Before we begin

Administrative matters…

— For the optimal webinar experience, please use headphones and close all other applications that could interfere with the webinar.

— Please keep your microphone muted throughout the whole presentation to avoid interruption of the webinar.

— However, questions can be asked throughout this presentation using the chat functionality: domain experts are following up on questions that might pop up in the chat during the presentation.

— At the end of the presentation a short Q&A is foreseen to address a selection of your questions to the speakers and/or experts in the live chat.

— Speakers participating in this webinar comply with the COVID-19 measures, respecting the social distancing rules. The presentation desk is disinfected each time a new speaker is participating.

KPMG

Cybersecurity with an IT-OT Convergence

June 2nd, 2020

Content

KPMG

Quick Operational Technology Overview

Operational Technology

OT

=

Technologies that focus on industrial processes

KPMG

The evolution of OT

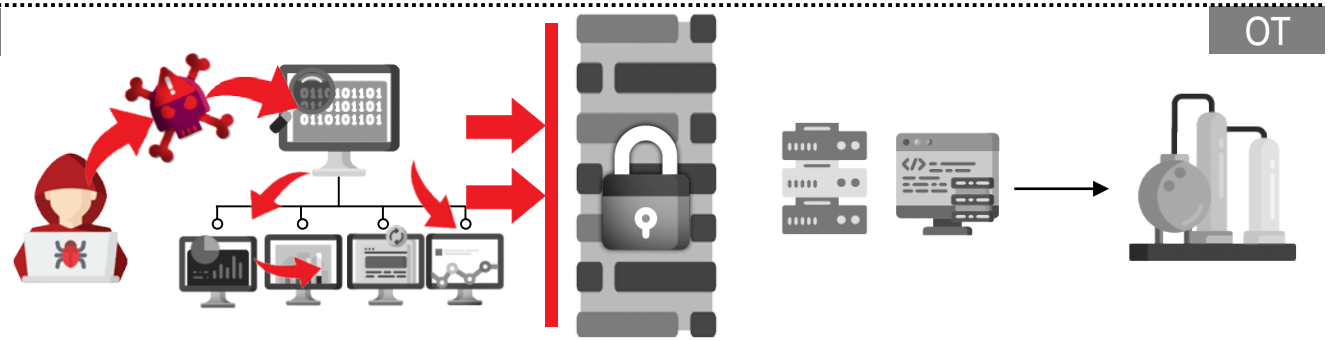
Evolution of Operational Technology

IT

OT

Stand-Alone

In the past there were no requirements to have the IT and the OT environments connected; therefore, were completely separated (Air Gap) and independently governed by IT and Engineering.

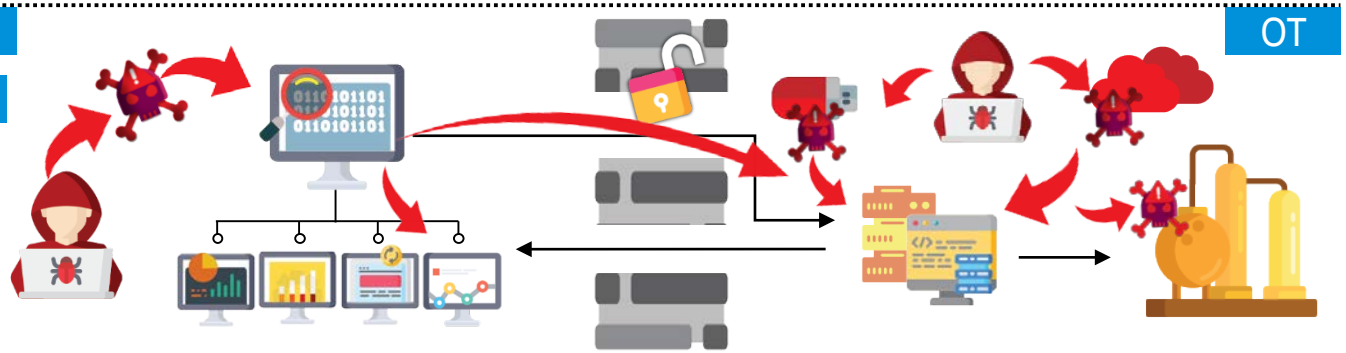


IT

OT

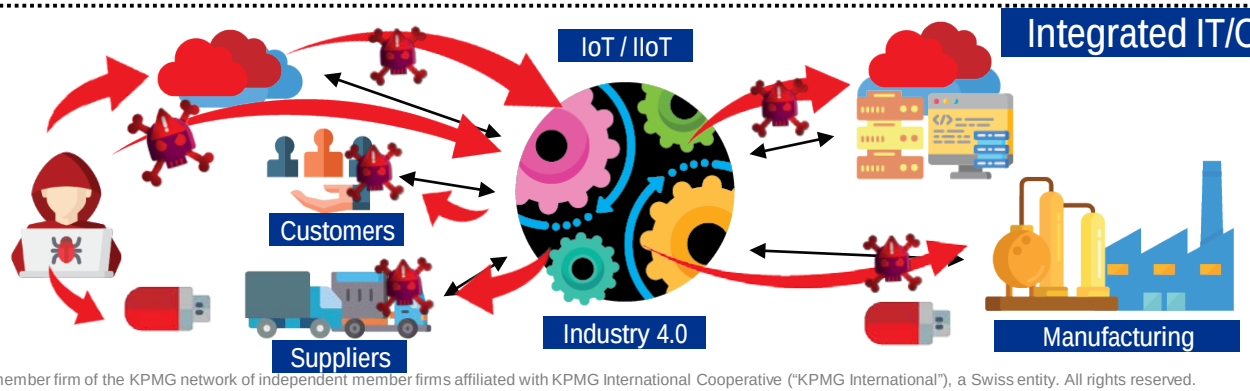
Loosely Connected

Nowadays, due to efficiency and costs, advanced network connectivity between IT and OT is required. This brings confusion with regards to governance, risk management and control implementation effectiveness between IT and Engineering.



Highly Connected

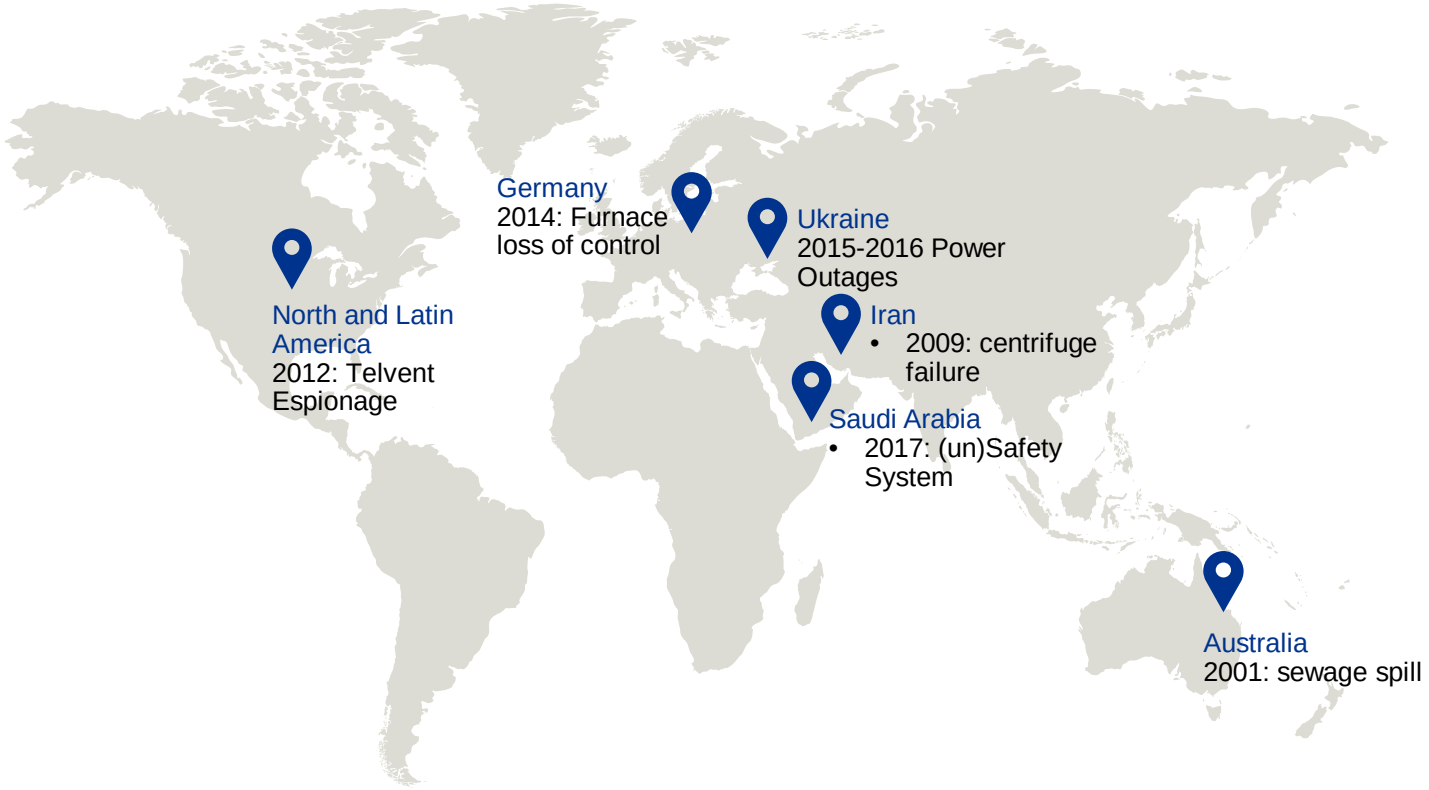
Tomorrow the intercommunication of all components – from the supplier to the customer – will be reality. Therefore, sustainable governance, risk management and control implementation effectiveness between IT and Engineering MUST be established.



KPMG

Why do we need to secure OT?

Why is this important?



Discovering vulnerable OT systems is becoming more and more easy thanks to search engine like **Shodan Safari** – the search engine for any internet connected service/device, including **Internet of Things (IoT), Power plants, building cameras, …**

EU Commission is attempting to increase the overall EU cybersecurity level with the Network and Information Systems (NIS) directive. It defines **requirements** around **incident response** and **technical security measures** based on **potential risks**.

However OT infrastructure is suffering from a paradox

KPMG

The OT paradox

What is the OT paradox?

If we look at the risks of IT and OT, the impact of OT incidents is significantly higher than that of IT incidents.

The OT paradox is that companies are investing a lot of money in securing their IT systems whereas it's actually their OT systems that are key to their survival.

From a business perspective, OT is carrying the most critical business processes. So focus should be more on OT security than IT.

Simple example:

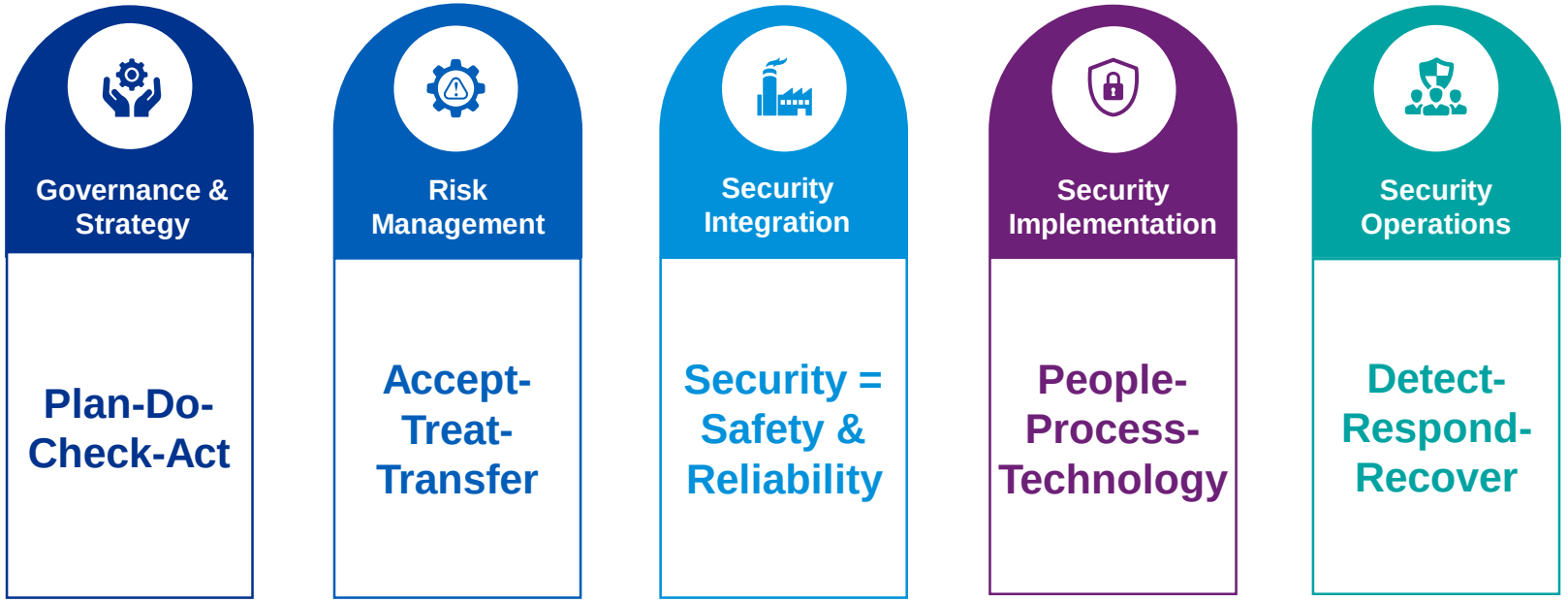
- IT: mailbox downtime is **tolerable**
- OT: production process downtime is **lethal** (24/7/365 uptime required)

KPMG

How do I secure this?

5 Pillars of OT Cyber Security

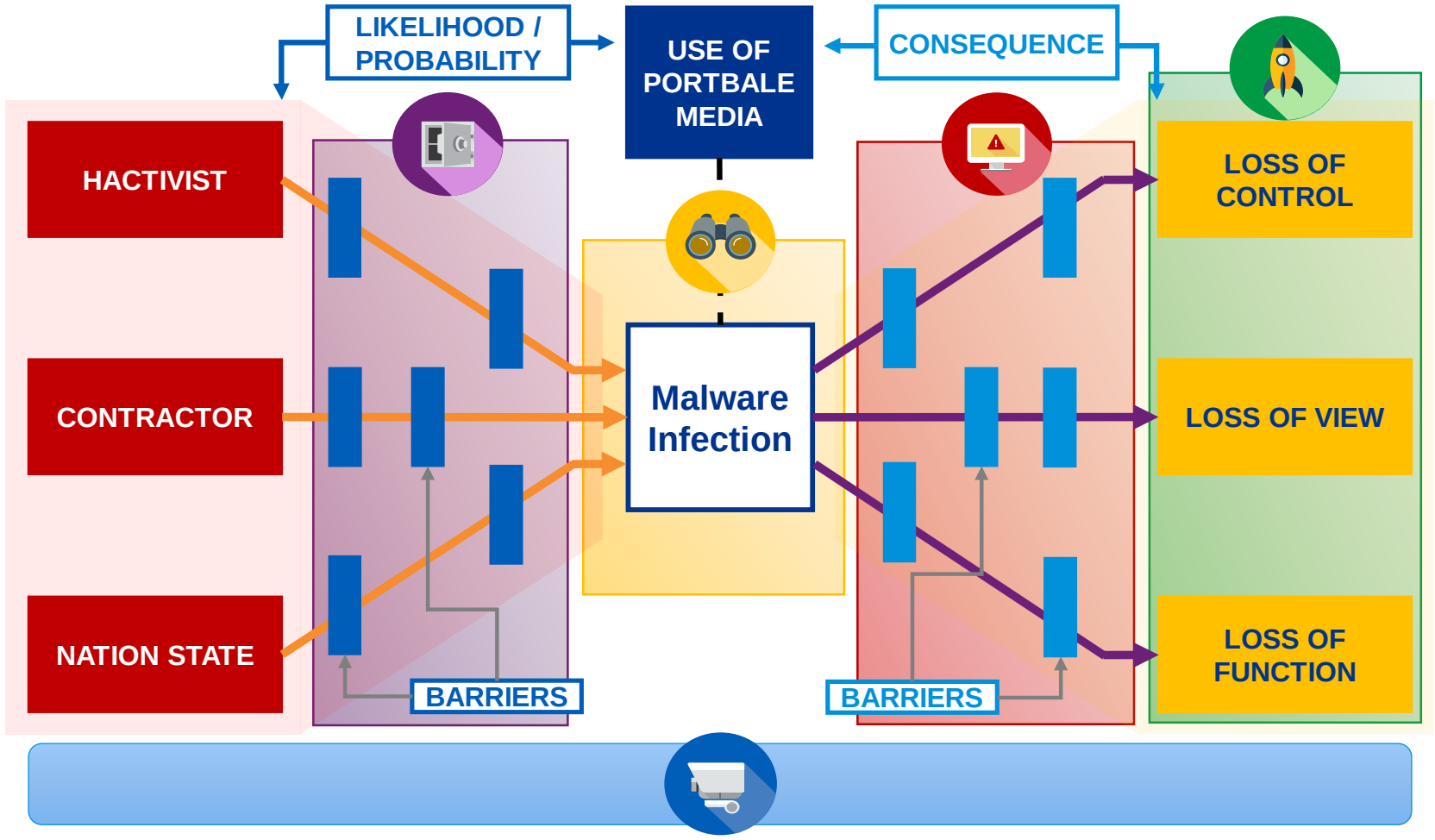
Outlined below are the five pillars of effective safeguarding against cyber threats for OT and IIoT environments.



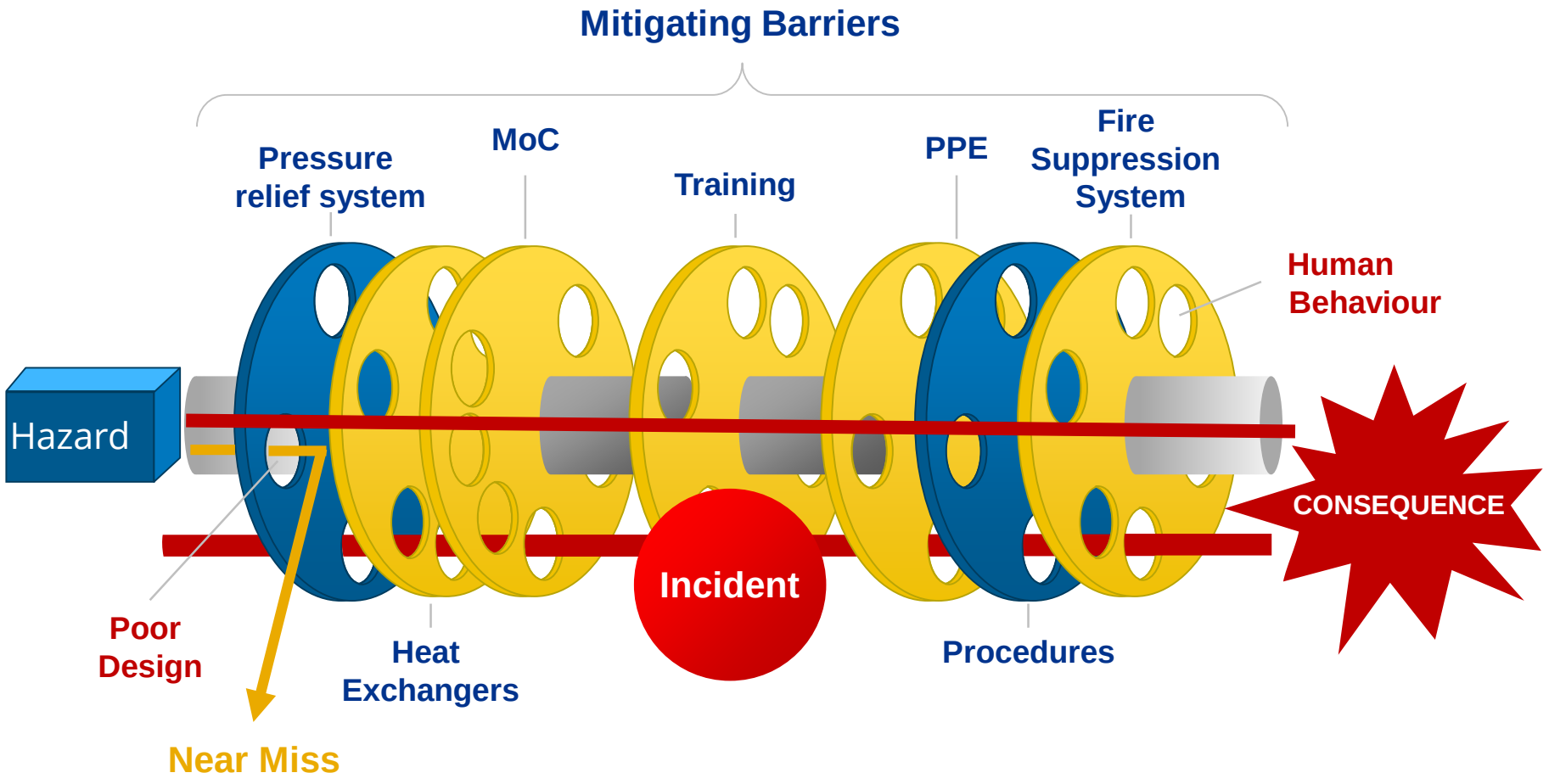
KPMG

Risk Management

The Safety Bow-Tie Model & Cyber



HSE Swiss Cheese Model



Understanding the key differences

	Classic IT Security	Classic OT Security
Priorities/Focus		
Consequences	• Loss of (sensitive) date.	• Loss of human life. • Loss of functionality of the industrial plant.
Impact	• Financial • Reputational	• Environmental • Safety

KPMG

Control Design & Implementation

KPMG ICS Security Framework

Governance

- SCADA/DCS security framework and assessments
- SCADA/DCS security policies, procedures and guidelines
- Risk management
- SCADA/DCS criticality analysis

People

- Security awareness
- Education on cyber security in SCADA/DCS
- Commitment, integrity and adherence to client's SCADA/DCS security standards

Process

- Change management
- Patch and software version management
- Physical security and situational awareness
- Security monitoring
- Asset management
- User management
- Third party/vendor (contractor management)
- (Security) incident management
- Cyber defence
- Vulnerability management
- Threat management

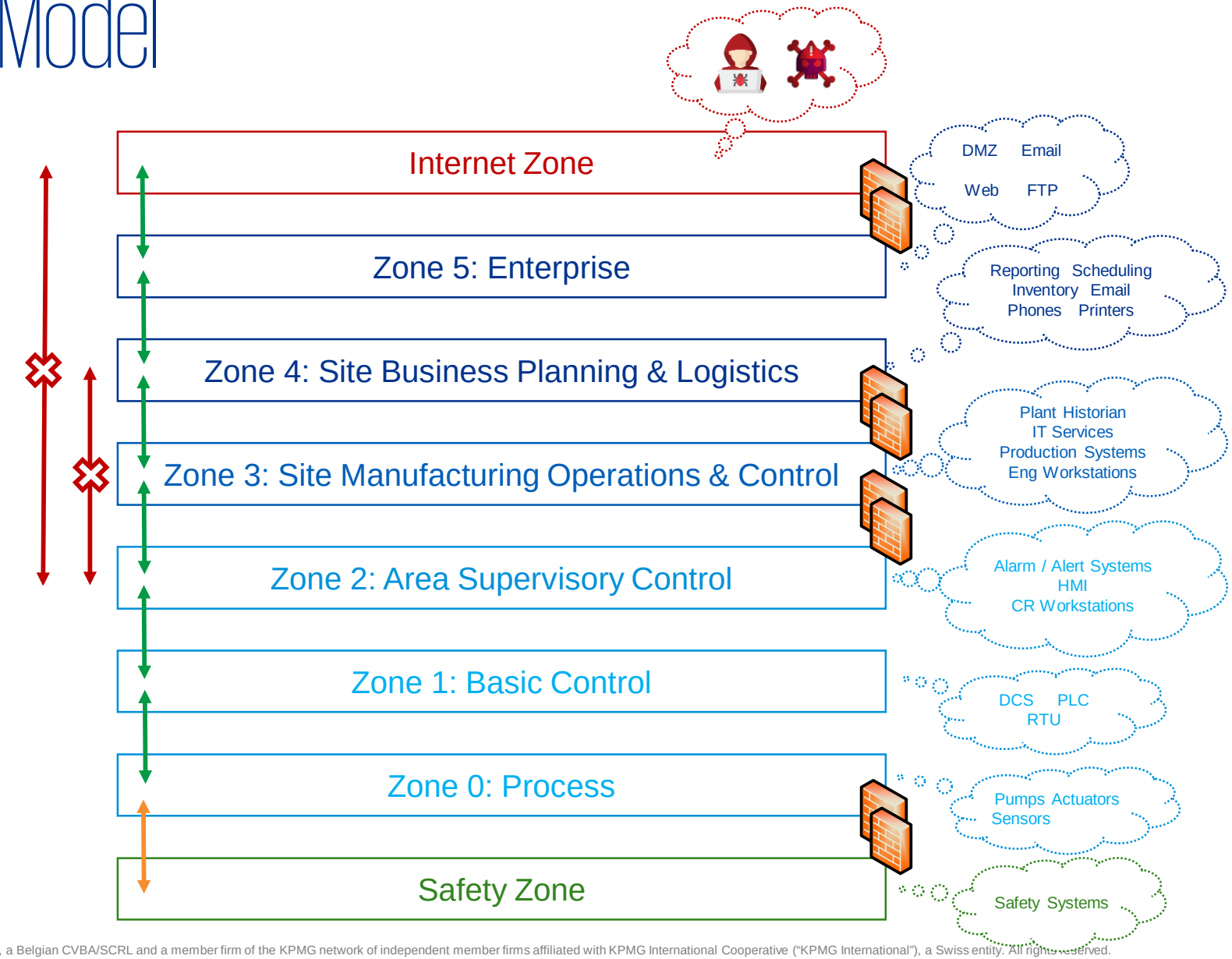
Technology

- System hardening and protection
- Anti-virus and malware protection
- System failsafe and resilience
- Logical access controls
- Secure failsafe infrastructure and administration
- Secure remote and third party access

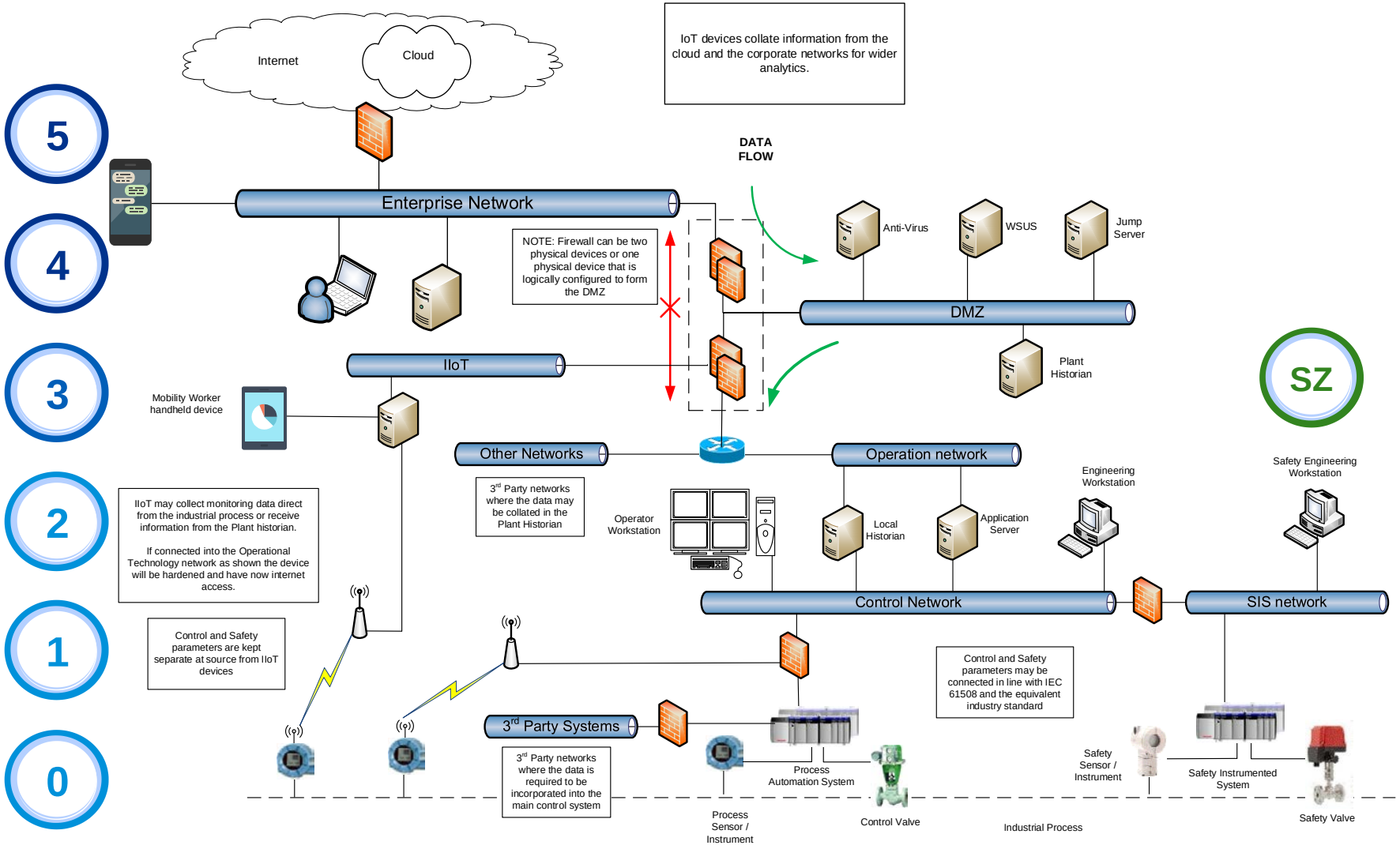
KPMG

OT Specifics

The Purdue Model



What does this actually look like?



KPMG

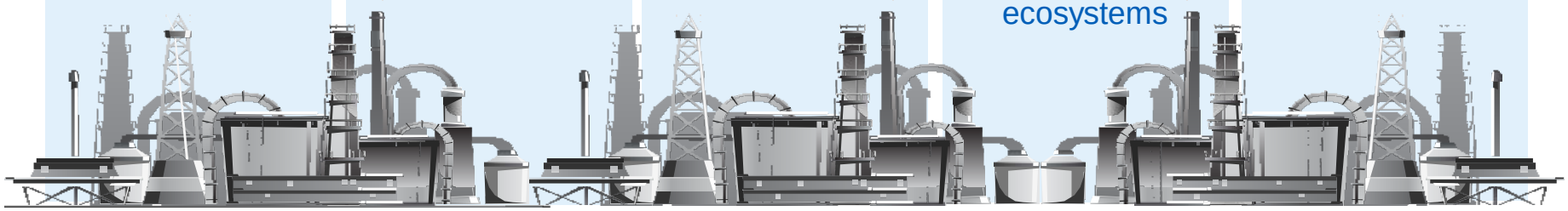
Industry insights

Five Cyber Security Myths of OT

1. The risks OT systems face are exactly the same as for IT systems.
2. A single or common cyber security strategy is impossible to develop and implement for OT and IT.
3. A single team reporting to one Executive should be responsible for OT, IT and IIoT cyber security
4. OT cyber security programmes are ‘just another’ IT cyber security programme
5. OT vendors and suppliers will ensure cyber security needs are met every time.

IT/OT Convergence – Top 10 Challenges

1	2	3	4	5
Not having a cyber security strategy	Lack of ownership / governance to manage cyber risks	Lack of Secure-By-Design in products and ecosystems	Not having cyber security skills and general cyber awareness for employees and ecosystems	Insufficient OT cyber security and privacy resources



6	7	8	9	10
Lack of security event identification monitoring	Insufficient operational cyber hygiene practices	Insufficient asset inventory and systems life cycle management	Lack of vulnerability identification and management	Lack of effective incident response processes

KPMG

Q&A


KPMG
Thank you

One more thing

1 Ways of Working	Does remote work become the new normal and in office / business travel become the exception? (work / life balance)
2 Labor Force	Will displaced jobs come back or will automation accelerate? What about labour shortage? New bottleneck professions?
3 Change in customer behaviour	Is this the tipping point for the dominance of the digital economy over the physical economy? Will consumer behavior change permanently?
4 Supply Chain and Manufacturing	Will existing supply chains return to normal or be reconfigured? Localisation?
5 Continuity and Resilience	How will BCP be bolstered to ensure resilience in future crises? How to increase responsiveness of an organization/ be more agile for future shocks?
6 Purpose, ESG	Will Purpose-driven companies take the lead? Will ESG be core to how businesses recover? Can this be done while sustaining desired economic outcomes?
7 Debt Burden of states and companies	Will the large debts weaken the recovery out of the crisis? Could it trigger a financial crisis? Will it increase inequality between competitors and trigger distressed M&A?
8 Globalization	Will countries increasingly look inwards for prosperity? Will regional and national borders be strengthened?