Physical Damage 101: Bread and Butter Attacks

Jason Larsen

Blackhat Vegas 2015

IOActive
Hardware | Software | Wetware
SECURITY SERVICES

ICS Village

- Lately I've had complaints that I only talk about chemical and haven't done a cool power talk lately
- This will be mostly chemical and manufacturing
- Power guys go to the ICS Village try to crash the east coast grid with Shaw and Culliss

"Software exploitation can be described as *unexpected computation*"

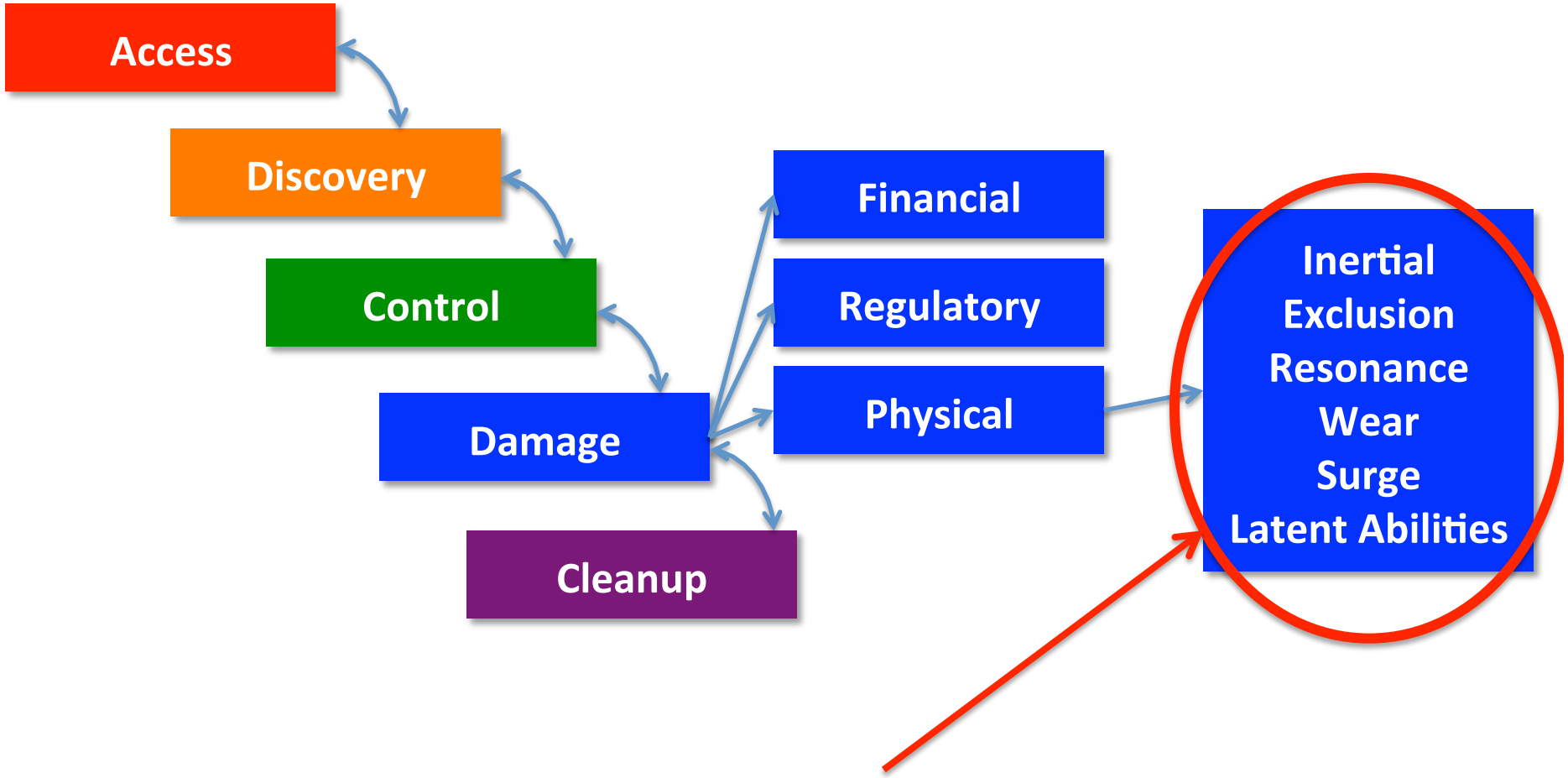
–Sergey Brattus

"CyberPhysical exploitation can be described as *unexpected physics*"

–Jason Larsen

IOActive

Stages of OT Hacking



IOActive

Parents Just Don't Understand

Me – "I have full control of the process"

Them – "OK, blow it up"

Me – "Ummmm… Give me a few weeks…"

Them – "I thought you said you had full control"

Me – "There's no big red self destruct button"

Them – "I thought you said you had full control"

Aaaaaarrrrrggggg!!!!!

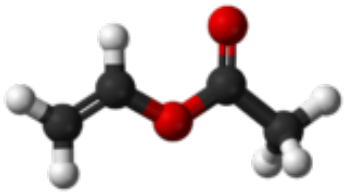
IOActive

Why Study Physical Damage

- For an attacker compromising a process is only the start of the work
  - The physics are much more challenging
- Luckily the defender mostly just gives you free reign once border defenses are defeated
  - Maybe defenders should study attack?
- Also, destroying stuff is just fun

IOActive

Process Specific Attacks

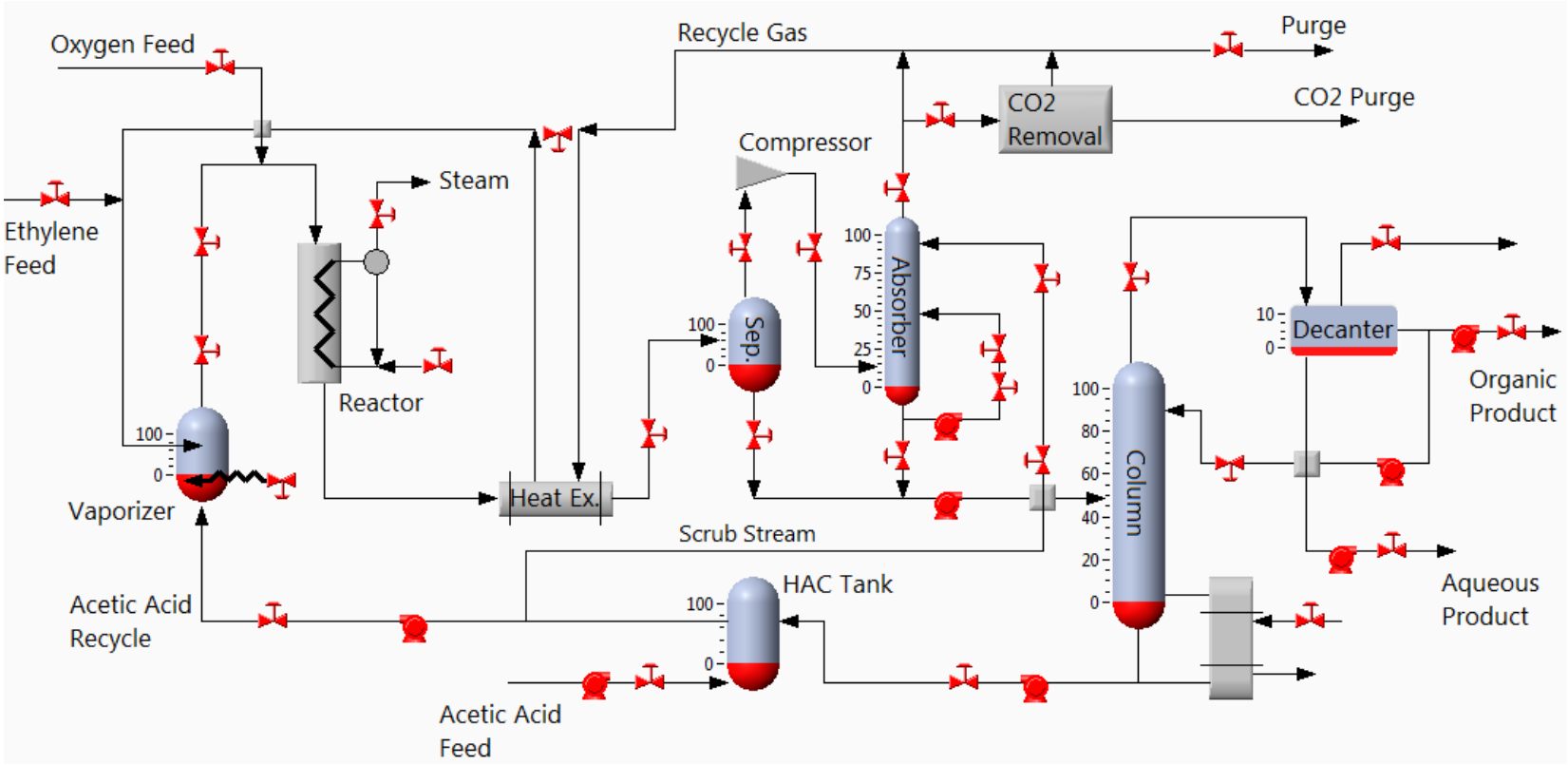


- There are more process specific attacks than there are generic ones
- Today we're going to cover as many of the generic ones as I have time

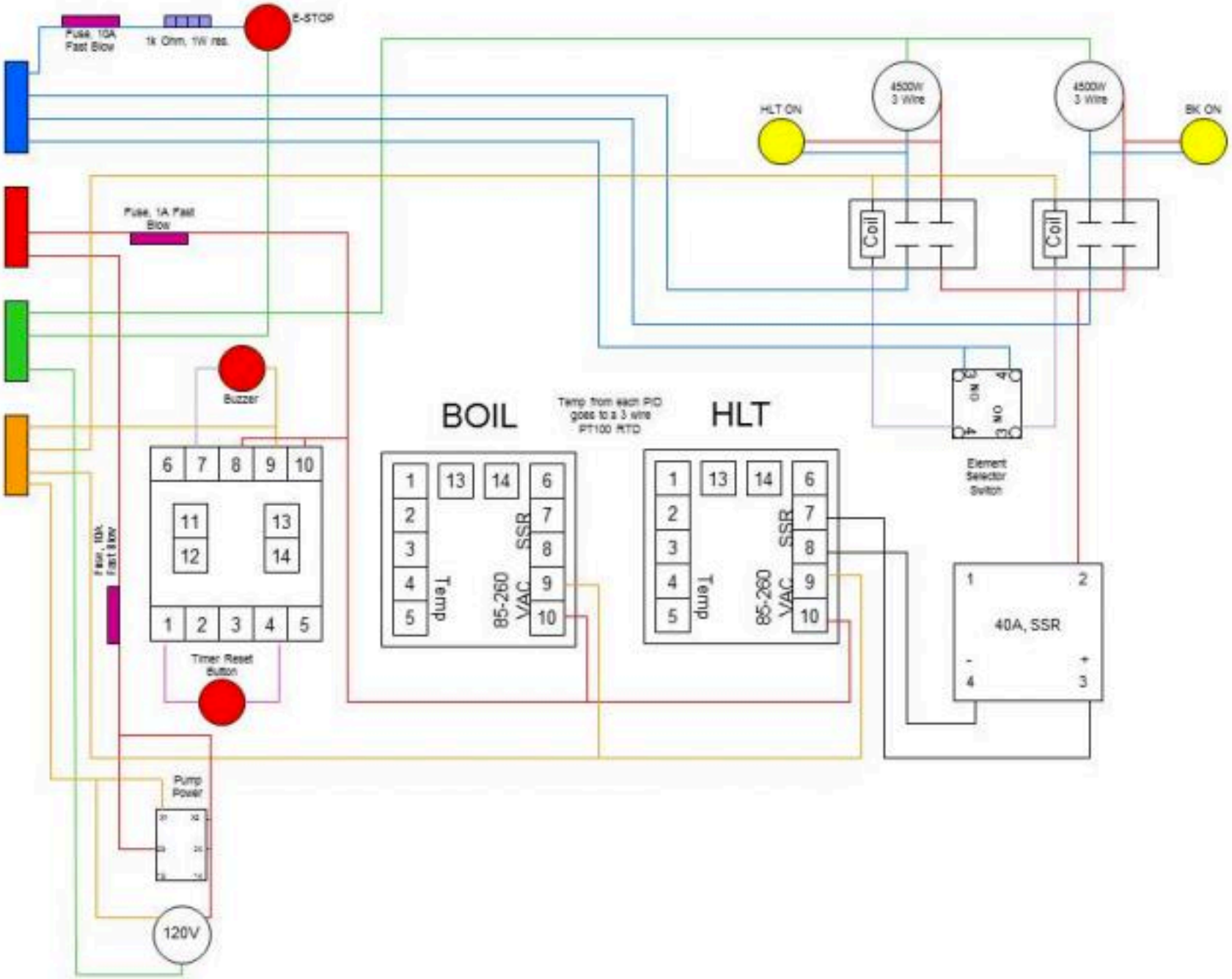
"The process constraints must be maintained …..

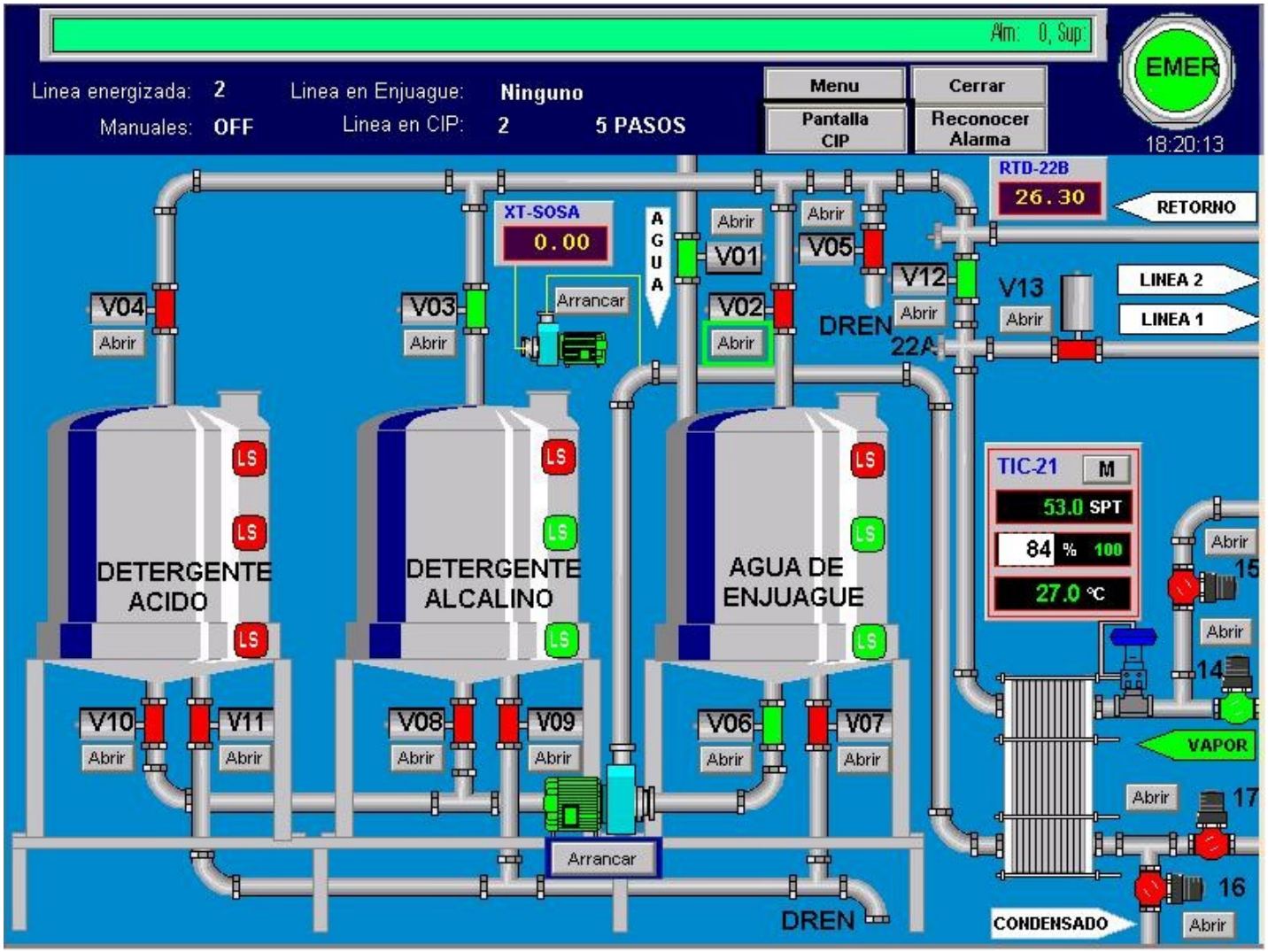
- The peak reactor temperature along the length of the tube must remain below 200◦C to prevent mechanical damage ….
- Liquid levels in the vaporizer, separator, absorber base, distillation column base, and decanter must operate within …
- Reactor inlet temperature and the hot side exit temperature form the heat exchanger must remain above 130◦C ….

IOActive


Oxygen Feed
Recycle Gas
Purge
CO2 Removal
CO2 Purge
Compressor
Steam
Ethylene Feed
Reactor
Absorber
Sep.
Decanter
Organic Product
Vaporizer
Heat Ex.
Column
Scrub Stream
HAC Tank
Acetic Acid Recycle
Aqueous Product
Acetic Acid Feed

IOActive.


E-STOP
Fuse, 10A Fast Blow
1k Ohm, 1W res.
HLT ON
4500W 3 Wire
4500W 3 Wire
BK ON
Coil
Coil
Fuse, 1A Fast Blow
Buzzer
BOIL
Temp from each PID goes to a 3 wire PT100 RTD
HLT
Element Selector Switch
6 7 8 9 10
11 12 13 14
1 2 3 4 5
Timer Reset Button
Fuse, 10A Fast Blow
1 13 14 6 7 8 9 10
2 3 4 5
Temp
85-260 VAC
SSR
40A, SSR
1 2
- +
4 3
Pump Power
120V



Consider this…….

IOActive

Starting Demo

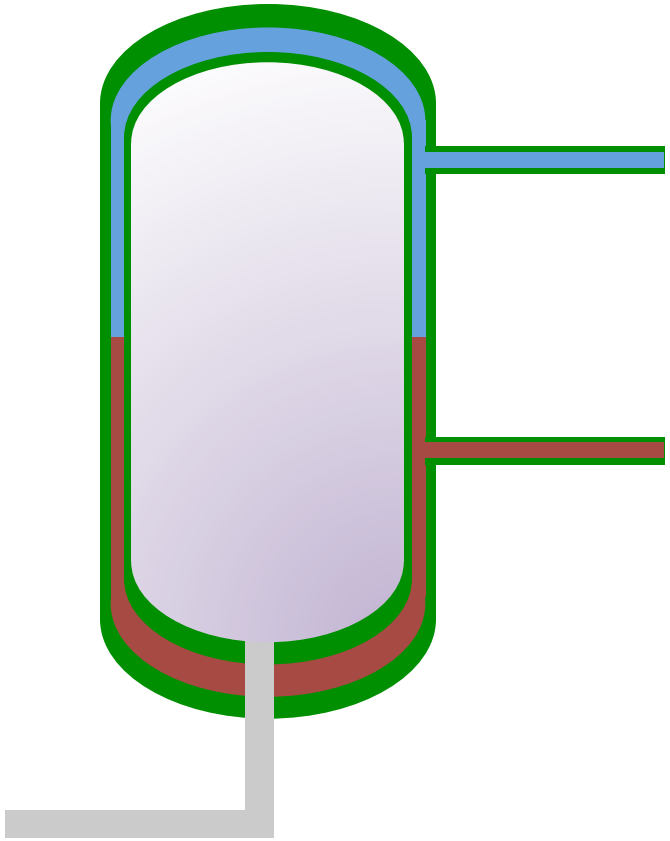
Screen shot of final HMI

When the reaction happens in that other place

Place Shifting Chemical Reactions

The chemical reaction is supposed to take place in here

IOActive



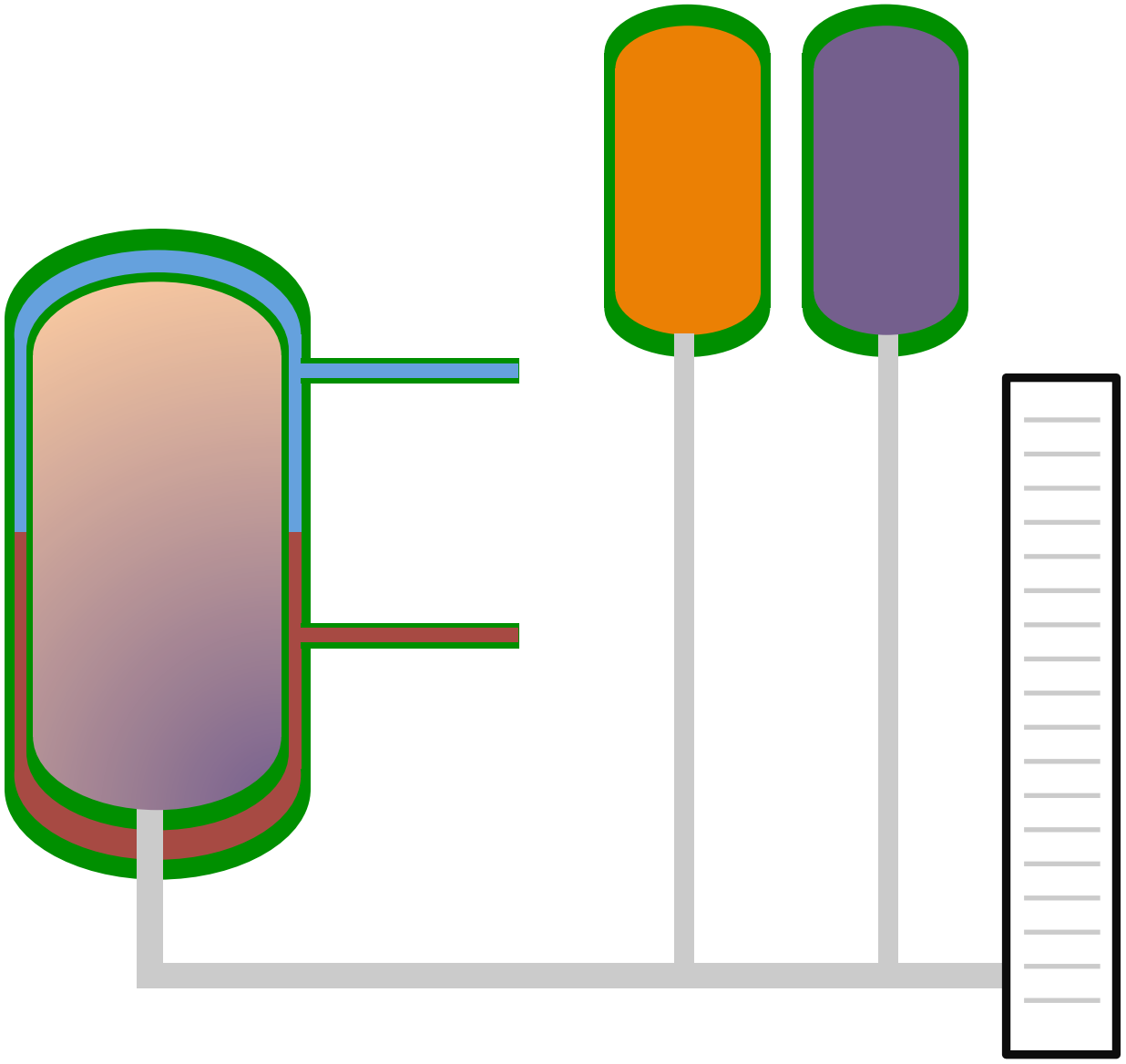
Pressure Relief Valve

Burst Disc

Catch Basin

ASME Rating

IOActive



Where and when is almost complete under cyber control

IOActive

Place Shifting Chemical Reactions

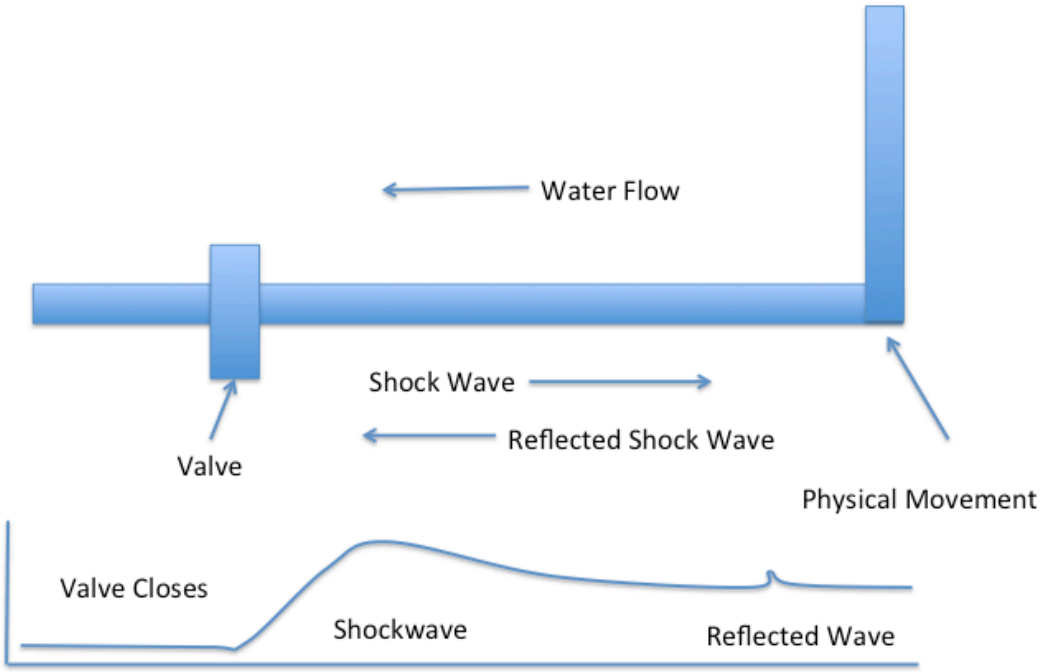
- The problem is the heat
  - Most reactions have an activation temperature
  - The attacker has to find a way to heat the reactants in some other part of the plant

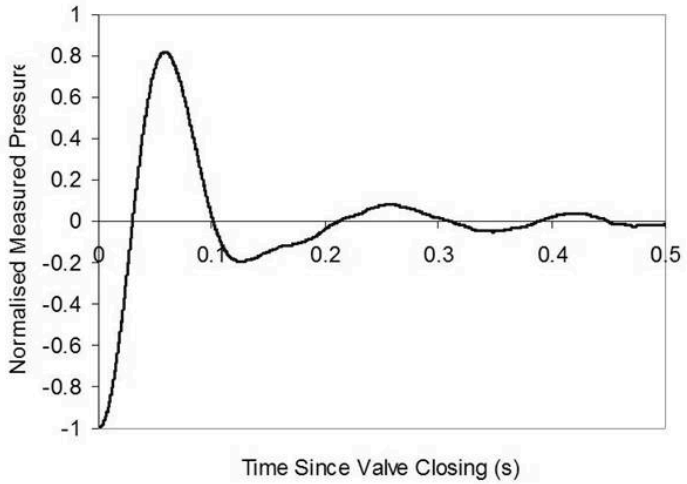
When water doesn’t stop suddenly

IOActive™

Pressure Transients

- Pressure transients are the basis for most attacks on piping infrastructure

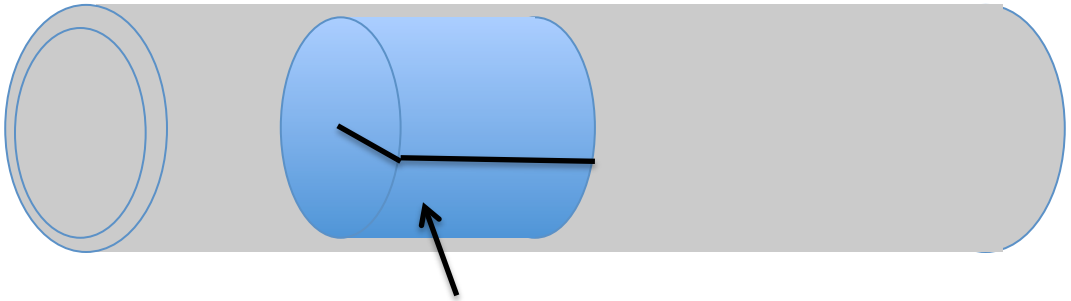




IOActive

Water Hammer

- When liquid in a pipe suddenly comes to a stop, the energy has to go somewhere
- The energy involved increases exponentially with pipe size



$PI*r^{2}*h$

4 inch pipe 60 feet long = xxx pounds
12 inch pipe 60 feet long = xxx pounds

IOActive

Water Hammer

- Whether the hammer forms depends solely on the speed of the valve closing
- Large industrial valves often have electronic controls for valve speed and profile
- The speed of the transient is equal to the speed of sound in the liquid
  - Roughly the speed of a bullet for water

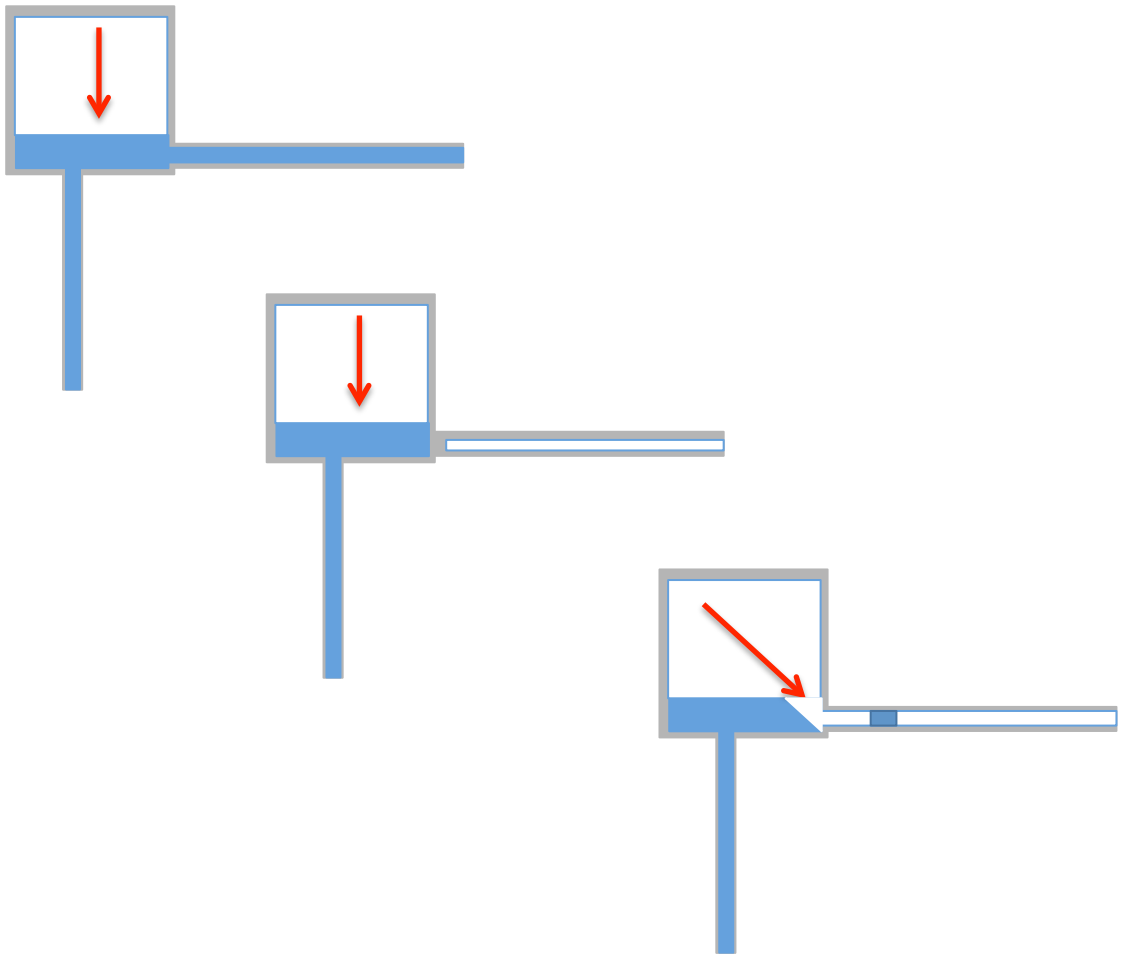
Column Separation

- If the stop is energetic enough, water can be turned into steam on the surface of the valve
- This steam pressure pushes back on the water
- An instant later, the steam turns back into water creating a vacuum
- This creates a huge pressure transient

Water Hammer Heating

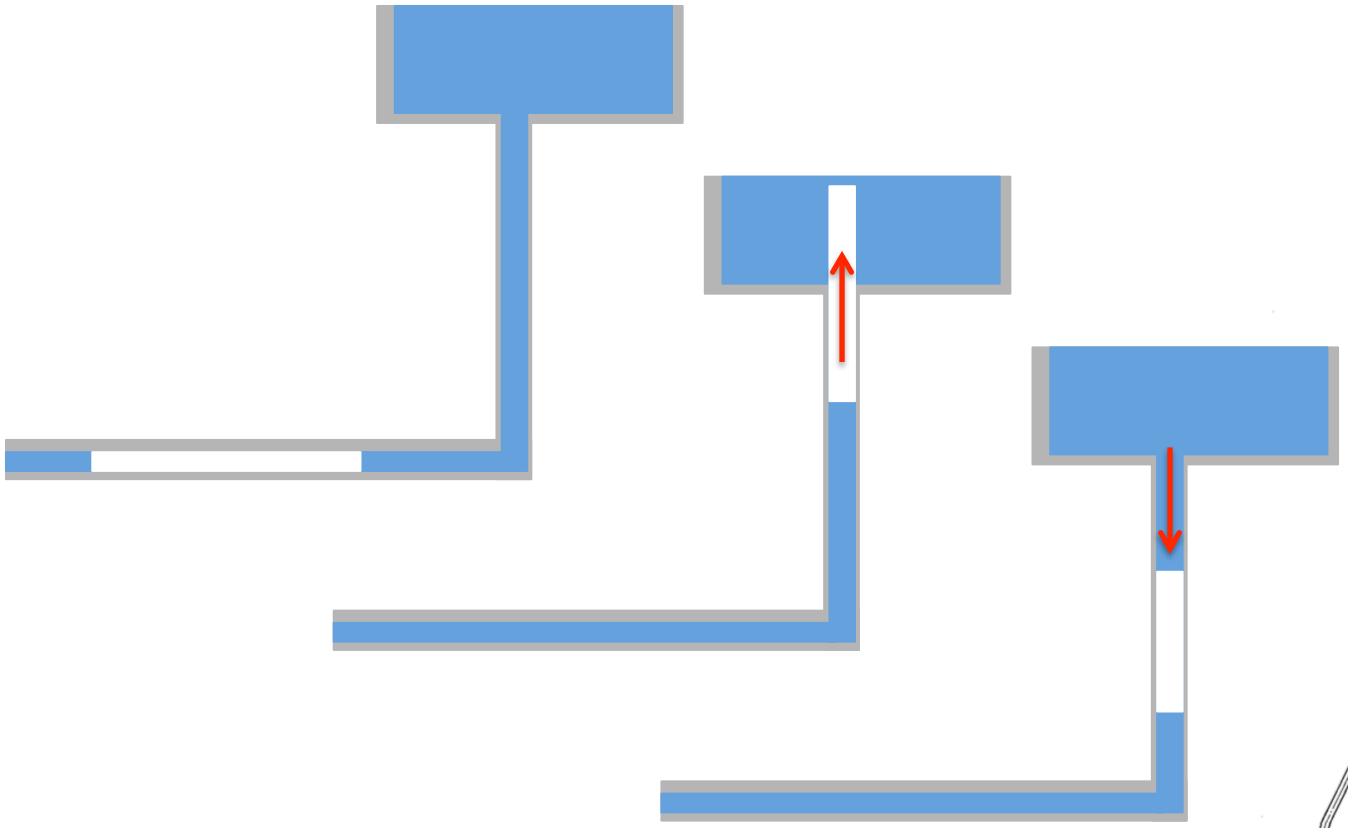
- Water hammers produce heat
- All that energy has to go somewhere and most of it is turned into heat
- A hammer can be used to heat water
- Remember this during place-shifting chemical reactions

Level Boundary Slug



IOActive

Gravity Hammer
Steam Void Collapse



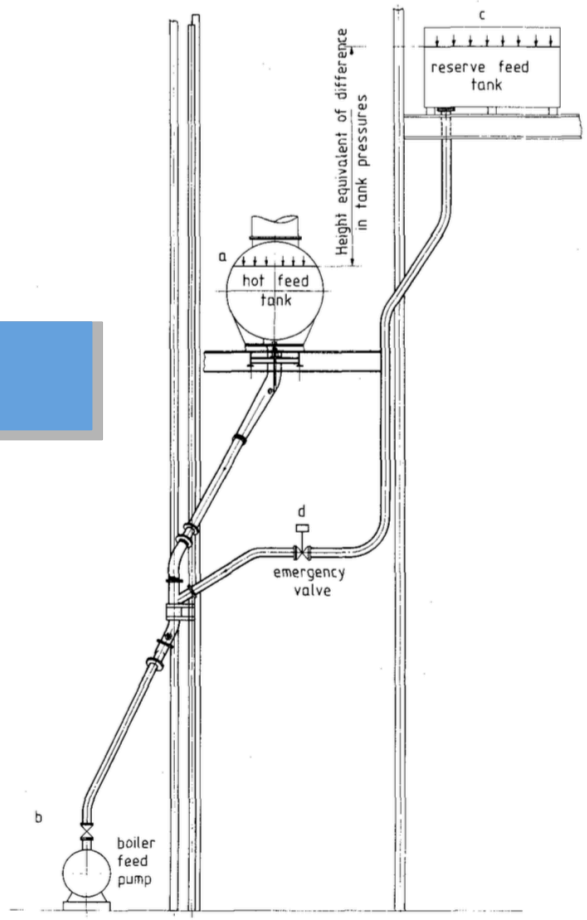


Fig. 3. Feed pump suction system at Nottingham Power Station

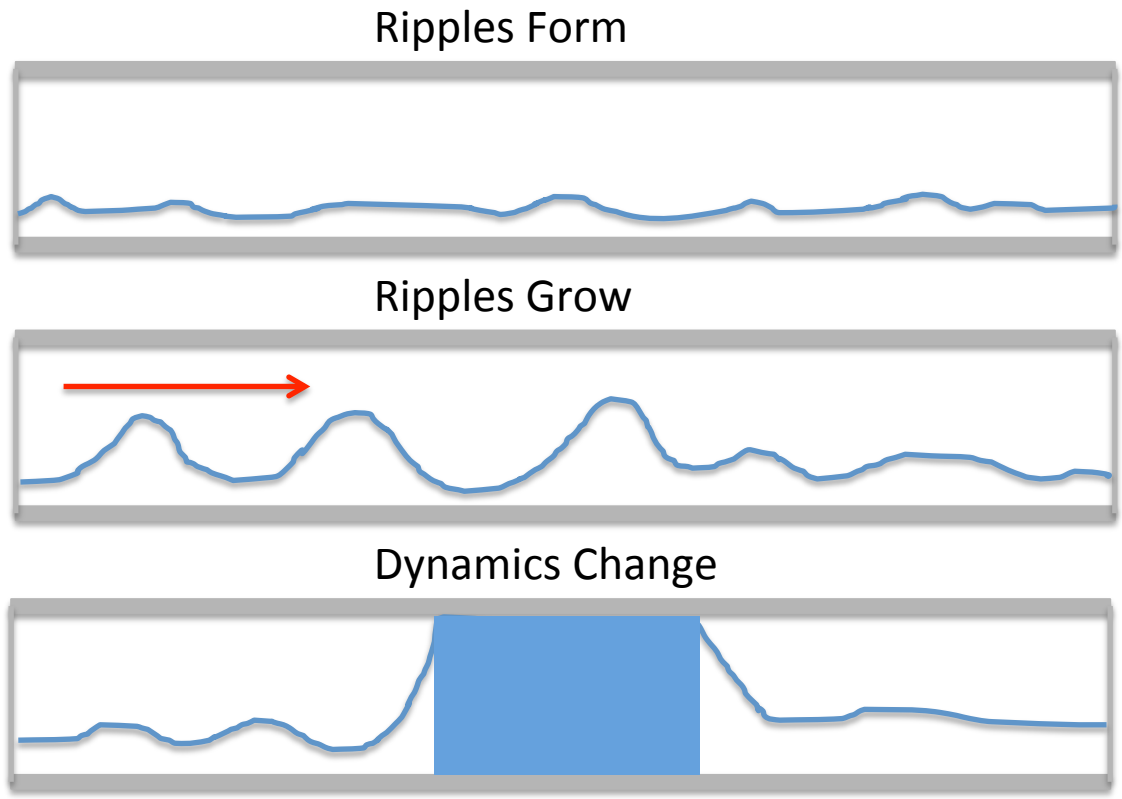
Proc Instn Mech Engrs Vol 194

IOActive.

When gas and liquid move at different speeds

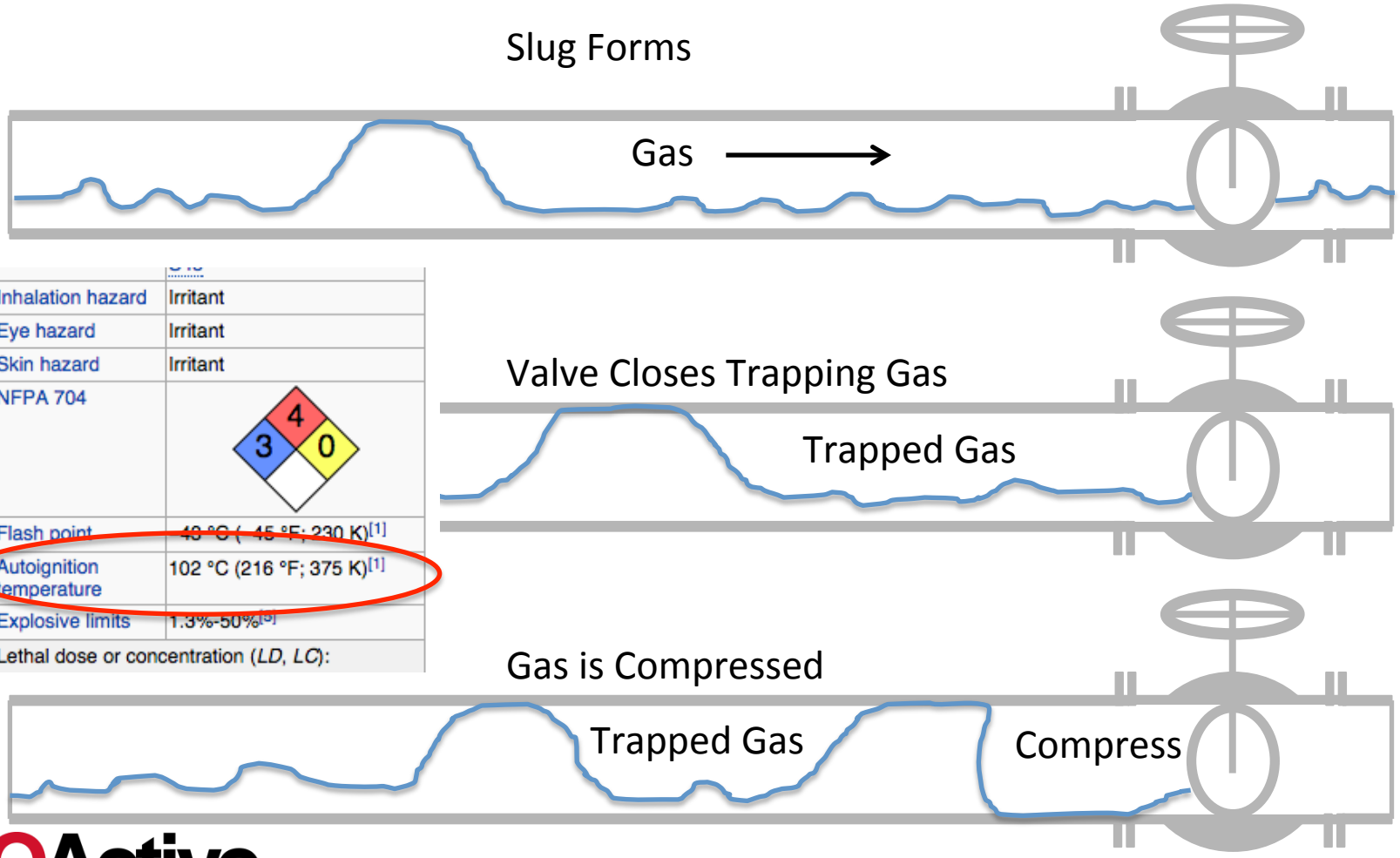
IOActive

Biphase Slug



IOActive

Biphase Slug with Piston Effect



Inhalation hazard	Irritant
Eye hazard	Irritant
Skin hazard	Irritant
NFPA 704	4 / 3 / 0
Flash point	43 °C (−45 °F; 230 K)[1]
Autoignition temperature	102 °C (216 °F; 375 K)[1]
Explosive limits	1.3%-50%[3]
Lethal dose or concentration (*LD*, *LC*):	

IOActive

When the pressure drops below zero

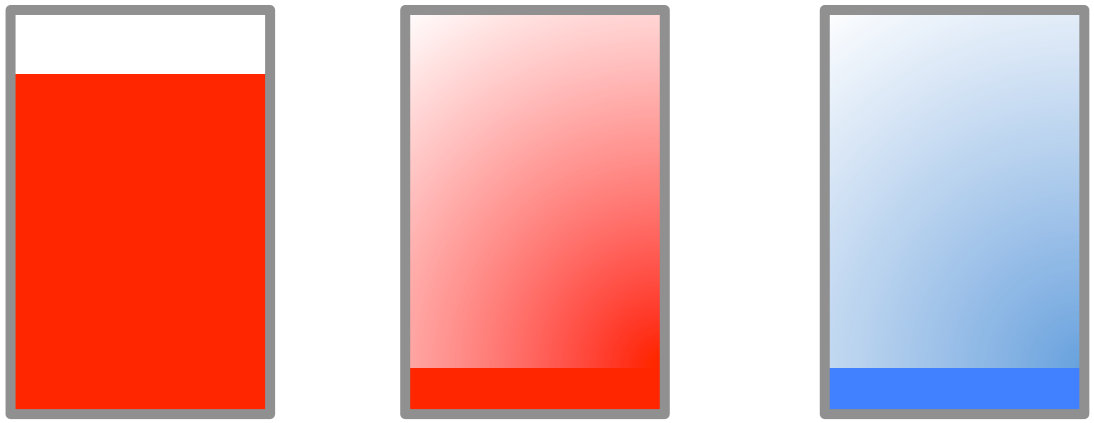
IOActive™

Vacuum Collapse

- Lots of structures can take very high positive pressures but can only take small negative pressures
- As we replace metal pipes with new types of plastic piping, this is becoming more common

-14.7 PSI = True Vacuum (on earth at least)

Steam Collapse



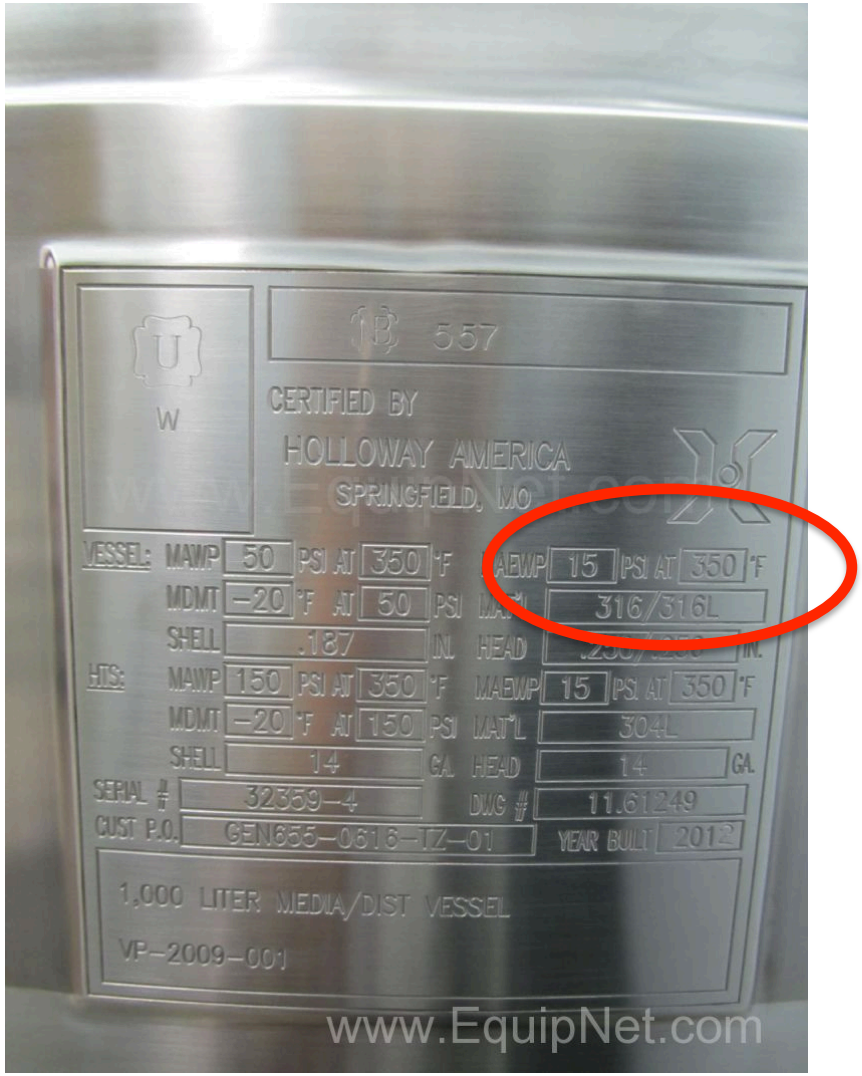
Ideal Gas Laws

$$\frac{P_1V_1}{T_1} = \frac{P_2V_2}{T_2}$$

1. Fill a space with hot stuff or hot gas
2. Remove the hot liquid
3. Let it cool down

IOActive

Steam Collapse

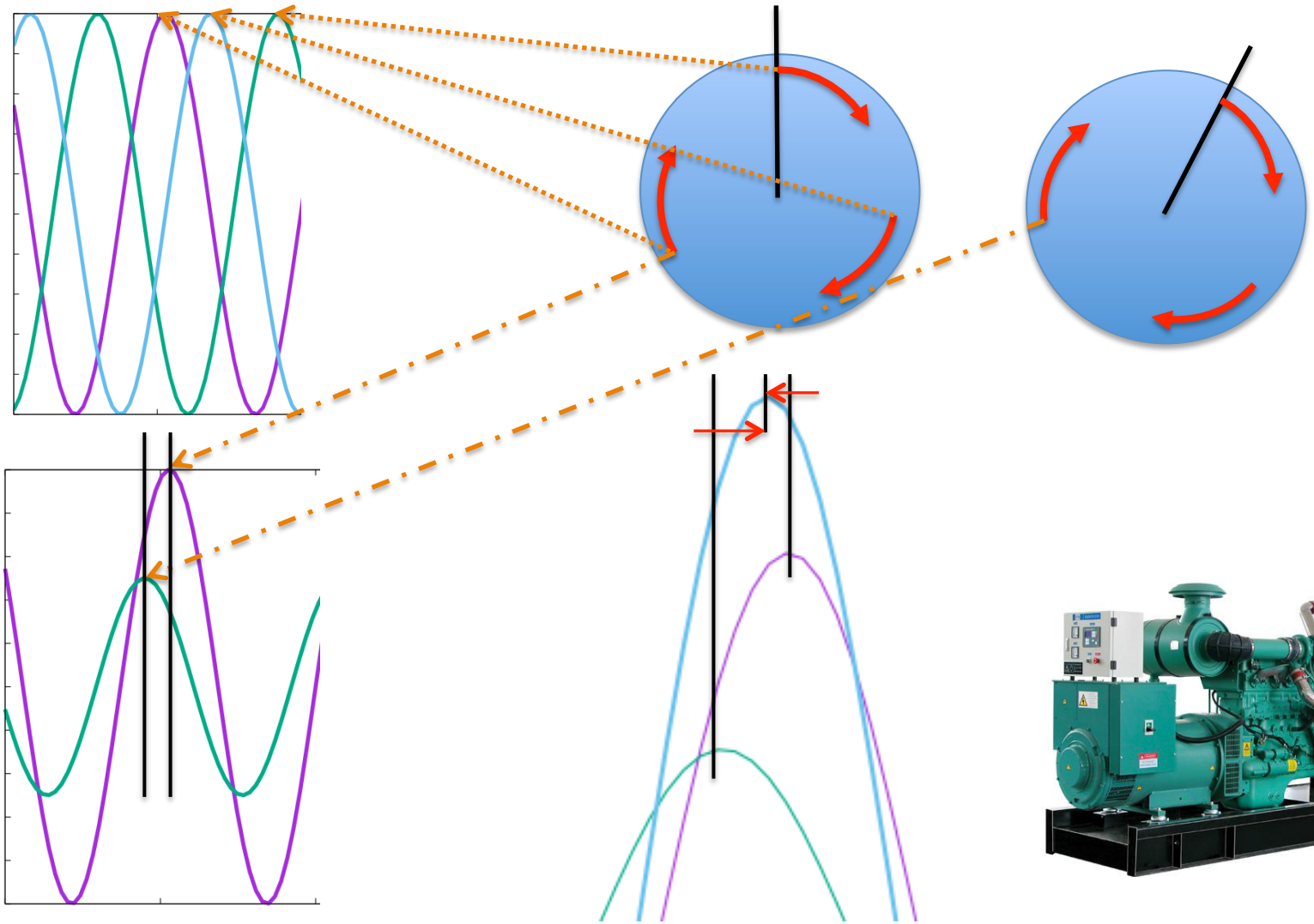


- Most pressure vessels can take a true vacuum
- The interesting part comes from all the external stuff we bolt on to the pressure vessel

IOActive

When you bring something in out of phase

Three-Phase Attacks



Newtonian Mechanics

- Speed of light in copper
- Rubber band effect
- It's all about the torque
- Big guys get to beat up little guys
- Far away guys are the same a little guys

IOActive

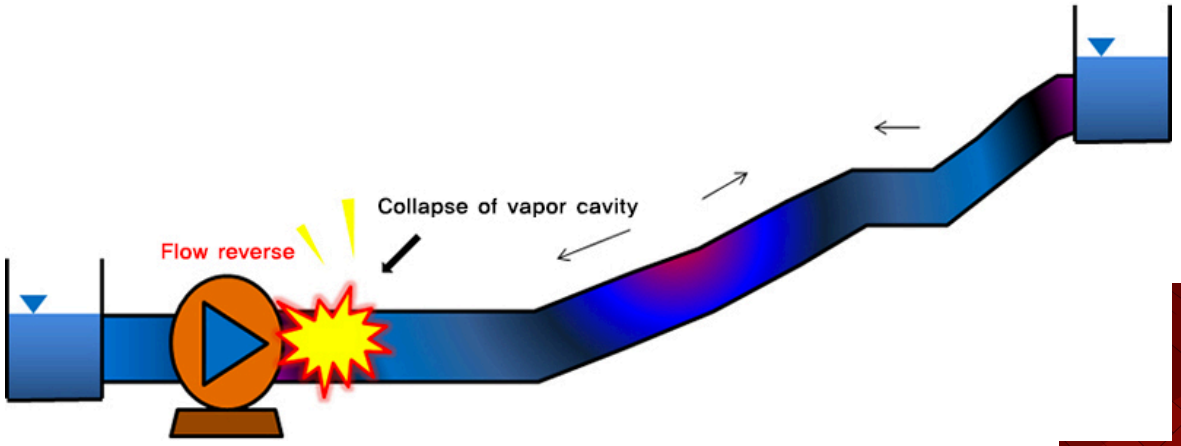
Combining

- Power outages caused the rupture of a water line

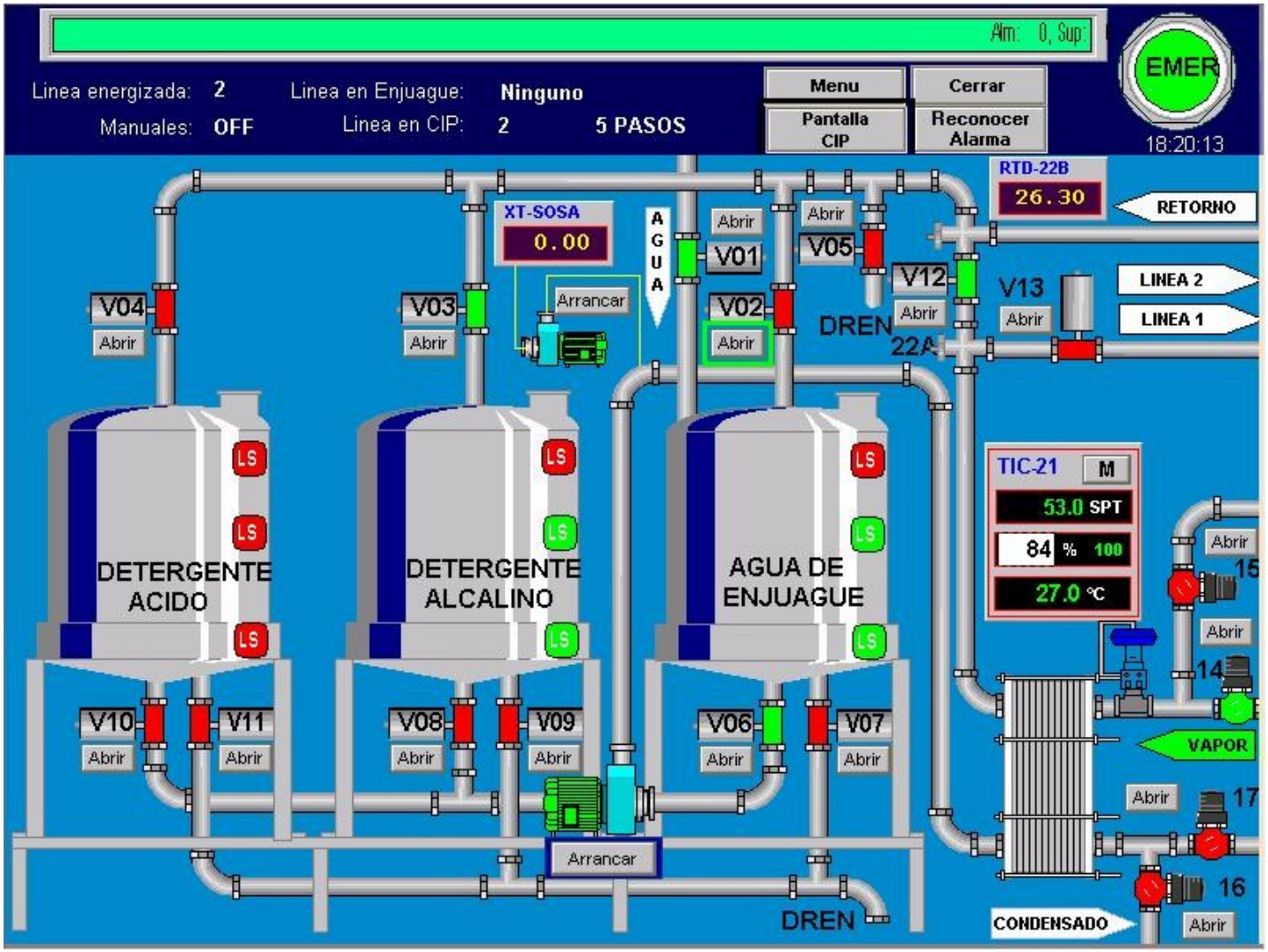
IOActive

Multi-Adaptive

- Last non-constant derivative of a polynomial



IOActive



Consider this…….

IOActive

Questions

Jason Larsen

Jason.larsen@ioactiv e.com

IOActive