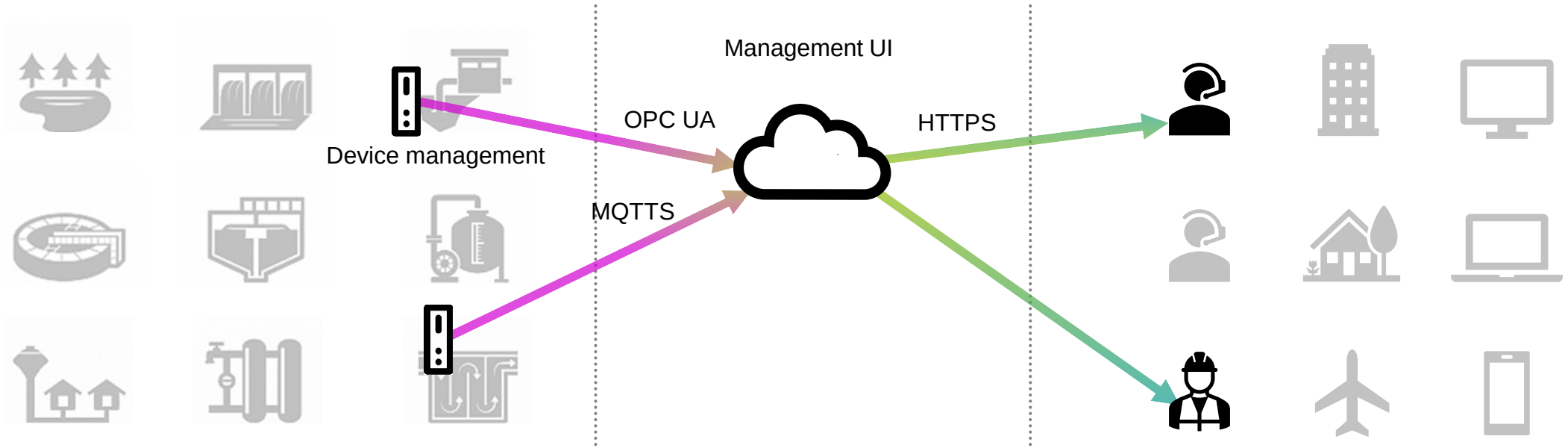
EP2

IoT Security – The Myth, Truth, and Advice

- Is your IoT solution as secure as you think?
- The conflicting megatrends: IoT vs. cybersecurity
- The new IEC62443-1-6 and zero trust approach
- Practical advice on securing your IoT-enabled systems

Industrial Internet of Things

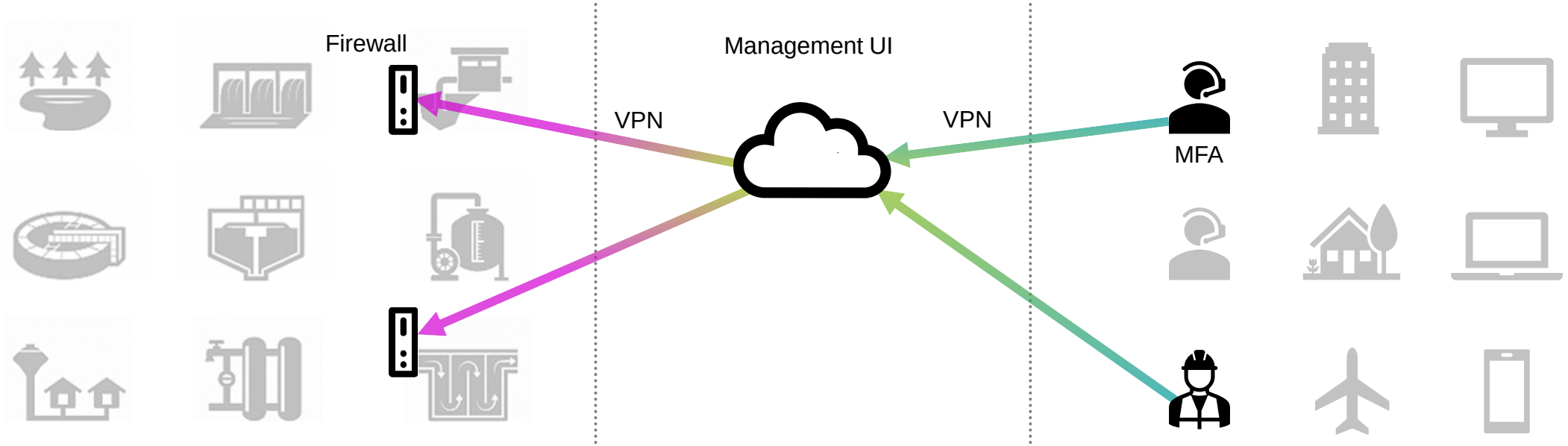
Digitalization



PHOENIX CONTACT
INSPIRING INNOVATIONS

Industrial Internet of Things

Remote Access



PHOENIX CONTACT
INSPIRING INNOVATIONS

Are you sure your IoT solution as secure as you think?

The conflicting megatrends

IoT vs. Cybersecurity

	IoT	Cybersecurity
Year	2010s -	2020s -
Sector	Cross sectors	Cross sectors
Focus	Cloud services Easy-to-use, fast deployment	Holistic Restrictions
Components	IoT edges, sensors (Good enough)	Everything (Security levels, Certificates)
Standard	Technology	More than technology
Entry barrier	Low	Very high Policy and Process System, Components, Certificates
Business Impact	Preferable	Regulations and laws

In Terms of IEC62443

General	1-1 Technology, concepts, and models	1-2 Master glossary of terms and abbreviations	1-3 System security compliance metrics	1-4 System security lifecycle and use case	1-5 Rules for IEC62443 profiles
Policies & Procedures	2-1 Requirements for an IACS security management system	2-2 Security protection rating	2-3 Patch management in the IACS environment	2-4 Requirements for IACS solution providers	2-5 Implementation guidance for IACS asset owners
System	3-1 Security technologies for IACS	3-2 Security risk assessment for system design	3-3 System security requirements and security levels		
Component	4-1 Secure product development lifecycle	4-2 Technical security requirements for IACS components			

In Terms of IEC62443

Component

- Security of the IoT gateway itself
- Security features of the IoT gateway
- Cloud availability, host security, data security, ...
- Security of the remote workstation
- ...

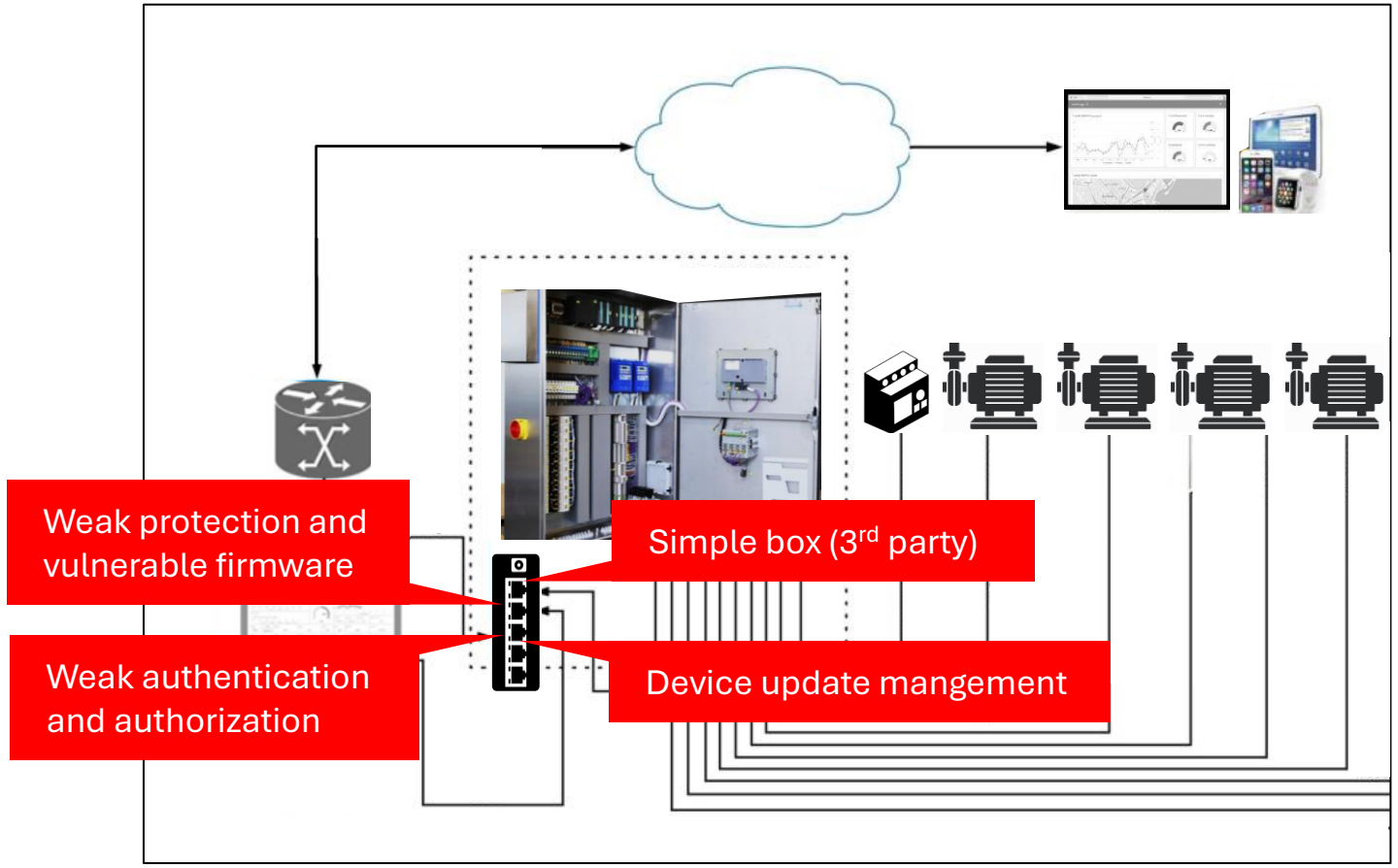
System

- Remote zone and machine zone
- User/ group/ machine management
- Restricted user and privileges
- On demand and 4-eye principle
- Supervise-able and revoke-able
- ...

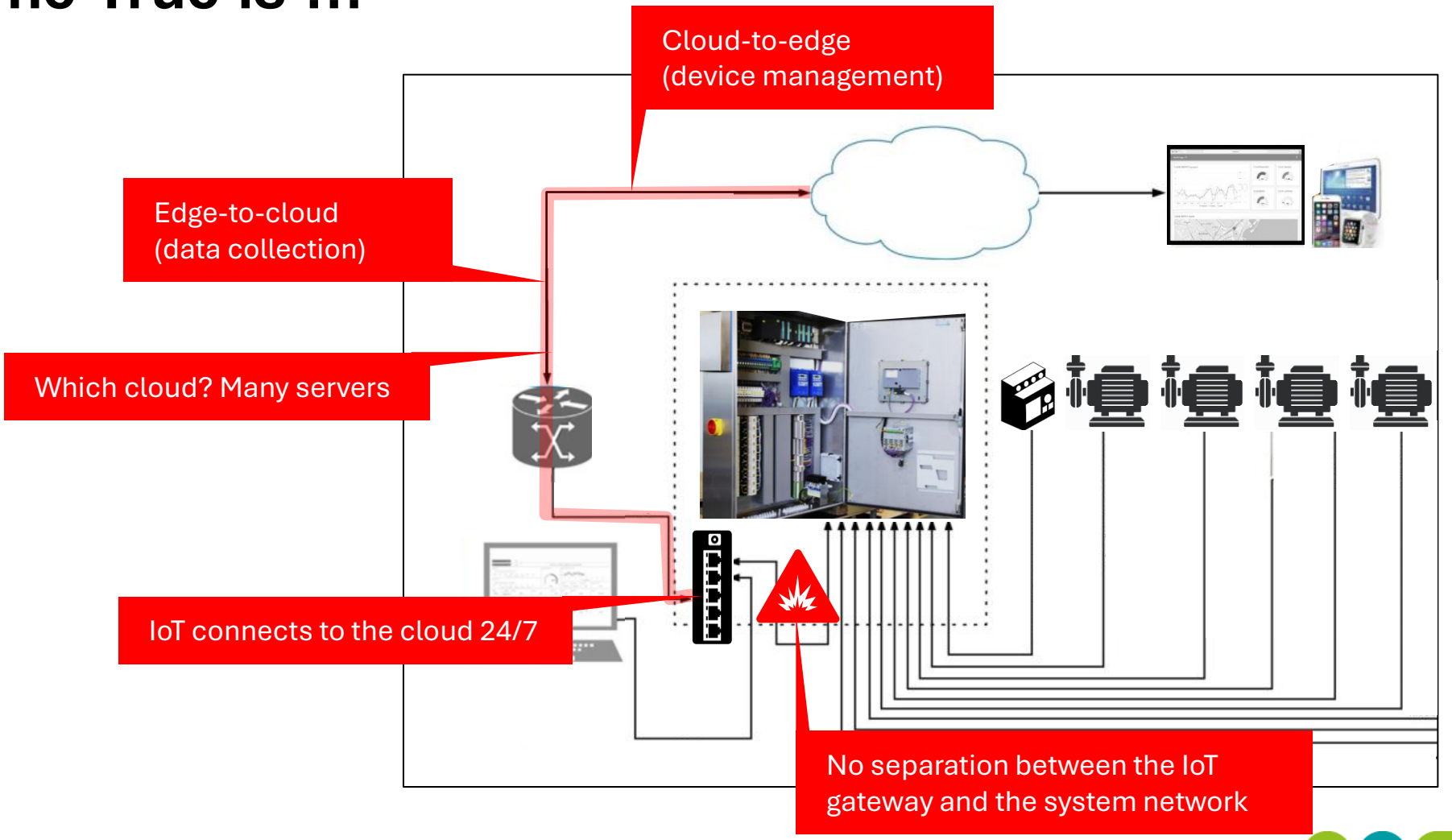
Supplier

- Cybersecurity management
- Policy, process and procedure
- Trustworthy technically, financially ...
- ...

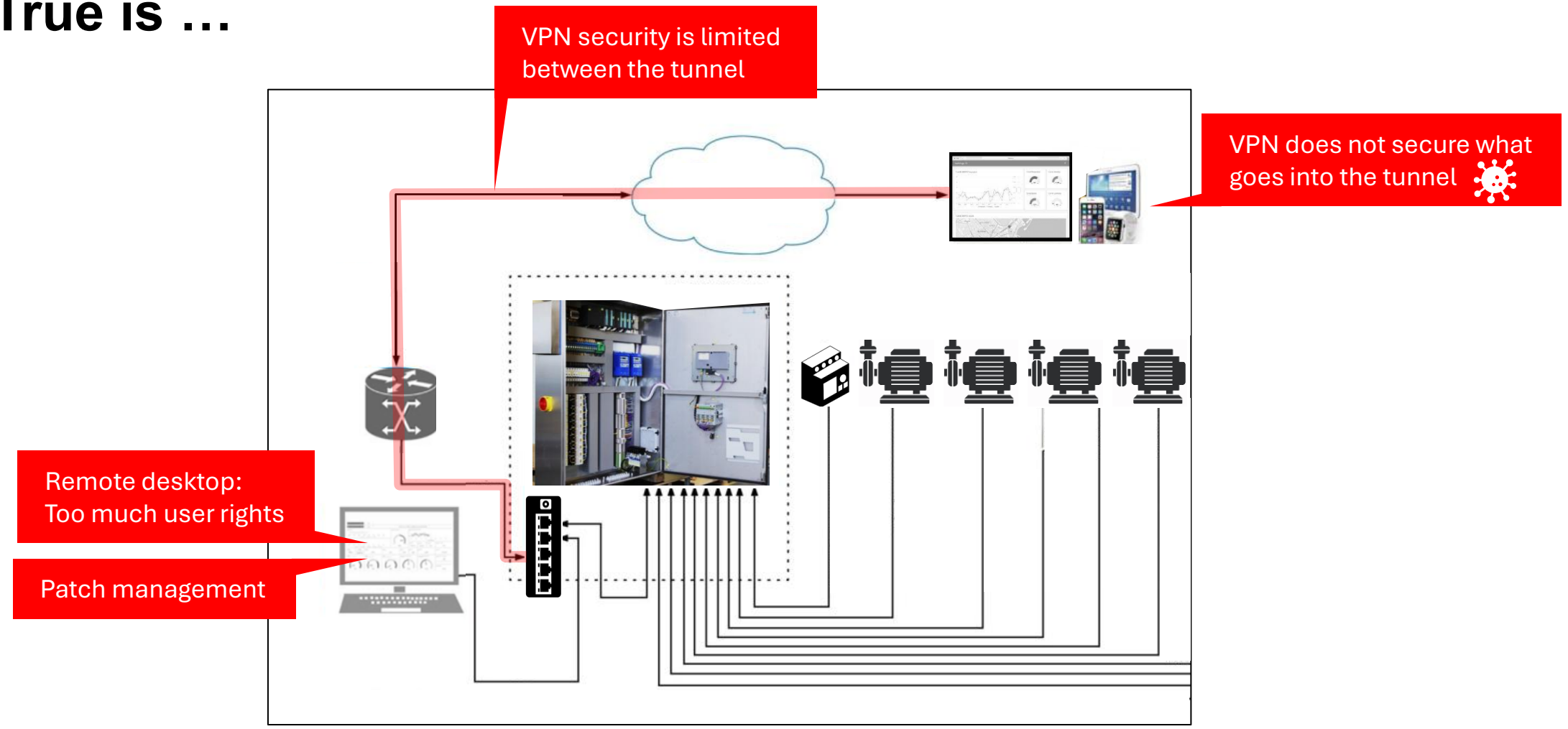
The True is …



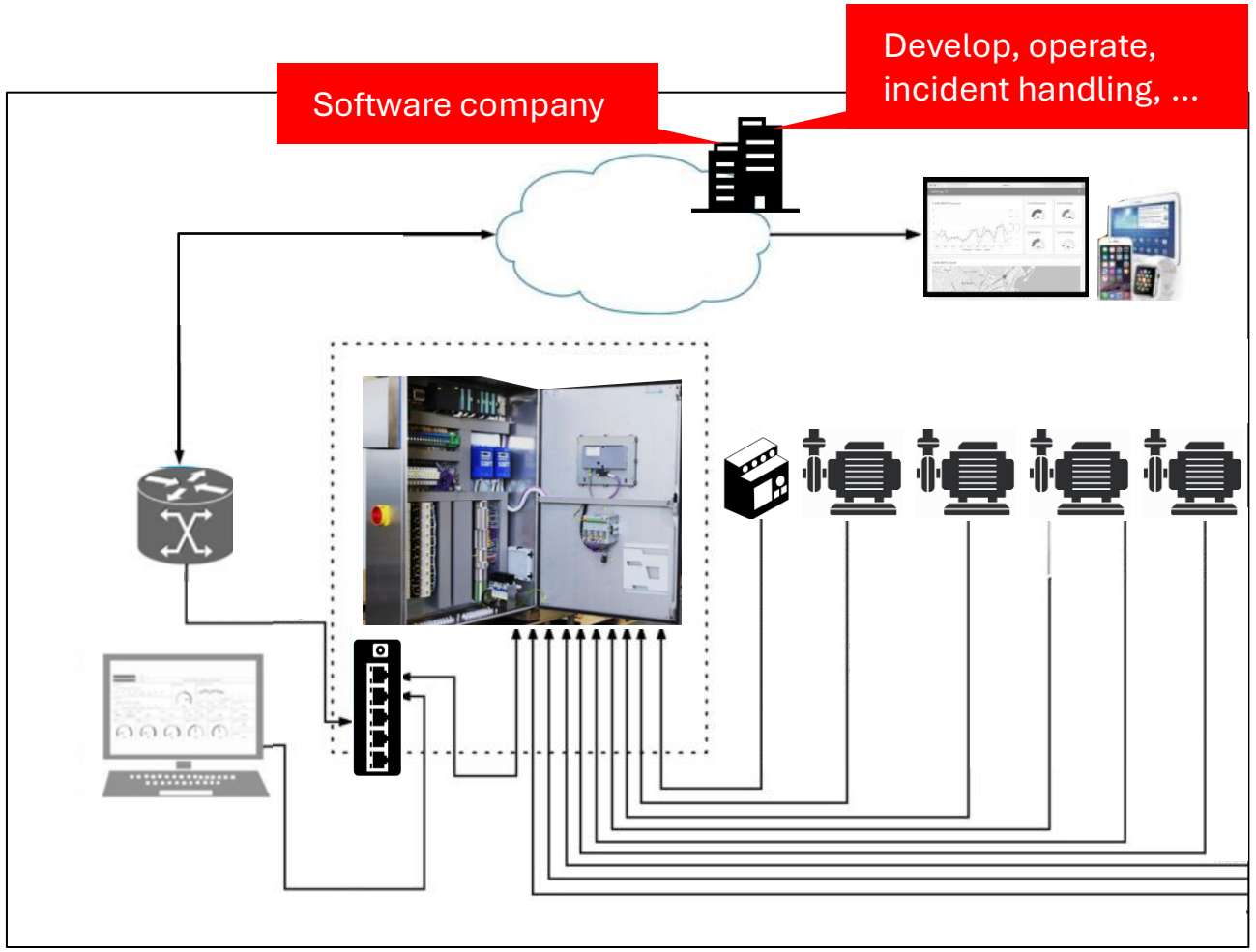
The True is …



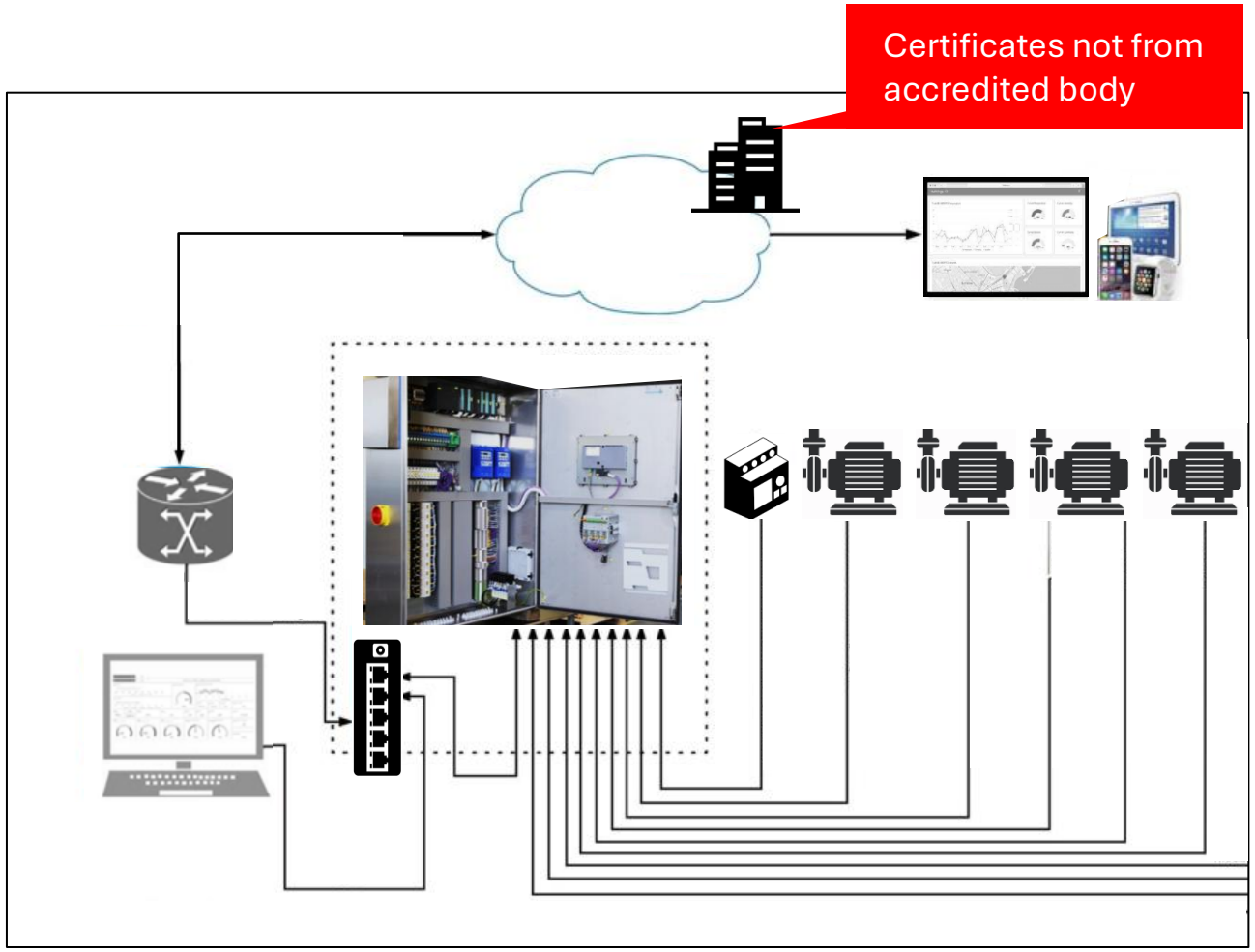
The True is …



The True is …



The True is …



The New IEC62443-1-6

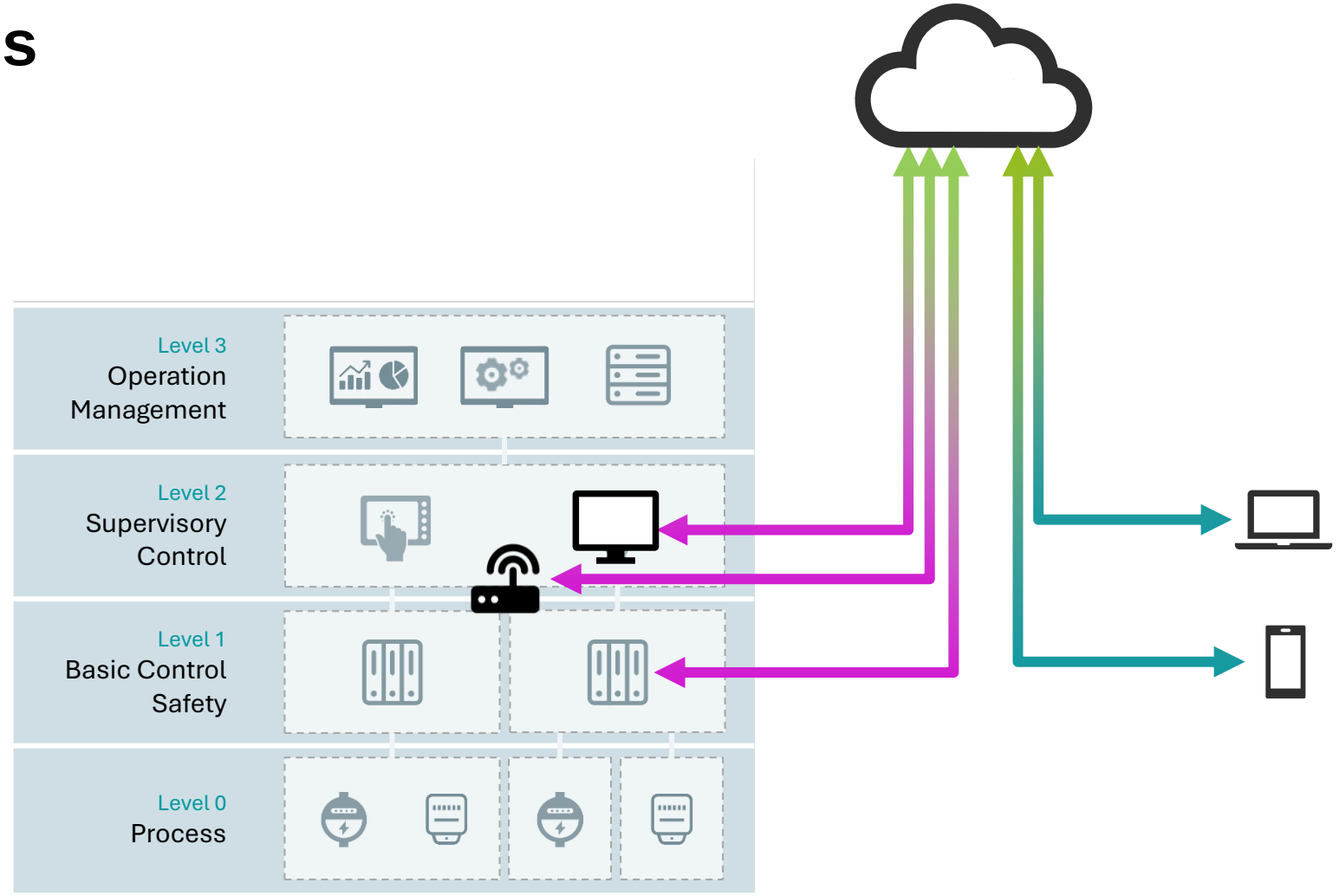
General	1-1 Technology, concepts, and models	1-2 Master glossary of terms and abbreviations	1-3 System security compliance metrics	1-4 System security lifecycle and use case	1-5 Rules for IEC62443 profiles	1-6 Application of the 62443 standards to industrial IoT
Policies & Procedures	2-1 Requirements for an IACS security management system	2-2 Security protection rating	2-3 Patch management in the IACS environment	2-4 Requirements for IACS solution providers	2-5 Implementation guidance for IACS asset owners	
System	3-1 Security technologies for IACS	3-2 Security risk assessment for system design	3-3 System security requirements and security levels			
Component	4-1 Secure product development lifecycle	4-2 Technical security requirements for IACS components				

- A technical report for asset owner, system integrator, and product supplier
- IoT security concerns and enhancement recommendations

IEC62443-1-6

IoT Security Concerns

- IoT breaks the IEC62443 reference model
- Bi-directional communication from/to the internet; back door
- Risk of hopping across levels or zones
- No separation between IoT and the automation control system



PHOENIX CONTACT
INSPIRING INNOVATIONS

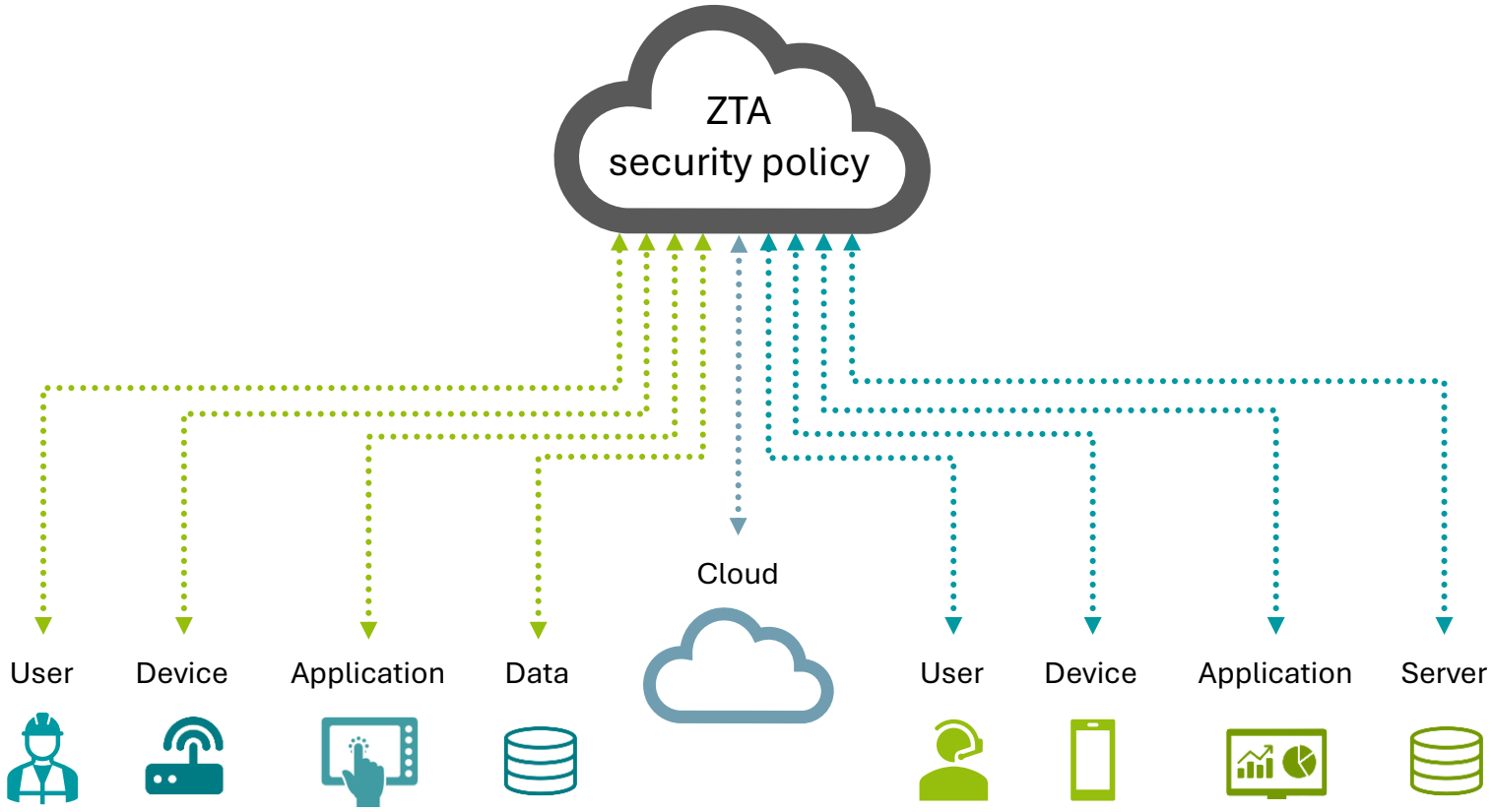
IEC62443-1-6

IoT Security Enhancement

- Zero Trust approach
  - Never trust, always verify
  - Nothing is accessible unless the user is authenticated and authorized
  - Authentication, Least Privilege
- vs. traditional approach
  - ‘Trust by default’ behind the firewall
  - ‘Trust by default’ via the VPN tunnel

- Zero Trust Security Model
- Zero Trust Architecture (ZTA)
- Zero Trust Network Access (ZTNA)

How It Works



Practical Questions

- Zero – to what extent?

- Everything? Where can we find such kind of component nowadays?

- Will the IEC62443 reference model be replaced by zero trust model?

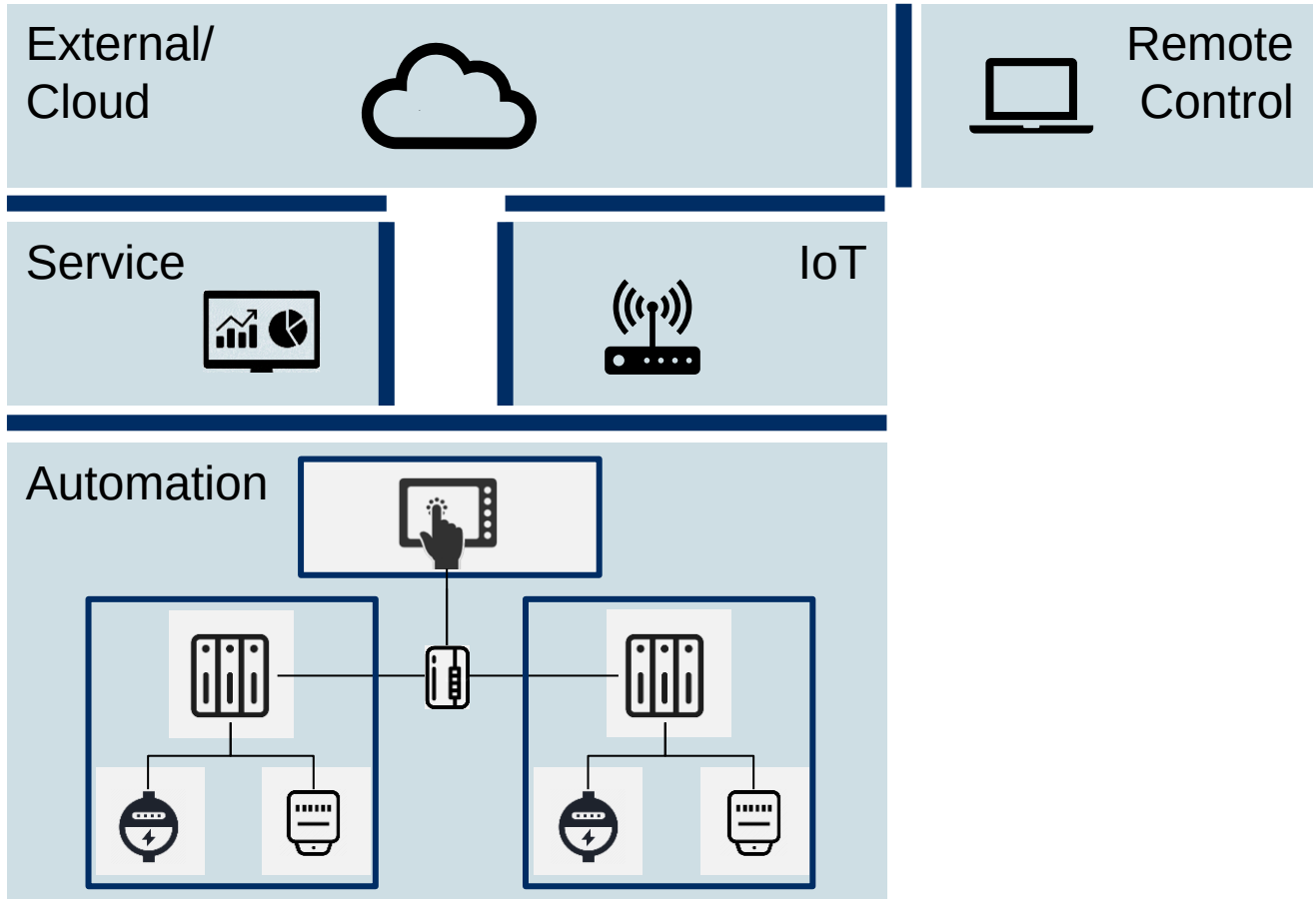
- Authentication
  - Human users
  - Hardware components
  - Software components
  - …

- Least Privilege
  - System
  - Subnet
  - Component
  - Software
  - Function
  - Data
  - …

Protect you IoT-enabled system

Practical Advice

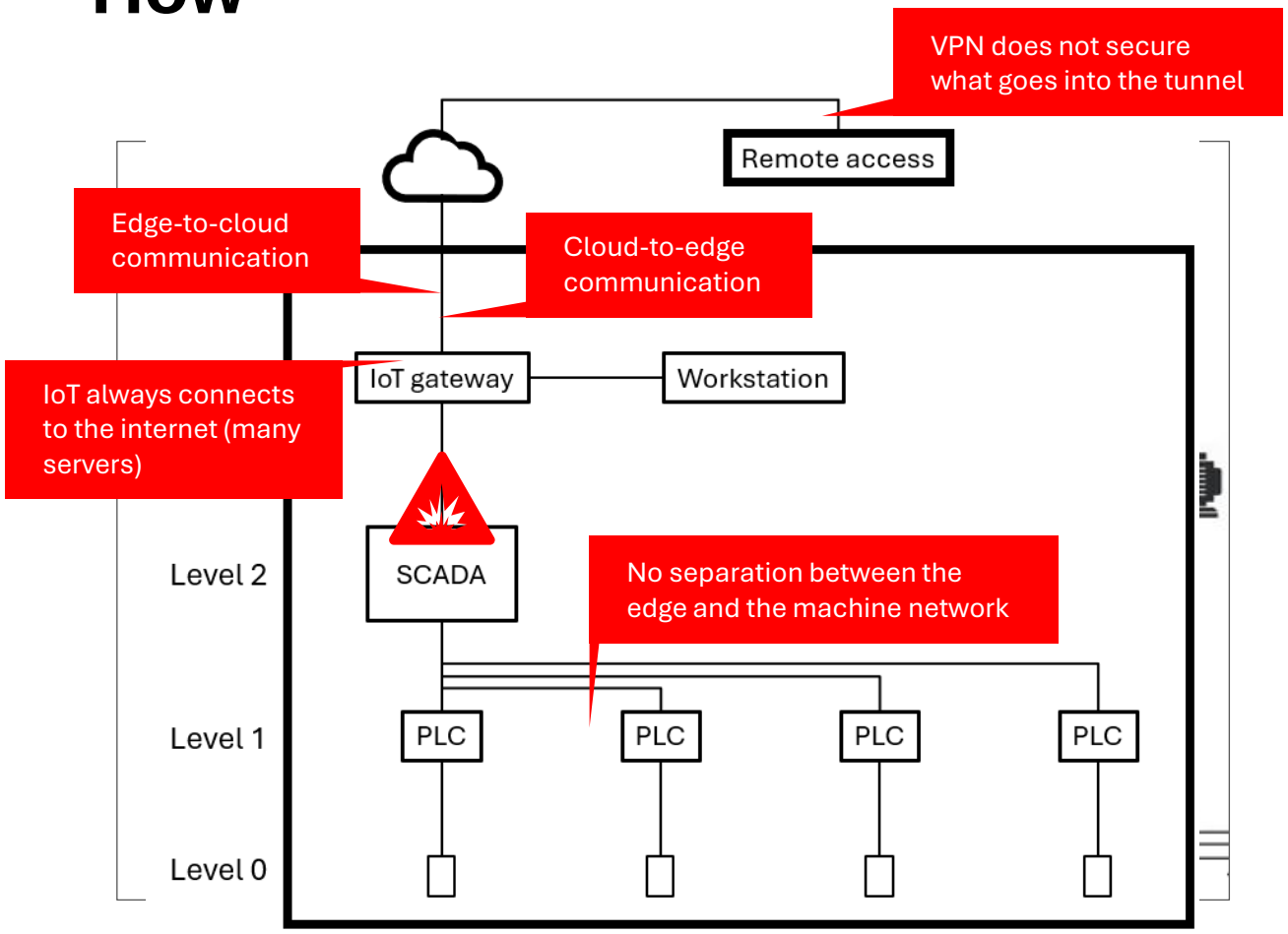
- Architect your system or machine network according to IEC62443 reference model: zones and conduits
- Create the smallest zone as a foundation to achieve a certain level of ‘zero trust’
- Consider open platform components for future development of zero trust



PHOENIX CONTACT
INSPIRING INNOVATIONS

Protect you IoT-enabled system

How

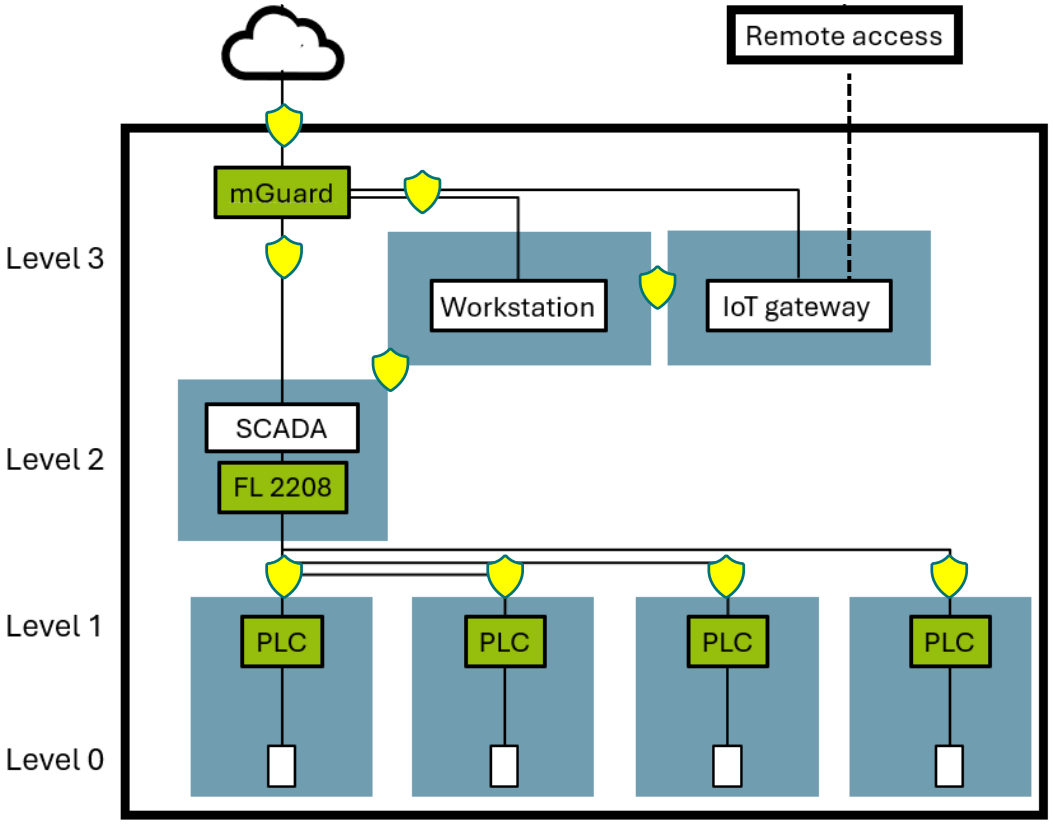


1. Review the system and network diagram with 4-eye principle
2. Revise the diagram according to the IEC62443 reference model
3. Security risk assessment

PHOENIX CONTACT
INSPIRING INNOVATIONS

Protect you IoT-enabled system

How



4. Find the optimal architecture according to IEC62443 zones and conduits

5. Protection between IoT/ Cloud/ Remote/ Operation/ Automation/ Safety/…

6. Build in Zero Trust concept by the network architecture or zero trust components (future-proof)

Protect you IoT-enabled system

mGuard Firewall and Zero Trust

- IEC 62443-4-1 product development process certified by accredited body TÜV SÜD
- IEC 62443-4-2 product certificate SL2
- TPM hardware-based root of trust
- Network architecture – create smallest zones
- Build in zero trust concept for remote access and on-site support
- DNV maritime approval

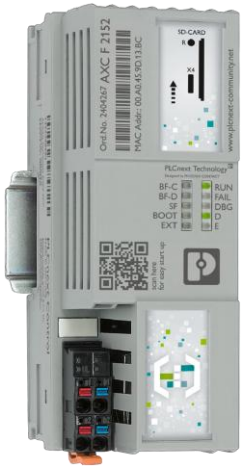
PHOENIX CONTACT
INSPIRING INNOVATIONS

Protect you IoT-enabled system

PLCnext Technology and Zero Trust

- IEC 62443-4-1 product development process certified by accredited body TÜV SÜD
- IEC62443-4-2 certified secure component by accredited body TÜV SÜD
- TPM hardware-based root of trust
- Firewall and Netload limiter
- Secure communication – VPN, OPC UA, MQTT, TLS…
- Role-based user management
- Open platform – Zero trust possible!
  - To itself
  - To the network

Automation



Safety

IoT

PHOENIX CONTACT
INSPIRING INNOVATIONS

NETWORK & CYBERSECURITY SERVICES

Together with Phoenix Contact, your cybersecurity journey will be future-proof

Why Phoenix Contact

Cybersecurity is a journey and Phoenix Contact is your trustworthy supplier with a leading pace towards NIS2, CRA, IEC 62443. We develop technologies and manufacture security products and use them to secure our worldwide production sites – as well as yours.

Your Benefits

Cybersecurity requires a holistic approach. Our 360° security, from product, service to solution, is a fast track for securing your system with Network, Safety, Automation, and IIoT – all from one place.

Start Your Journey

- ☑ **Overview & Review** FREE
  Learn how IEC62443 standards affect you, and review your system's network security, machine modularity, redundancy, remote access, etc.
- ☐ **Assess & Advice**
  Conduct security risk assessment and give risk mitigation advice on your system based on best practices such as NIST 800-30 and IEC62443.
- ☐ **Revise Network Design**
  Put the advice into practice. Optimize your network design, detail security rules and settings. Create manuals for implementation.
- ☐ **Network & Cybersecurity Training**
  Hands-on training: L2 switching, L3 routing, VLAN, NAT, firewall, VPN, and remote access. Theory education: IEC62443 standards.
- ☐ **IEC62443 Certified Security Service**
  Tailored services performed by Phoenix Contact's IEC62443 certified service team.

PHOENIX CONTACT

1 Execute Summary

The current state of the system, referred to as SuC As-Is, consists of a plane network that connects to owner's network and the internet, complete with a remote access backdoor. This setup exposes the system to significant risks from both internal and external cyber threats.

To enhance cybersecurity and protect against these risks, the following risk mitigation strategies should be implemented: network segmentation, system hardening, stronger access control, least privilege principle, use control, event monitoring. Additionally, adopting a zero-trust approach is recommended. Best practice options for an improved network structure, Network To-Be, are provided as guidance.

2 Risk Assessment

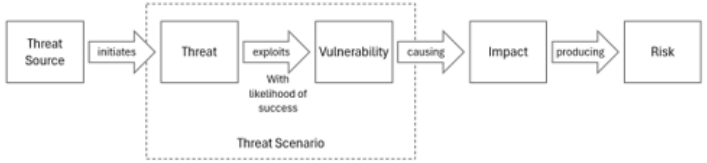
2.1 Initial Cybersecurity Risk Assessment

An *initial cybersecurity risk assessment* aims to provide a fundamental understanding of the worst-case unmitigated risks associated with systems under consideration (SuC). According to the international cybersecurity standard IEC 62443-3-2, "Security Risk Assessment for System Design", this assessment is a prerequisite for network segmentation.

This initial cybersecurity risk assessment follows the method outlined in NIST 800-30, "Guide for Conducting Risk Assessments." This includes the risk model, assessment approach, analysis approach, and the overall risk assessment process:

2.2 Method

2.2.1 Risk Model



A *risk model* outlines the *risk factors* to be evaluated and the relationships among those factors. A *threat source* is any potential actor that has the capability, either intentionally or unintentionally, to execute a *threat* aimed at exploiting a *vulnerability* within the SuC, which can lead to harmful consequences. A *threat scenario* illustrates how a threat poses by a threat source can result in damage.

The level of *risk* is determined by assessing two key elements: the likelihood of a threat's success and the severity of its potential impact. In an initial cybersecurity risk assessment, it is assumed that the likelihood of a threat is high (set to one), allowing for a focus on evaluating the worst-case scenario. This approach enables a quick assessment of the risk associated with the SuC.

2.2.2 Assessment Approach

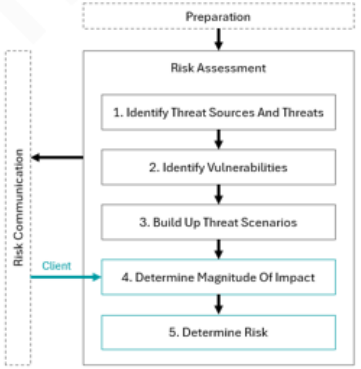
The evaluation of impact and risk determination is specific to each client. This initial cybersecurity risk assessment uses a qualitative approach to communicate risks to the client. The client can then further specify the risk level using either a qualitative or semi-qualitative assessment, based on their preference.

2.2.3 Analysis Approach

Based on the Client's input, which includes the network diagram, system inventory, data flows, and use scenario, the focus is more on the SuC rather than on threats or impacts. This assessment uses a vulnerability-oriented analysis approach. This means that the assessment begins by identifying vulnerabilities within the SuC and then considers potential threats that could exploit those vulnerabilities, leading to various threat scenarios and possible impacts.

2.2.4 Risk Assessment Process

The risk assessment process consists of several steps. Vulnerabilities, threats, and threat scenarios are developed based on the most common cyberattacks targeting industrial control systems. This report is intended for risk communication to the Client, who will ultimately decide the magnitude of impact and the level of risk.



2.3 Risk Factors

2.3.1 Threat Sources

Type	Description

2.4 Risk Assessment

2.4.1 Identify Vulnerabilities of SuC As-is

Based on the Client's input, which includes the network diagram, system inventory, data flows, and use scenarios to find out potential vulnerabilities:

Vulnerability	Review

2.4.2 Threat Scenarios

Threat scenarios to the SuC are predicted based on the list of vulnerabilities and threats. Potential threat scenarios are included but not limited to the items in the table.

Vulnerability	Threat	Threat Scenario	Impact	Risk

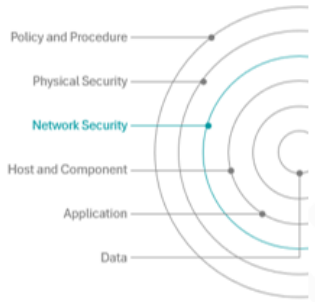
2.4.3 Impact and Risk Determination

Client should assess the threat scenarios and their impact on the system, business, and company to determine the level of risk.

3 Risk Mitigation Advice

3.1 Cybersecurity Approaches

Defense-in-depth



Using multiple layers of defense helps create various types of barriers, making it more challenging to breach the system.

Network security plays a crucial role in this defense-in-depth strategy through several means, including perimeter firewalls, network segmentation, micro-segmentation, access control, authentication of users and devices, authorization, and encrypted data communication.

Minimize Attack Surface

Also known as system hardening, this process involves reducing potential contact and entry points, both physically and logically, to prevent unauthorized access. For example, close unused ports, disable unnecessary services, and remove software that is not in use.

Least Privilege

Limiting user access to the minimum required to perform tasks essential for system interaction. The principle of least privilege safeguards against malicious access and insider threats.

4-eye Principle

Also referred to as dual approval or the two-person rule, this internal control policy mandates that critical changes receive approval from a second individual. The four-eye principle helps minimize errors and mitigate insider threats.

Keep It Simple, Stupid (KISS)

Achieving a balance between security and user-friendliness to reduce management complexity, minimize errors, and improve overall usability. The Client should consider whose own capability for the best implementation.

3.2 Advice List

Recommended actions and security countermeasures that should be taken to protect the system.

	Topics	Items	Priority	Check
1	**Network Segmentation**			
1.1		1)	High	
		2)	High	
		3)	Middle	
1.2		1)	High	
		2)	Middle	
		3)	Low	
1.3		1)	High	
		2)	High	
		3)	Middle	
2	**Minimize Attack Surface**			
2.1		1)	High	
		2)	High	
		3)	Middle	
2.2		1)	High	
		2)	High	
		3)	Low	
2.3		1)	High	
		2)	High	
		3)	Middle	
3	**Identification and Authentication**			
3.1		1)	Middle	
		2)	Middle	
		3)		
3.2		1)	Middle	
		2)	Middle	
		3)		
3.3		1)	Middle	
		2)	Middle	
		3)		
4	**Use Control**			
4.1		1)	High	
		2)	High	

4 Network To-Be

4.1 Network Segmentation

The network is redesigned based on the results of risk assessment and recommendations for risk mitigation. The diagrams are created in accordance with best practice reference models and cybersecurity standards.

- The Purdue Model, IEC 62264-1
- Zones and Conduits approach, IEC 62443-3-2

4.1.1 Trusted zones

- .
- .
- .

4.1.2 Untrusted zones

- .
- .
- .

4.2 Multi-layered Defense

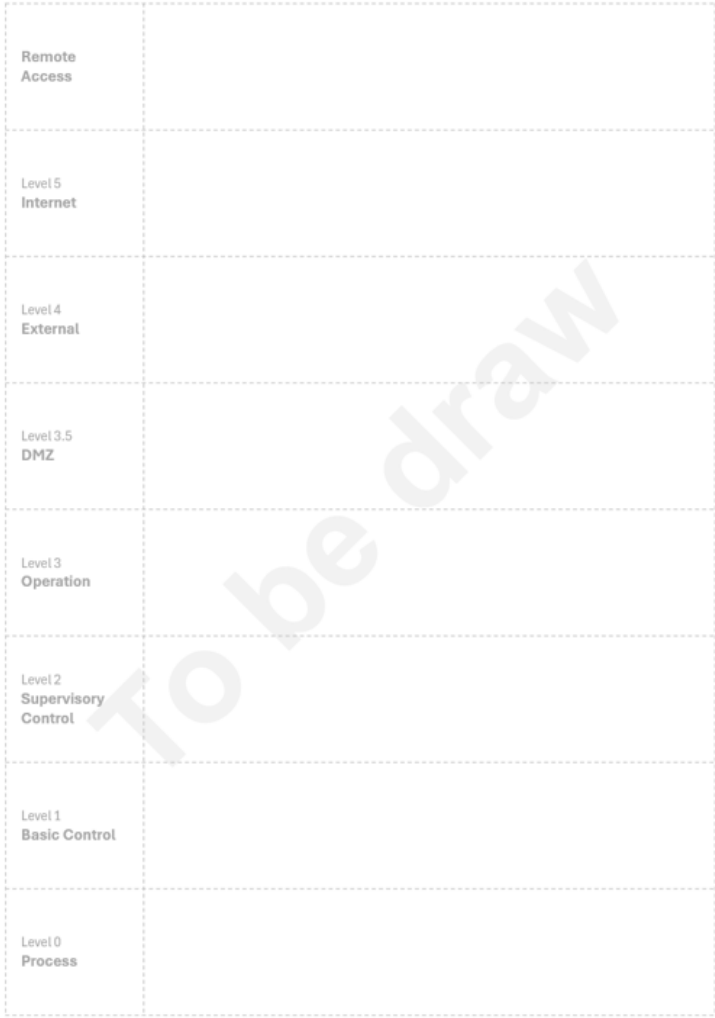
The trusted zones are further protected by **multi-layered defense**:

- .
- .
- .

OSI Layer	Protect	Monitor & detect

4.3 Network Design Diagram

4.3.1 Design Option A



4.3.3 Comparison Between Options

Option A	Option B

4.4 Firewall Rule Guides

4.4.1 Regular Rules Between Security Zones

- .
- .
- .

4.4.2 Temporary Rules Based on Circumstances

- .
- .
-

4.4.3 Rules for Secure Remote Access

- .
- .
- .

4.5 VLAN Setting Guides

- .
- .
- .

4.6 NAT Setting Guides

- .
- .
- .
-

4.7 Products and Features

5 Next Step

6 Revision

Version	Date	Change History	Author/Editor

Summary

- Review your IoT solution in 3 levels: component, system, supplier; a cybersecurity certificate should come from an accredited body
- IEC62443-1-6 zero trust approach is not a replacement, but an enhancement, to the existing IEC62443 reference model
- Design your IoT-enabled system/machine with built-in zero trust concept and future-proof components
- Network and cybersecurity service

Thank you

PHOENIX CONTACT
INSPIRING INNOVATIONS