Anatomy of an Attack

~~Two~~ One ICS Attack Vector and How to Defend Against It

Nick Cappi
Director, Technical Consulting
ncappi@pas.com

13 July 2017

Agenda

- Threat Landscape
- Today's Response
- Anatomy of an Attack: Malicious Insider

Industrial Control System Cyber Attack Sources

External Threats

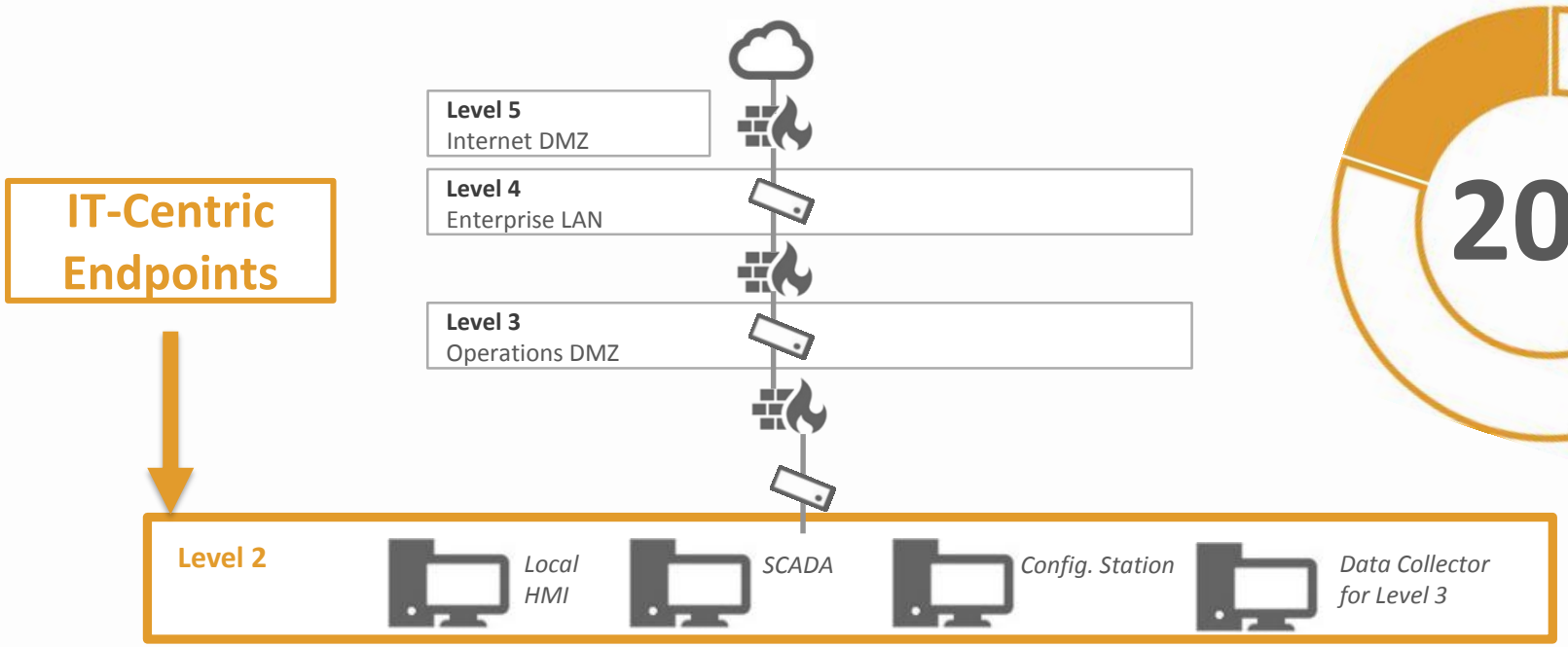
- ICS attacks up 7x from ‘10 to ’16 (1)
- 39.2% of industrial enterprise technology infrastructure attacked in 2016 (2)

Internal Threats

- 60% of attacks are insiders – 44.5% malicious & 15% inadvertent (3)
- Top BoD and CISO spending focus

(1) ICS-CERT Year in Review: Industrial Control Systems Cyber Emergency Response Team 2016
(2) Kaspersky Lab ICS Cert: Threat Landscape of Industrial Automation Systems in the Second Half of 2016
(3) IBM X-Force Research, 2016 Cyber Security Intelligence Index

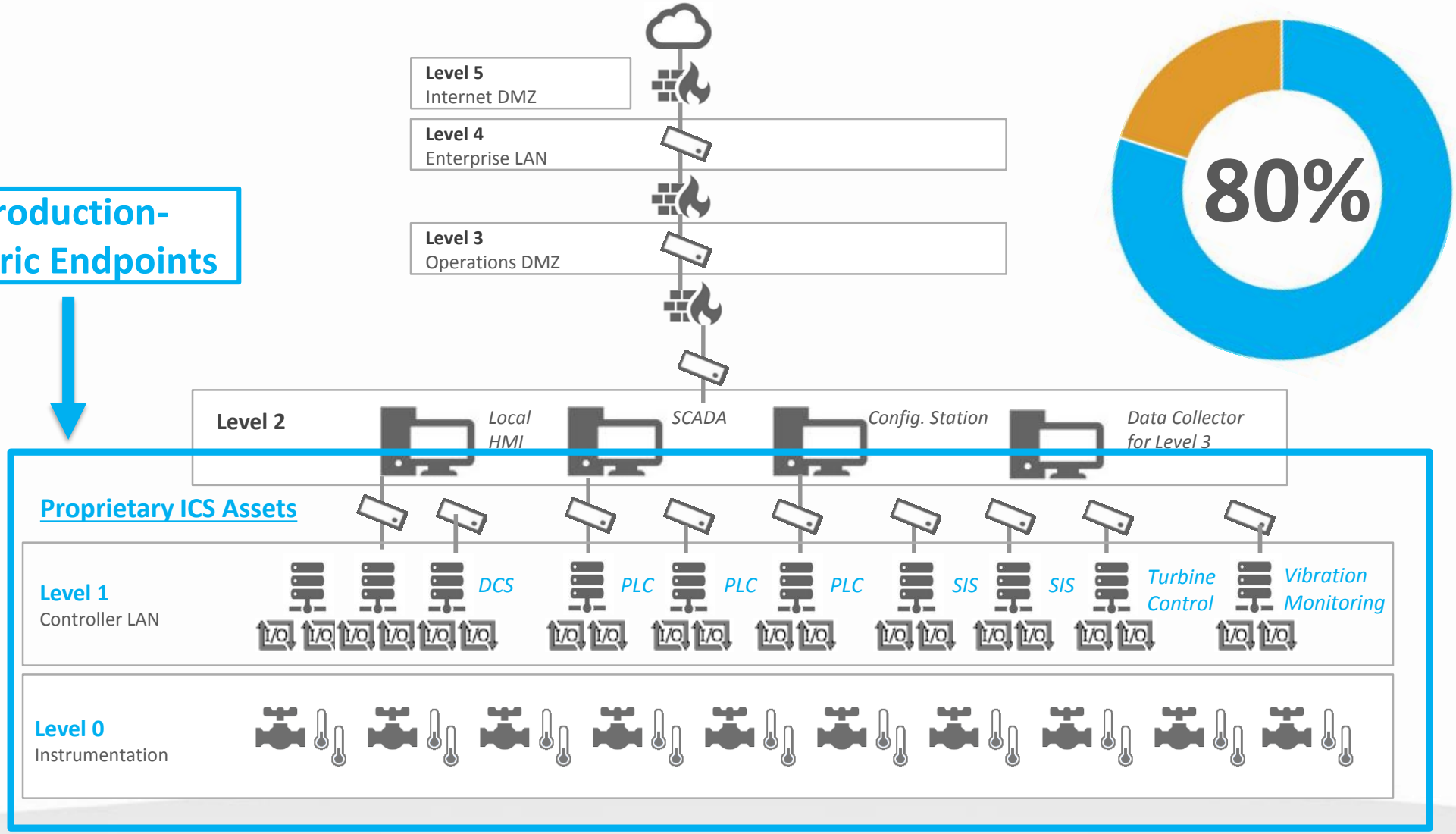
Today's IT-Centric Approach Incomplete



- Network Segmentation
- Perimeter-based Protection
- Anti-virus Software
- Air Gapping
- Security by Obscurity
- Access Controls

Production-Centric Endpoints

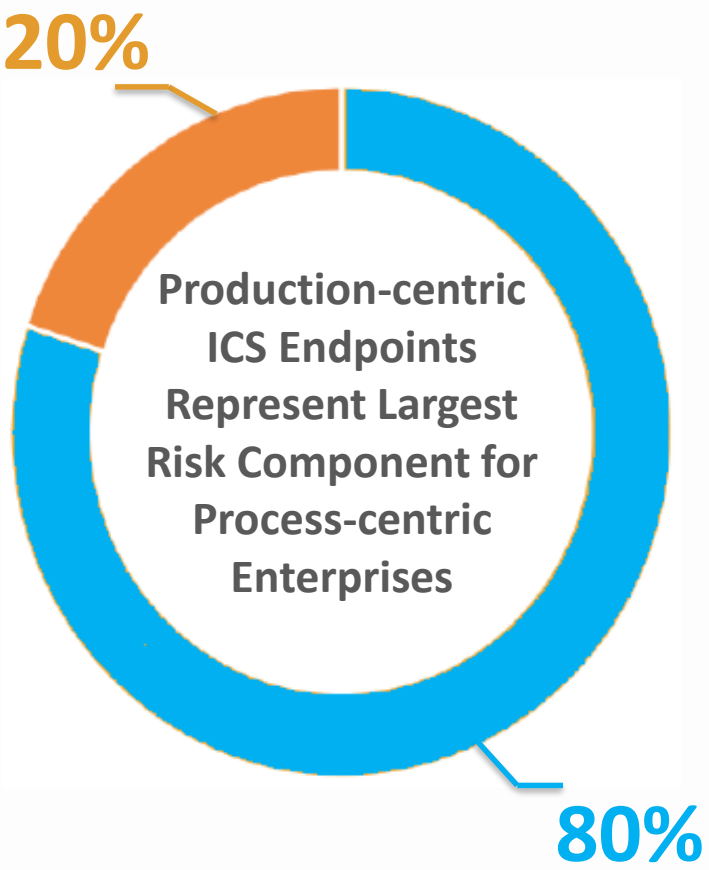
Production-Centric Endpoints



IT-Centric vs Production-cCentric Endpoints

Traditional IT-Centric Endpoints

- Windows/Unix/Linus based, common protocols
- IP addressable
- Agent software friendly
- Readily discoverable/able to interrogate servers, PCs, routers)
- Vendors such as IBM/Lenovo, Dell, HP, and Cisco Systems

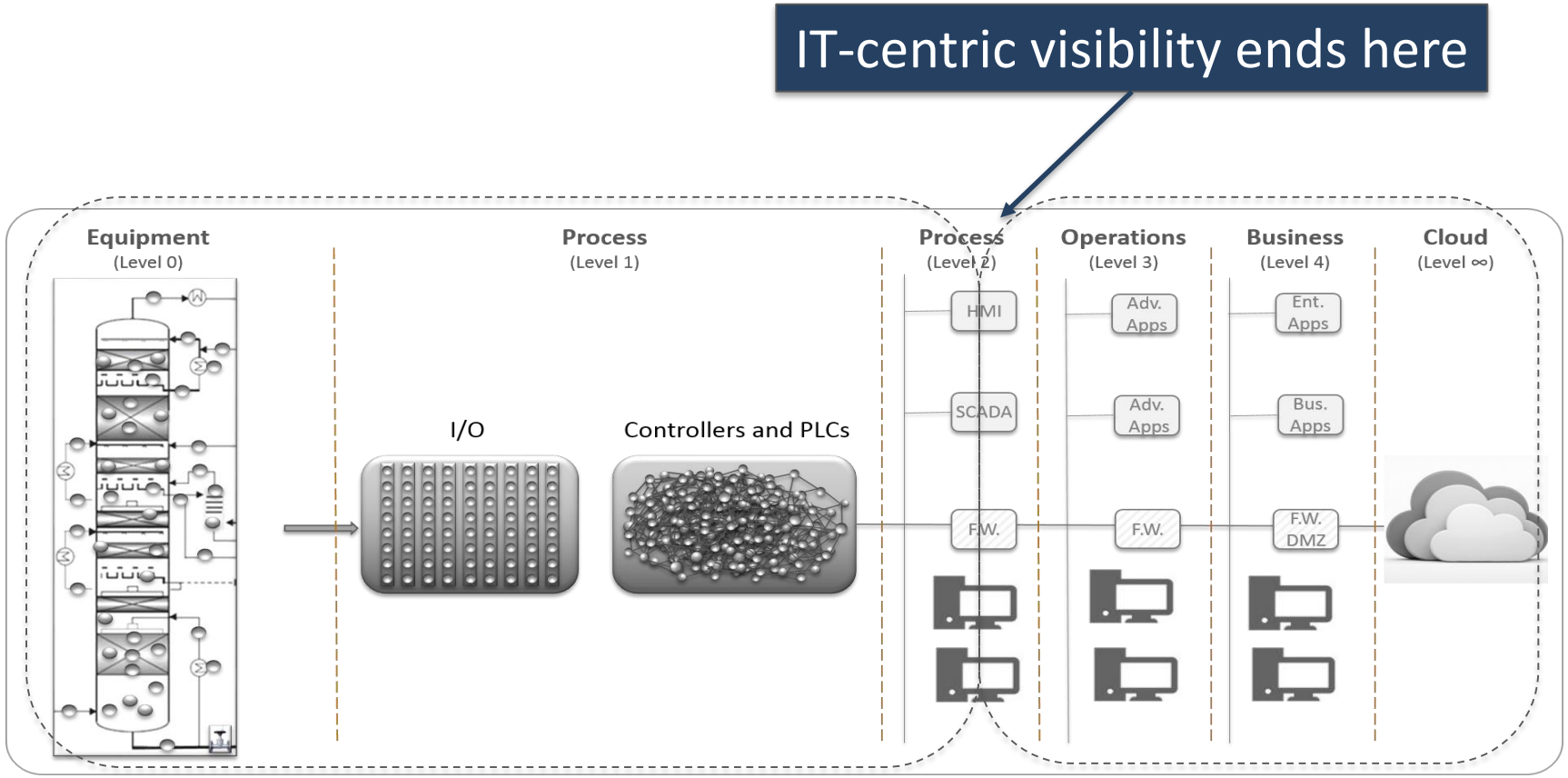


Production-Centric Endpoints

- Heterogeneous, proprietary systems, complex architectures
- Incompatible with agent technology
- “Hidden” endpoints – I/O cards, firmware, installed software, configuration, etc.
- Vendors such as ABB, Emerson, Honeywell, Yokogawa, Siemens, Schneider, Rockwell, & more…

Scenario 1 – Malicious Insider

Major Gap - Limited Level 1 and 0 Visibility

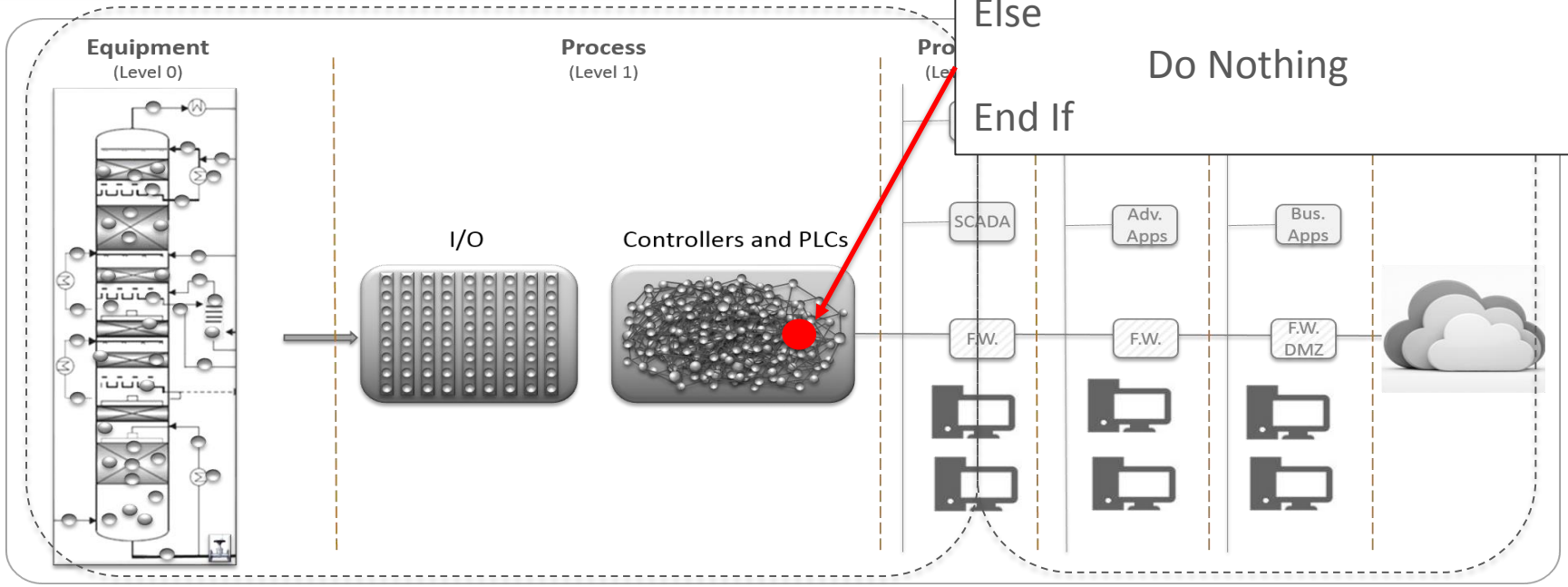


Some Protection Built-in – But Not Enough

The system will do nothing if Setpoint value outside of engineered range

Example Logic:

```
If FC001.SP >= FC001.Low Range And _
   FC001.SP <= FC001.High Range Then
            Run Normal PID Error Handling
Else
            Do Nothing
End If
```

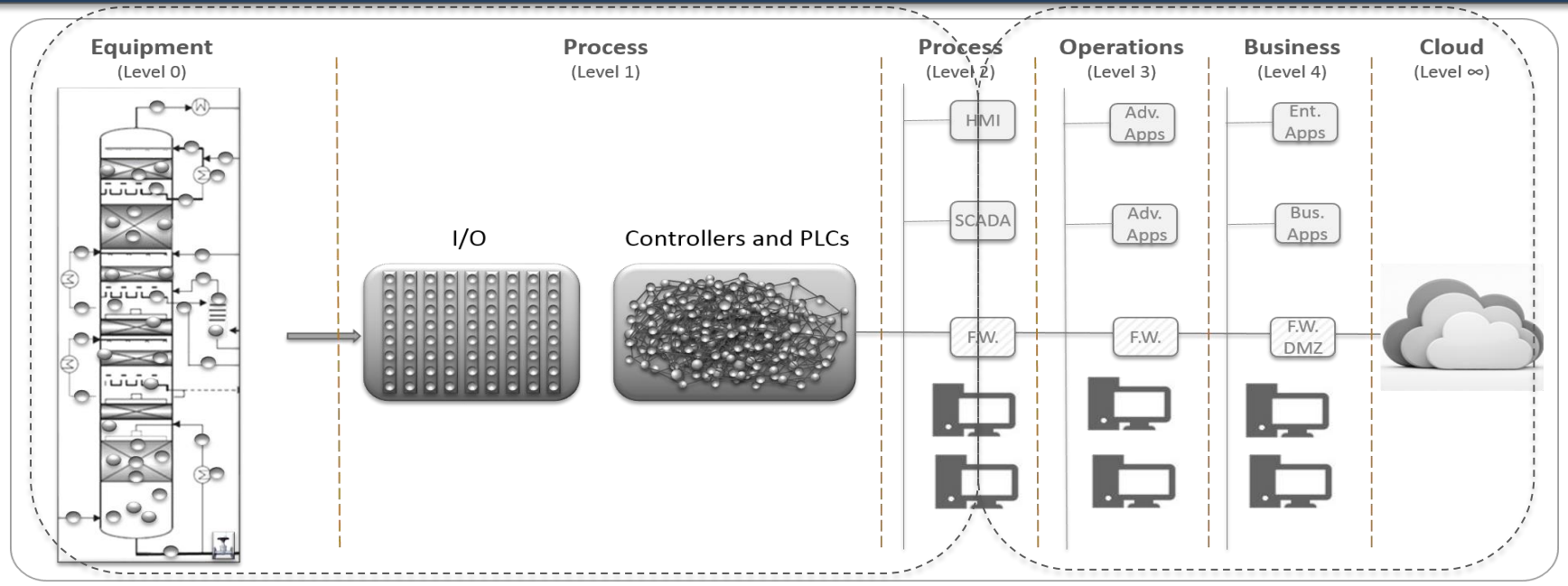


Scenario Summary

First, a malicious offline Engineering Configurator Project Change is made – BUT NOT DOWNLOADED!

Then, an authorized change is made and downloaded

Consequences - process shuts down

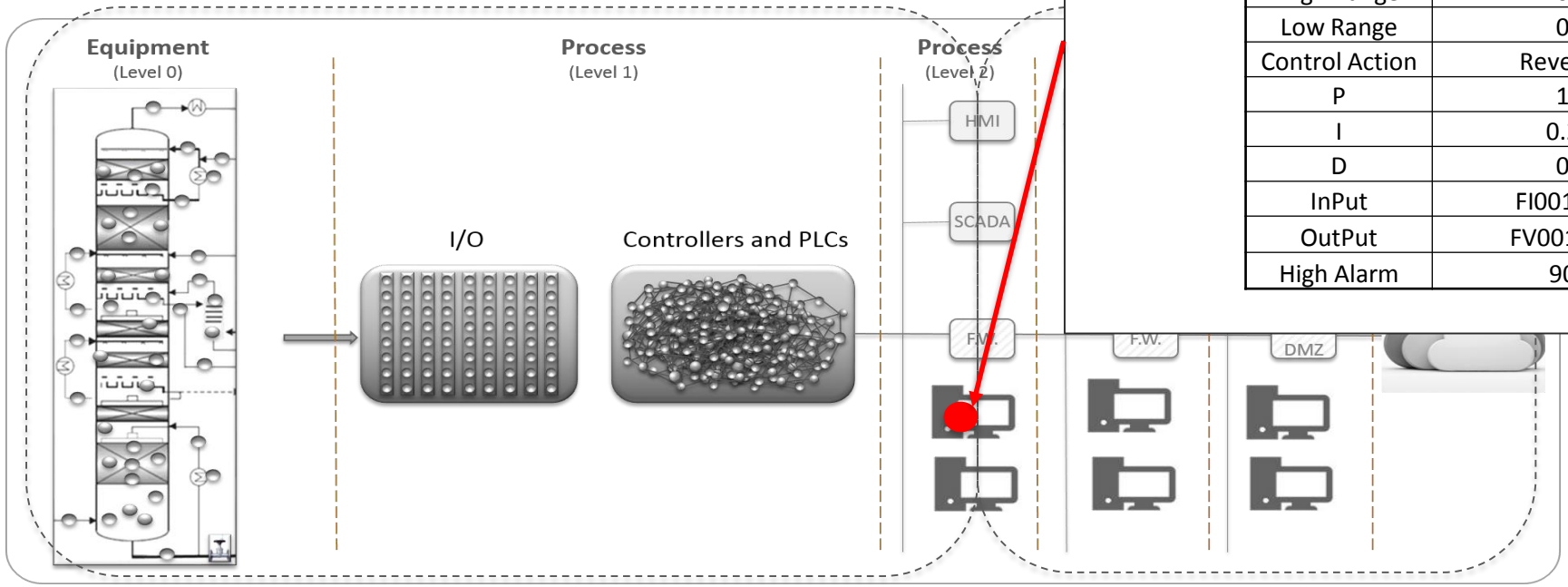


System Before Change

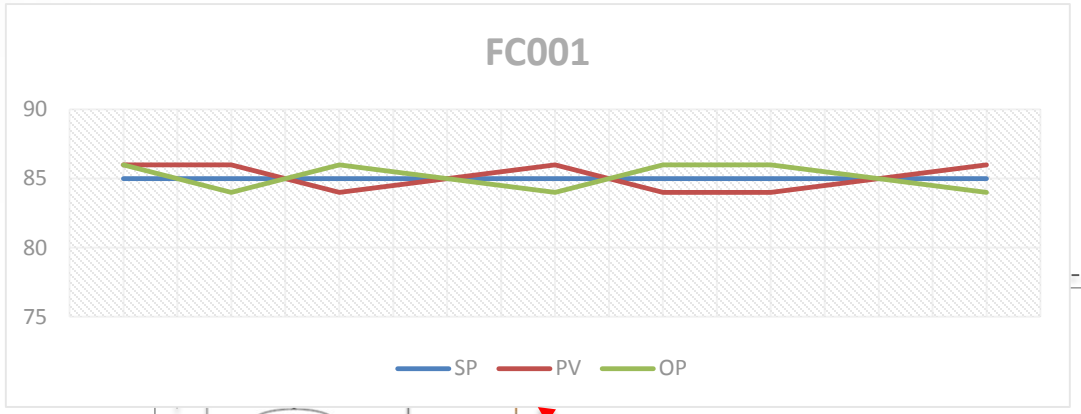
Configurator project before the change

Example Flow Controller Configuration:

FC001 Configuration	
Parameter	**Value**
Name	FC001
Description	Flow to Reactor
Engineering Unit	BPH
High Range	100
Low Range	0
Control Action	Reverse
P	1
I	0.2
D	0
InPut	FI001.PV
OutPut	FV001.OP
High Alarm	90



System Before Change



Operator Settings:

FC001.SP = 85 BPH (Target Value)

FC001.PV = ~85 BPH (Actual Value) (17.6 Milliamps)

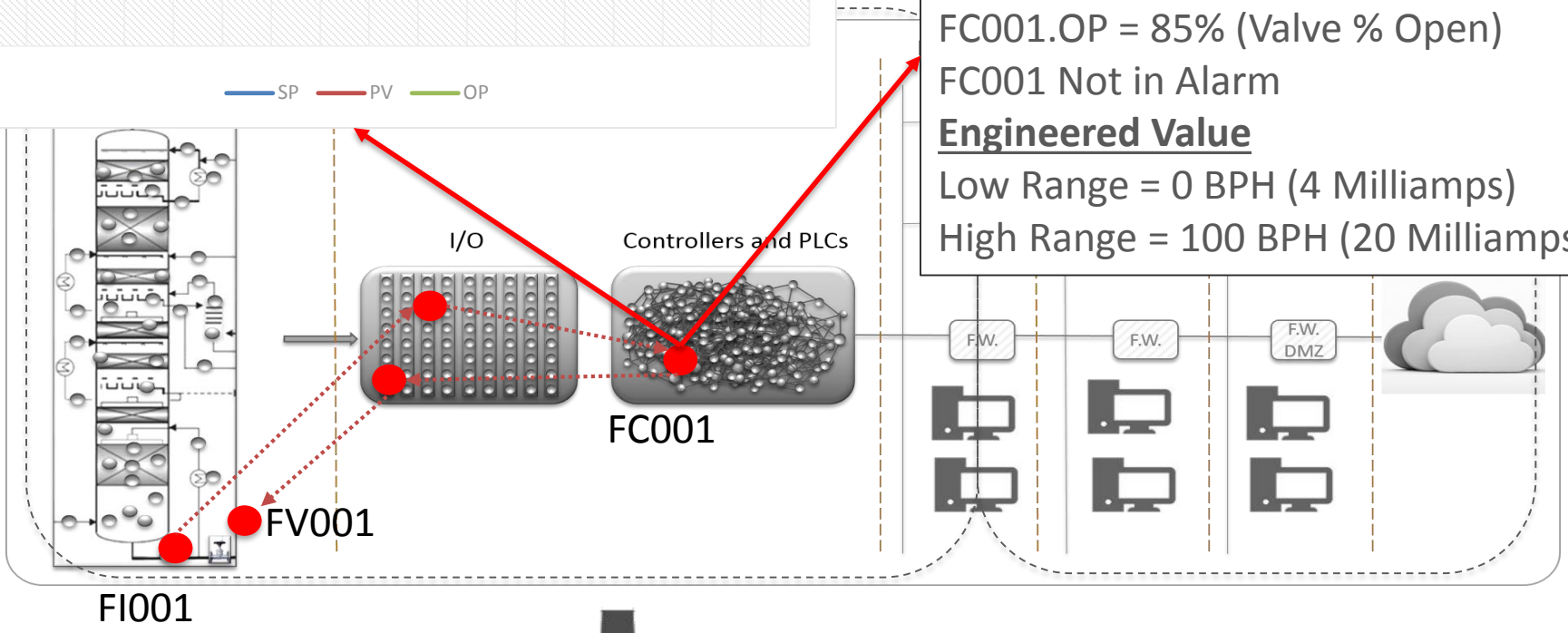
FC001.OP = 85% (Valve % Open)

FC001 Not in Alarm

Engineered Value

Low Range = 0 BPH (4 Milliamps)

High Range = 100 BPH (20 Milliamps)

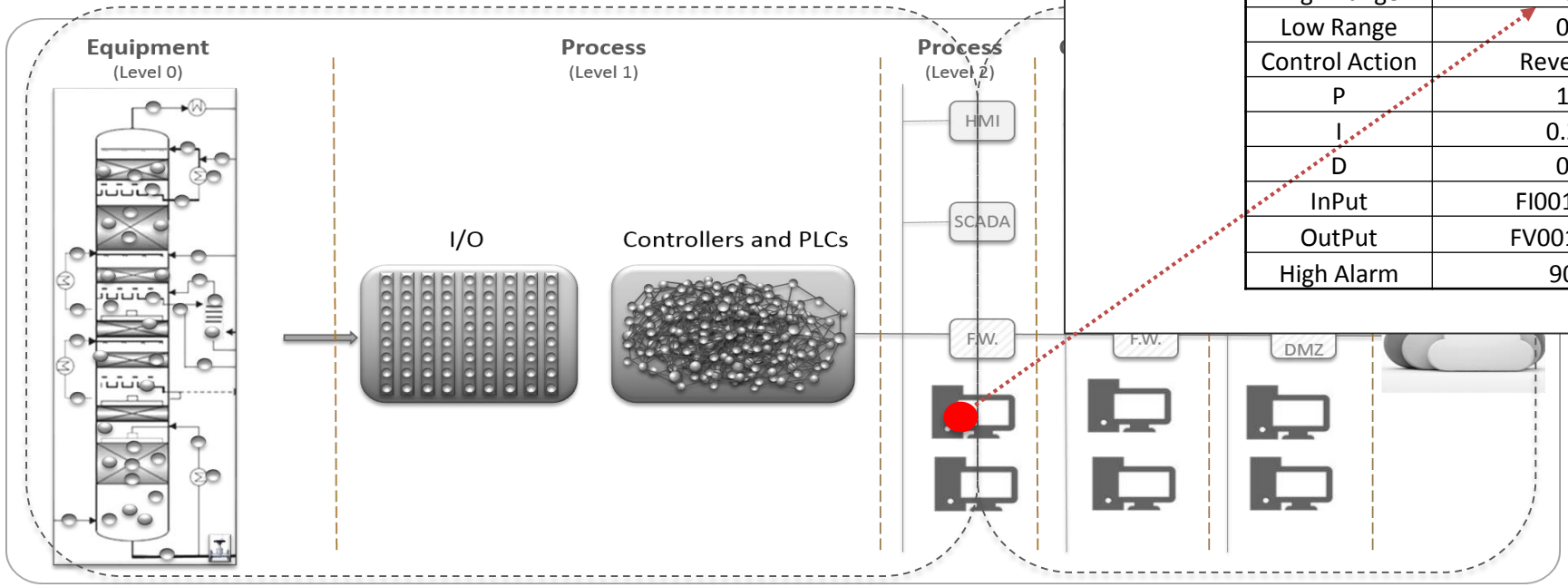


Action 1 – Malicious Insider Makes Offline Change

Configurator project after the change
High Range changed from 100 to 10

Example Flow Controller Configuration:

FC001 Configuration	
Parameter	**Value**
Name	FC001
Description	Flow to Reactor
Engineering Unit	BPH
High Range	10
Low Range	0
Control Action	Reverse
P	1
I	0.2
D	0
InPut	FI001.PV
OutPut	FV001.OP
High Alarm	90

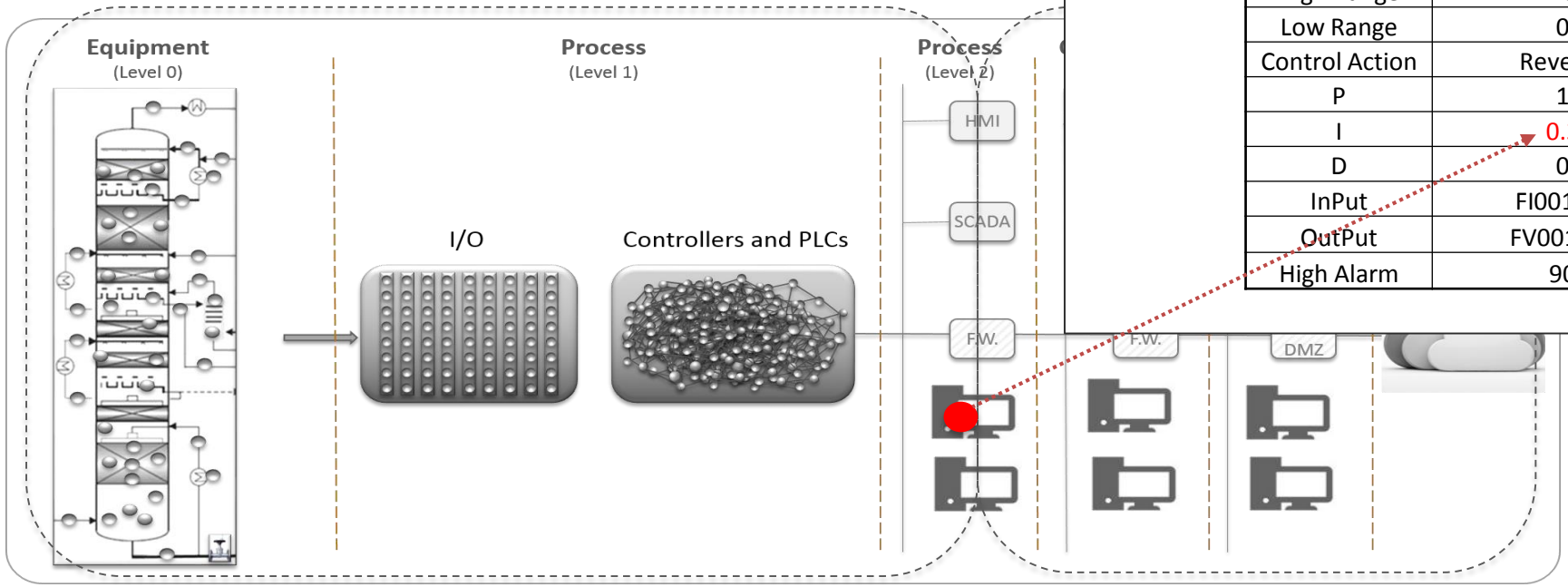


Action 2 – Authorized Change Made

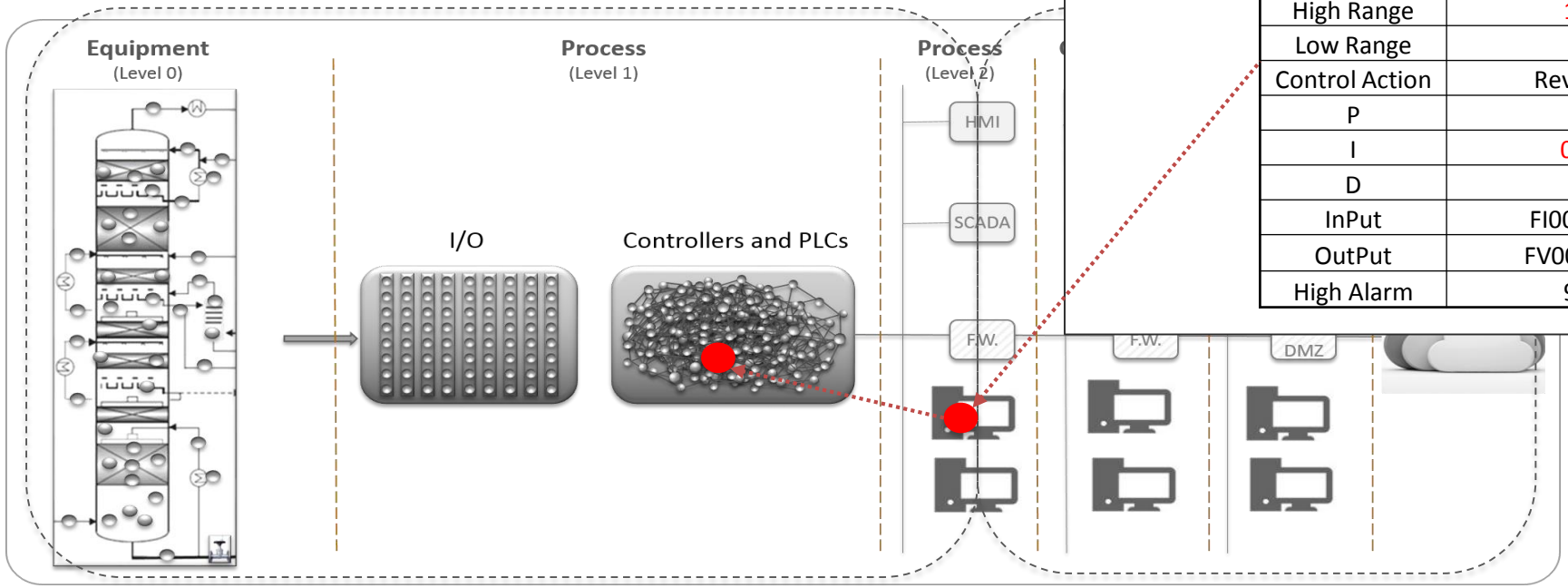
PID Integral changed from .2 to .3

Example Flow Controller Configuration:

FC001 Configuration	
Parameter	**Value**
Name	FC001
Description	Flow to Reactor
Engineering Unit	BPH
High Range	10
Low Range	0
Control Action	Reverse
P	1
I	0.3
D	0
InPut	FI001.PV
OutPut	FV001.OP
High Alarm	90



Action 2 Continued – Download to Flow Controller

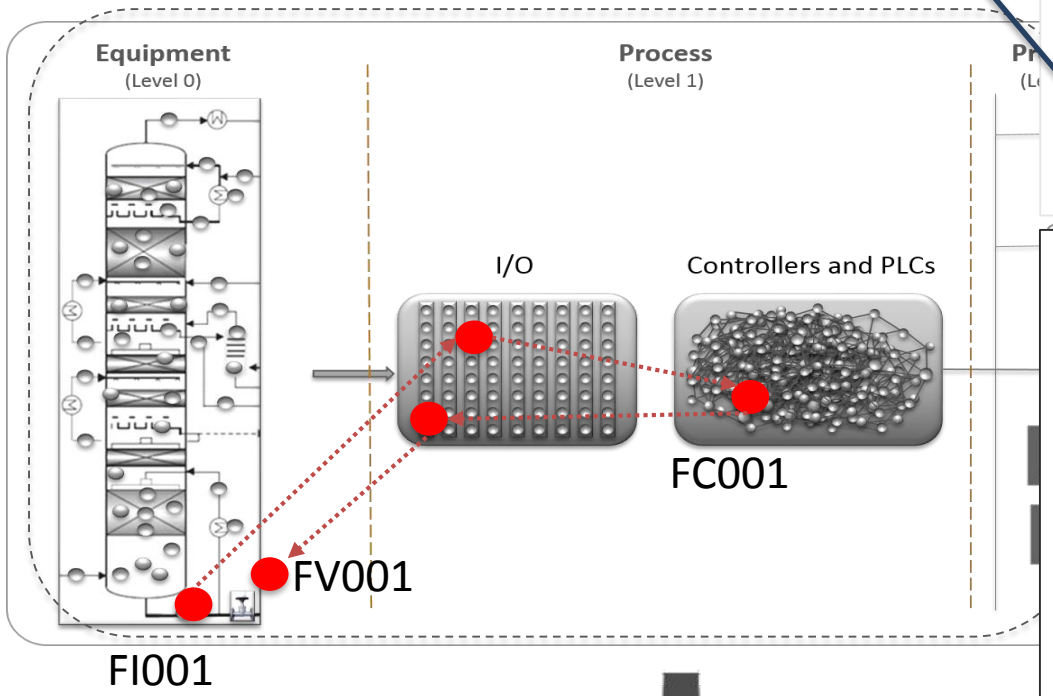


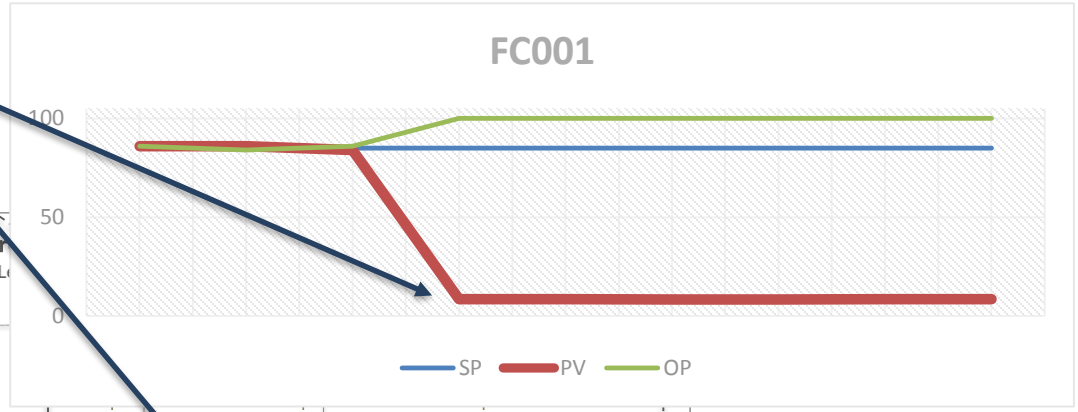
Example Flow Controller Configuration:

FC001 Configuration	
Parameter	**Value**
Name	FC001
Description	Flow to Reactor
Engineering Unit	BPH
High Range	10
Low Range	0
Control Action	Reverse
P	1
I	0.3
D	0
InPut	FI001.PV
OutPut	FV001.OP
High Alarm	90

Consequences of the Change

Factor of 10 decrease in High Range Flow Controller calculates 8.5 BPH





Operator Settings:

FC001.SP = 85 BPH (Target Value)

FC001.PV = ~8.5 BPH (Actual Value) (17.6 Milliamps)

FC001.OP = 85% (Valve % Open)

FC001 Not in Alarm

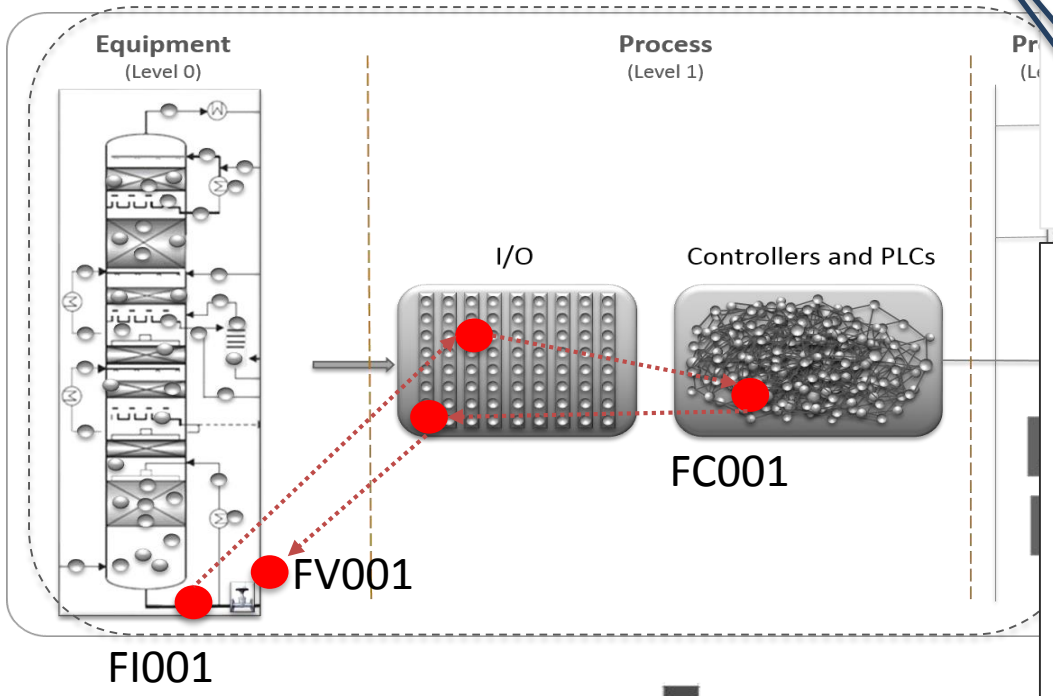
Engineered Value

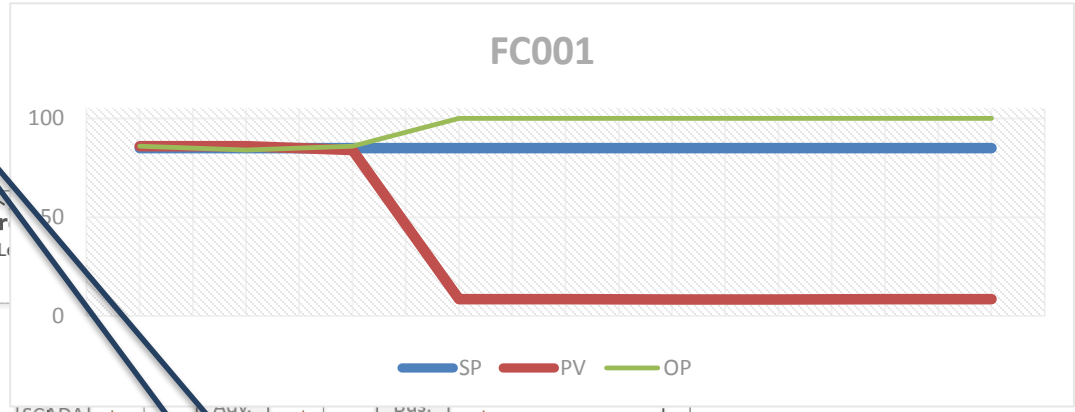
Low Range = 0 BPH (4 Milliamps)

High Range = 10 BPH (20 Milliamps)

Consequences of the Change

Now there is a greater deviation between Setpoint (Target Value) and Process Value (Actual Value)





Operator Settings:

FC001.SP = 85 BPH (Target Value)

FC001.PV = ~8.5 BPH (Actual Value) (17.6 Milliamps)

FC001.OP = 85% (Valve % Open)

FC001 Not in Alarm

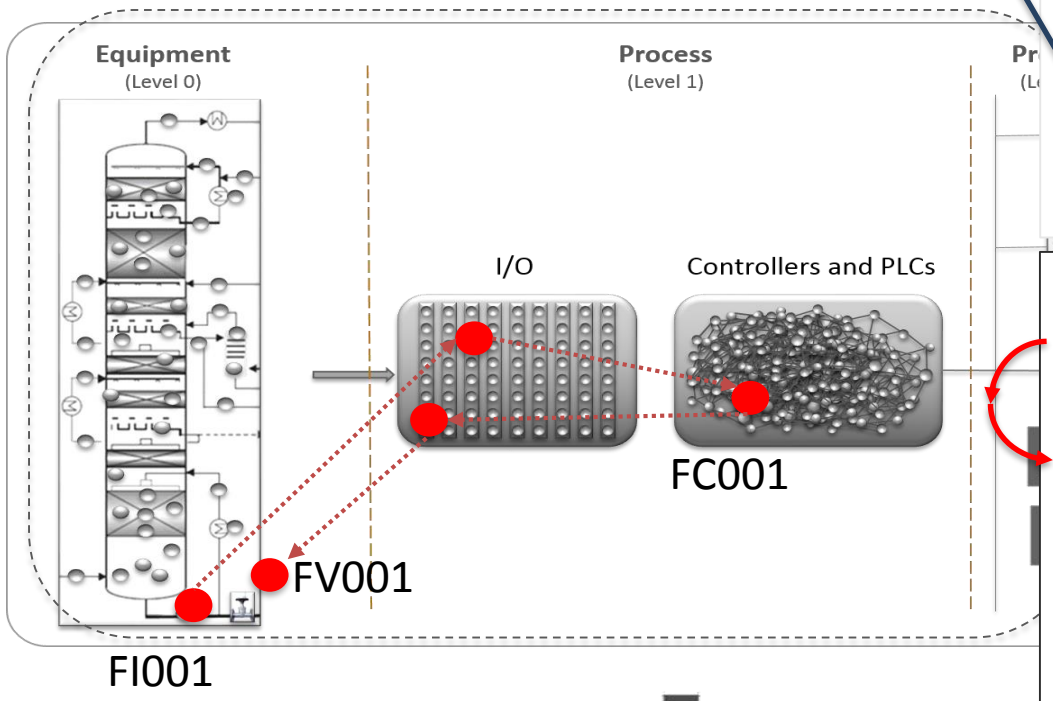
Engineered Value

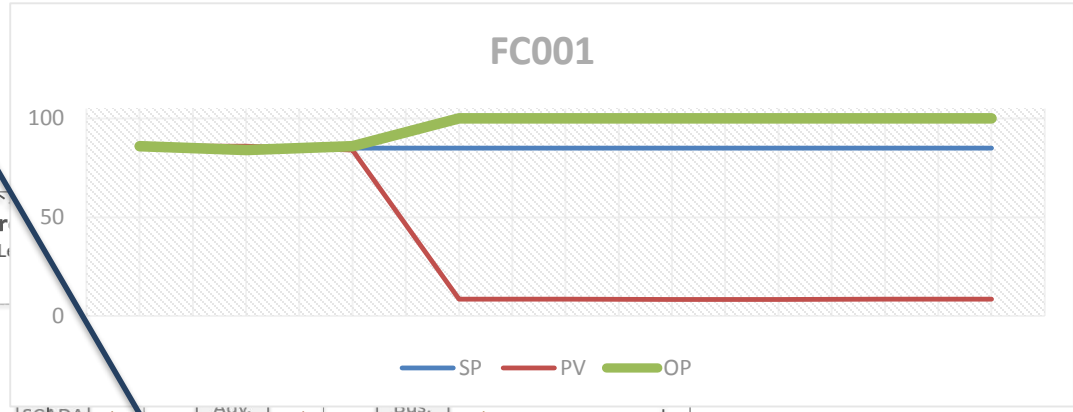
Low Range = 0 BPH (4 Milliamps)

High Range = 10 BPH (20 Milliamps)

Consequences of the Change

The OP (Valve) Increases to try and Reach SP (Target Value) – goes from 85% to 100%





Operator Settings:

FC001.SP = 85 BPH (Target Value)

FC001.PV = ~8.5 BPH (Actual Value) (17.6 Milliamps)

FC001.OP = 100% (Valve % Open)

FC001 Not in Alarm

Engineered Value

Low Range = 0 BPH (4 Milliamps)

High Range = 10 BPH (20 Milliamps)

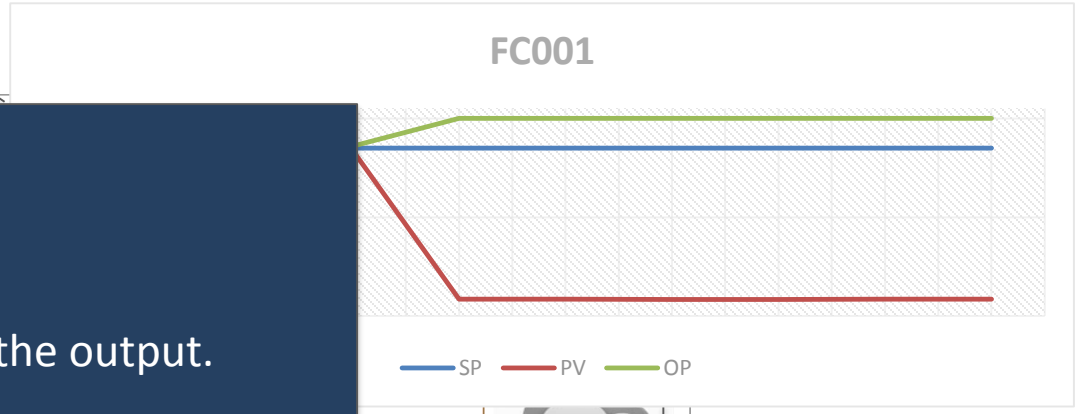
Impact Summary – Confusion & Process Shuts Down

Operator Confusion

- Why is the valve at 100%?
- Why is there no alarm?
- If caught quickly - place the valve in manual and control the output.
- If not caught quickly - unit shuts down (hopefully safely)

Engineer Confusion

- How could the PID Integral change form .2 to .3 result in this behavior?
- There is no record of the Malicious change as a result the issue will most likely get classified as an inadvertent change



s:

PH (Target Value)

BPH (Actual Value) (17.6 Milliamps)

% (Valve % Open)

rm

e

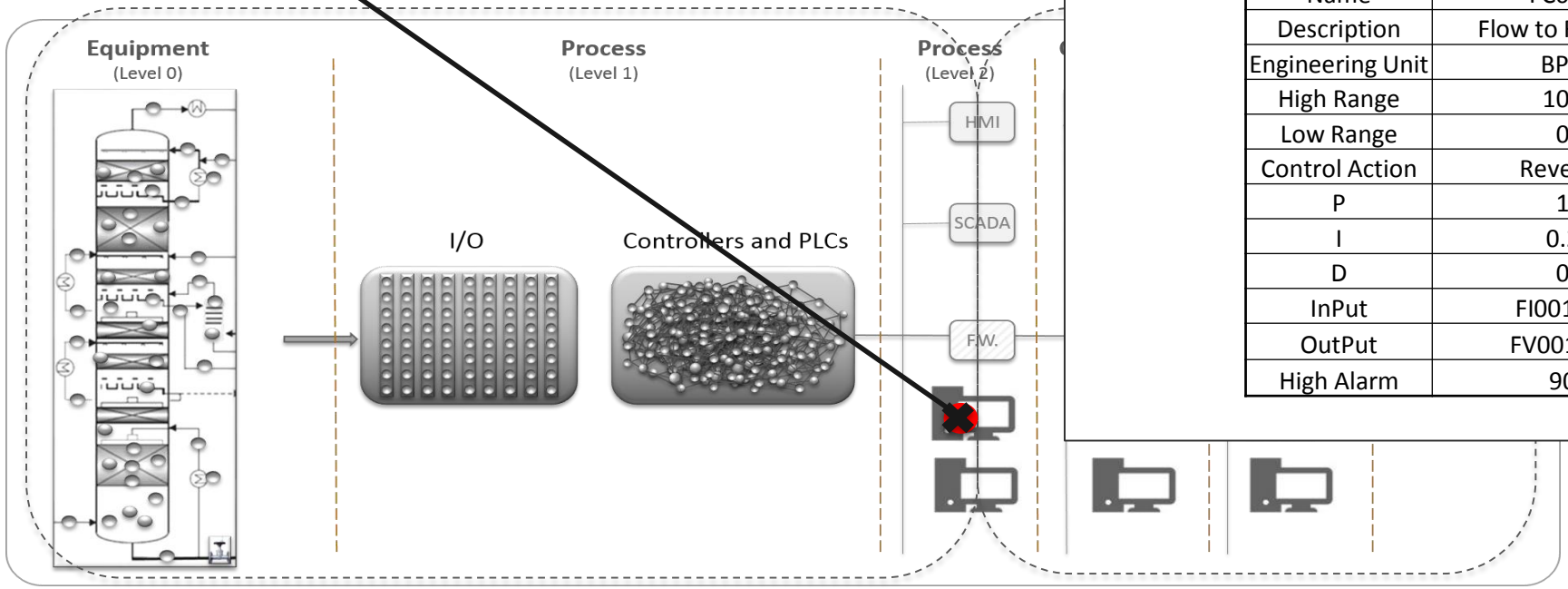
Low Range = 0 BPH (4 Milliamps)

High Range = 10 BPH (20 Milliamps)

SCENARIO 1 - DEFENDING

Defending

Monitor the offline configuration of the Control System

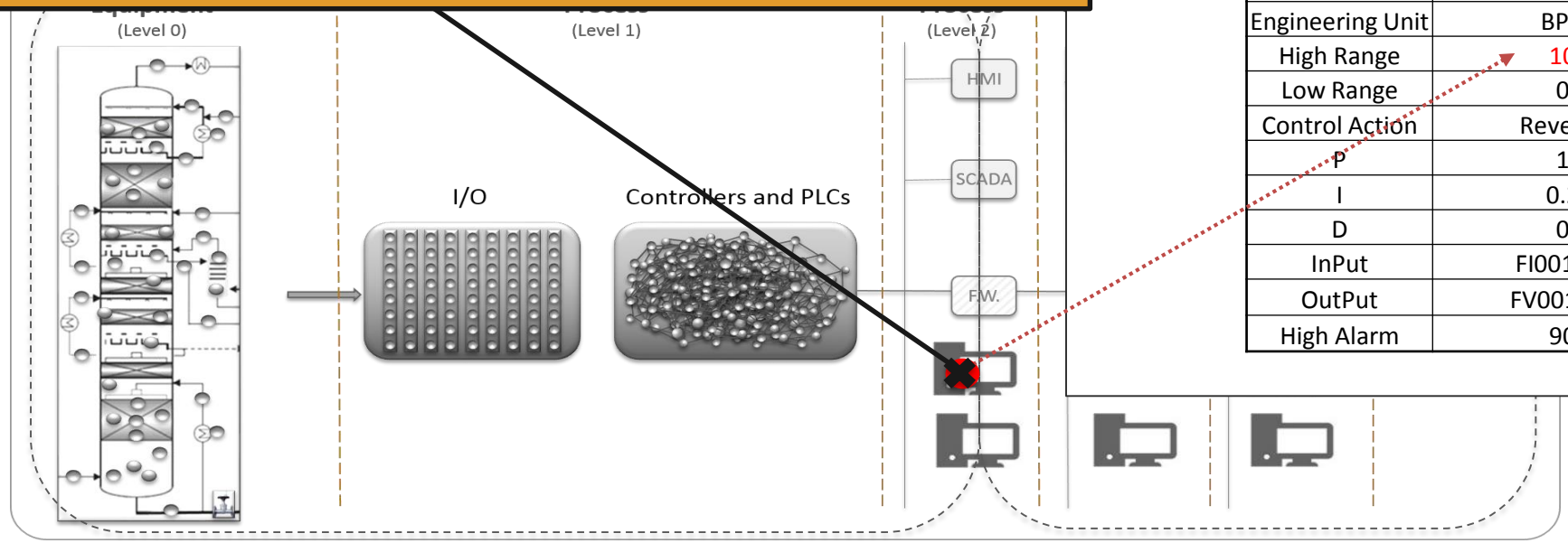


Example Flow Controller Configuration:

FC001 Configuration	
Parameter	**Value**
Name	FC001
Description	Flow to Reactor
Engineering Unit	BPH
High Range	100
Low Range	0
Control Action	Reverse
P	1
I	0.2
D	0
InPut	FI001.PV
OutPut	FV001.OP
High Alarm	90

Defending

- Detect access and change within the environment.
- You must have context at this point because the configurator UI shows nicely formatted data but the actual control system config file is binary

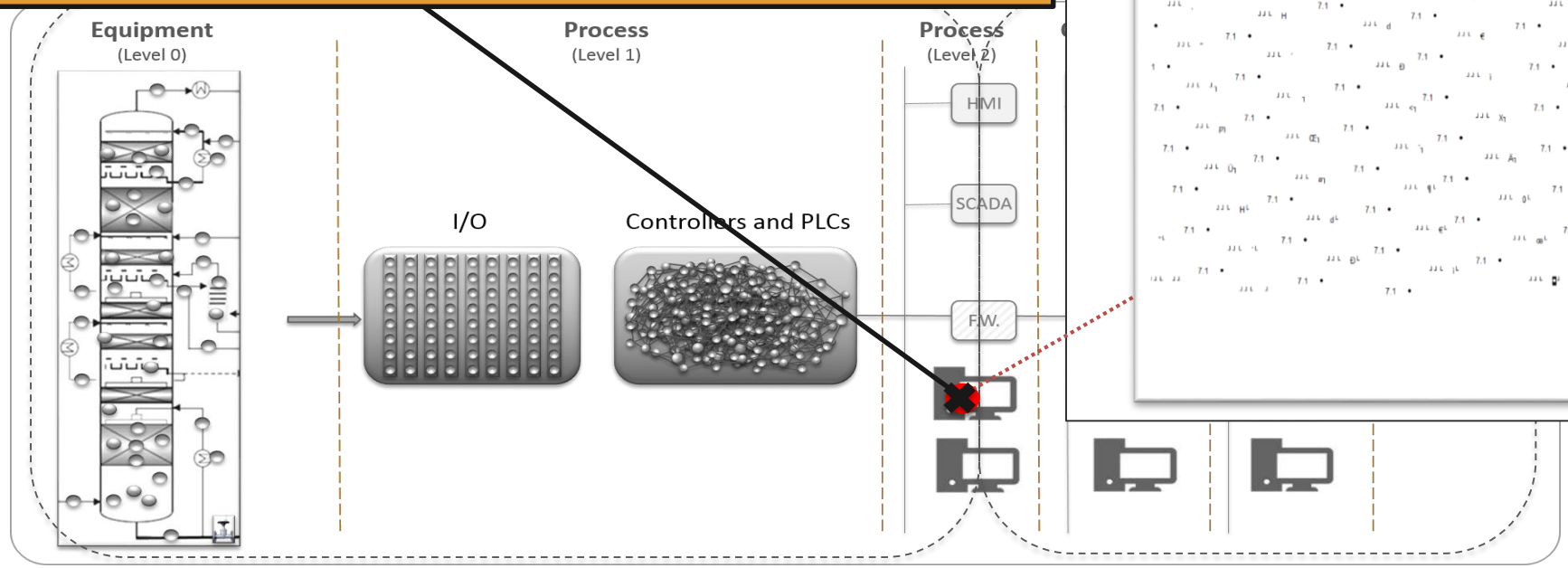


Example Flow Controller Configuration:

FC001 Configuration	
Parameter	**Value**
Name	FC001
Description	Flow to Reactor
Engineering Unit	BPH
High Range	10
Low Range	0
Control Action	Reverse
P	1
I	0.2
D	0
InPut	FI001.PV
OutPut	FV001.OP
High Alarm	90

Defending

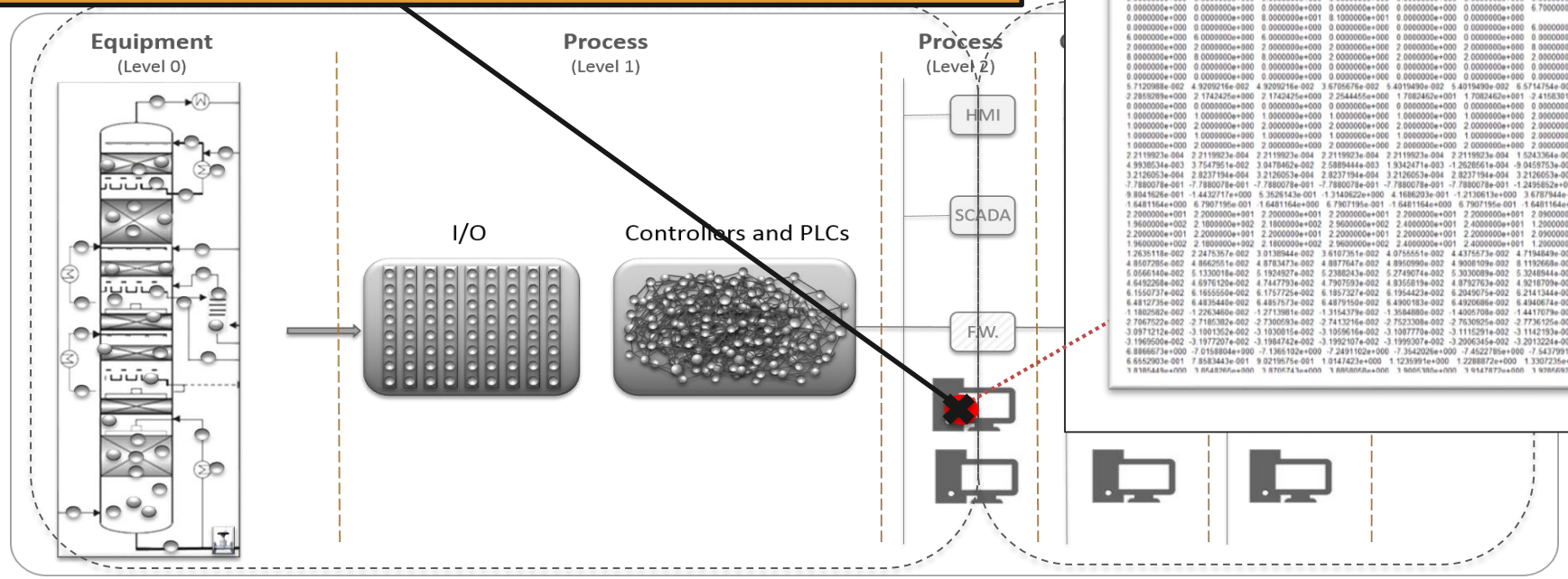
Detect Access and change within the environment - must be able to interpret binary configuration files.



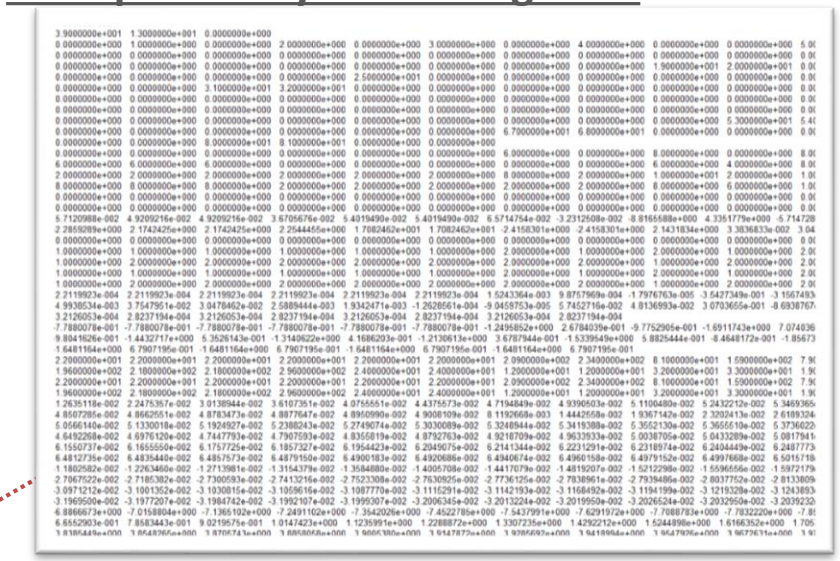
Example Yokogawa Config. File:

Defending

Detect Access and change within the environment - must be able to interpret binary configuration files.

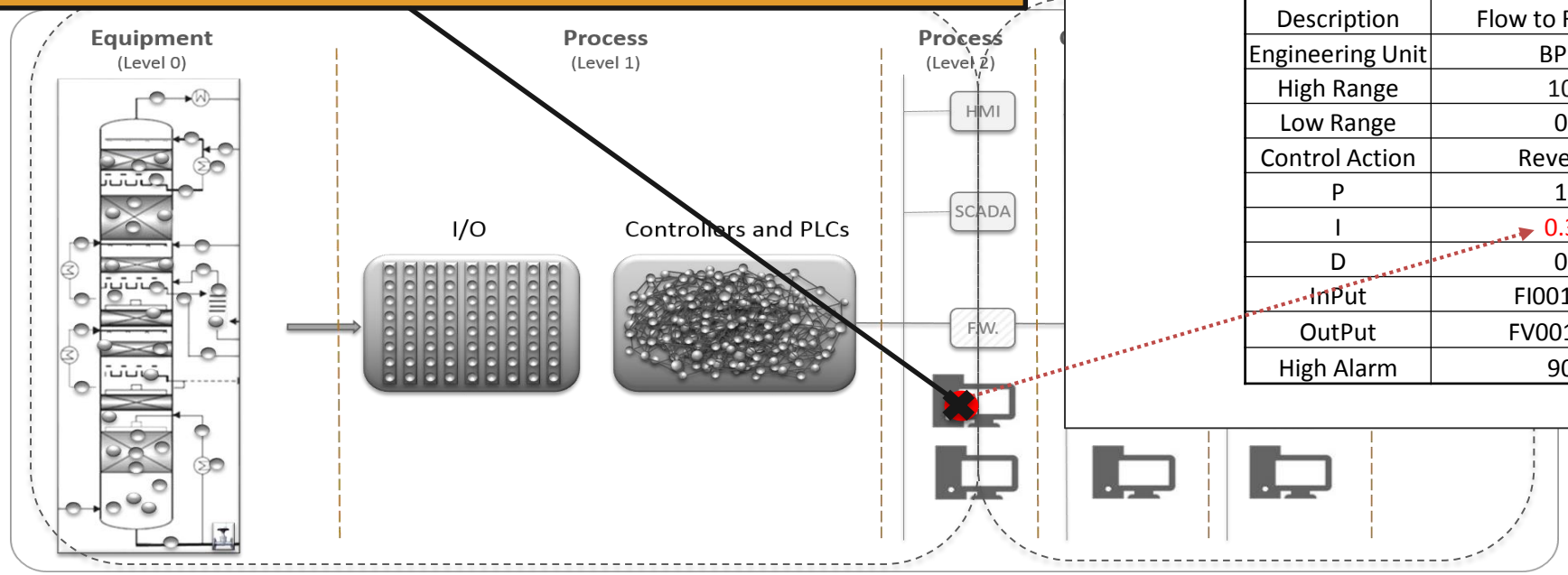


Example Honeywell Config. File:



Defending

You must have something or someone who understands what's a normal operational change compared to a potential security change

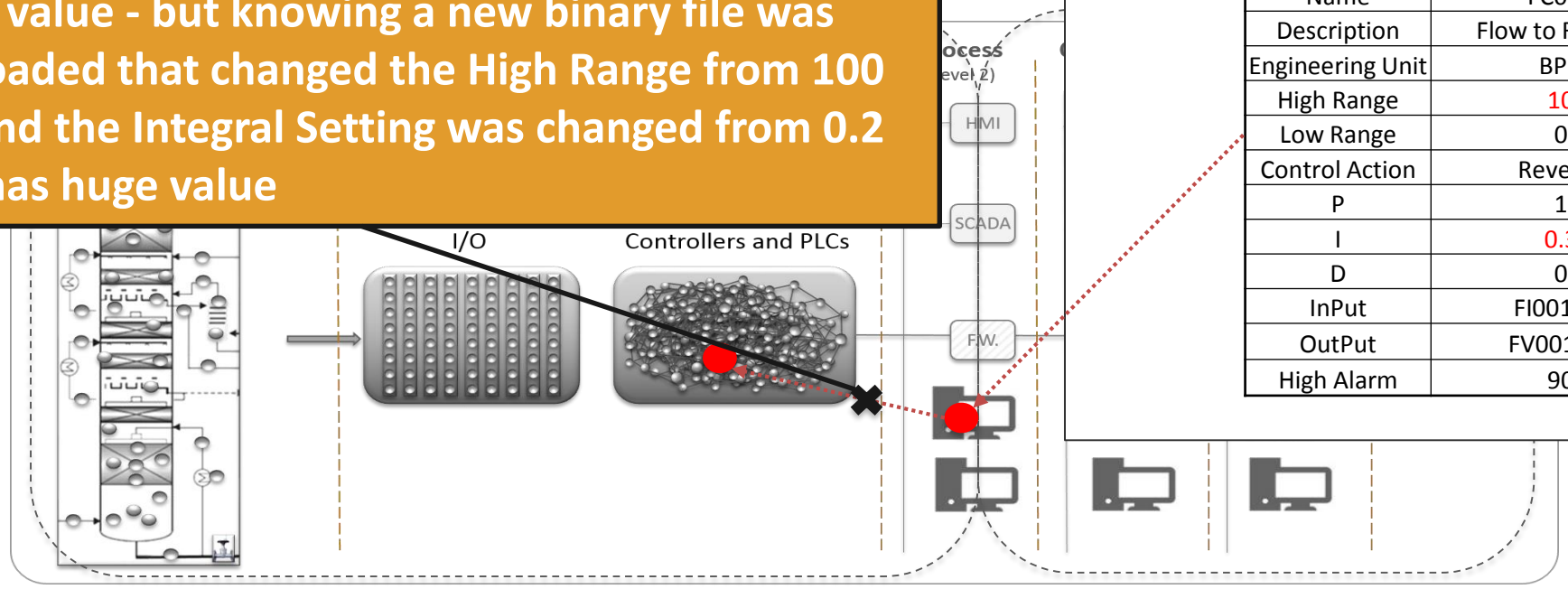


Example Flow Controller Configuration:

FC001 Configuration	
Parameter	**Value**
Name	FC001
Description	Flow to Reactor
Engineering Unit	BPH
High Range	10
Low Range	0
Control Action	Reverse
P	1
I	0.3
D	0
InPut	FI001.PV
OutPut	FV001.OP
High Alarm	90

Defending

- You need to be able to detect the download event
- Its equally important to understand the context of what's being downloaded.
- Knowing a new binary file was downloaded has limited value - but knowing a new binary file was downloaded that changed the High Range from 100 to 10 and the Integral Setting was changed from 0.2 to 0.3 has huge value



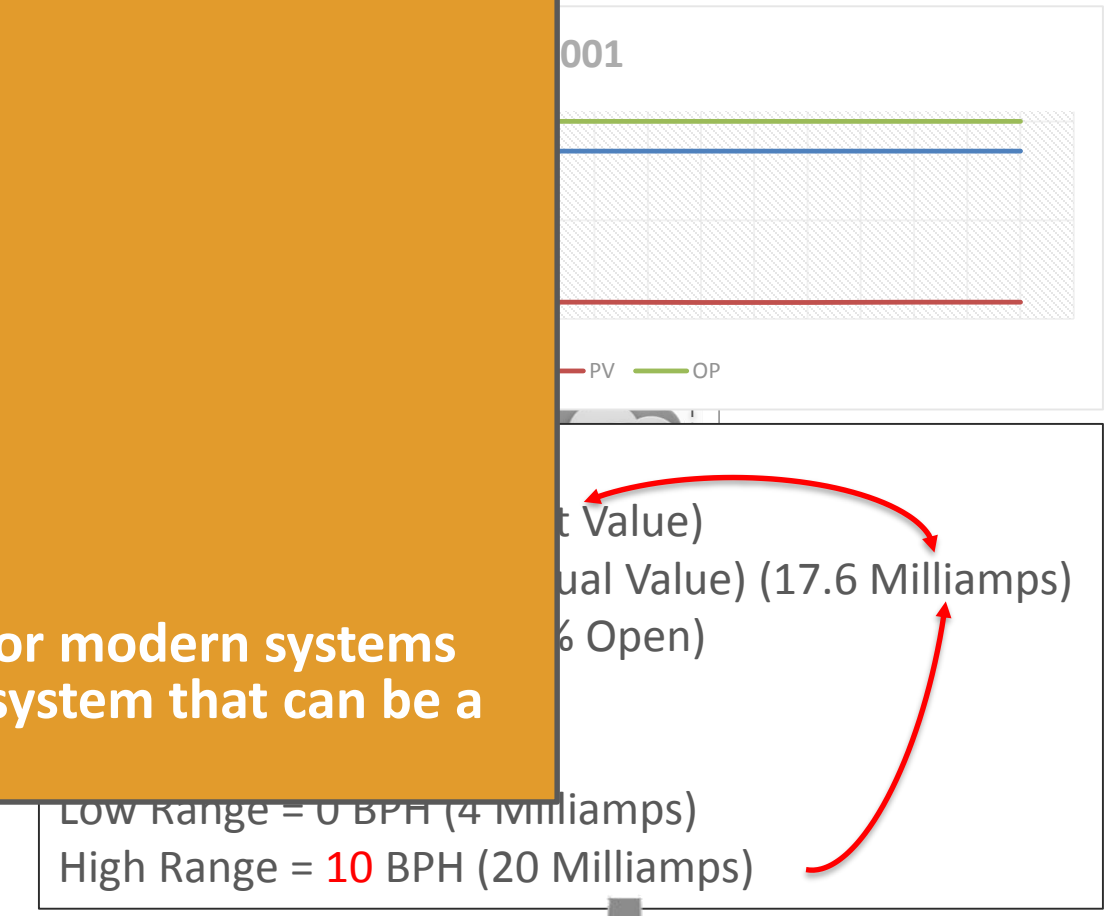
Example Flow Controller Configuration:

FC001 Configuration	
Parameter	**Value**
Name	FC001
Description	Flow to Reactor
Engineering Unit	BPH
High Range	10
Low Range	0
Control Action	Reverse
P	1
I	0.3
D	0
InPut	FI001.PV
OutPut	FV001.OP
High Alarm	90

Defending – Summary Actions to Take

You need:

- A tool that allows you access to forensic details:
  - Online Changes
  - Offline Changes
  - Events
    - Application
    - Security
    - System Events
    - Operator Actions
    - Process Alarms
  - Normal Behavior compared to Abnormal Behavior
- Access to Restore Points to Revert the Change - for modern systems that's an easier problem to solve, but for legacy system that can be a challenging problem

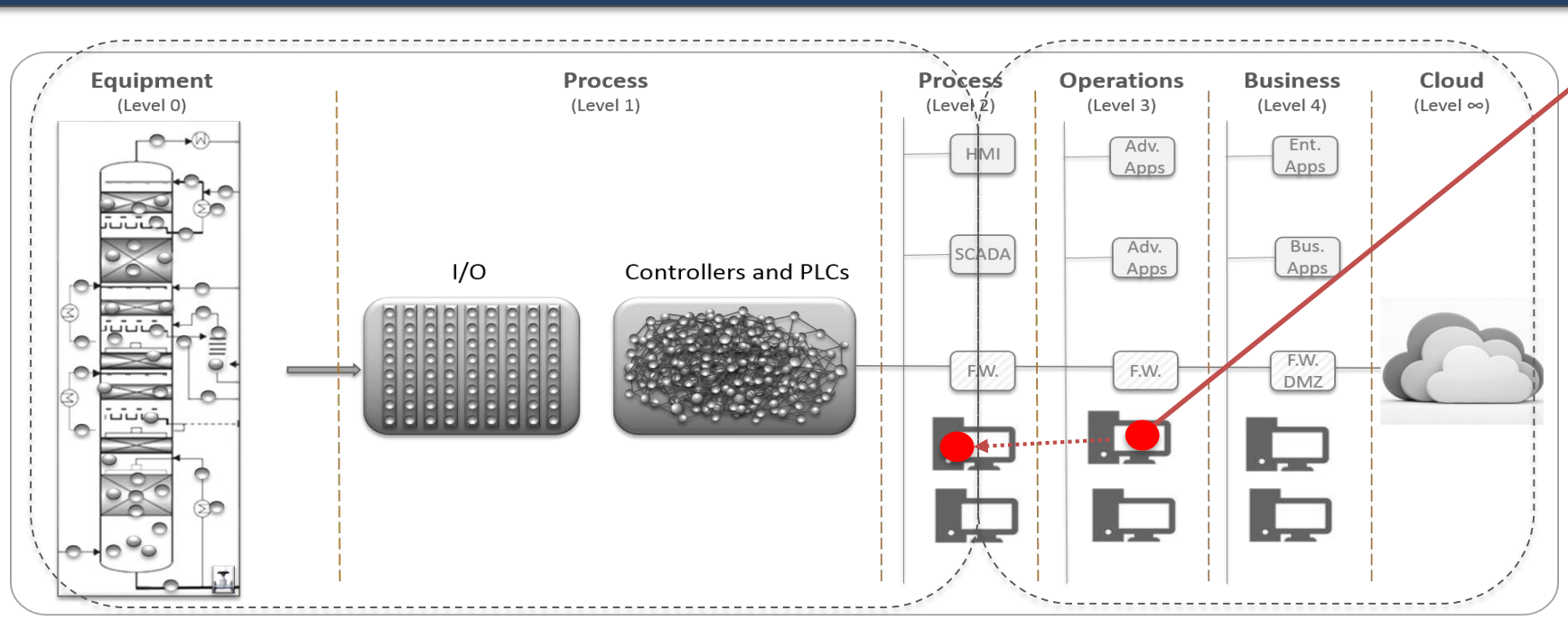


Thank You

Scenario 2 – Privileged Remote User

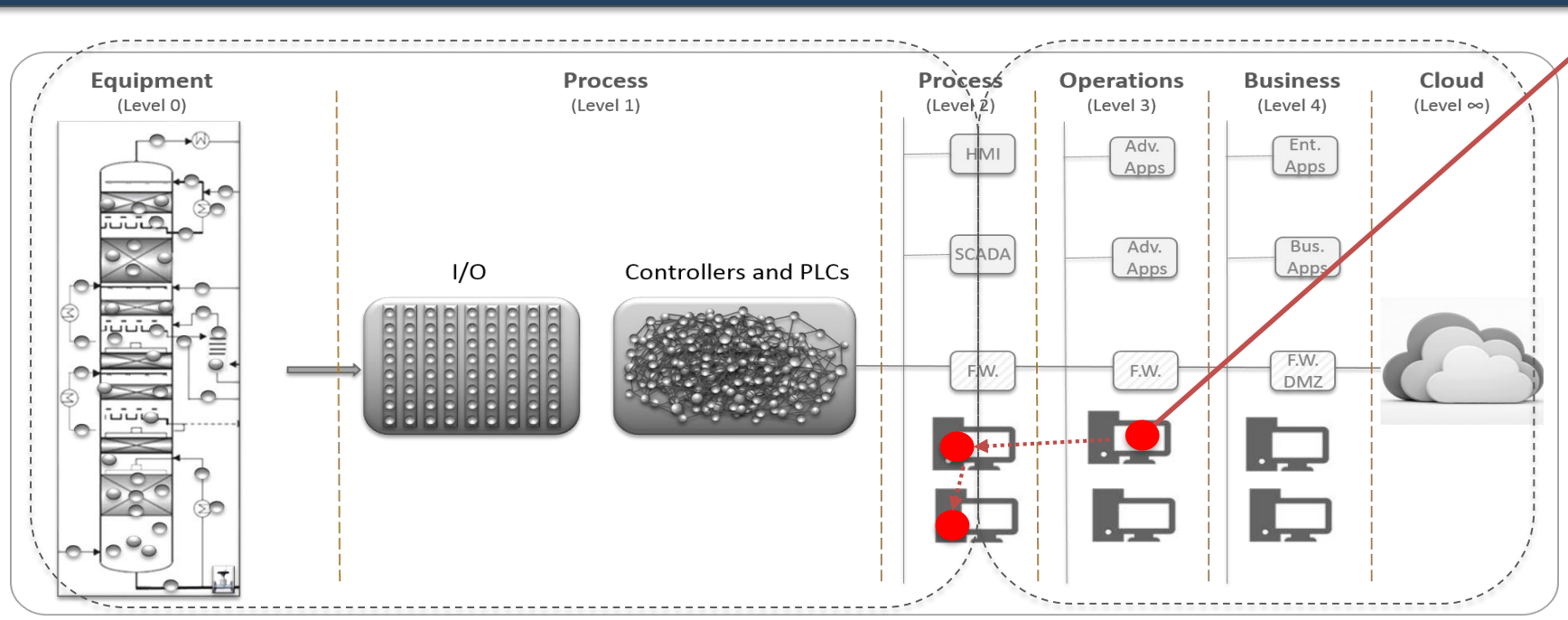
Malicious/Inadvertent Action by Privileged Remote User

Accesses an engineering station and makes malicious / inadvertent change



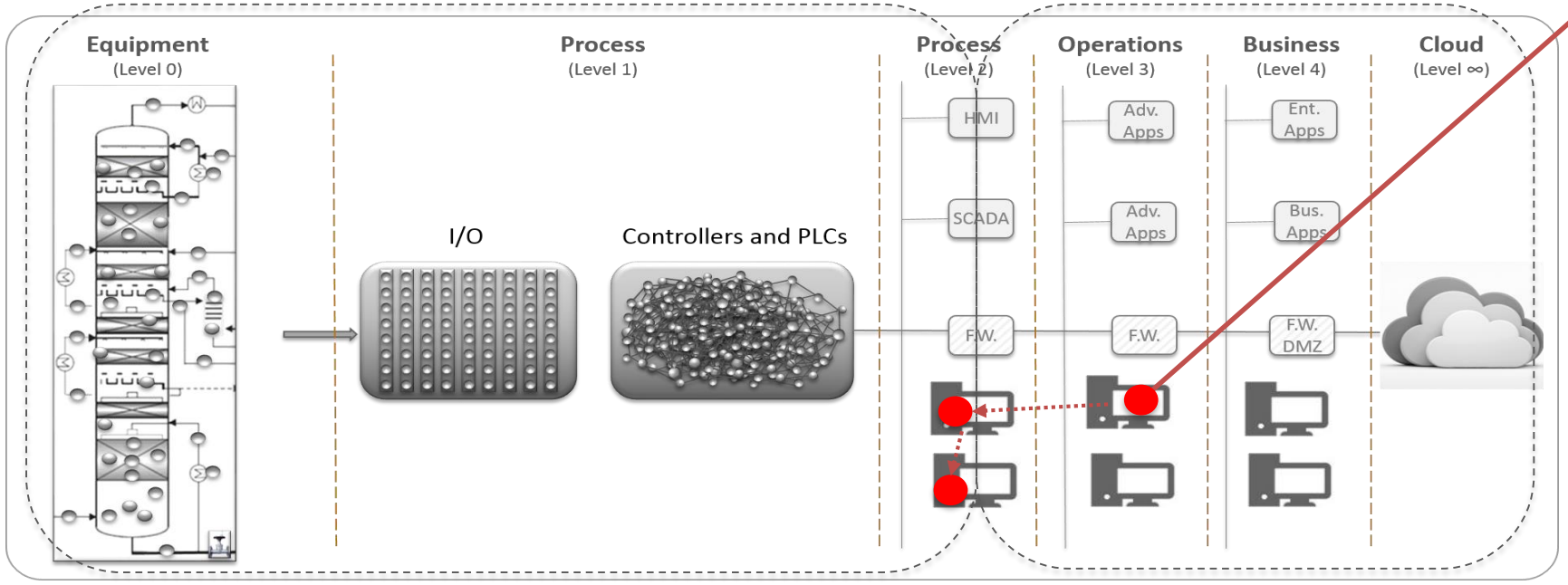
Action 1 – Remote User Deletes Backups to Impact Recovery

Deletes Backup on Remote Host (Assuming Malicious)



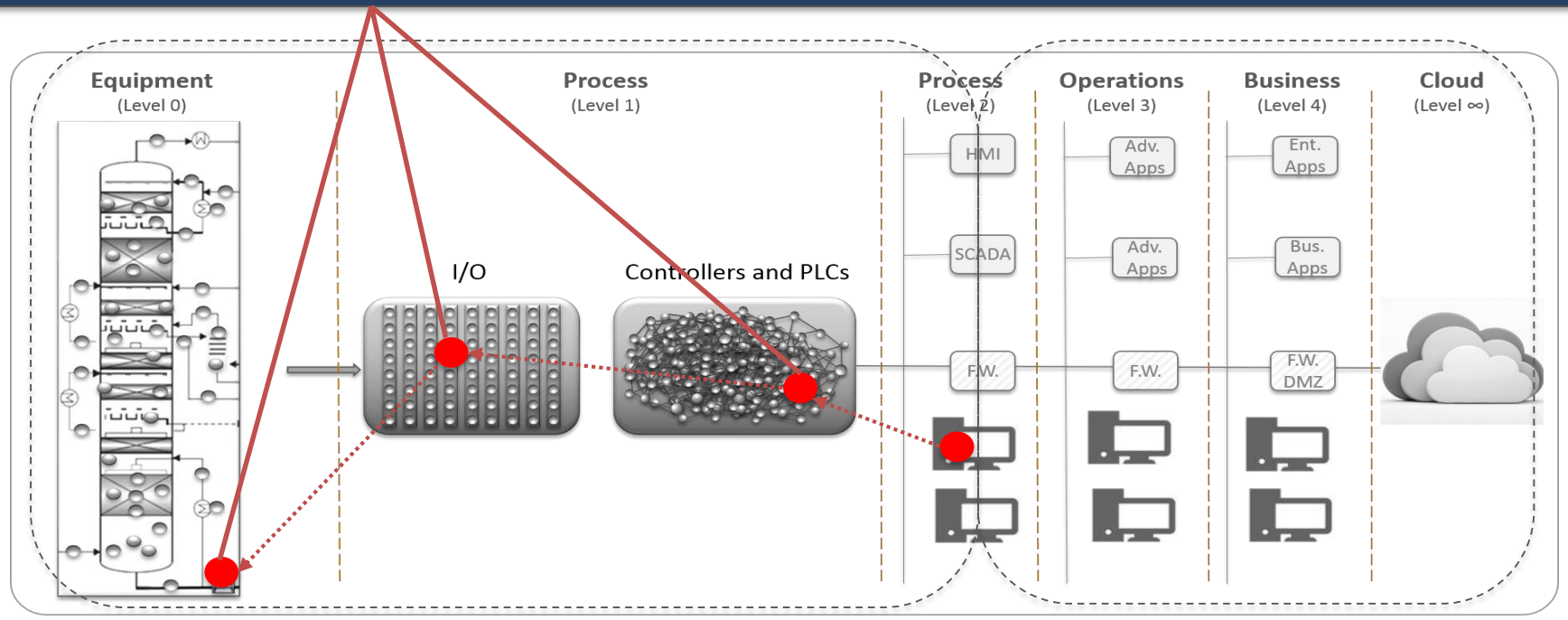
Action 2 – Remote User Makes Malicious/Inadvertent Change(s)

Changes made - possibly to SIS project
Changes made - possibly to DCS



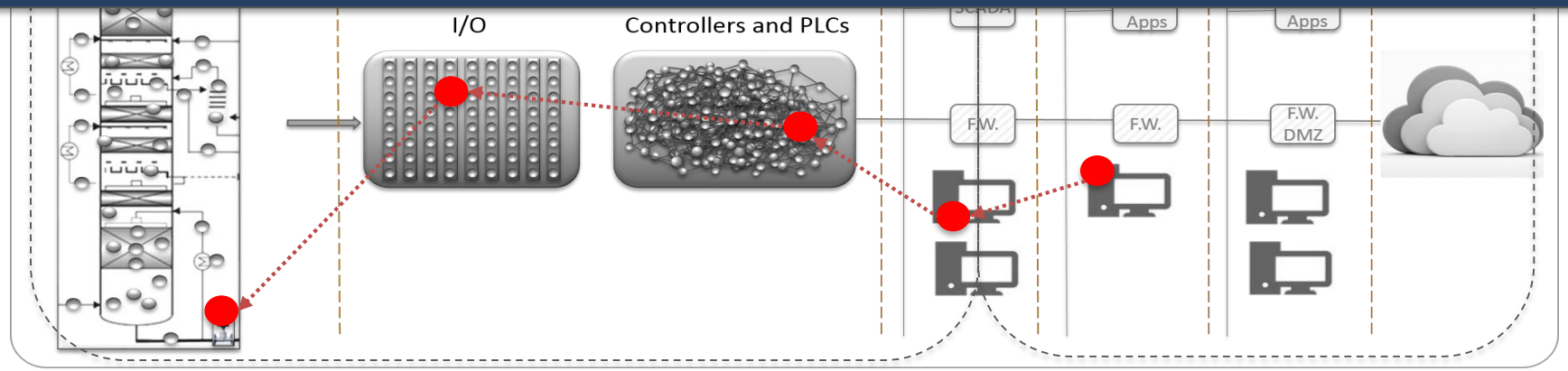
Action 3 – System Propagates Changes

Level 1 and 0 system settings are changed



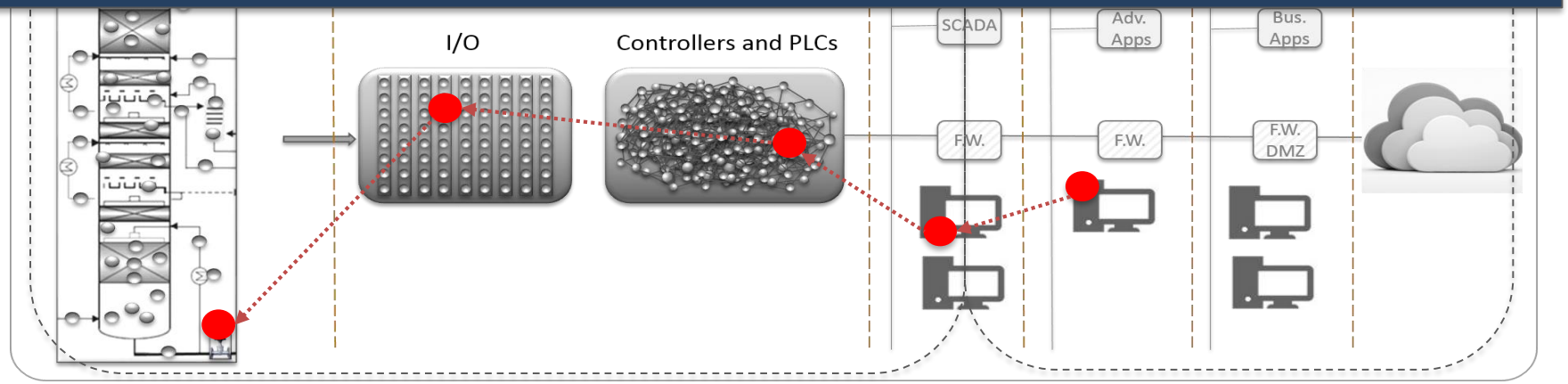
Consequences of the Change

- Plant Shuts Down (Hopefully Safely)
- Nobody Knows Why
- An Incident Investigation Occurs
    - Hours turns to days, days turns to weeks and the plant isn't making money
    - Eventually the actions that caused this events are understood (enough); system is re-engineered, tested, and re-started



Impact Summary – Confusion & Process Shuts Down

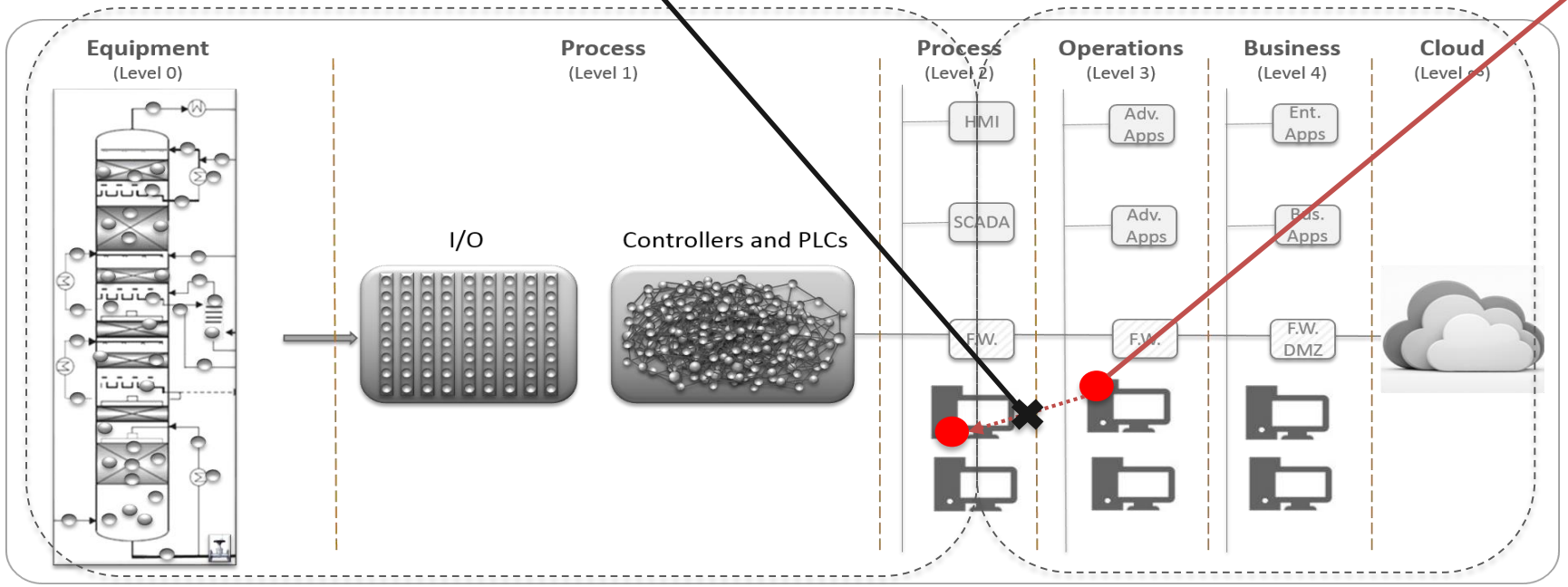
- Millions of revenue lost
- Hundreds of man-hours wasted
- Increased risk to safety
- Potential impacts to good neighbor relations



SCENARIO 2 – DEFENDING

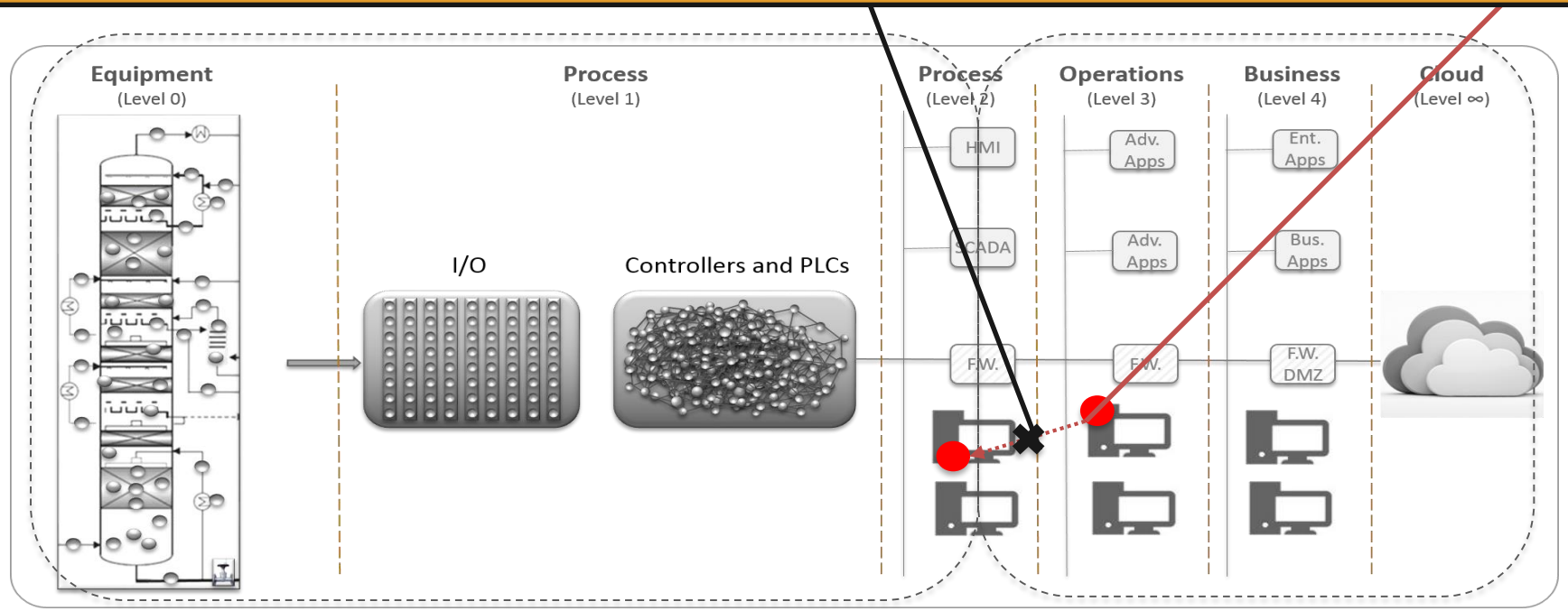
Defending

- **Monitor all communication that occurred between Remote Console and Engineering Station**



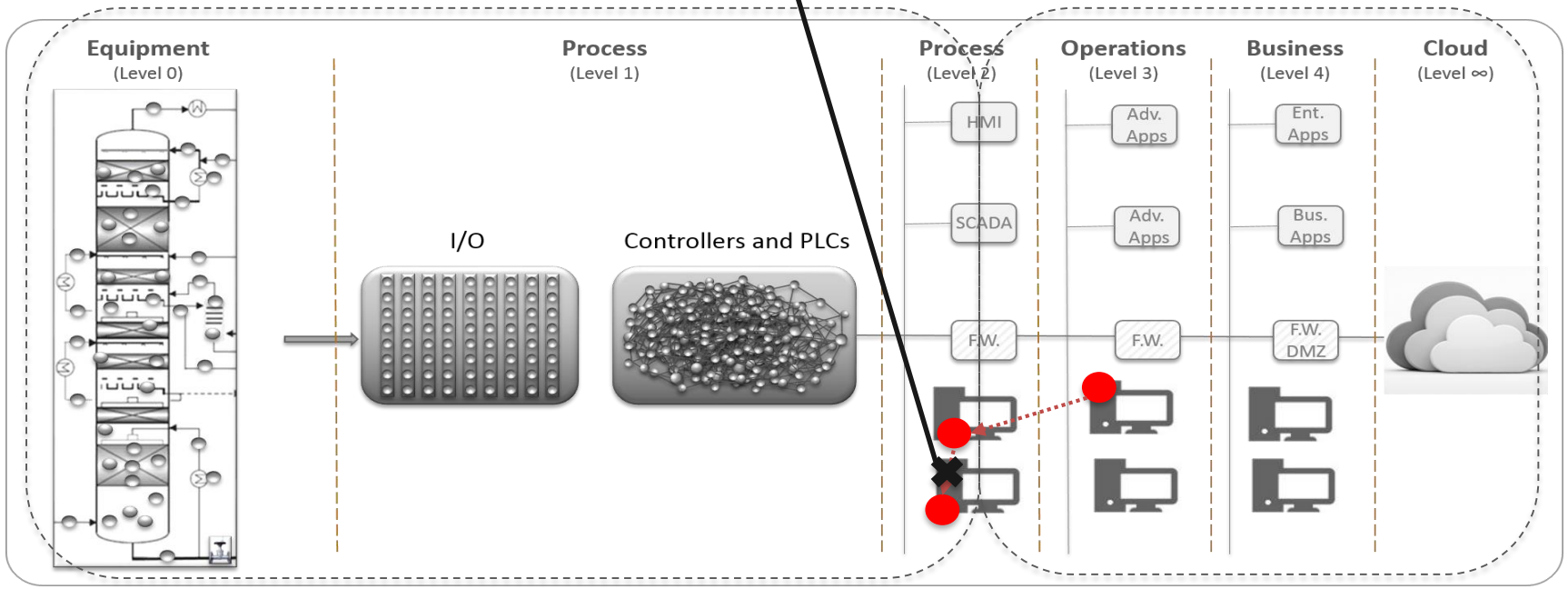
Defending

- Detect suspicious activity across your IT & OT environments
- Stop cyber-attacks in their earliest stages
- Reduce the amount of time to detect, investigate and remediate cyber threats



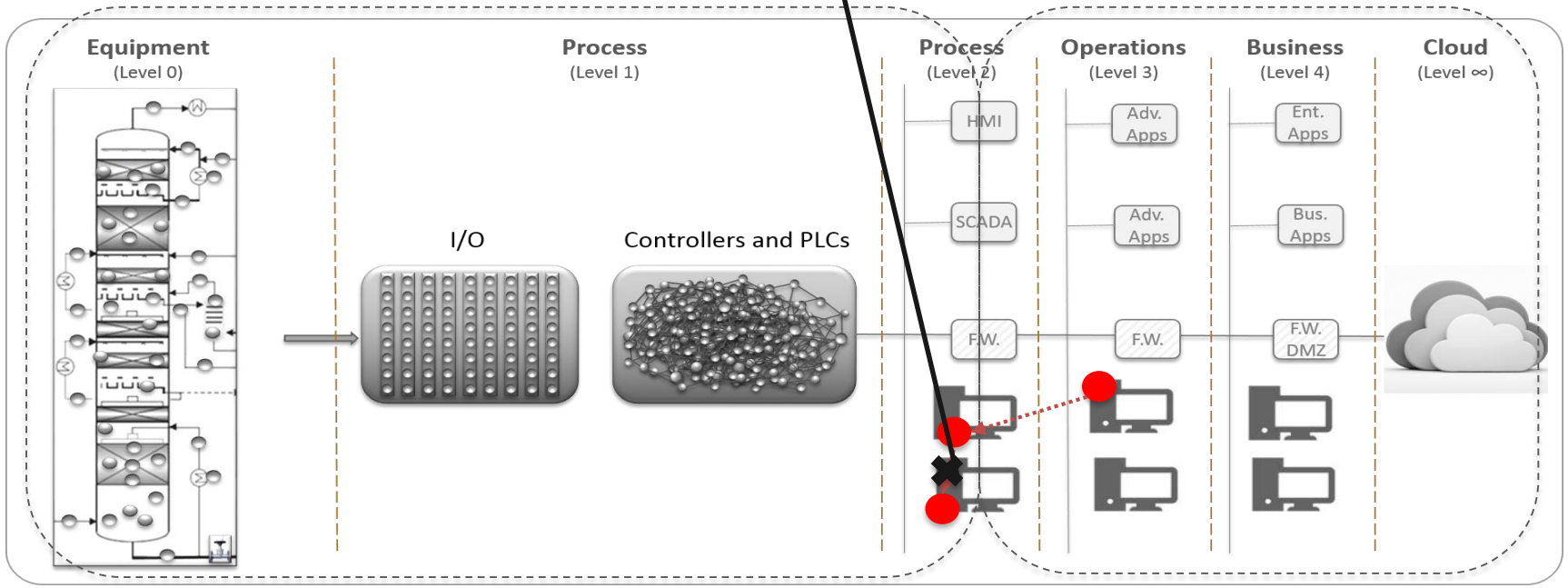
Defending

- **Monitor all communication that occurred between Engineering Station and other Windows stations on the Process Control Network (PCN)**



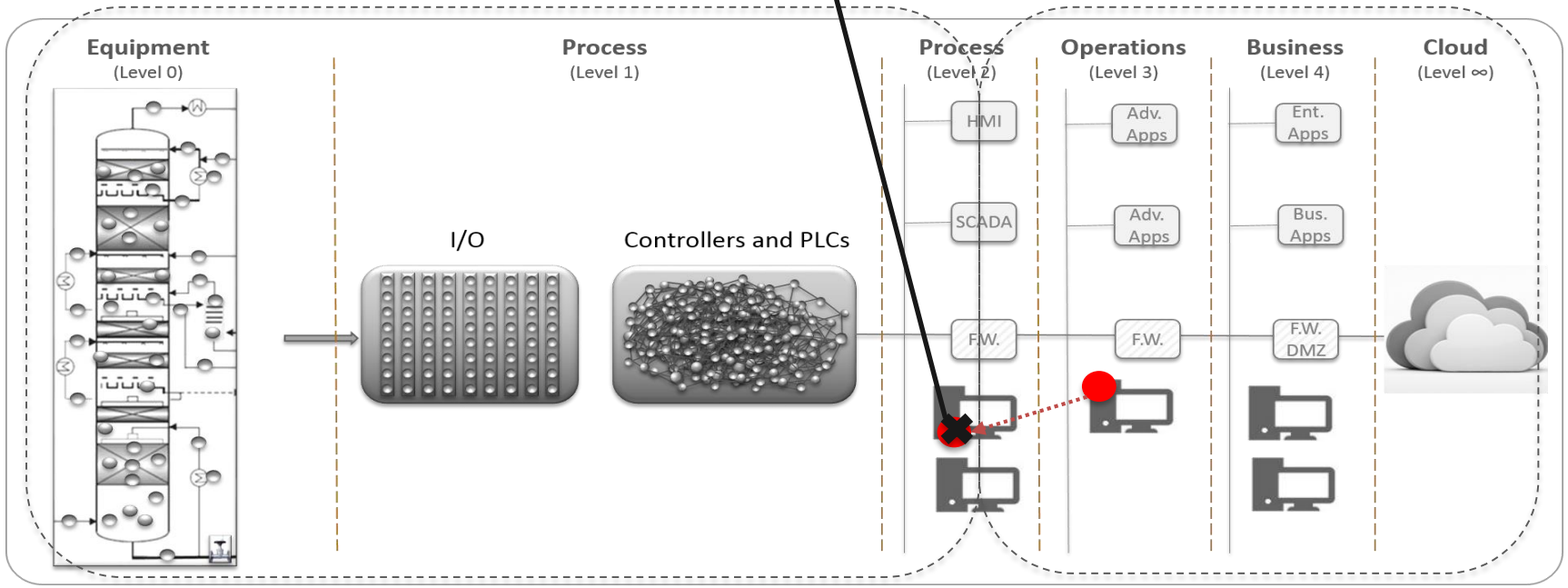
Defending

- Detect suspicious activity across your IT & OT environments
- Reduce the amount of time to detect, investigate and remediate cyber threats



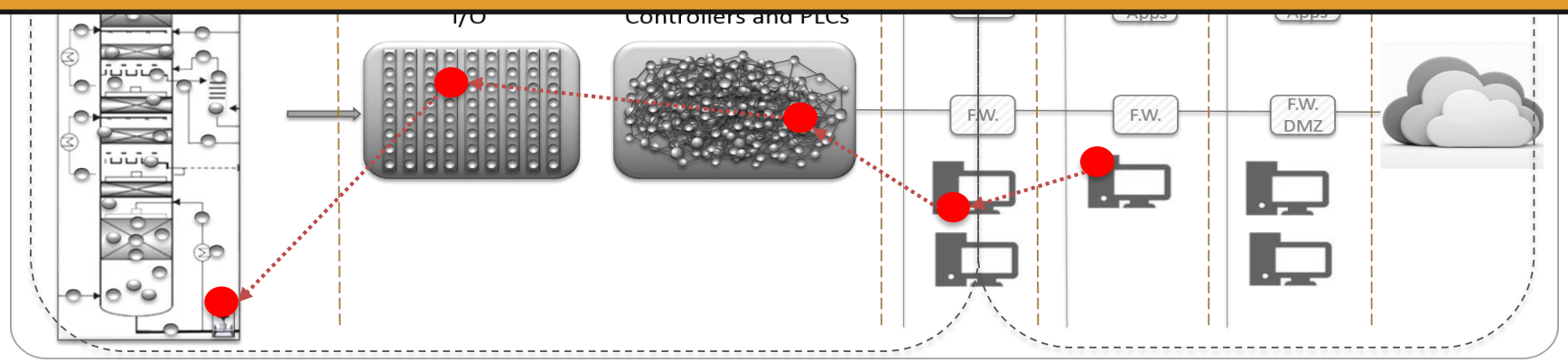
Defending

- Monitor all Operator Actions, System Events, and Process Alarms on PCN
- Monitor all offline changes made by the Engineering Configurator



Summary Actions to Take

- **You Need Tools to Help You:**
  - Detect suspicious activity across your IT & OT environments
  - Stop cyber-attacks in their earliest stages
  - Cut the cost, time and scope of cyber incident response
  - Reduce the amount of time it takes to detect, investigate and remediate cyber incident s
  - Identify the “covert channels” and command-and-control communications that indicate the presence of malware in your IT & OT environments



Thank You

Nick Cappi
Director, Technical Consulting
ncappi@pas.com
13 July 2017