Quimicefa for hackers: Attacking (and trying to defend) chemical processes

Mikel Iturbe

$ whoami

- Mikel Iturbe
  - Researcher at the Intelligent Systems for Industrial Systems (~~ISIS~~ SISI) Group of Mondragon Unibertsitatea.
  - Work mainly in ICS Security
    - Intrusion (Anomaly) detection
  - Among other things
    - Data analysis

MONDRAGON
UNIBERTSITATEA

GOI ESKOLA
POLITEKNIKOA

FACULTY OF
ENGINEERING

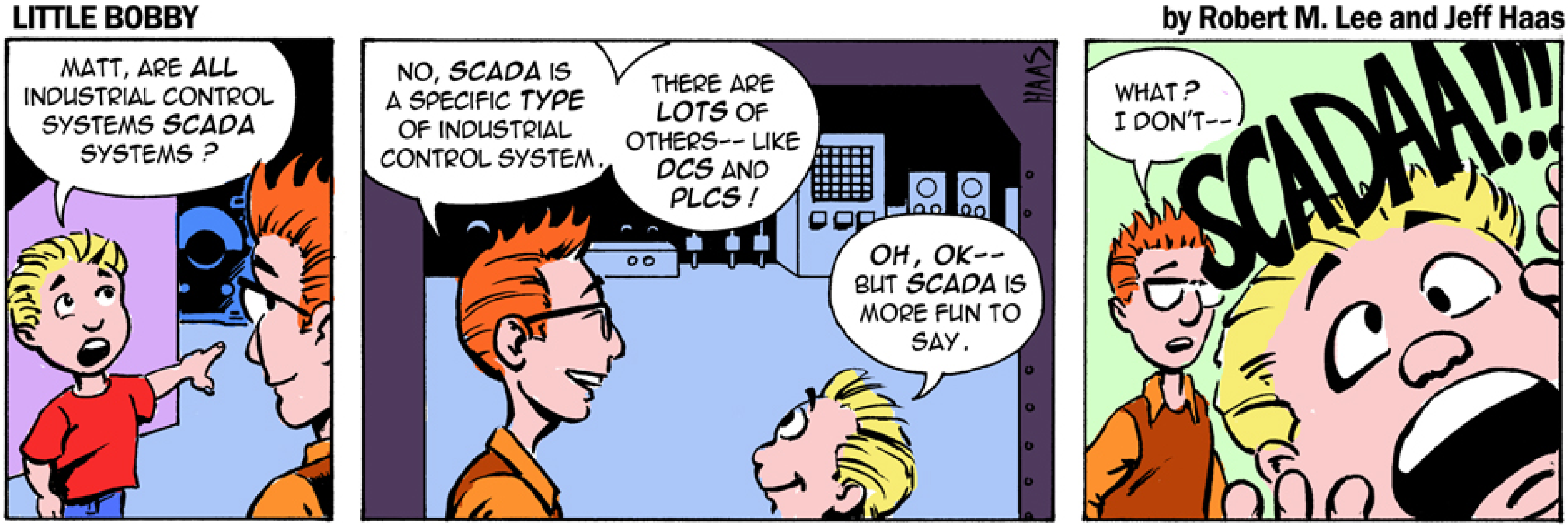
What I’ll talk about

- Intro to ICS/PCS/SCADA/IN/Industrial… security
- Process-level security
- Attacks on chemical plants
  - Demo
- Countermeasures
  - Example
- Conclusions

Control Systems

Control Systems

- ICS/IACS/IN/SCADA/DCS...


LITTLE BOBBY
by Robert M. Lee and Jeff Haas
MATT, ARE ALL INDUSTRIAL CONTROL SYSTEMS SCADA SYSTEMS?
NO, SCADA IS A SPECIFIC TYPE OF INDUSTRIAL CONTROL SYSTEM.
THERE ARE LOTS OF OTHERS-- LIKE DCS AND PLCS!
OH, OK-- BUT SCADA IS MORE FUN TO SAY.
HAAS
WHAT? I DON'T--
SCADAA!!!...

A bit of history

- Trans-Siberian pipeline explosion (1982)
  - Source unconfirmed (myth?)
  - Two hypotheses on the cause:
    - Operator mistake
    - Malicious and leaked software caused the explosion

A bit of history

- Maroochy Water Breach (2004)
  - 142 pumping stations
- Ex-employee attacks the system with stolen equipment
- >1m liters of sewage water spilled with no control.

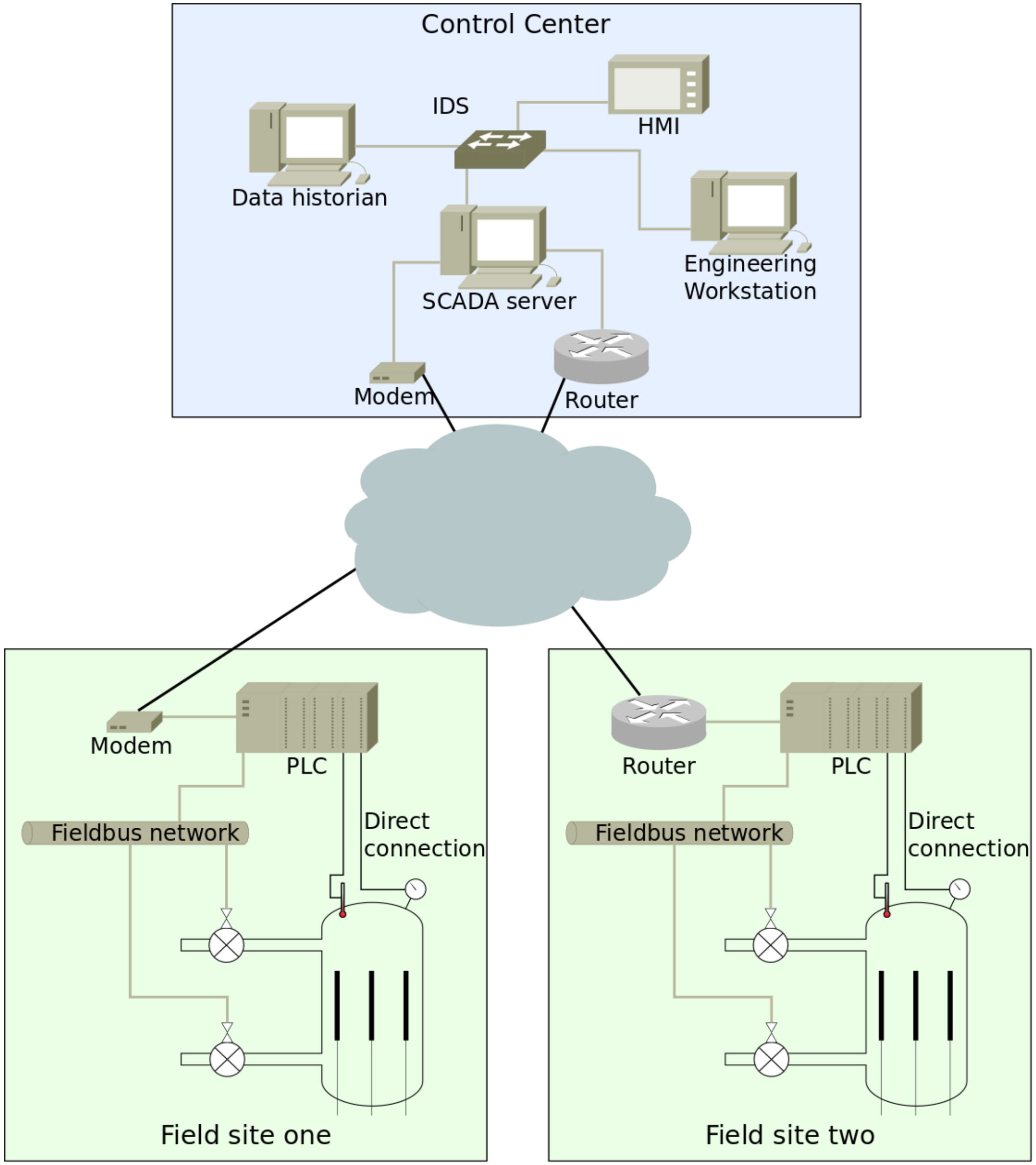
A bit of history

- Stuxnet (2010)
  - Designed to disrupt Iran’s nuclear program
  - 4 zero-days
  - Sabotaged uranium centrifuges by spinning them faster

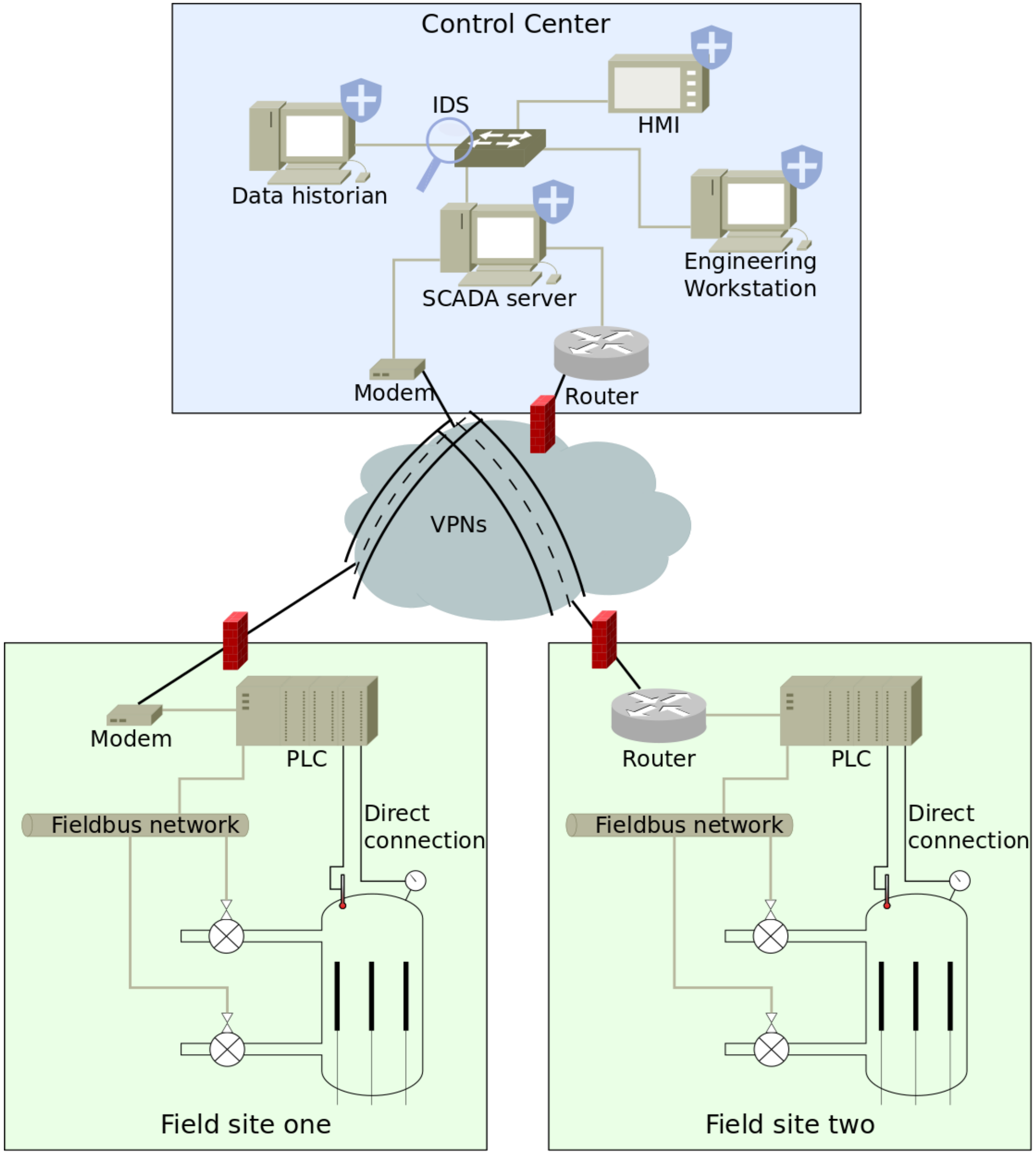
A bit of history

- German Steel Mill Incident (2014)
  - Not much known (who,where…)
  - Spear-Phishing > IT network > OT network
  - A blast furnace could not be shut down properly. “Massive” losses.

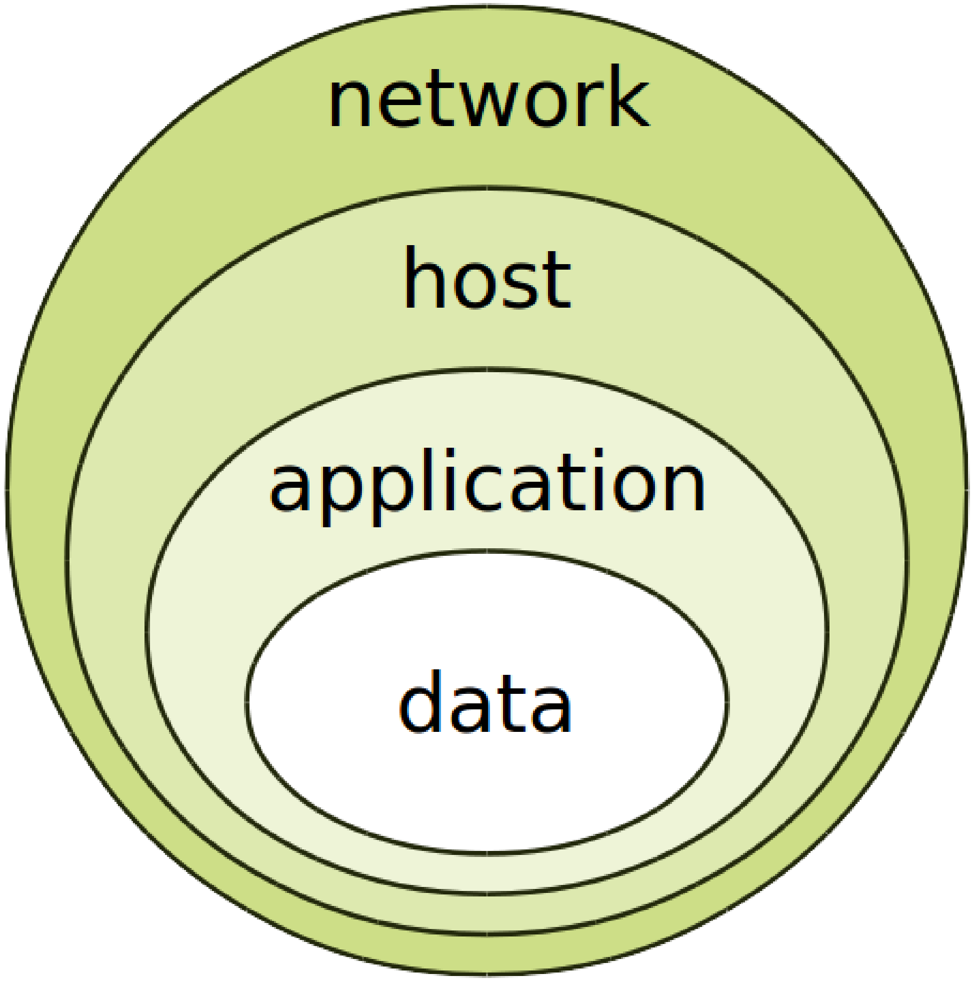
(Defensive) ICS Security



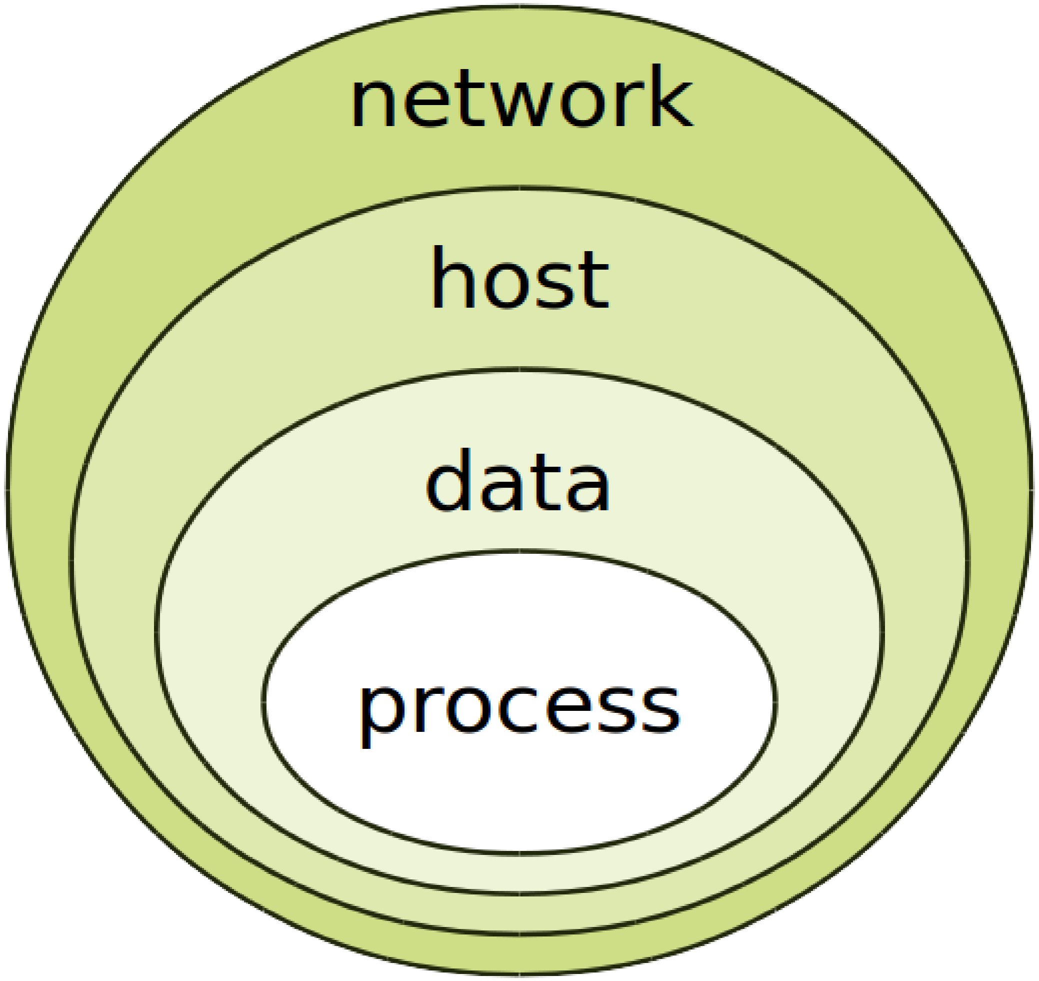
(Defensive) ICS Security



IT layers



ICS layers

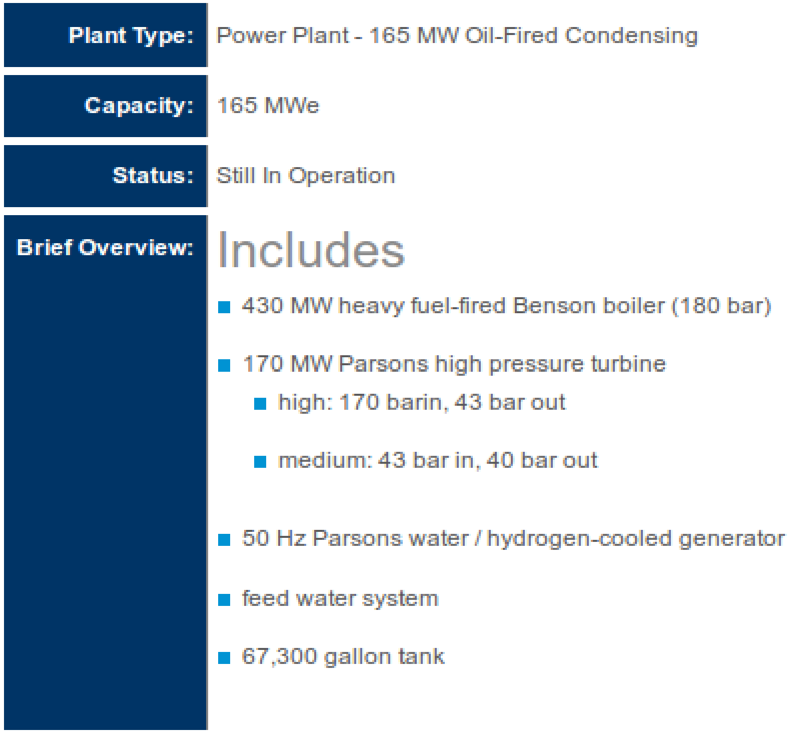


Ok! Let’s start then

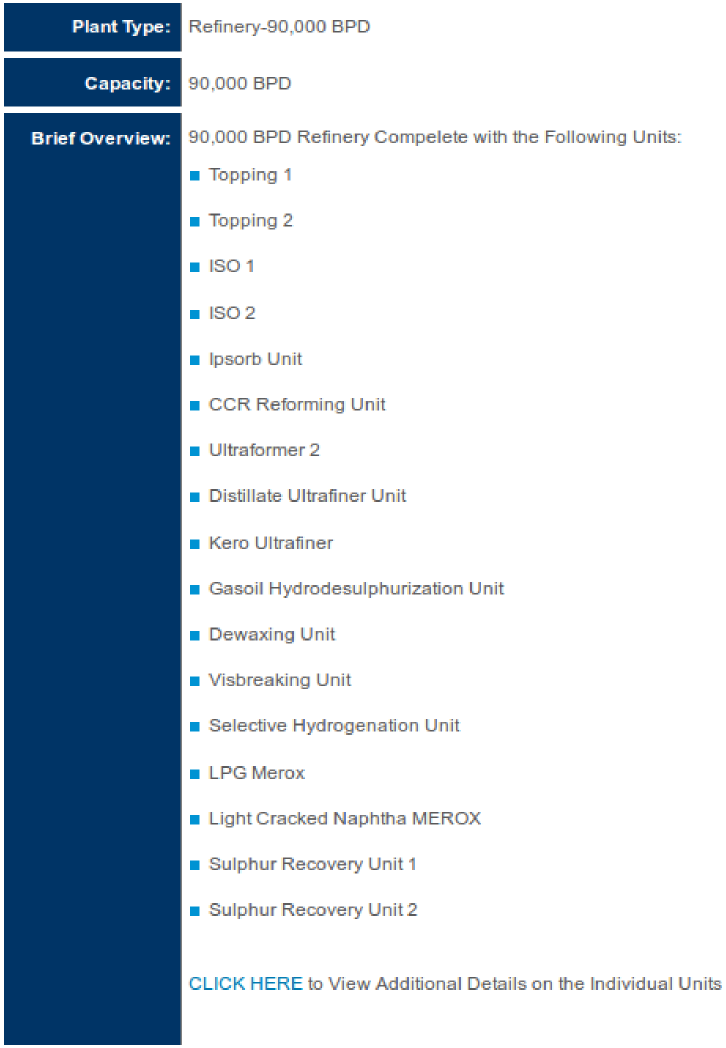
- Realistic environment for research
- Conducting attacks with physical impact requires large domain knowledge
  - Process (what is this?)
  - Control (how it behaves?)
  - Objective (what do I want to achieve?)

Ok! Lets start then

- http://www.ippe.com/Plants
- http://usedplants.com



Plant Type:	Power Plant - 165 MW Oil-Fired Condensing
Capacity:	165 MWe
Status:	Still In Operation
Brief Overview:	Includes ■ 430 MW heavy fuel-fired Benson boiler (180 bar) ■ 170 MW Parsons high pressure turbine ■ high: 170 barin, 43 bar out ■ medium: 43 bar in, 40 bar out ■ 50 Hz Parsons water / hydrogen-cooled generator ■ feed water system ■ 67,300 gallon tank



Plant Type:	Refinery-90,000 BPD
Capacity:	90,000 BPD
Brief Overview:	90,000 BPD Refinery Compelete with the Following Units: ■ Topping 1 ■ Topping 2 ■ ISO 1 ■ ISO 2 ■ Ipsorb Unit ■ CCR Reforming Unit ■ Ultraformer 2 ■ Distillate Ultrafiner Unit ■ Kero Ultrafiner ■ Gasoil Hydrodesulphurization Unit ■ Dewaxing Unit ■ Visbreaking Unit ■ Selective Hydrogenation Unit ■ LPG Merox ■ Light Cracked Naphtha MEROX ■ Sulphur Recovery Unit 1 ■ Sulphur Recovery Unit 2 CLICK HERE to View Additional Details on the Individual Units

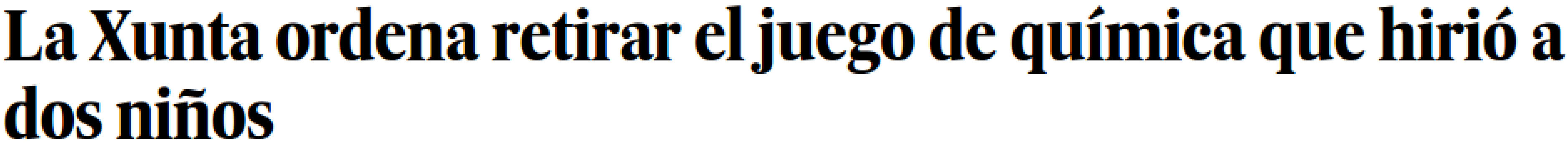
Ok! Let’s start then

- Realistic environment for research
- Let’s not break the bank

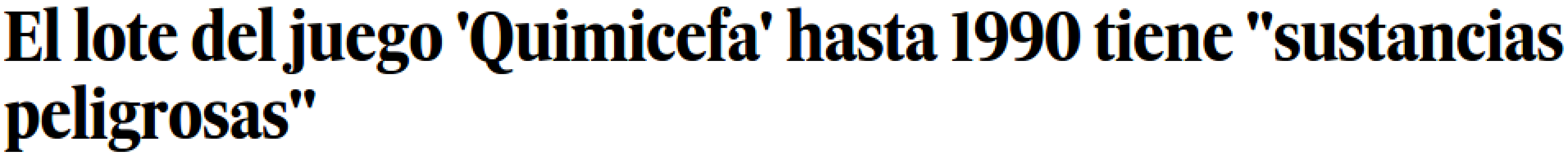
Ok! Let’s start then

QUIMICEFA 1
LABORATORIO EXPERIMENTAL
MAS DE 35 EXPERIENCIAS QUIMICAS
ESTE JUEGO NO CONTIENE PRODUCTOS PELIGROSOS
CEFA

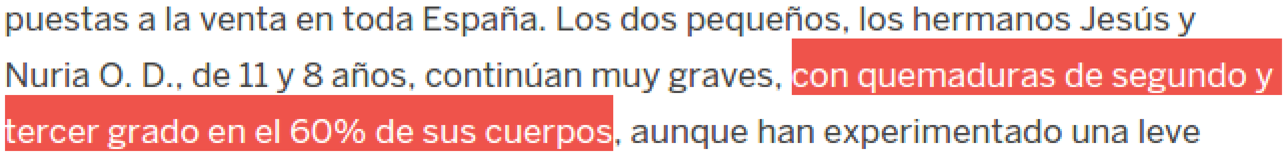
Ok! Let’s start then



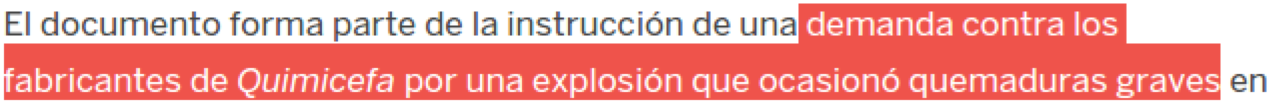
La Xunta ordena retirar el juego de química que hirió a dos niños



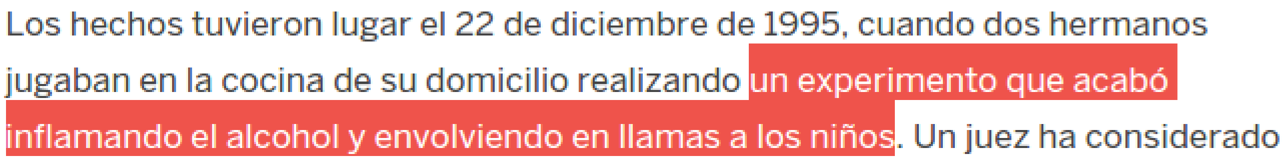
El lote del juego 'Quimicefa' hasta 1990 tiene "sustancias peligrosas"



puestas a la venta en toda España. Los dos pequeños, los hermanos Jesús y Nuria O. D., de 11 y 8 años, continúan muy graves, con quemaduras de segundo y tercer grado en el 60% de sus cuerpos, aunque han experimentado una leve



El documento forma parte de la instrucción de una demanda contra los fabricantes de *Quimicefa* por una explosión que ocasionó quemaduras graves en



Los hechos tuvieron lugar el 22 de diciembre de 1995, cuando dos hermanos jugaban en la cocina de su domicilio realizando un experimento que acabó inflamando el alcohol y envolviendo en llamas a los niños. Un juez ha considerado

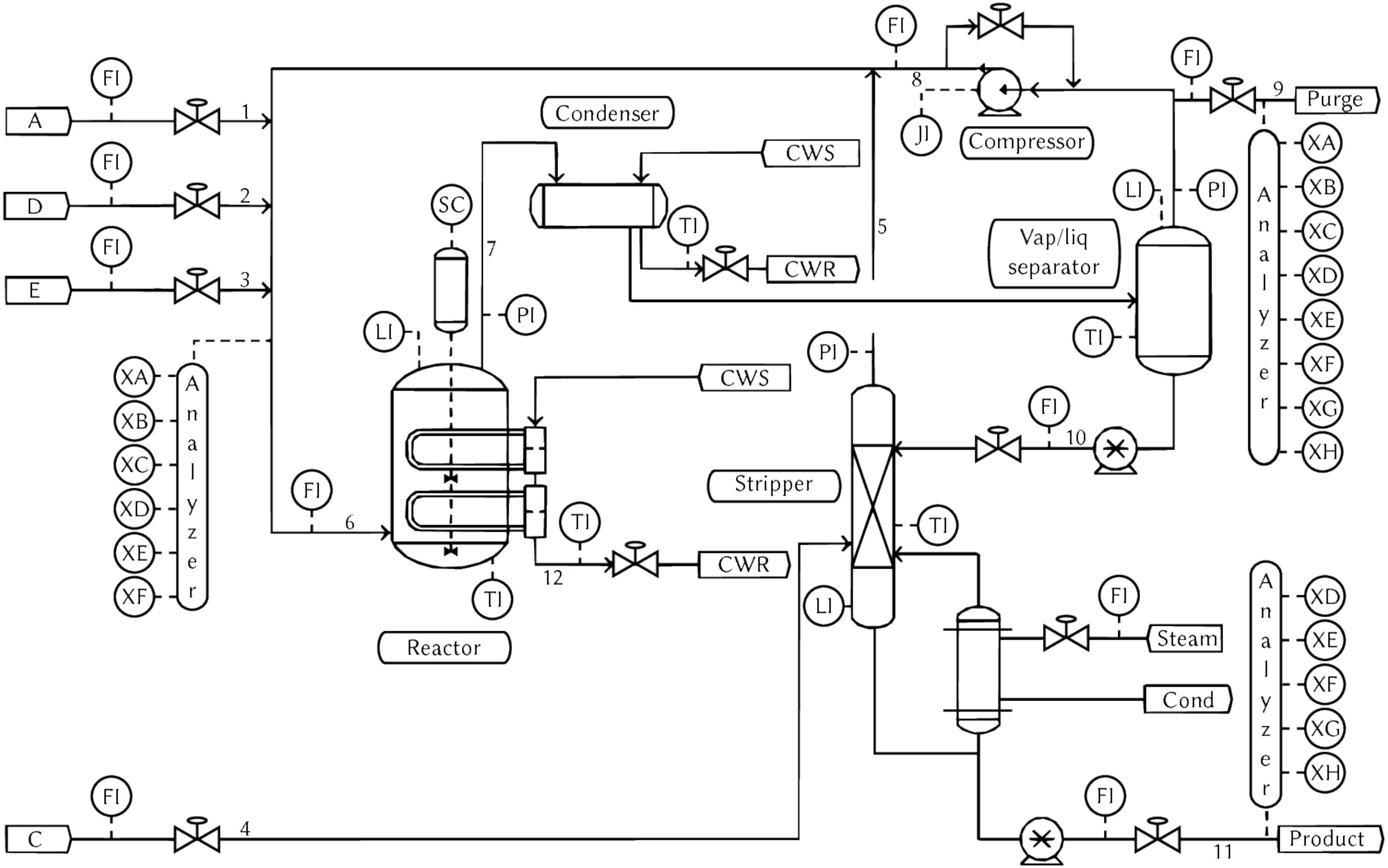
Ok! Let’s start then

- Realistic environment for research
- Let’s not break the bank
- Let’s not get ourselves killed

Simulation: DVCP

- Damn Vulnerable Chemical Process
  - Presented by Krotofil and Larsen
  - Two variants
    - Tennessee-Eastman (TE)
    - Vinyl Acetate Monomer (VAM)
  - Developed over Matlab & Simulink
    - Process in C
    - Control/Execution in Simulink

DVCP-TE


A
D
E
C
FI
1
2
3
4
5
6
7
8
9
10
11
12
Condenser
CWS
CWR
SC
PI
LI
TI
JI
Compressor
Purge
Vap/liq separator
Analyzer
XA
XB
XC
XD
XE
XF
XG
XH
Reactor
Stripper
Steam
Cond
Product

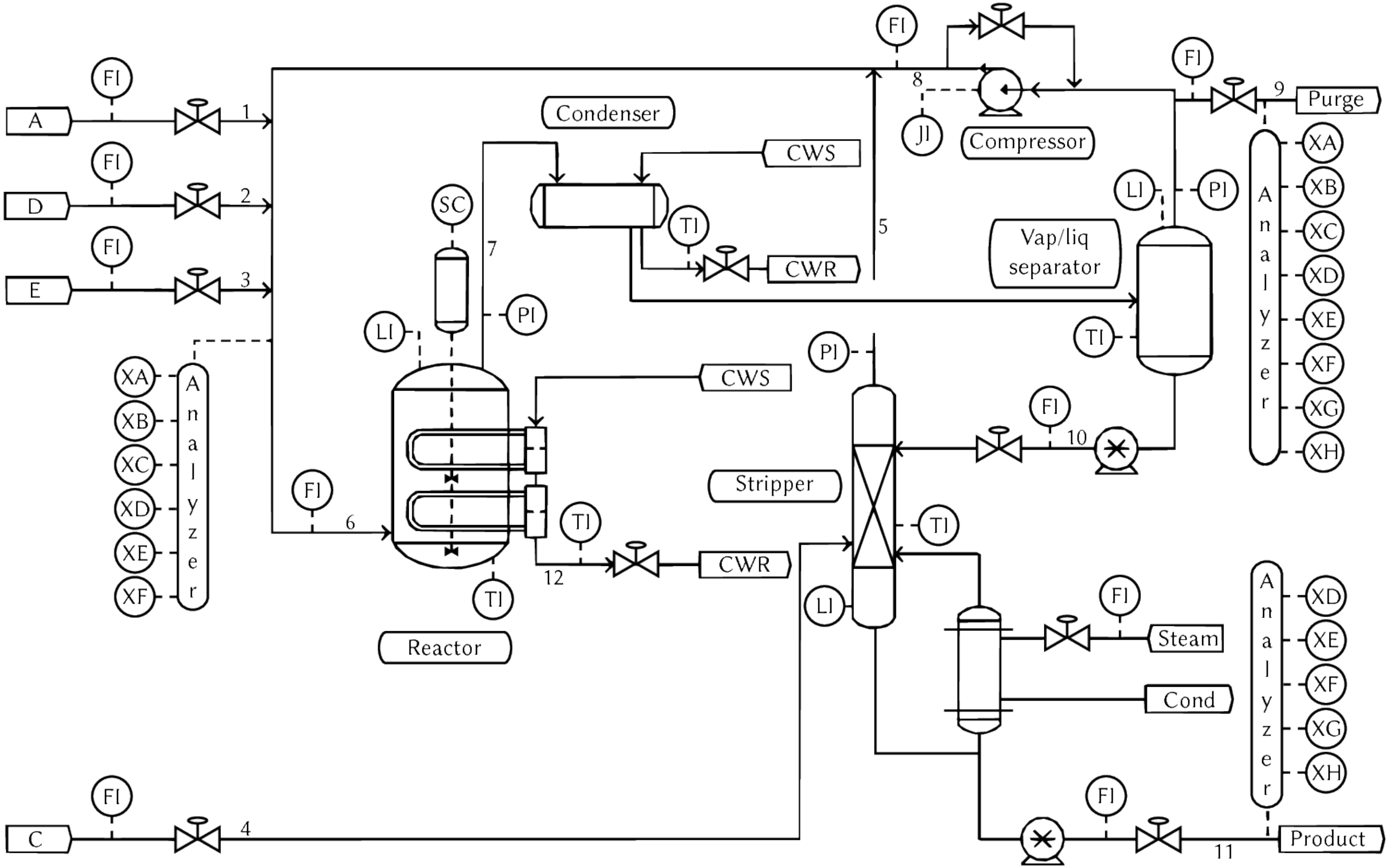
Attacking chemical processes

- Necessary to have wide domain knowledge
  - Knowledge of the process and its control
- Main types of attacks
  - Equipment damage (break stuff...)
  - Economic damage (make it expensive...)

Equipment attacks

- Pipe damage (Clogging, water hammer)
- Reactor damage. (kabooom)

DVCP-TE


A
D
E
C
FI
1
2
3
4
5
6
7
8
9
10
11
12
Condenser
CWS
CWR
TI
SC
PI
LI
JI
Compressor
Purge
Vap/liq separator
Analyzer
XA
XB
XC
XD
XE
XF
XG
XH
Reactor
Stripper
Steam
Cond
Product

Economic attacks

- Produce product of inferior quality (huge impact)
- Increase cost of operation
- More stealthy than equipment attacks

Demo: Attacks

Countermeasures

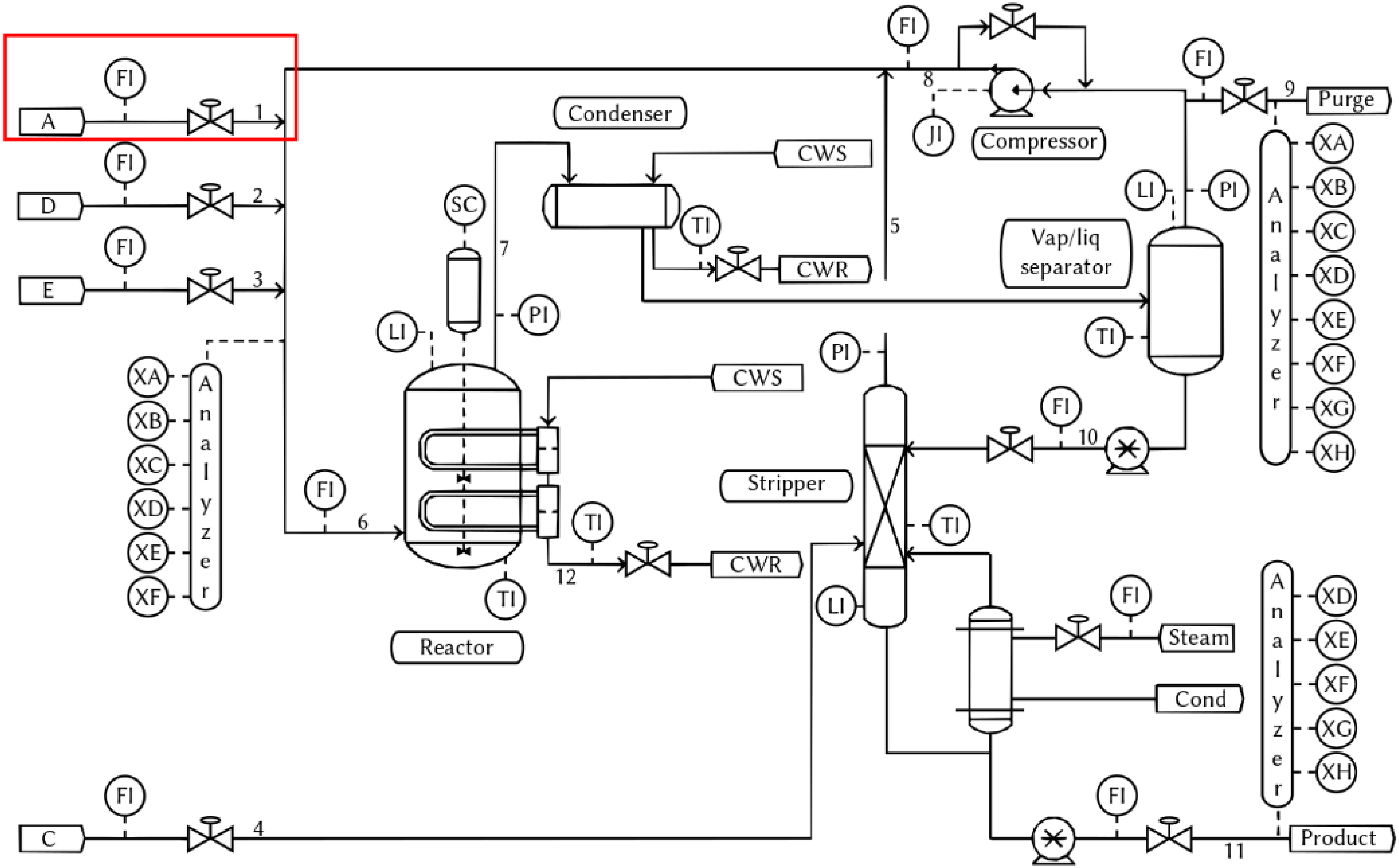
- Monitoring variable values
- Signal noise analysis for replay attacks
- Predictive approaches
- Non-predictive approaches

Multivariate Statistical Proc. Control

- Previously used for fault detection/quality control
- By using PCA, it transforms the original variable space into a new subspace
- Two statistics are computed, *D* and *Q* and these are monitored
- Once an anomaly is detected, by using contribution plots we diagnose its cause

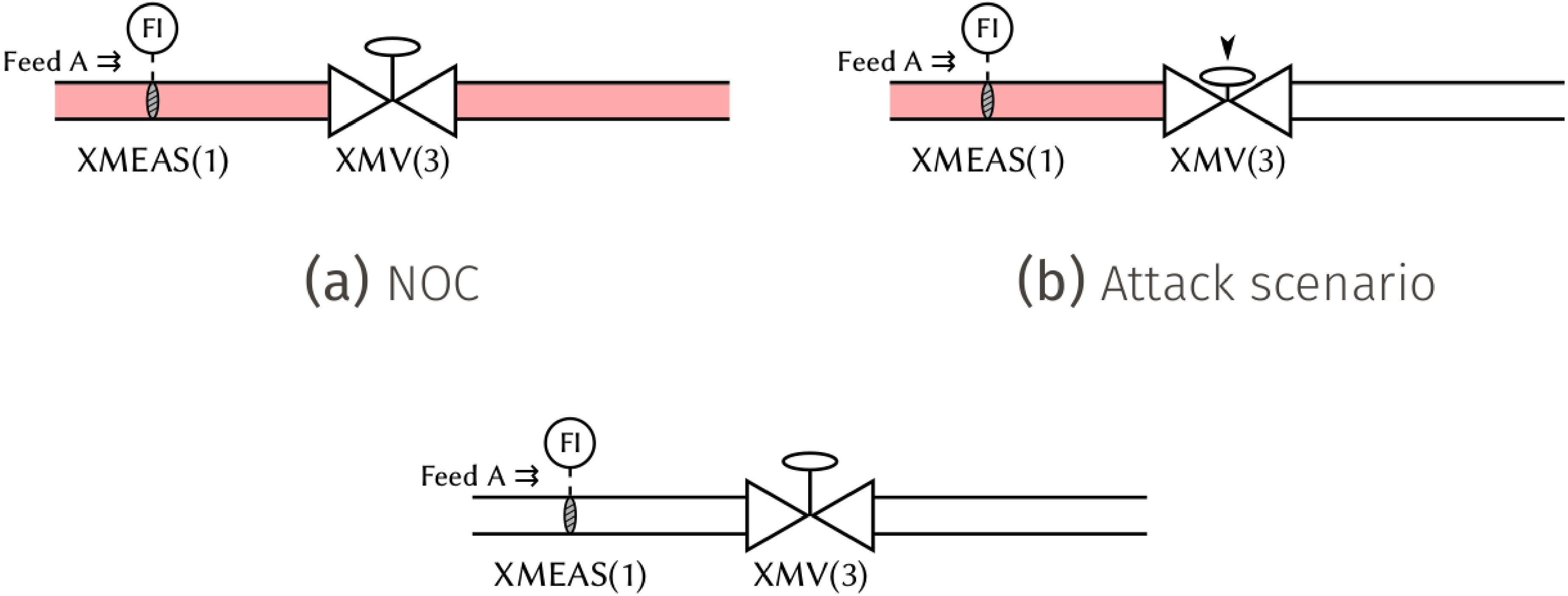
Teodora Kourti. Process analysis and abnormal situation detection: from theory to practice
Control Systems, IEEE, IEEE, 2002, 22, 10-25

Example



Mikel Iturbe, José Camacho, Iñaki Garitano, Urko Zurutuza, Roberto Uribeetxeberria. On the Feasibility of Distinguishing Between Process Disturbances and Intrusions in Process Control Systems Using Multivariate Statistical Process Control 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W), IEEE, 2016, 155-160

Example

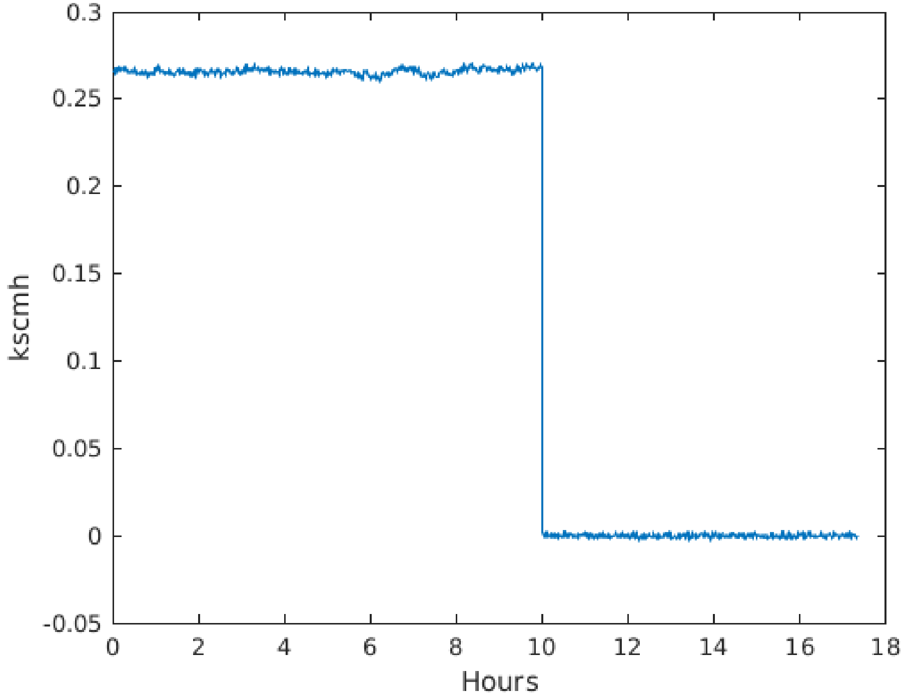


(a) NOC

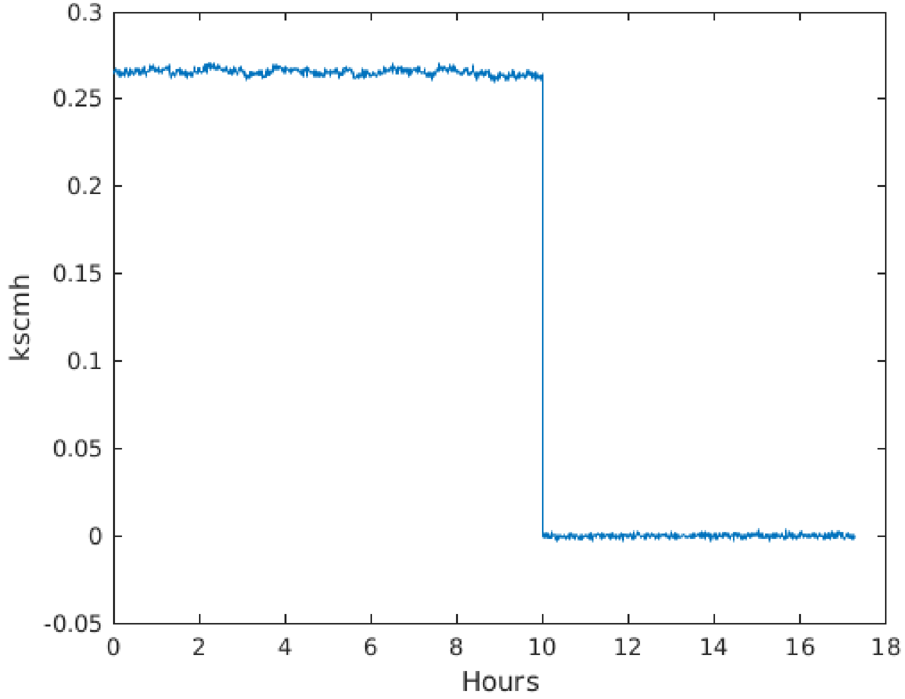
(b) Attack scenario

(c) IDV(6)

Example

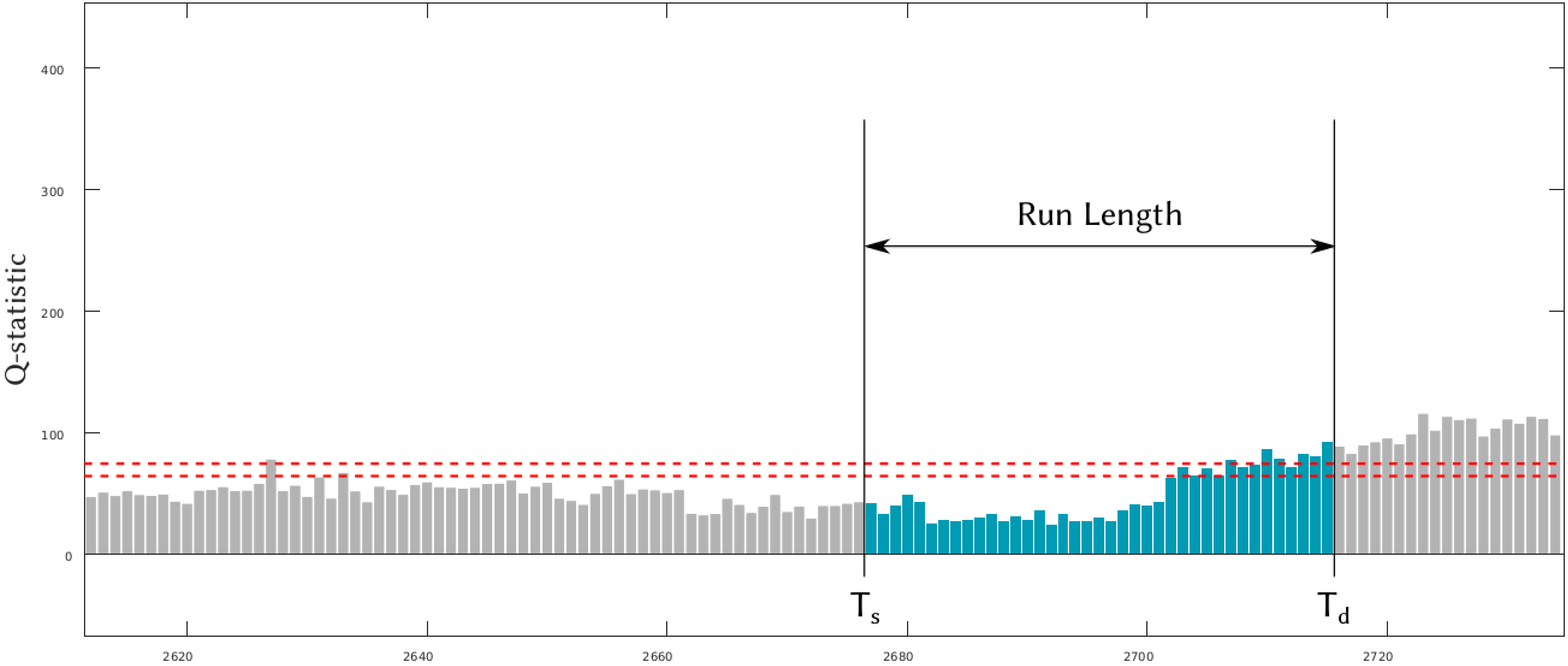


(a) IDV(6)

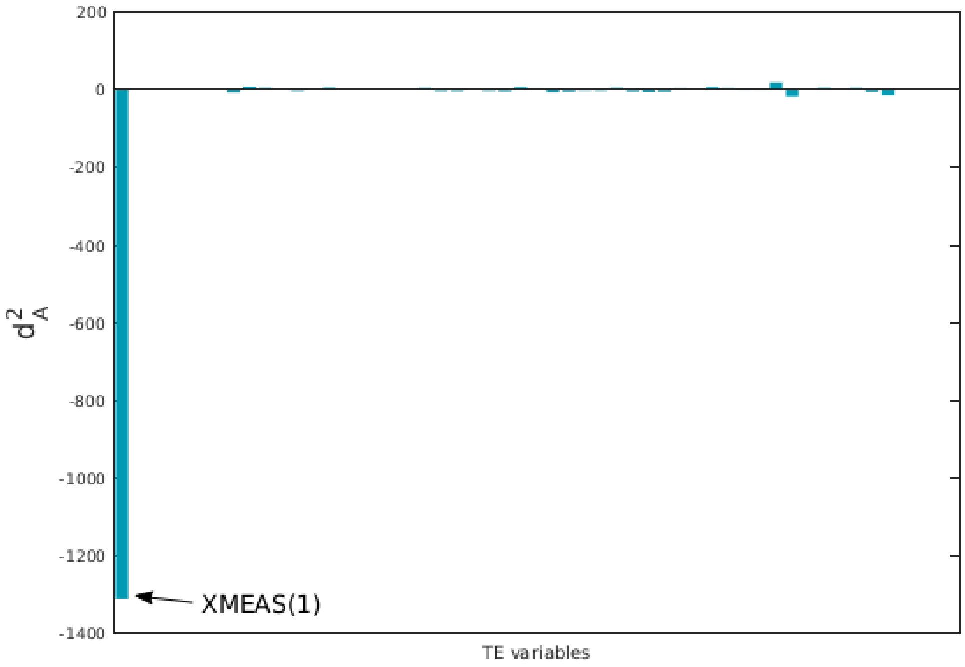


(b) Attack on XMV(3)

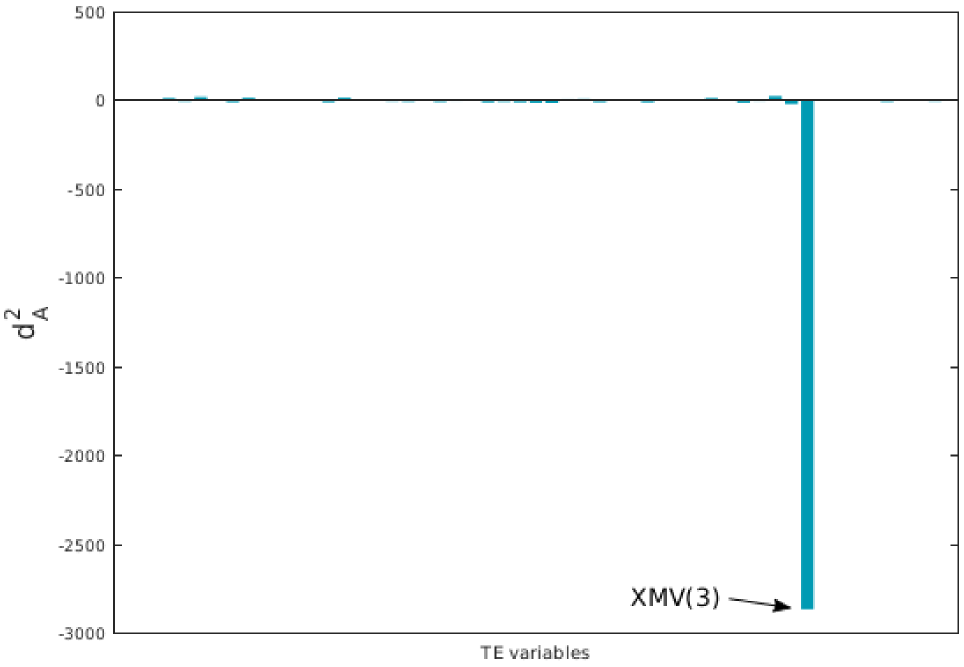
Example: Detection



Example: Diagnosis



(a) IDV(6)



(b) Int. att. on XMV(3)

Doing now

- I first wrote MSPC over Apache Spark
  - Replicating functionalities from existing Matlab toolbox
  - Yeah, you know, “Big Data”
- Rewriting it in pure Python
- Finishing a Modbus bridge for DVCP-TE

Conclusions

- ICS and IT security are different
  - Specially when exploiting systems
- Current protection approaches disregard process dynamics
  - I think this will change
- There are PoC for intrusion detection at the process level
- This field requires a multidisciplinary point of view

Still much to do!!!!!!!

- This field is still underdeveloped when compared to other sec fields
- Much to do, much to learn. Not many resources though, :-/
  - Formal training: control theory, chemical engineering, academic papers.
  - Con talks (Marina Krotofil, Jason Larsen...)

Eskerrik asko

- mikel@hamahiru.org
- miturbe@mondragon.edu
- Twitter: @azken_tximinoa
- https://iturbe.info