

Railway Industry: People training and Cybersecurity

4th ERA-ENISA Conference on Cybersecurity in
Railways

Lucia Capogna - 3rd October 2024

SYSTRA



SYSTRA: A global leader for transportation solutions

SYSTRA is one of the world's leading engineering and consulting groups specialising in public transport and mobility solutions



**+65
YEARS**



A turnover of
€1.071Bn



76% of turnover
achieved abroad



Orders of
€1.3 Bn



An operational
presence in
80 countries



SYSTRA has
contributed to **1 in 2**
High-Speed lines in the
world (>250 kph,
outside China)



SYSTRA has designed
1 Metro network in
service out of **2**
in the world

Figures as at end of 2023

About me

Lucia Capogna

Cyber Security and Software Assurance Team Leader

- Computer Science Engineer (BSc) and Systems Engineer (MSc) with over 17 years of experience in Software, Cyber Security, Requirements Management and Verification & Validation across various industries:
 - Cyber Security Technical Expert
 - Software and Software Assurance Technical Expert
 - Independent Lead Assessor
- Member of several CENELEC (Safety – EN 50129, Cybersecurity - TS 50701 & Software – EN 50716) and IEC Standardisation Groups (Cybersecurity – IEC 63452)
- School of Engineering, University of Birmingham:
 - Industrial Advisory Board member
 - Royal Academy of Engineering Visiting Professor in OT Cybersecurity
- STEM Ambassador & Woman in Rail (WiR) East Midlands committee member



Digitalisation – Stating the obvious

Digitalisation has been introduced exponentially in the railway solutions



New technologies and digitalisation provide a railway that is:

- more flexible,
- inter-connected,
- easier to enhance/customise,
- more advanced,
- more responsive to sub-system failures.



The digital evolution introduces new and diverse risks that evolve over time: Cybersecurity risks.

Do we have the right skills and competencies to manage and prevent these risks and/or recover from cyber incidents?

Skill Shortage

S04: Cutting-edge competencies and capabilities in cybersecurity across the Union



[Link](#)



[Link](#)

TOP 10 EMERGING CYBER-SECURITY THREATS FOR 2030



Cybersecurity experts

Is it sufficient to have just more cybersecurity experts?

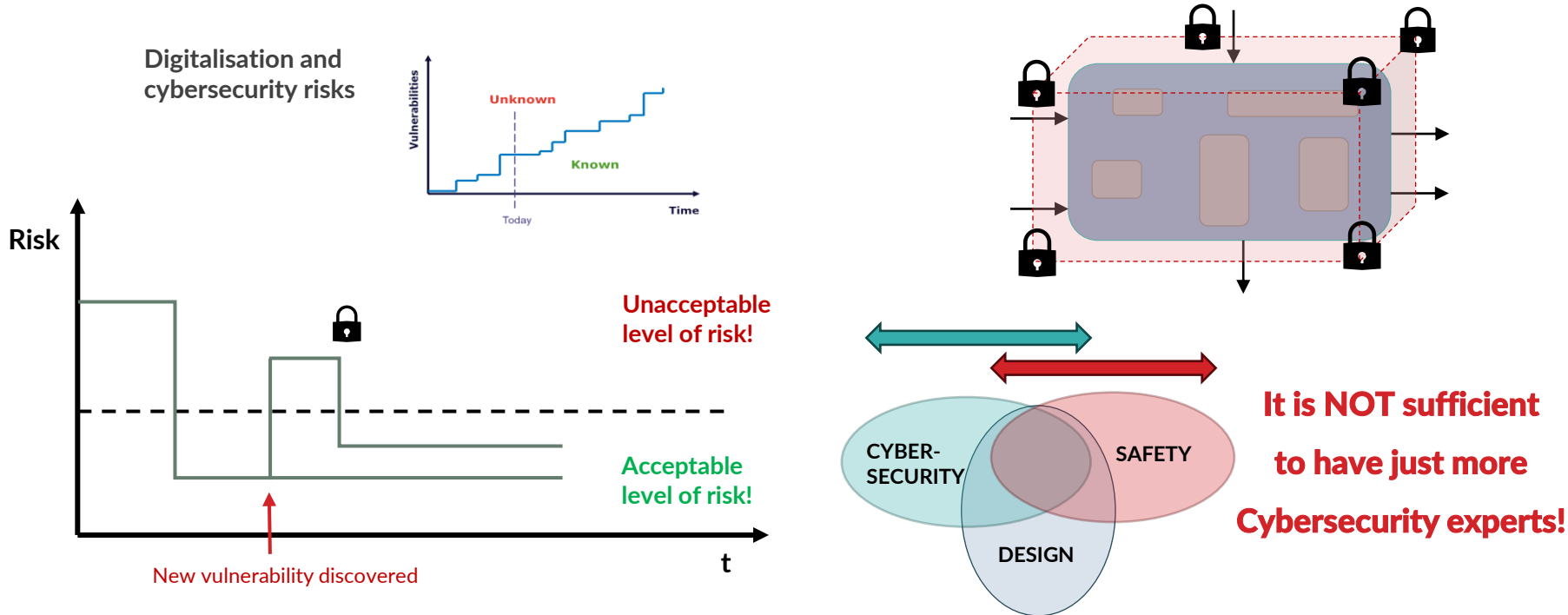
Table 1. New prioritisation of threats

	THREAT	IMPACT * LIKELIHOOD	IMPACT	LIKELIHOOD
1.	Supply Chain Compromise of Software Dependencies	17,71	4,21	4,21
2.	Skill Shortage	17,20	4,10	4,20
3.	Human Error and Exploited Legacy Systems within Cyber-Physical Ecosystems	16,69	3,96	4,22
.....				

Defining the problem

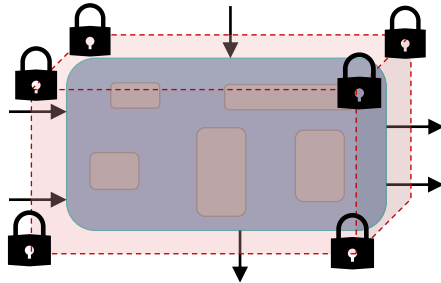
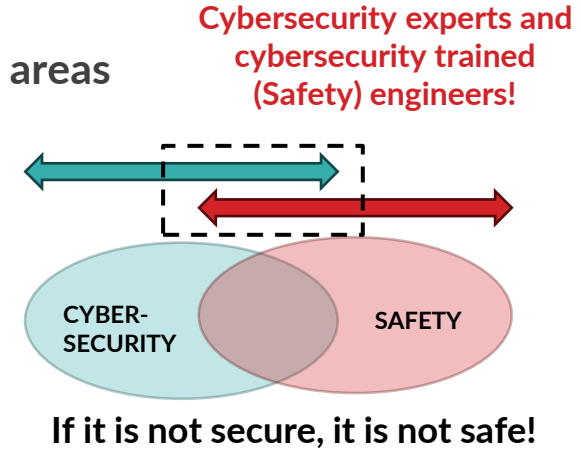
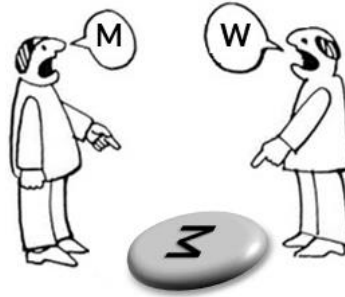
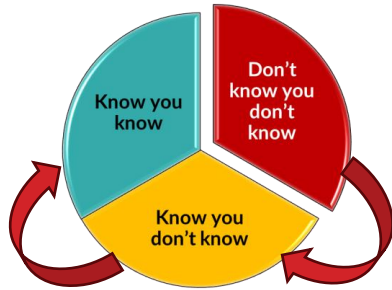
Rail systems are designed and built to achieve specific objectives/targets for Safety, Reliability, Availability and Functionality.

Fact: In most cases, cybersecurity is addressed separately from system design and engineering.



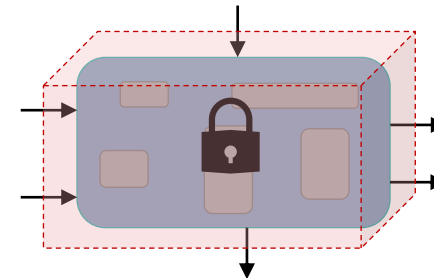
Goal – Increase resilience

Improve cybersecurity understanding of people working in critical areas

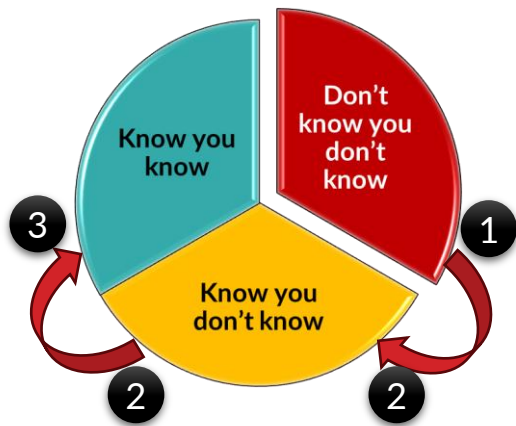


- Needs additional/external security technology
- More costly
- Less effective

- Reduces cybersecurity (and safety) risks
- Reduce costs
- Increases efficiency and effectiveness



How: Step by Step



**Keep testing you
still know**

1

Provide awareness across the industry and target people in critical areas

Safety

Assurance

Incident
Investigation

Design

Approval

...

2

Embed Operational Technology (OT) cybersecurity into formal education and training (focused and oriented – a learning journey)

- Domain specific
- Linked to role and responsibility / ambitions
- Use terminology and examples specific to the role
- Teach what is needed only
- Use scenarios that are critical and relevant
- Highlight the importance of cybersecurity from concept phase

3

Collaborate, contribute and coordinate with “Body of Knowledge”

- Cybersecurity BoKs
- Individual discipline BoKs incorporating cybersecurity

Conclusion

- Digitalisation and new technologies demand more knowledge in cybersecurity to keep systems safe, reliable, available, etc.. → **To make system more resilient.**
- The Railway Industry needs **professionals working in critical areas to be cybersecurity trained**
- Collaboration with cybersecurity experts is crucial from concept phase:
 - know you don't know and
 - know you know
- Training and teaching techniques must be specific and relevant to the role to be effective
- Initiatives to improve understanding and knowledge in critical areas are already ongoing:
 - Formal education is embedding OT cybersecurity in the engineering programs
 - National and international “Body of Knowledge” are more focused on specific needs

OT cybersecurity shall protect safe, reliable and available physical operations.



It is NOT sufficient to have solely more Cybersecurity experts.

SYSTRA

More information:
systra.com/uk
systra.com/ireland



CONFIDENCE MOVES THE WORLD