Adventures in a new dimension: Physical process as communication medium

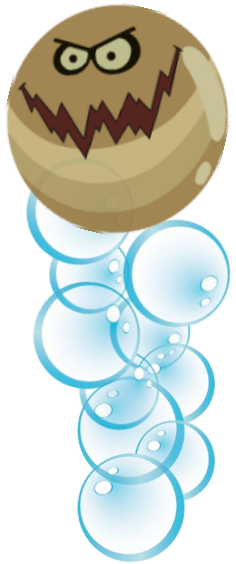
Marina Krotofil

COINS summer school on Security Applications, Lesbos, Greece
26-27.07.2019

Note

This session is based on the talk:

M. Krotofil “Evil Bubbles or How to Deliver Attack Payload via the Physics of the Process”, Black Hat, Las Vegas, USA, 2017.



https://www.blackhat.com/docs/us-17/wednesday/us-17-Krotofil-Evil-Bubbles-Or-How-To-Deliver-Attack-Payload-Via-The-Physics-Of-The-Process.pdf

If it’s in a Hollywood movie… it’s cool ;-)

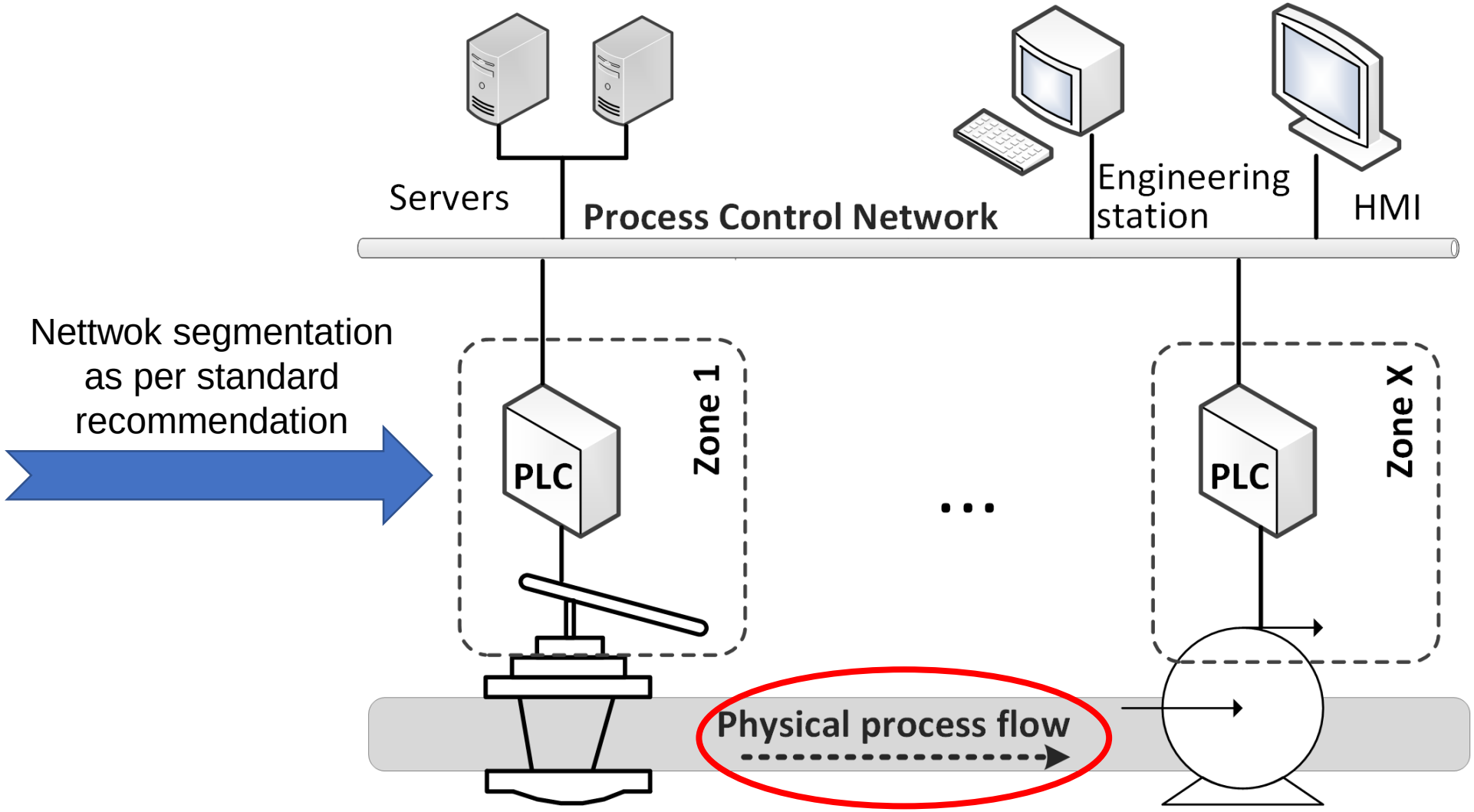
The Hunt for Red October (1990)

Cavitation is cool!

The Hunt for Red October (1990)

Motivation for this research

IEC 62443-1-1 standard

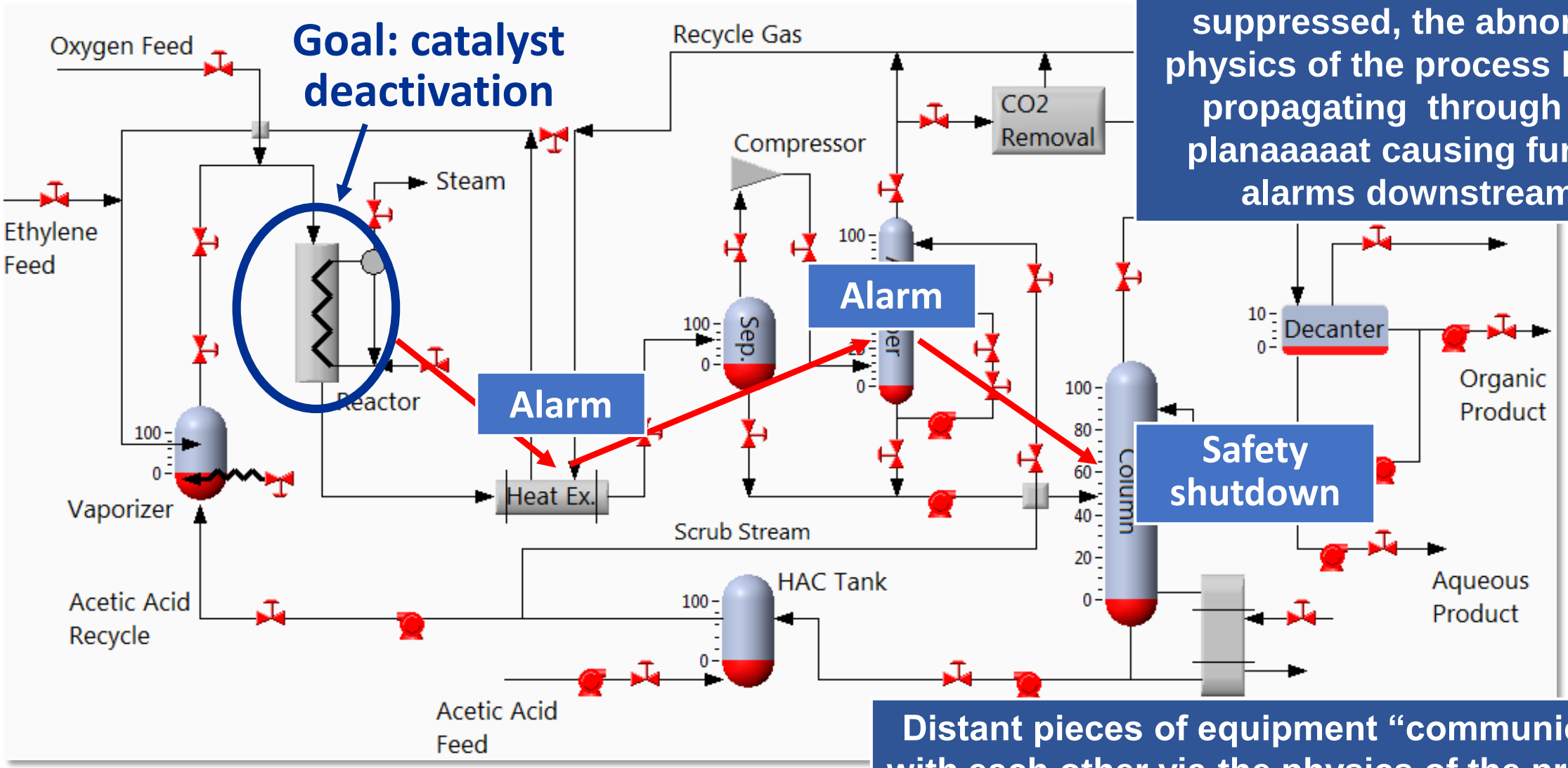


My Black Hat talk back in 2015

Source: simentari.com

Attack goal: persistent economic damage

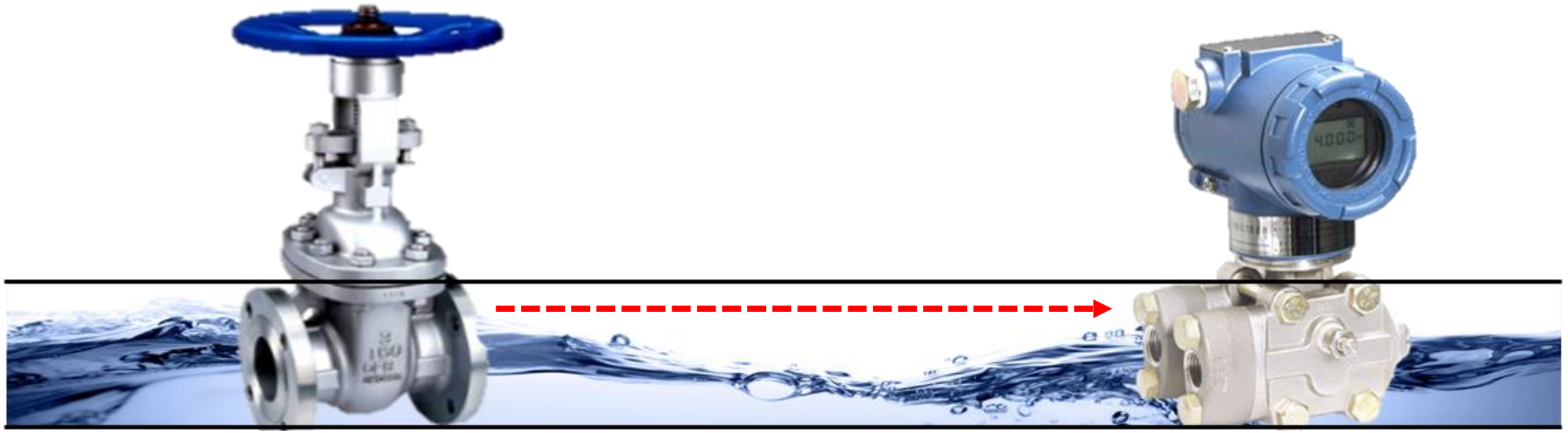
Failed scenario: Alarm and physics propagation



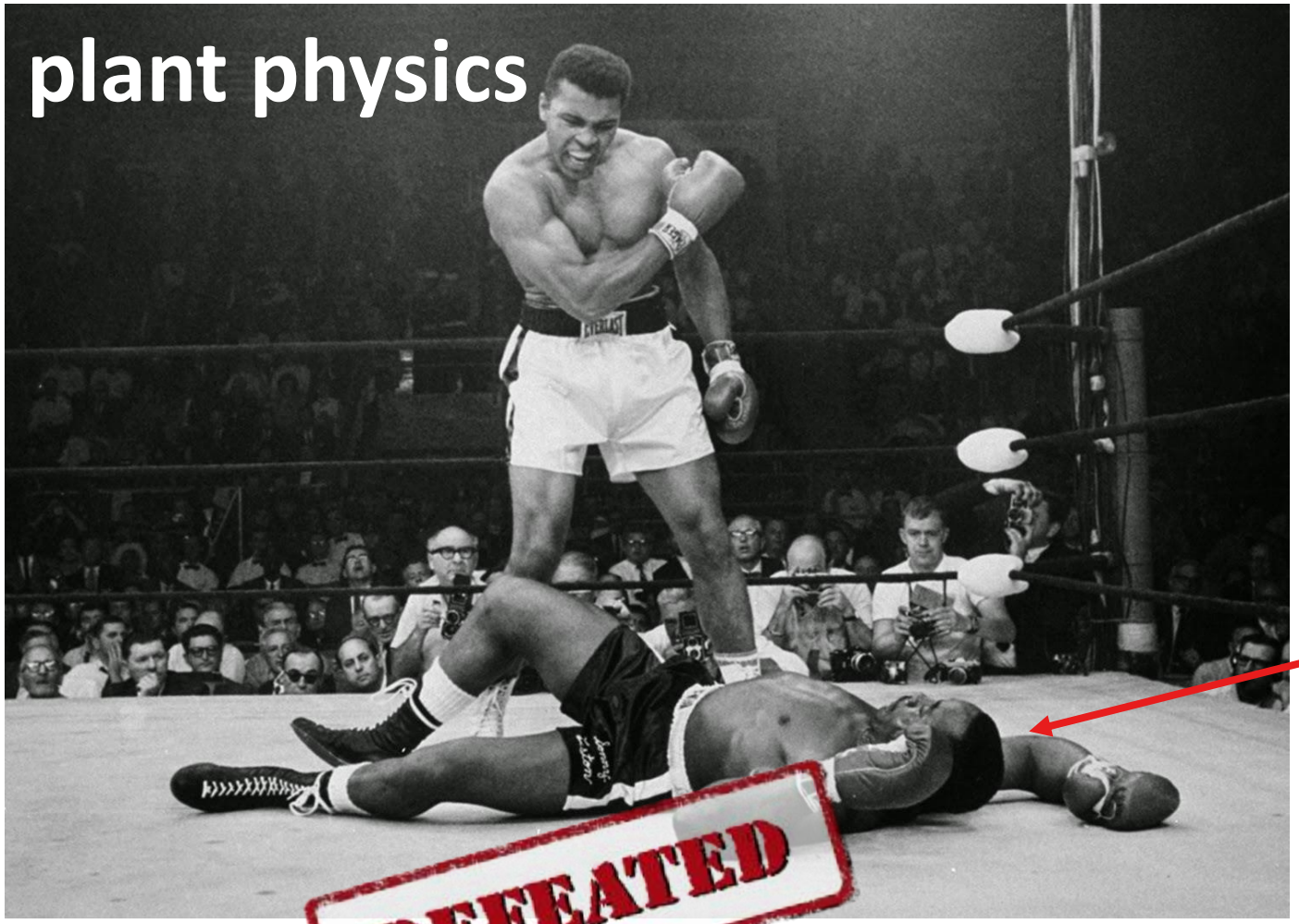
Even if digital alarms are suppressed, the abnormal physics of the process keeps propagating through the planaaaaat causing further alarms downstream.

Distant pieces of equipment "communicate" with each other via the physics of the process

Physical process is a communication medium



Process Physics vs. Attacker

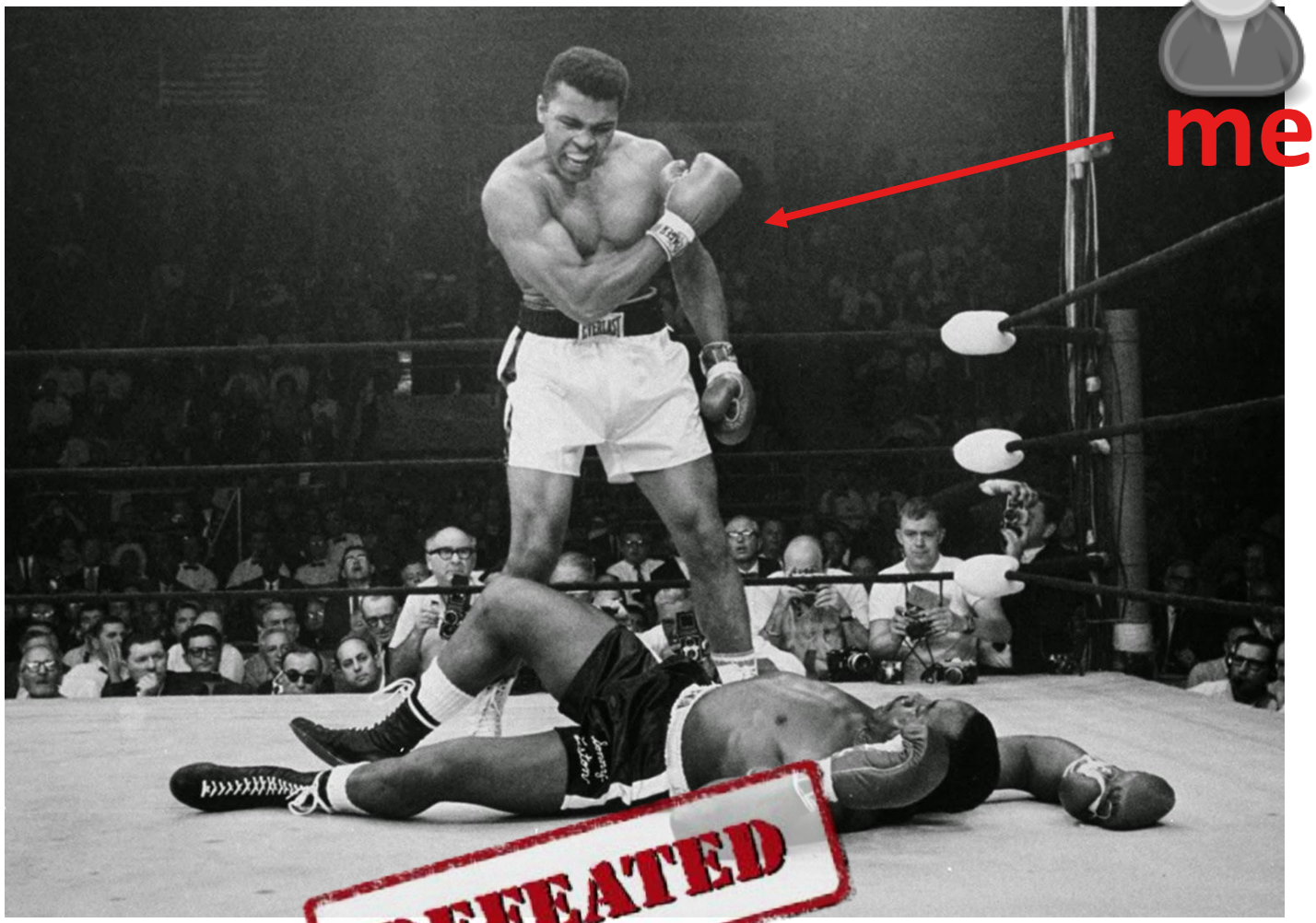


http://100photos.time.com

me

I felt very angry

The attacker always wants to win!

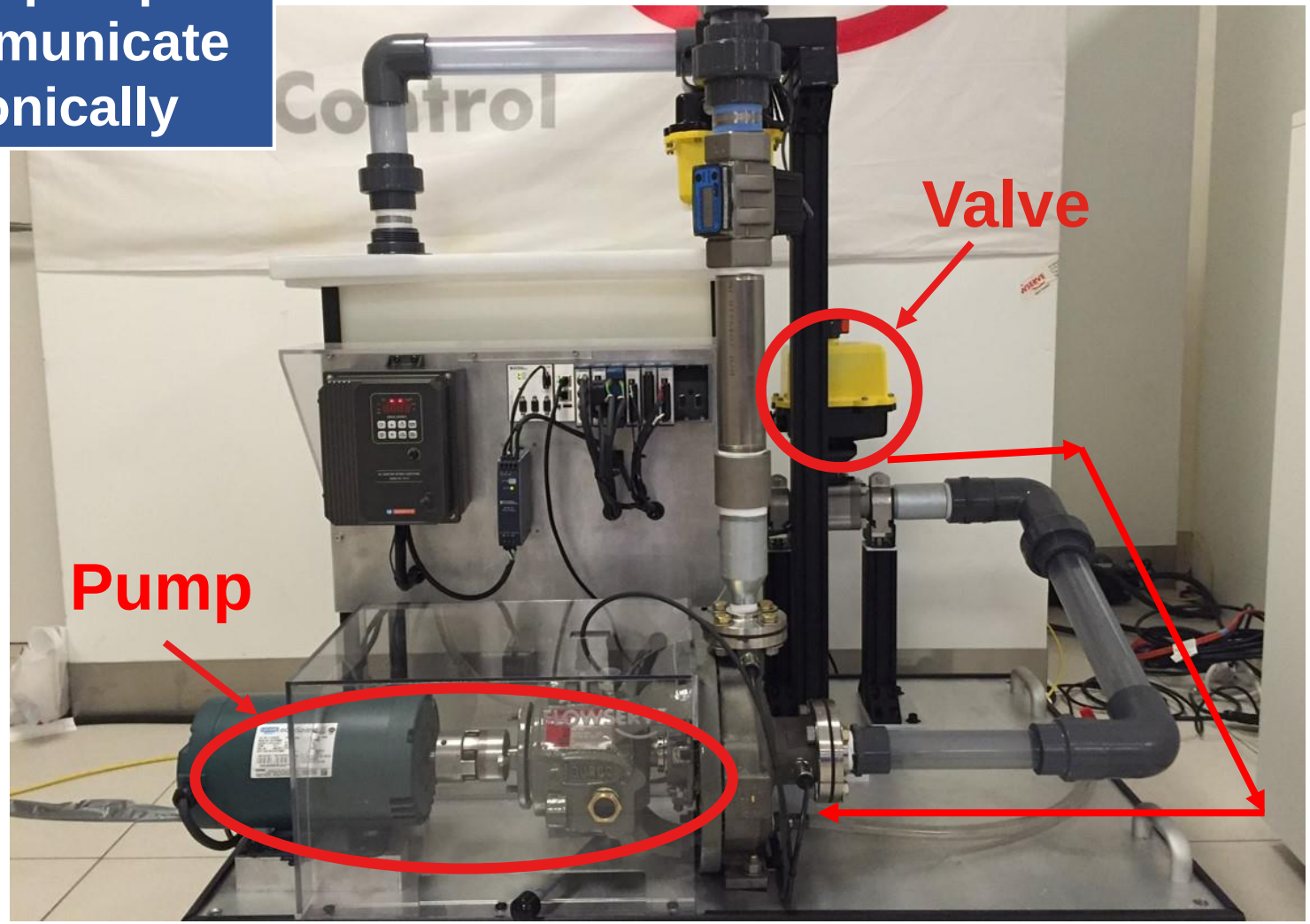


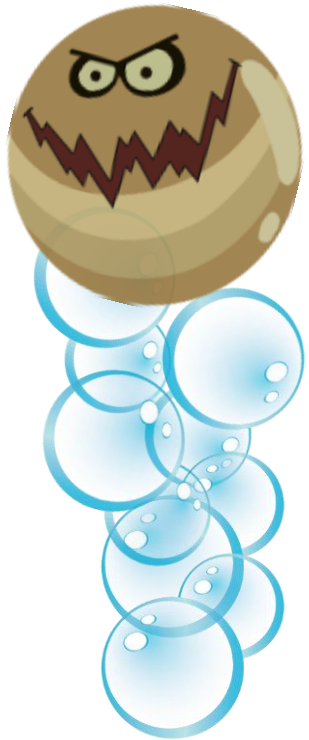
http://100photos.time.com

me (wishfully)

Novel attack vector: Delivery of attack payload via process physics

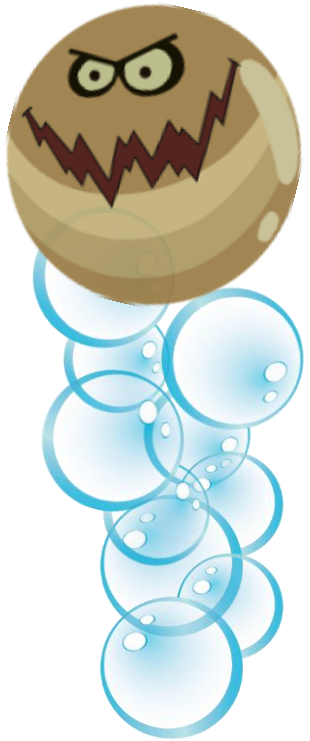
Valve and pump do not communicate electronically





Evil Bubbles

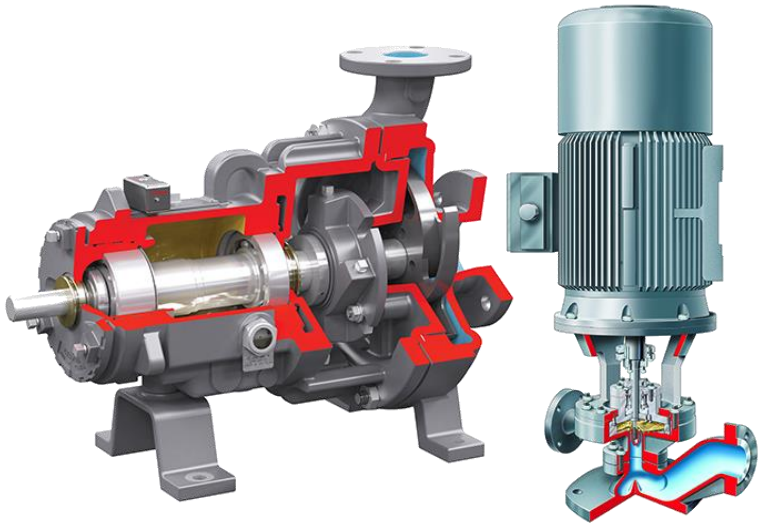
Attack payload propagation



Evil Bubbles

Introduction to pumps

Pumps

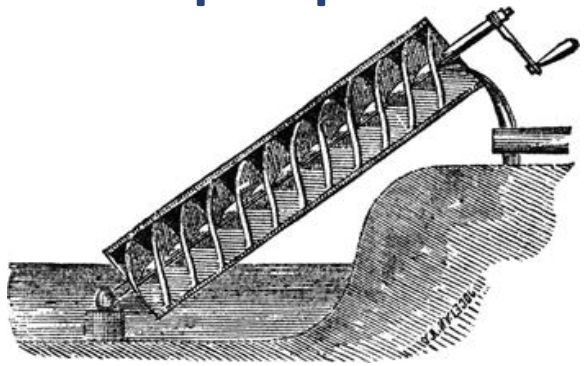


Function of the pump

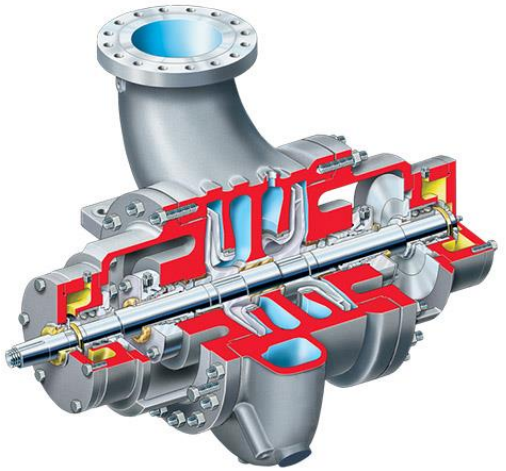
A piece of equipment which <u>elevates</u> or <u>moves liquids</u> at the expense of power input

- Our current lifestyle would not be possible without pumps
  - From air conditioning to pumping oil, from cutting steal to chemical production-> you name it
- Invented by Archimedes in the 3rd century BD (screw pump)
- Global market is ~ 45 billions per year
- Comes in all shapes and sizes, often customized engineering
  - Production of a medium sized pump takes 25-50 weeks and up to 1 year for customized highly engineered pumps

Archimedes screw pump



https://en.wikipedia.org/wiki/Archimedes%27_screw

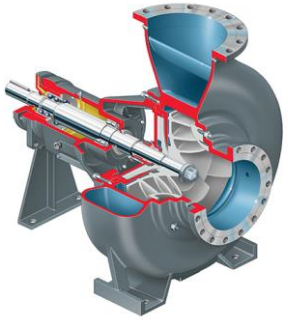


Types of pumps

COLOSSAL

VS.

humble

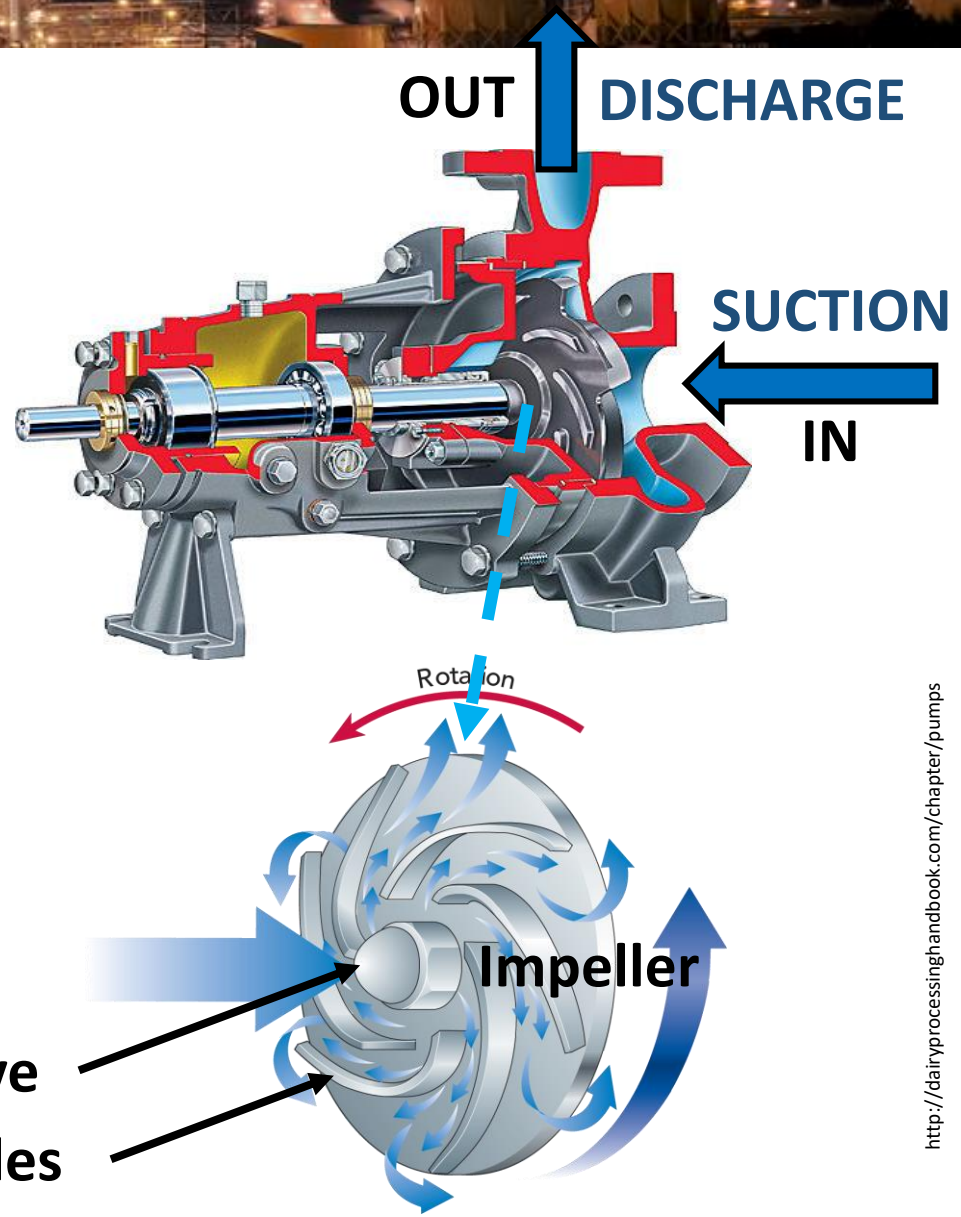


Expensive. Heavy. Break easily -> instrumented for health/safety monitoring

“Cheap”. Light. More resilient to failures -> typically not instrumented for monitoring

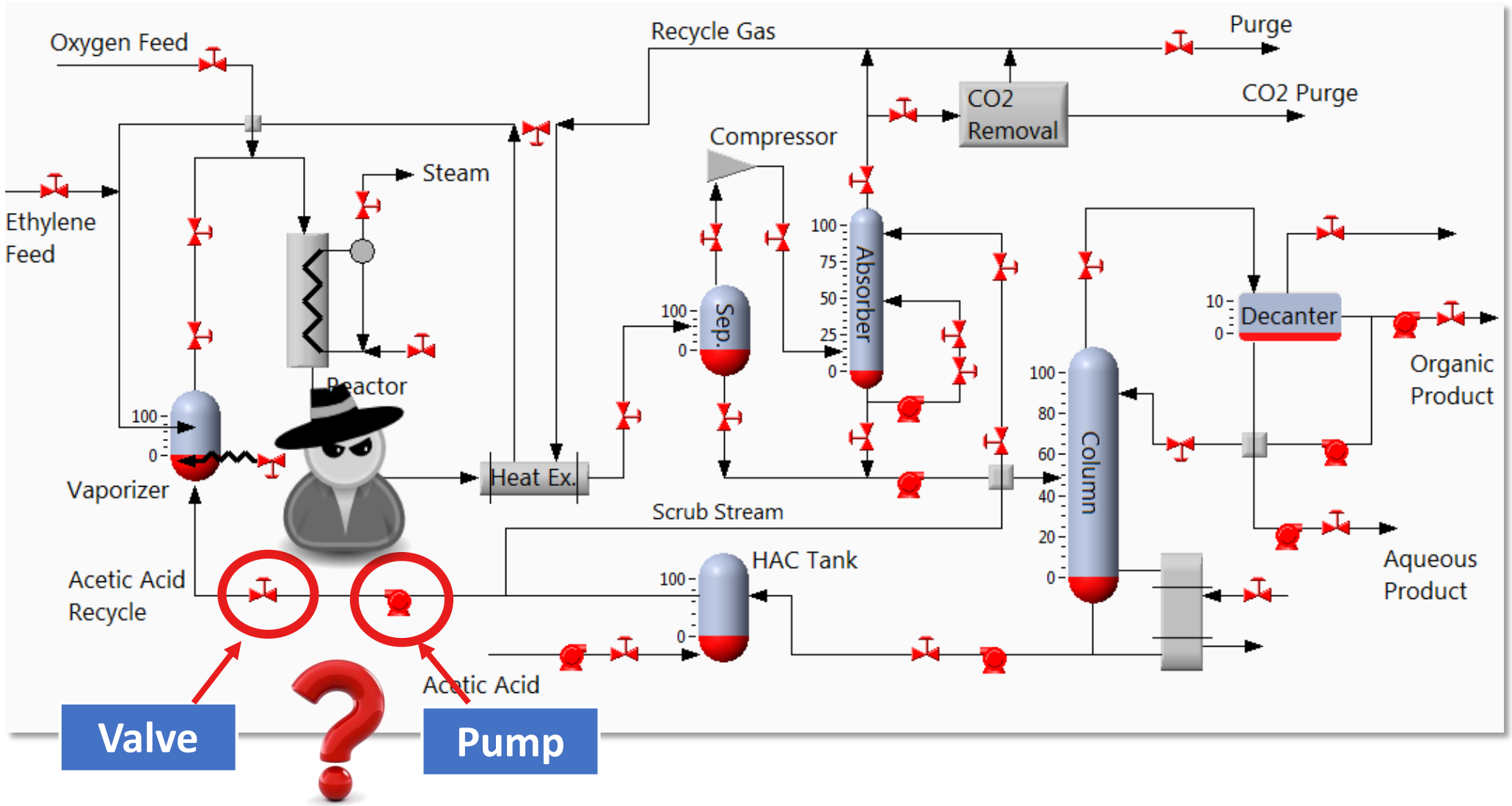
Centrifugal pump

- A centrifugal pump increases the speed of a liquid in a pipe system by using a rotating impeller
- Impeller spins the liquid giving it centrifugal acceleration
- A mechanical energy of the motor is translated into hydraulic energy of the liquid



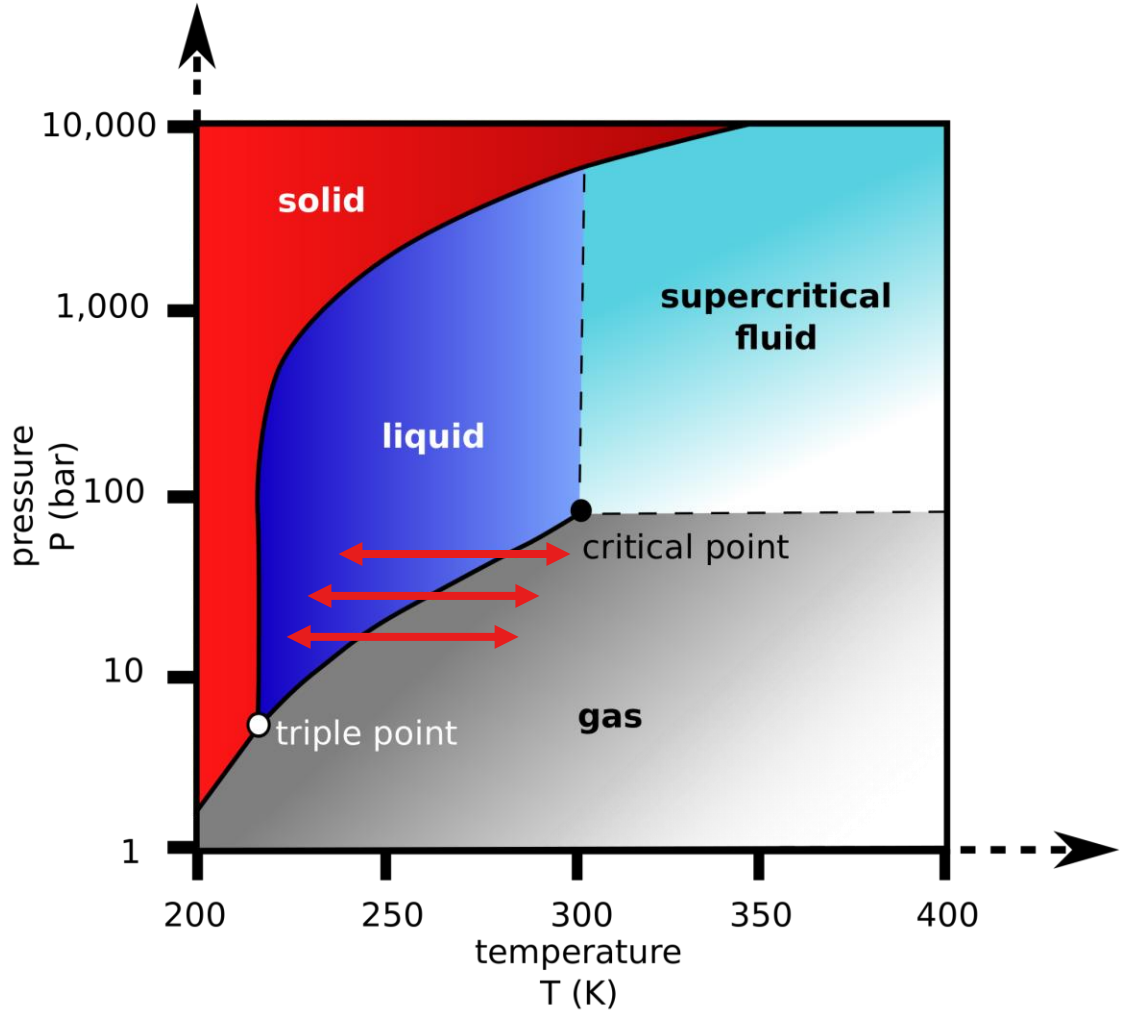
http://dairyprocessinghandbook.com/chapter/pumps

Is it a target worth the effort?



Cavitation

States of physical substances



https://commons.wikimedia.org/wiki/File:Carbon_dioxide_pressure-temperature_phase_diagram-fr.svg

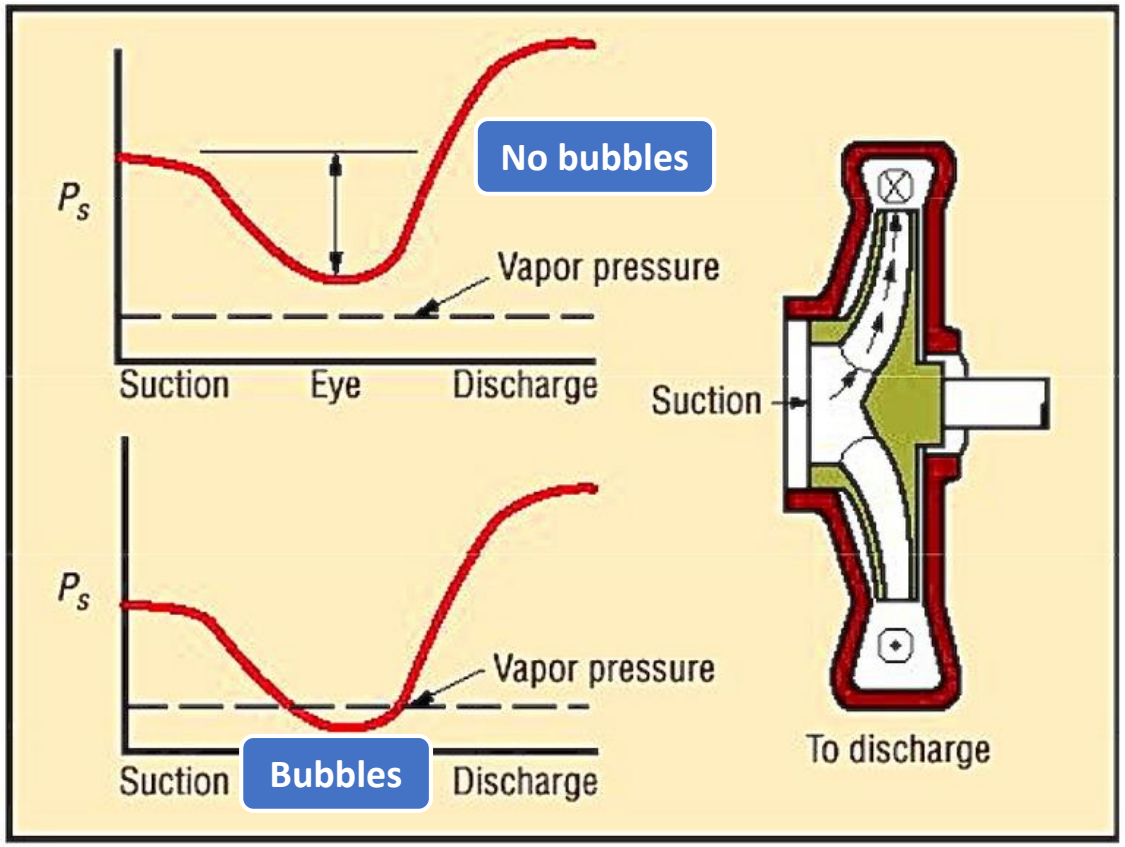
- If the pressure of the substance drops or its temperature increases, it begins to vaporize, just like boiling water

  -> formation of bubbles :-)

Carbon dioxide pressure-temperature phase diagram

The bubbles we all like

Pump cavitation

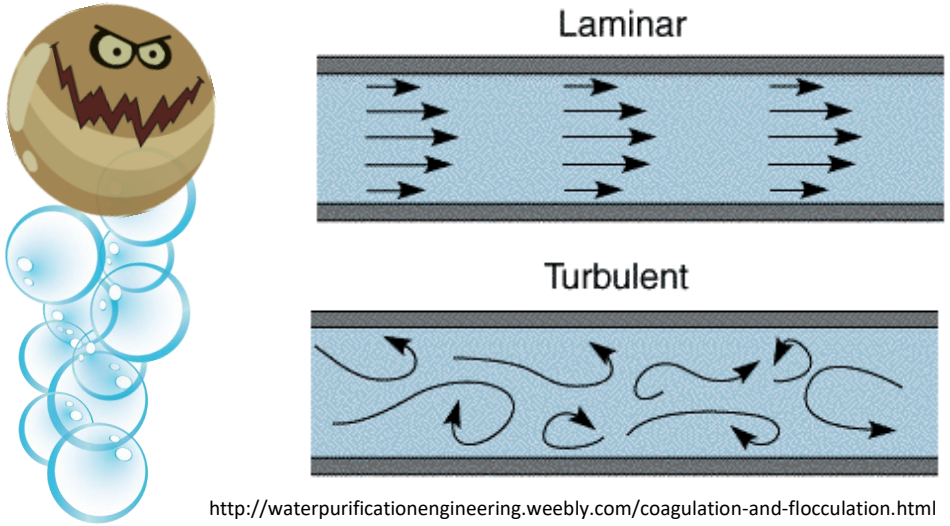


http://jmpcoblog.com/hvac-blog/how-to-read-a-pump-curve-part-2

Cavitation is formation and bursting of vapor bubbles due to change in liquid pressure

- Cavitation occurs when the pressure in the suction line is too low relative to the vapor pressure of the pumped liquid
- The pressure increases as the liquid flows further into impeller causing bubbles to condense (implode) very rapidly
- The vapor bubbles collapse at a very high [velocity & local pressure], creating massive shock waves

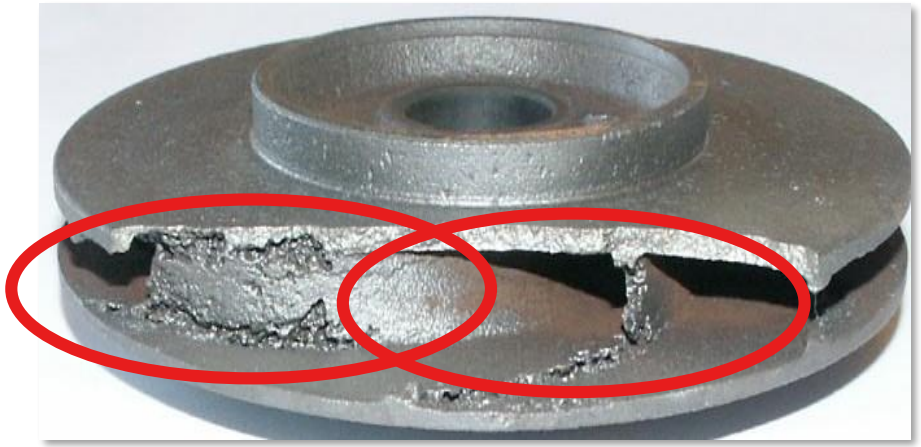
Damaging effect of cavitation



http://waterpurificationengineering.weebly.com/coagulation-and-flocculation.html

1 Reduced efficiency

- All pumps require a smooth, regular symmetrical inlet flow profile for efficient operation
- The collapse of gas bubbles leads to the development of fast turbulent streams -> reducing efficiency up to inability to pump



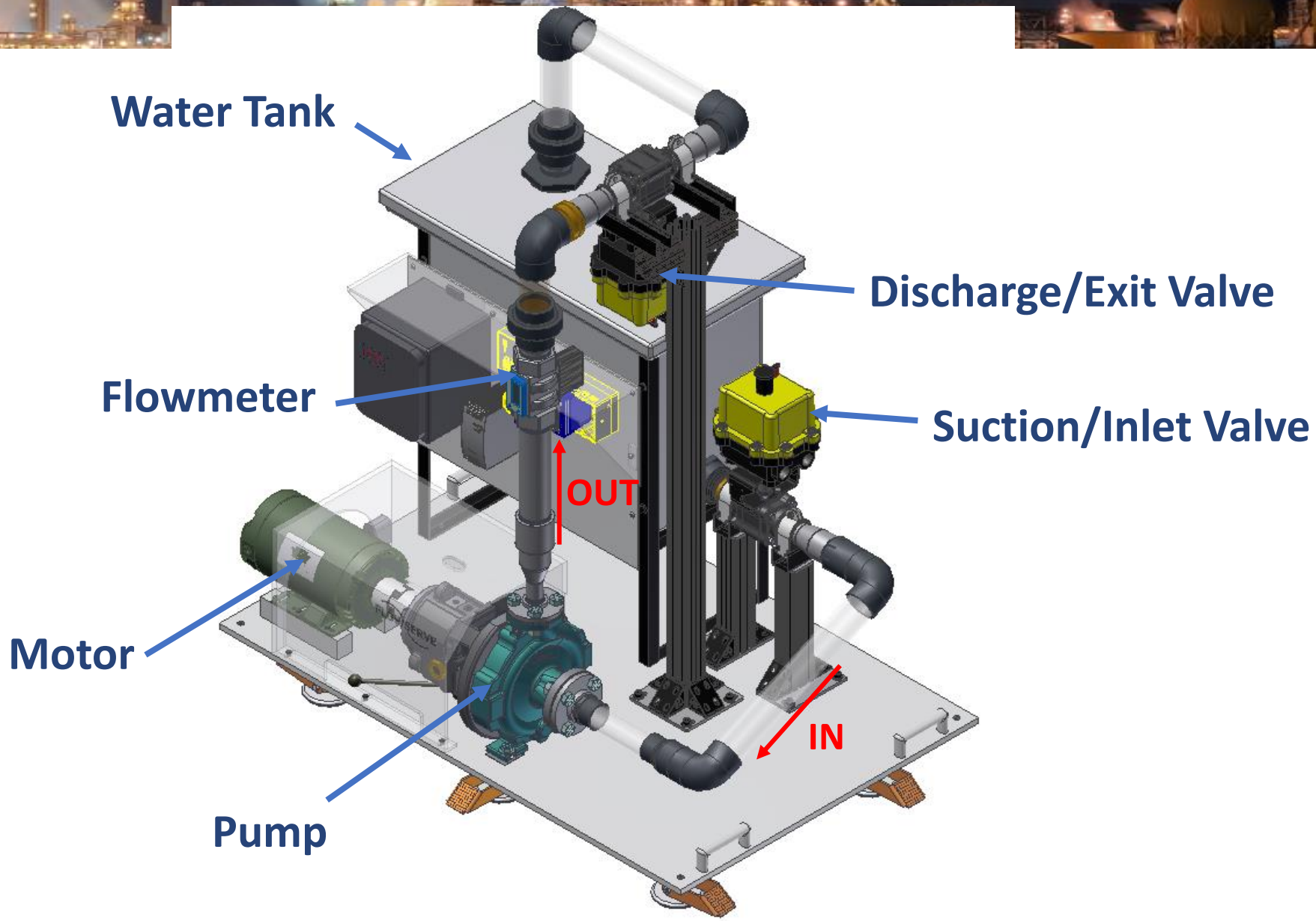
https://commons.wikimedia.org/wiki/File:Kavitation_at_pump_impeller.jpg

2 Premature failure of the pump

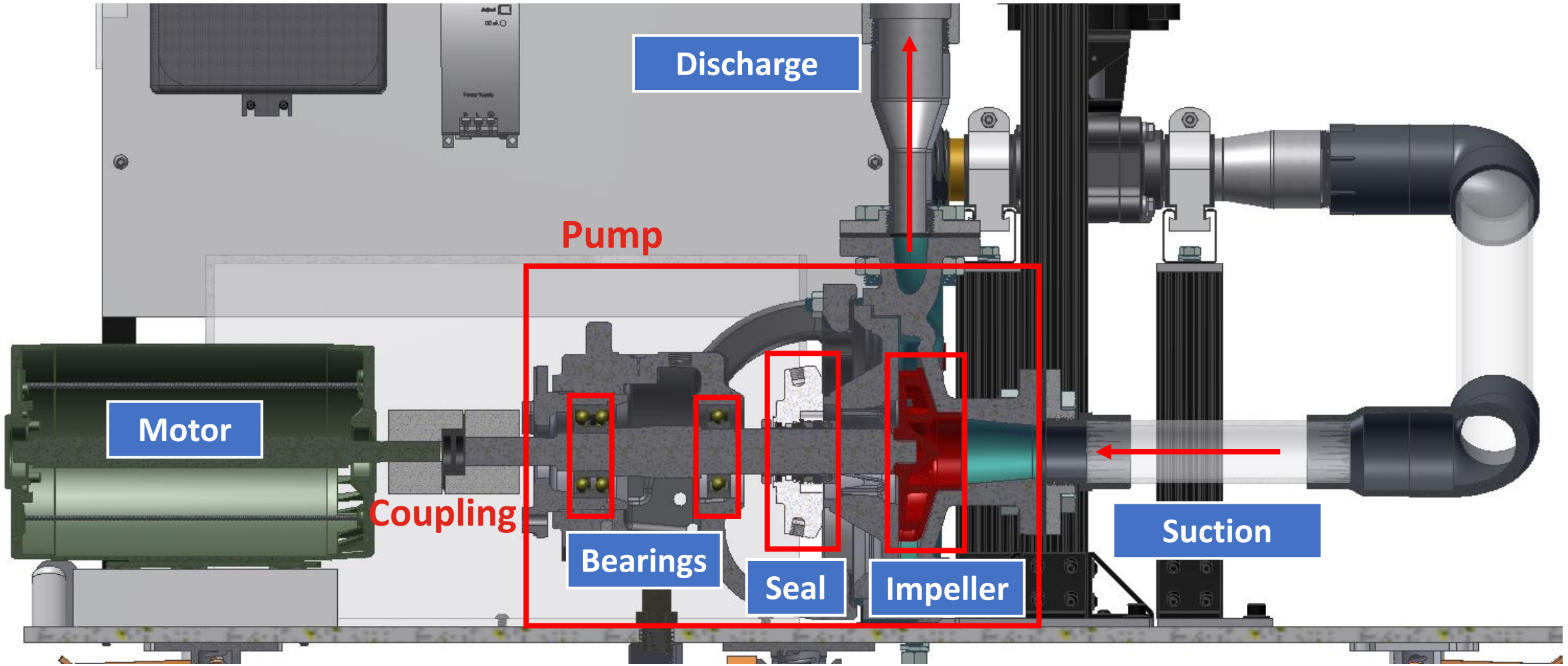
- Bubble collapse causes excessive vibrations which can damage rings, seals & bearings
- Shock waves creates small pits on the edges of impeller blades, eventually wearing them completely

Demo rig overview and experiment demo

Overview of the demo rig

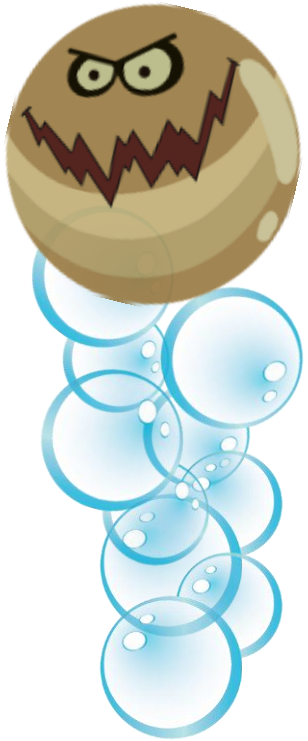


Inside the pump



DEMO

Video of experiment

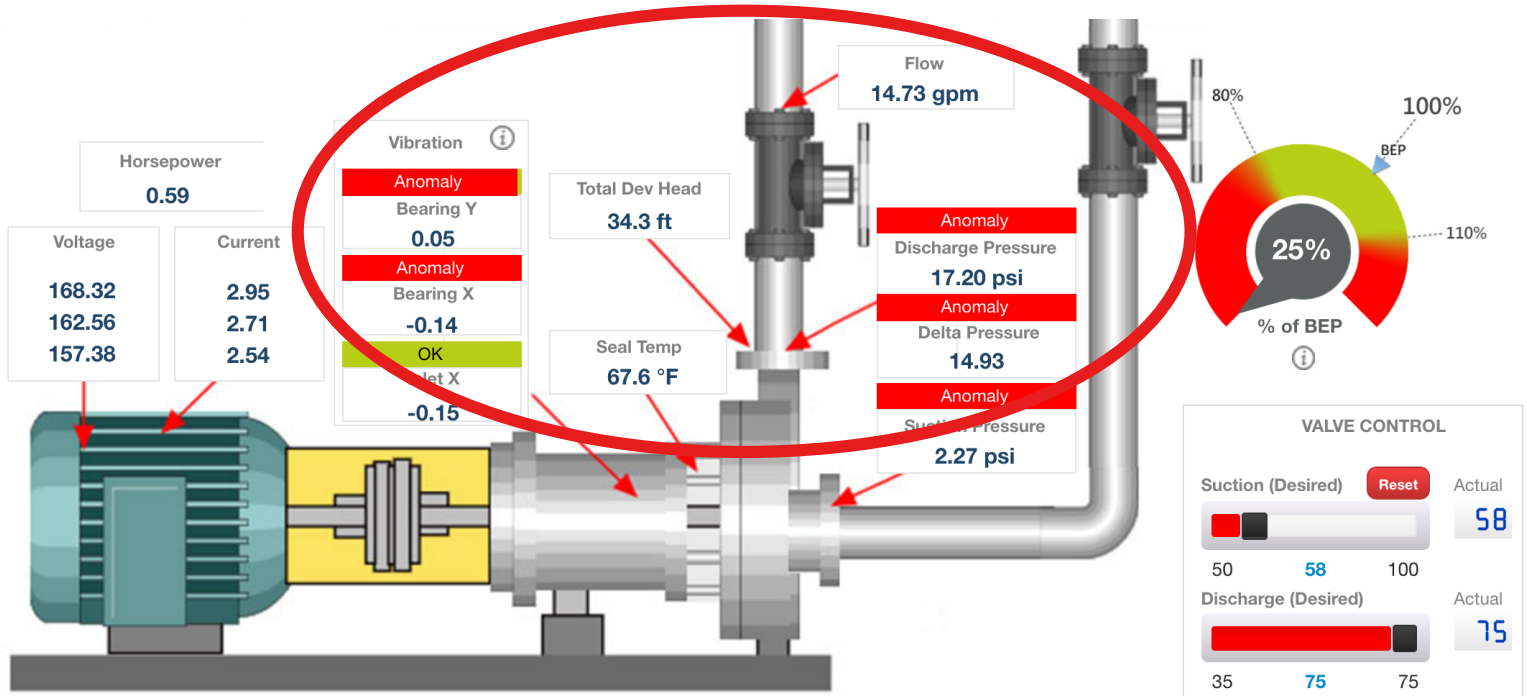


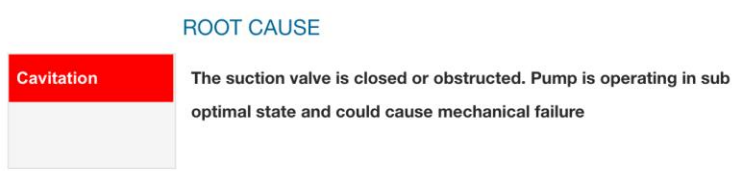
Evil Bubbles

Detecting cavitation

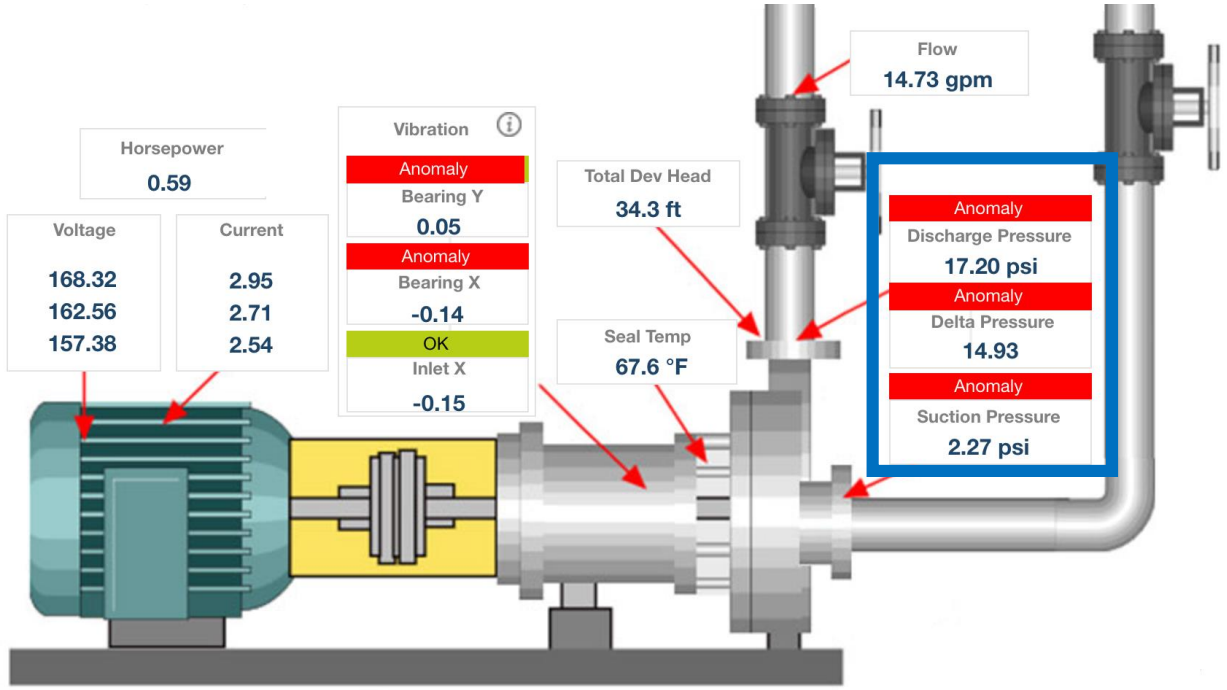
Detection with asset monitoring applications

Pump is instrumented with sensors to monitor its state





Pump monitoring



Fluid pressure

- Suction pressure (inflow), psi
- Discharge pressure (outflow), psi
- Delta pressure, psi
- Total developed head, ft

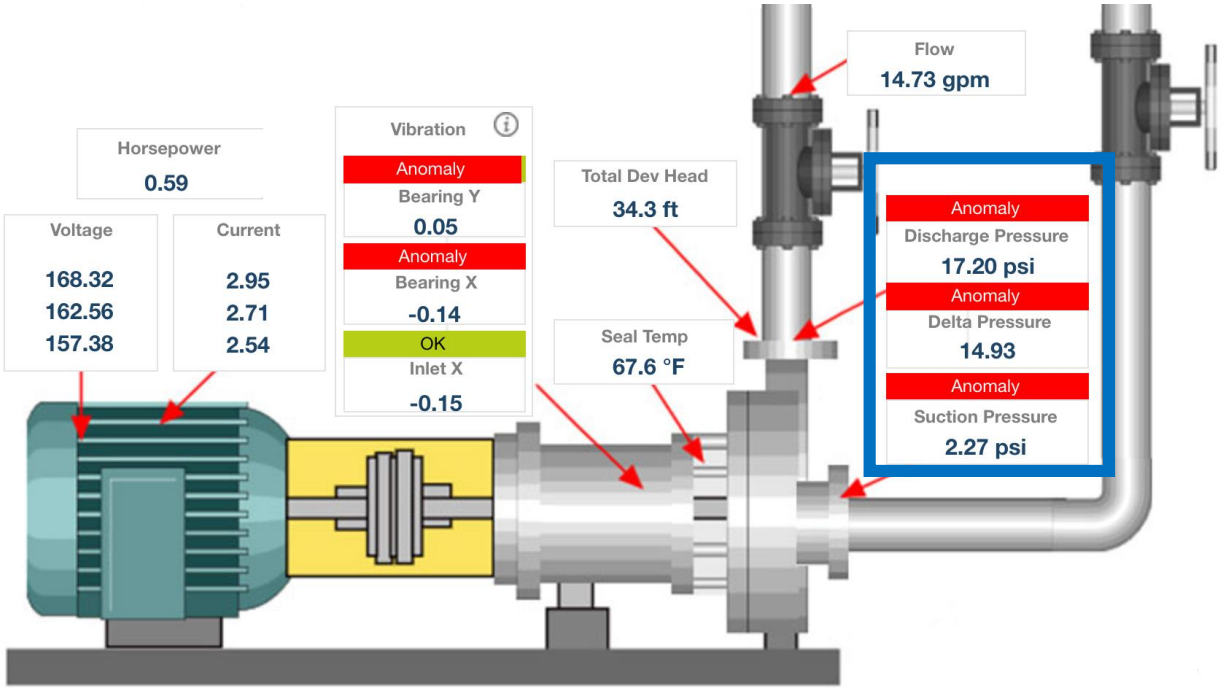
Temperature

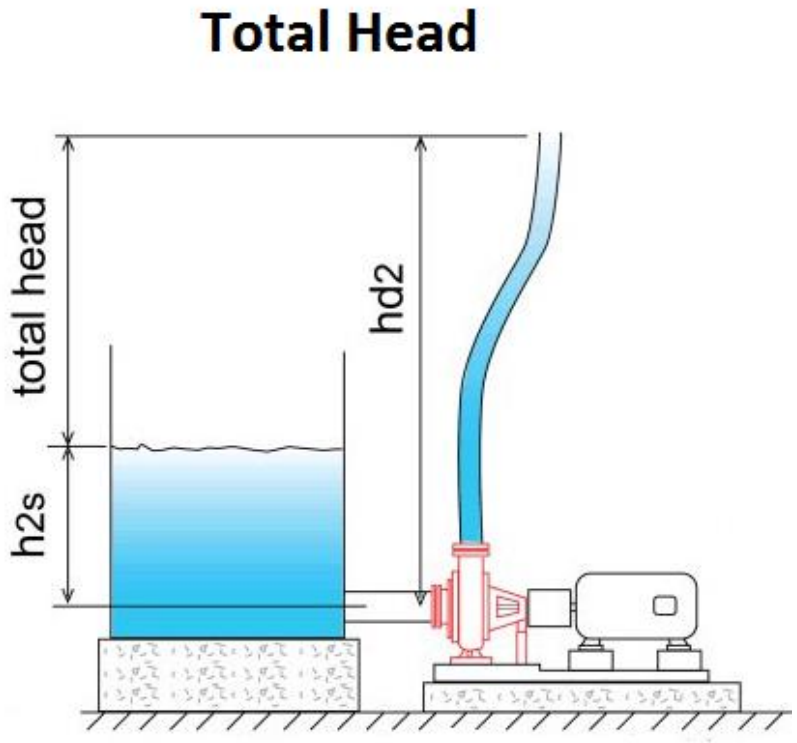
- Seal temperature, F

Vibration

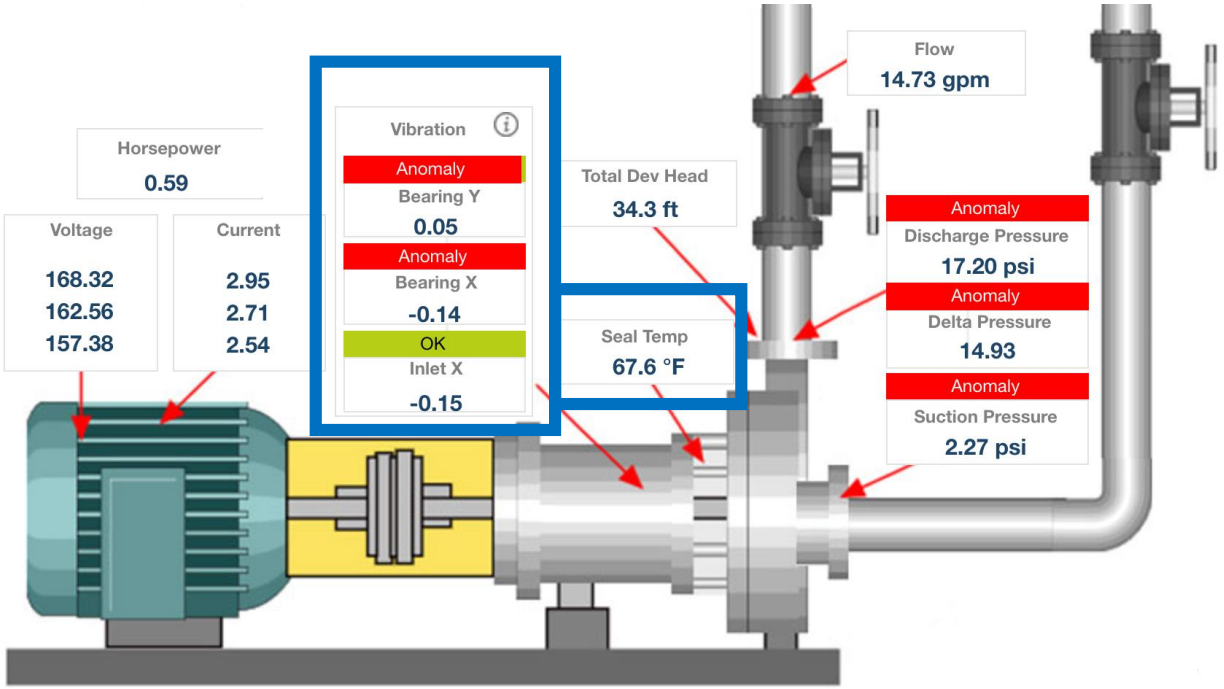
- Vibration bearing X (horizontal)
- Vibration bearing Y (vertical)
- Vibration pump inlet X

Pump monitoring





Pump monitoring



Fluid pressure

- Suction pressure (inflow), psi
- Discharge pressure (outflow), psi
- Delta pressure, psi
- Total developed head, ft

Temperature

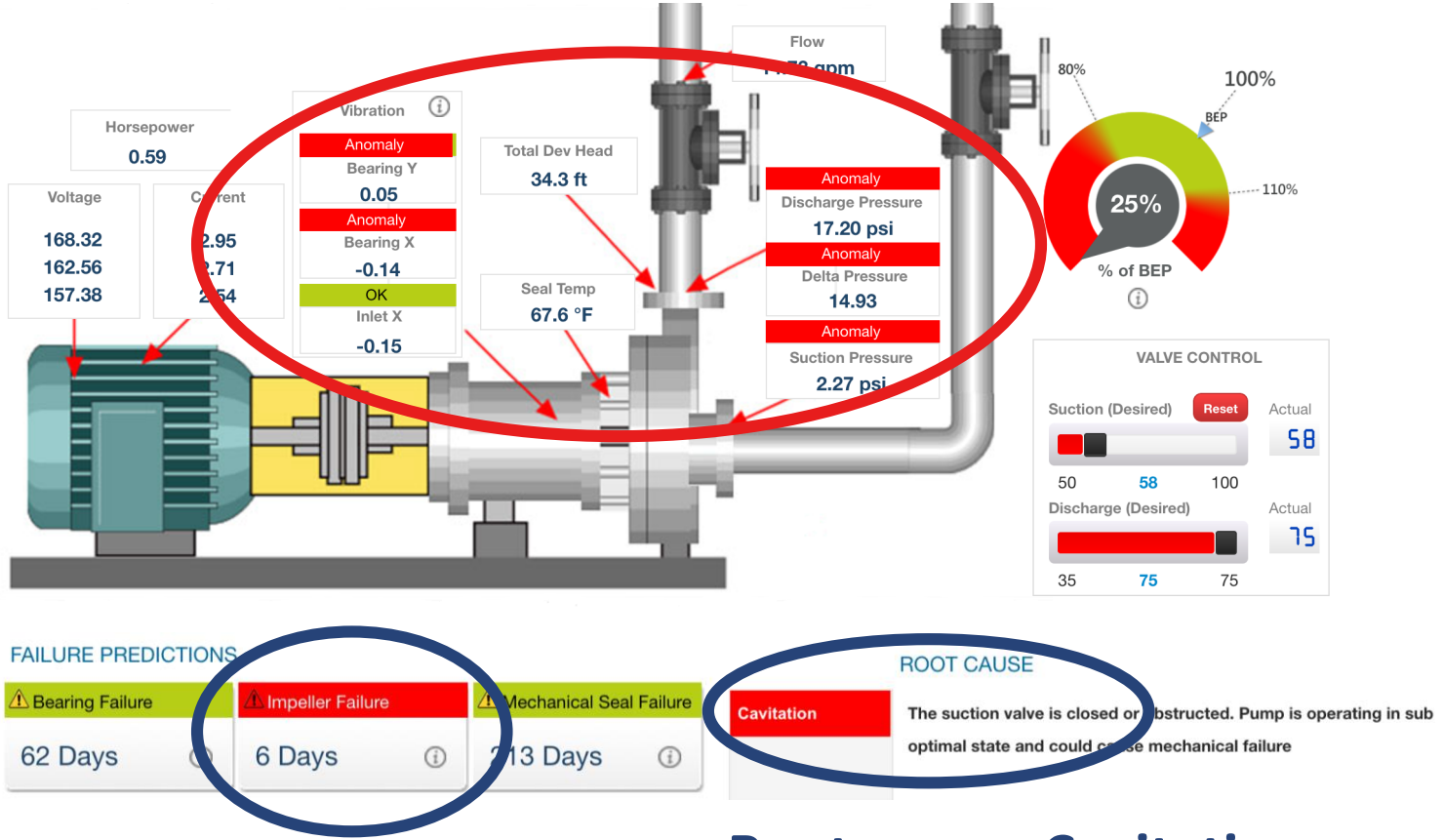
- Seal temperature, F

Vibration

- Vibration bearing X (horizontal)
- Vibration bearing Y (vertical)
- Vibration pump inlet X

Detection of the cyber-physical attacks

Detection of the cyber-physical attacks requires
process engineering methods

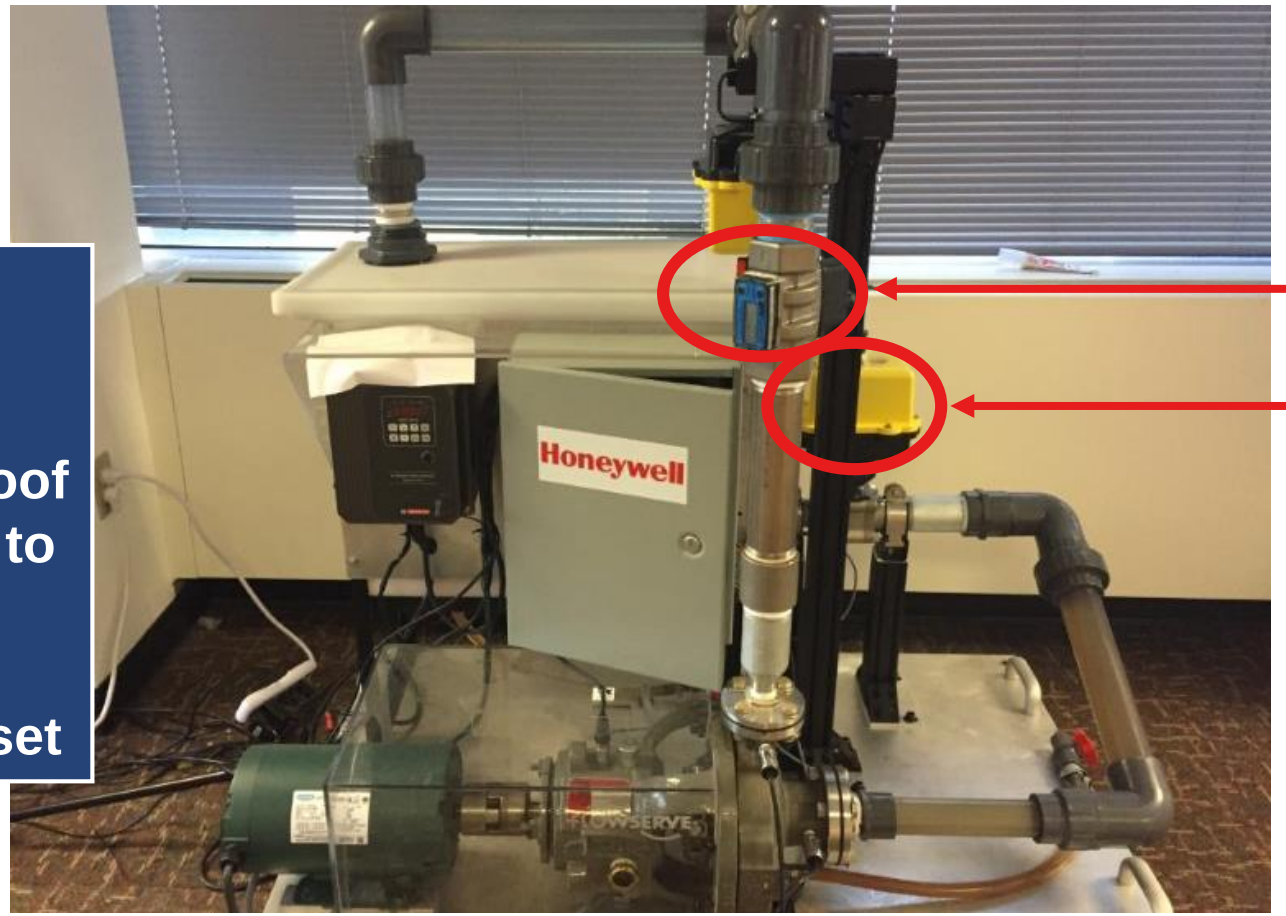


Root cause: Cavitation

Defending competent adversary

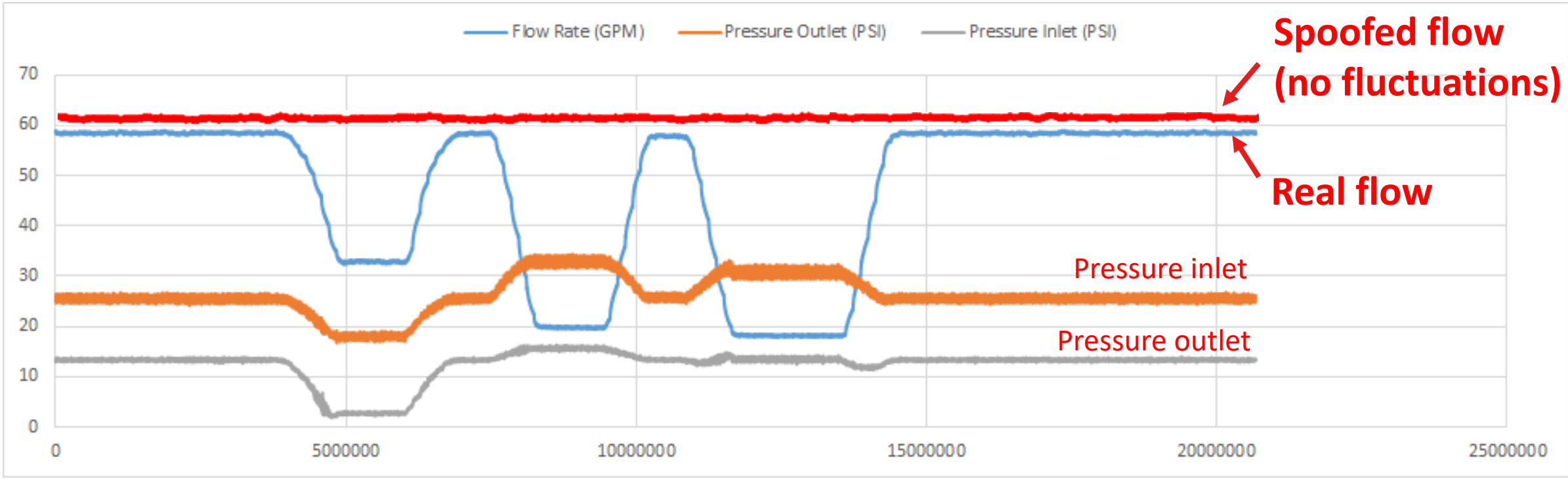
The attacker will spoof certain process values (sensor readings & actuators states) to avoid detection

Since pump damage doesn't happen instantaneously, the attacker will have to spoof certain process values to avoid detection by impeding root cause analysis of process upset



Defending competent adversary

The attacker will spoof sensor readings



FAQ: But how does one spoof process data?

Algorithm 1 Runs Analysis

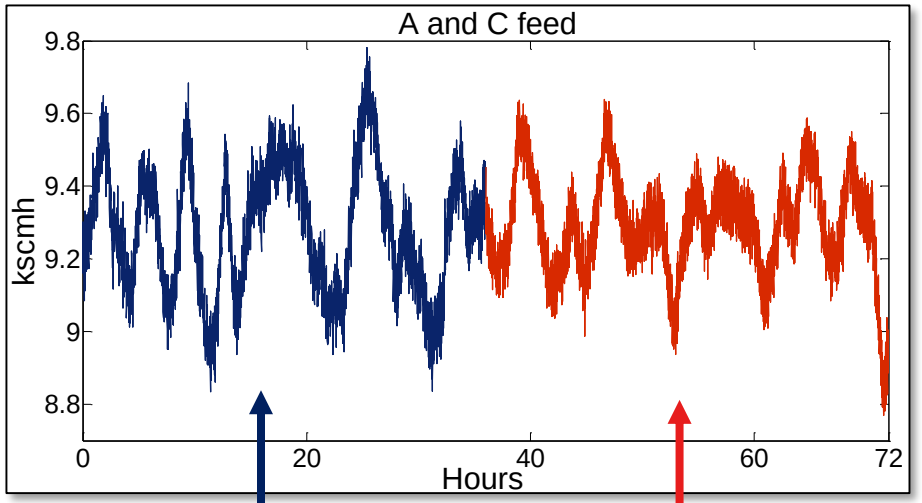
```
1: procedure EXPLORE                                   ▷ 1: analyse phase
2:     signal ← signal to analyse

3:     while not an end of signal do
4:         while moving up do
5:             runs++                                  ▷ count positives moves
6:             value = sum(changes)                    ▷ positive steps change
7:             if direction change then                ▷ save results
8:                 positivesruns(runs)++
9:                 positivesvalues(runs) = value
10:        while movi
11:            runs++
12:            value = s
13:            if directi
14:                negat
15:                negat
16:        if no change
17:            nils++
18:    return runs, va
```

Algorithm 2 Triangles

```
1: procedure EXPLORE                                   ▷ 1: analyse phase
2:     signal ← signal to analyse
3:     window ← learning window
4:     noiselvl ← noise parameter

5:     step = window * 10
6:     topslope = −999.99
7:     bottomslope = 999.99
8:     while not an end of signal do
9:         if first elements then
10:            current = value
11:            index = 1
12:        while index < window do                     ▷ learning phase of i−th bucket
13:            upperslope = (current − (last + noiselvl))/index
14:            lowerslope = (current − (last − noiselvl))/index
15:            if upperslope > topslope then
16:                topslope = upperslope
17:            if lowerslope < bottomslope then
```



Find X differences

(1) http://blackhat.com/docs/us-14/materials/us-14-Larsen-Miniturization.pdf

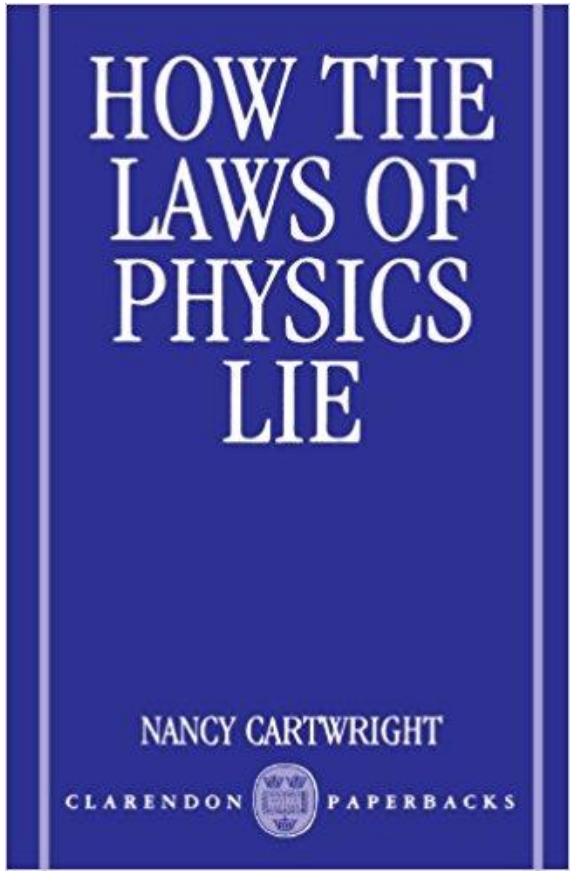
(2) https://conference.hitb.org/hitbsecconf2015ams/materials/D2T1%20-%20Marina%20Krotofil%20and%20Jason%20Larsen%20-%20Hacking%20Chemical%20Processes.pdf

Laws of physics

PHYSICS

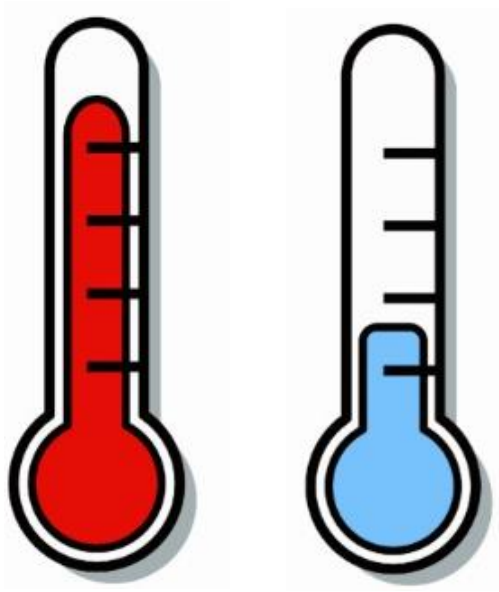
~~HIPS~~ DON'T LIE

Shakira

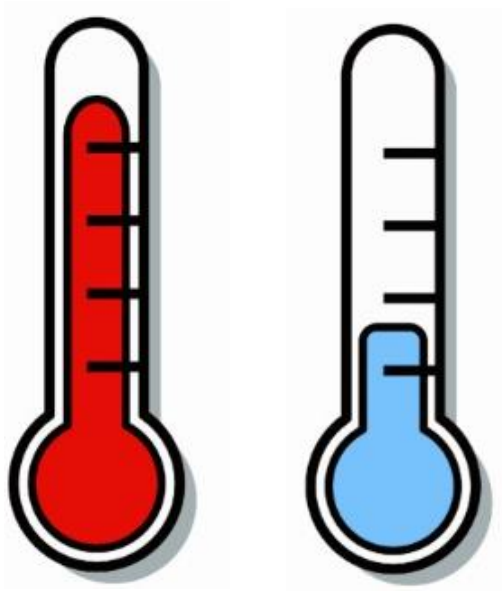


https://www.amazon.com/How-Laws-Physics-Nancy-Cartwright/dp/0198247044

Physical correlations



Physical correlations

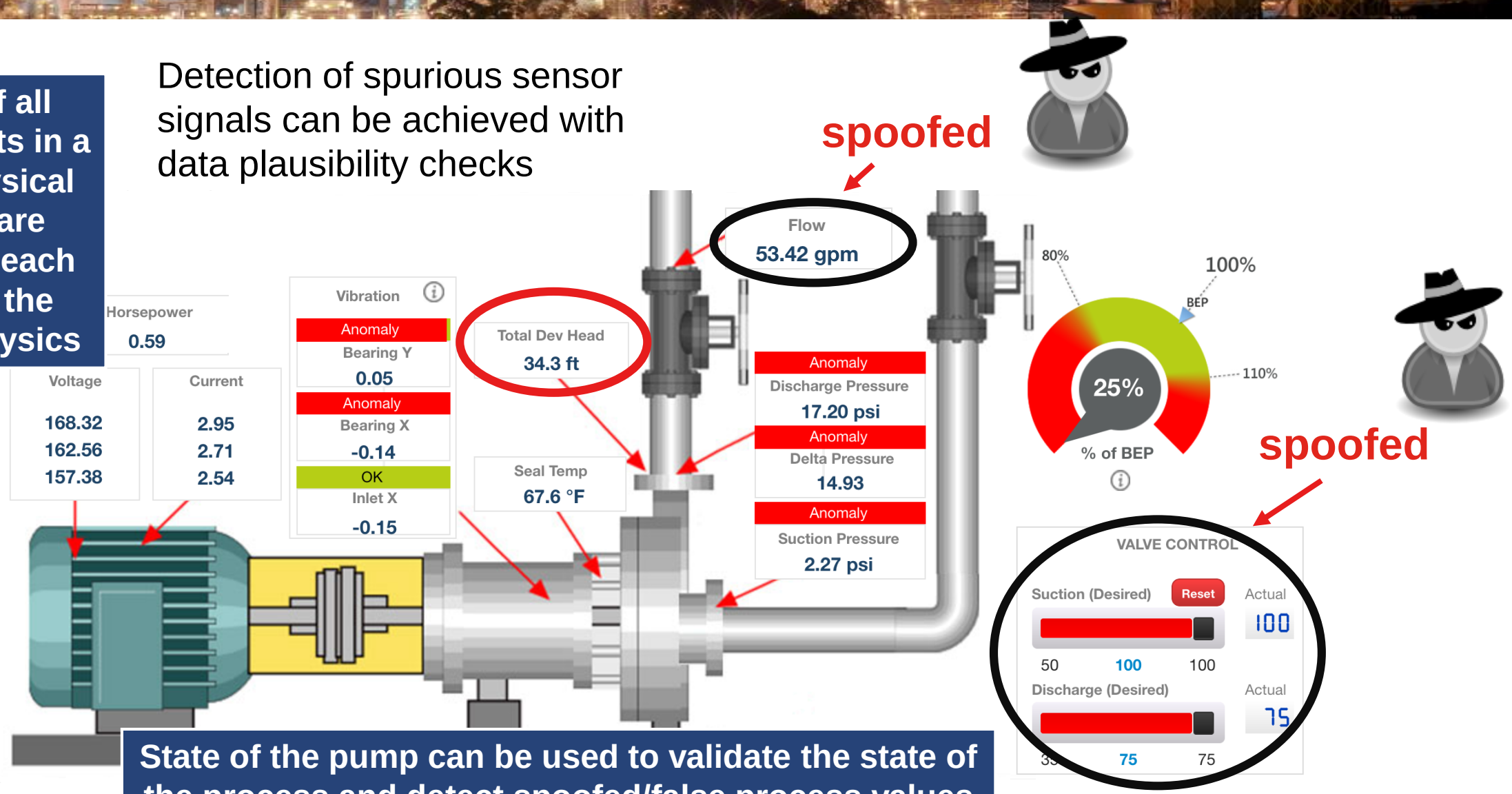


THIS DOES NOT MAKE SENSE

Detection of spurious sensor signals

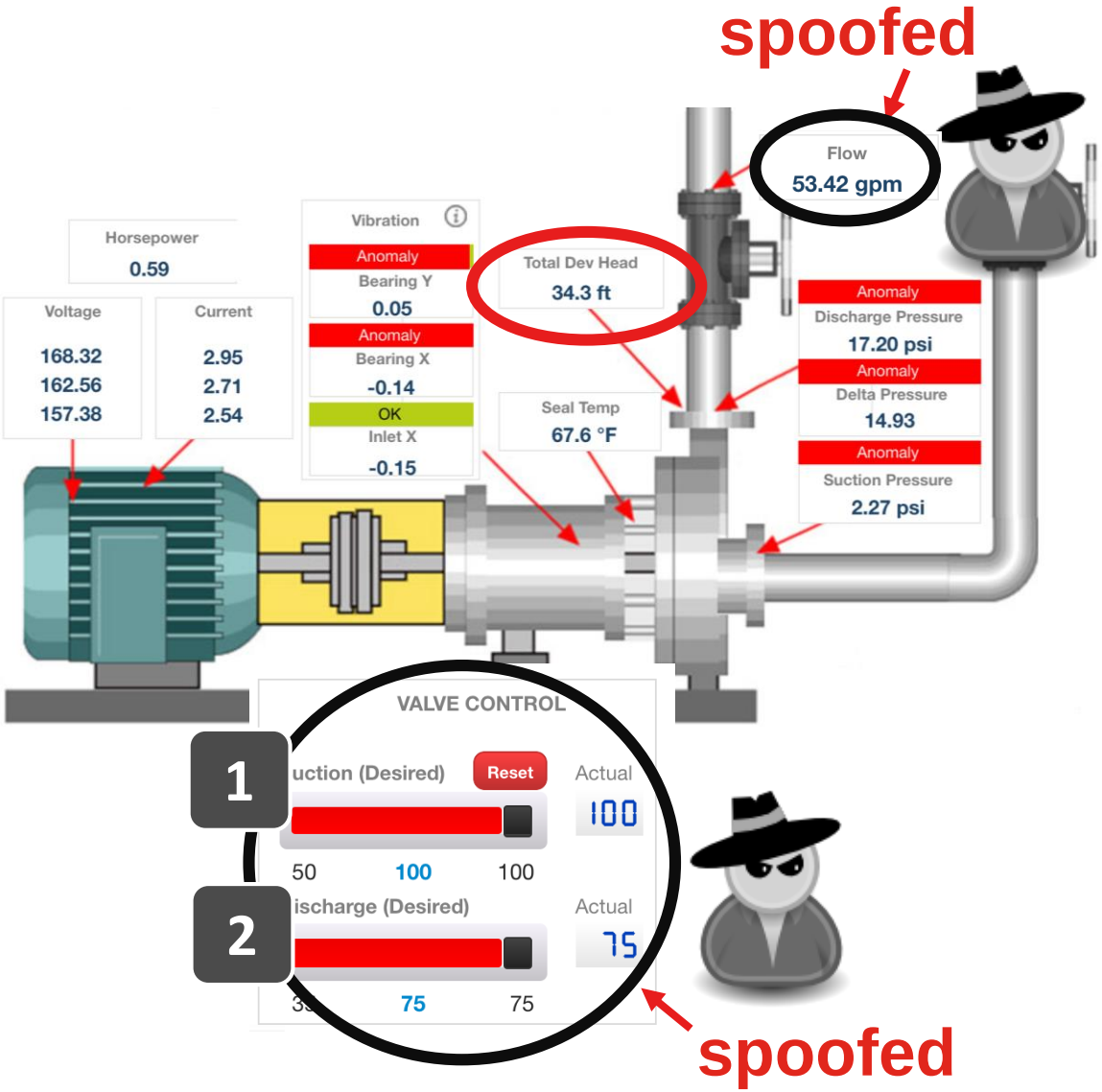
States of all components in a cyber-physical system are related to each other by the laws of physics

Detection of spurious sensor signals can be achieved with data plausibility checks



State of the pump can be used to validate the state of the process and detect spoofed/false process values

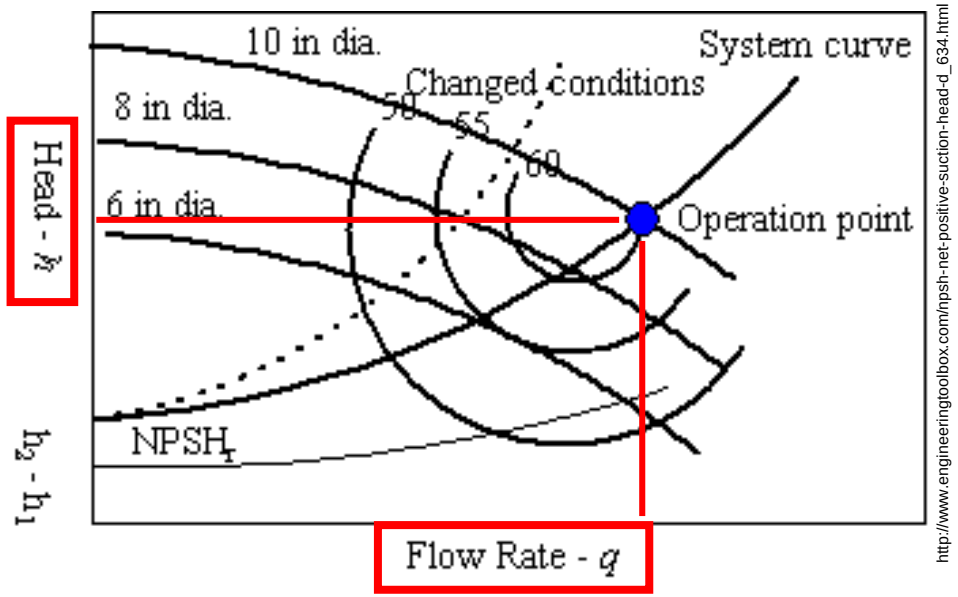
Verification of valve positions



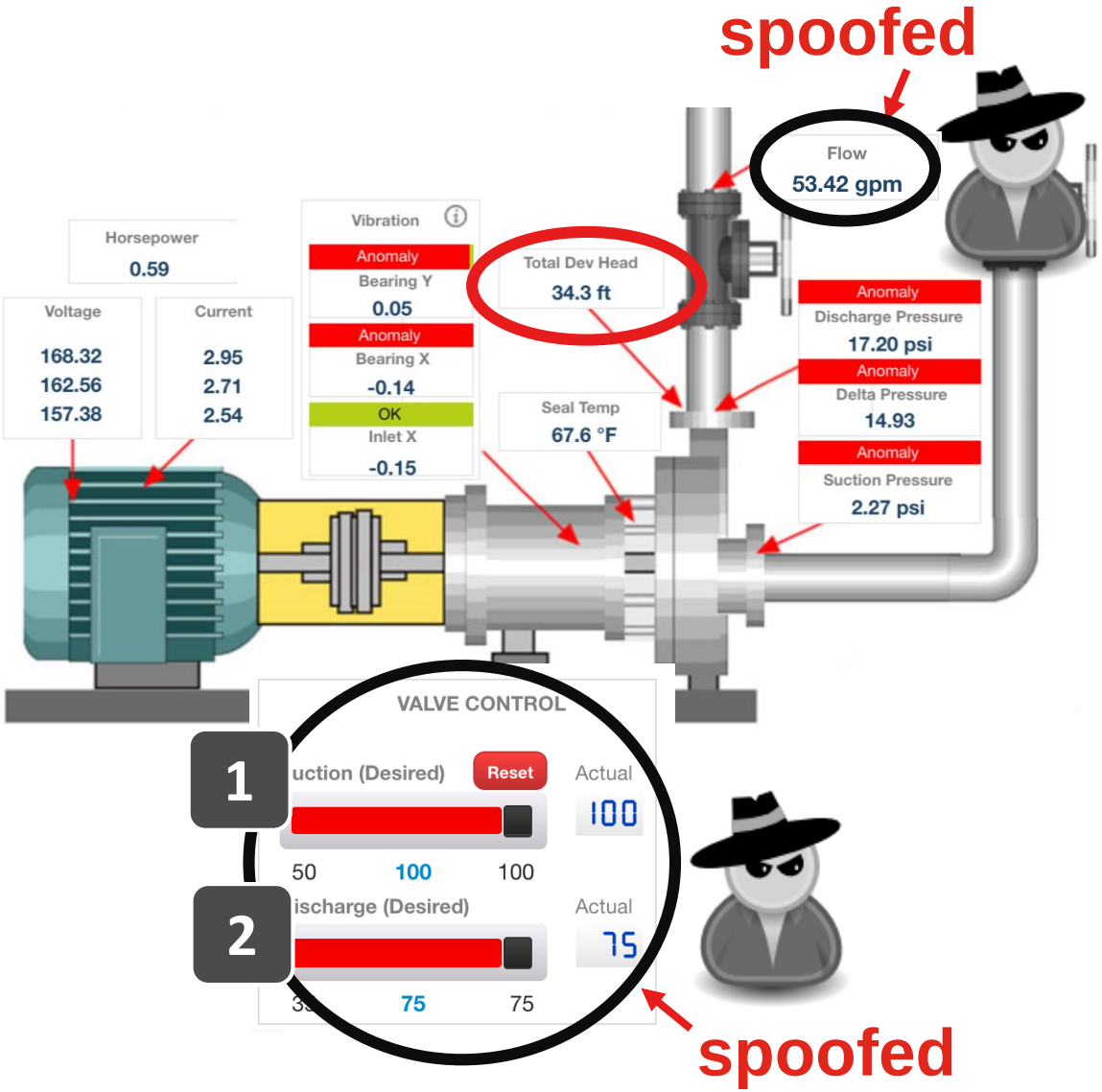
Curve of the demo pump would suggest:

Head 34,3 ft ~ flow 21-22 gpm

Flow reading **53,42 gpm** is implausible



Verification of valve positions



Curve of the demo pump would suggest:

Head 34,3 ft ~ flow 21-22 gpm

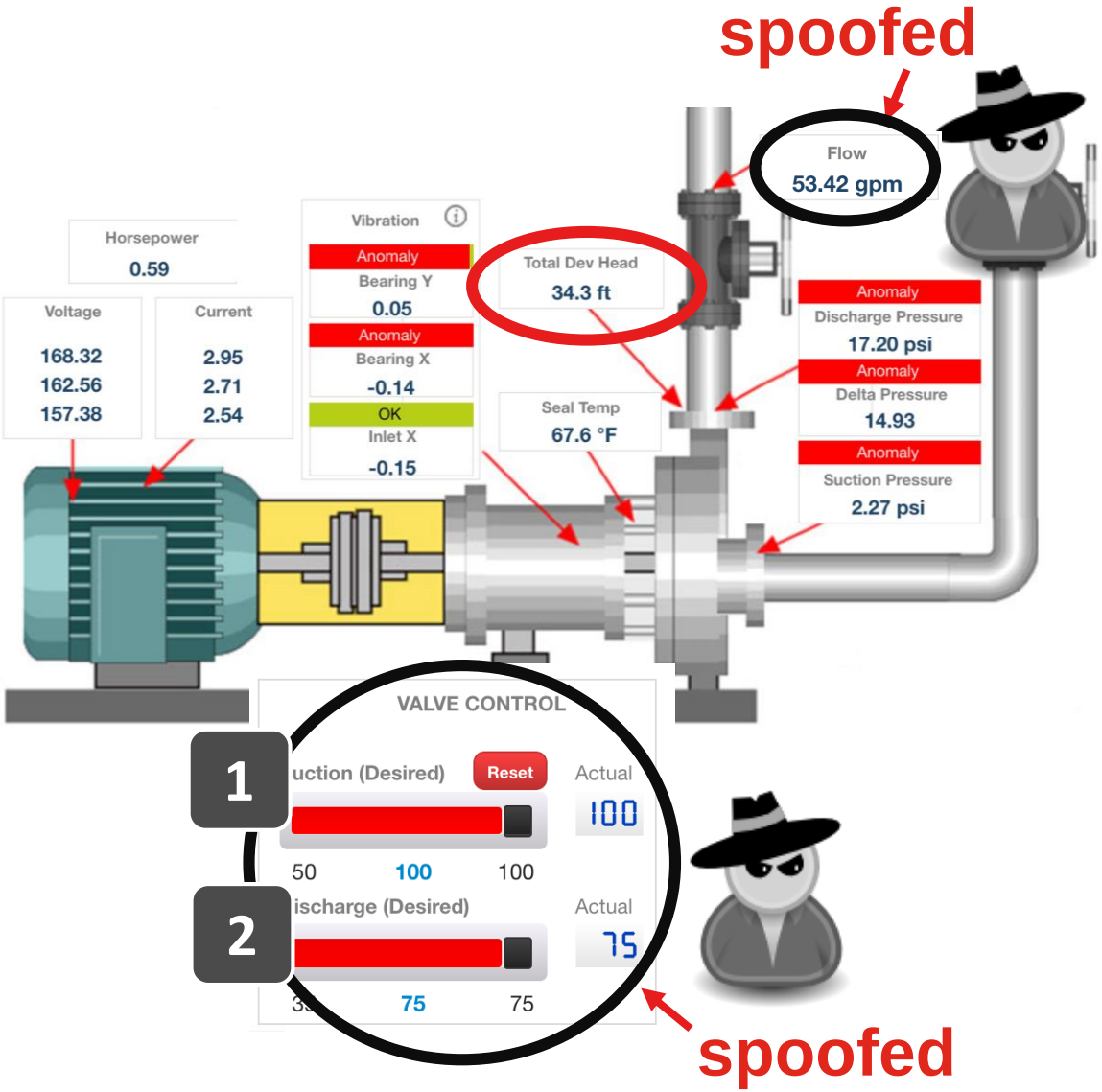
↓

We know that the flow is reduced

↓

Either of valve positioners is forged

Verification of valve positions



1

FAILURE PREDICTIONS

Bearing Failure	Impeller Failure	Mechanical Seal Failure
62 Days	6 Days	213 Days

Impeller stress

ROOT CAUSE

Cavitation

The suction valve is closed or obstructed. Pump is operating in sub optimal state and could cause mechanical failure

Root cause: Cavitation

2

FAILURE PREDICTIONS

Bearing Failure	Impeller Failure	Mechanical Seal Failure
5 Days	313 Days	10 Days

Mechanical stress

ROOT CAUSE

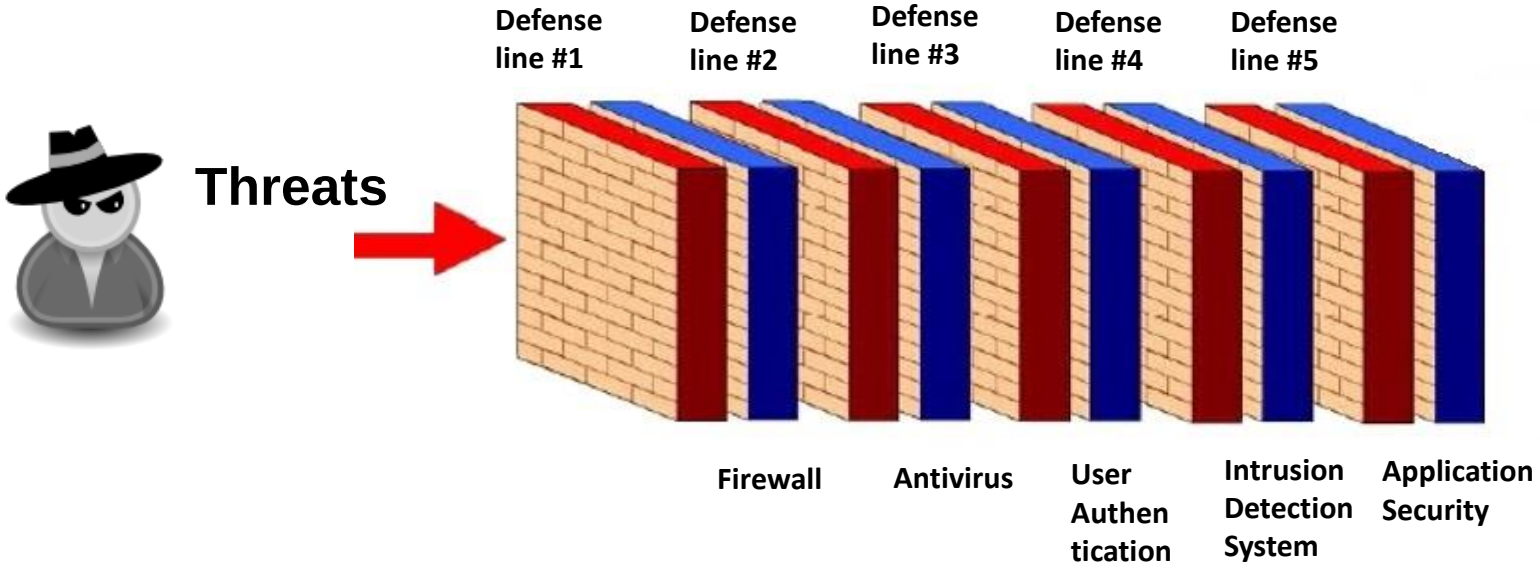
Low Flow

The discharge valve is closed or obstructed. Pump is operating in sub optimal state and could cause mechanical failure

Root cause: Low flow

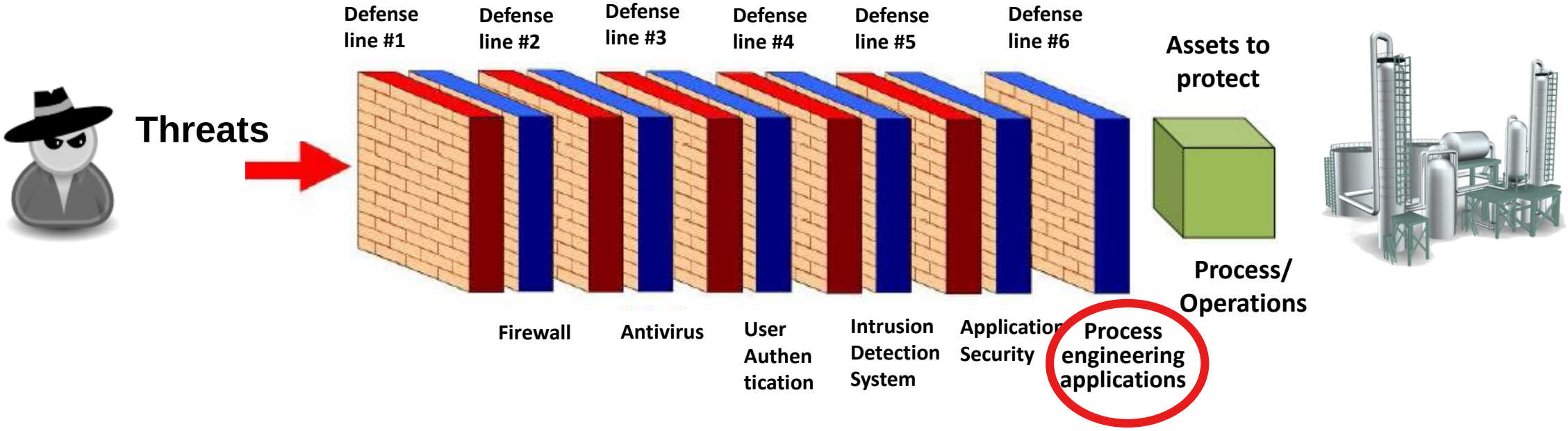
Defense in depth philosophy

- Defense in depth concept suggest multiple layers of security
  - If an attack causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect the system



Defense in depth philosophy

- Defense in depth concept suggest multiple layers of security
  - If an attack causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect the system



Detection with asset monitoring solutions

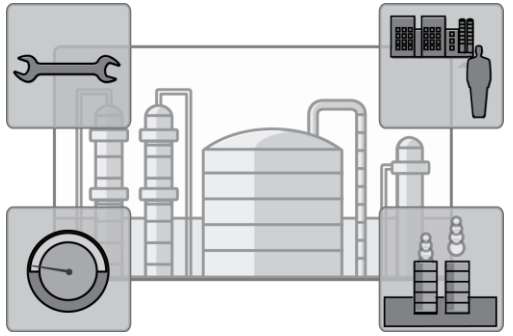
FAQ: So, Asset Monitoring solutions can detect cyber-physical attacks?

- NO. They provide us with data which can be used to extract information related to cyber-physical attacks detection
  - Process engineering (OT) security controls should be in place to detect and prevent unwanted/malicious process manipulations

Cyber-physical security

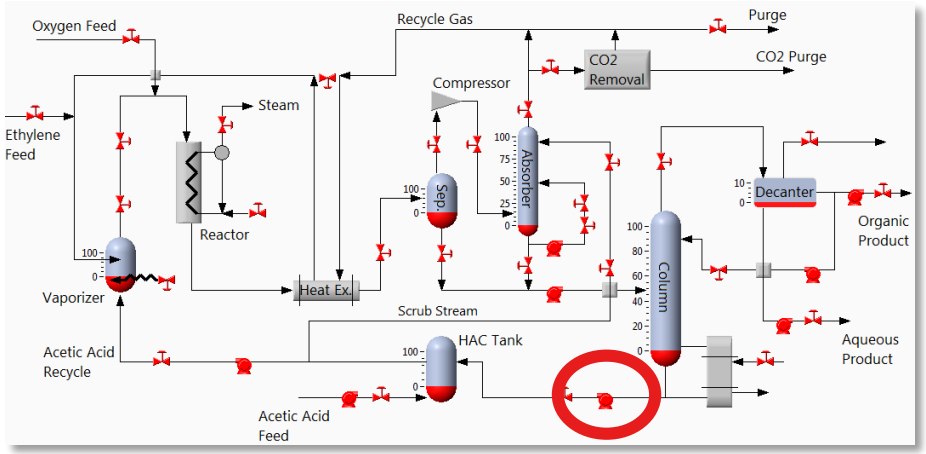
- In cyber-physical systems, physical process is a communication media for equipment and sub-systems
  - It can be leveraged for delivering attack payload (even to those assets which are not connected to the communication infrastructure)

- Equipment/Asset monitoring solutions are part of defense in depth strategy in cyber-physical systems
  - Malicious process upsets and spurious process values can be detected by the same approaches as natural upsets and faulty sensors



Cyber-physical research

- Is **VERY** resource-demanding
  - The cost of this (very) simple demo rig is $50k (yap)
  - It weights 610 lbs (276 kg)
  - Multitudinous support personnel
  - Troubleshooting takes long hours and weeks ($$ of man hours)



Demo rig

- **UBSOLUTELY needed for anticipation of future threats**
  - Better understanding work and hurdles of the attacker
  - To develop workable defenses (by the time they will be needed)

Q & A

Marina Krotofil
@marmusha
marmusha@gmail.com