black hat®
USA 2017

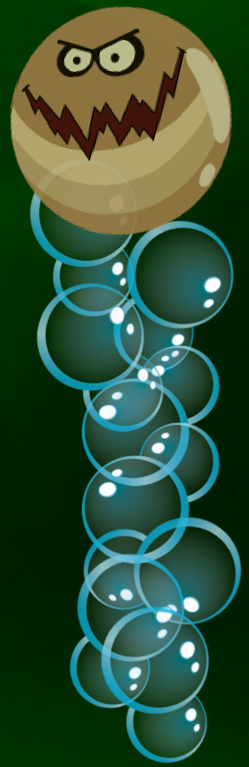
JULY 22-27, 2017
MANDALAY BAY / LAS VEGAS

EVIL BUBBLES

or

How to Deliver Attack Payload via the Physics of the Process

(and How to Defend against such Attacks)



Marina Krotofil

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)

Captain, we’re cavitating! He can hear us!

In this talk we will learn

❑ How to deliver attack payload over the physics of the process

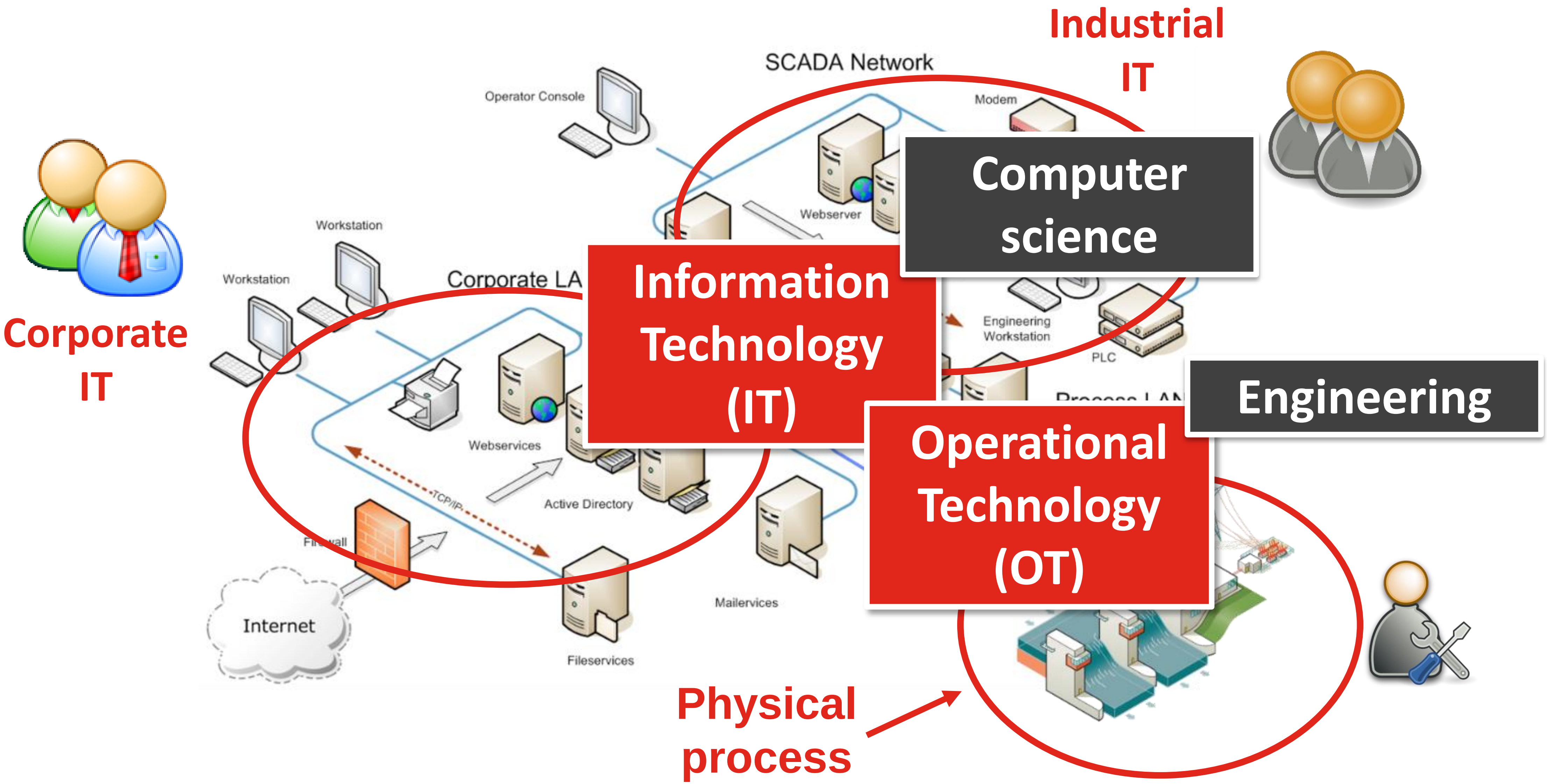
❑ How to use bubbles to cause physical destruction

❑ How to detect ongoing cavitation before equipment breaks

❑ Whether the attacker is that almighty (as many think)

Motivation for this talk

Industrial Control Systems



Industrial IT

Computer science

Corporate IT

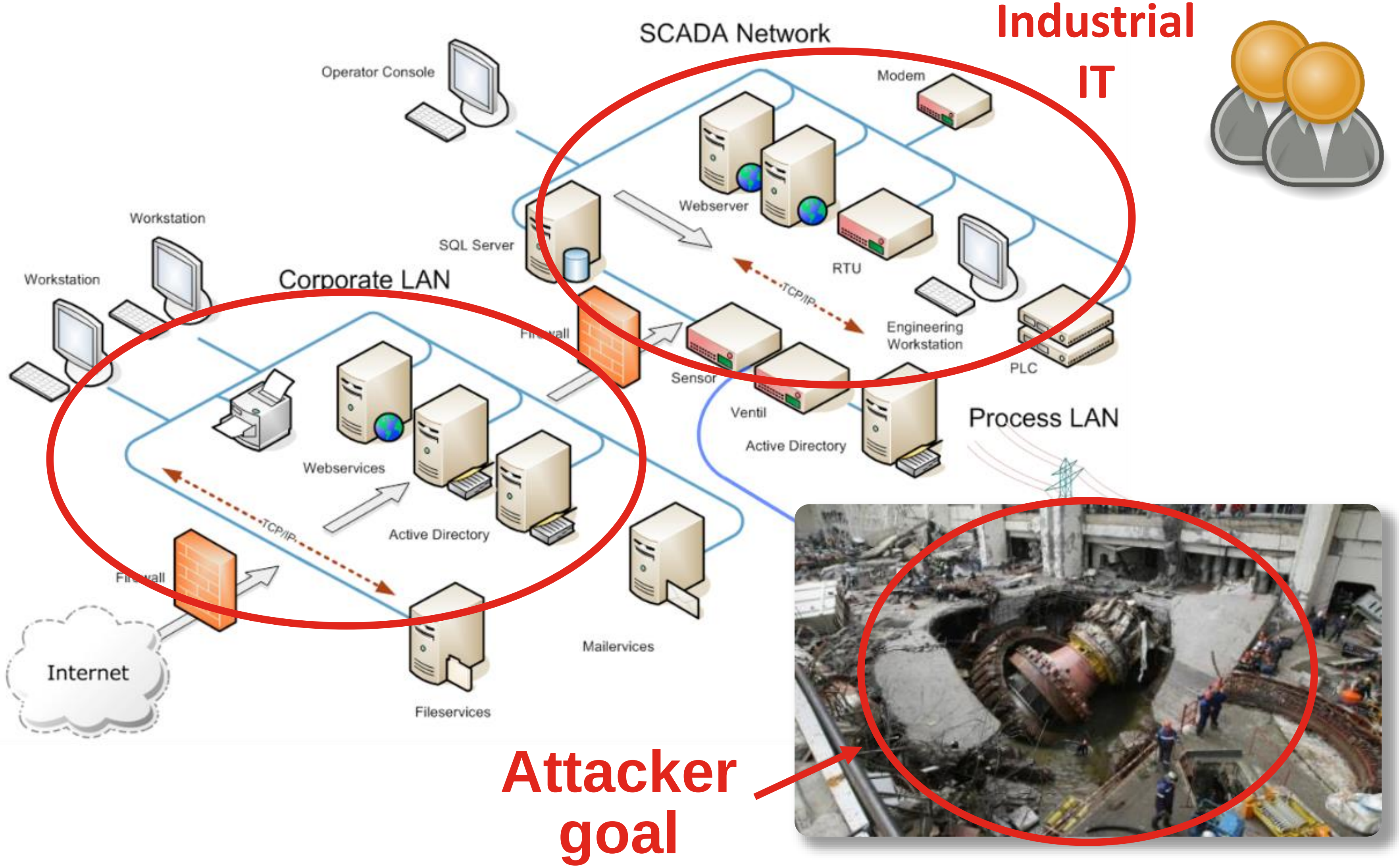
Information Technology (IT)

Engineering

Operational Technology (OT)

Physical process

Industrial Control Systems

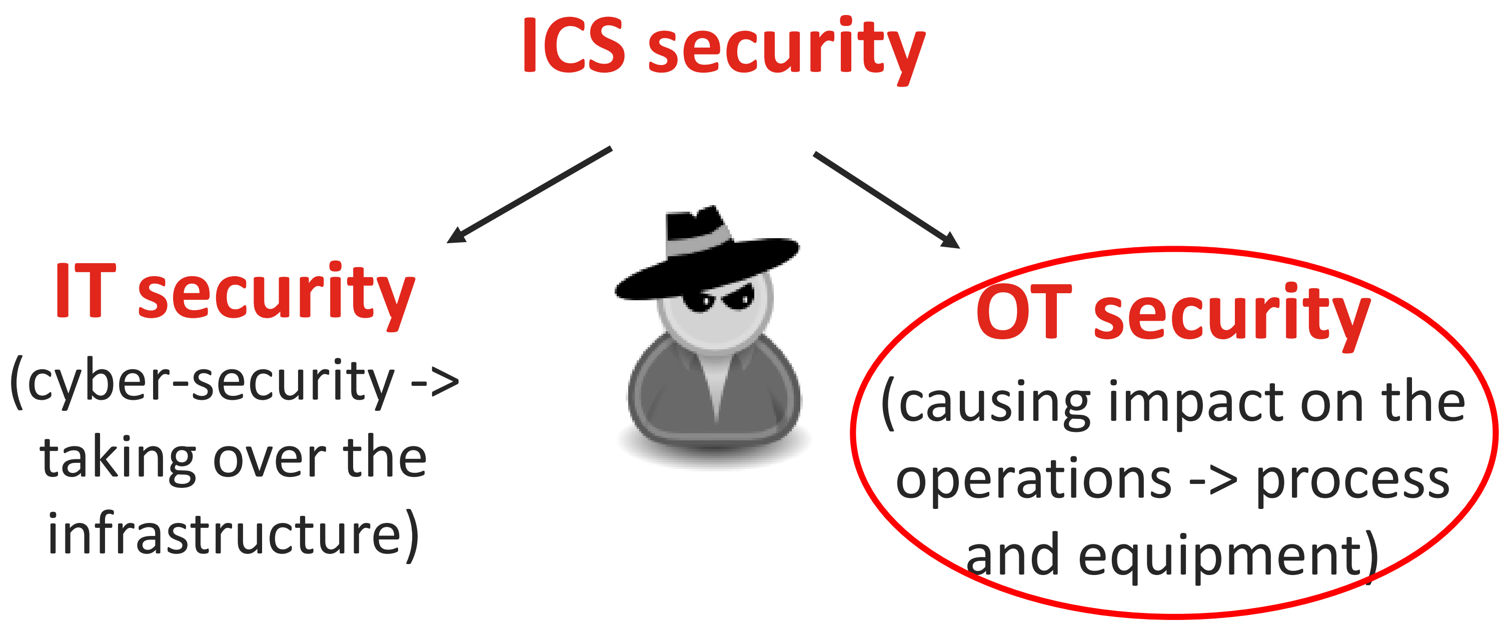


Corporate IT

Industrial IT

Attacker goal

IT security vs. OT security



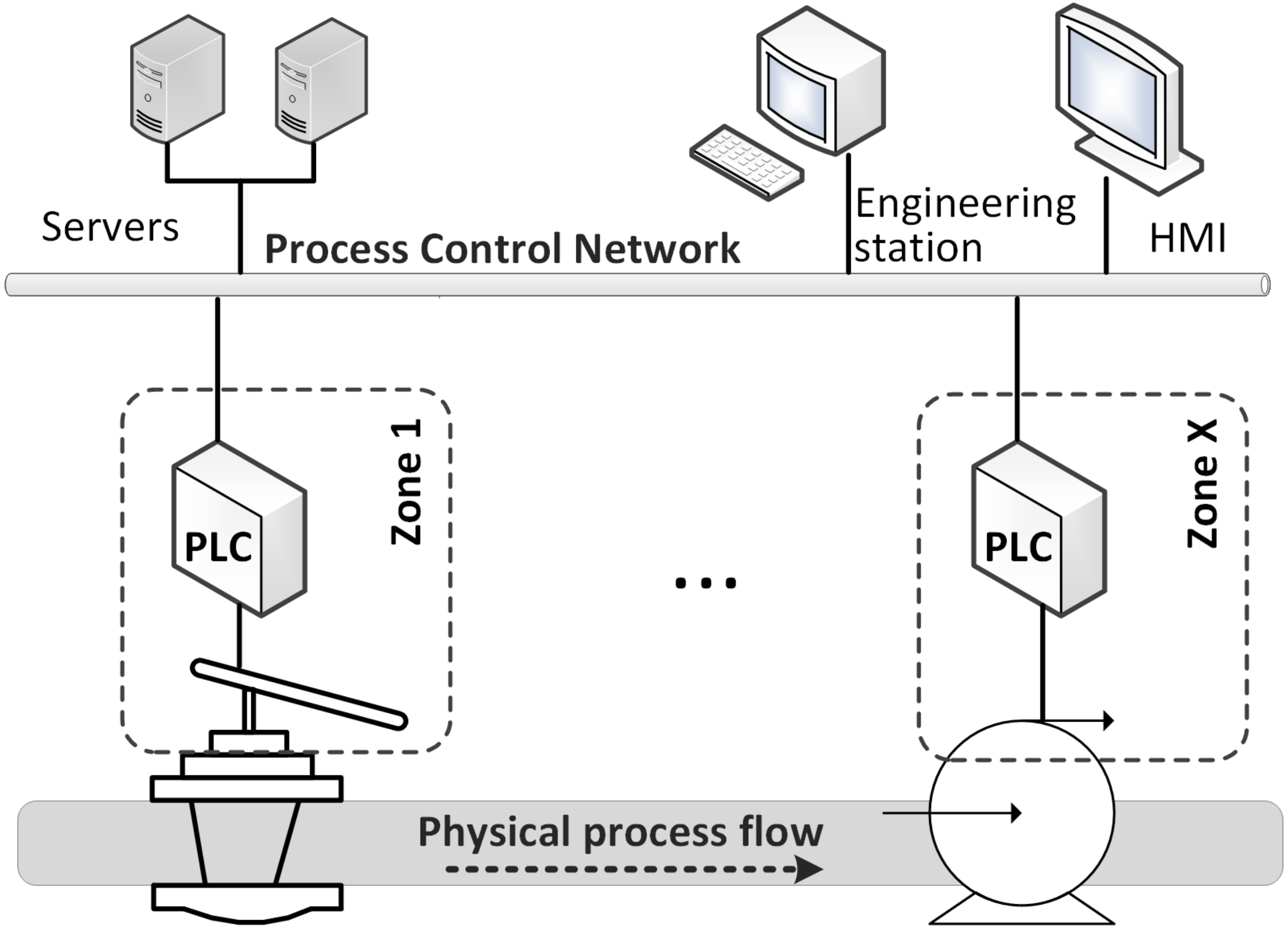
ICS security

IT security
(cyber-security -> taking over the infrastructure)

OT security
(causing impact on the operations -> process and equipment)

Focus of the talk

IEC 62443-1-1 standard

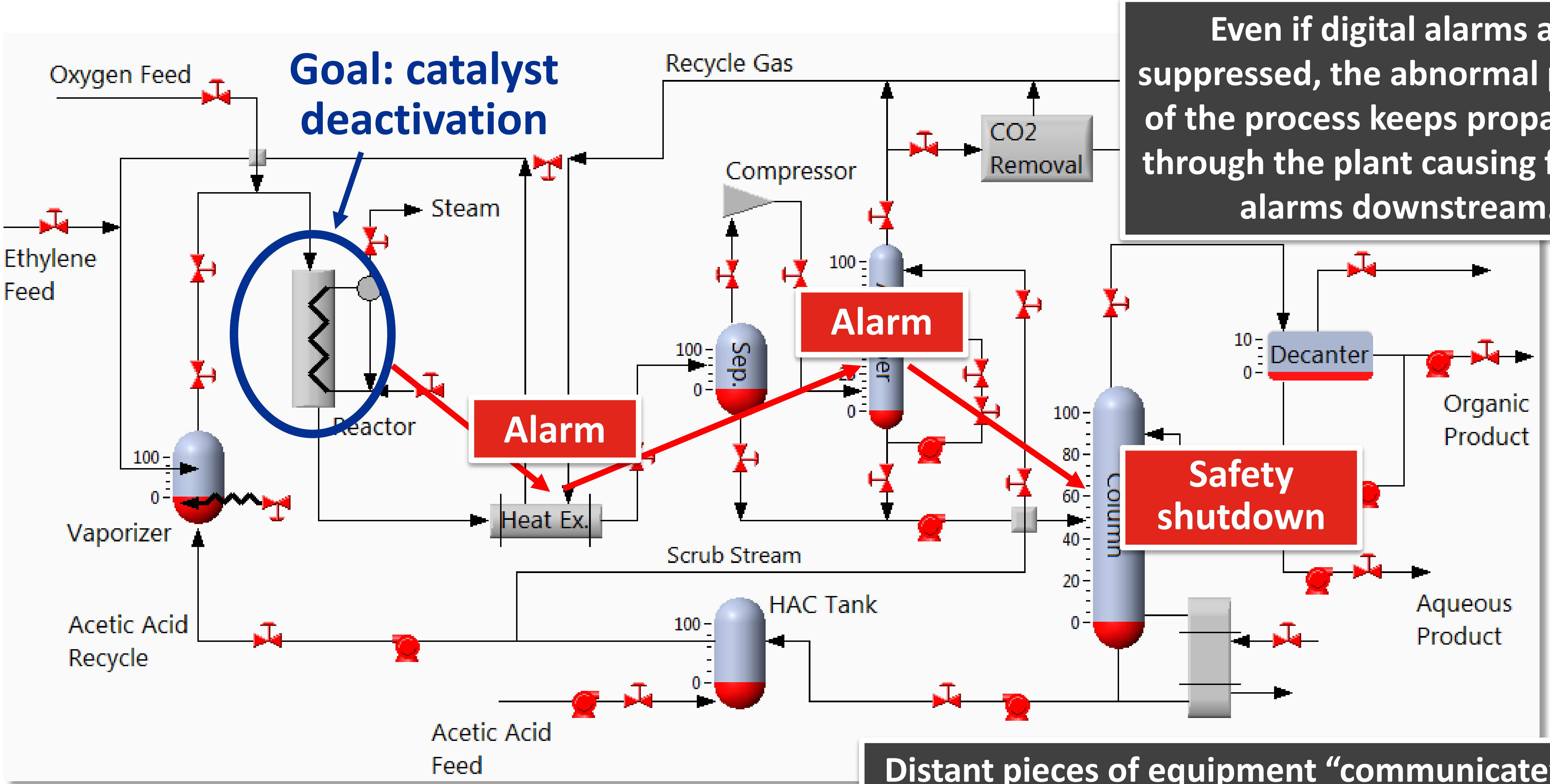


My Black Hat talk back in 2015

Source: simentari.com

Attack goal: persistent economic damage

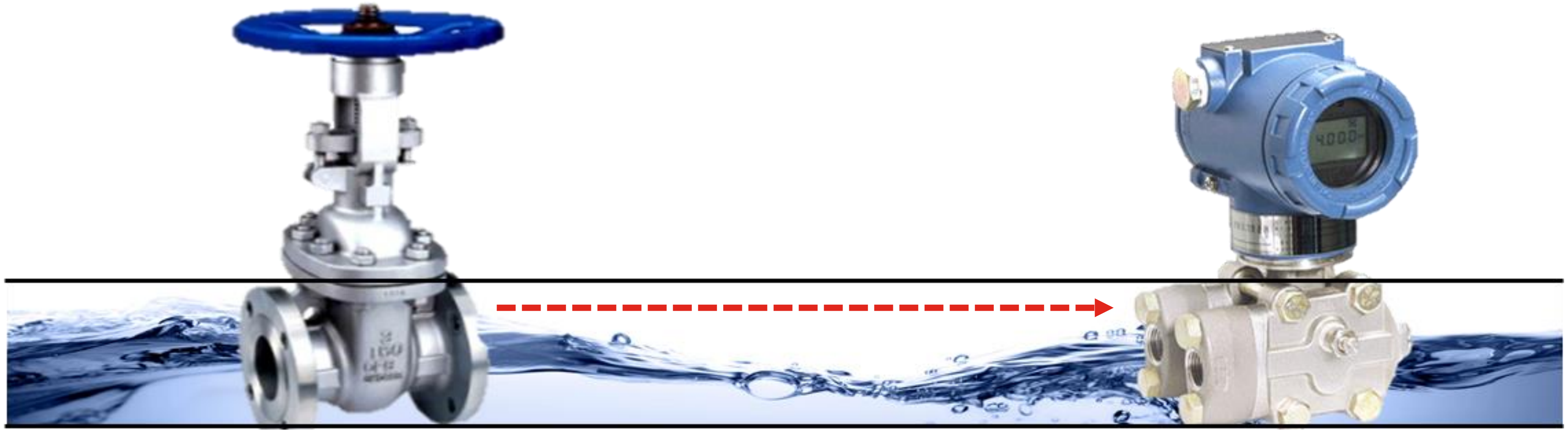
Failed scenario: Alarm and physics propagation



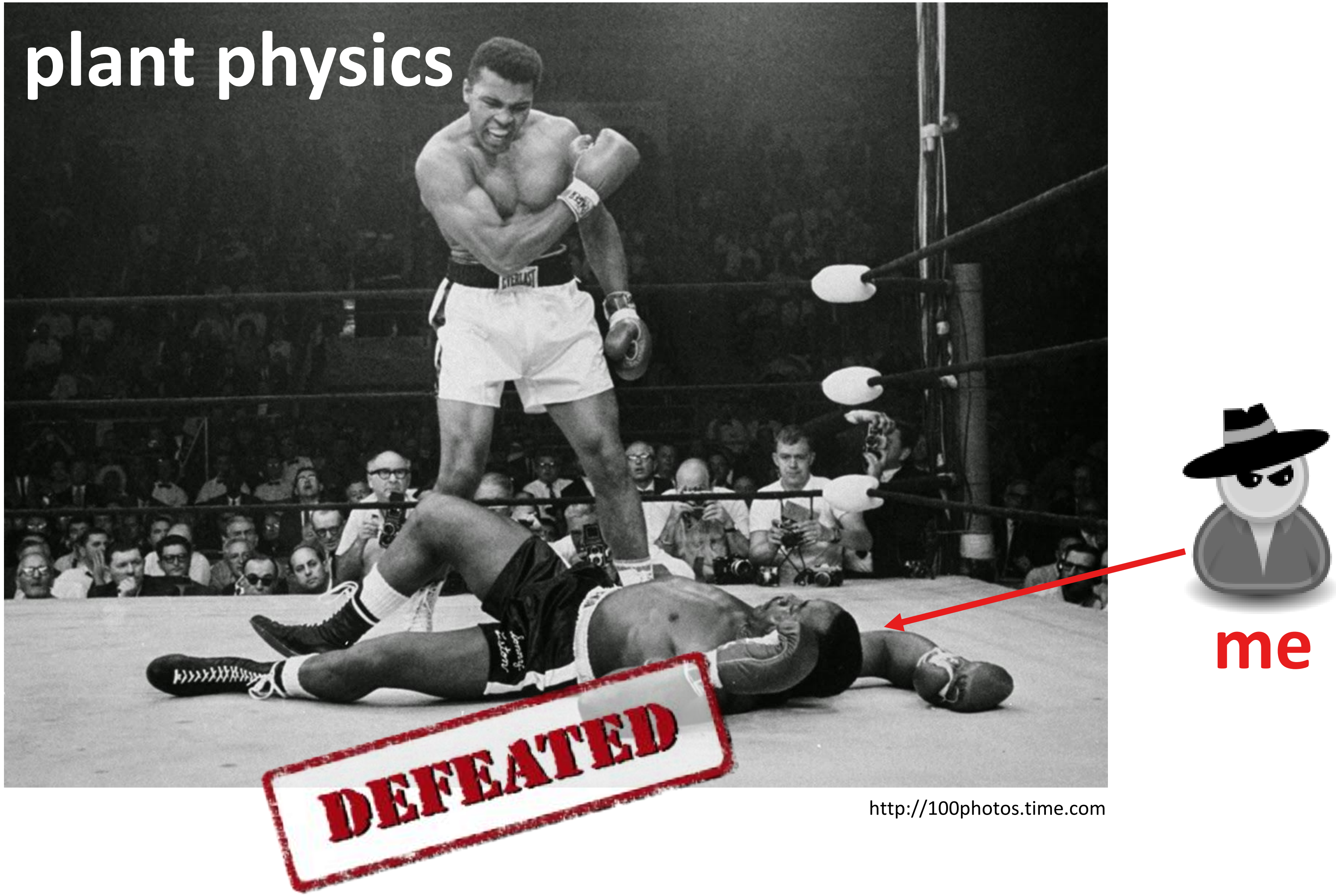
Even if digital alarms are suppressed, the abnormal physics of the process keeps propagating through the plant causing further alarms downstream.

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

Point (1): Physical process is a communication media



Process Physics vs. Attacker



http://100photos.time.com

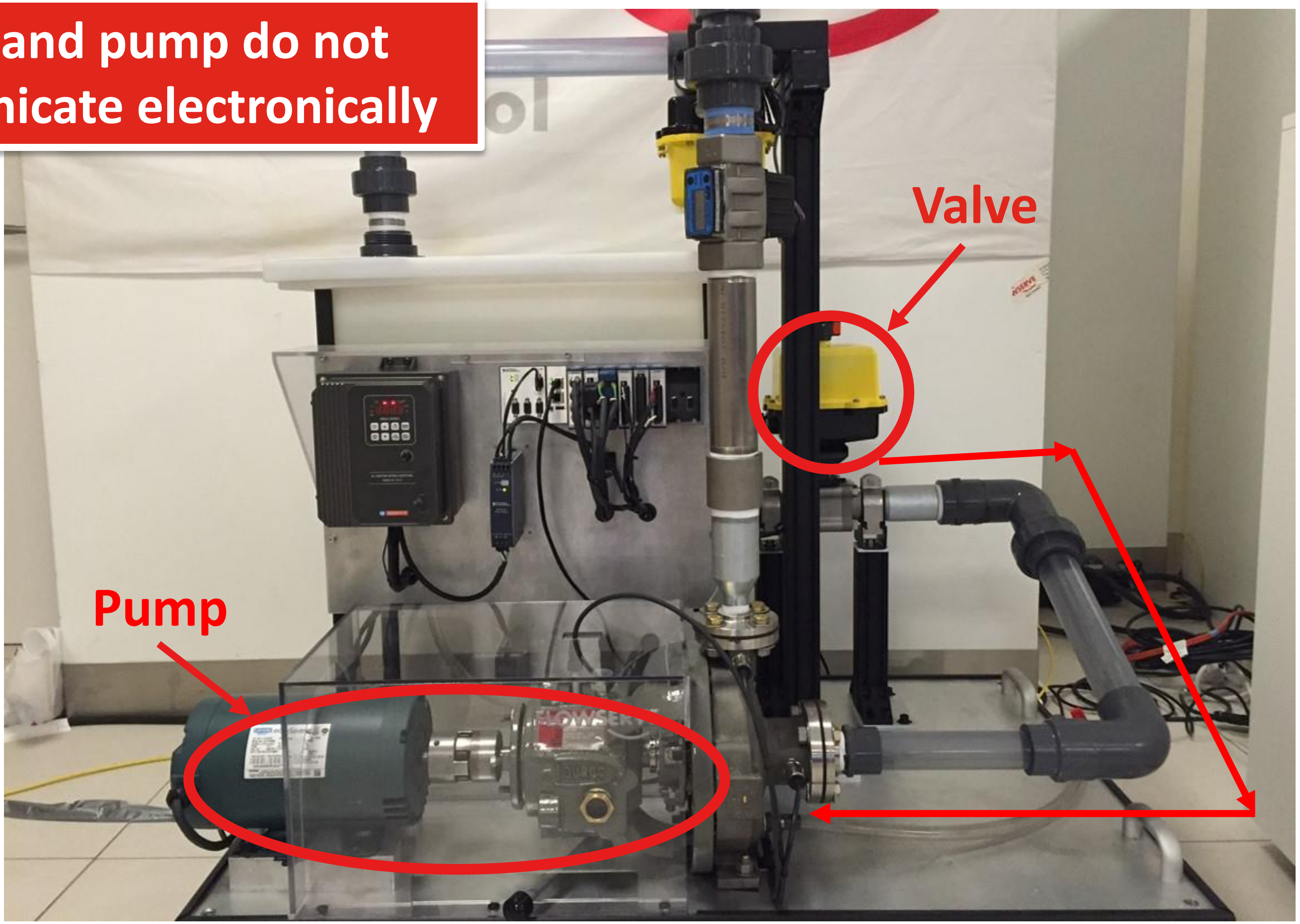
I felt very angry

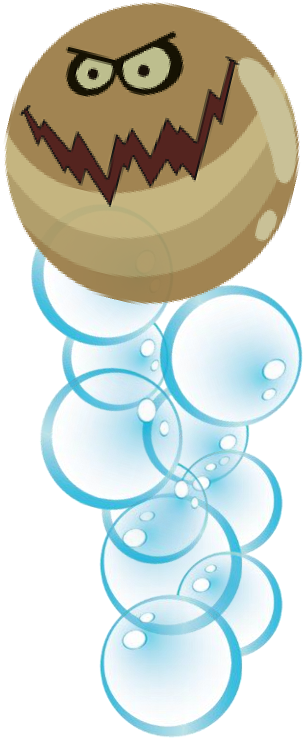
The attacker always wants to win!

http://100photos.time.com

Novel attack vector: Delivery of attack payload via process physics

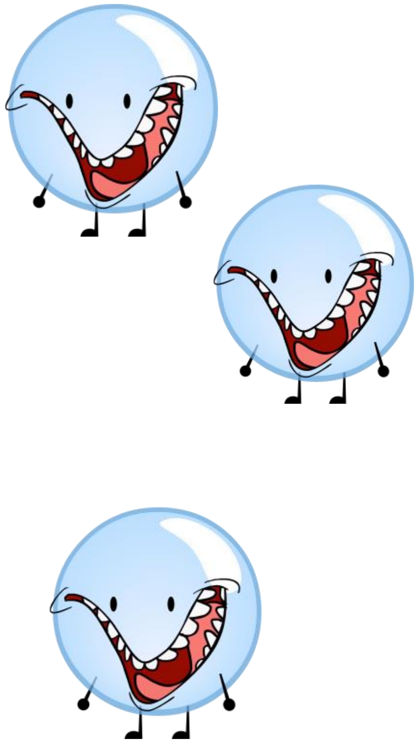
Valve and pump do not communicate electronically





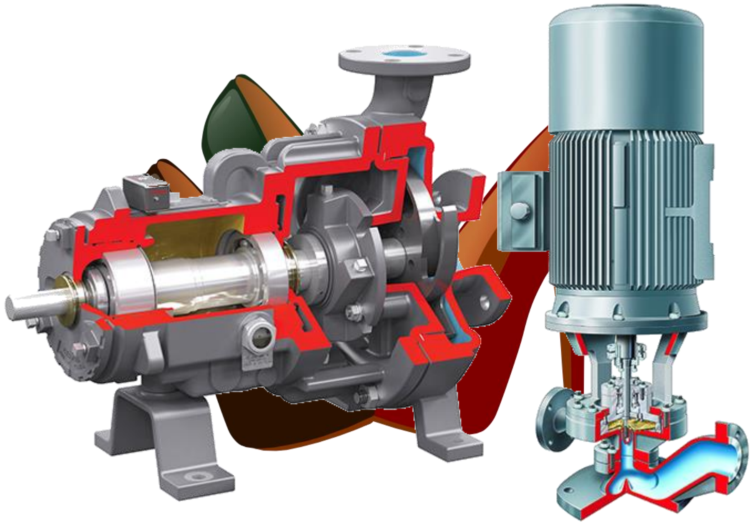
Evil Bubbles

Attack payload propagation



Evil Bubbles

Pumps

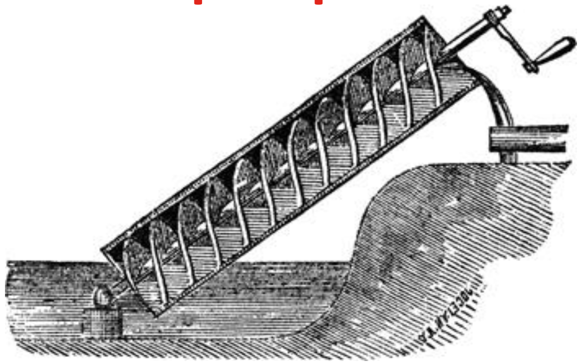


Function of the pump

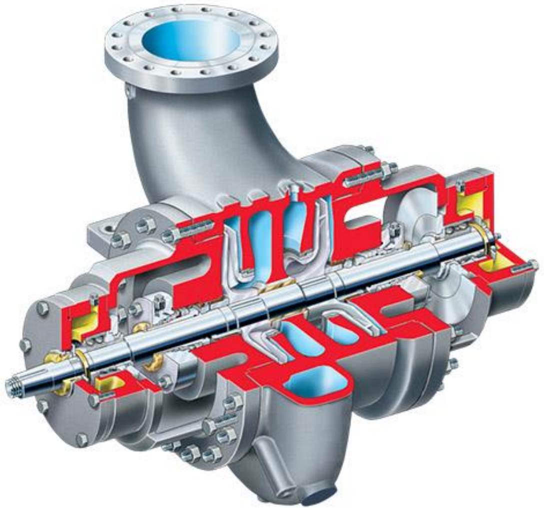
A piece of equipment which <u>elevates</u> or <u>moves liquids</u> at the expense of power input

- ❑ Our current lifestyle would not be possible without pumps
  - From air conditioning to pumping oil, from cutting steel 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

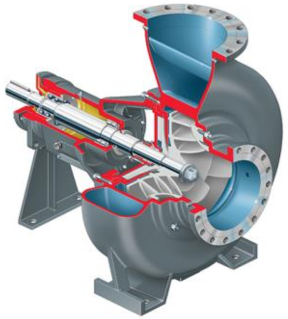


Types of pumps

COLOSSAL

humble

VS.

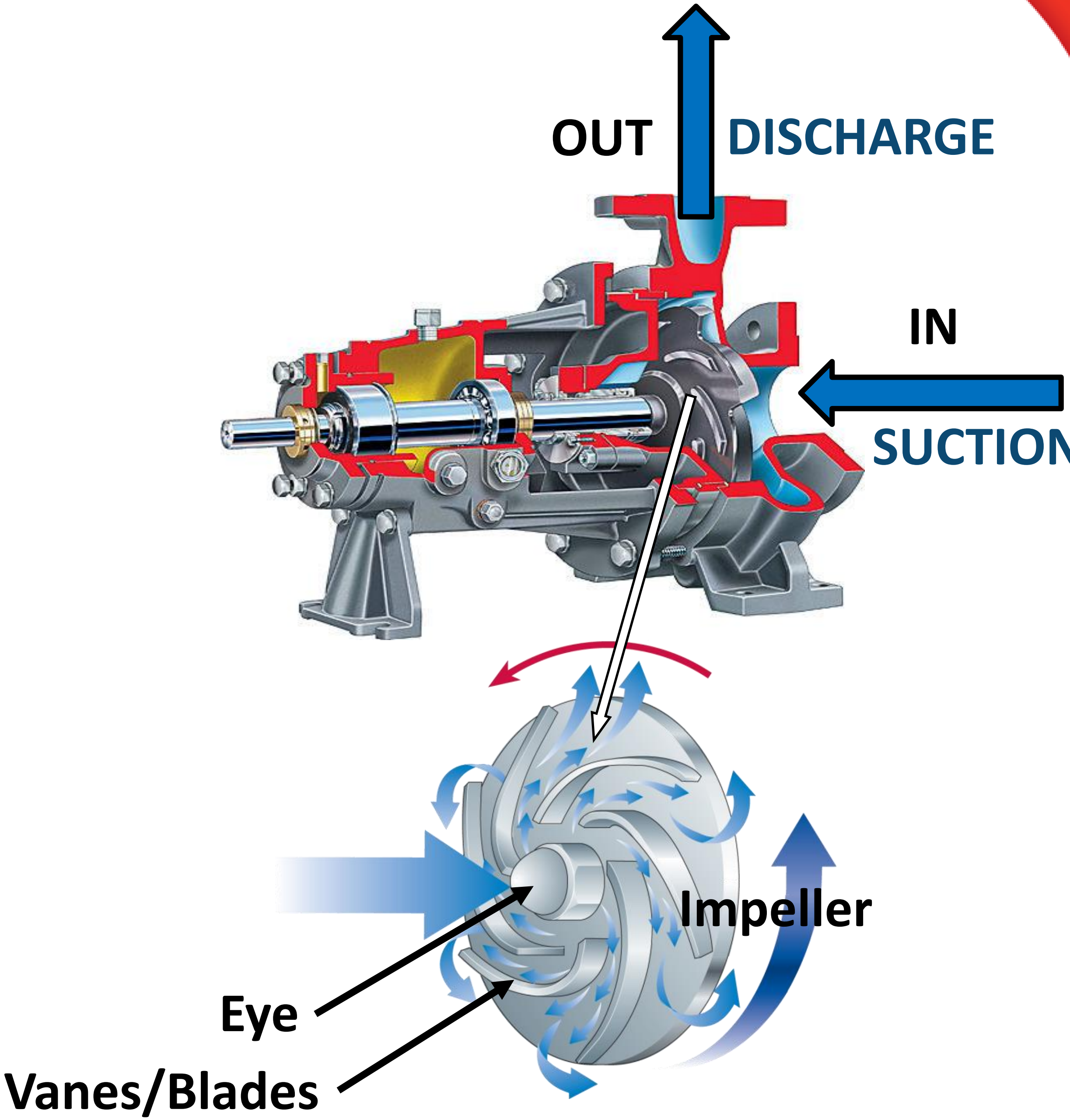


Expensive. Heavy. Sensitive to incorrect operation -> instrumented for health/safety monitoring

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

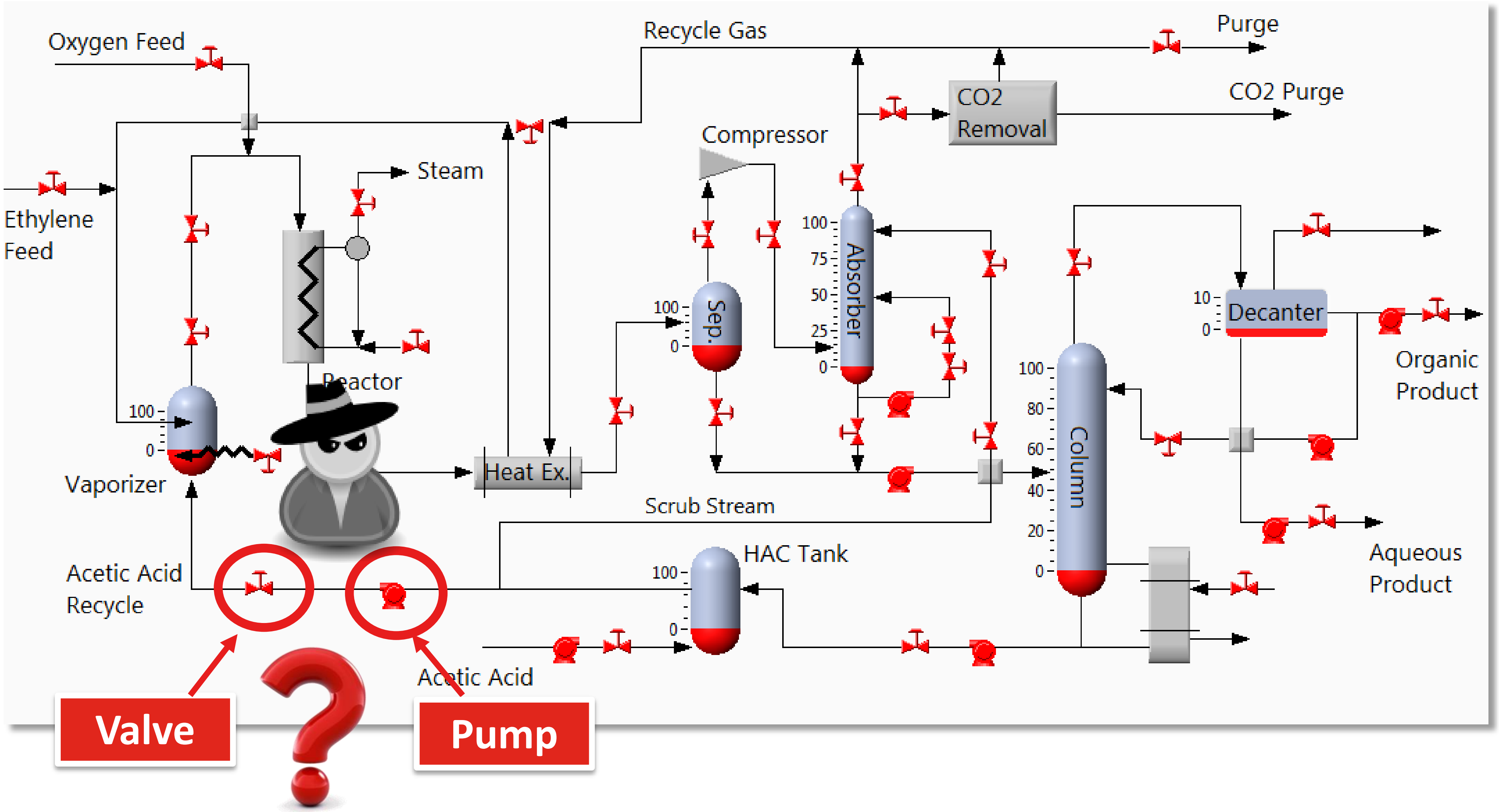
Centrifugal pump

- 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



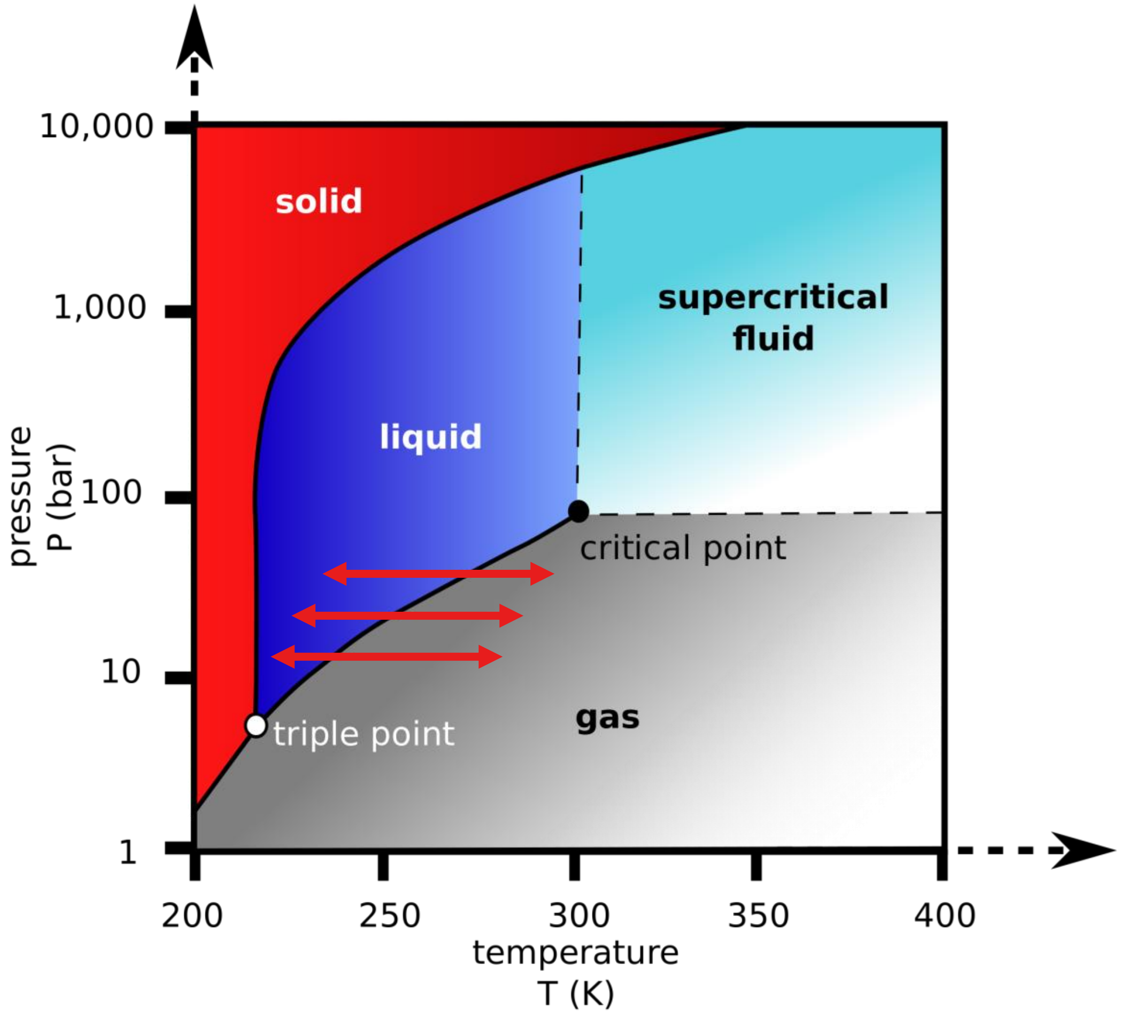
http://dairyprocessinghandbook.com/chapter/pumps

Is it a target worth the effort?



Cavitation

States of physical substances



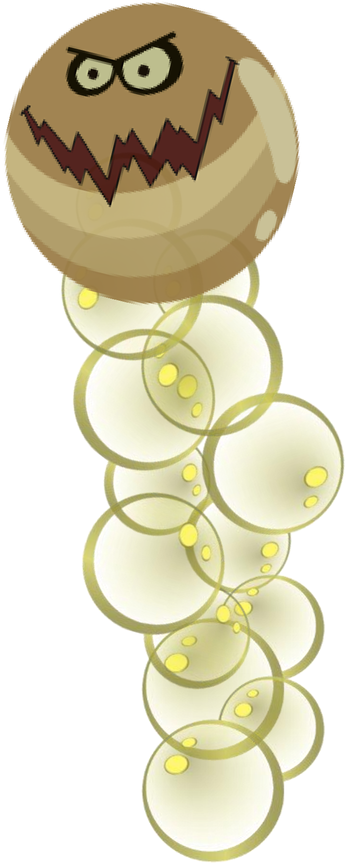
Carbon dioxide pressure-temperature phase diagram

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

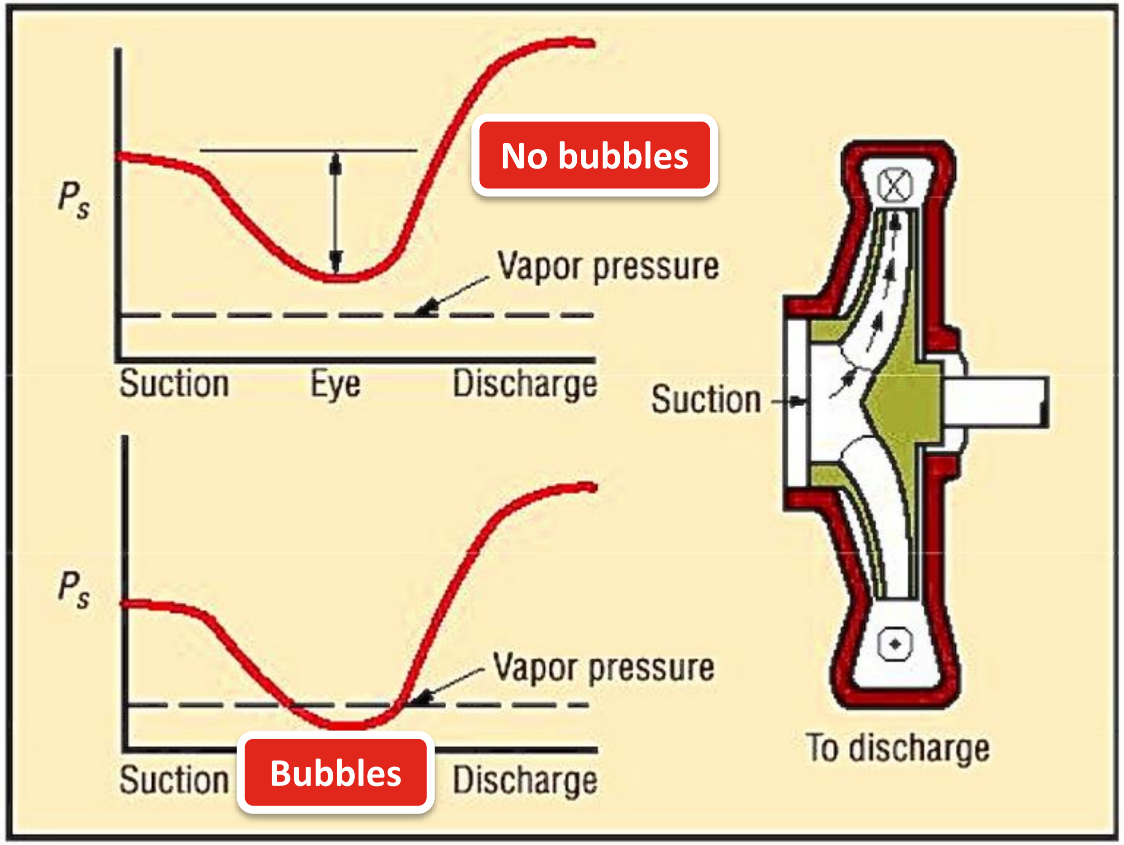
- If the pressure of the substance drops or its temperature increases, it begins to vaporize, just like boiling water

-> formation of bubbles :-)

The bubbles we all like



Pump cavitation

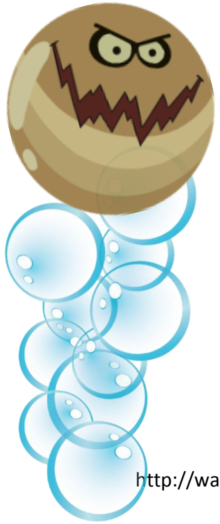


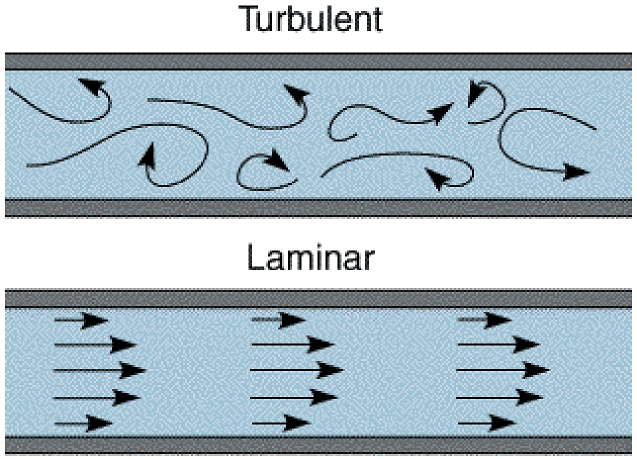
http://jmpcoblog.com/hvac-blog/how-to-read-a-pump-curve-part-2

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

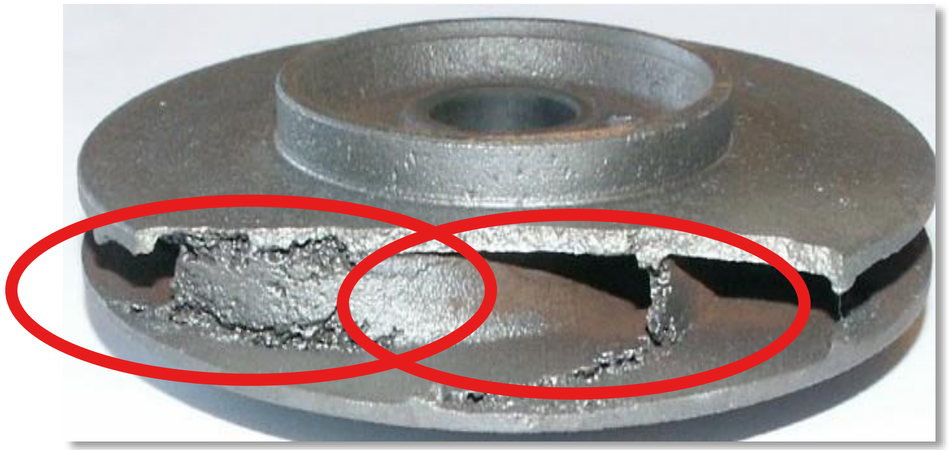
- ❑ Cavitation occurs when the pressure in the suction line is too low relative to the vapor pressure of the pumped liquid
- ❑ The pressure increases as the liquid flows further into impeller causing bubbles to condense (implode) very rapidly
- ❑ The vapor bubbles collapse at a very high [velocity &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

Damaging effect of cavitation





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



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

1 Reduced efficiency

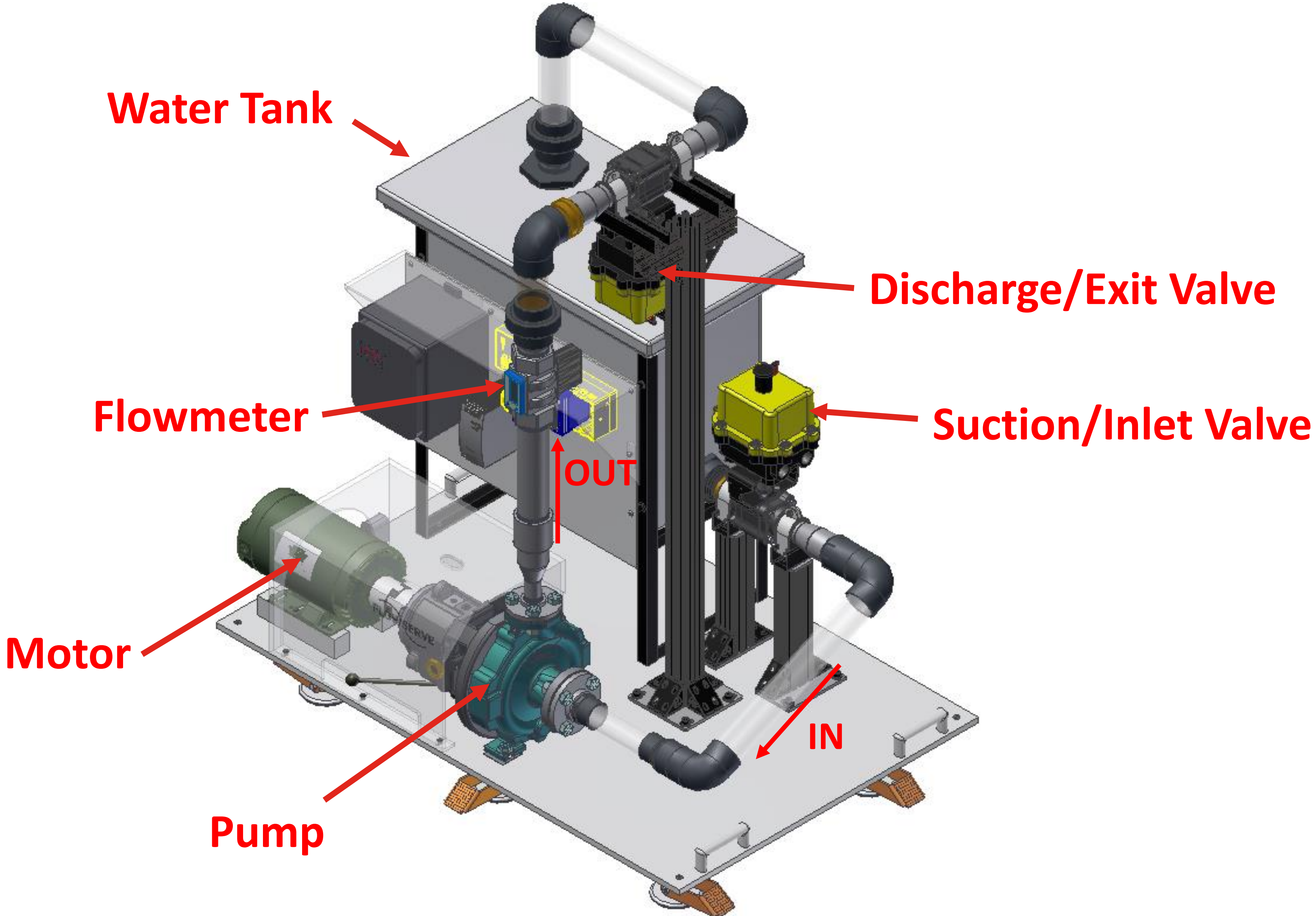
- □ All pumps require a smooth, regular symmetrical inlet flow profile for efficient operation
- □ The collapse of gas bubbles leads to the development of fast turbulent streams -> reducing efficiency up to inability to pump

2 Premature failure of the pump

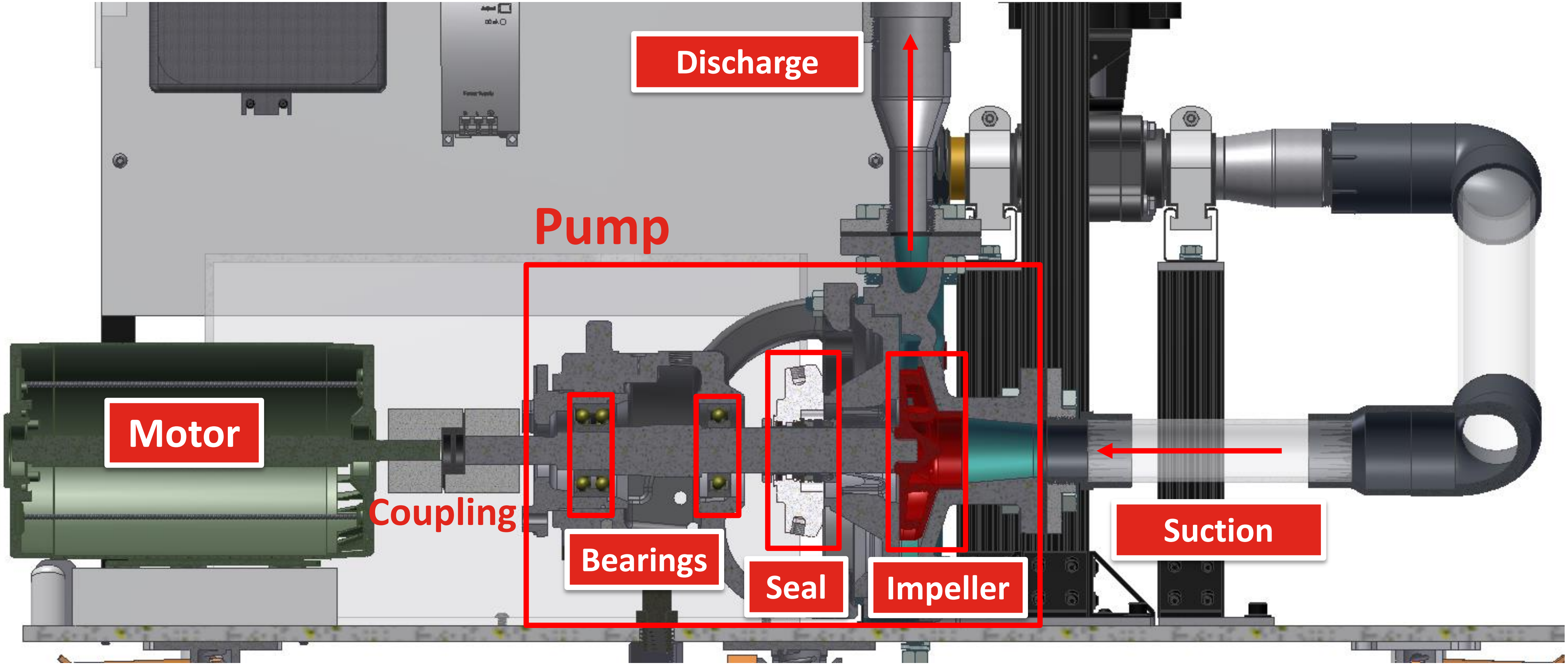
- □ Bubble collapse causes excessive vibrations which can damage rings, seals and bearings
- □ Shock waves creates small pits on the edges of impeller blades, eventually wearing them completely

Show time!

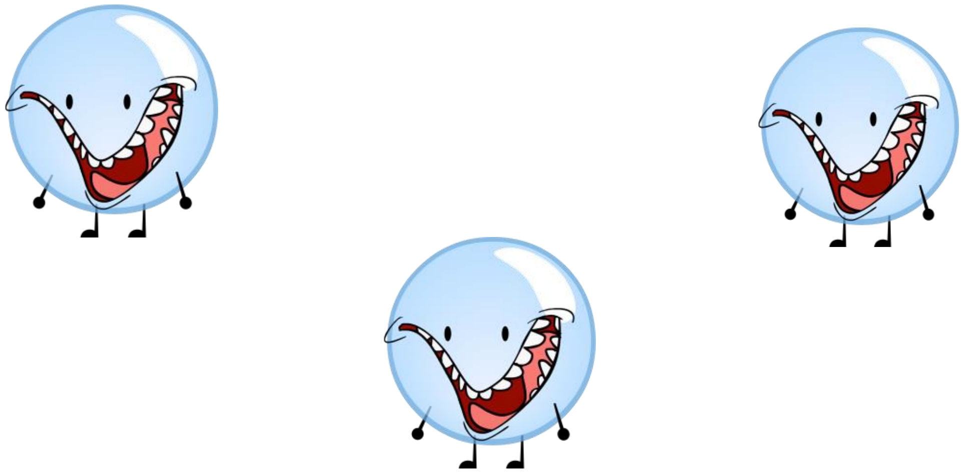
Overview of the demo rig



Inside the pump



DEMO

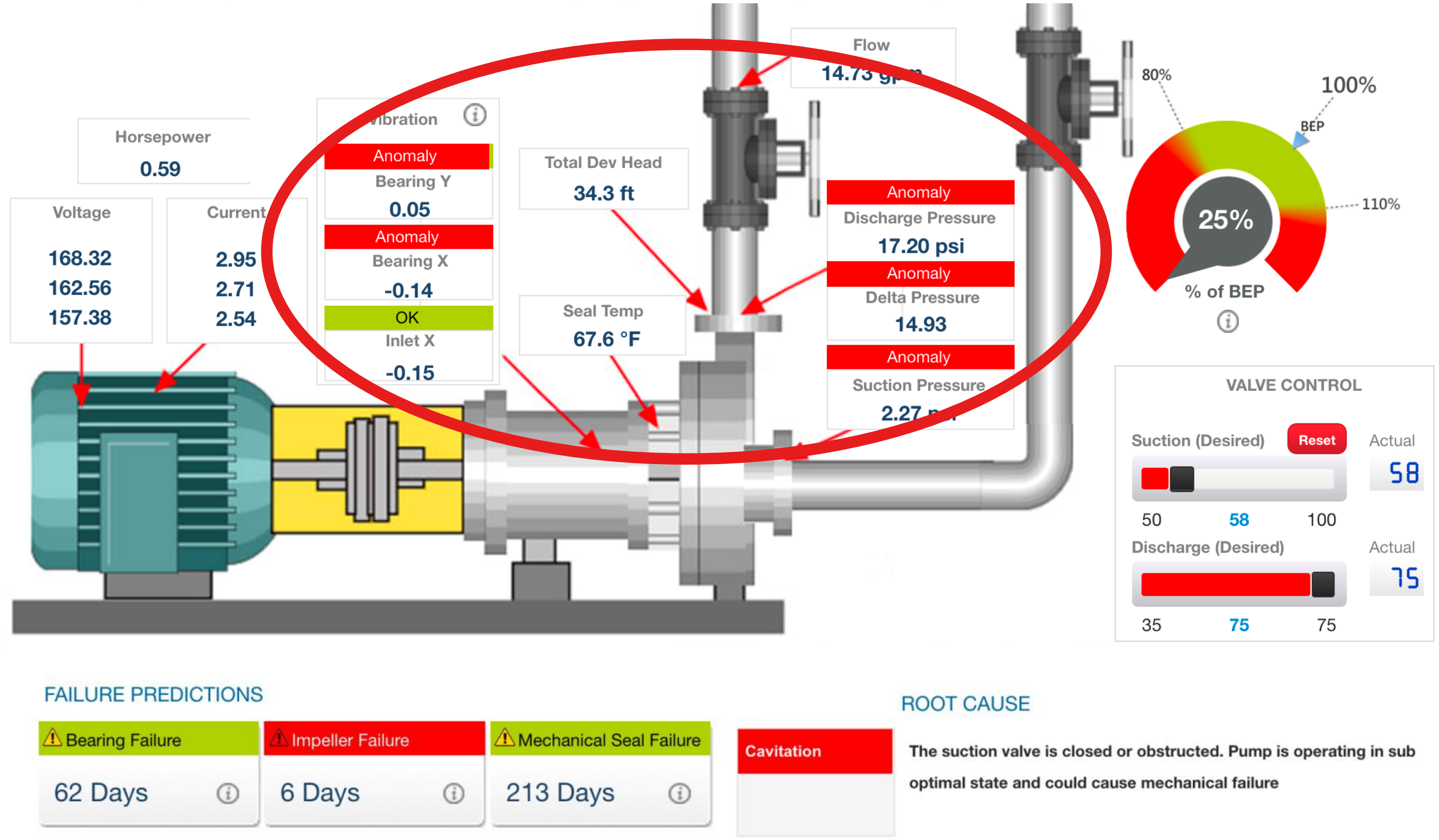


Evil Bubbles

Detecting cavitation

Detection with asset monitoring applications

Pump is instrumented with sensors to monitor its state



Horsepower 0.59

Voltage 168.32 162.56 157.38

Current 2.95 2.71 2.54

Vibration

Anomaly
Bearing Y 0.05

Anomaly
Bearing X -0.14

OK
Inlet X -0.15

Total Dev Head 34.3 ft

Seal Temp 67.6 °F

Flow 14.73 gpm

Anomaly
Discharge Pressure 17.20 psi

Anomaly
Delta Pressure 14.93

Anomaly
Suction Pressure 2.27 psi

VALVE CONTROL

Suction (Desired) Reset Actual 58
50 58 100

Discharge (Desired) Actual 75
35 75 75

FAILURE PREDICTIONS

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

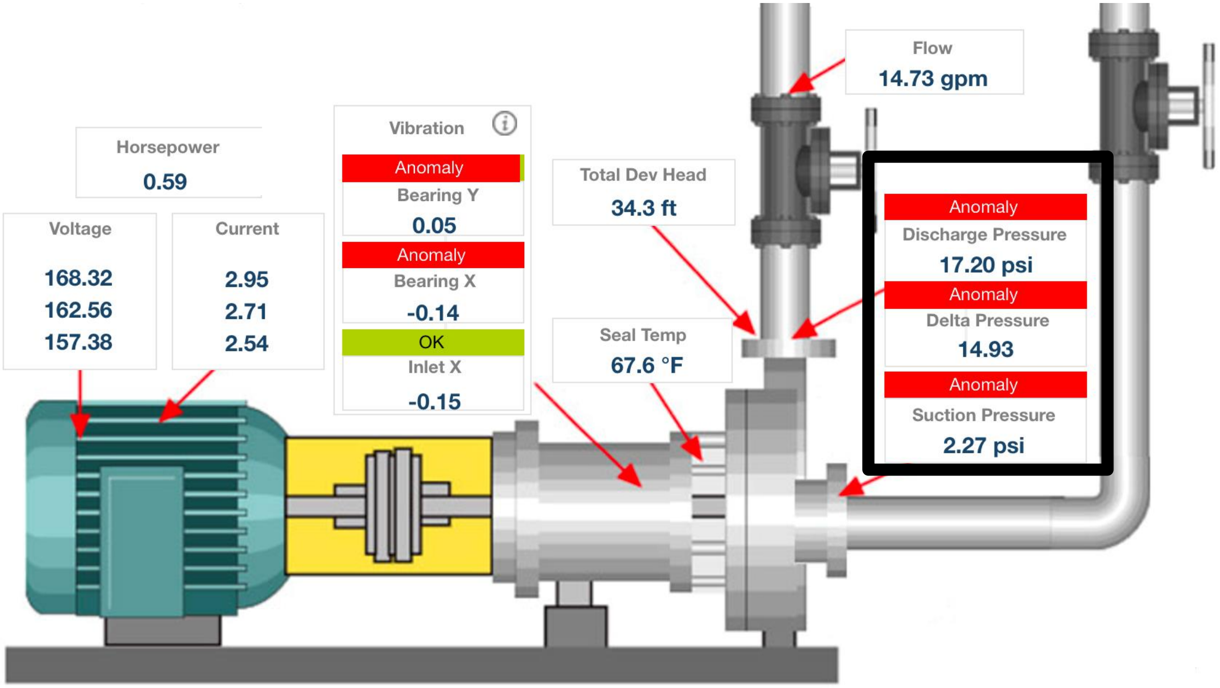
ROOT CAUSE

Cavitation

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

FLOWSERVE

Pump monitoring



Fluid pressure

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

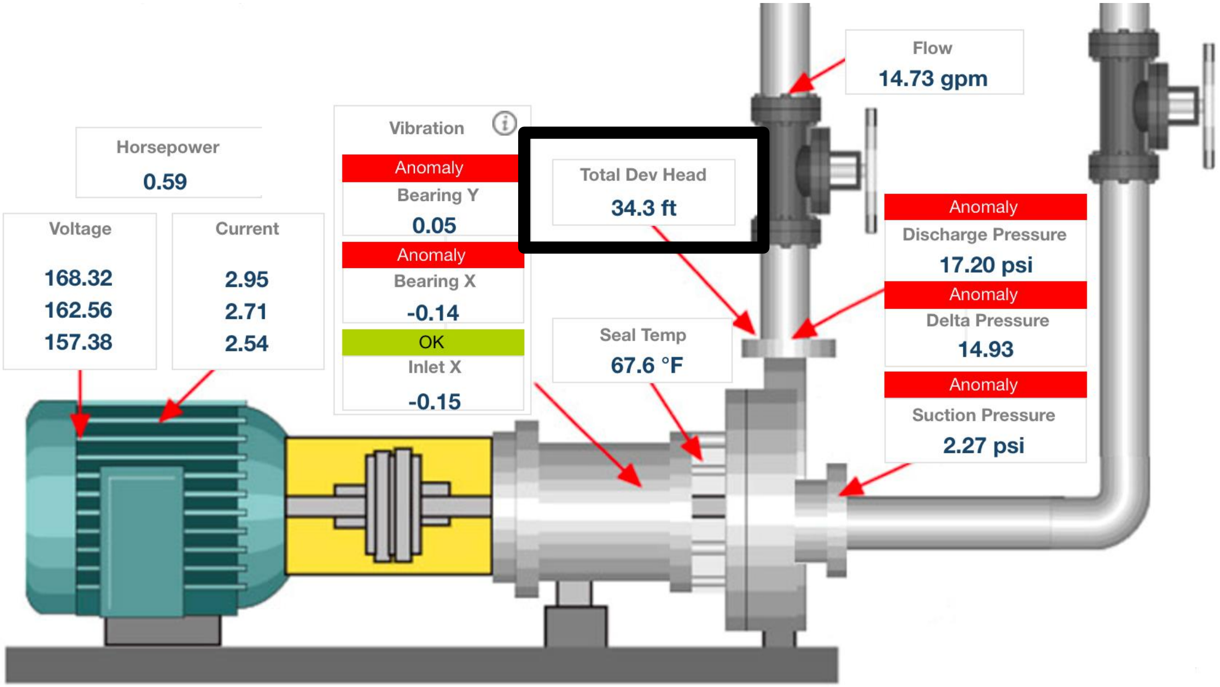
Temperature

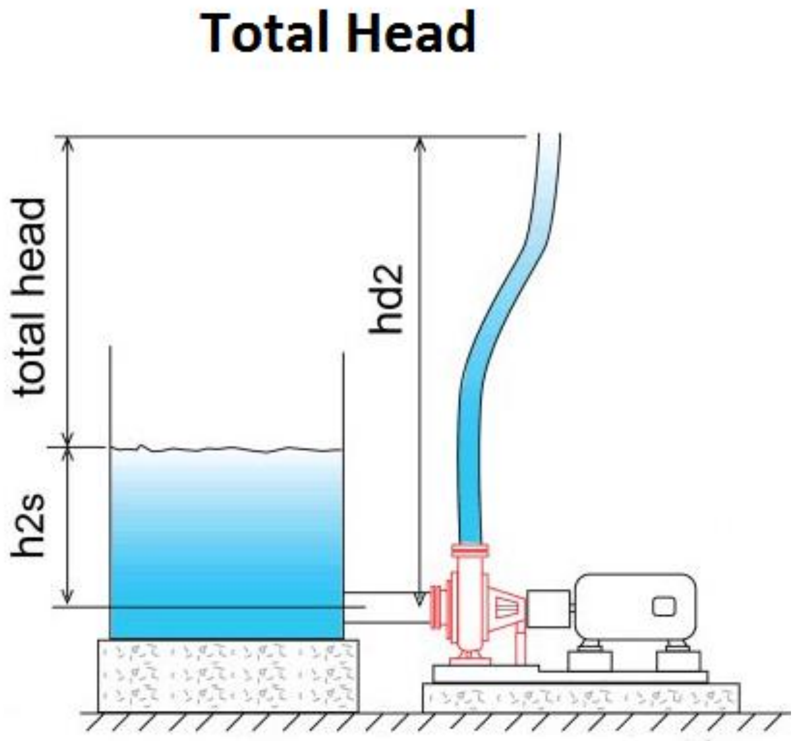
- Seal temperature, F

Vibration

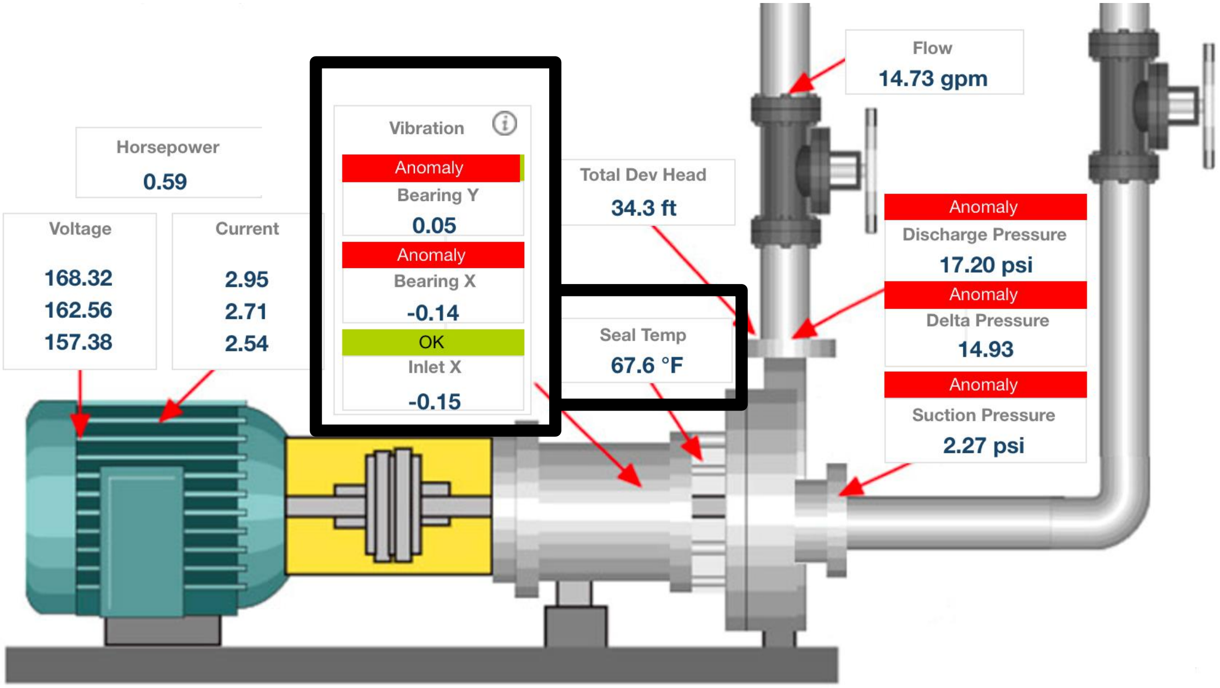
- Vibration bearing X (horizontal)
- Vibration bearing Y (vertical)
- Vibration pump inlet X

Pump monitoring





Pump monitoring



Fluid pressure

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

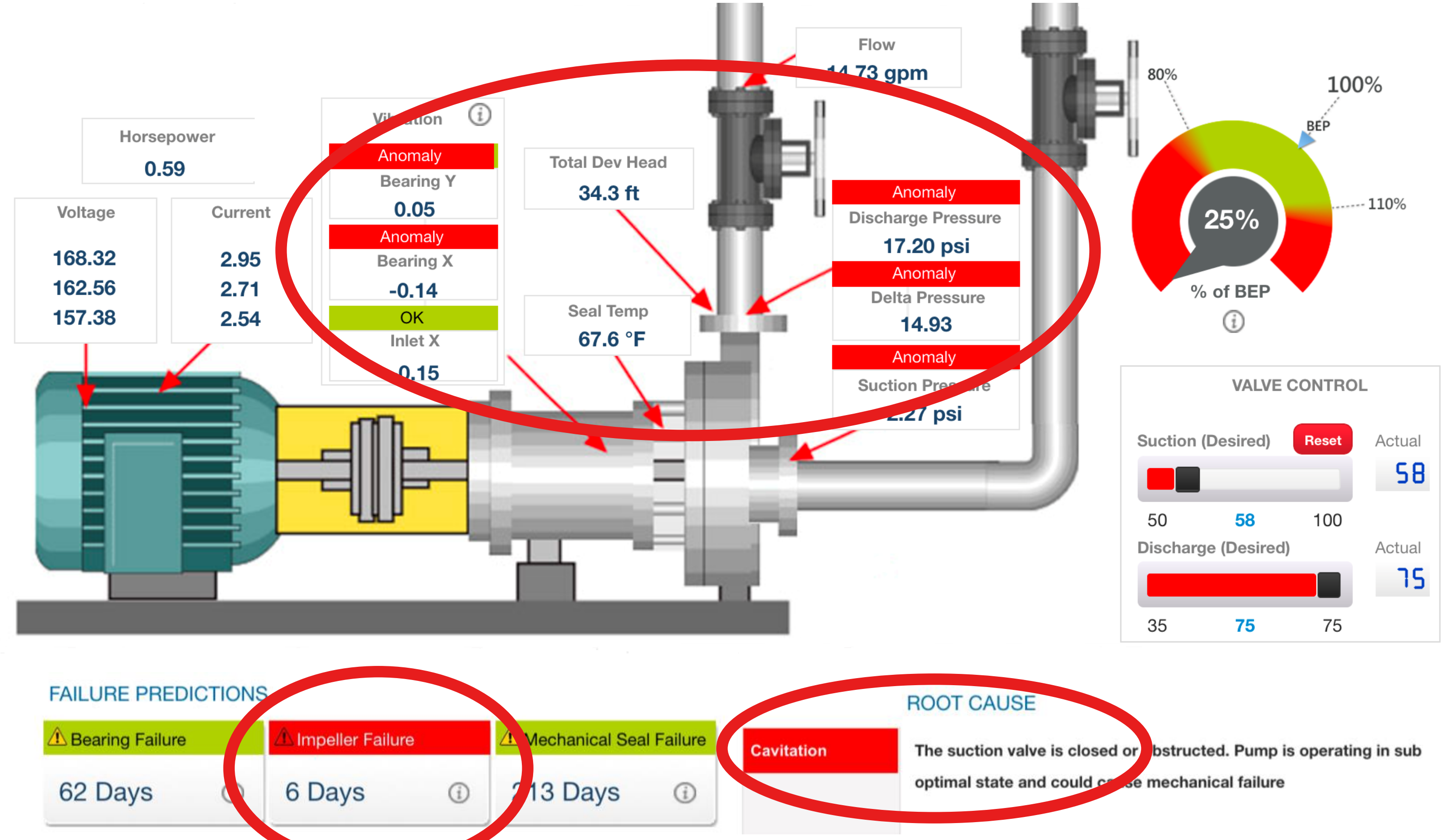
Temperature

- Seal temperature, F

Vibration

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

Point (2): Detection of the cyber-physical attacks requires process engineering methods



Horsepower
0.59

Voltage
168.32
162.56
157.38

Current
2.95
2.71
2.54

Vibration

Anomaly
Bearing Y
0.05

Anomaly
Bearing X
-0.14

OK
Inlet X
0.15

Total Dev Head
34.3 ft

Seal Temp
67.6 °F

Flow
14.73 gpm

Anomaly
Discharge Pressure
17.20 psi

Anomaly
Delta Pressure
14.93

Anomaly
Suction Pressure
2.27 psi

VALVE CONTROL

Suction (Desired) Reset Actual 58
50 58 100

Discharge (Desired) Actual 75
35 75 75

FAILURE PREDICTIONS

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

ROOT CAUSE

Cavitation

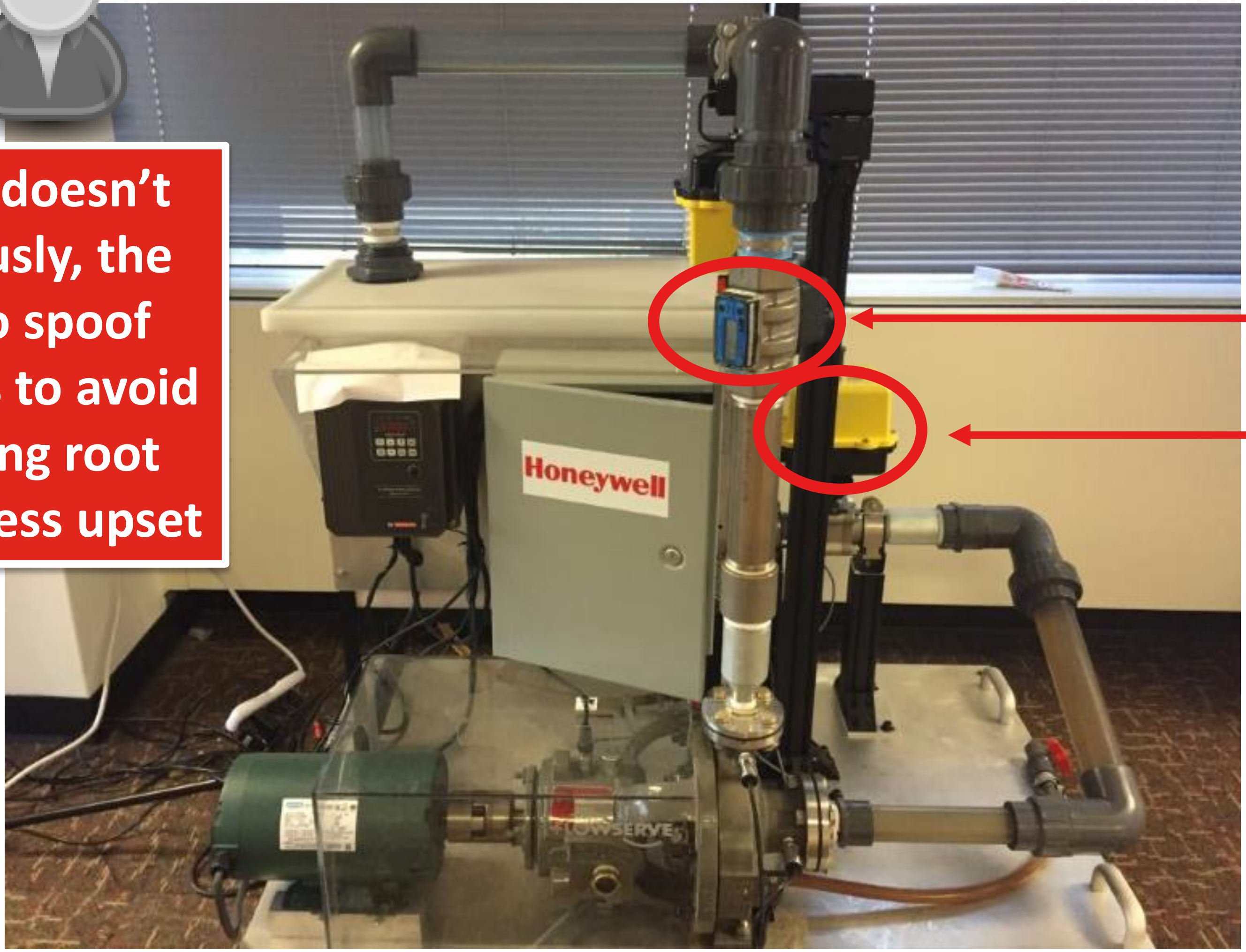
The suction valve is closed or obstructed. Pump is operating in sub optimal state and could cause mechanical failure

Root cause: Cavitation

Defending competent adversary

The attacker will spoof certain process values to avoid detection

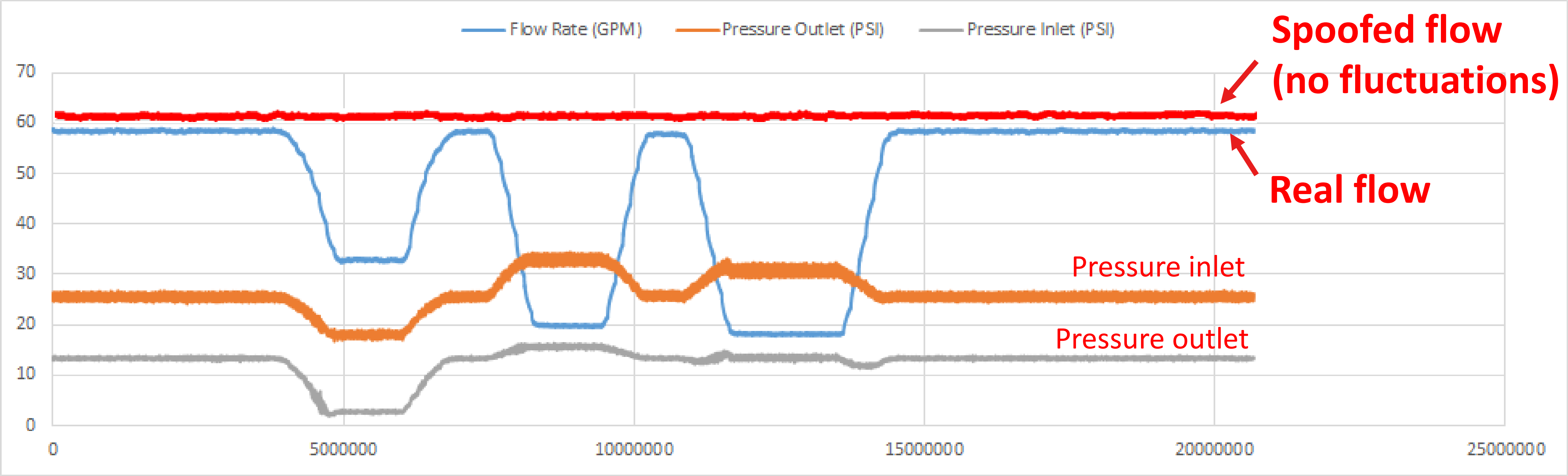
Since pump damage doesn't happen instantaneously, the attacker will have to spoof certain process values to avoid detection by impeding root cause analysis of process upset



Flow

Positioner of the valve

The attacker will spoof certain process values to avoid detection



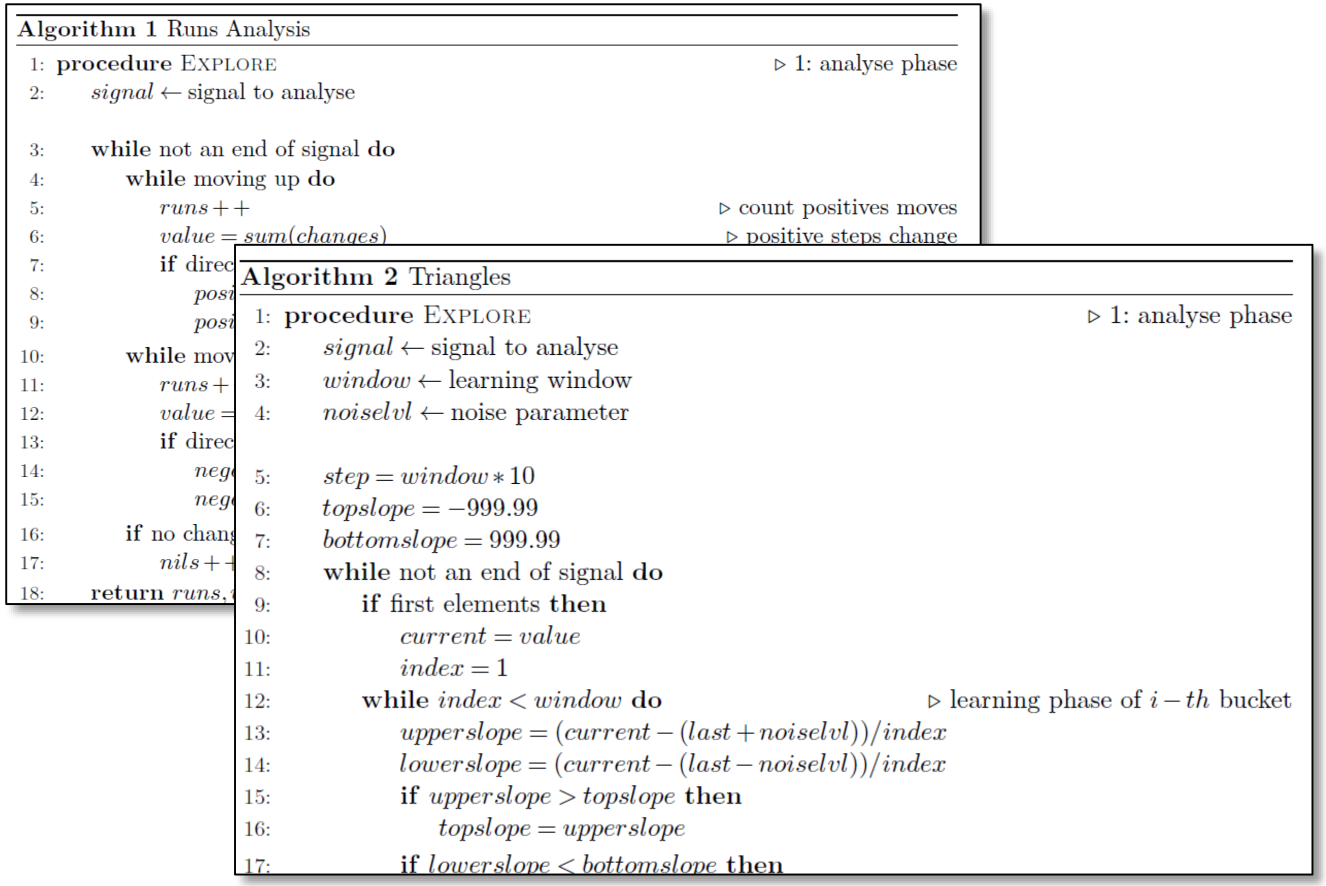
Spoofed flow (no fluctuations)

Real flow

Pressure inlet

Pressure outlet

FAQ: But how does one spoof process data?



Algorithm 1 Runs Analysis

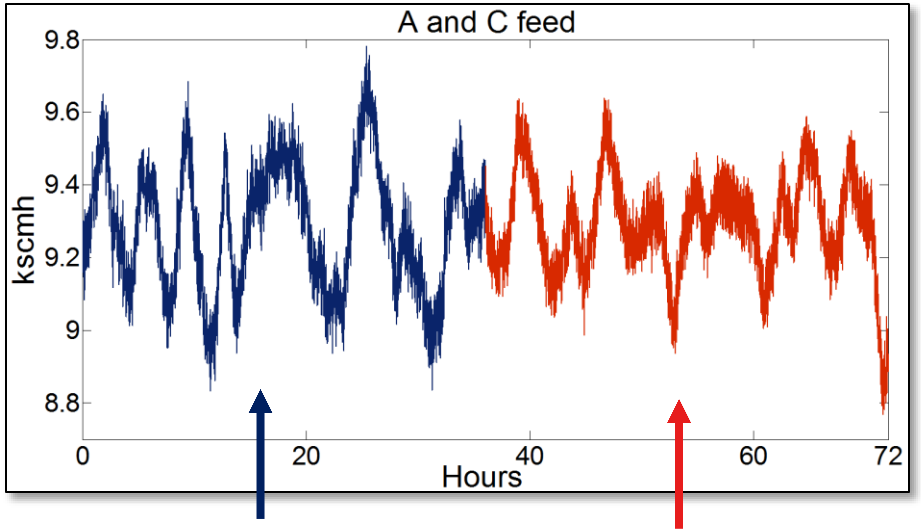
```
procedure EXPLORE                                   ▷ 1: analyse phase
    $signal$ ← signal to analyse

    while not an end of signal do
        while moving up do
            $runs$++                                ▷ count positives moves
            $value = sum(changes)$                  ▷ positive steps change
            if direc
                posi
                posi
        while mov
            $runs$+
            $value$ =
            if direc
                neg
                neg
        if no chang
            $nils$++
    return $runs$,
```

Algorithm 2 Triangles

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

    $step = window * 10$
    $topslope = -999.99$
    $bottomslope = 999.99$
    while not an end of signal do
        if first elements then
            $current = value$
            $index = 1$
        while $index < window$ do                   ▷ learning phase of $i-th$ bucket
            $upperslope = (current - (last + noiselvl))/index$
            $lowerslope = (current - (last - noiselvl))/index$
            if $upperslope > topslope$ then
                $topslope = upperslope$
            if $lowerslope < bottomslope$ then
```



Original

Spoofed

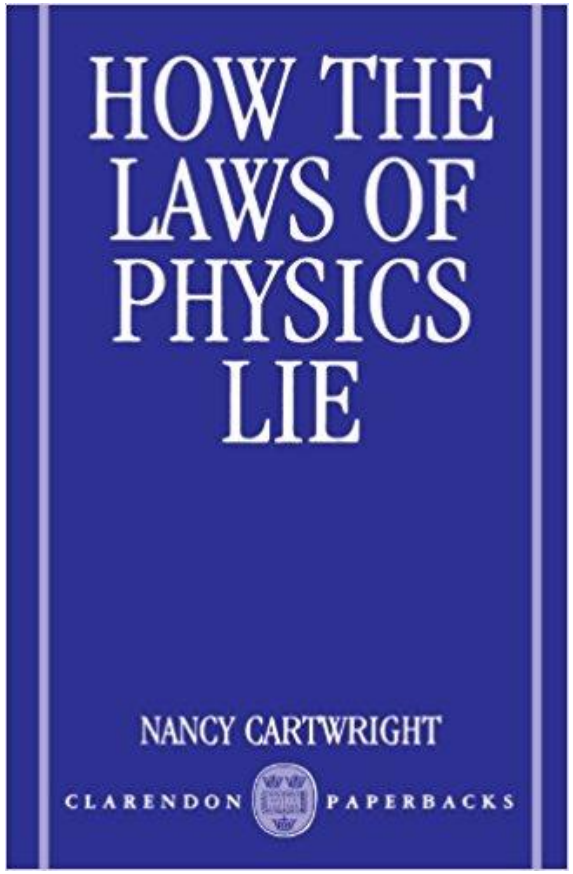
Find X differences

(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

PHYSICS
~~HIPS~~ DON'T LIE

Shakira



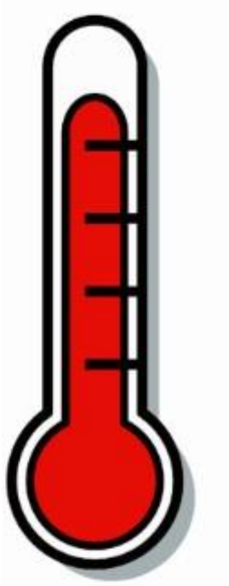
HOW THE LAWS OF PHYSICS LIE

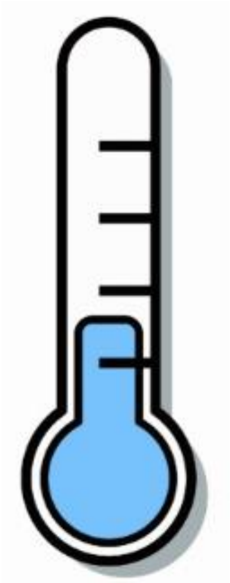
NANCY CARTWRIGHT

CLARENDON PAPERBACKS

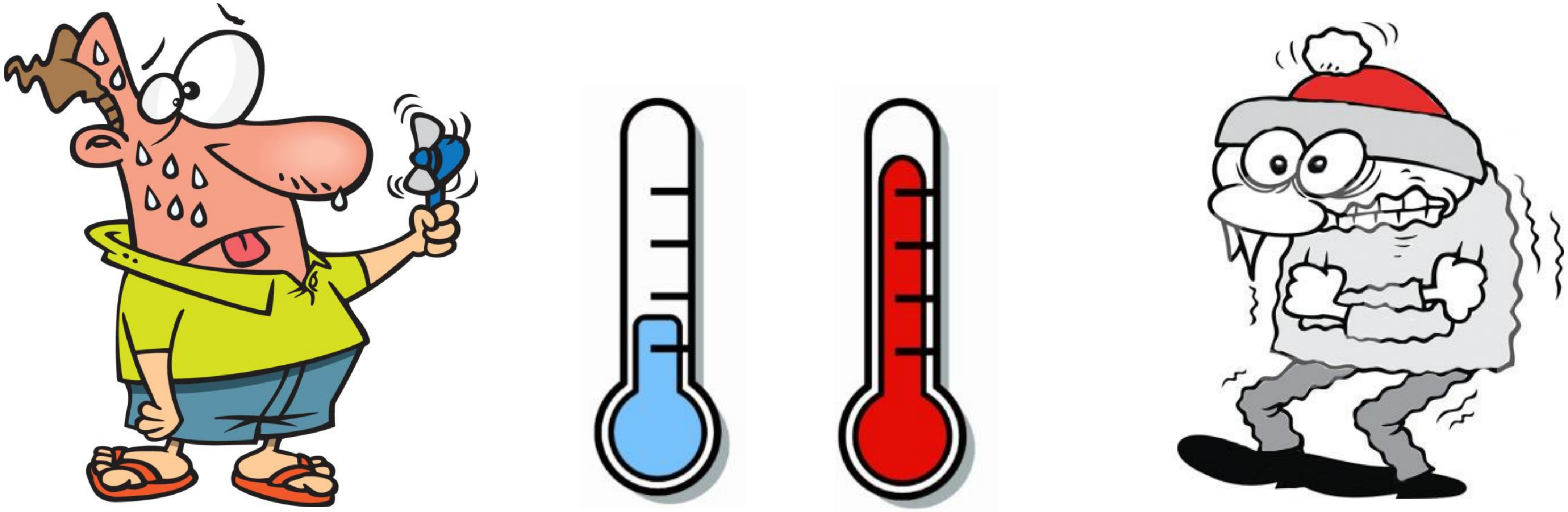
https://www.amazon.com/How-Laws-Physics-Nancy-Cartwright/dp/0198247044

Physical correlations





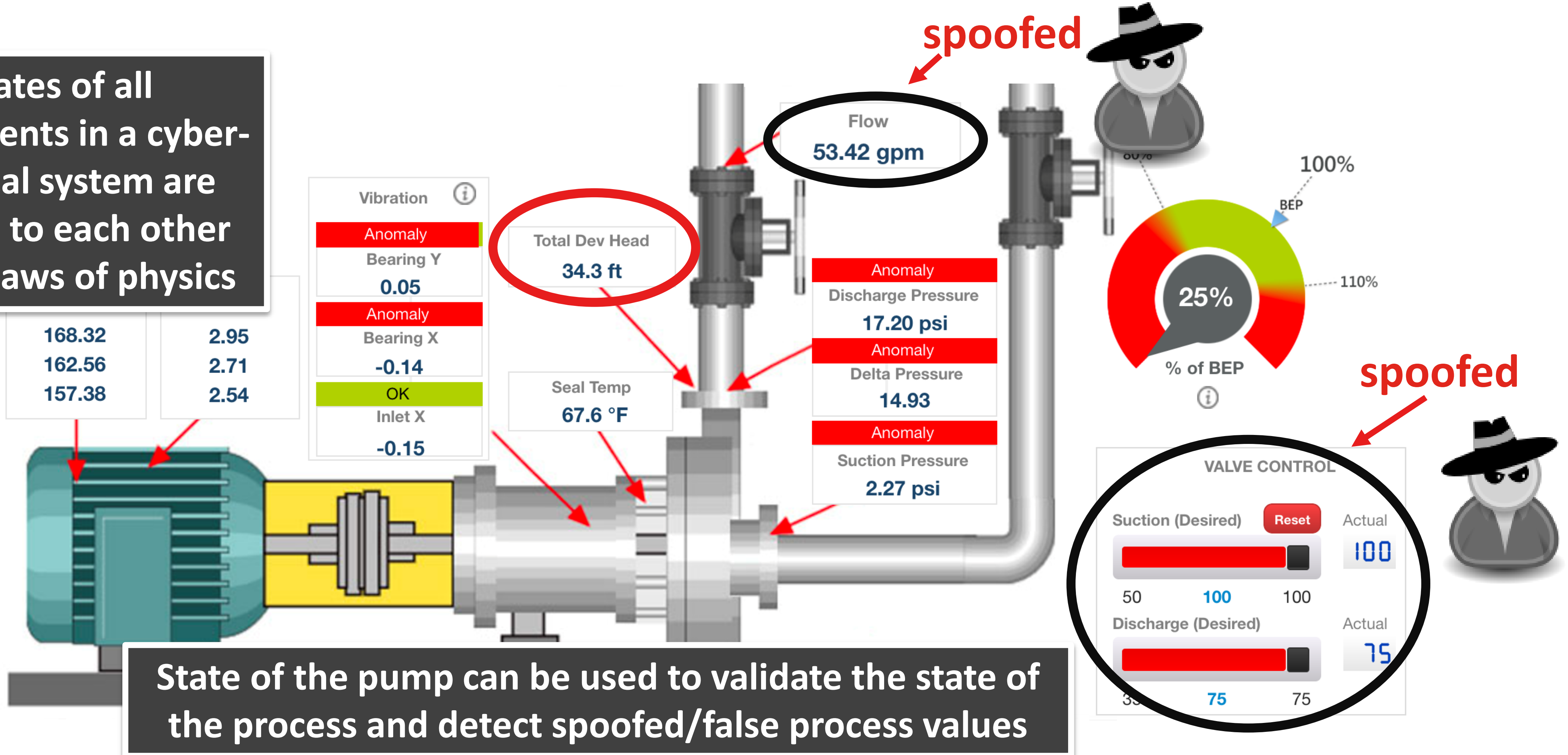
Physical correlations



THIS DOES NOT MAKE SENSE

Point (3): Detection of spurious sensor signals can be achieved with data plausibility checks

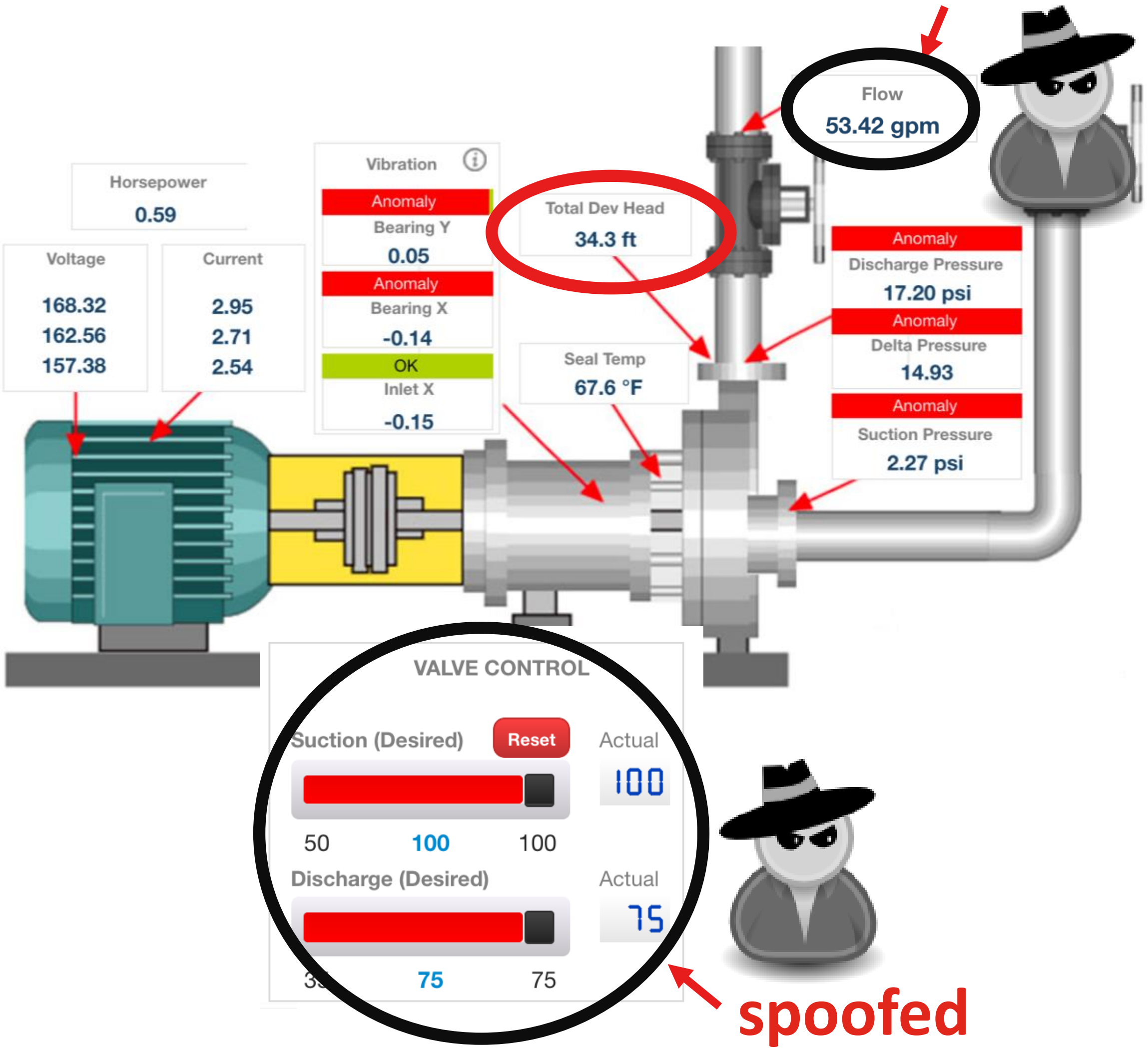
States of all components in a cyber-physical system are related to each other by the laws of physics



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

Verification of flow

spoofed



Horsepower
0.59

Voltage
168.32
162.56
157.38

Current
2.95
2.71
2.54

Vibration
Anomaly
Bearing Y
0.05
Anomaly
Bearing X
-0.14
OK
Inlet X
-0.15

Total Dev Head
34.3 ft

Seal Temp
67.6 °F

Flow
53.42 gpm

Anomaly
Discharge Pressure
17.20 psi
Anomaly
Delta Pressure
14.93
Anomaly
Suction Pressure
2.27 psi

VALVE CONTROL

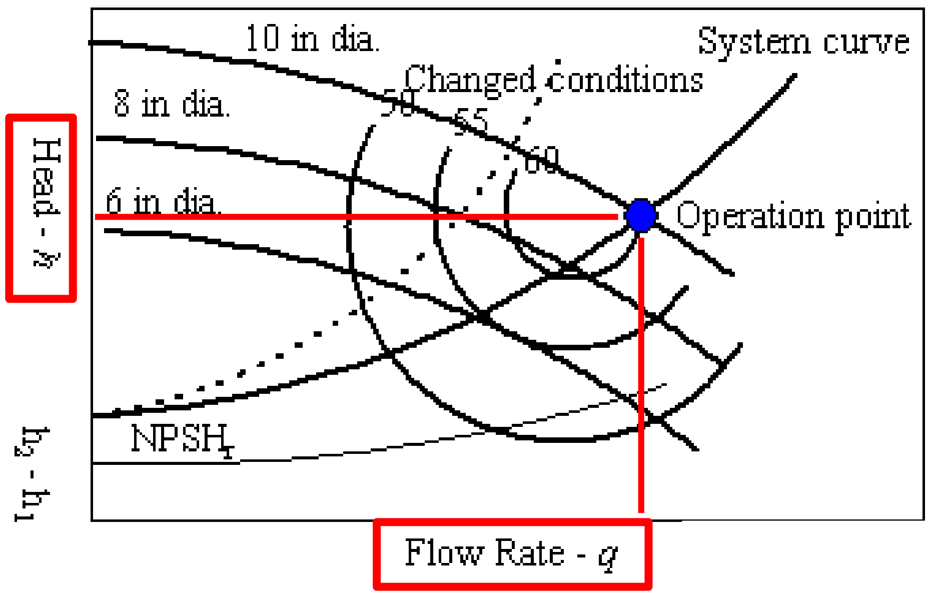
Suction (Desired) Reset Actual 100
50 100 100

Discharge (Desired) Actual 75
35 75 75

spoofed

Curve of the demo pump would suggest:
Head 34.3 ft ~ flow 21-22 gpm

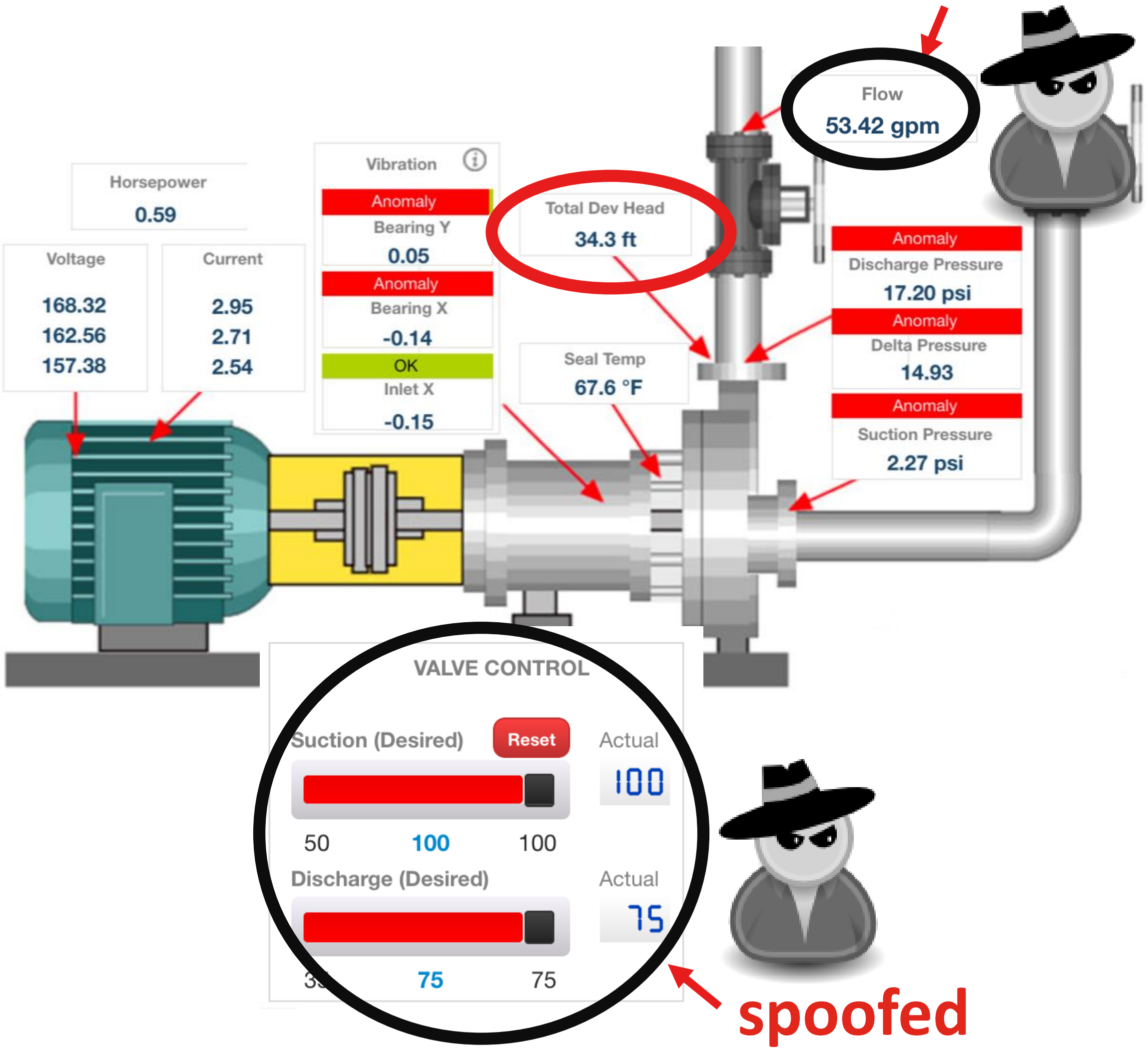
Flow reading **53.42 gpm** is <u>implausible</u>



http://www.engineeringtoolbox.com/npsh-net-positive-suction-head-d_634.html

Verification of valve positions

spoofed



Horsepower 0.59

Voltage
168.32
162.56
157.38

Current
2.95
2.71
2.54

Vibration
Anomaly
Bearing Y 0.05
Anomaly
Bearing X -0.14
OK
Inlet X -0.15

Total Dev Head 34.3 ft

Seal Temp 67.6 °F

Flow 53.42 gpm

Anomaly
Discharge Pressure 17.20 psi
Anomaly
Delta Pressure 14.93
Anomaly
Suction Pressure 2.27 psi

VALVE CONTROL

Suction (Desired) Reset Actual 100

50 100 100

Discharge (Desired) Actual 75

3 75 75

spoofed

Curve of the demo pump would suggest:

Head 34.3 ft ~ flow 21-22 gpm

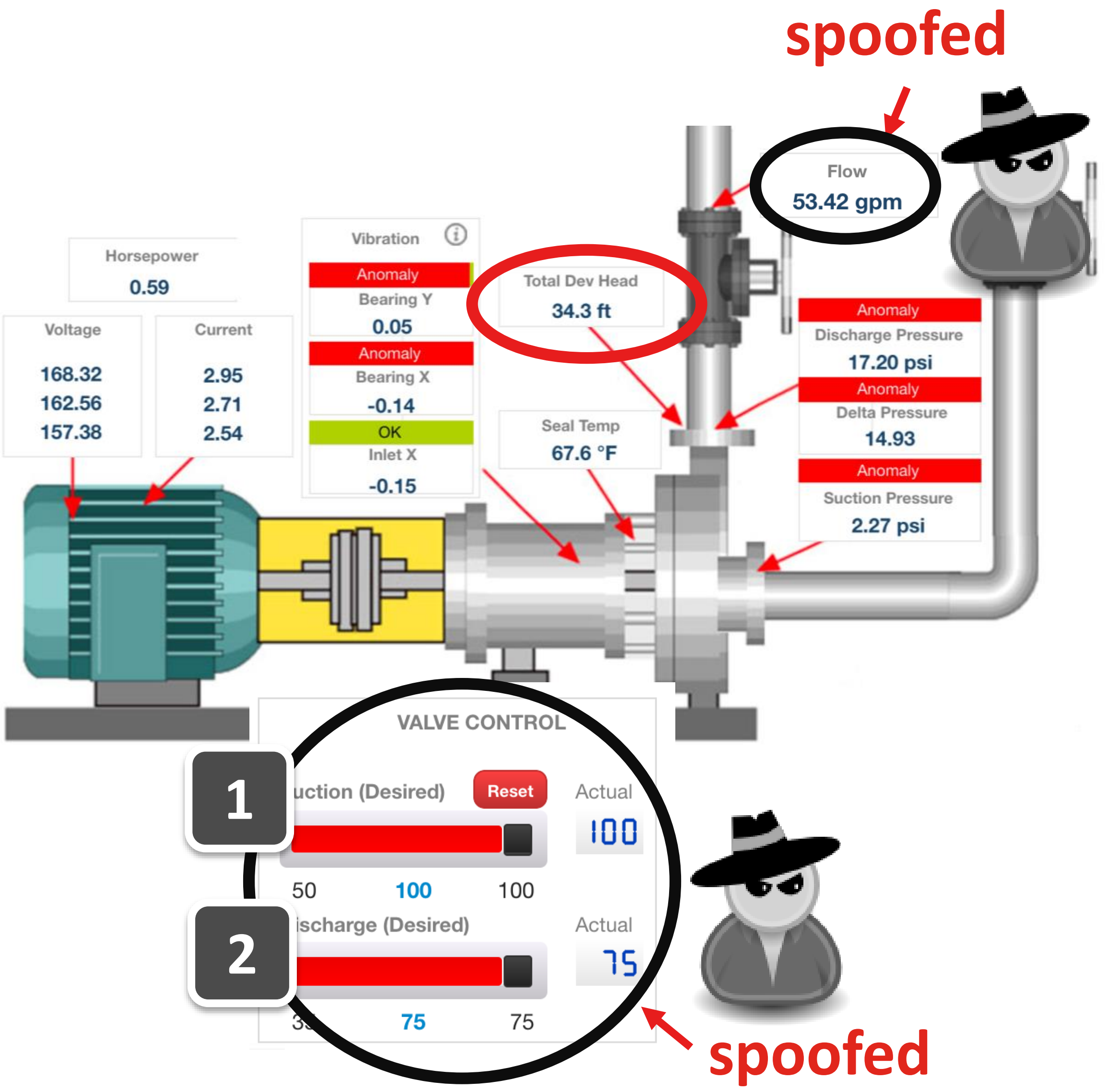
↓

We know that the flow is reduced

↓

<ins>**Either**</ins> of valve position sensors is forged

Verification of valve positions



Flow
53.42 gpm

Horsepower
0.59

Vibration
Anomaly
Bearing Y
0.05
Anomaly
Bearing X
-0.14
OK
Inlet X
-0.15

Total Dev Head
34.3 ft

Voltage
168.32
162.56
157.38

Current
2.95
2.71
2.54

Seal Temp
67.6 °F

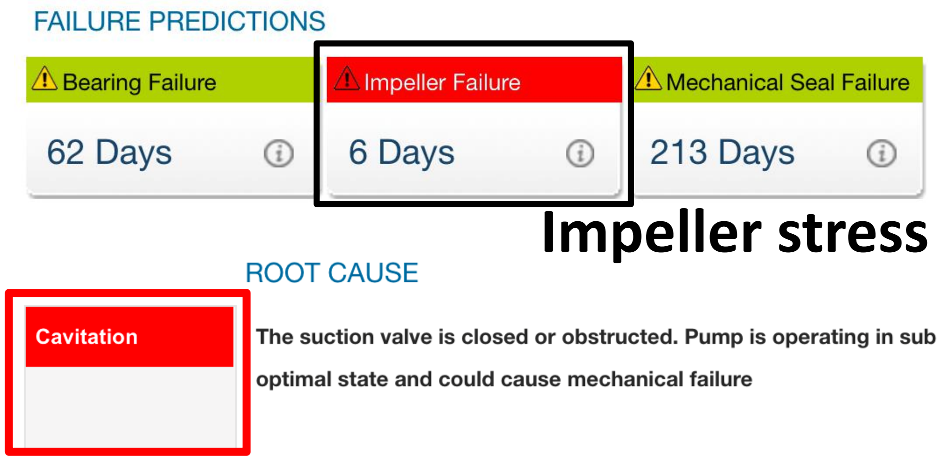
Anomaly
Discharge Pressure
17.20 psi
Anomaly
Delta Pressure
14.93
Anomaly
Suction Pressure
2.27 psi

VALVE CONTROL

uction (Desired) Reset Actual 100
50 100 100

ischarge (Desired) Actual 75
3 75 75

1



FAILURE PREDICTIONS

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

ROOT CAUSE

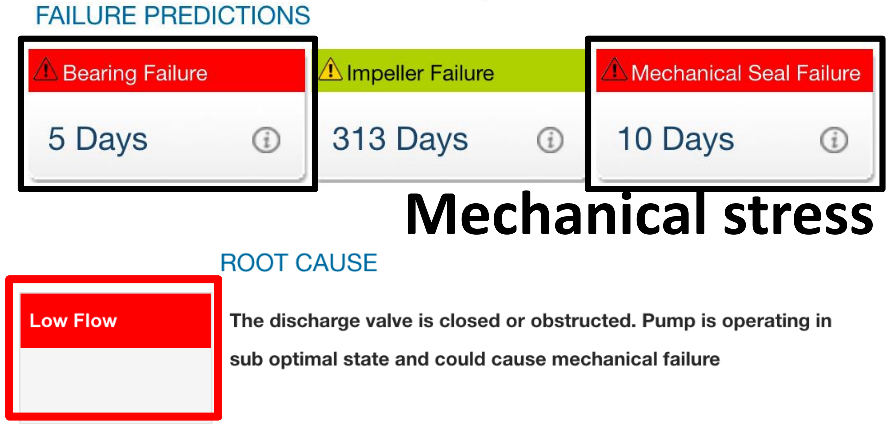
Cavitation

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

Impeller stress

Root cause: Cavitation

2



FAILURE PREDICTIONS

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

ROOT CAUSE

Low Flow

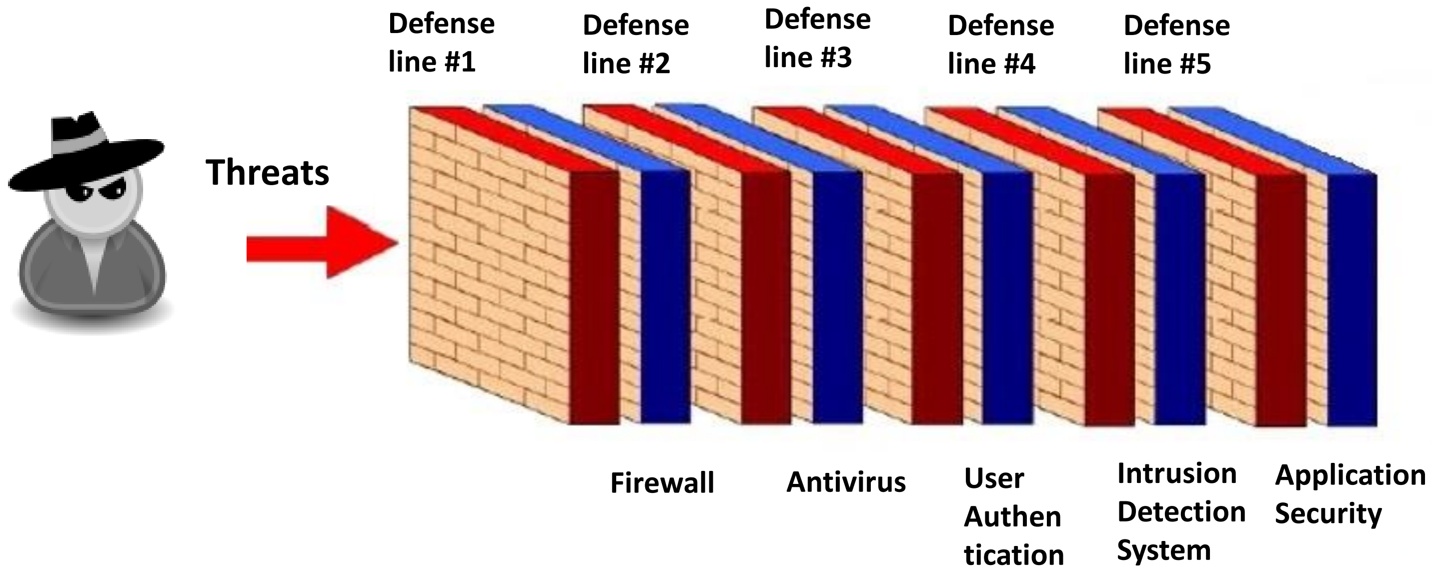
The discharge valve is closed or obstructed. Pump is operating in sub optimal state and could cause mechanical failure

Mechanical stress

Root cause: Low flow

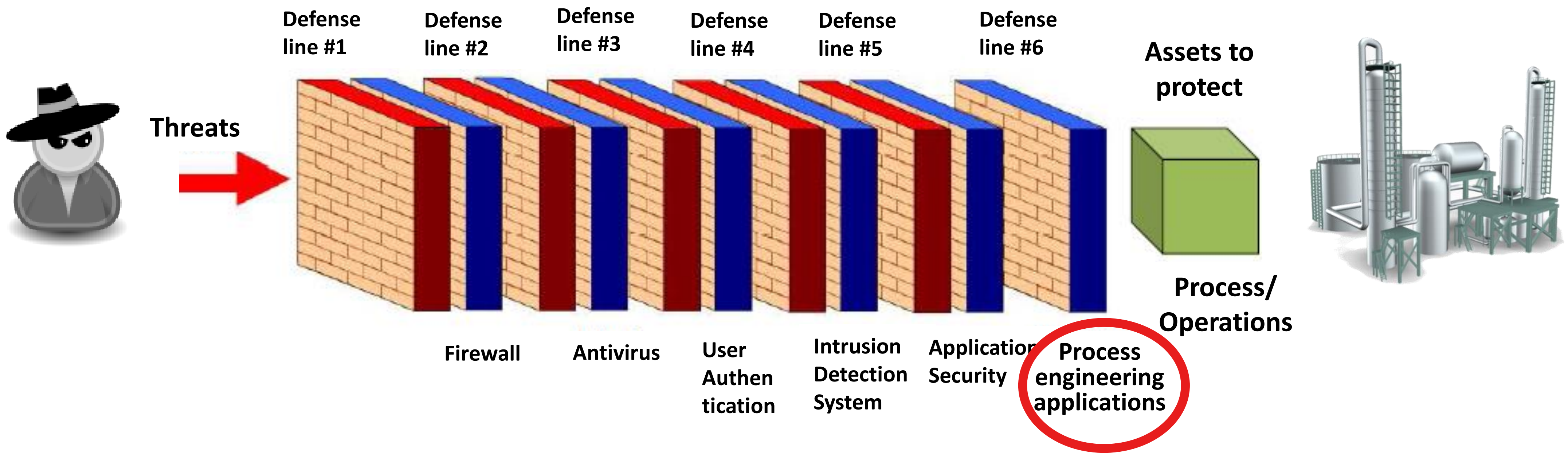
Defense in depth philosophy

- 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



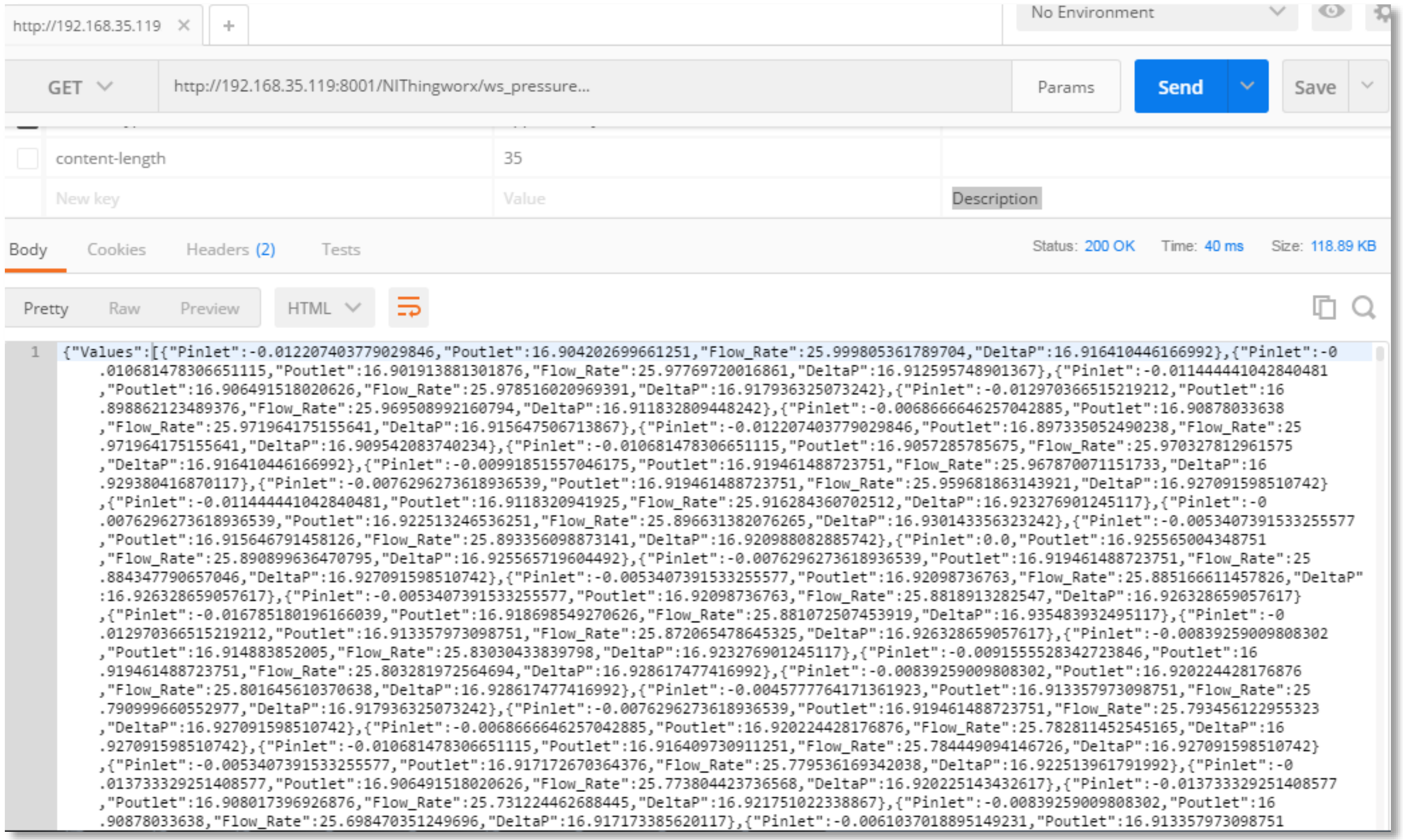
Defense in depth in cyber-physical systems

- If the attacker manages to bypass all traditional IT security defenses,
  - Process engineering (OT) security controls should be in place to detect and prevent unwanted/malicious process manipulations



FAQ: So, Asset Monitoring solutions are capable of detecting cyber-physical attacks?

- NO. They provide us with the data, which can be used to detect cyber-physical attacks



GET http://192.168.35.119:8001/NIThingworx/ws_pressure...

content-length	35	
New key	Value	Description

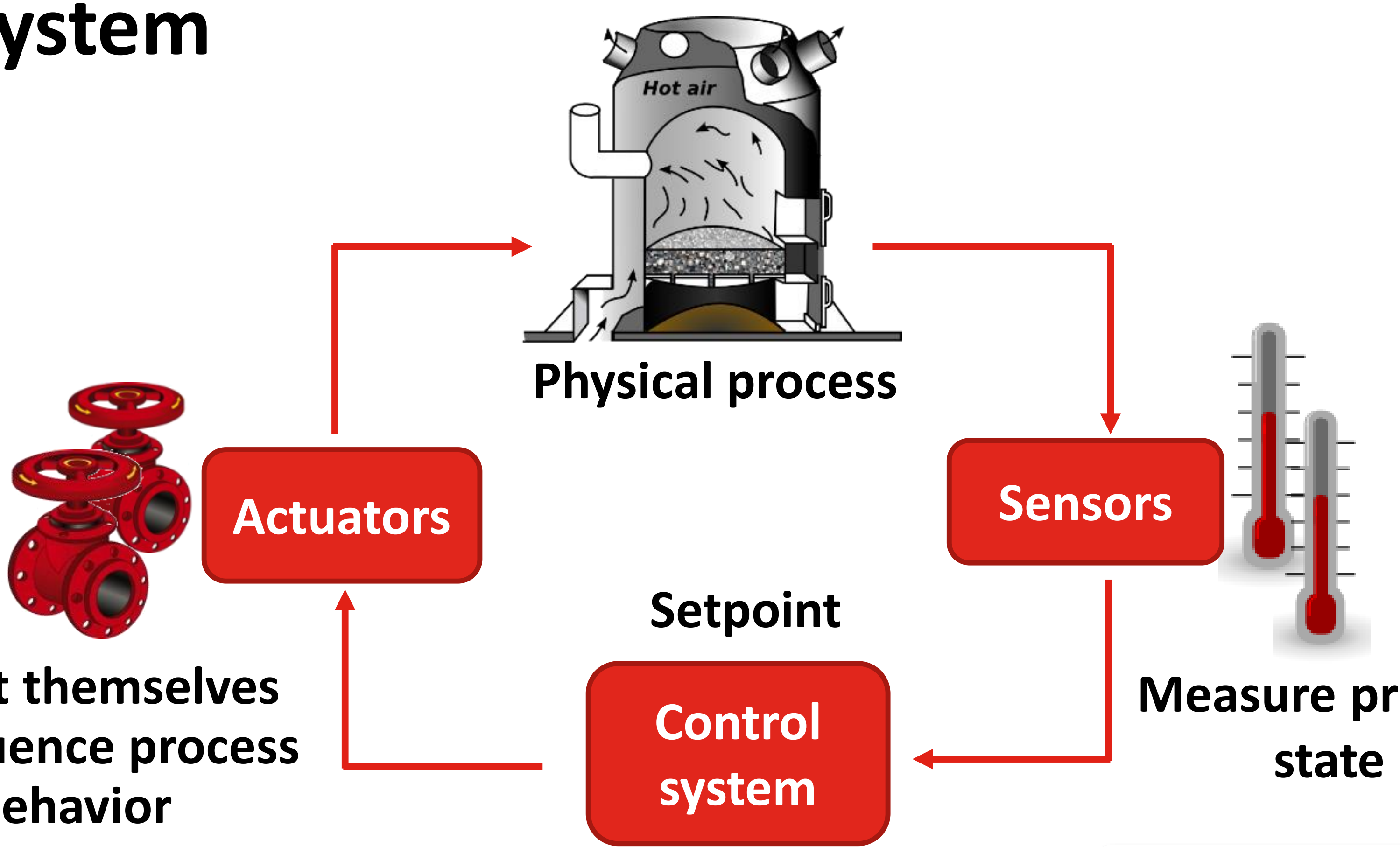
Status: 200 OK Time: 40 ms Size: 118.89 KB

```
{"Values":[{"Pinlet":-0.012207403779029846,"Poutlet":16.904202699661251,"Flow_Rate":25.999805361789704,"DeltaP":16.916410446166992},{"Pinlet":-0
    .010681478306651115,"Poutlet":16.901913881301876,"Flow_Rate":25.97769720016861,"DeltaP":16.912595748901367},{"Pinlet":-0.011444441042840481
    ,"Poutlet":16.906491518020626,"Flow_Rate":25.978516020969391,"DeltaP":16.917936325073242},{"Pinlet":-0.012970366515219212,"Poutlet":16
    .898862123489376,"Flow_Rate":25.969508992160794,"DeltaP":16.911832809448242},{"Pinlet":-0.0068666646257042885,"Poutlet":16.90878033638
    ,"Flow_Rate":25.971964175155641,"DeltaP":16.915647506713867},{"Pinlet":-0.012207403779029846,"Poutlet":16.897335052490238,"Flow_Rate":25
    .971964175155641,"DeltaP":16.909542083740234},{"Pinlet":-0.010681478306651115,"Poutlet":16.9057285785675,"Flow_Rate":25.970327812961575
    ,"DeltaP":16.916410446166992},{"Pinlet":-0.00991851557046175,"Poutlet":16.919461488723751,"Flow_Rate":25.967870071151733,"DeltaP":16
    .929380416870117},{"Pinlet":-0.0076296273618936539,"Poutlet":16.919461488723751,"Flow_Rate":25.959681863143921,"DeltaP":16.927091598510742}
    ,{"Pinlet":-0.011444441042840481,"Poutlet":16.9118320941925,"Flow_Rate":25.916284360702512,"DeltaP":16.923276901245117},{"Pinlet":-0
    .0076296273618936539,"Poutlet":16.922513246536251,"Flow_Rate":25.896631382076265,"DeltaP":16.930143356323242},{"Pinlet":-0.0053407391533255577
    ,"Poutlet":16.915646791458126,"Flow_Rate":25.893356098873141,"DeltaP":16.920988082885742},{"Pinlet":0.0,"Poutlet":16.925565004348751
    ,"Flow_Rate":25.890899636470795,"DeltaP":16.925565719604492},{"Pinlet":-0.0076296273618936539,"Poutlet":16.919461488723751,"Flow_Rate":25
    .884347790657046,"DeltaP":16.927091598510742},{"Pinlet":-0.0053407391533255577,"Poutlet":16.92098736763,"Flow_Rate":25.885166611457826,"DeltaP"
    :16.926328659057617},{"Pinlet":-0.0053407391533255577,"Poutlet":16.92098736763,"Flow_Rate":25.8818913282547,"DeltaP":16.926328659057617}
    ,{"Pinlet":-0.016785180196166039,"Poutlet":16.918698549270626,"Flow_Rate":25.881072507453919,"DeltaP":16.935483932495117},{"Pinlet":-0
    .012970366515219212,"Poutlet":16.913357973098751,"Flow_Rate":25.872065478645325,"DeltaP":16.926328659057617},{"Pinlet":-0.00839259009808302
    ,"Poutlet":16.914883852005,"Flow_Rate":25.83030433839798,"DeltaP":16.923276901245117},{"Pinlet":-0.0091555528342723846,"Poutlet":16
    .919461488723751,"Flow_Rate":25.803281972564694,"DeltaP":16.928617477416992},{"Pinlet":-0.00839259009808302,"Poutlet":16.920224428176876
    ,"Flow_Rate":25.801645610370638,"DeltaP":16.928617477416992},{"Pinlet":-0.0045777764171361923,"Poutlet":16.913357973098751,"Flow_Rate":25
    .790999660552977,"DeltaP":16.917936325073242},{"Pinlet":-0.0076296273618936539,"Poutlet":16.919461488723751,"Flow_Rate":25.793456122955323
    ,"DeltaP":16.927091598510742},{"Pinlet":-0.0068666646257042885,"Poutlet":16.920224428176876,"Flow_Rate":25.782811452545165,"DeltaP":16
    .927091598510742},{"Pinlet":-0.010681478306651115,"Poutlet":16.916409730911251,"Flow_Rate":25.784449094146726,"DeltaP":16.927091598510742}
    ,{"Pinlet":-0.0053407391533255577,"Poutlet":16.917172670364376,"Flow_Rate":25.779536169342038,"DeltaP":16.922513961791992},{"Pinlet":-0
    .013733329251408577,"Poutlet":16.906491518020626,"Flow_Rate":25.773804423736568,"DeltaP":16.920225143432617},{"Pinlet":-0.013733329251408577
    ,"Poutlet":16.908017396926876,"Flow_Rate":25.731224462688445,"DeltaP":16.921751022338867},{"Pinlet":-0.00839259009808302,"Poutlet":16
    .90878033638,"Flow_Rate":25.698470351249696,"DeltaP":16.917173385620117},{"Pinlet":-0.0061037018895149231,"Poutlet":16.913357973098751
```

Is Evil Bubbles attack easy to pull off?

It depends.... :-)

Control system



Physical process

Actuators

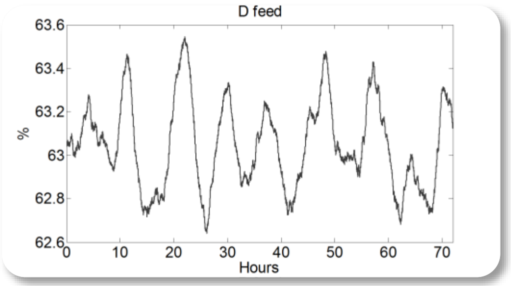
Sensors

Setpoint

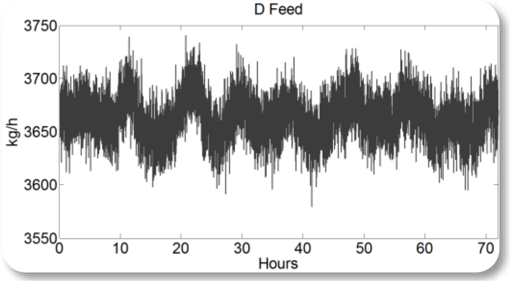
Control system

Adjust themselves to influence process behavior

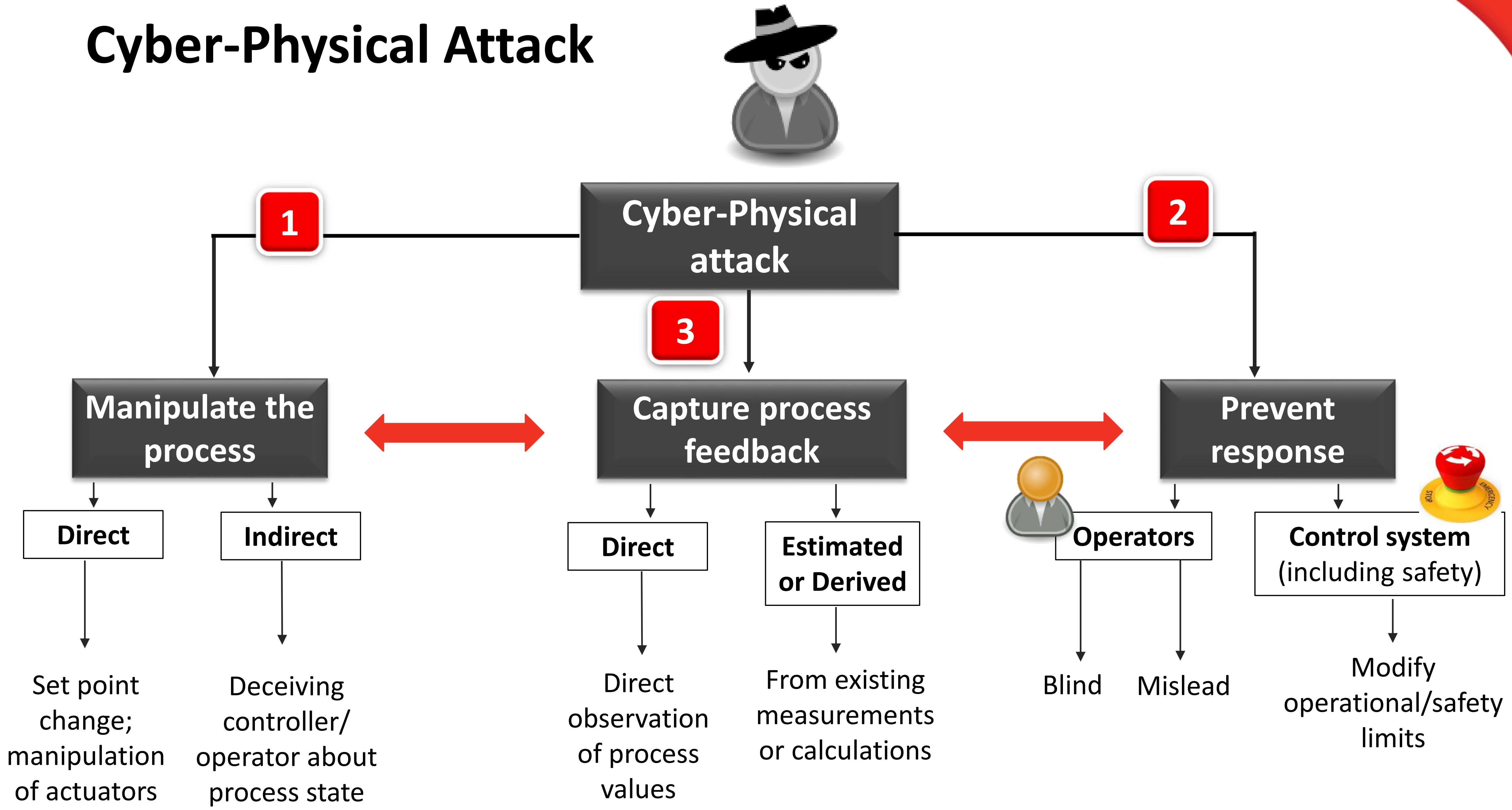
Measure process state



Computes control commands for actuators

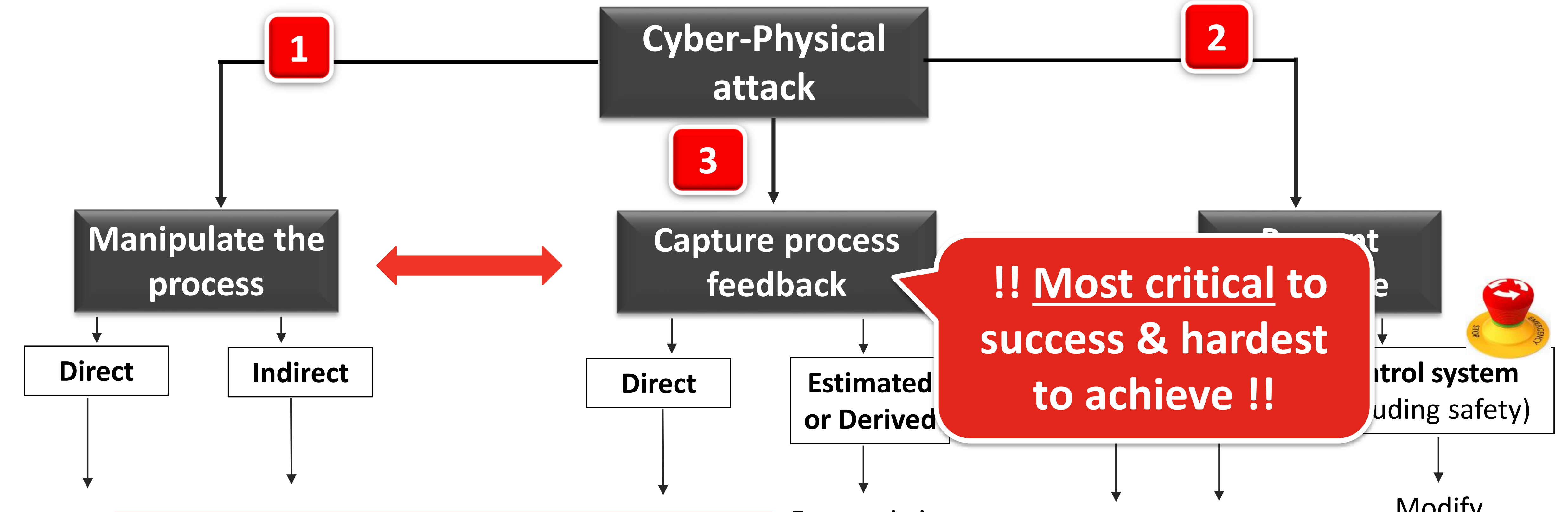


Cyber-Physical Attack



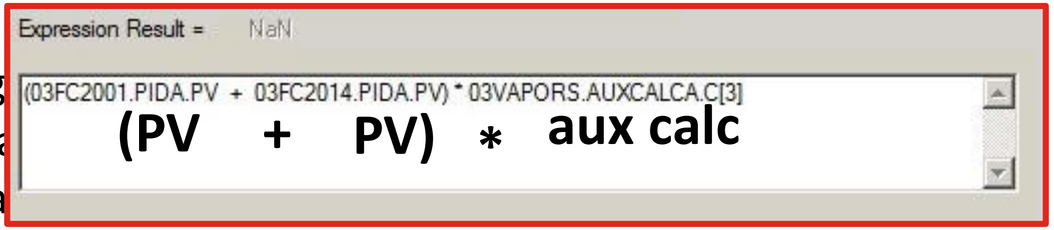
Cyber-Physical attack
1
2
3
Manipulate the process
Capture process feedback
Prevent response
Direct
Indirect
Direct
Estimated or Derived
Operators
Control system (including safety)
Set point change; manipulation of actuators
Deceiving controller/ operator about process state
Direct observation of process values
From existing measurements or calculations
Blind
Mislead
Modify operational/safety limits

Cyber-Physical Attack



!! Most critical to success & hardest to achieve !!

Set po
chang
manipula
of actua



Expression Result = NaN

(03FC2001.PIDA.PV + 03FC2014.PIDA.PV) * 03VAPORS.AUXCALCA.C[3]

(PV + PV) * aux calc

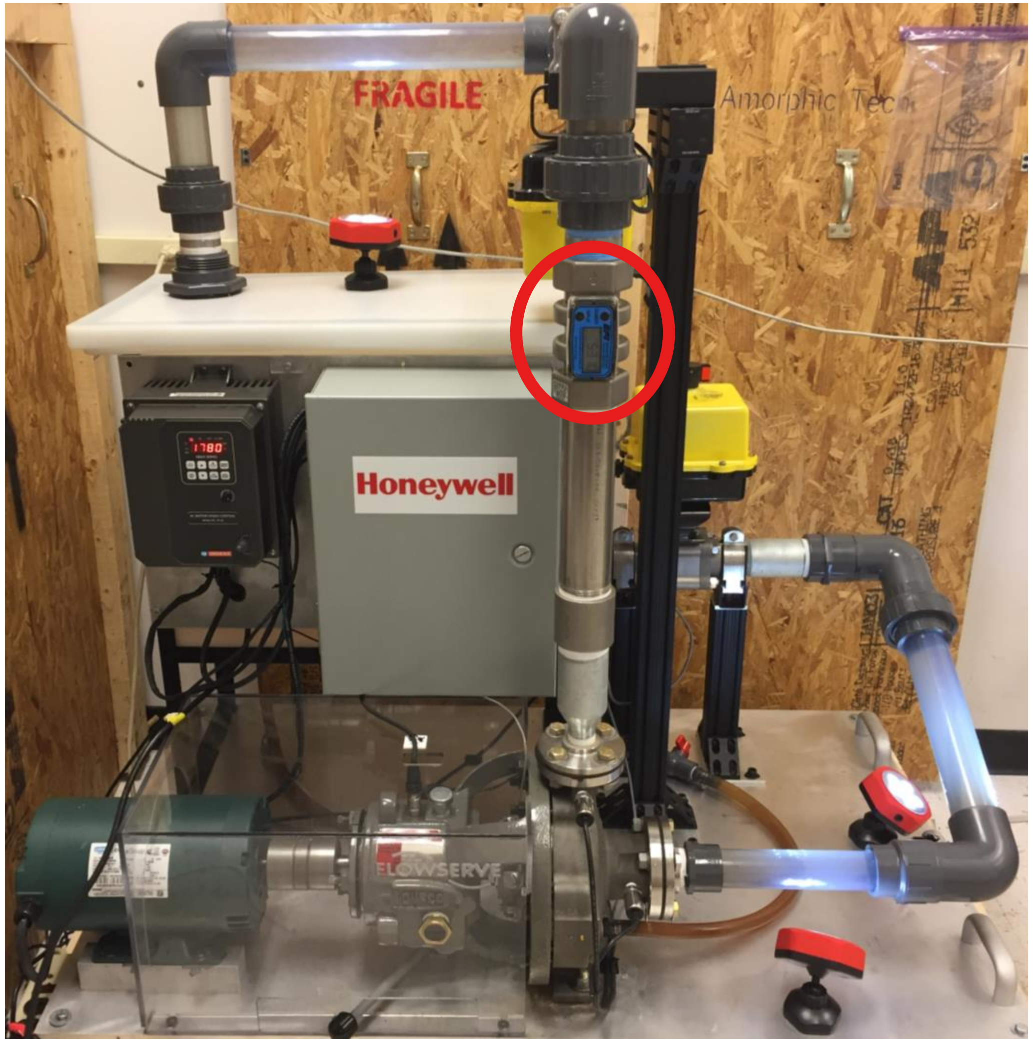
From existing measurements or calculations

Blind

Mislead

Modify operational/safety limits

In “as is” setting



1 **On one hand, the attacker does not have (easy) feedback loop**

- □ To know whether the pump is cavitating & with what intensity
- □ To estimate Time-to-Damage to plan concealment

2 **On the other hand, the attacker might have needed information**

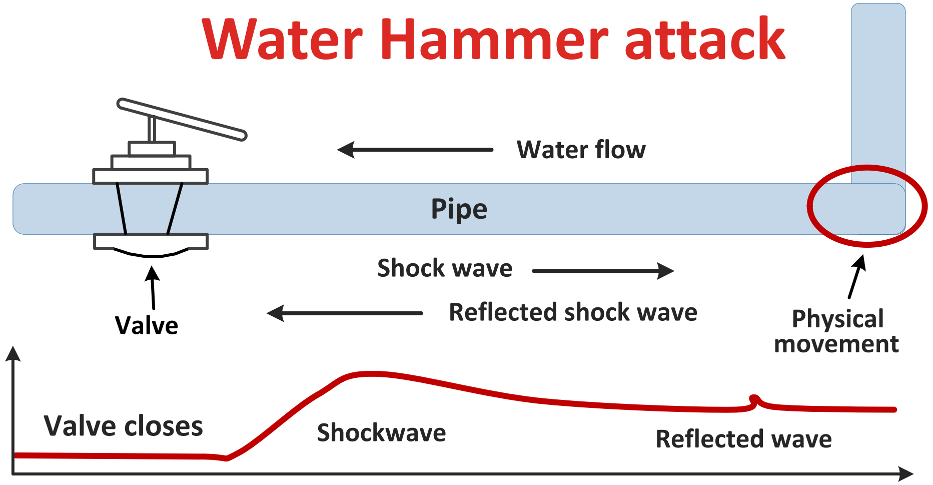
- □ E.g. stolen pump damage report
- □ Pump spec sheet

It depends…. :-)

Near-future unlikely mass-scale attack

- Complex cyber-physical attacks
  - Of high engineering precision
  - Requiring high coordination
  - Requiring considerable time & effort

Water Hammer attack



J. Larsen. Miniaturization. Black Hat USA (2014)

- Attacks which take unknown/extended time to cause needed impact
  - Deactivation of catalyst vs. disconnecting circuit breakers
- In general all attacks which require feedback loop
- Attacks with unclear collateral damage

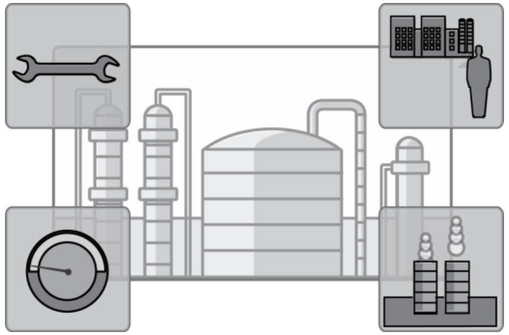
Boutique attacks

Summary

Cyber-physical security

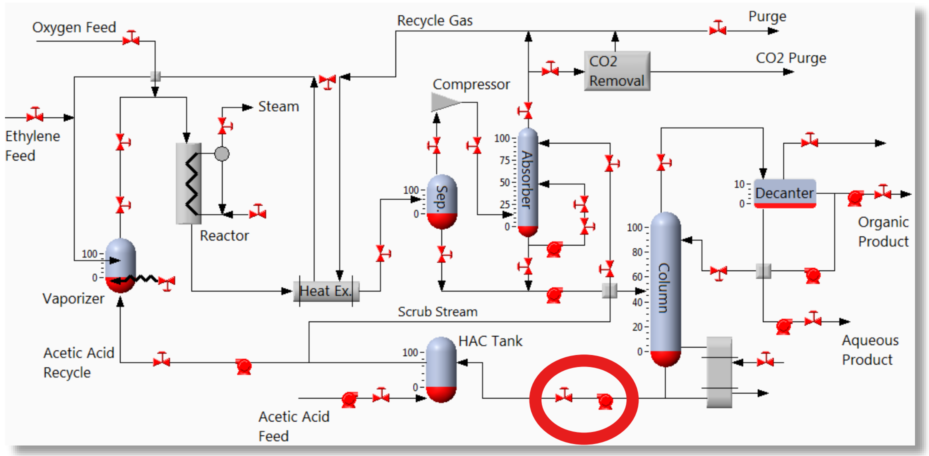
- In cyber-physical systems, physical process is a communication media for equipment and sub-systems
  - It can be leveraged for delivering attack payload (even to those assets which are not connected to the communication infrastructure)

- 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

- ❑ **ABSOLUTELY 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)

Acknowledgements

□ Flowserve and their supportive team

- For the demo rig, for playing along and for continuous support

□ AMAZING Honeywell co-workers

- Atlanta Software Center
- Industrial Cyber Security Lab
- Vancouver EDAQ team

□ ICS security community

- Friends who were there to help with tricky issues

Let’s talk

Marina Krotofil
marina.krotofil@honeywell.com
@marmusha

Honeywell