TÜV Rhienland Cybersecurity Trends 2020

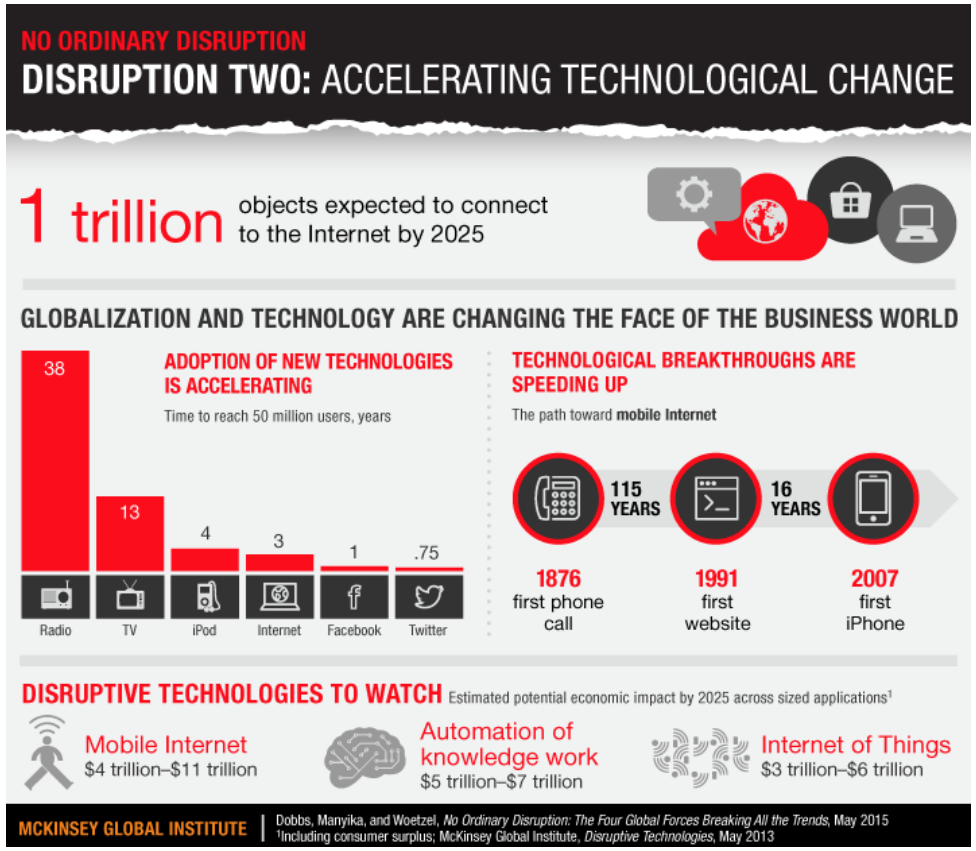
And the case for real-time cyber risk management in operational technology

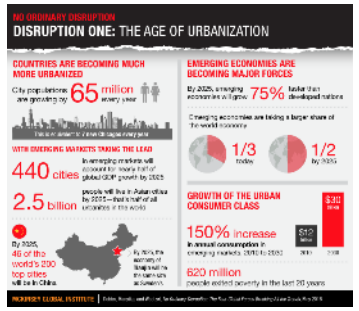
Cybersecurity in Aluminium Workshop
February 27th, 2020

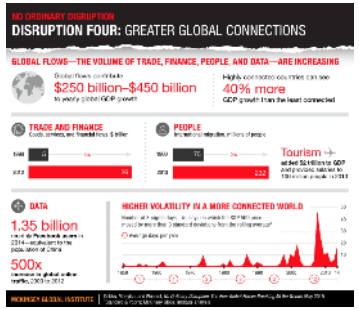
2MC
A TÜV Rheinland Company

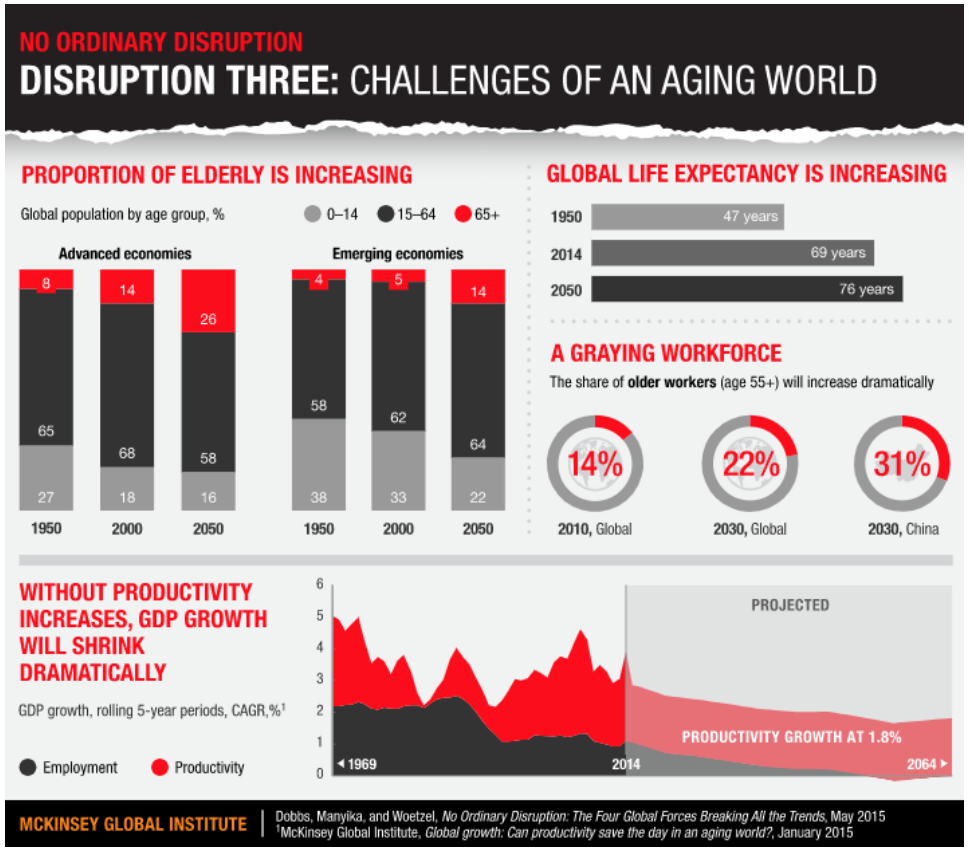
McKinsey Global Institute predicts the global workforce will peak by 2030

This colossal economic pressure demands the adoption of automation through digitalisation to accelerate







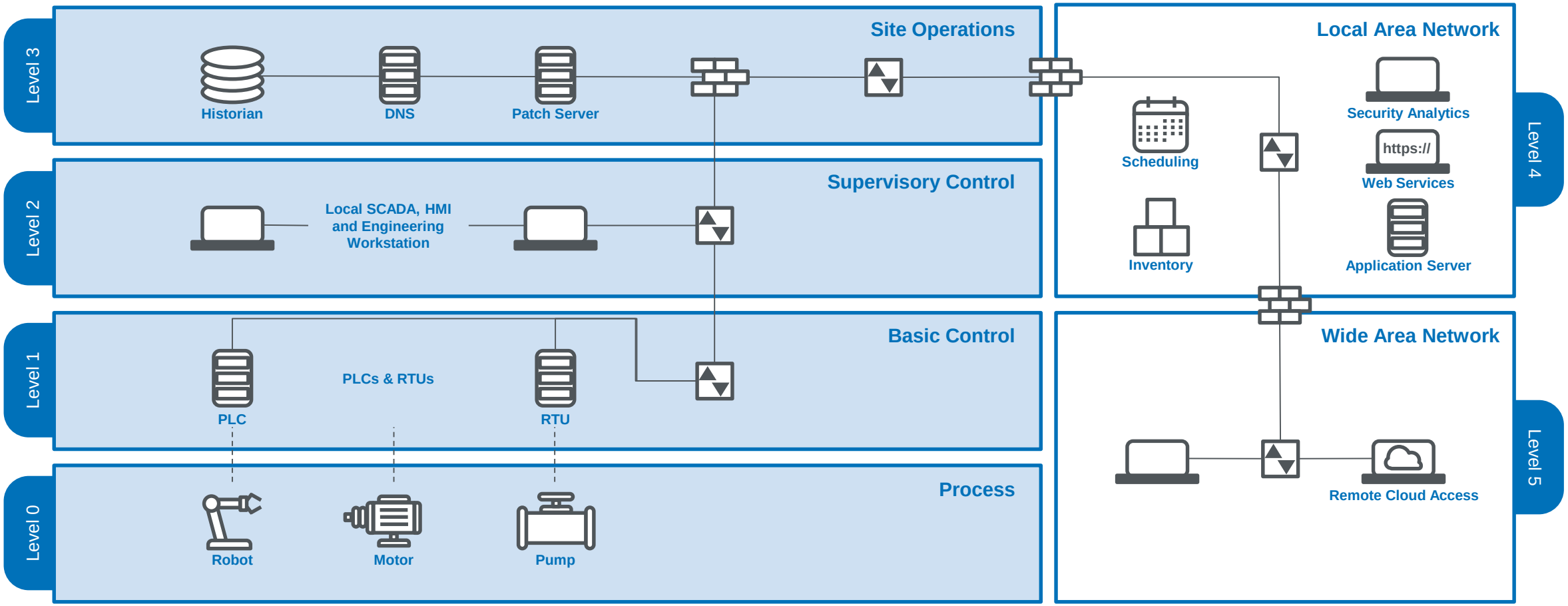


! All of us in this room are tasked with delivering growth

2MC A TÜV Rheinland Company

IT/OT convergence leaves physical processes vulnerable to cyber attack

OT Cyber Risk affects the HW/SW dedicated to detecting or causing changes in physical processes (e.g. Valves, Pumps)



2MC A TÜV Rheinland Company

Our Cybersecurity Trends for 2020 looked at some of the implications

Looking at cybercrime and our physical safety, potential impacts on society and risks to the environment

1

The unregulated mining of personal data risks destabilising digital society

- Judith Duportail asked a dating company for her personal data
- She received an 800-page document incl. FB likes, rankings, and every online conversation she'd had with all 870 matches since 2013

2

Smart supply chains will be targeted by hackers, rendering them 'dumb'

- Supply chains increasingly use IoT automation, robotics, and big data management to lower costs
- Although the smart supply chain is dynamic and efficient, it is also fragile

3

Smart consumer devices are multiplying faster than they can be secured

- Every year, the number and capability of the smart things in our live expands exponentially
- The commercial pressure on product development costs and lifecycles, continues to prioritise features over security

4

Threats to the shipping industry have moved from theory to reality

- Seaborne trade continues to grow as time in port shortens
- There is ample evidence that nation states are experimenting with direct attacks on navigation systems, while ransomware attacks are now being reported

2MC A TÜV Rheinland Company

Our Cybersecurity Trends for 2020 looked at some of the implications

Looking at cybercrime and our physical safety, potential impacts on society and risks to the environment

5 Realtime operating systems superflaws risk creating a post-patching era

- Every IoT device has its own software stack, many of which use outsourced and potentially vulnerable components
- Patching, if available, becomes less effective in older, orphaned components that remain in use

6 ‘Bring your own medical device’ is an internet health crisis in the making

- Over the past decade, personal medical devices have been connected to the Internet
- Researchers discovering a growing number of software vulnerabilities
- The complex task of maintaining devices is revealed to be uncoordinated, weak or non-existent

7 Vehicles and transport infrastructure are a new candidate for cyber-attack

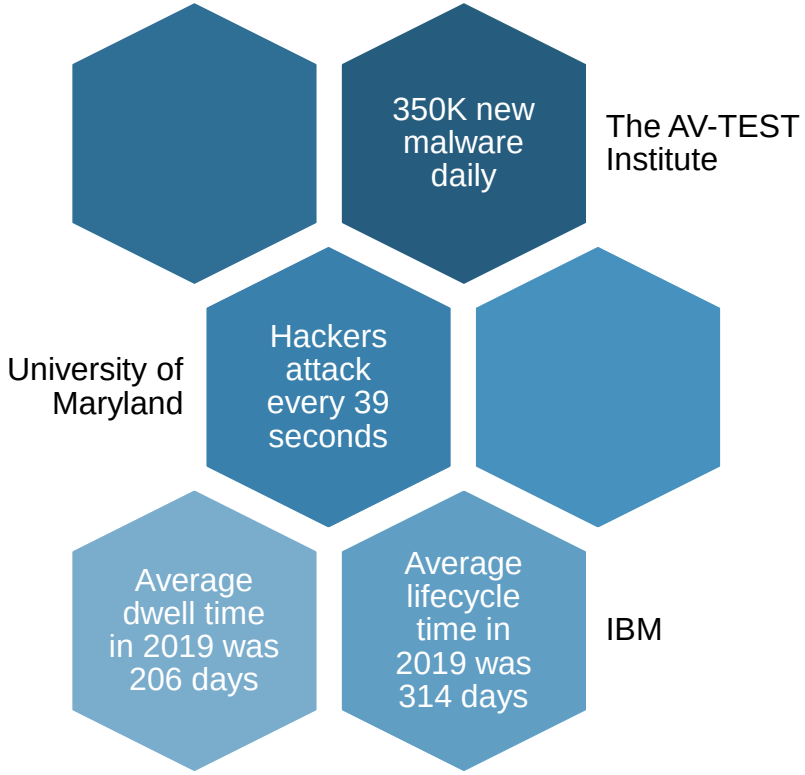
- Vehicles and traffic infrastructure are becoming increasingly integrated
- The downside is the rise in vulnerabilities that might be exploited
- A large-scale attack could have disruptive impact for transportation and safety in the urban evironment

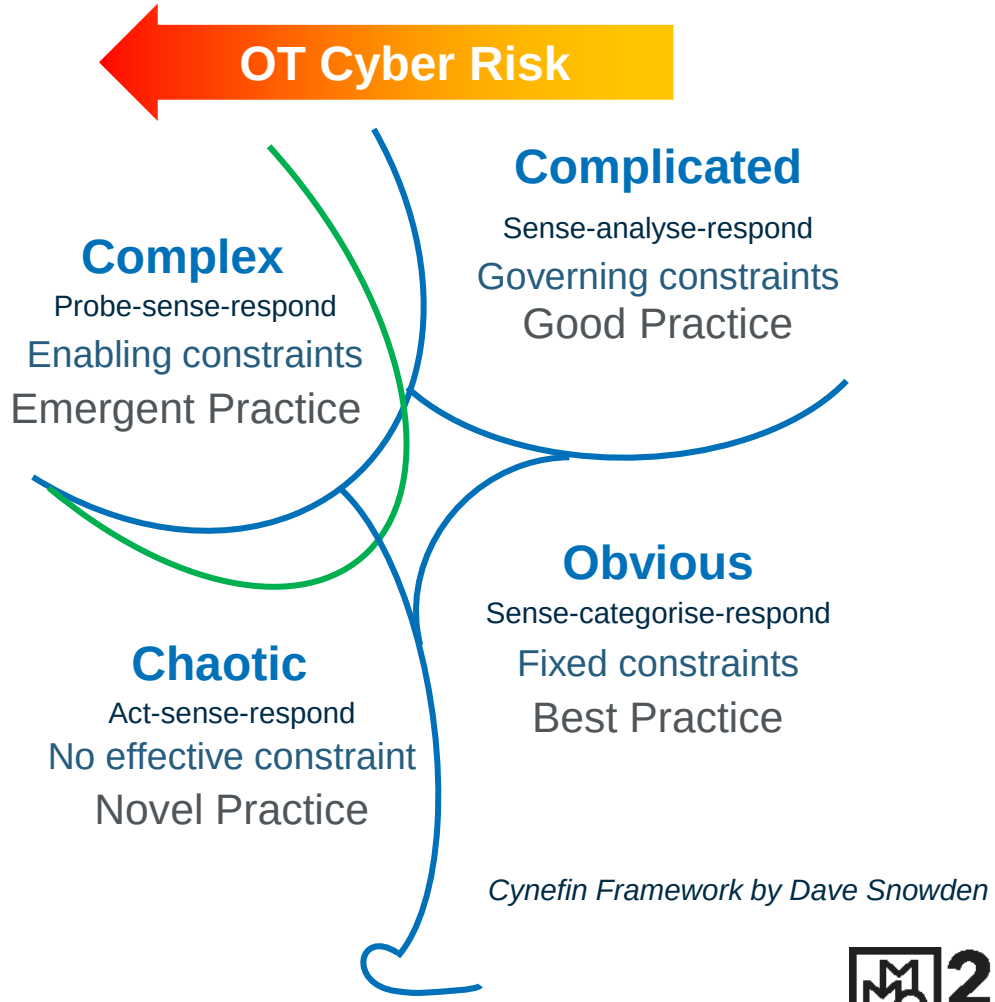
https://www.tuv.com/landingpage/en/cybersecurity-trends/

2MC A TÜV Rheinland Company

Digitalisation is driving a transition from Complicated to Complex risk

Digital complexity, combined with volume and sophistication attacks, demands new emergent practices

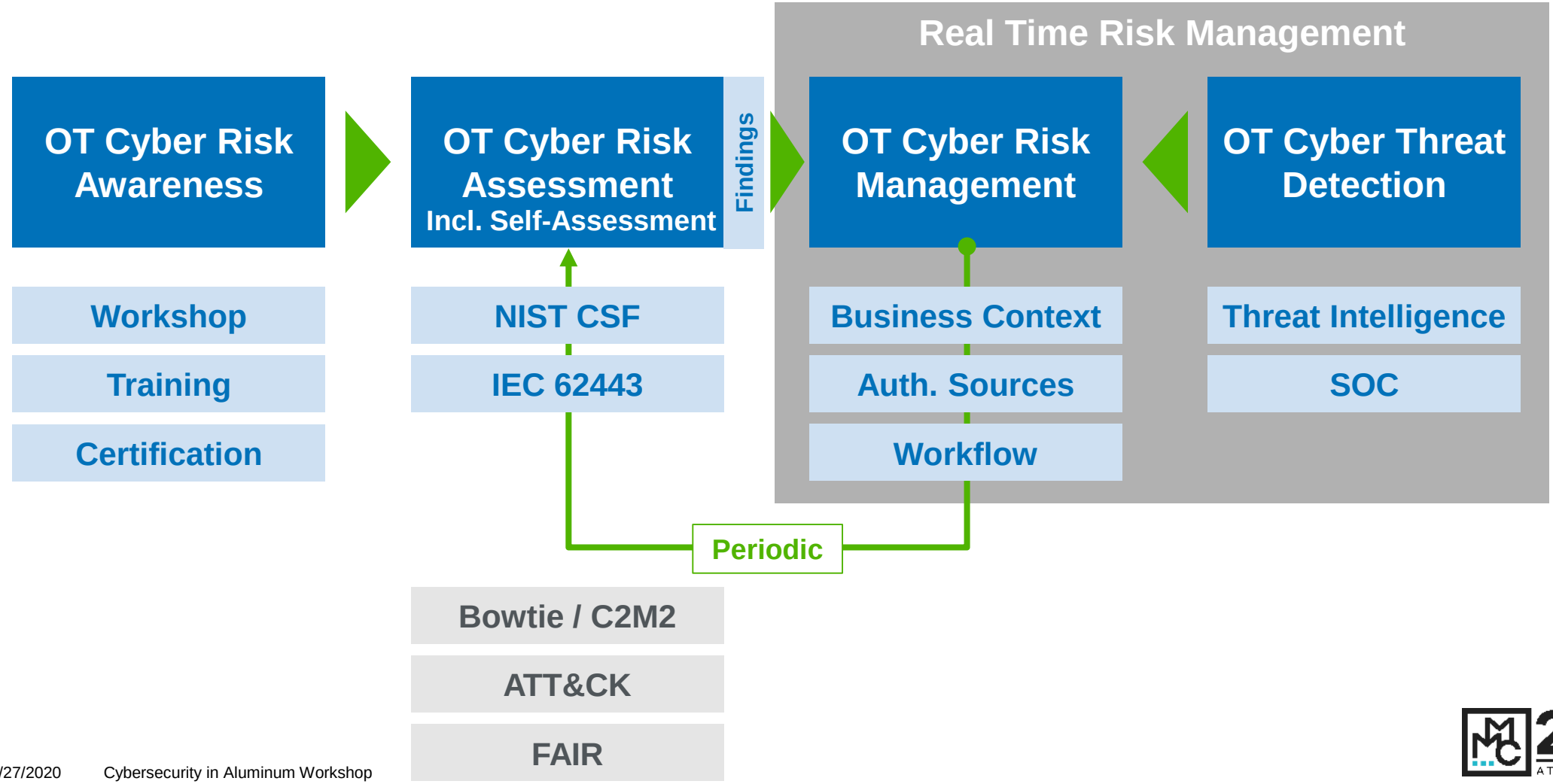




Cynefin Framework by Dave Snowden

Has the risk of cyberattack disrupting operations changed?

It's a simple operations and safety critical question that traditional risk management approaches can't answer



2MC A TÜV Rheinland Company

Industrial Security in 2019: A TUV Rheinland Perspective

We surveyed 370 industrial organisations, predominantly manufacturing, to test likely preparedness

FIGURE 1
What industry sector are you primarily involved with?

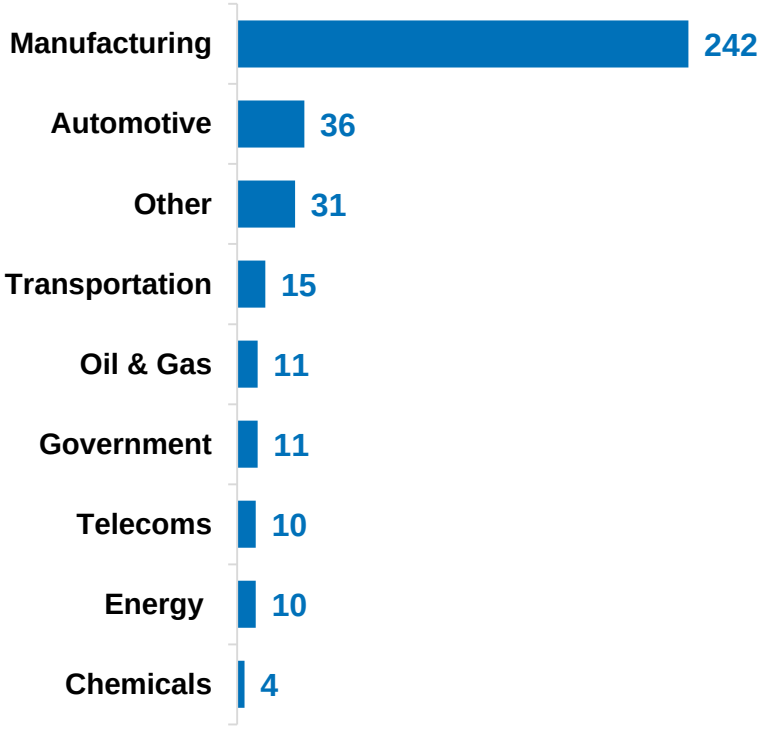


FIGURE 4
Have you ever conducted an OT cyber risk assessment?

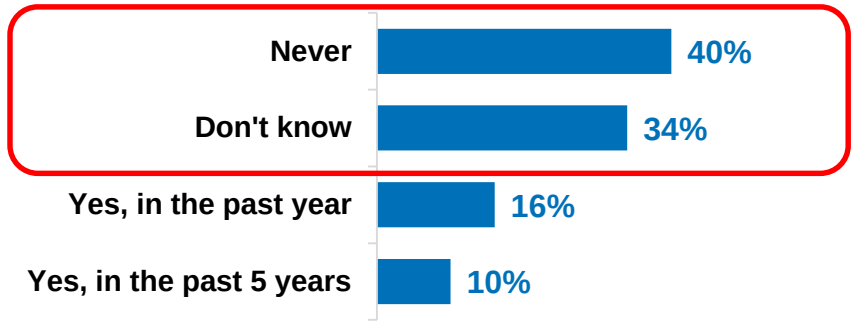


FIGURE 7
Are you able to detect all the endpoints on your OT network?

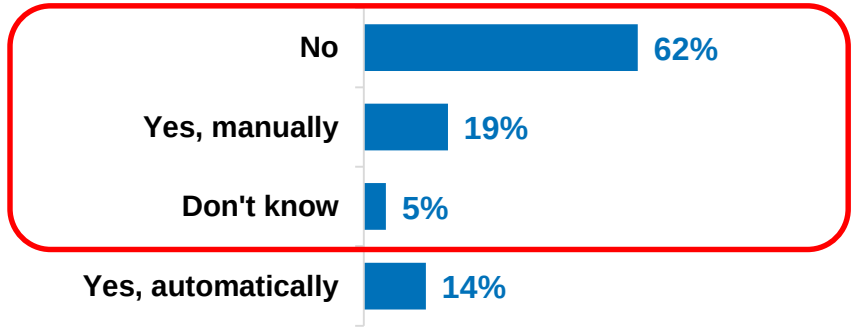
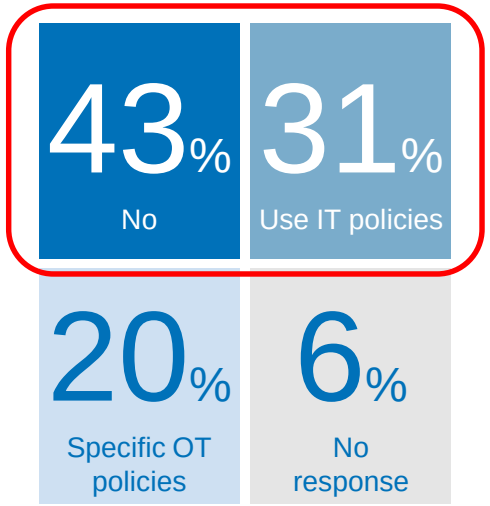


FIGURE 8
Have you implemented OT-related cybersecurity policies and procedures in your business?



2MC A TÜV Rheinland Company

Any questions?

Anthony Dickinson
Chief Revenue Officer, TUV Rheinland 2MC

Email: adickinson@2mc.co

Phone: 07824 306 739

www.2mc.co

TÜVRheinland®
Precisely Right.