RSA Conference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

HT-F03

Hacking Critical Infrastructure Like You're Not a N00b

Jason Larsen

CyberSecurity Researcher

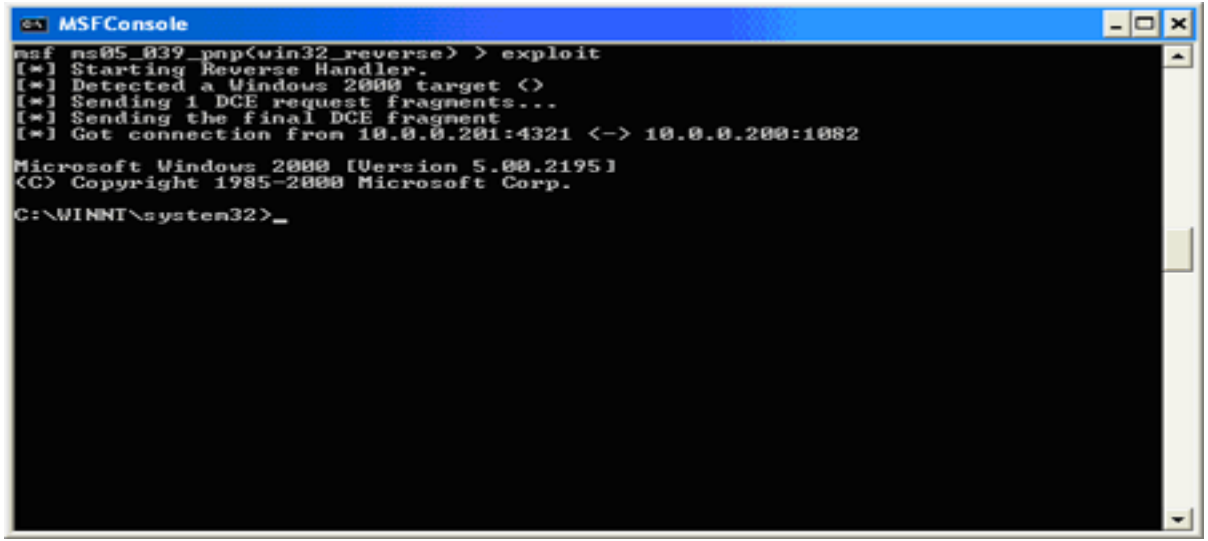
IOActive

IOActive™

COMPREHENSIVE COMPUTER SECURITY SERVICES

#RSAC

I just got a shell on the control system, now what?



Inherent Dangers

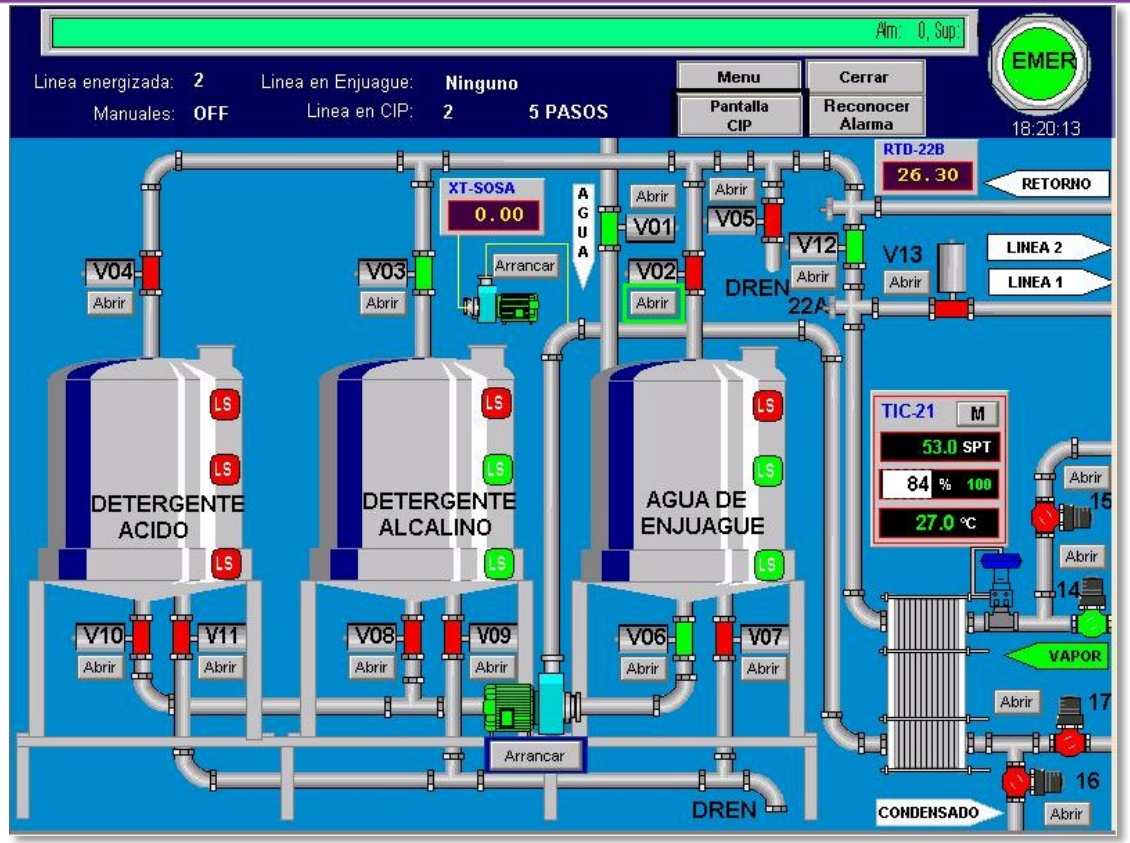
Researching Hazards

ACS
Chemistry for Life®

Hazard Mitigations

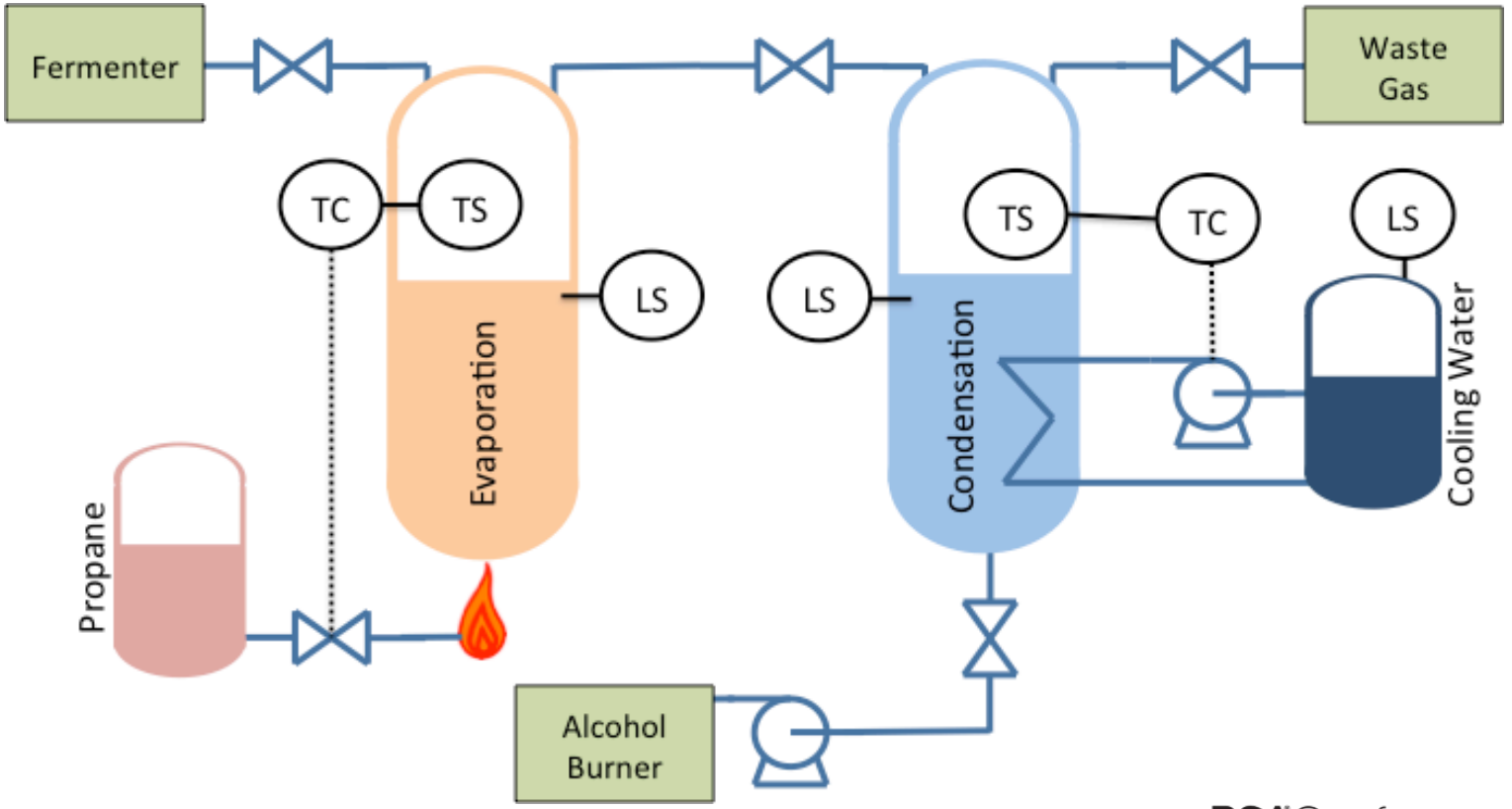
- Nearly every hazard will have some mitigation
- Just because there is a mitigation, doesn't mean that mitigation is effective
- There is always a strong pressure to declare a problem solved

Typical HMI Screen



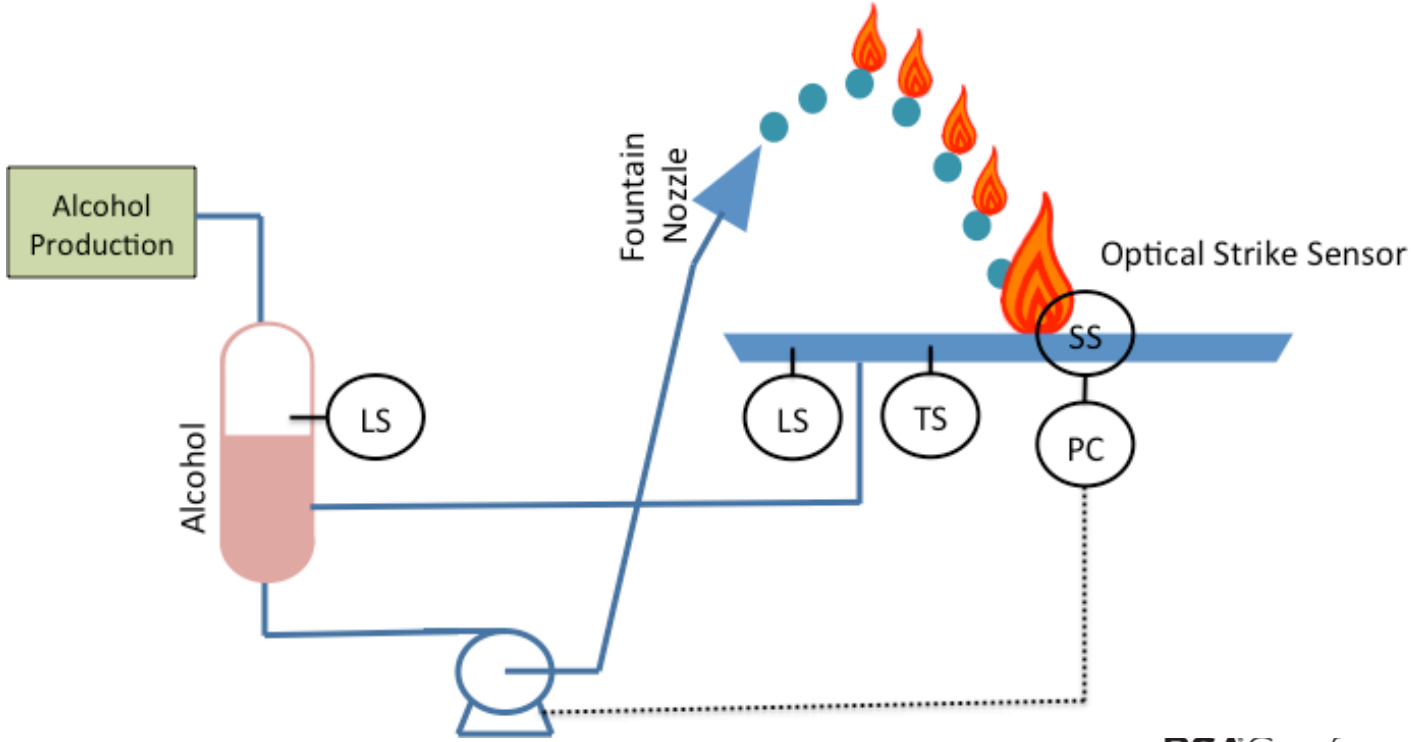
Let's Make Some Moonshine

Let's Make Some Moonshine



Let's Make Some Moonshine

Moonshine tastes awful! Burn it instead!



Easy Button Attacks

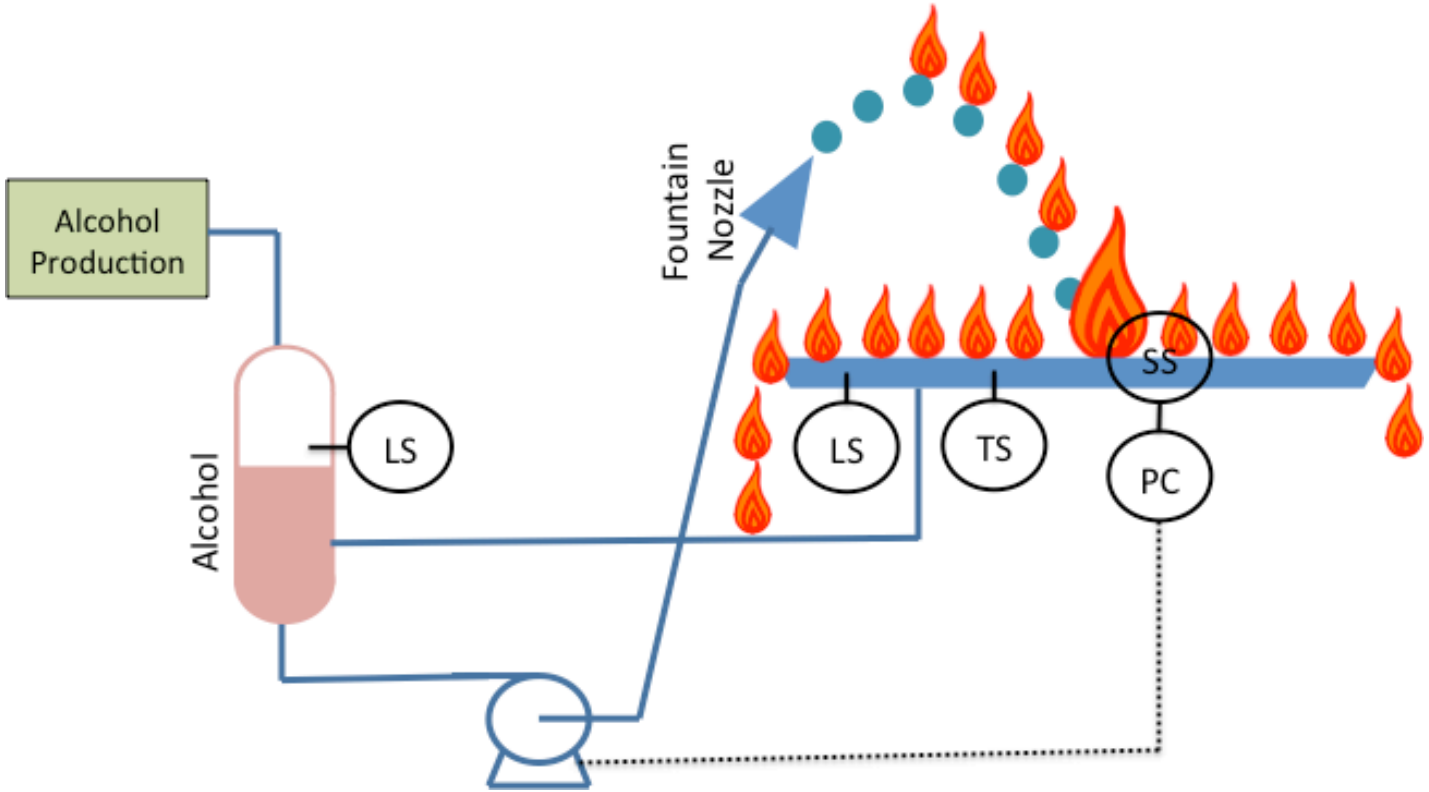
- At S4 Reid Wightman described one such attack…..
- Variable frequency drives have skip frequencies to stop the VFD from operating at a resonant frequency
  - The engineer has already calculated the exact VFD frequency that is a problem
- Easy button attacks are great if they happen to line up with what you want to achieve

What if there is no easy button?

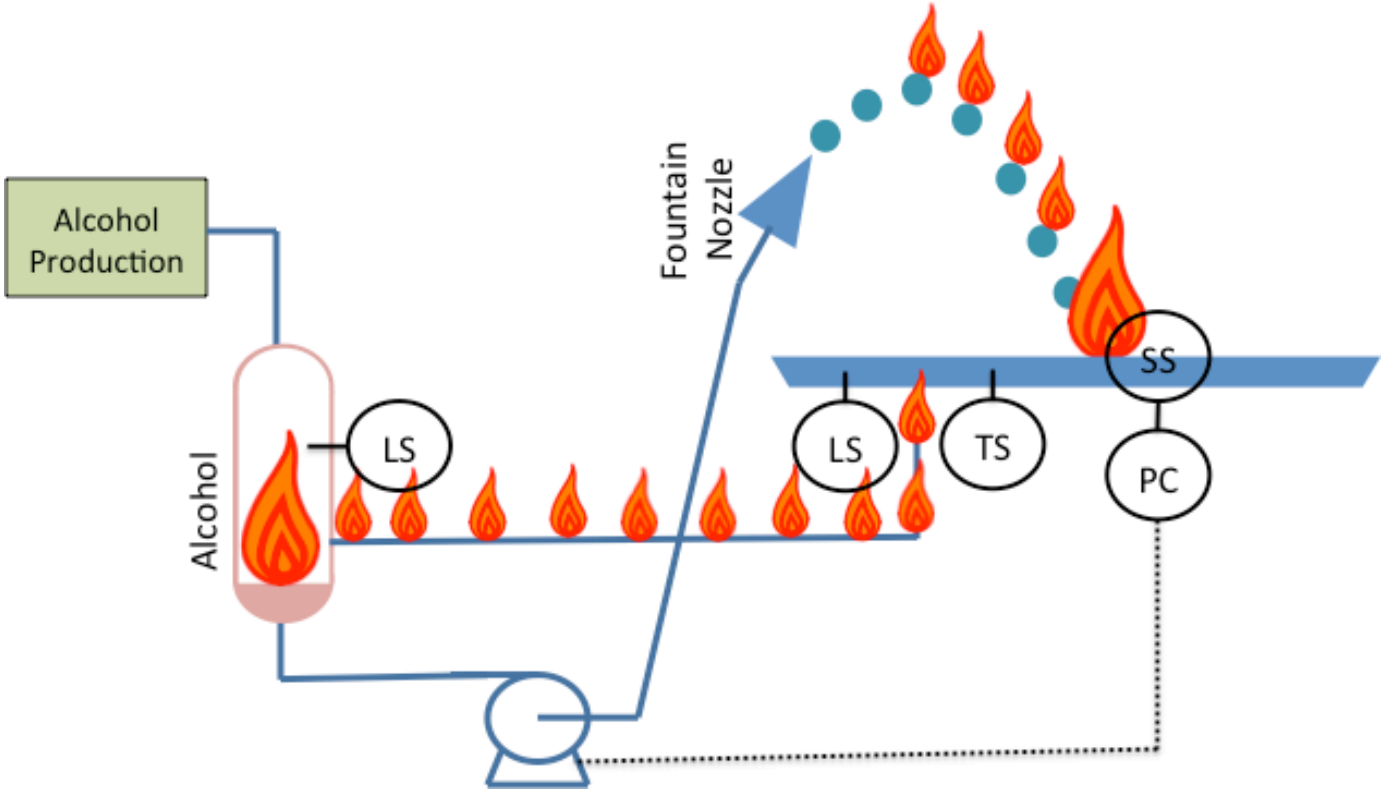
Possible Weaponization Strategies

- Flaming pool of death
- Flaming inferno of death
- Steam Collapse

Flaming Pool of Death



Flaming Inferno of Death

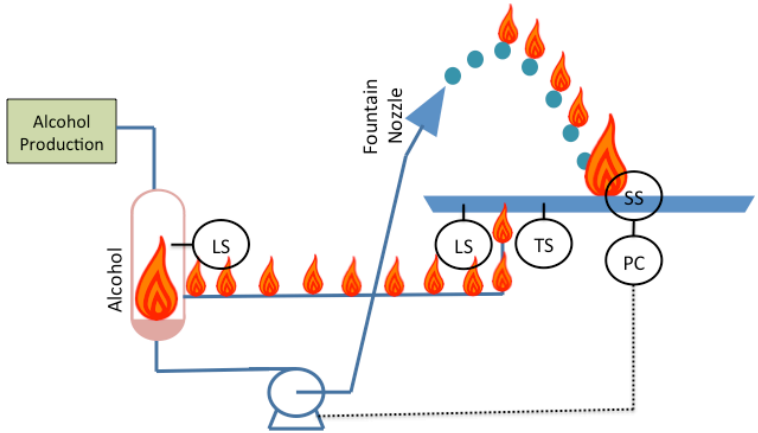


Steam Collapse

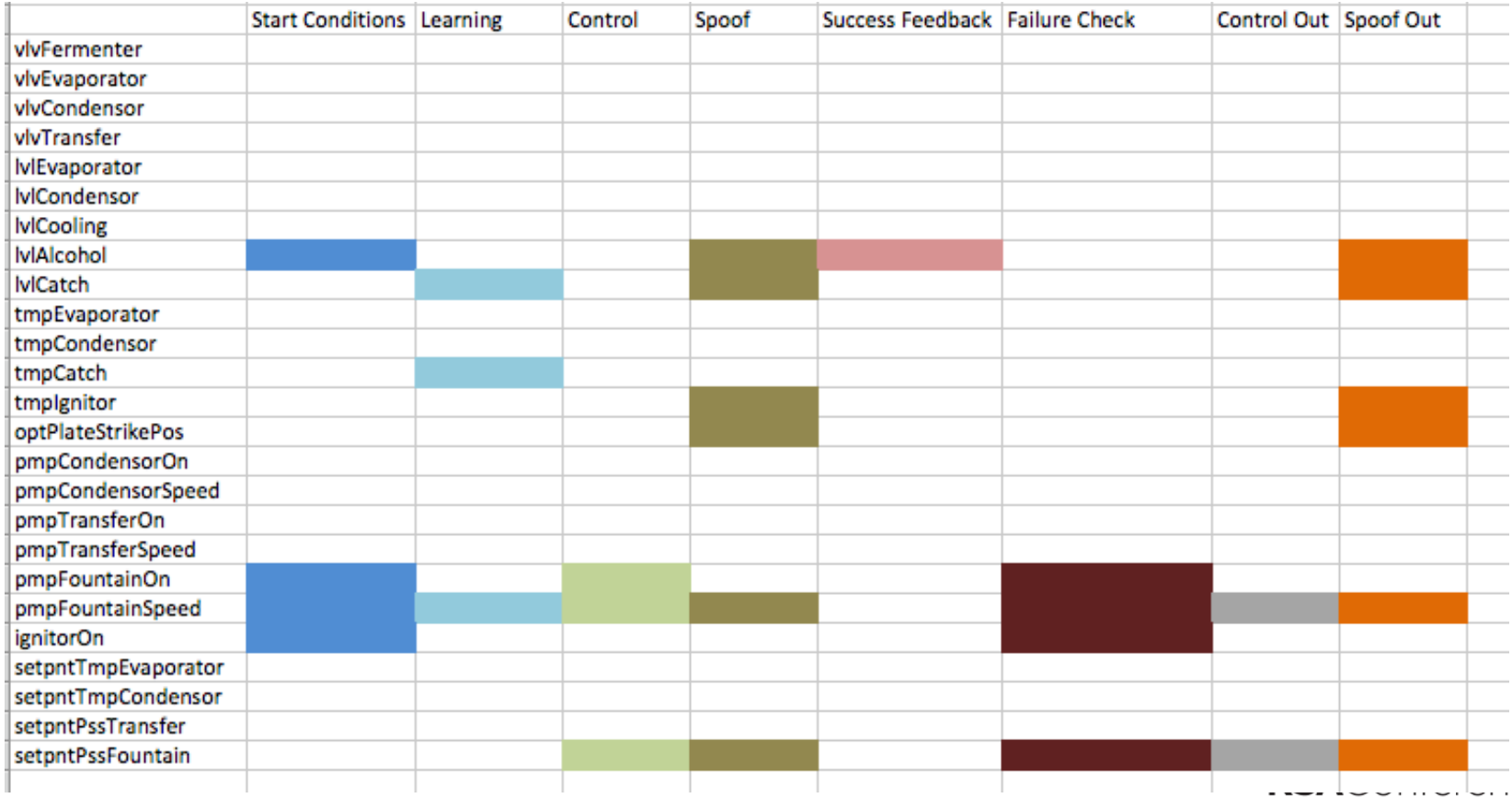
Point Database

3	
4	vlvFermenter
5	vlvEvaporator
6	vlvCondensor
7	vlvTransfer
8	lvlEvaporator
9	lvlCondensor
10	lvlCooling
11	lvlAlcohol
12	lvlCatch
13	tmpEvaporator
14	tmpCondensor
15	tmpCatch
16	optPlateStrikePos
17	pmpCondensorOn
18	pmpCondensorSpeed
19	pmpTransferOn
20	pmpTransferSpeed
21	pmpFountainOn
22	pmpFountainSpeed
23	setpntTmpEvaporator
24	setpntTmpCondensor
25	setpntPssTransfer
26	setpntPssFountain

- The attacker will need to extract the point database
- This is a toy process so it only has 22 points



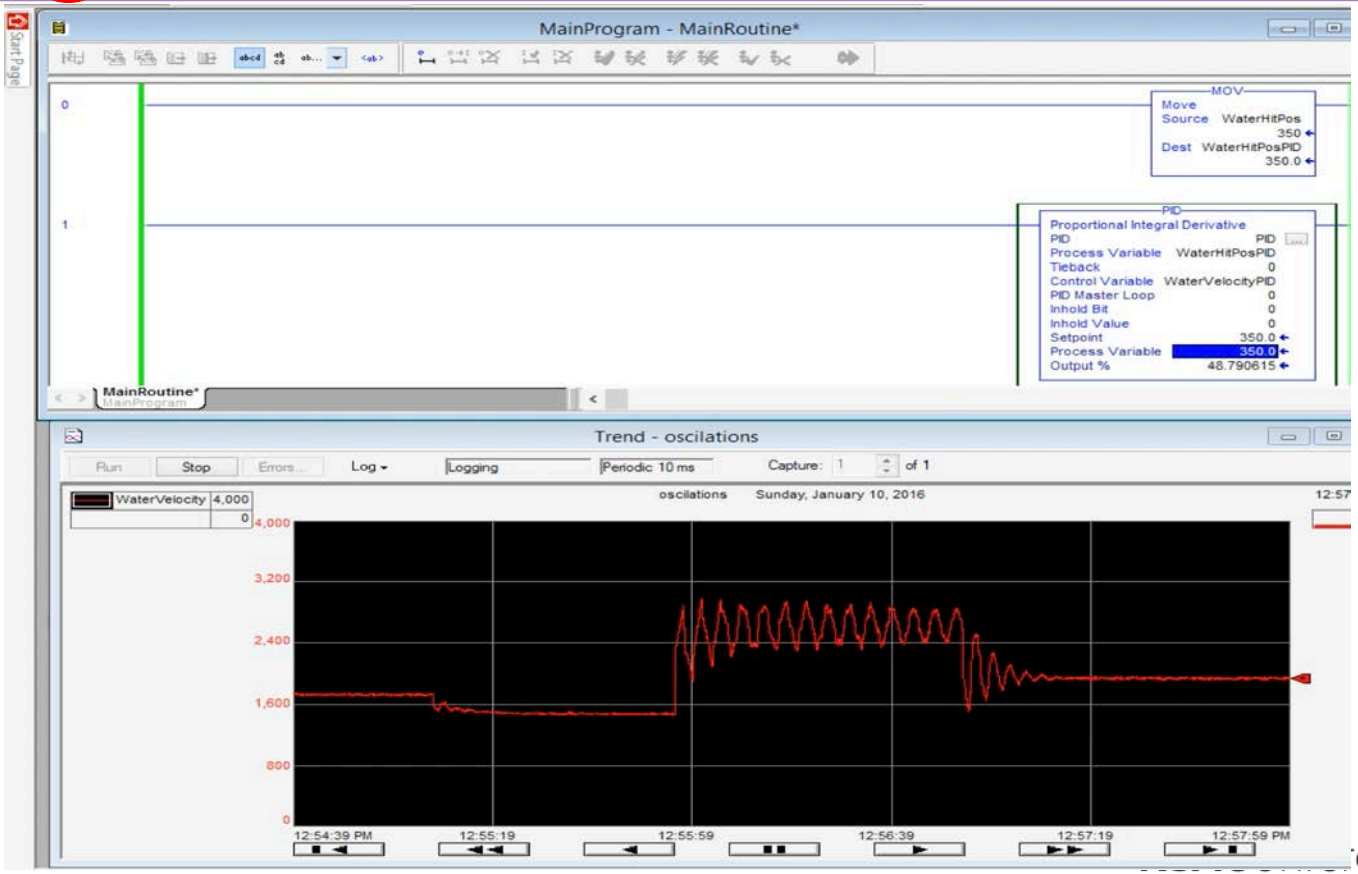
Timing And State Diagrams (TSD)

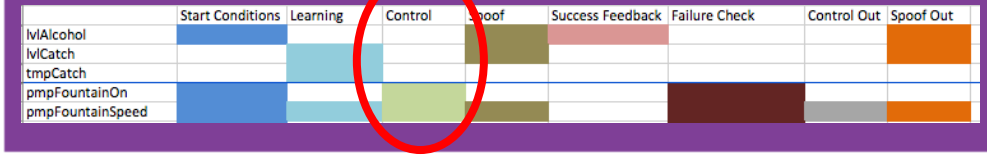


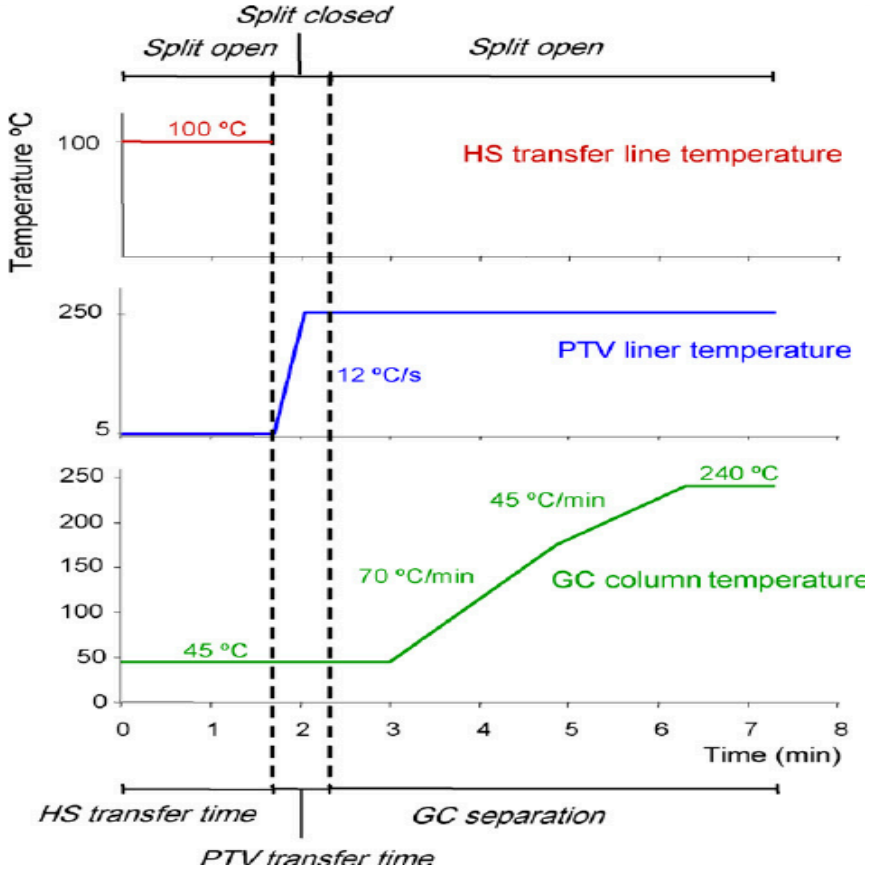
	Start Condition	Learning	Control	Spoof	Success Feedback	Failure Check	Control Out	Spoof Out
lvlAlcohol								
lvlCatch								
tmpCatch								
pmpFountainOn								
pmpFountainSpeed								

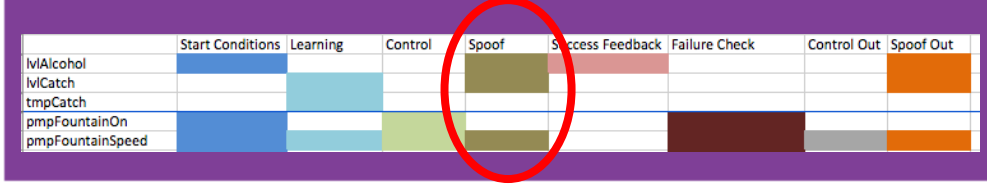
Processes aren't vulnerable all the time

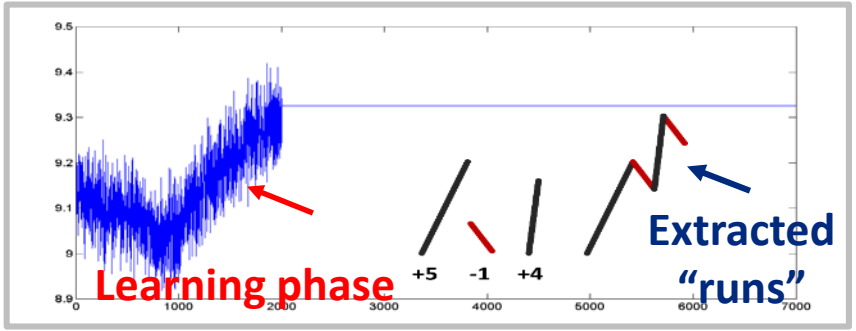
	Start Condition	Learning	Control	Spoof	Success Feedback	Failure Check	Control Out	Spoof Out
lvlAlcohol								
lvlCatch								
tmpCatch								
pmpFountainOn								
pmpFountainSpeed								

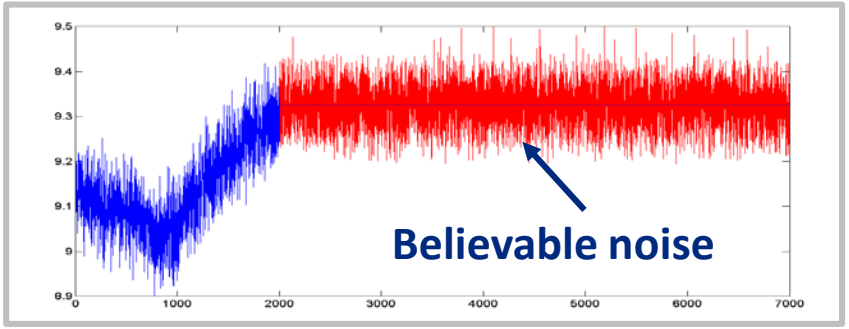


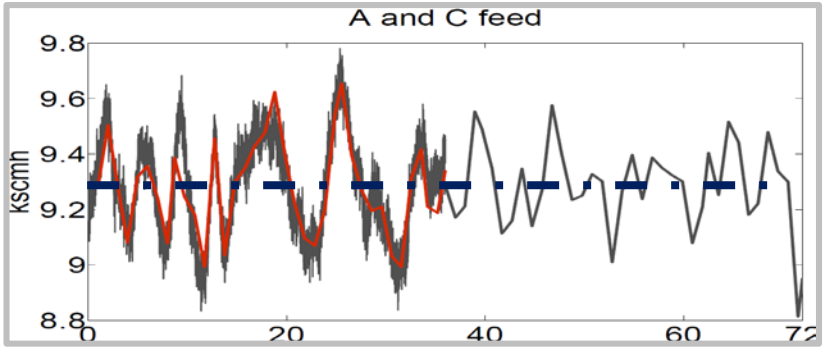

Start Conditions
Learning
Control
Spoof
Success Feedback
Failure Check
Control Out
Spoof Out
lvlAlcohol
lvlCatch
tmpCatch
pmpFountainOn
pmpFountainSpeed

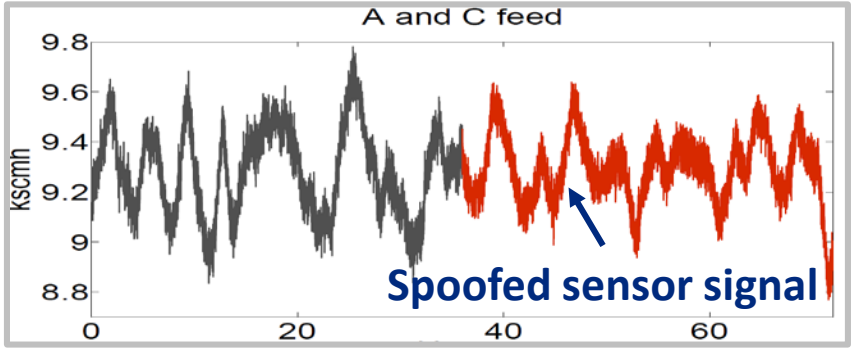

Split closed
Split open
Split open
Temperature °C
100
100 °C
HS transfer line temperature
250
5
12 °C/s
PTV liner temperature
250
200
150
100
50
0
45 °C
70 °C/min
45 °C/min
240 °C
GC column temperature
0
1
2
3
4
5
6
7
8
Time (min)
HS transfer time
GC separation
PTV transfer time


Start Conditions
Learning
Control
Spoof
Success Feedback
Failure Check
Control Out
Spoof Out
lvlAlcohol
lvlCatch
tmpCatch
pmpFountainOn
pmpFountainSpeed

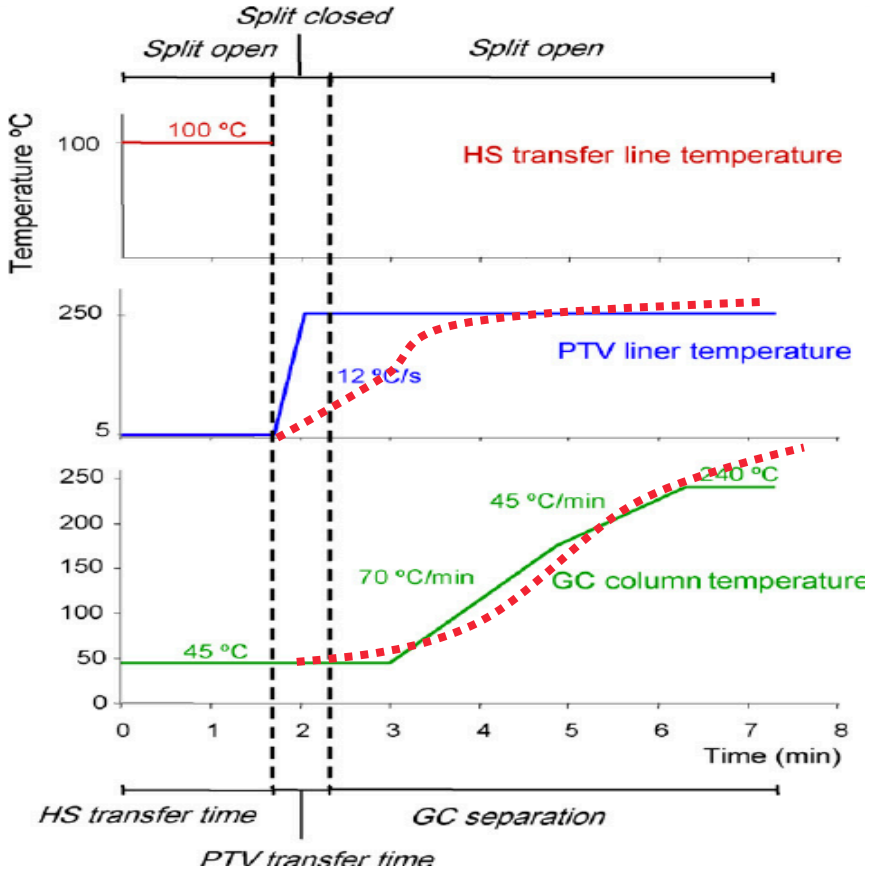

Learning phase
+5
-1
+4
Extracted
"runs"


Believable noise


A and C feed
kscmh

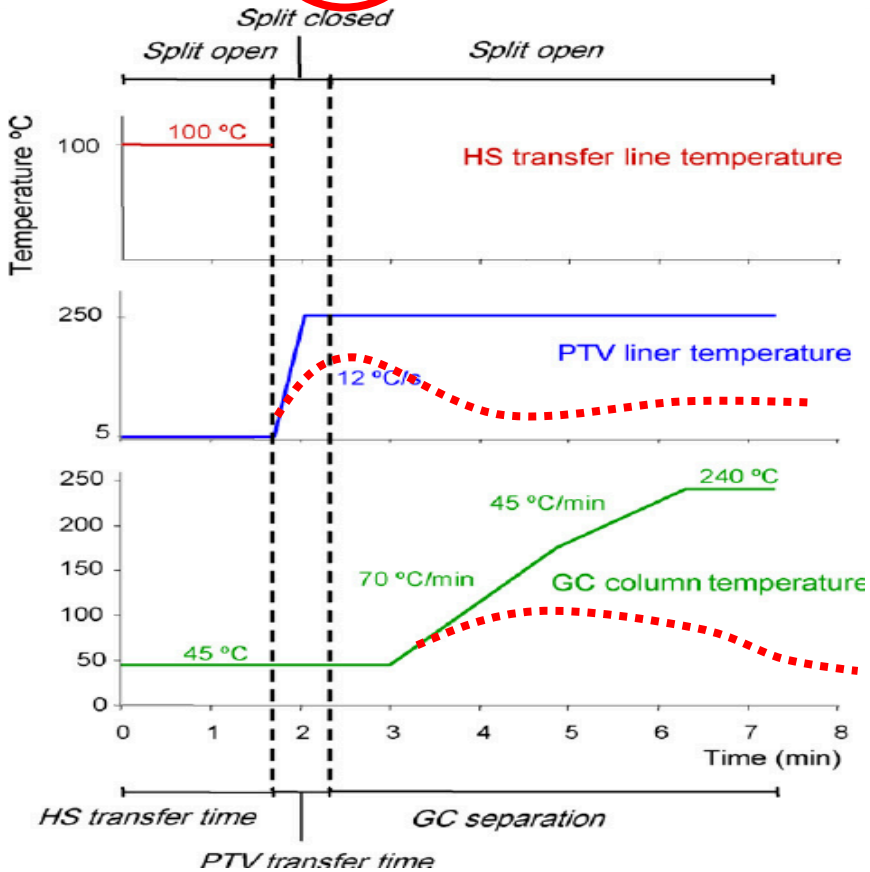

A and C feed
kscmh
Spoofed sensor signal

	Start Conditions	Learning	Control	Spoof	Success Feedbac	Failure Check	Control Out	Spoof Out
lvlAlcohol								
lvlCatch								
tmpCatch								
pmpFountainOn								
pmpFountainSpeed								



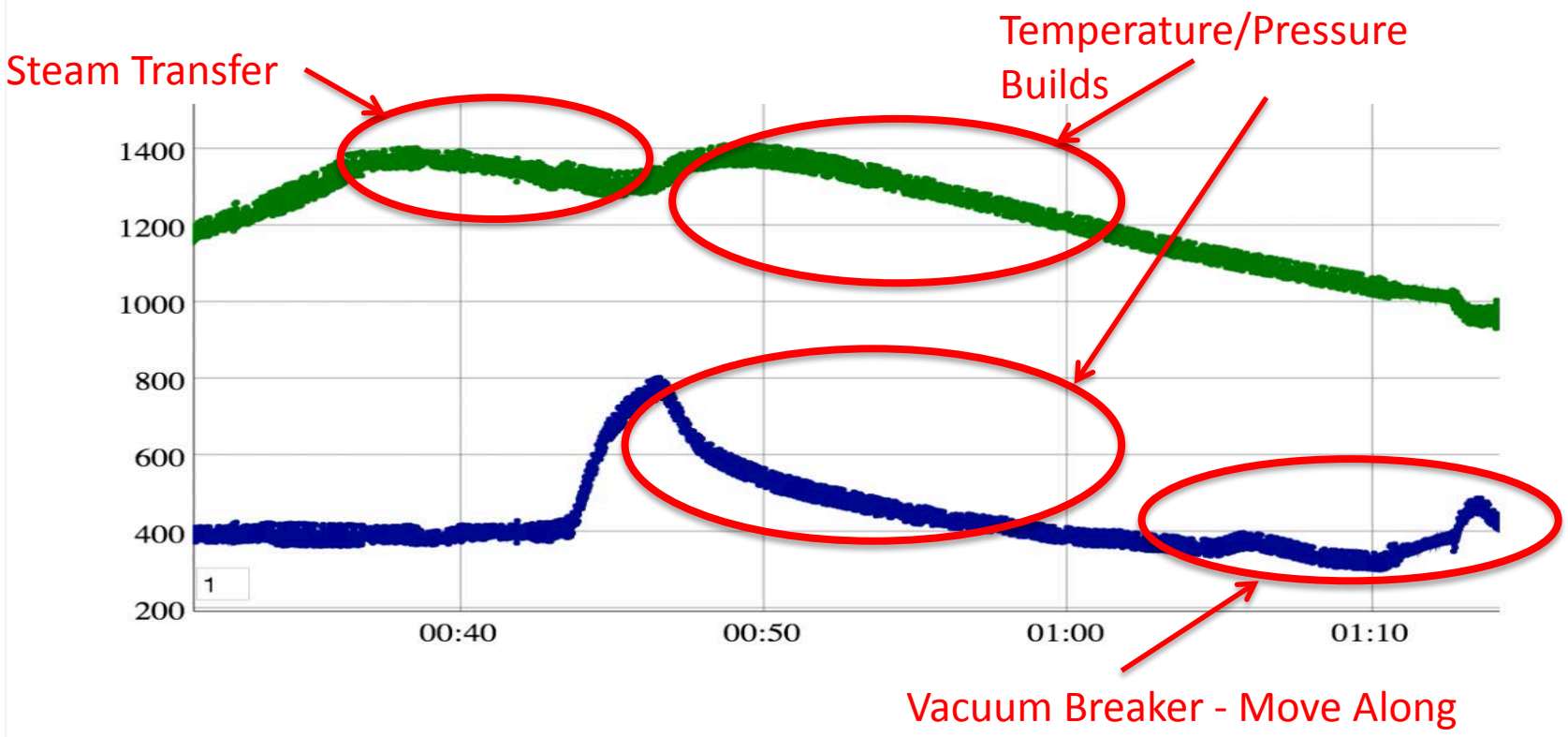
We're winning!!

	Start Conditions	Learning	Control	Spoof	Success Feedback	Failure Check	Control Out	Spoof Out
lvlAlcohol								
lvlCatch								
tmpCatch								
pmpFountainOn								
pmpFountainSpeed								

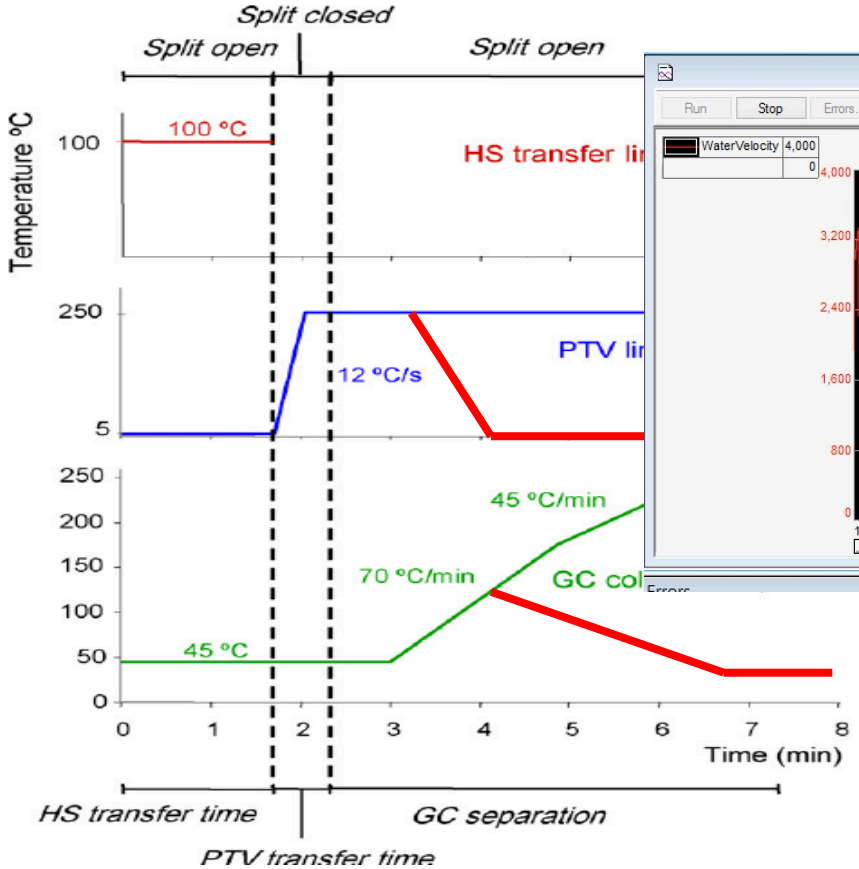


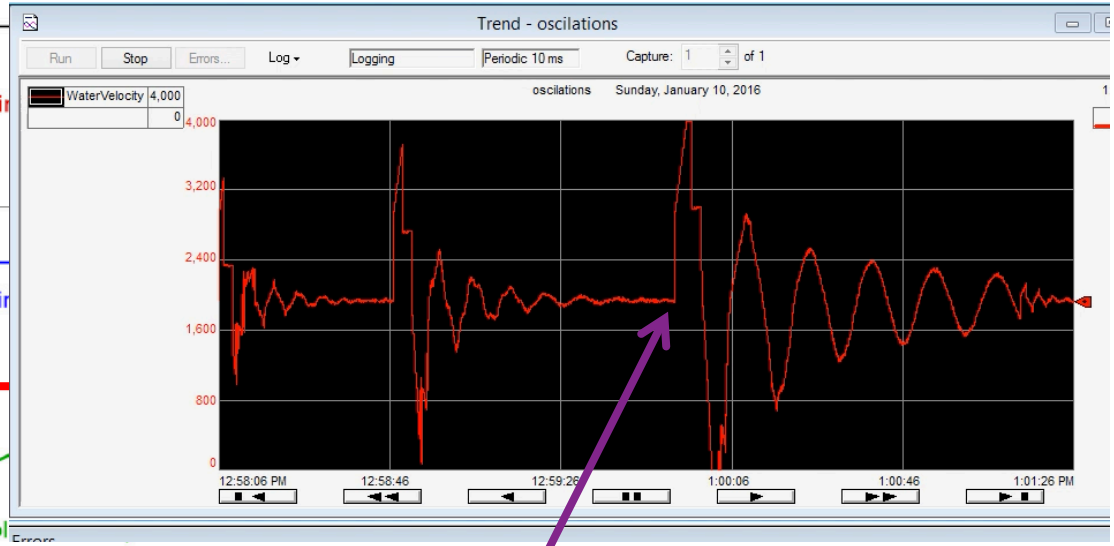
That's not right!

	Start Conditions	Learning	Control	Spoof	Success Feedback	Failure Check	Control Out	Spoof Out
lvlAlcohol								
lvlCatch								
tmpCatch								
pmpFountainOn								
pmpFountainSpeed								



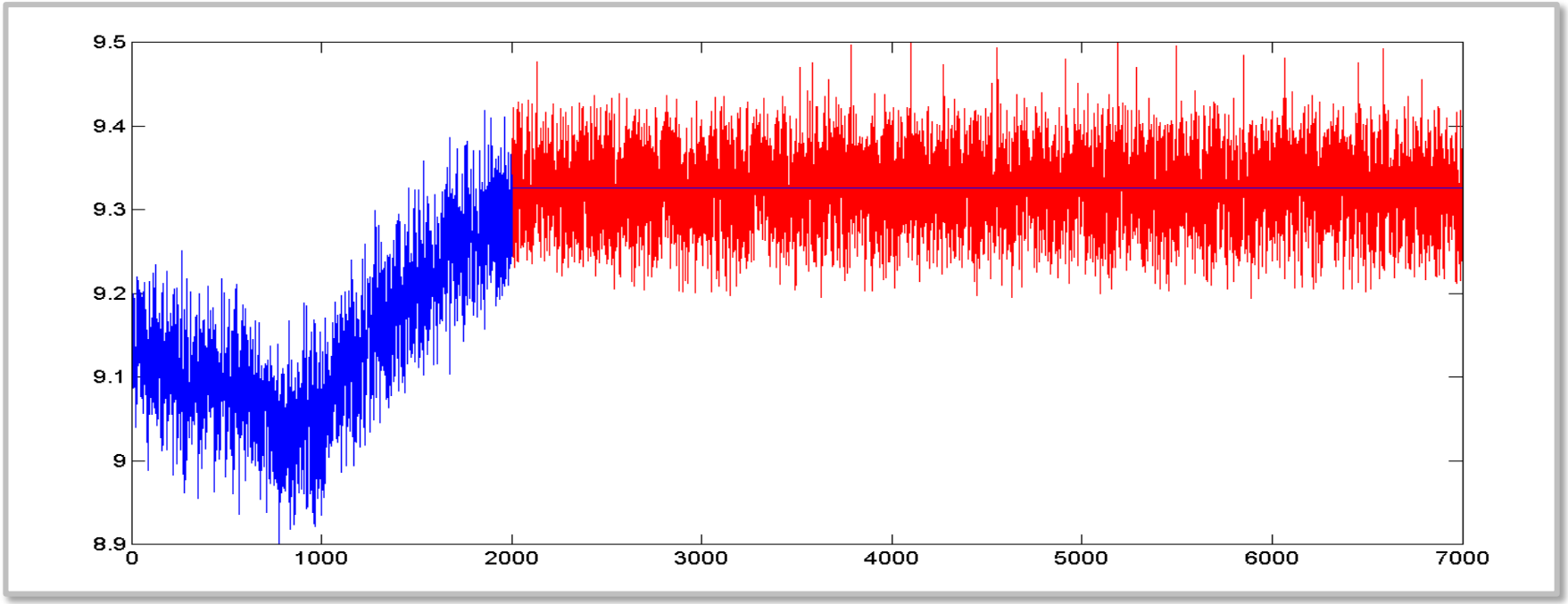
	Start Conditions	Learning	Control	Spoof	Success Feedback	Failure Check	Control Out	Spoof Out
lvlAlcohol								
lvlCatch								
tmpCatch								
pmpFountainOn								
pmpFountainSpeed								





Just letting go is like ringing a bell

	Start Conditions	Learning	Control	Spoof	Success Feedback	Failure Check	Control Out	Spoof Out
lvlAlcohol								
lvlCatch								
tmpCatch								
pmpFountainOn								
pmpFountainSpeed								



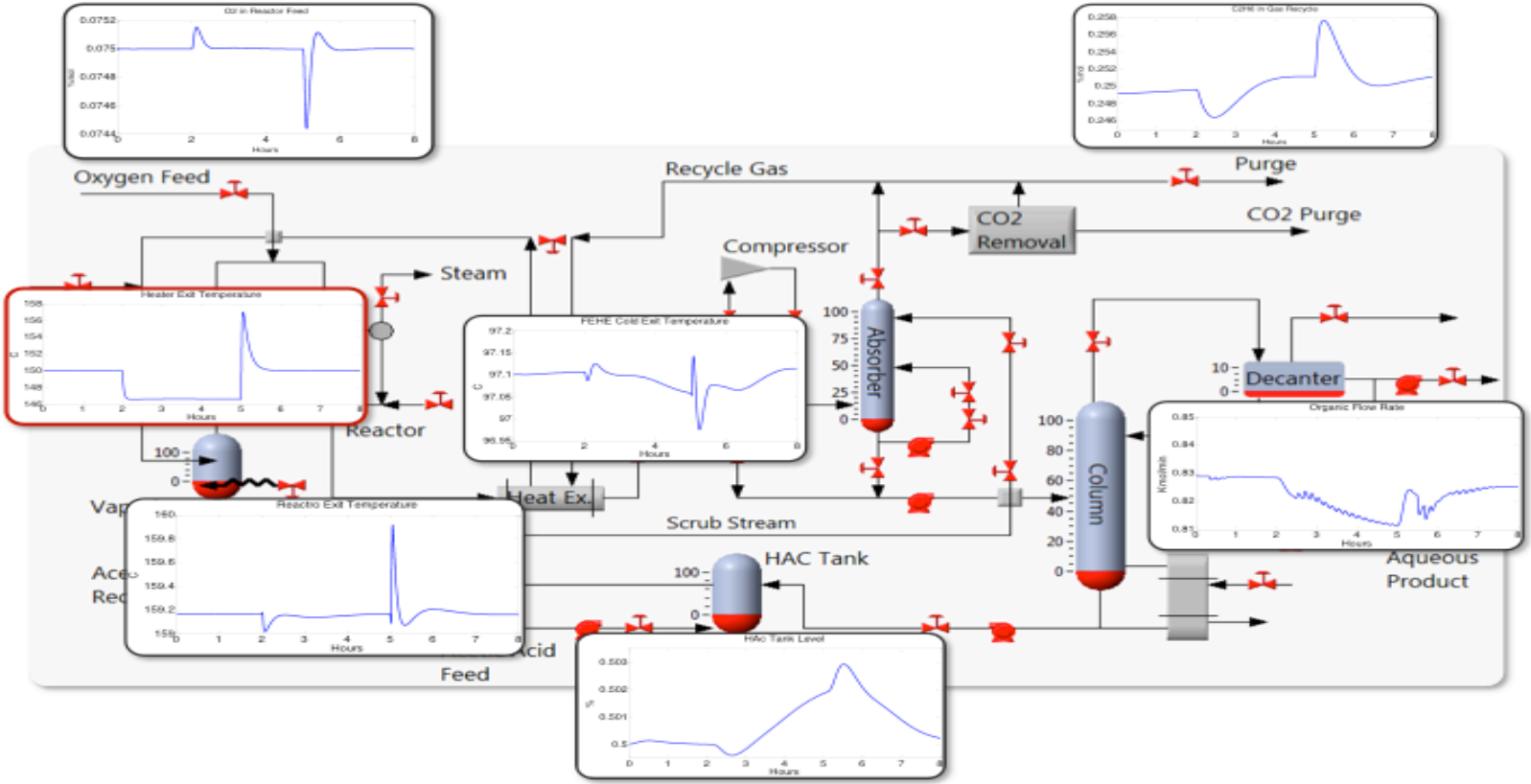
Mapping TSD to Devices

Alarm Pathways and Sanity Checks as well as Data Flows

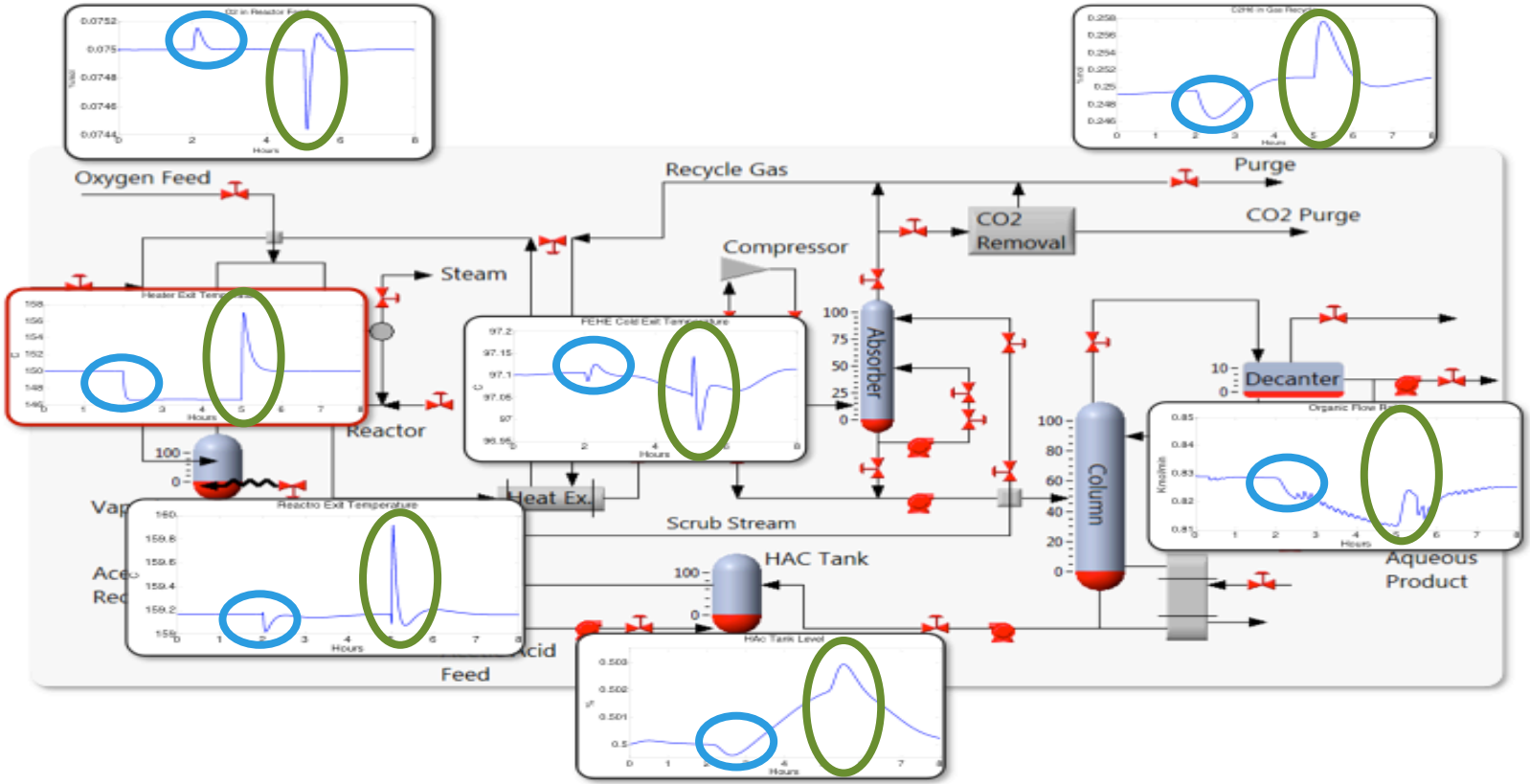
Distributed Checks

- Sending messages between devices is messy
  - The process doesn't stop to wait on your message
  - This causes lots and lots of edge cases
- Autonomous agents in each control "zone" works better
  - Each agent will need it's own independent TSD logic
- Mapping Devices to Implants

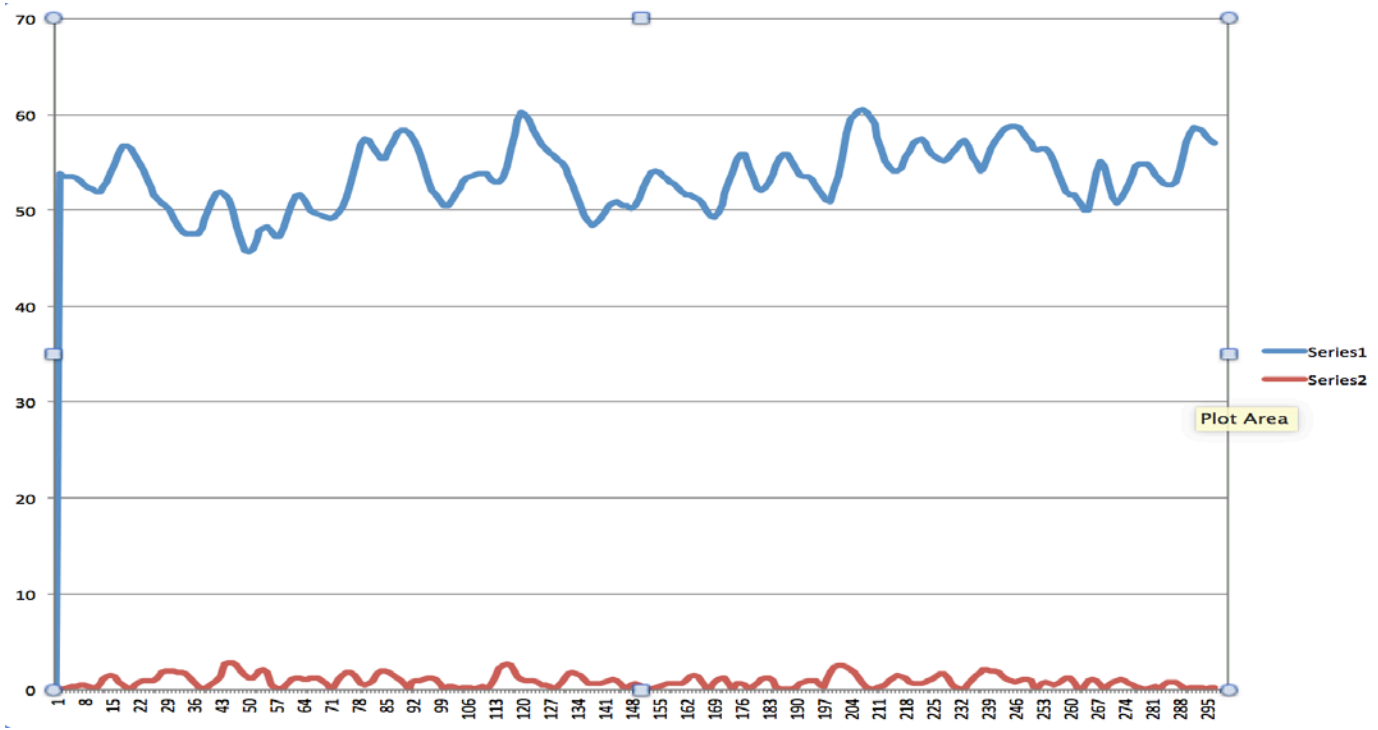
Creating and Validating TSD



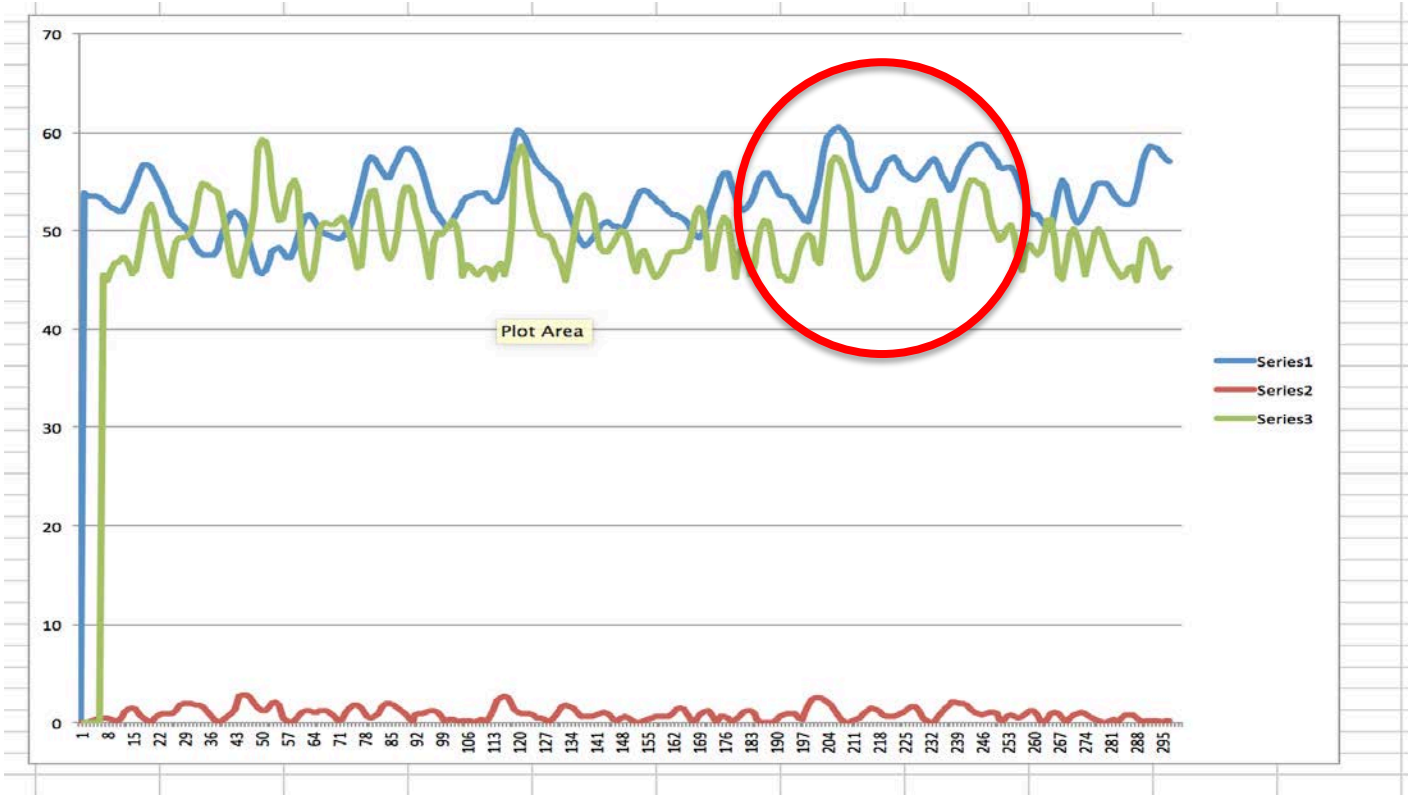
Creating and Validating TSD



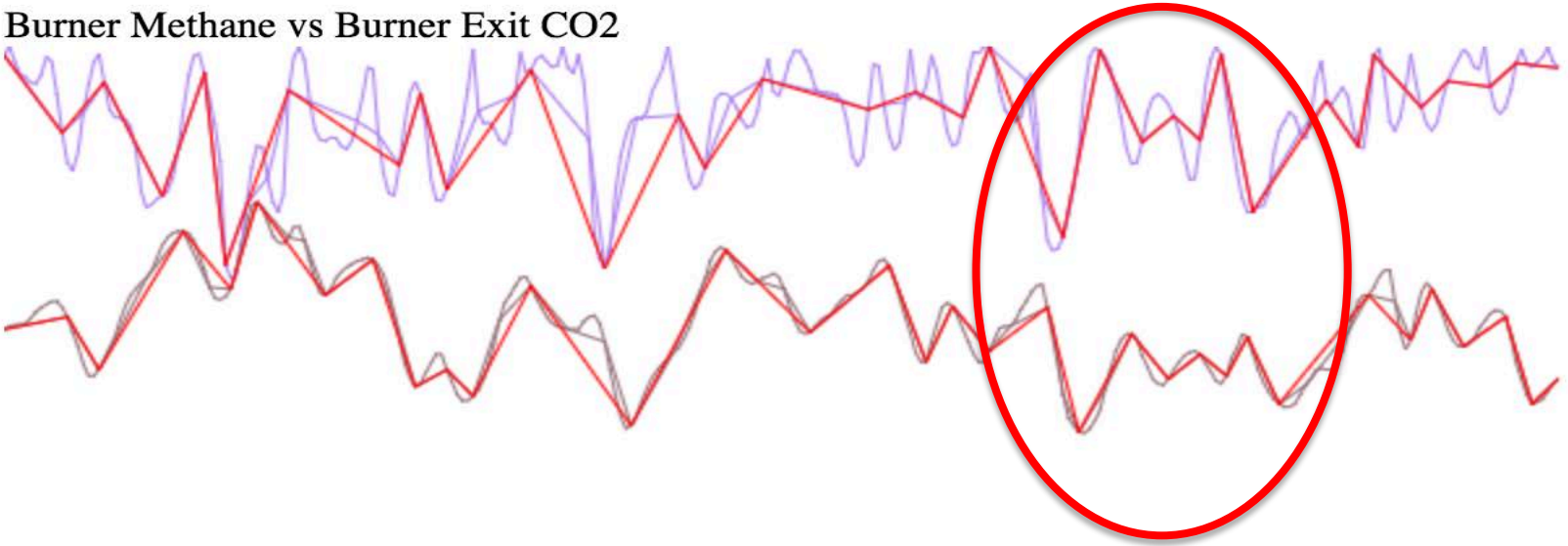
Methane vs CO_2



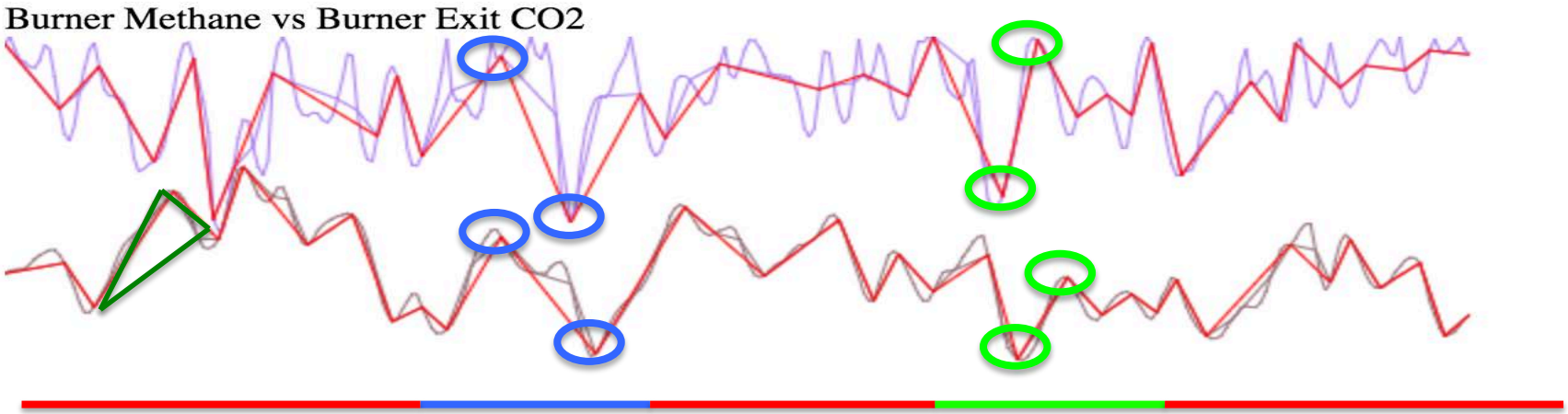
Simple Scaling



Best-Fit Monotonic Line Approximation



Force Relaxing



Relaxing a graph matches points based on artifacts just like a human would

Model Outputs

- For every pair of time series, we can calculate
  - Scale – 5.25
  - Offset - 52.64
  - Slope – 2.28
  - Delay – 9 seconds
  - Fitness – 88.06%

In general, the greater the disturbance in the loop, the better the correlation matrix will work

Let’s overlay the correlation matrix on top of our existing TSD diagram

	Start Conditions	Learning	Control	Spoof	Success Feedback	Failure Check	Control Out	Spoof Out
lvlAlcohol								
lvlCatch								
tmpCatch								
tmpIgnitor								
optPlateStrikePos								
pmpFountainOn								
pmpFountainSpeed								
ignitorOn								
setpntPssFountain								

Uncertainty Tables

	Start Conditions	Learning	Control	Spoof	Success Feedback	Failure Check	Control Out	Spoof Out
lvlAlcohol				95	95			
lvlCatch				85				
tmpCatch								
tmpIgnitor				81				
optPlateStrikePos				82				
pmpFountainOn			82					
pmpFountainSpeed			95	95		95		
ignitorOn						90		
setpntPssFountain			91	91		91		
						Total Uncertainty	1168	
						Number of Implants	2	
						Total	2336	

An exploit chain can always be built, but how confident are you it will work?

Comparing Attack Strategies

	Start Conditions	Learning	Control	Spoof	Success Feedback	Failure Check	Control Out	Spoof Out
vlvFermenter	82							
vlvEvaporator	87		86	86			82	
vlvCondensor	93						85	
vlvTransfer	84		97	92				
lvlEvaporator		85		84				87
lvlCondensor		81		86				83
lvlCooling		91		80				85
lvlAlcohol	90			97	97			80
lvlCatch		81		92				93
tmpEvaporator	96	90		89				93
tmpCondensor		86		82	82	82		80
tmpCatch		91		95	96	87		
tmpIgnitor				81				83
optPlateStrikePos				98				81
pmpCondensorOn			85	85			80	
pmpCondensorSpeed		80	85	85			85	84
pmpTransferOn			92	92				
pmpTransferSpeed			87	87				
pmpFountainOn	82		84			84		
pmpFountainSpeed	98	82	93	93		93	81	85
ignitorOn	86					92		
setpntTmpEvaporator		97	86	86				95
setpntTmpCondensor		82	96	96				91
setpntPssTransfer			86					
setpntPssFountain			89	89		89	97	85

Implants	
Implant PLC1	90
Implant PLC2	81

PoolOfDeath	7102
InfernoOfDeath	7020
SteamCollapse	13781

Feedback with Topology

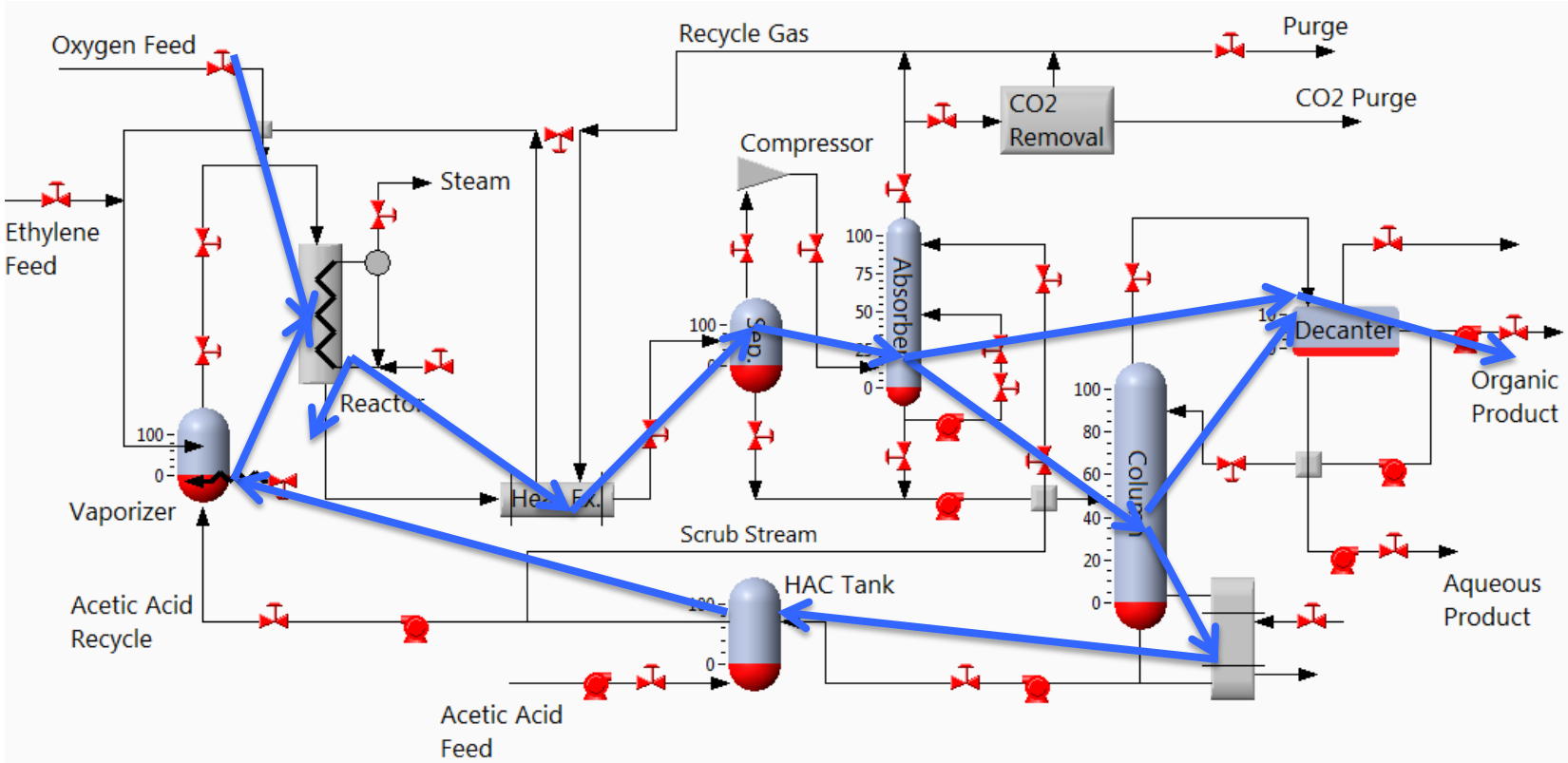
- How do you know when something has gone horribly wrong on the far side?

There is no “Pipe Roundness” sensor

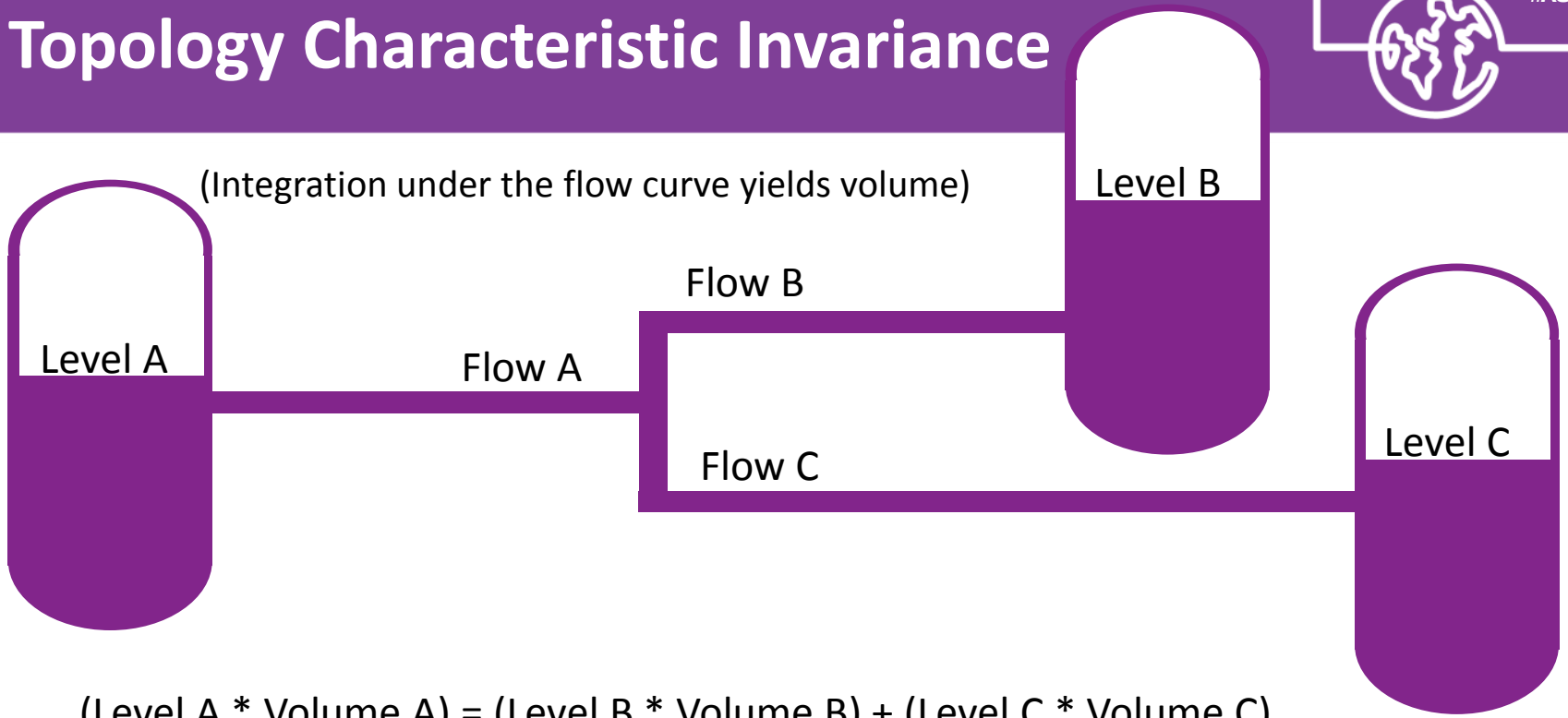
Topology Invariance

- Topologies are generally static in a process operating in the same mode
  - Individual characteristics of a topology *may* be conserved

Topology Invariance



Topology Characteristic Invariance



$$\frac{\begin{array}{l}(\text{Level A} * \text{Volume A}) = (\text{Level B} * \text{Volume B}) + (\text{Level C} * \text{Volume C}) \\ (\text{Flow A}) = (\text{Flow B}) + (\text{Flow C})\end{array}}{(\text{Level A} * \text{Volume A}) = (\text{Flow B}) + (\text{Flow C})}$$

Mostly true, but stuff happens

Change in Physics

Feedback Till Topology Changes

- Success can often be registered as a topology change
- Often some values that are conserved are no longer conserved during the damage phase

Why don’t we see more “Cyber Weapons”?

- Given the amount of work, there is also a high degree of uncertainty that the weapon will actually work
- You’re not always at war with someone so you need a kindler-gentler way of testing
- Economic disruption can be used to validate future cyber weapons against real targets
  - Expect to see an increase in economic disruptions in high-value targets

Ukraine Attack

This is more of an easy-button attack with some force multipliers

- Attackers only had to turn off the power
  - No great knowledge of the process required
- Typical DoS against the call center

Questions?

- Jason Larsen
- Jason.larsen@ioactive.com

IOActive™

COMPREHENSIVE COMPUTER SECURITY SERVICES