CSA SINGAPORE | SG Passion Made Possible

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

22 – 23 AUGUST 2023

How to turn SECURITY BY DESIGN from myth to reality – A model-based approach

Sarah Fluchs, admeritia

FOREIGN AFFAIRS

Stop Passing the Buck on Cybersecurity

Why Companies Must Build Safety Into Tech Products

By Jen Easterly and Eric Goldstein February 1, 2023

TLP:CLEAR

National Cyber Security Centre
a part of GCHQ

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

Federal Office for Information Security

National Cyber Security Centre
Ministry of Justice and Security

certnz

National Cyber Security Centre
PART OF THE GCSB

Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default

Publication: April 13, 2023

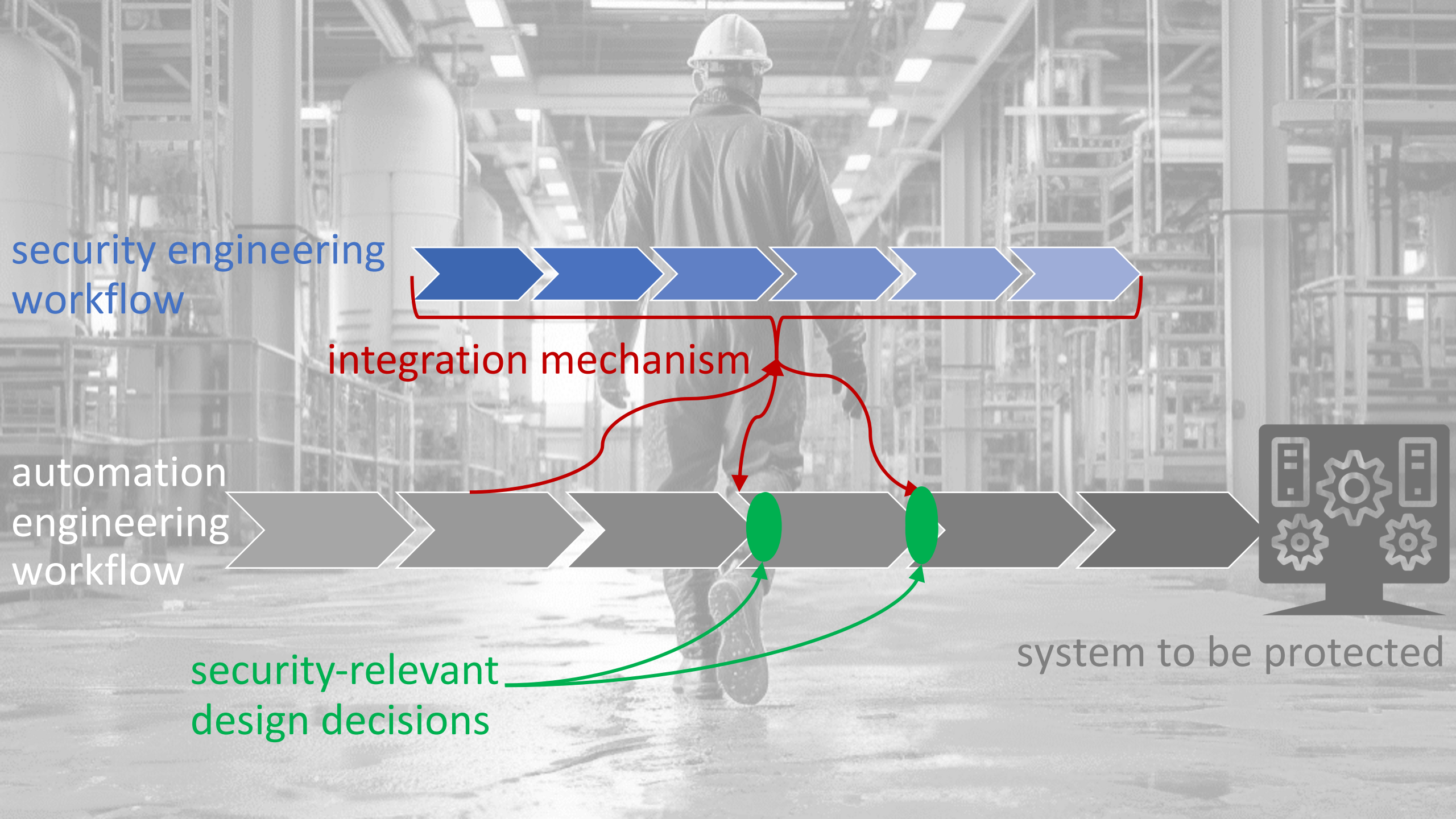
Cybersecurity and Infrastructure Security Agency

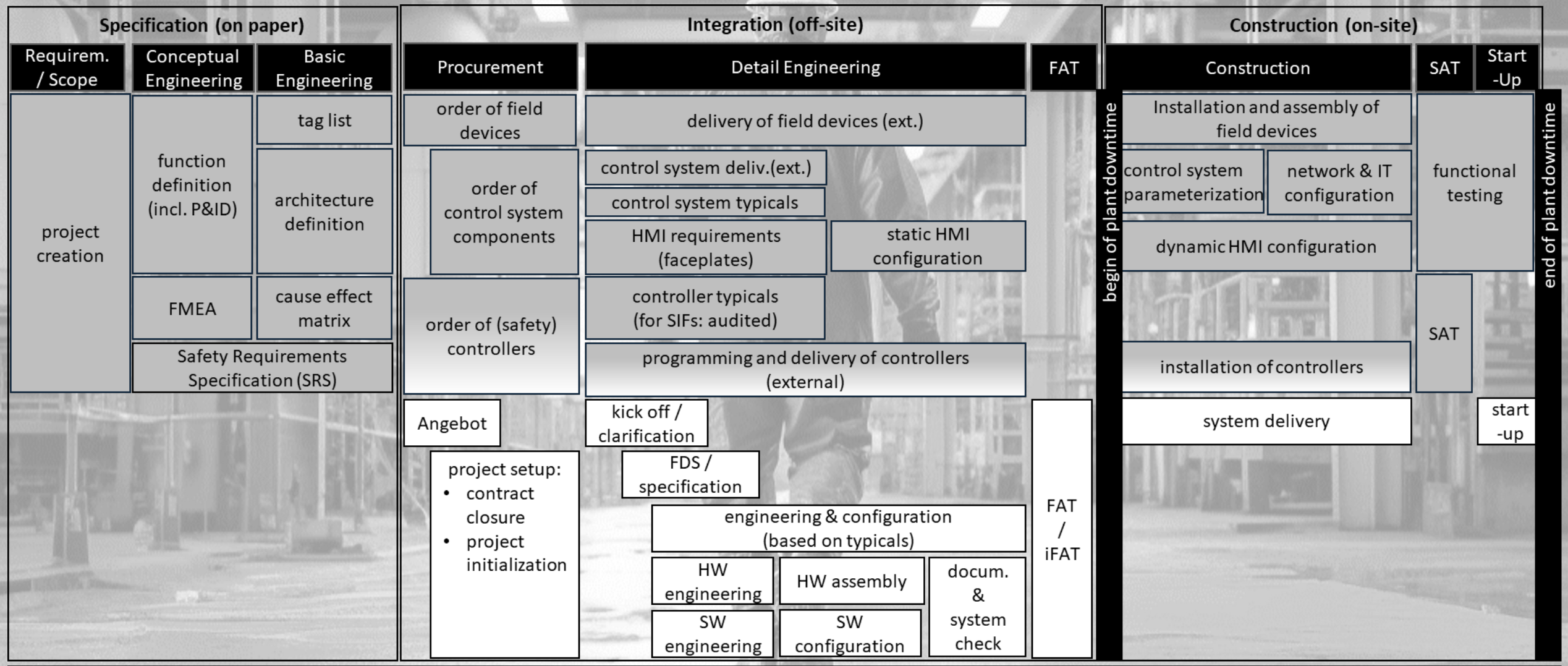
NSA | FBI | ACSC | NCSC-UK | CCCS | BSI | NCSC-NL | CERT NZ | NCSC-NZ


Security by Design
myth
reality

Myth 1

Security by Design is a vendors‘ problem.


security engineering workflow
integration mechanism
automation engineering workflow
security-relevant design decisions
system to be protected



Key

Base workflow:

- ≈ NAMUR NA35
- asset owner
- manufacturer (controllers)

Reality

Security by Design is ~~a vendors' problem.~~
a common problem of vendors
and asset owners

Function library

Select all functions that apply to your scope

Search

F037 Remote maintenance
Engineering 0 8

F072 Collection of sensor values and transfer to PLC
Basis automation 0 6

F073 Physically change process (actuation)
Administration 0 0

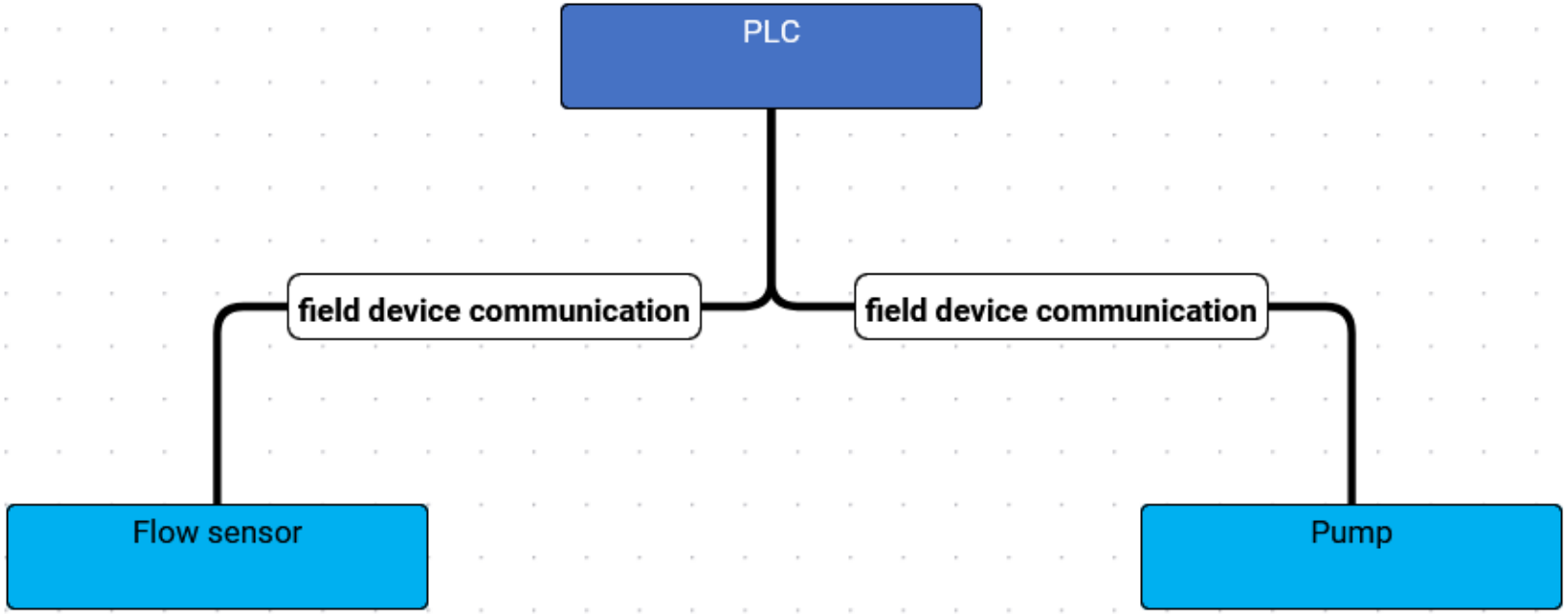
F075 Test and debug PLC logic
Engineering 0 0

F076 Force PLC outputs
Control system 0 0

F078 Change operating modes
Control system 0 0

F084 Sensor calibration
Engineering 0 0

F072 Collection of sensor values and transfer to PLC



Function library

Select all functions that apply to your scope

Search

F020 Operate and Observe
Control system 0 8

F021 Video observation of process
Control system 0 0

F022 Offline data analysis
Cloud 0 0

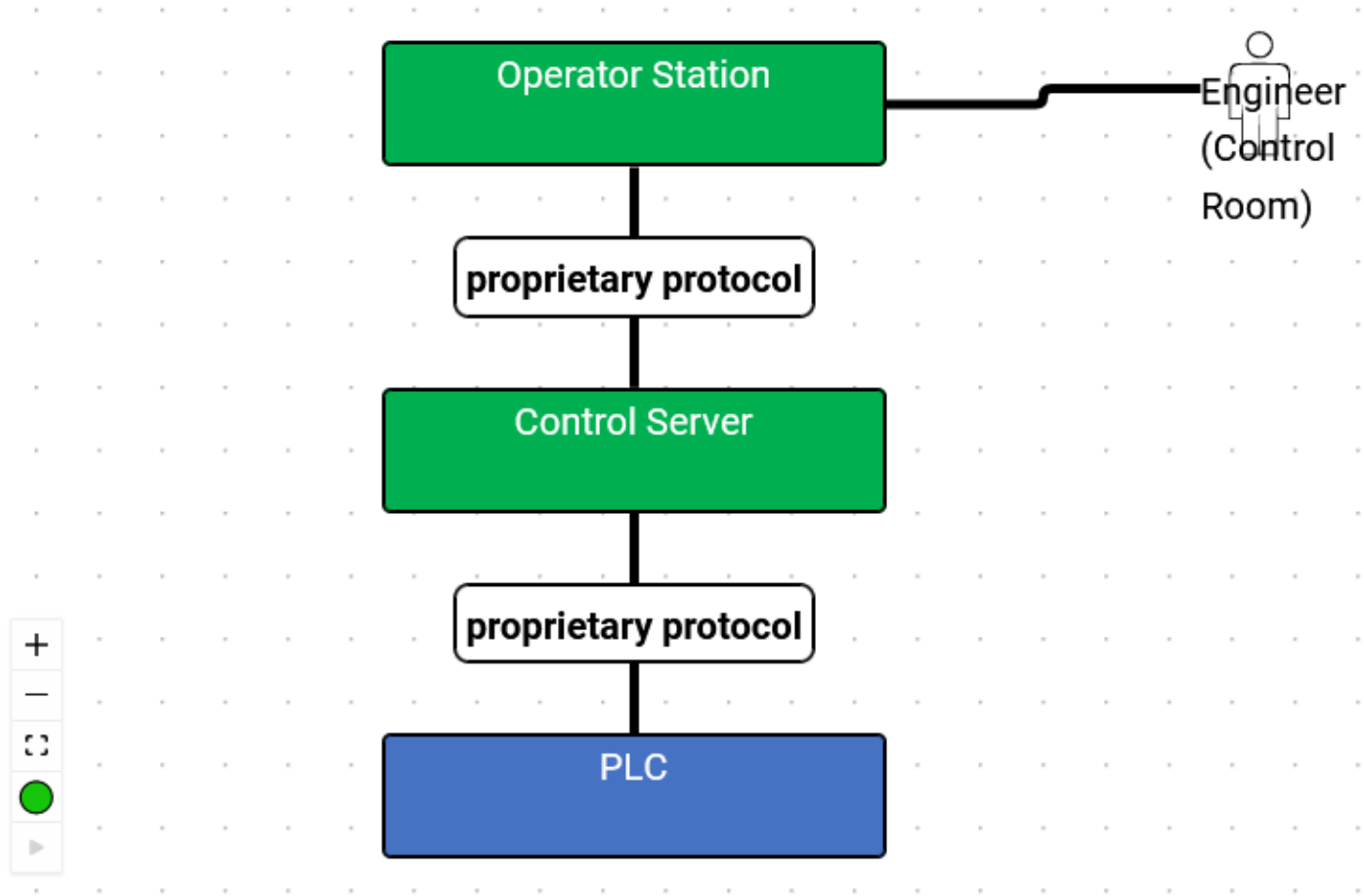
F030 Bridge PLC values from control system
Engineering 0 0

F031 Engineering of APC
Engineering 0 0

F032 Engineering of PLC logic
Engineering 0 8

F033
Integration of field device / PLC into control system
Engineering 0 0

F020 Operate and Observe



Function library

Select all functions that apply to your scope

Search

F011 Advanced Process Control
Basis automation 0 0

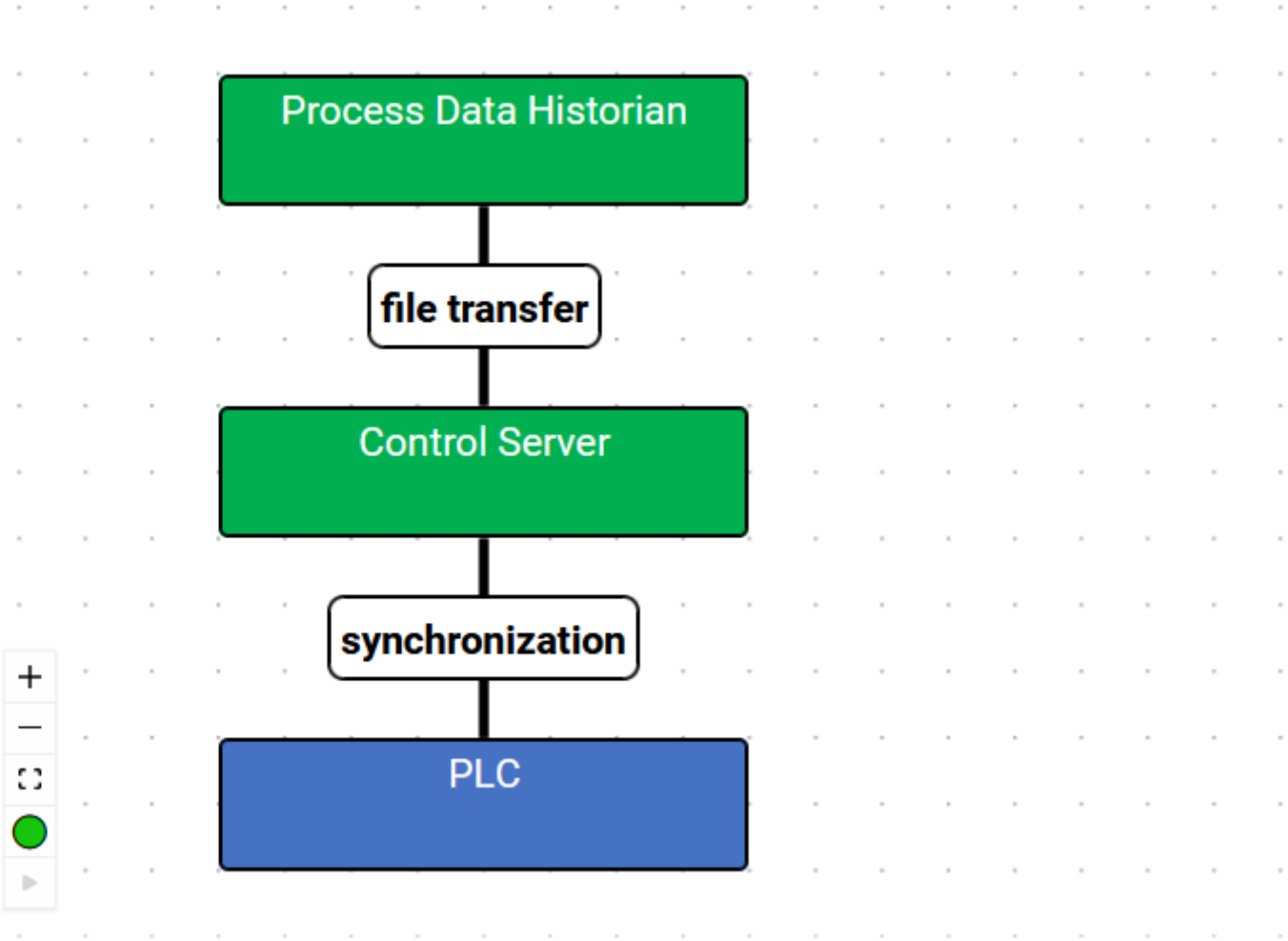
F021 Video observation of process
Control system 0 0

F073 Physically change process (actuation)
Administration 0 0

F085 Alarm for critical process values
Control system 0 0

F150 Collection of process information
Control system 0 8

F150 Collection of process information



Function library

Select all functions that apply to your scope

Search

F030 Bridge PLC values from control system

Engineering 0 0

F031 Engineering of APC

Engineering 0 0

F032 Engineering of PLC logic

Engineering 0 8

F033

Integration of field device / PLC into control system

Engineering 0 0

F034 Optimization / loop tuning of control function

Engineering 0 0

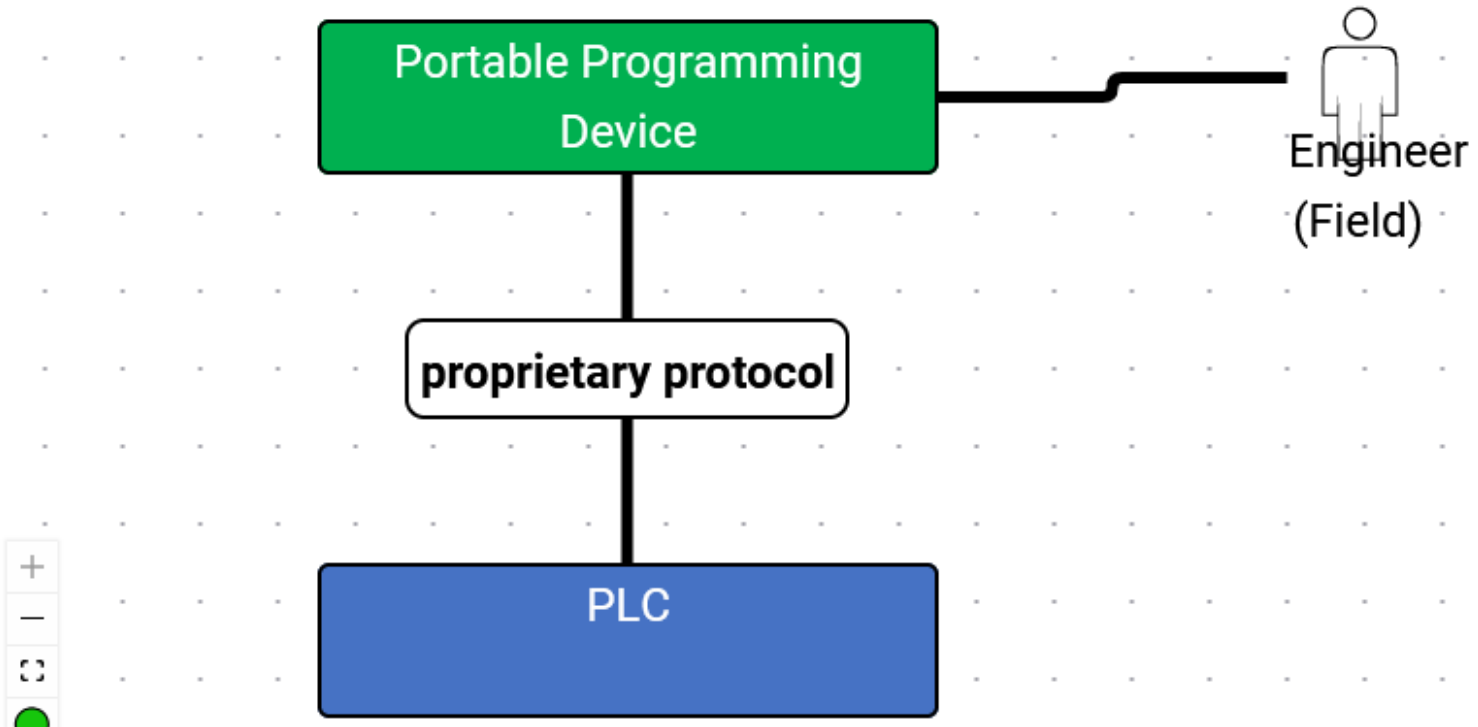
F035 Configure sensors and actuators

Engineering 0 0

F036 Engineering of safety PLC logic

Engineering 0 0

F032 Engineering of PLC logic



Function library

Select all functions that apply to your scope

Search

F006 Malware signature distribution
Security function 0 4

F007 Pasword management
Security function 0 0

F008 Software distribution
Administration 0 0

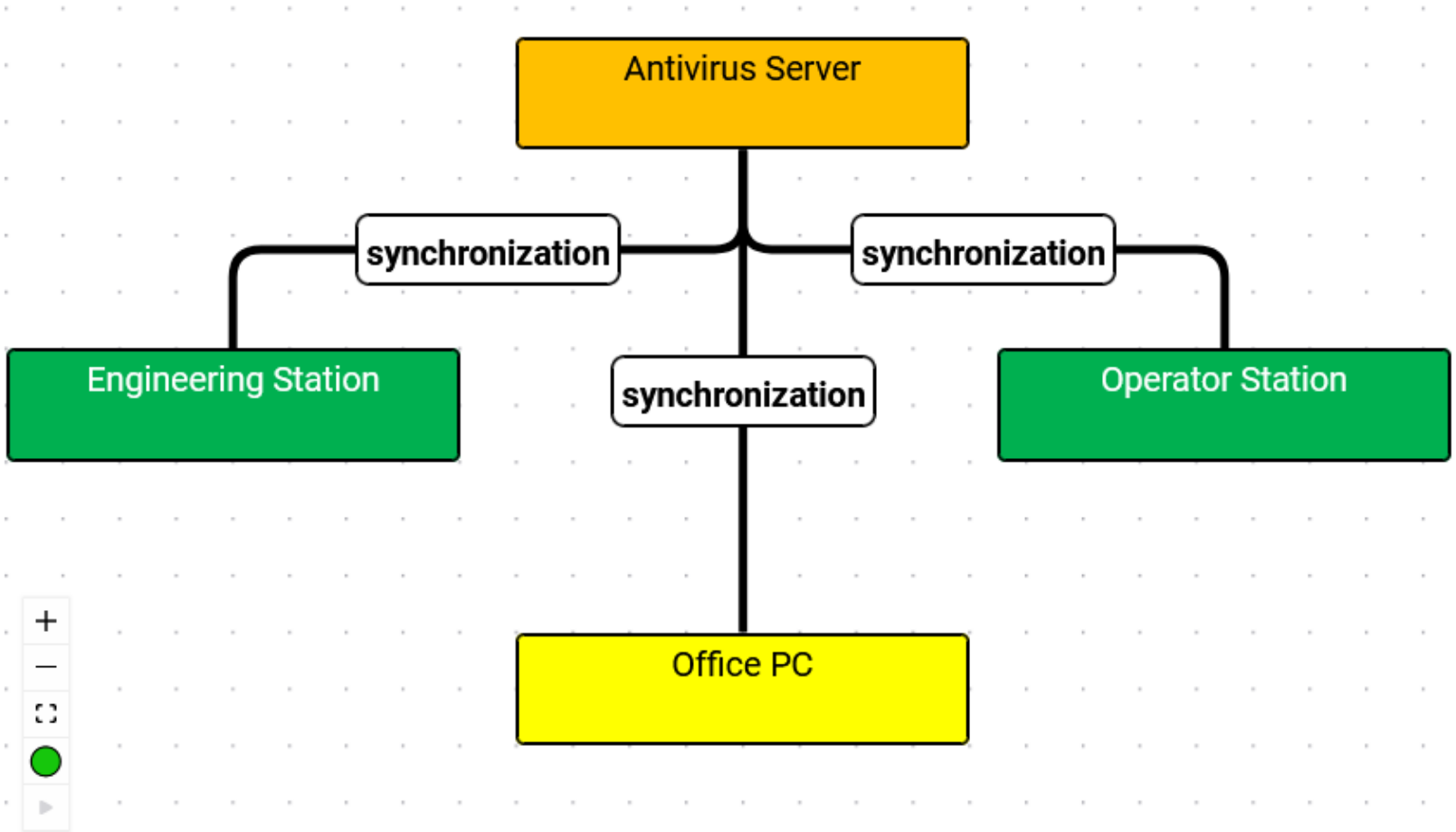
F009 Certificate management / PKI
Security function 0 0

F010 Centralized user and access management
Administration 0 0

F011 Advanced Process Control
Basis automation 0 0

F012 Safety function
Basis automation 0 6

F006 Malware signature distribution



Function library

Select all functions that apply to your scope

Search

F033
Integration of field device / PLC into control system
Engineering 0 0

F034 Optimization / loop tuning of control function
Engineering 0 0

F035 Configure sensors and actuators
Engineering 0 0

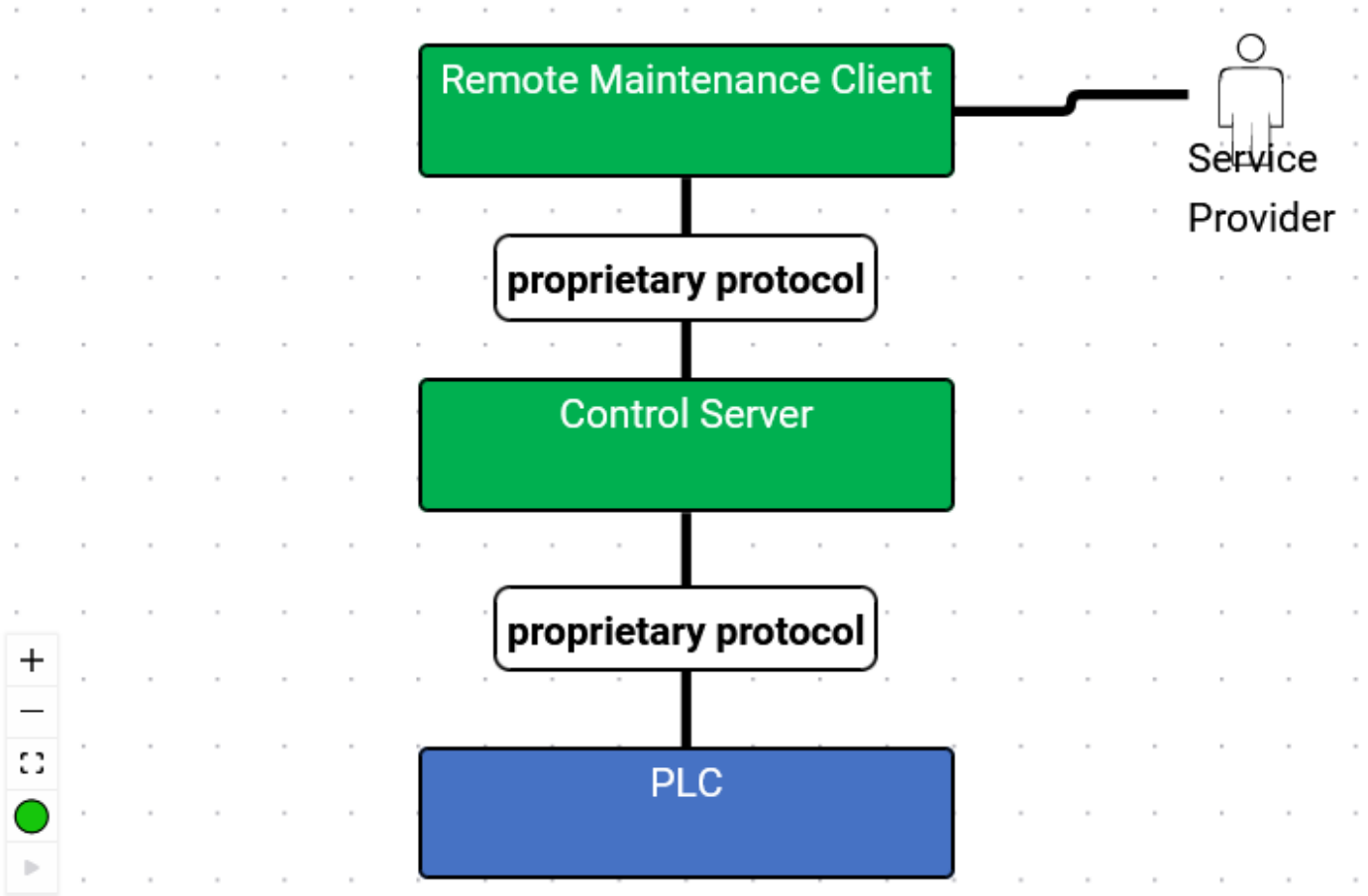
F036 Engineering of safety PLC logic
Engineering 0 0

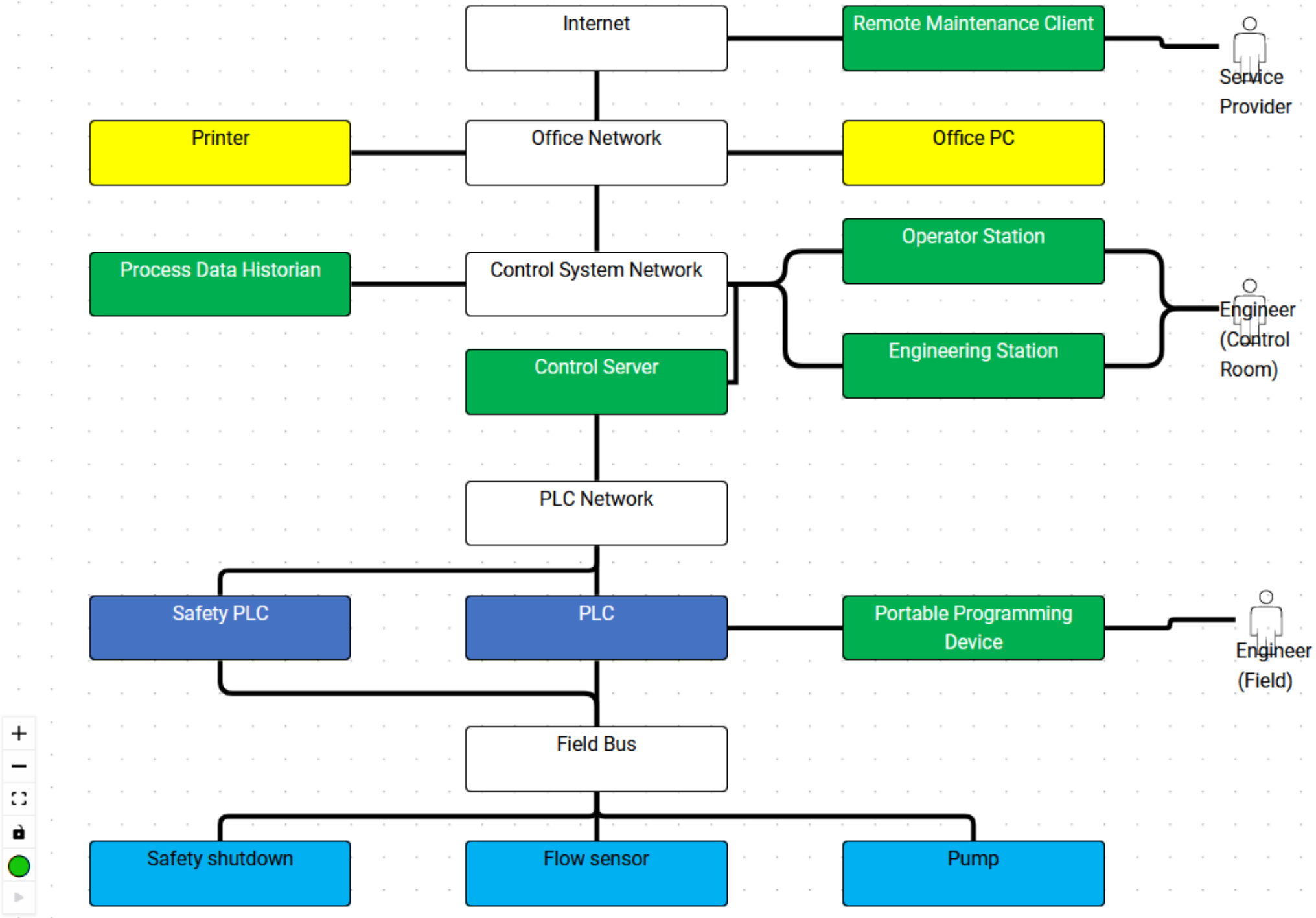
F037 Remote maintenance
Engineering 0 8

F072 Collection of sensor values and transfer to PLC
Basis automation 0 6

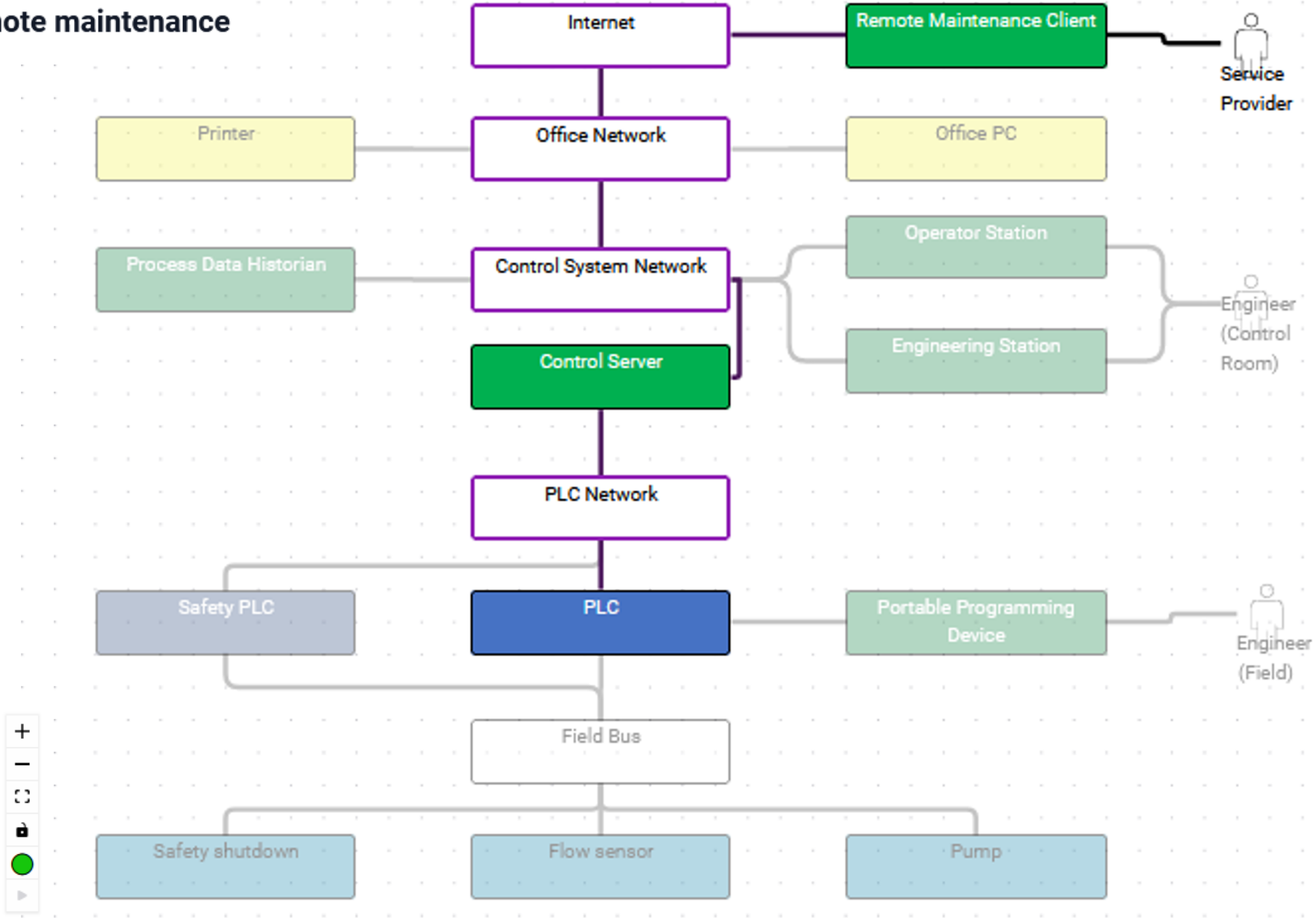
F073 Physically change process (actuation)
Administration 0 0

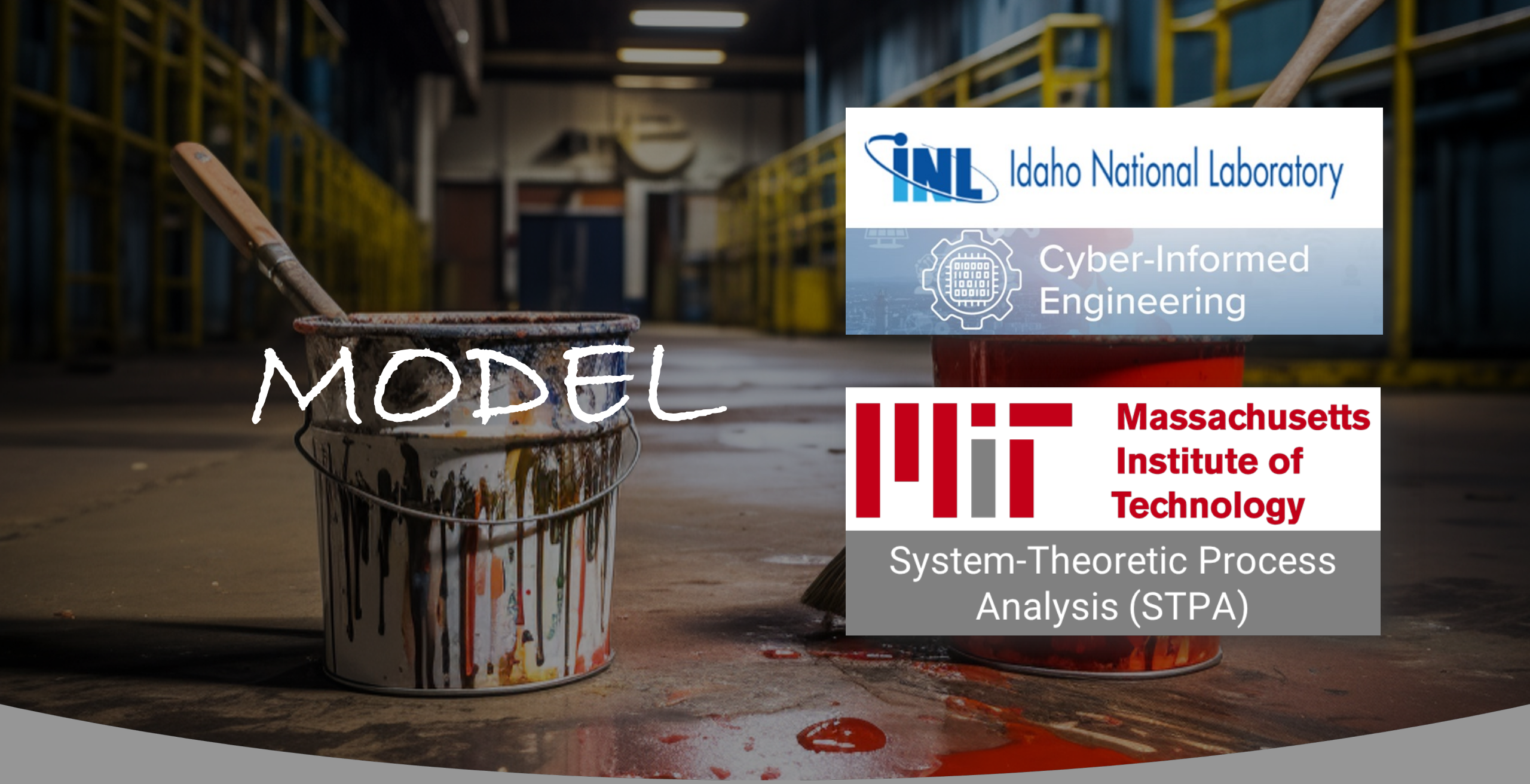
F037 Remote maintenance




Internet
Remote Maintenance Client
Service Provider
Printer
Office Network
Office PC
Process Data Historian
Control System Network
Operator Station
Engineering Station
Engineer (Control Room)
Control Server
PLC Network
Safety PLC
PLC
Portable Programming Device
Engineer (Field)
Field Bus
Safety shutdown
Flow sensor
Pump

F037 Remote maintenance





Idaho National Laboratory

Cyber-Informed Engineering

Massachusetts Institute of Technology

System-Theoretic Process Analysis (STPA)

Model-based security by design

Myth 2

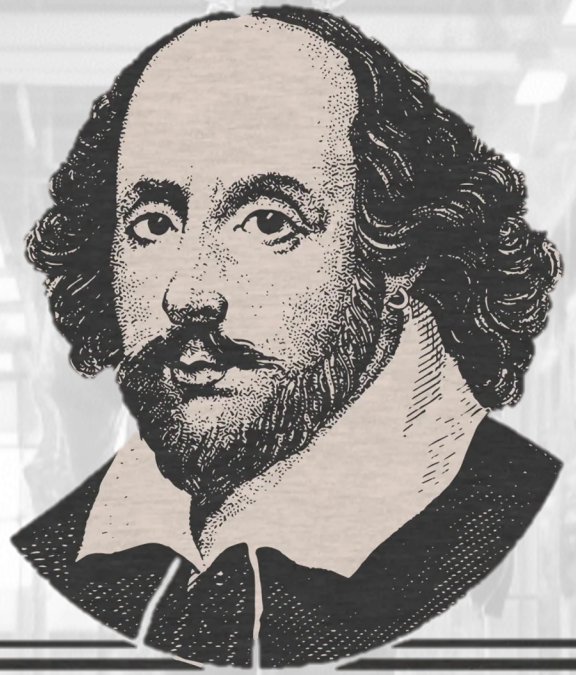
Security by design is done by following secure-by-design-principles.

NCSC	Cavoukian	OWASP	solarwinds
Establish context, then design system	Proactive not Reactive	Minimise attack surface area	use the right tools
Make compromise difficult	Secure by Default	Establish secure defaults	use appropiate techniques
Make disruption difficult	Embedded into Design	Least privilege	follow procedures
Make compromise detection easier	Positive-Sum, not Zero-Sum	Defence in depth	target the SDLC
Reduce the impact of Compromise	End-to-End Security	Fail securely	guarantee Access
	Visibility and Transparency	Don't trust services	Build Systems
	Respect for the User	Separation of duties	Data Center
		Avoid security by obscurity	Clouds
		Keep security simple	Endpoints
		Fix security issues correctly	Identities
			Applications

Marco Joost, Security by Design in Information System Research: A Systematic Literature Research (Bachelor's thesis, 2023)

Reality

Security by design is done by
~~following secure-by-design principles~~.
making (explicit) security decisions during design



To quote HAMLET

Act III, Scene III, Line 92

"NO"

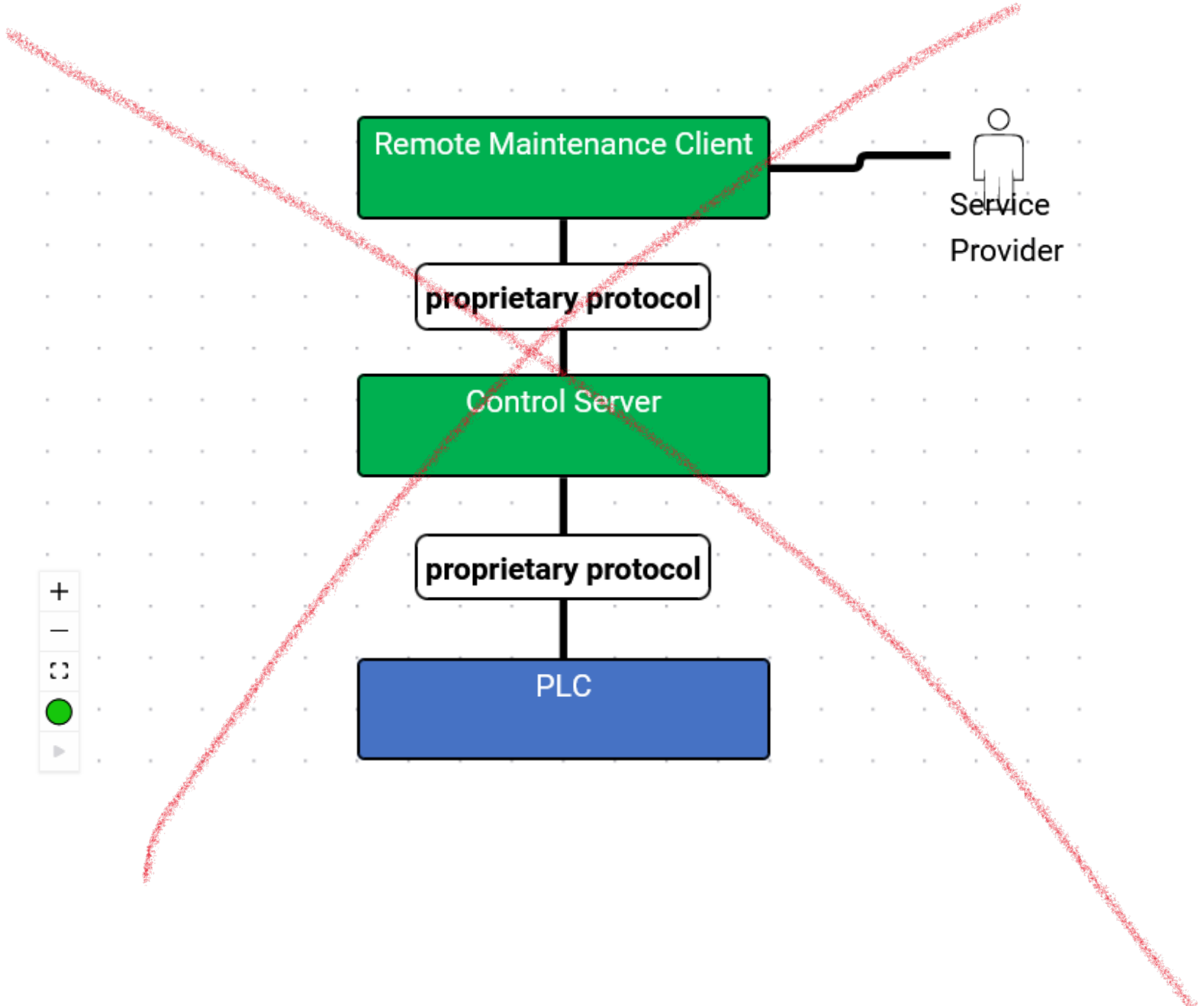
https://www.gf5tees.com/products/william-shakespeare-hamlet-no-quote-mens-cotton-poly-tee


37%

Security by design decisions workflow

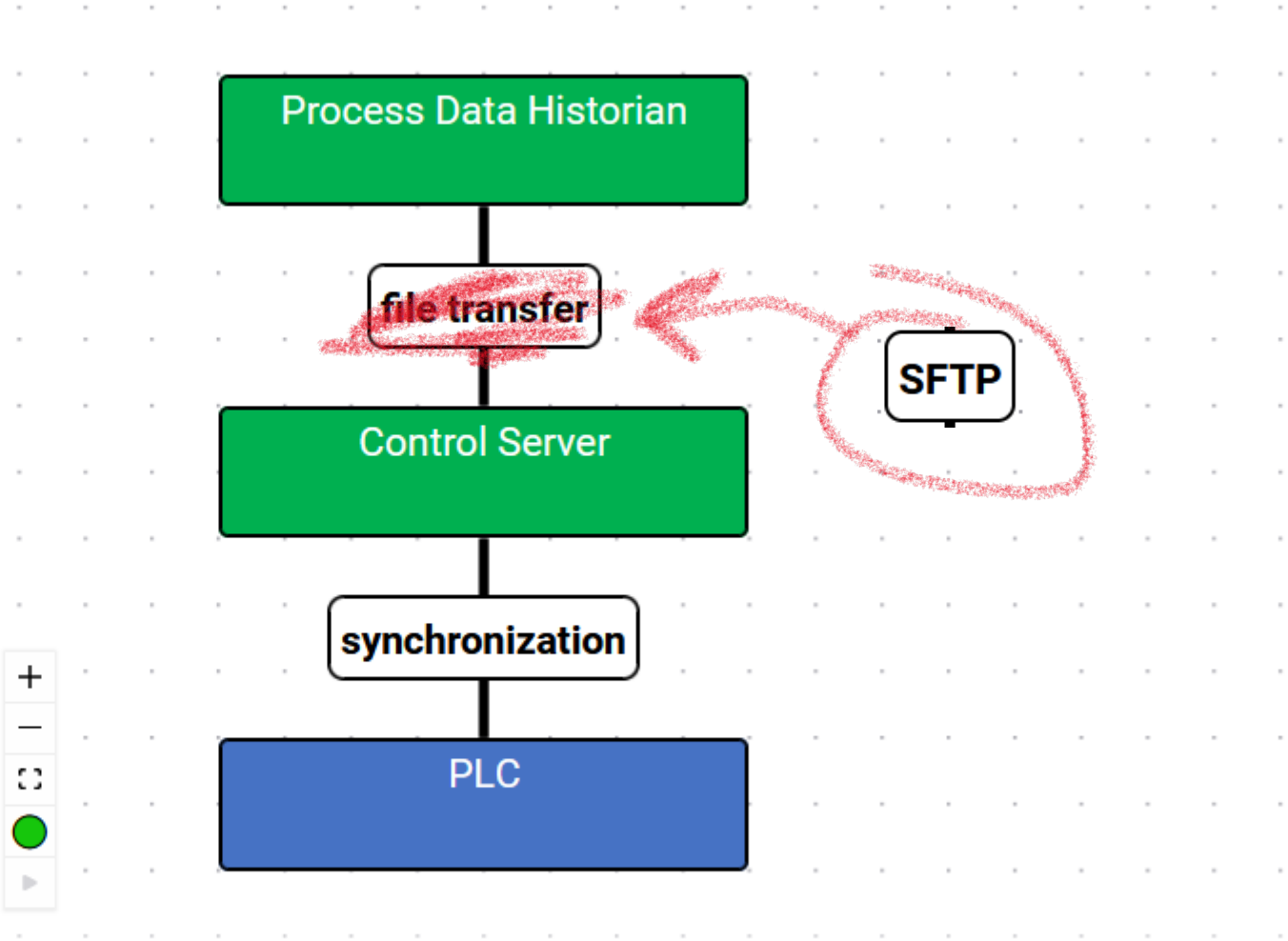
ELIMINATE FUNCTION

F037 Remote maintenance



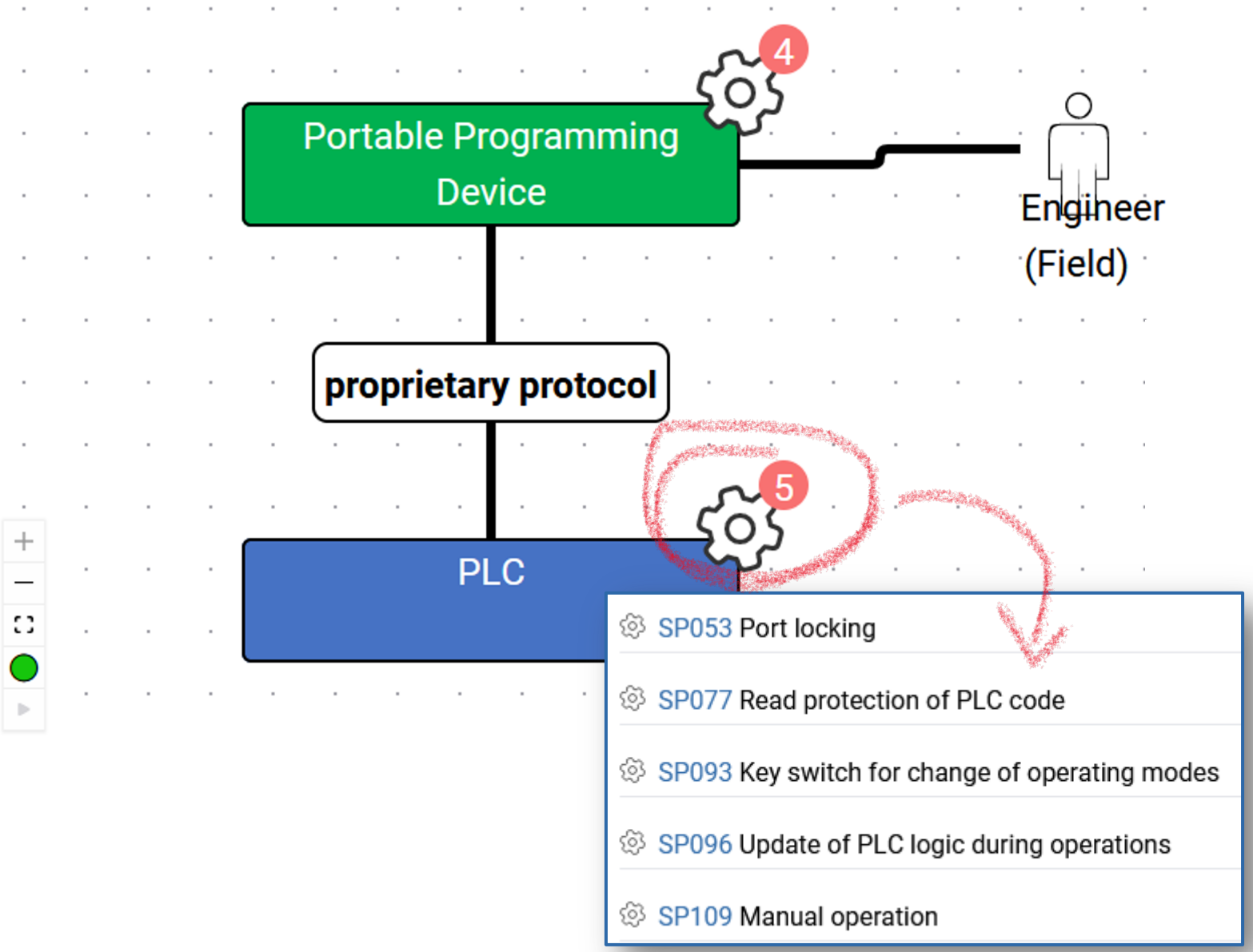
CHOOSE PROTOCOL

F150 Collection of process information



F032 Engineering of PLC logic

CONFIGURE FUNCTION COMPONENTS



F032 Engineering of PLC logic

LANDMARK DECISIONS

How can **changes** to the function be made?

- SP053 Port locking
- SP096 Update of PLC logic during operations

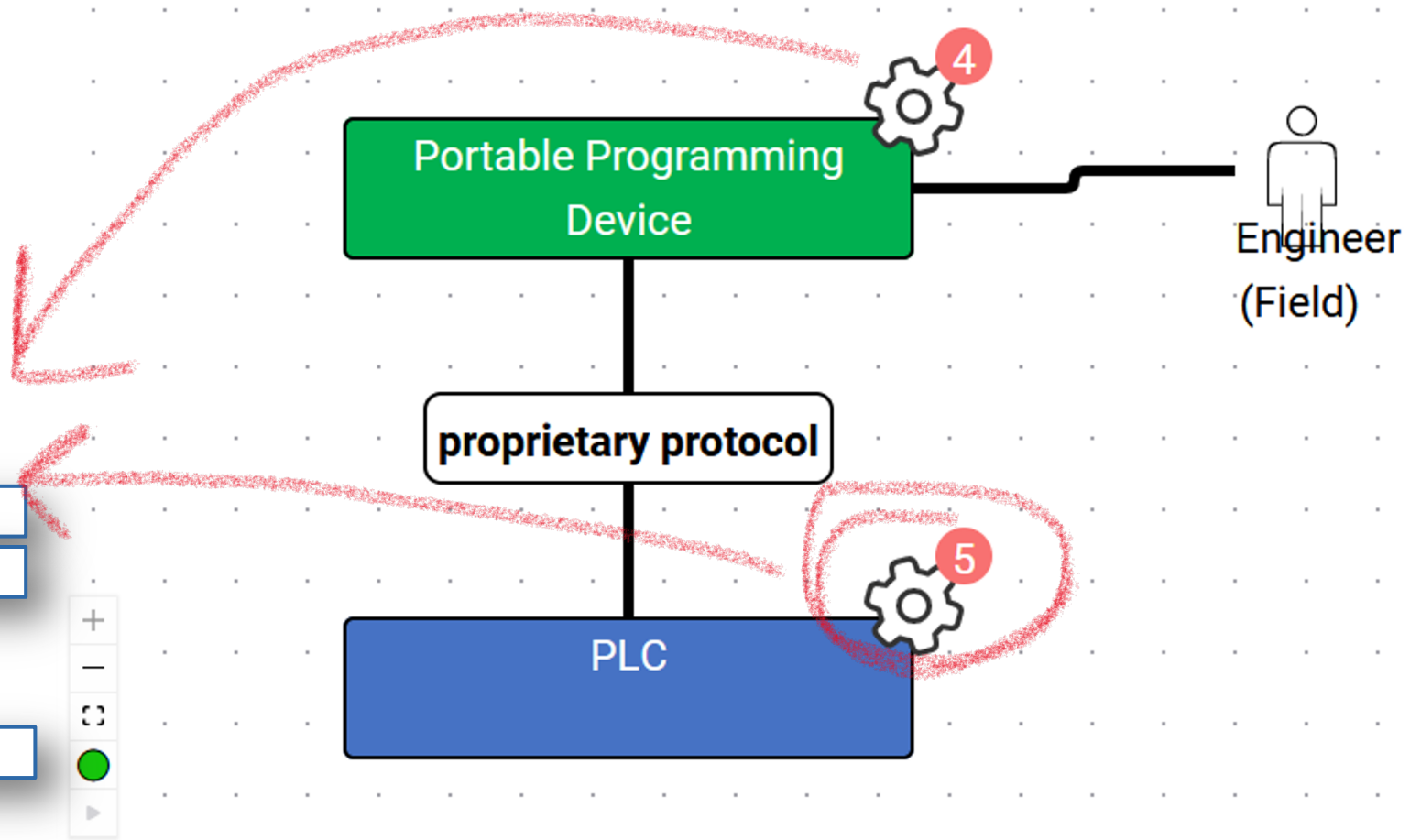
How is **resiliency** of the function ensured in case of an attack?

- SP109 Manual operation

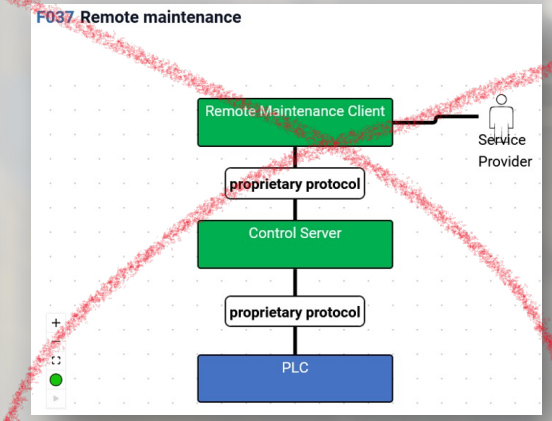
How should **humans** interact with the function?

- SP093 Key switch for change of operating modes

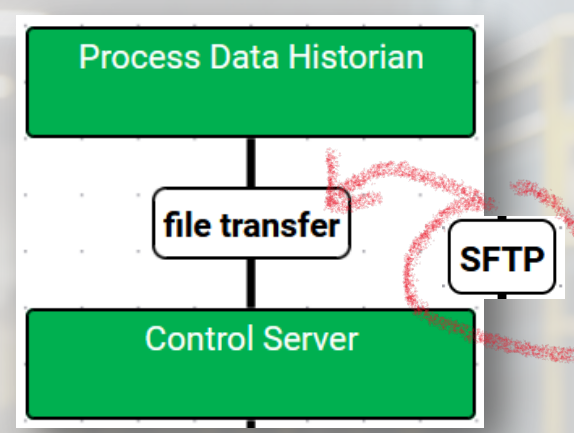
...



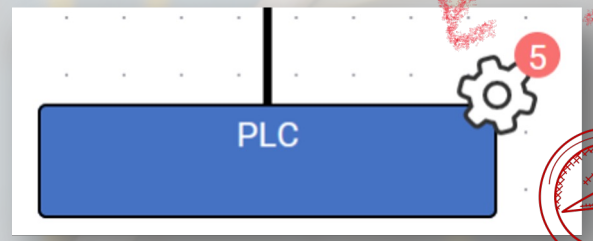
Function decisions



ELIMINATE FUNCTIONS

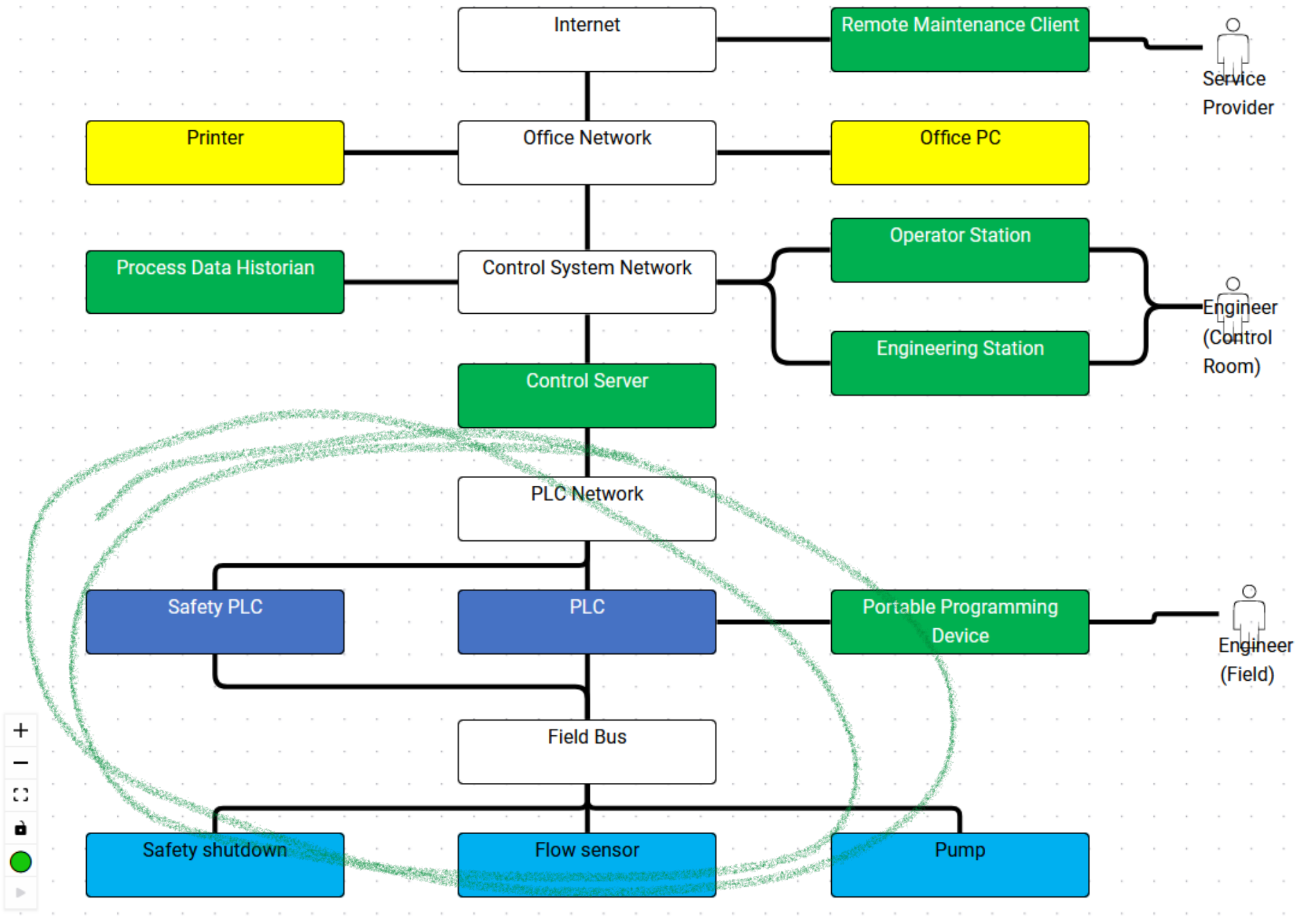


CHOOSE PROTOCOLS

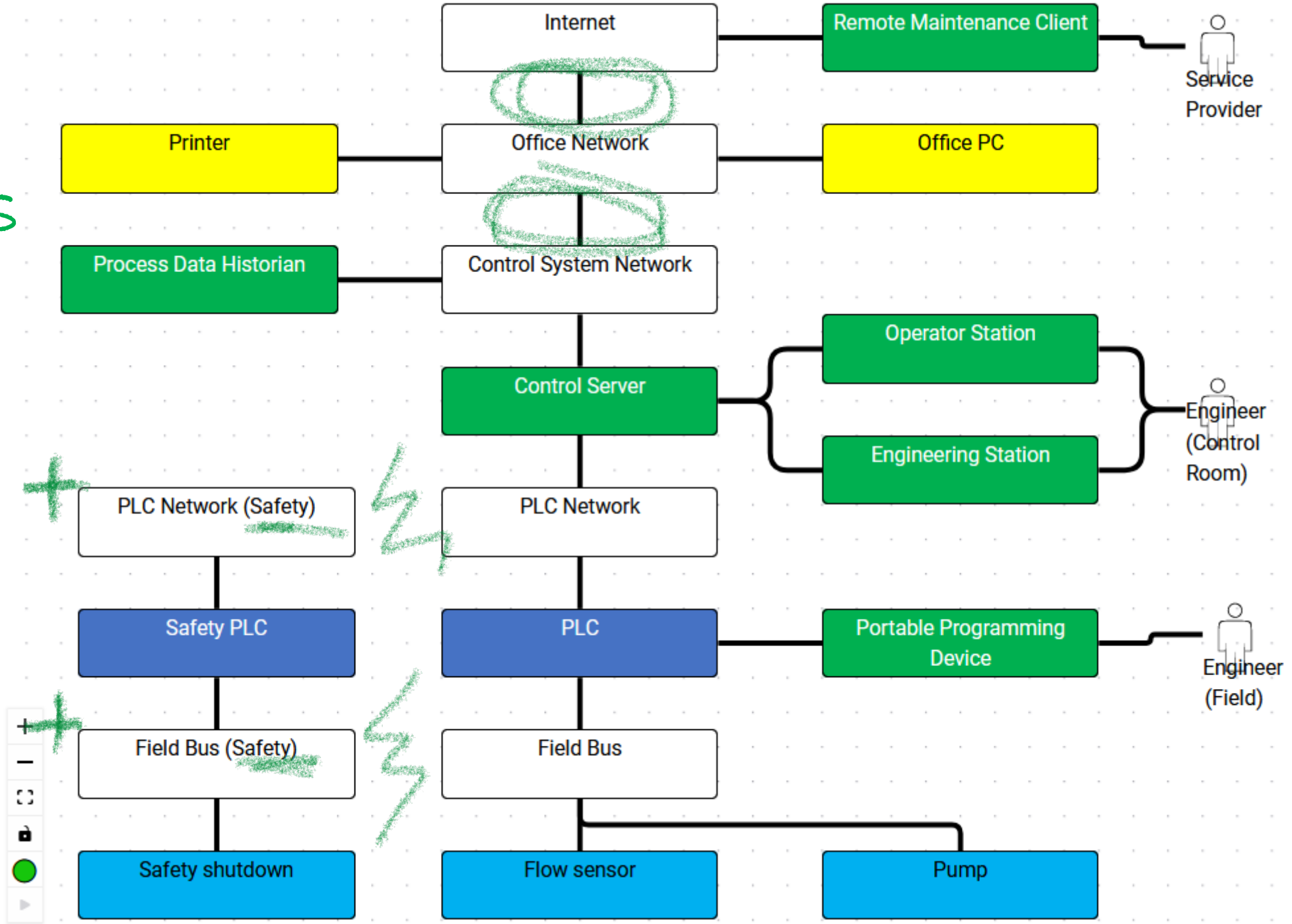


CONFIGURE FUNCTION COMPONENTS

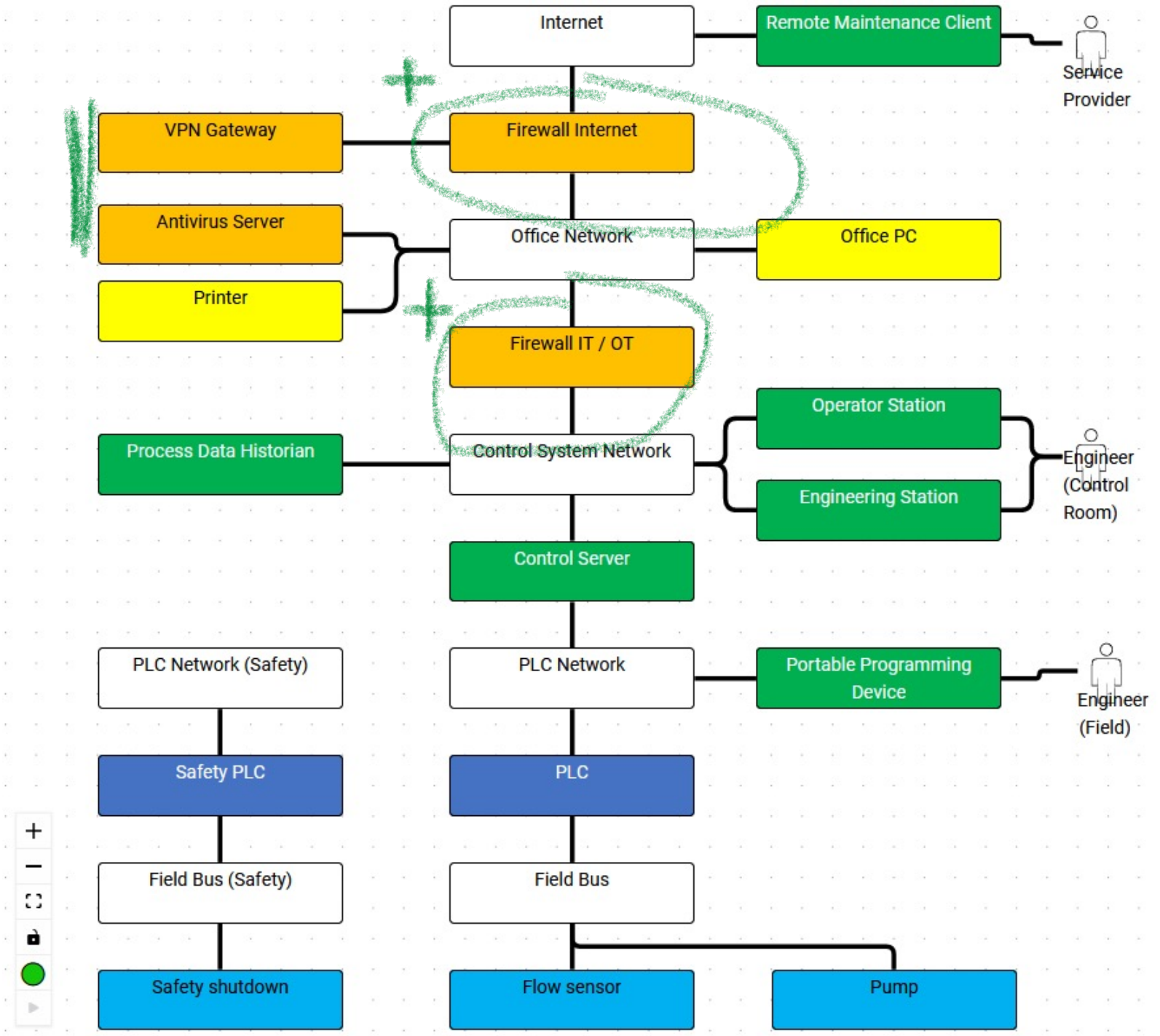
Security by design decision types


Internet
Remote Maintenance Client
Service Provider
Printer
Office Network
Office PC
Operator Station
Process Data Historian
Control System Network
Engineer (Control Room)
Engineering Station
Control Server
PLC Network
Safety PLC
PLC
Portable Programming Device
Engineer (Field)
Field Bus
Safety shutdown
Flow sensor
Pump

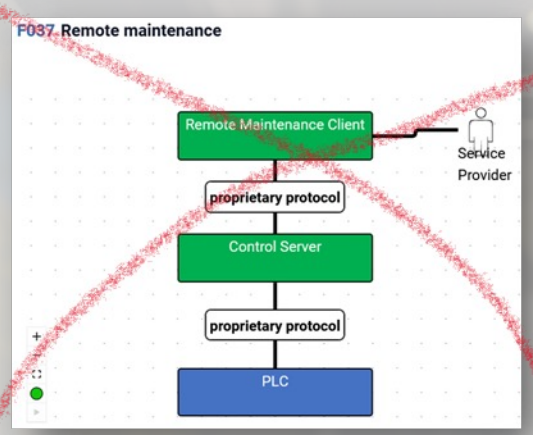
ADD NETWORK SEGMENTS



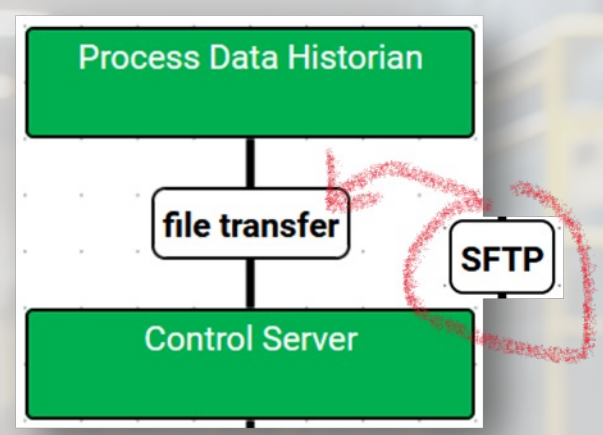
ADD SECURITY COMPONENTS



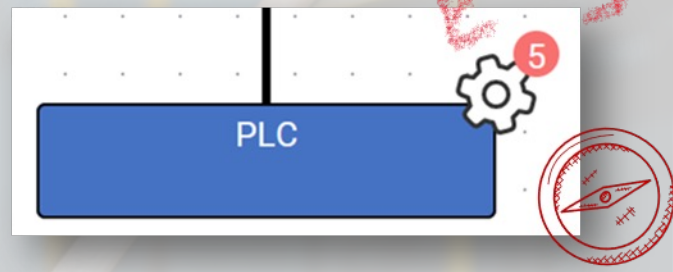
Function decisions



ELIMINATE FUNCTIONS



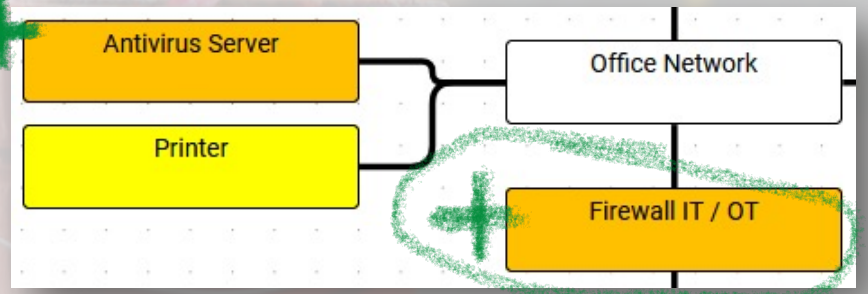
CHOOSE PROTOCOLS



CONFIGURE FUNCTION COMPONENTS

Architecture decisions

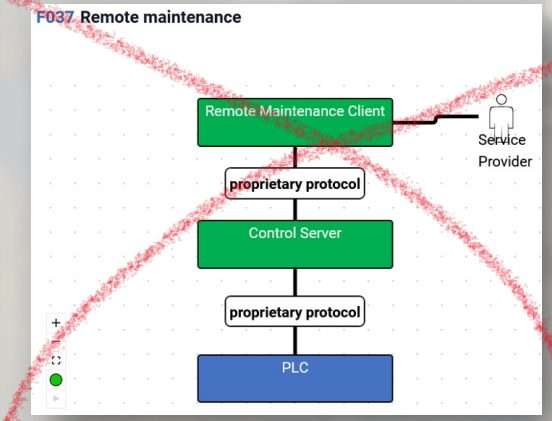
ADD NETWORK SEGMENTS



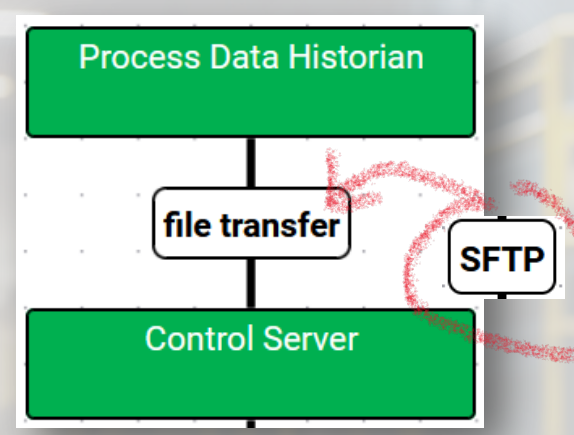
ADD SECURITY COMPONENTS

Security by design decision types

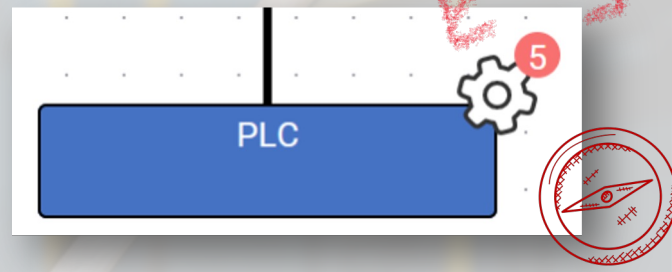
Function decisions



ELIMINATE FUNCTIONS

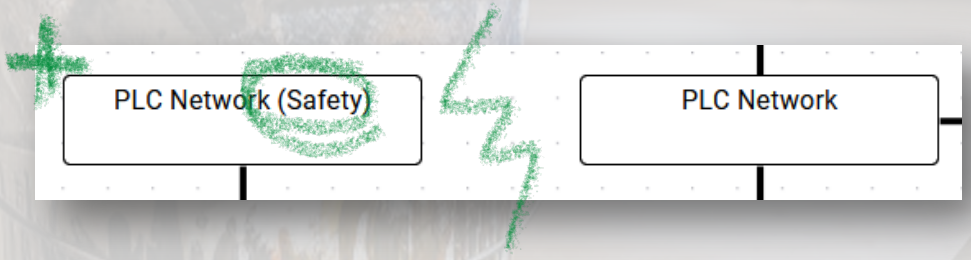


CHOOSE PROTOCOLS

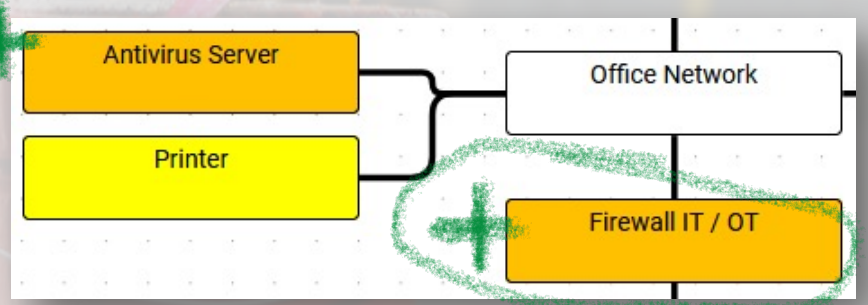


CONFIGURE FUNCTION COMPONENTS

Architecture decisions



ADD NETWORK SEGMENTS



ADD SECURITY COMPONENTS

Lifecycle decisions

PROCUREMENT CRITERIA

MONITORING IN CONTROL SYSTEM

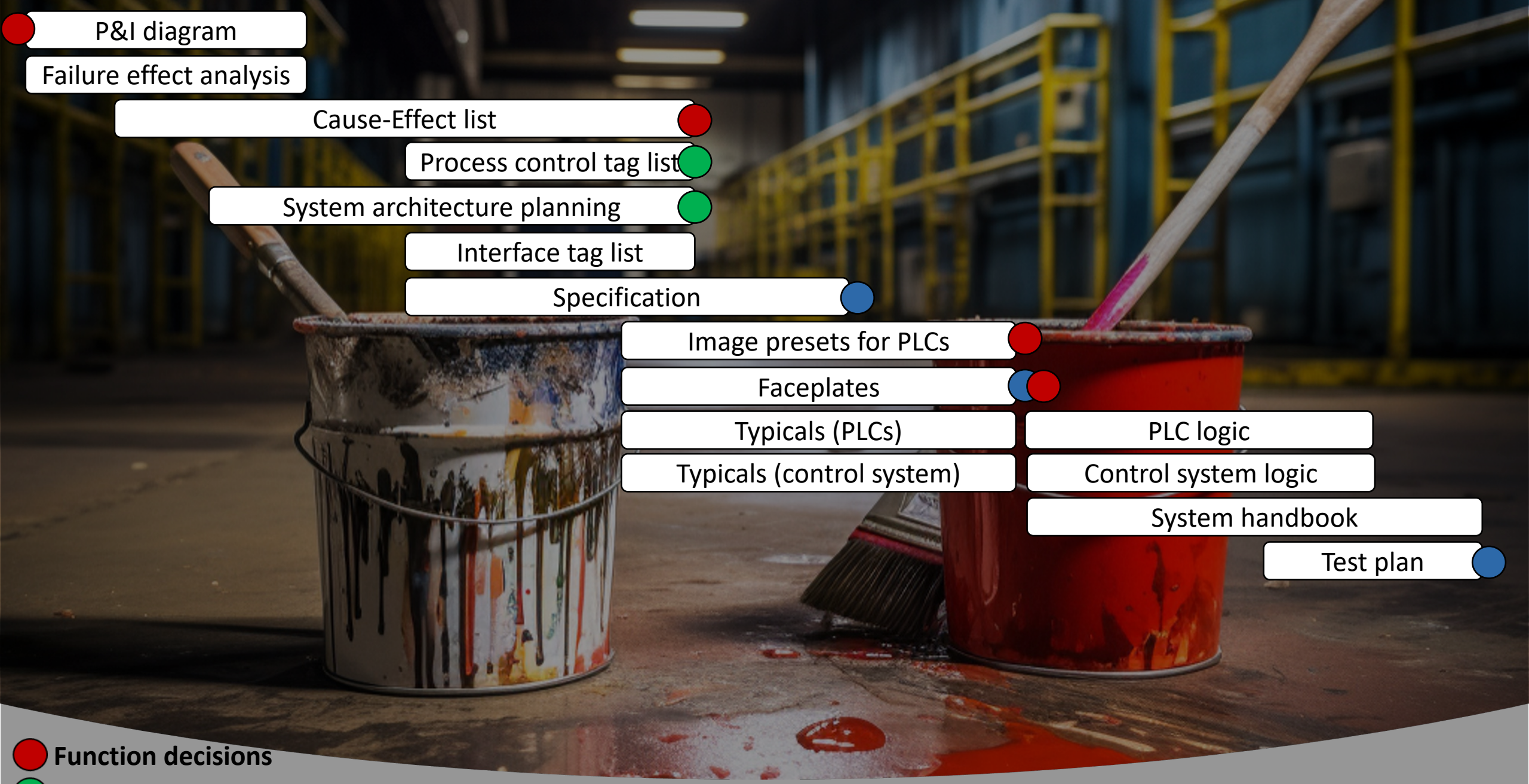
SECURITY ACCEPTANCE TESTS

Security by design decision types

Integration of security into engineering workflow

- Failure effect analysis
- Specification
- Image presets for PLCs
- Test plan
- P&I diagram
- Faceplates
- Cause-Effect list
- PLC logic
- Interface tag list
- Process control tag list
- System architecture planning
- Control system logic
- System handbook
- Typicals (PLCs)
- Typicals (control system)

Function decisions
Architecture decisions
Lifecycle decisions



Function decisions
Architecture decisions
Lifecycle decisions

Integration of security into engineering workflow

Myth 3

Security by Design is successful if after the design no vulnerabilities emerge.

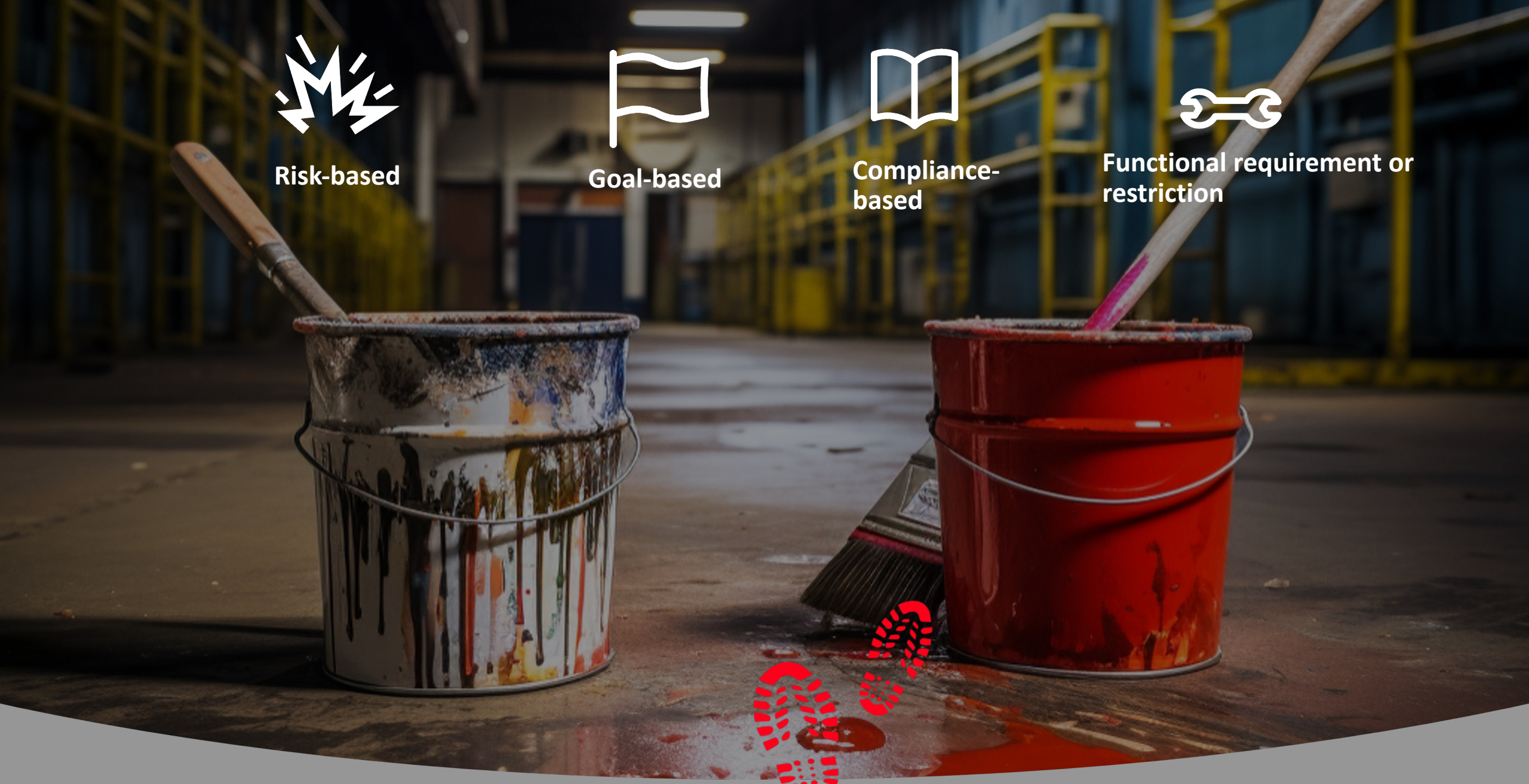
Reality

Security by Design is successful if after the design

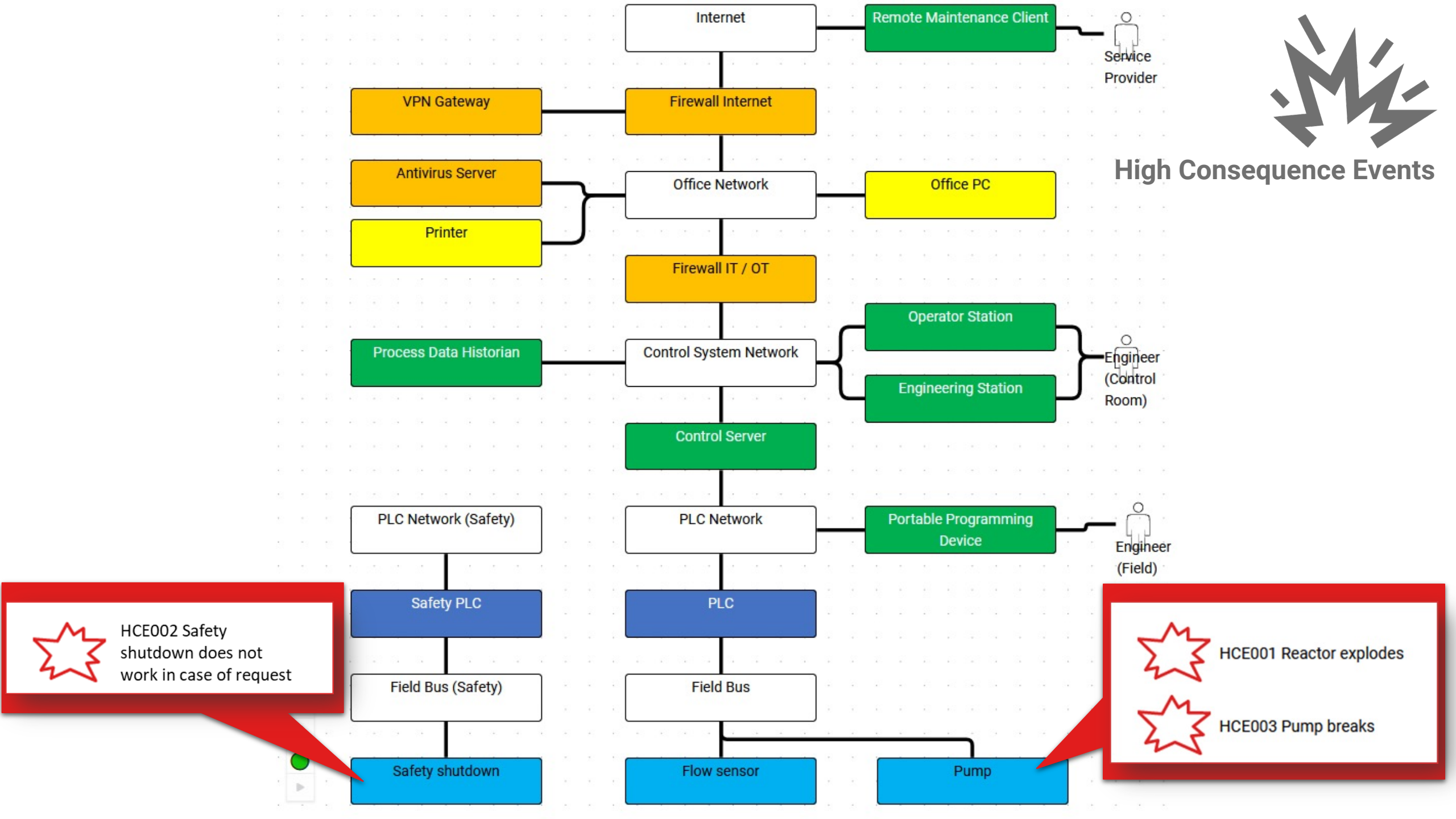
~~no vulnerabilities emerge.~~

all security decisions are traceable by third parties.


Security decisions
must leave traces



Reasons for a security decision


High Consequence Events
Internet
Remote Maintenance Client
Service Provider
VPN Gateway
Firewall Internet
Antivirus Server
Office Network
Office PC
Printer
Firewall IT / OT
Operator Station
Process Data Historian
Control System Network
Engineer (Control Room)
Engineering Station
Control Server
PLC Network (Safety)
PLC Network
Portable Programming Device
Engineer (Field)
Safety PLC
PLC
HCE002 Safety shutdown does not work in case of request
Field Bus (Safety)
Field Bus
HCE001 Reactor explodes
HCE003 Pump breaks
Safety shutdown
Flow sensor
Pump

F032 Engineering of PLC logic

Function Diagram | Security Decision Diagram | Attack Diagram

Attack scenarios

E009 PLC

Attack points

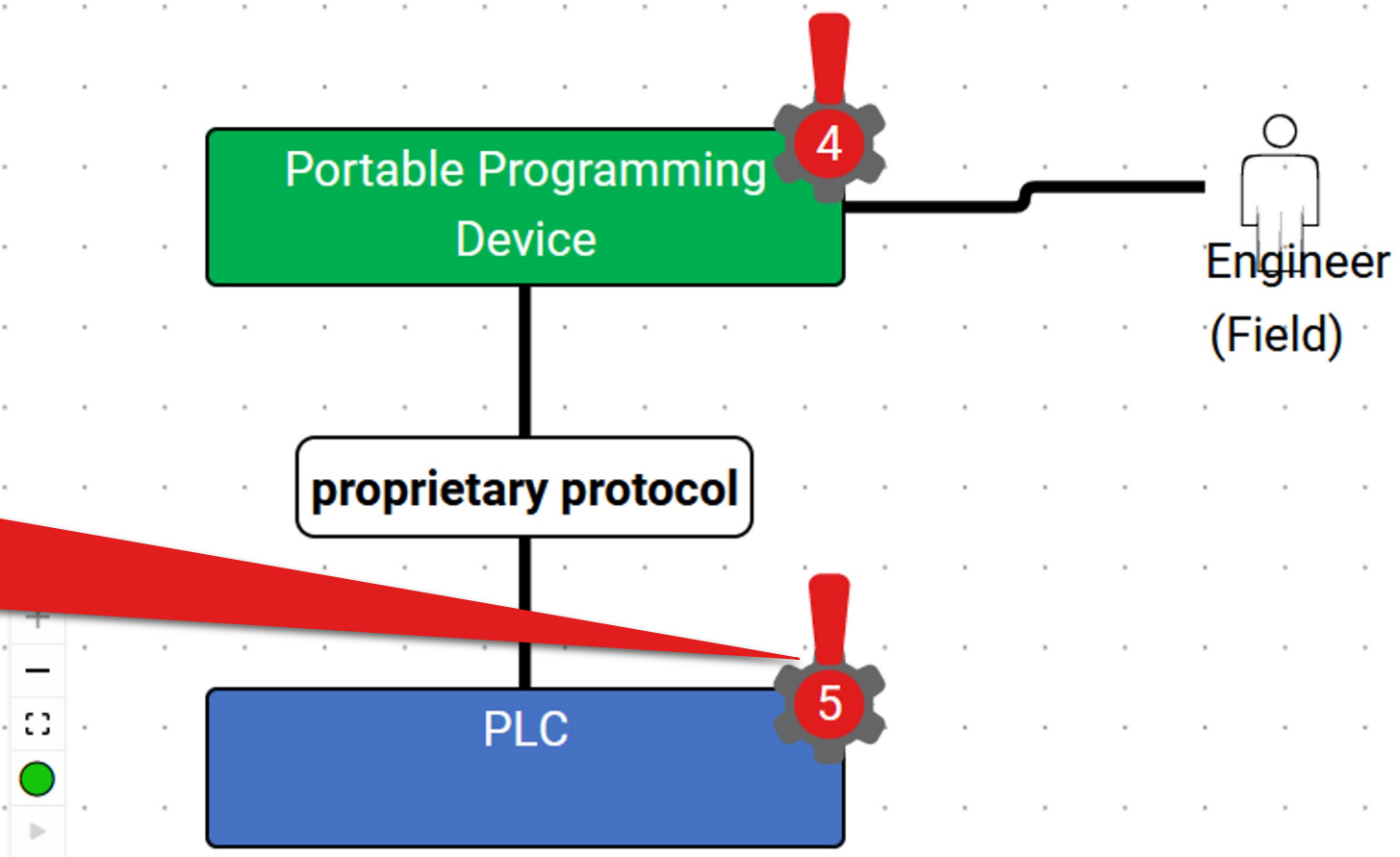
SP053 Port locking
- ❗ None

SP077 Read protection of PLC code
- ❗ No protection

SP093 Key switch for change of operating modes
- ❗ None
- ❗ Software switch

SP096 Update of PLC logic during operations
- ❗ Enabled

SP109 Manual operation
- ❗ Not possible



F032 Engineering of PLC logic

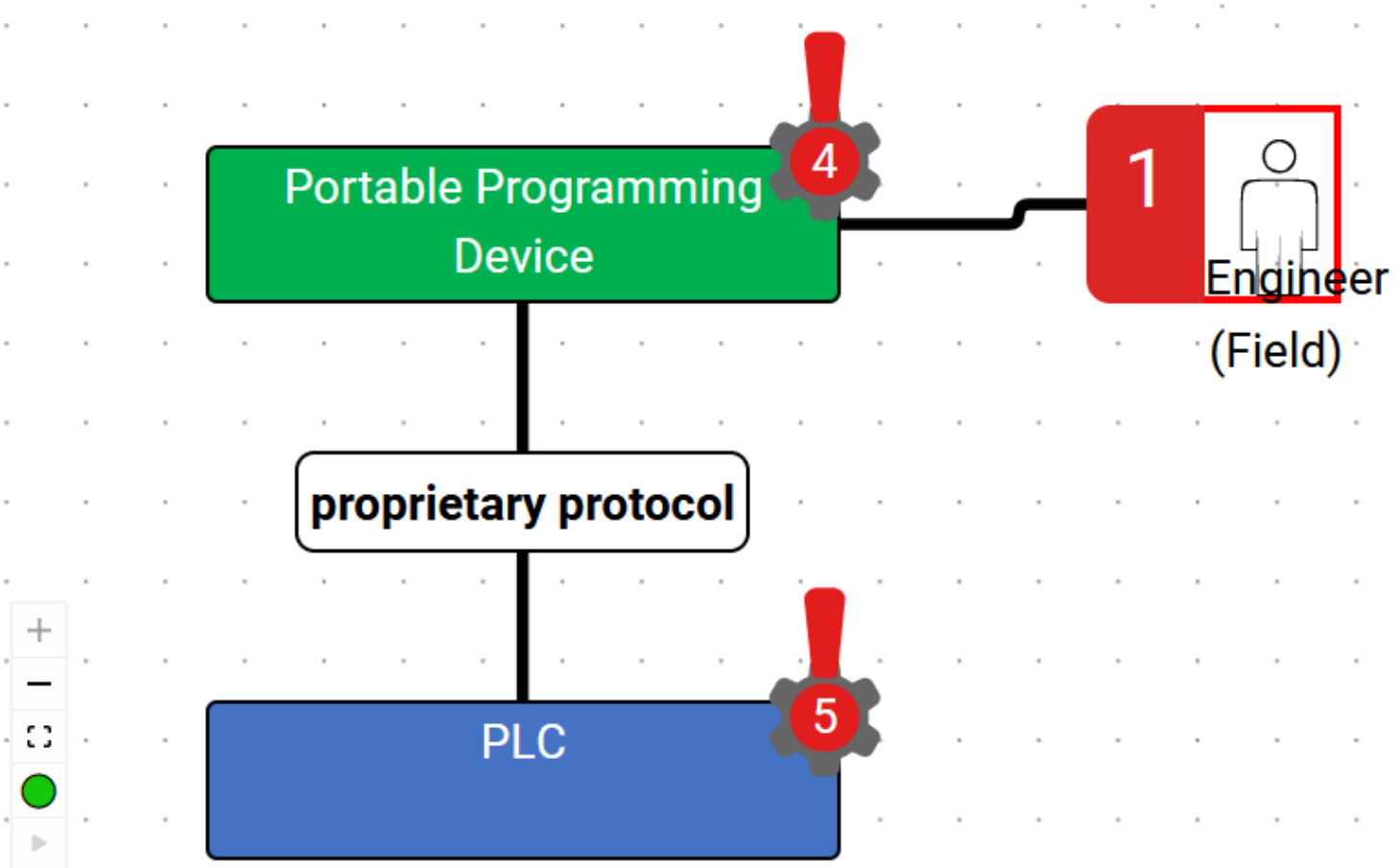
Function Diagram | Security Decision Diagram | **Attack Diagram**

Attack scenarios

Attack scenario:
Malicious change of PLC logic

1 TA0108 Initial Access: T0865 Spearphishing Attachment

E006 Engineer (Field)



High Consequence Events

HCE001 Reactor explodes

F032 Engineering of PLC logic

Function Diagram | Security Decision Diagram | **Attack Diagram**

Attack scenarios

Attack scenario:
Malicious change of PLC logic

1 TA0108 Initial Access: T0865
Spearphishing Attachment

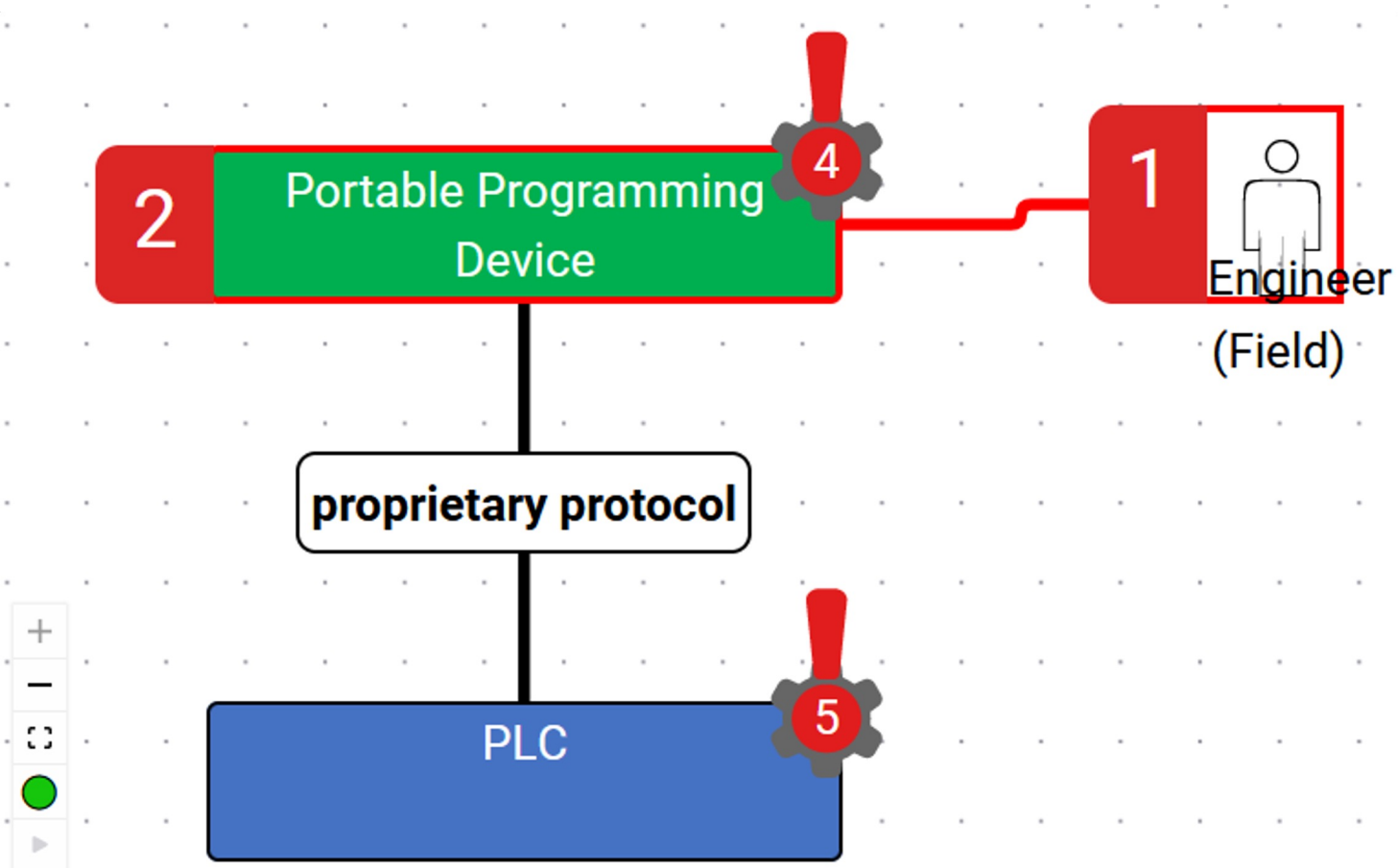
E006 Engineer (Field)

2 TA0109 Lateral Movement: T0891
Hardcoded Credentials

E008 Portable Programming Device

! SP046 Logging of authentication events: Disabled

! SP018 Password storage: Clear text in file



High Consequence Events

HCE001 Reactor explodes

F032 Engineering of PLC logic

Function Diagram | Security Decision Diagram | **Attack Diagram**

Attack scenarios

Attack scenario:
Malicious change of PLC logic

1 TA0108 Initial Access: T0865 Spearphishing Attachment

E006 Engineer (Field)

2 TA0109 Lateral Movement: T0891 Hardcoded Credentials

E008 Portable Programming Device

SP046 Logging of authentication events: Disabled

SP018 Password storage: Clear text in file

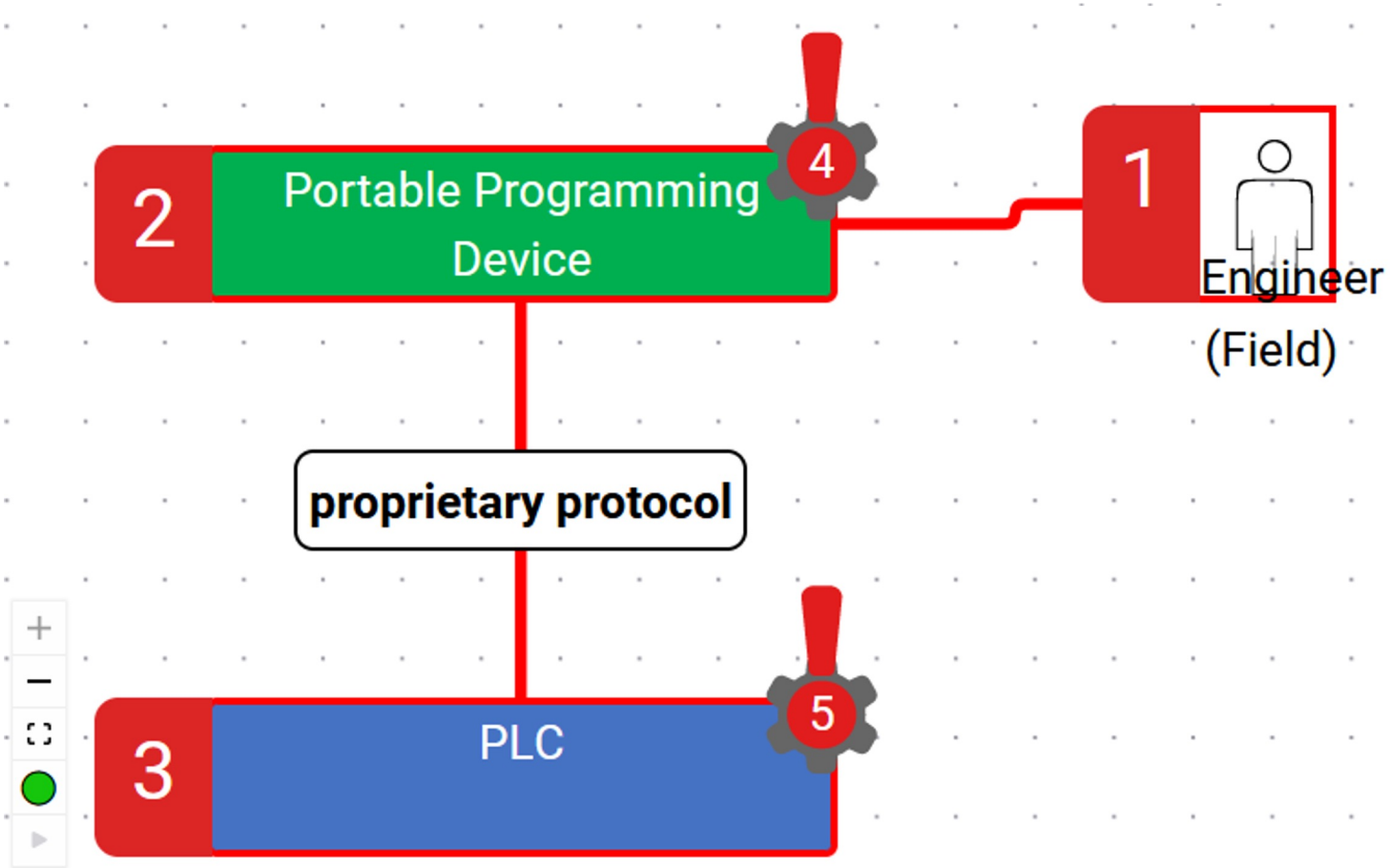
3 TA0105 Impact: T0831 Manipulation of Control

E009 PLC

SP096 Update of PLC logic during operations: Enabled

High Consequence Events

HCE001 Reactor explodes



F032 Engineering of PLC logic

Function Diagram | Security Decision Diagram | **Attack Diagram**

Attack scenarios

Attack scenario: Malicious change of PLC logic

1 TA0108 Initial Access: T0865 Spearphishing Attachment

- E006 Engineer (Field)

2 TA0109 Lateral Movement: T0891 Hardcoded Credentials

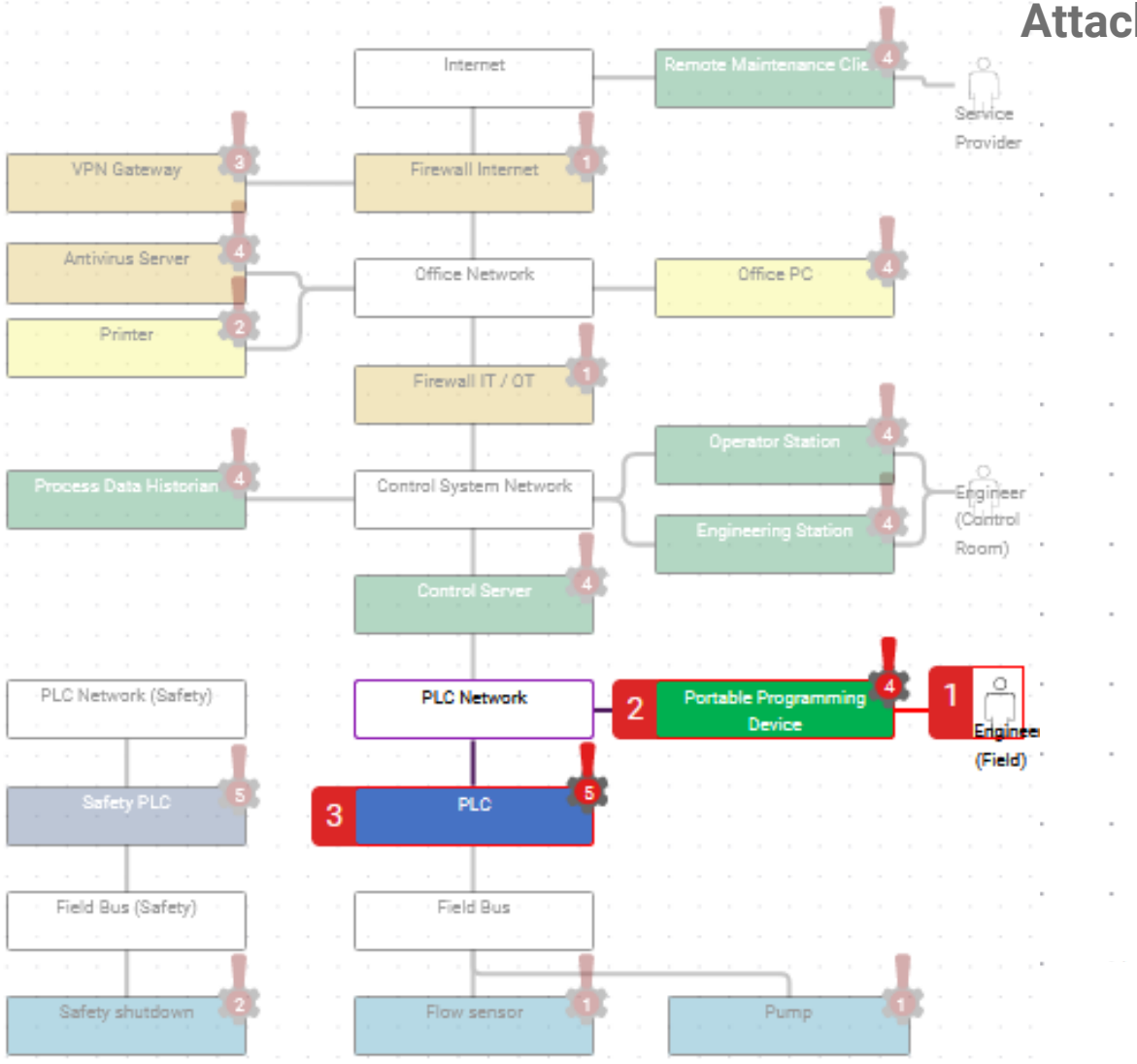
- E008 Portable Programming Device
- ! SP046 Logging of authentication events: Disabled
- ! SP018 Password storage: Clear text in file

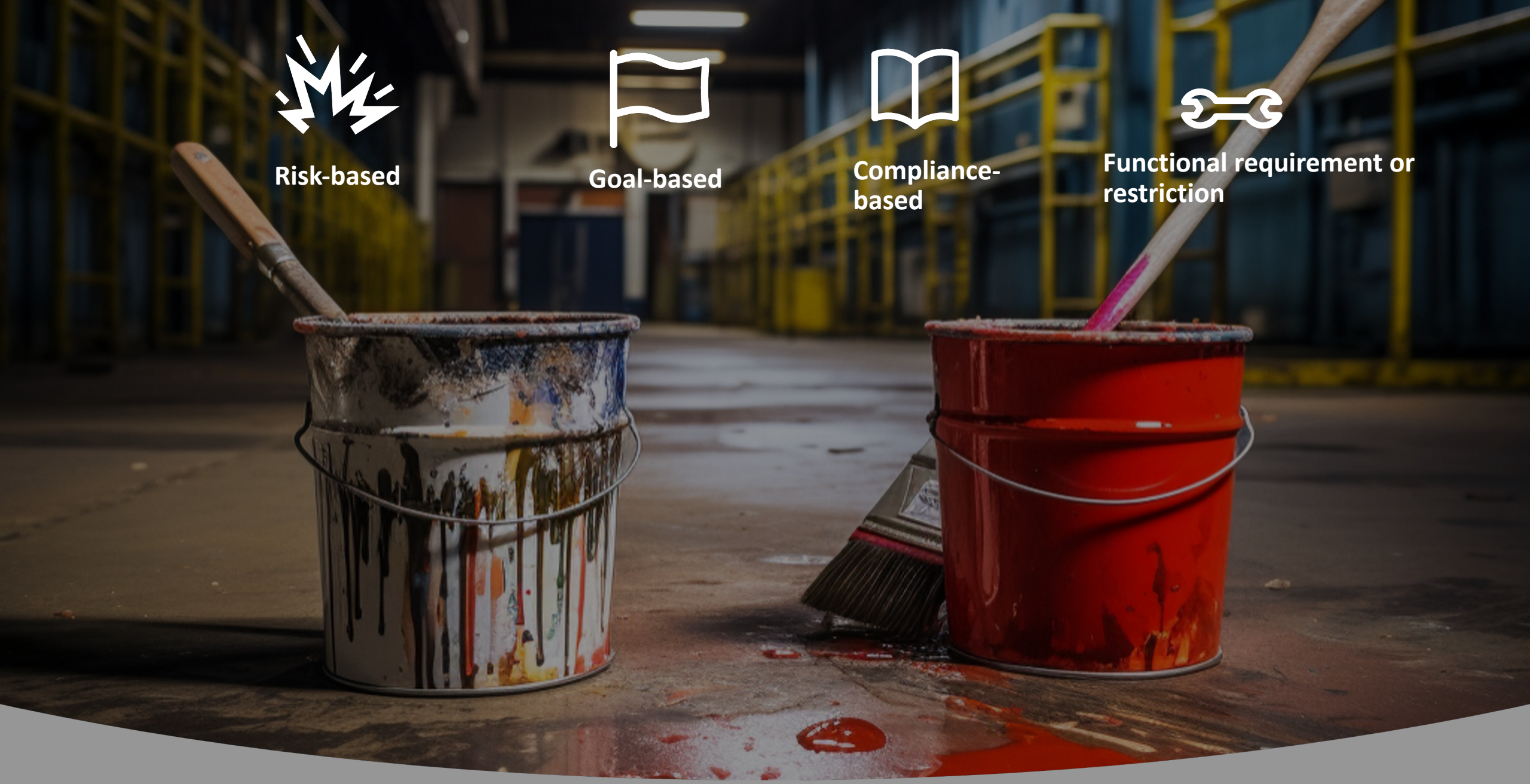
3 TA0105 Impact: T0831 Manipulation of Control

- E009 PLC
- ! SP096 Update of PLC logic during operations: Enabled

High Consequence Events

HCE001 Reactor explodes





Reasons for a security decision

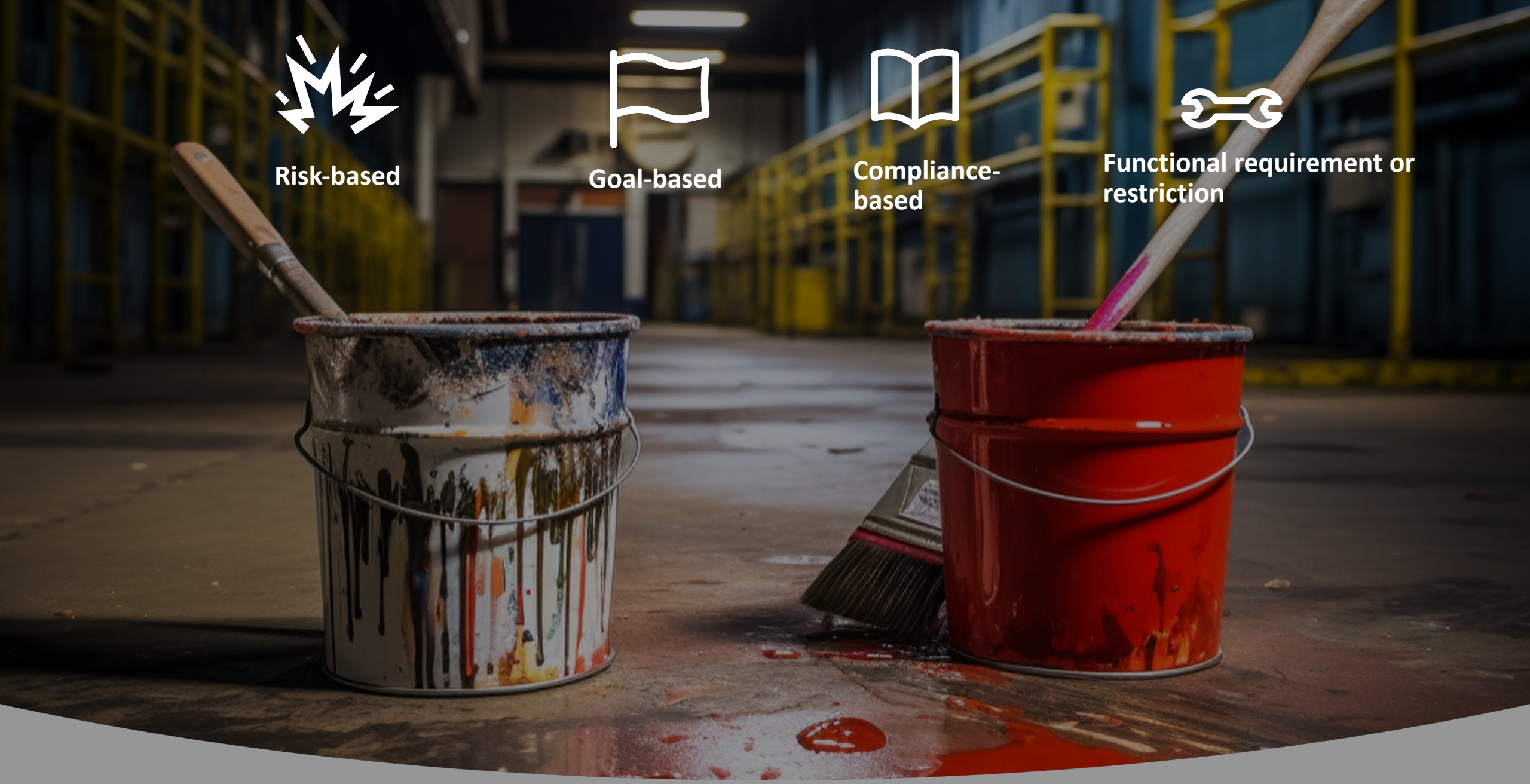
Security Goals

SG001
Portable programming device can only be used by authorized personnel

SG002
Integrity of safety shutdown logic

SG003
Control system components can only be accessed read-only from external networks

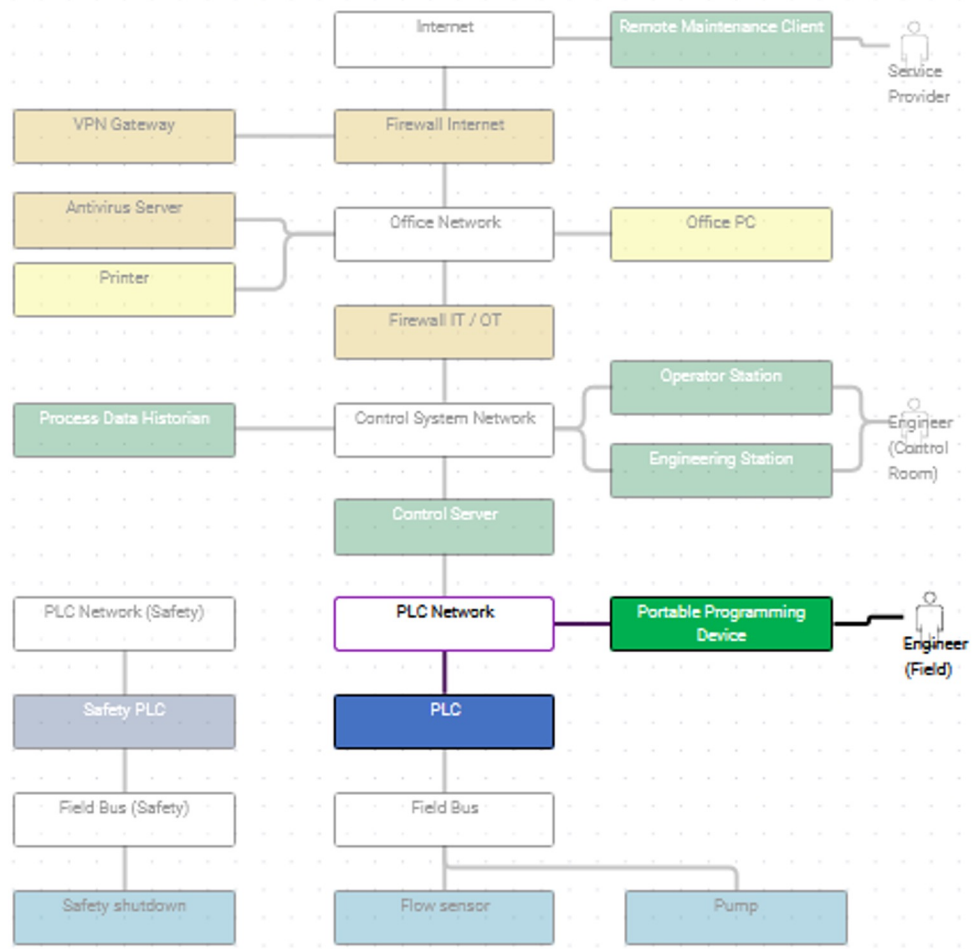
SG004
Pump always stays within safe operating range



Reasons for a security decision

F032 Engineering of PLC logic

Function Diagram | Security Decision Diagram | Attack Diagram



F032 Engineering of PLC logic

3 TA0105 Impact: T0831 Manipulation of Control

E009 PLC

SP096 Update of PLC logic during operations: Enabled

Function Diagram | Security Decision Diagram | Attack Diagram

Security Goals 4 | High Consequence Events 3 | Attack Scenarios 3 | Standards 1

Decision

SP096 Update of PLC logic during operations

- Disabled
- Enabled

Rationale

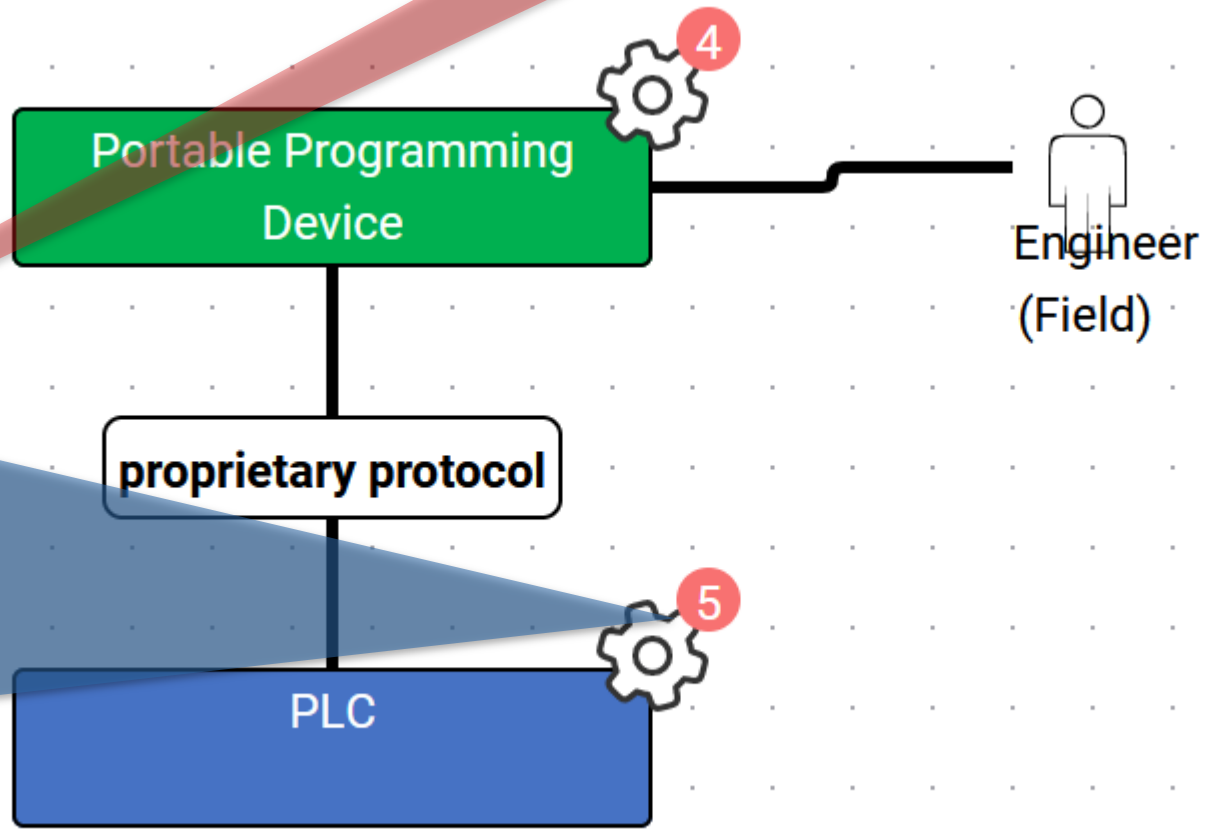
- Goal-based decision
- Compliance-based decision
- Risk-based decision

ASC001 Malicious change of PLC logic

HCE001 Reactor explodes

HCE003 Pump breaks

- Decision driven by functional requirement or restriction



F032 Engineering of PLC logic

Decision

SP096 Update of PLC logic during operations

- Disabled
- Enabled

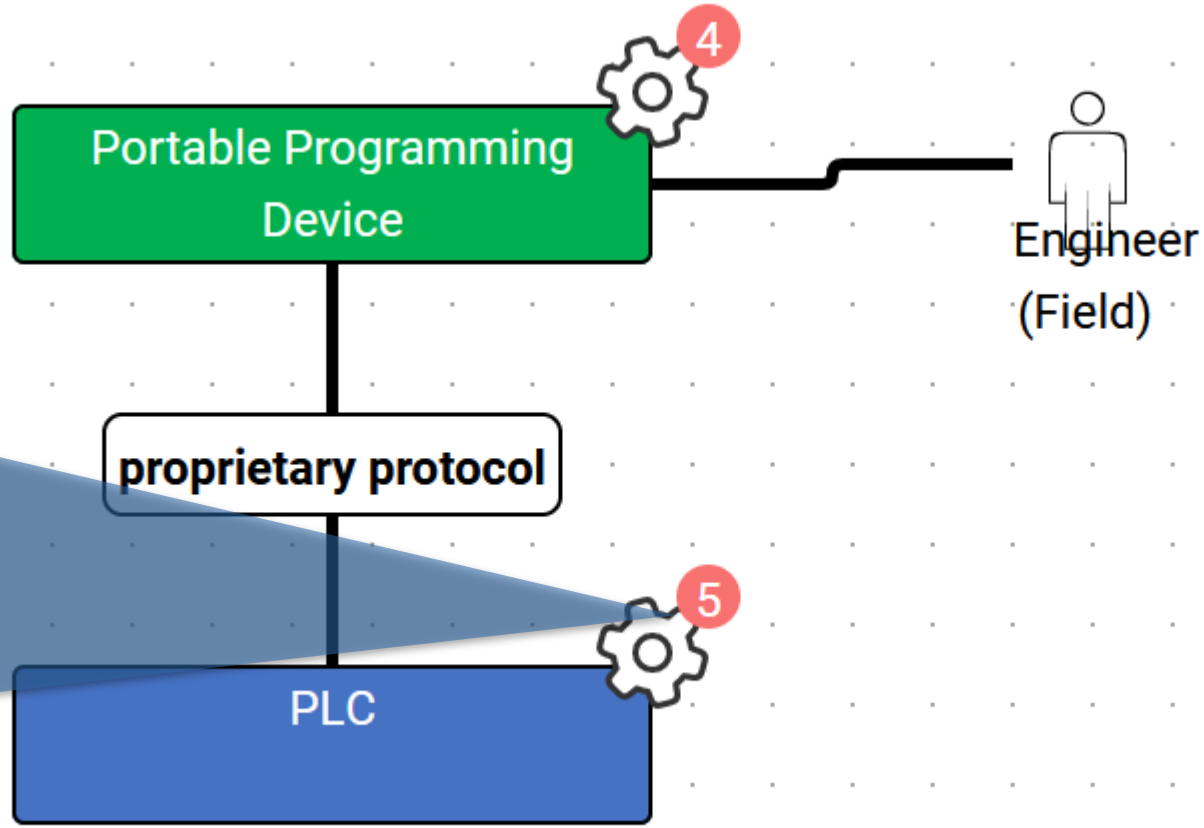
Rationale

- Goal-based decision
- Compliance-based decision
- Risk-based decision
- Decision driven by functional requirement or restriction

57%

Function Diagram | Security Decision Diagram | Attack Diagram

Security Goals 4 | High Consequence Events 3 | Attack Scenarios 3 | Standards 1



Security by Design...

...is ~~a vendors' problem.~~
a common problem of vendors and asset owners.

...is done by ~~following secure by design principles.~~
making explicit security decisions during design.

... is successful if after design ~~no vulnerabilites emerge.~~
all security decisions are traceable by third parties.

admeritia

MODEL

DECIDE

Security by design project „IDEAS“: admeritia.de/ideas

LinkedIn: linkedin.com/in/sarah-fluchs

Blog: fluchsfriction.medium.com

Make security by design a reality.