CyberSafety – An Integrated Approach for Protecting Safety-Critical Railway Systems

Timo Latvala, Huld Oy

huld

About the Presenter

- Timo Latvala, Chief Sales Officer, Huld Oy

- Program Committee Member: SafeComp 2012 – 2020, SafeAI 2019, WAISE 2018 – 2021, …
- Space Systems Finland Oy: Co-owner and entrepreneur, 2011-2019
- Post-Doctoral Research Fellow, University of Illinois at Urbana-Champaign, 2005-2007
- Dr Sc (Tech), Helsinki University of Technology, 2005

huld

Our vision is to be

The Boldest Technology and Design House in the Galaxy.

huld

Beyond tomorrow

Our mission is to

Make The World More Intelligent and Solve The Challenges of Society with Technology and Design, Humanely and Boldly.

What we offer:

- Safety & Security
- Embedded Solutions
- Product Design & Development
- Digital Services & Software

Huld stands for

Humane and Bold

The Challenge

SAFETY & SECURITY DO MEET

- Assessment methods
- Concepts
- Requirements and V&V activities

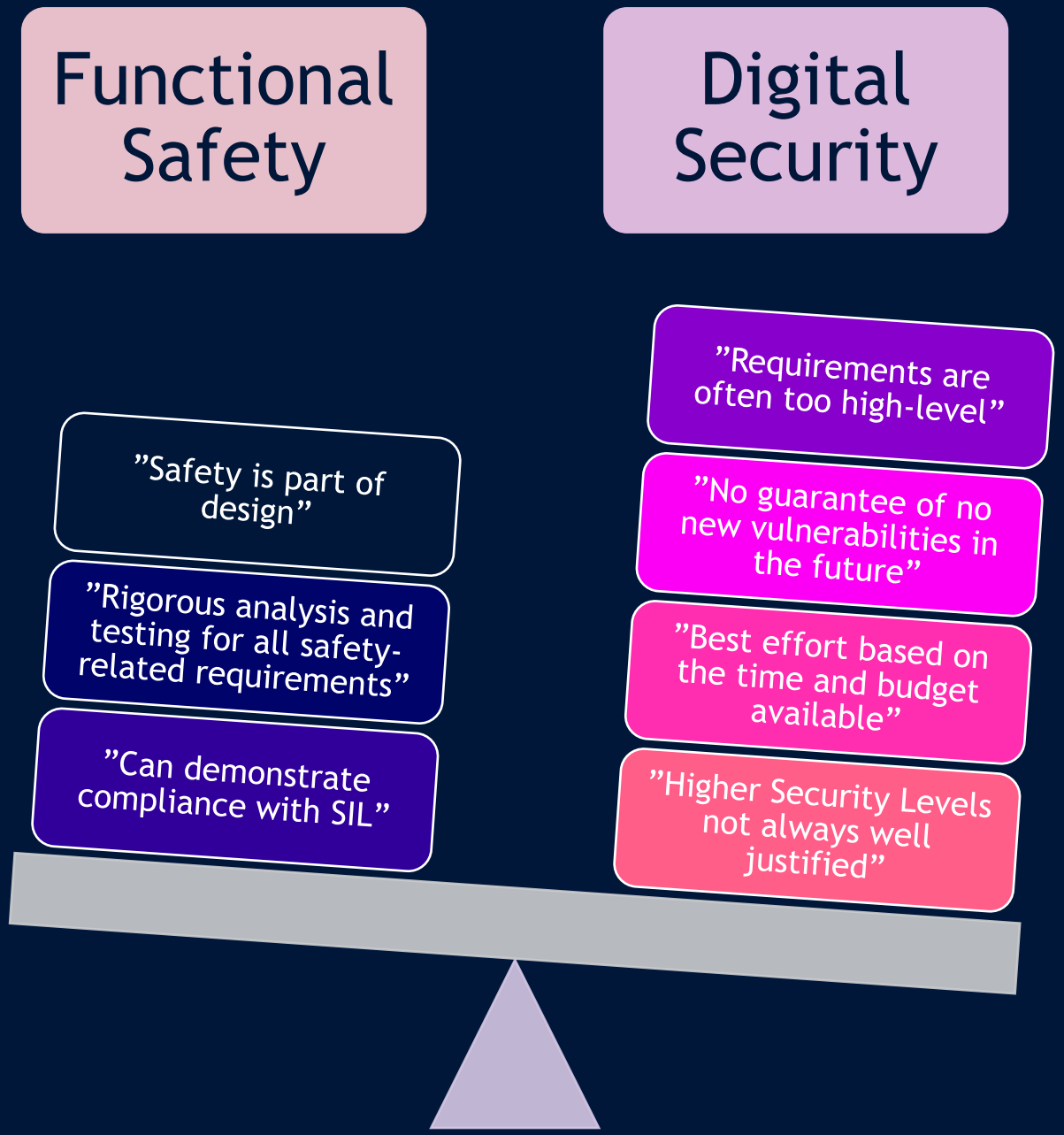
- New safety-critical features such as remote access, remote configuration changes and remote software updates are becoming more common in the railway products
- Railway industry has a strong safety engineering culture, however security has in practice often been seen as an afterthought
- Safety and security are two risk-driven activities, but they are currently tackled mainly as separate topics in most railway projects
- Integrating safety & security issues in railway projects would benefit stakeholders by lowering the actual risk levels and project costs.

The Burden Of Proof

On paper, it’s as simple as following TS 50701 ” Railway applications – CyberSecurity”, however…

- Many companies’ Secure Development Lifecycle frameworks are not fully complatible with Security Levels as prescribed in IEC 62443, or the maximum SL achivable through their SDL is too low for higher-SIL applications
- Many security threats and vulnerabilities are specific to detailed implementation (particualrly for SW), therefore they could be identified late or missed altogether in case security activities are performed separate from the safety design cycle
- More generally, security is often seen as ”best effort using whatever project resources are available”, as opposed to an absolute property. The level of confidence for any staements of compliance for security is not as high as for functional safety.

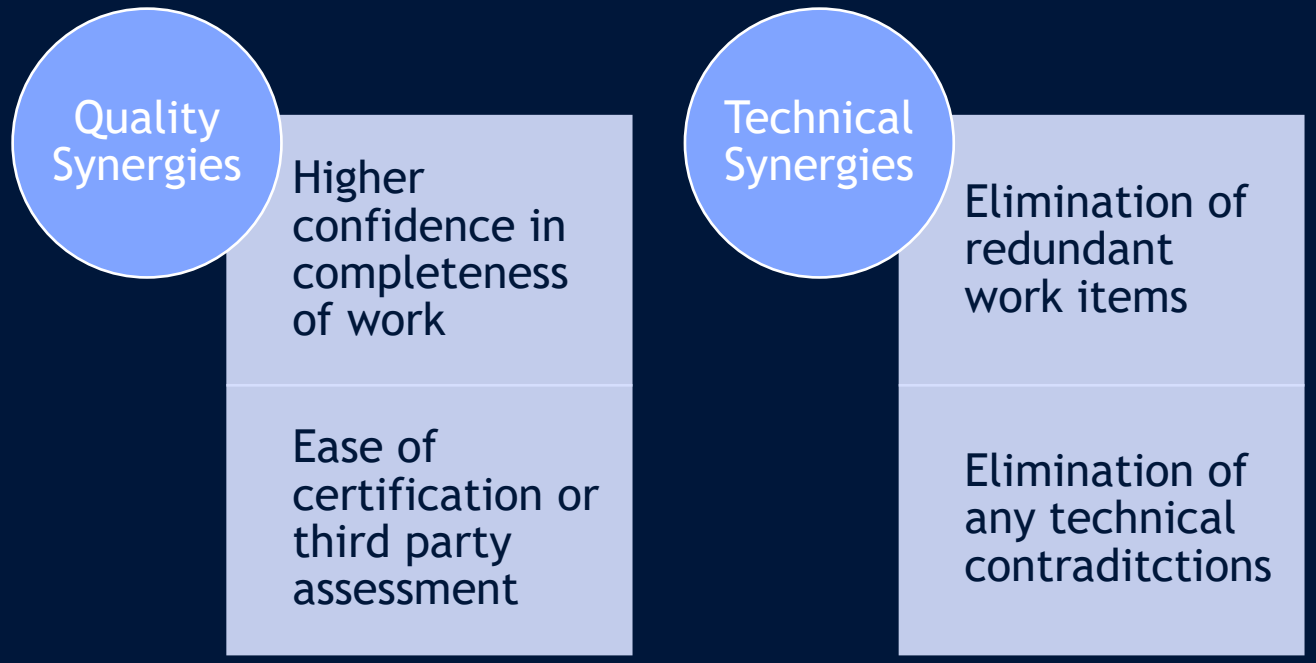
Ask from design teams and safety & security specialists, and you would most likely get these answers:



huld

The CyberSafety Approach

The only way to maximise the synergies between safety and security, and to eliminate any shortfall in rigour of demonstration, is to follow a fully integrated cyber-safety approach.



huld

Cybersafety Key Features and Enablers

Planning

- Joint safety and security plan
- Security activities part of gated reviews
- Safety and security impact assessment of all changes

Requirements Based Engineering

- Security requirements part of systems engineering and V&V
- V&V evidence supporting the safety & security case

Competencies

- Cross-training of personnel
- Safety and security people working side by side, maybe even the same person

Unified Hazard log

- Hazard log includes security threats
- Security threats status is regularly reviewed along the design lifecycle

huld

Beyond tomorrow