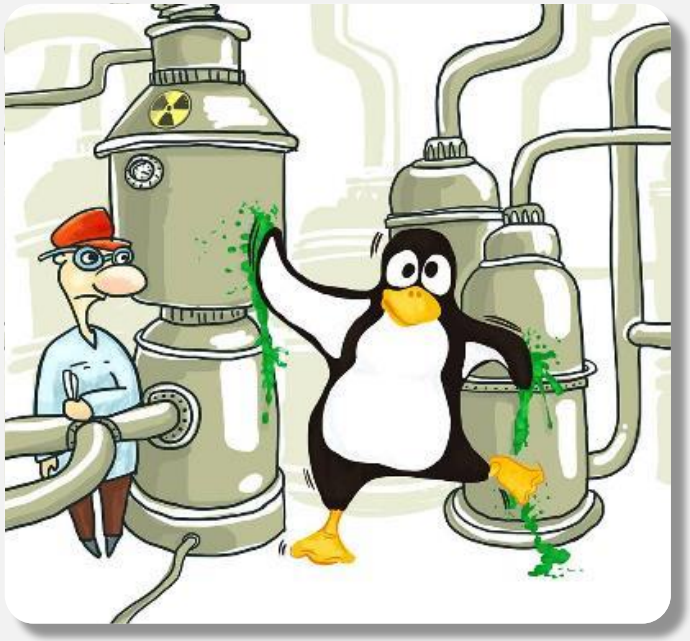
- Few hundreds of bytes of combined data and code
- Accurate for most types of sensor signals
- Scale free; few tuning parameters

The future

Good control vs. good crypto

- Security specialists define required security protections
  - Signatures for authentication and integrity protection
  - Encryption for confidentiality
- Mathematicians do their magic and come up with strong cryptographic primitives and algorithms
- **It is no different with secure controls**
  - Specify the problem and a desired outcome
  - Let control guys do what they do best





marina.krotofil@encs.eu
alexander.isakov@studentpartners.de
pavel.gurikov@tuhh.de
jason.larsen@ioactive.com

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