SECURITY GOVERNANCE IN RALWAYS:
Bridging the worlds of CCS, Operations & Corporate

S. Appiah

Co-financed by the European Union
Connecting Europe Facility

Content

- ERTMS Users Group (EUG)
- Security Governance
- IACS Cybersecurity
- Challenges
- Framework

EUG Mission

To help the railways in applying ERTMS/ ETCS in a harmonised and interoperable way, to enable the free flow of trains and a competitive railway

The added value of the ERTMS Users Group is to offer a platform for railway peers to share experiences and to consolidate their views.

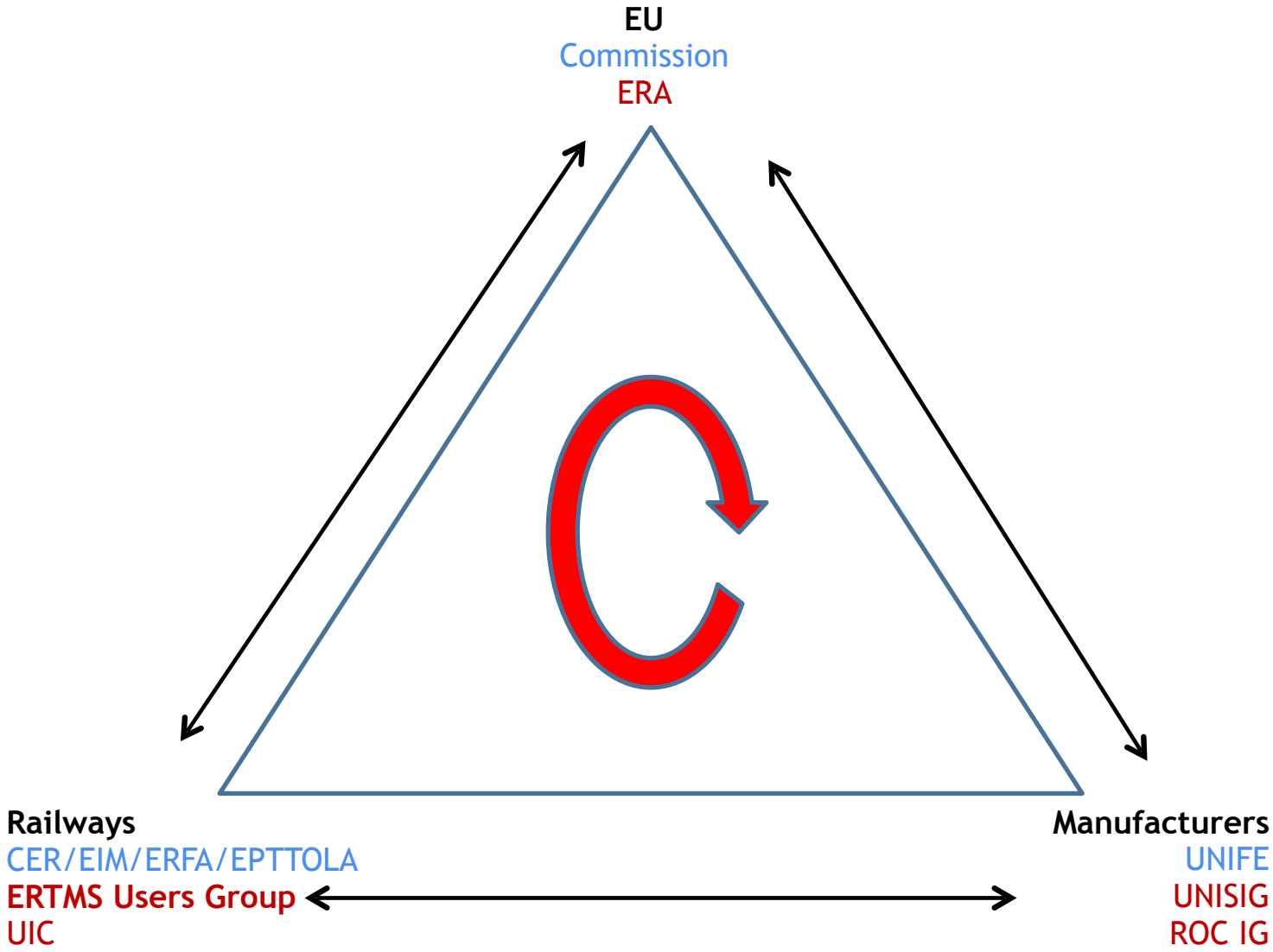
EUG Members


Bane NOR
Trafikverket
Banedanmark
Network Rail
ProRail
Infrabel
DB
SNCF Réseau
SBB
ADIF
RFI

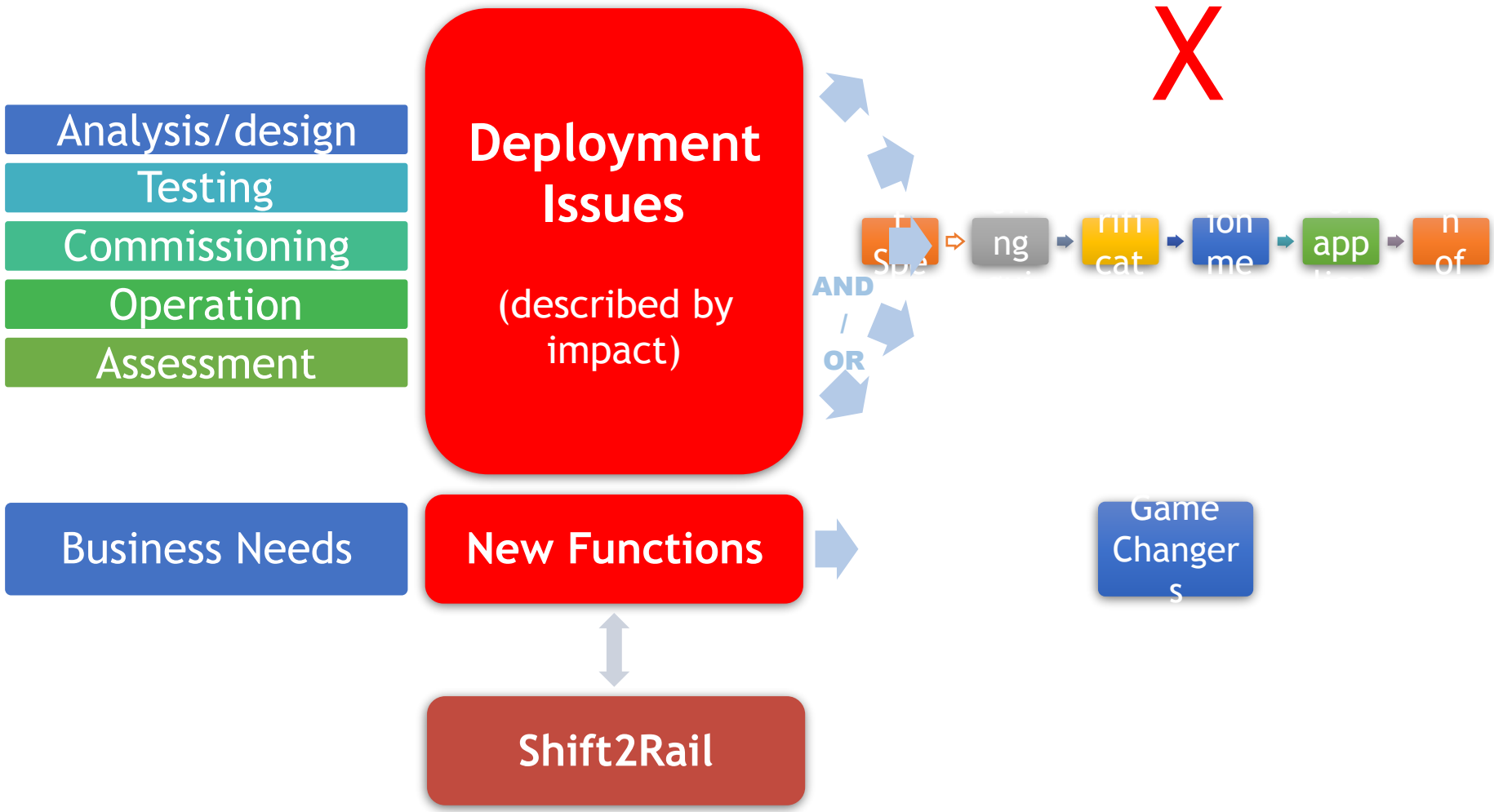
EUG RU ERTMS/ETCS Platform

- Railway Undertaking ERTMS/ETCS platform set up in 2013
- Aim: to share ERTMS/ETCS experiences and ideas
- Discussed are the relevant and practical issues concerning specification, design, certification, installation, authorisation, performance, reliability, operation, tendering and maintenance of ETCS On-Board Units in rolling stock
- Participants:
  - DB Fernverkehr, DB Cargo, MRCE, NS, ÖBB, SBB, SNCB, SNCF, Trenitalia (substantial (potential) ERTMS investments, > € 50 million)
  - ATOC, CER, ERFA, EPTTOLA, UIC
  - Other stakeholders (suppliers, ERA, EC, NSA's, NoBo's, laboratories) are invited.

Role and level



EUG's Activities

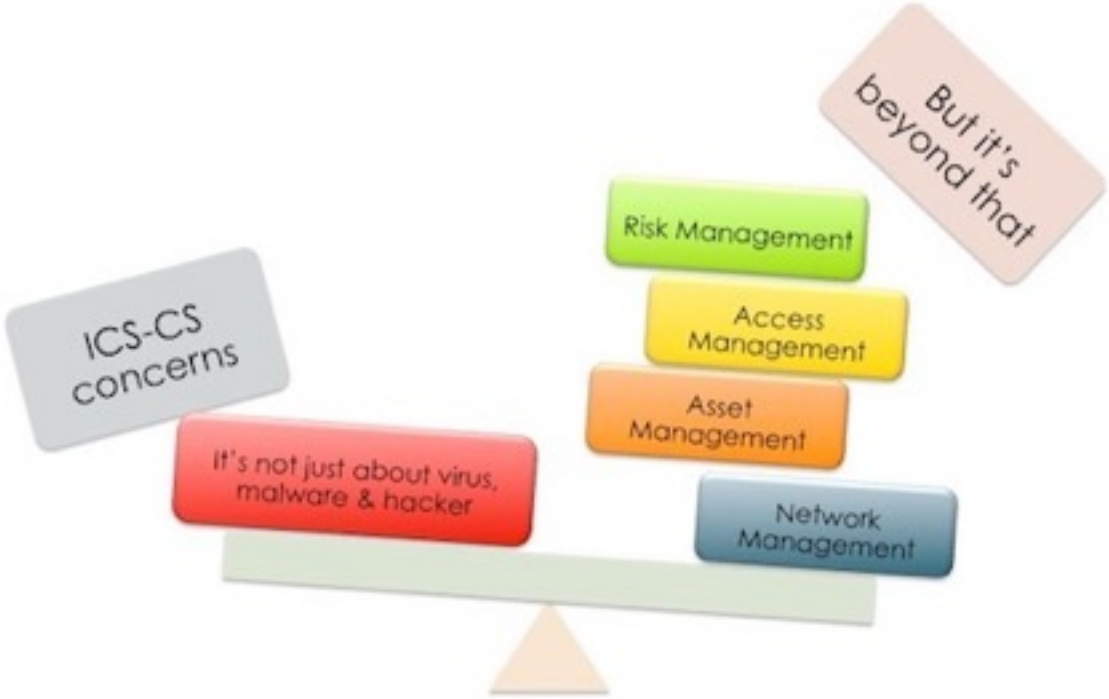


Security Governance

- Security has to be driven all the way from the top of the organisation.
- Aligned with the business objectives and provide added value to the business

IACS Cybersecurity

- IACS – CS is not just about the virus and malware but it is beyond that mindset.
- Integrated of several management system that related into it e.g. Access Management, Asset Management
- All of the related entities within the organization to take part, from management to the technician.
- ICS security is not just one man show activities

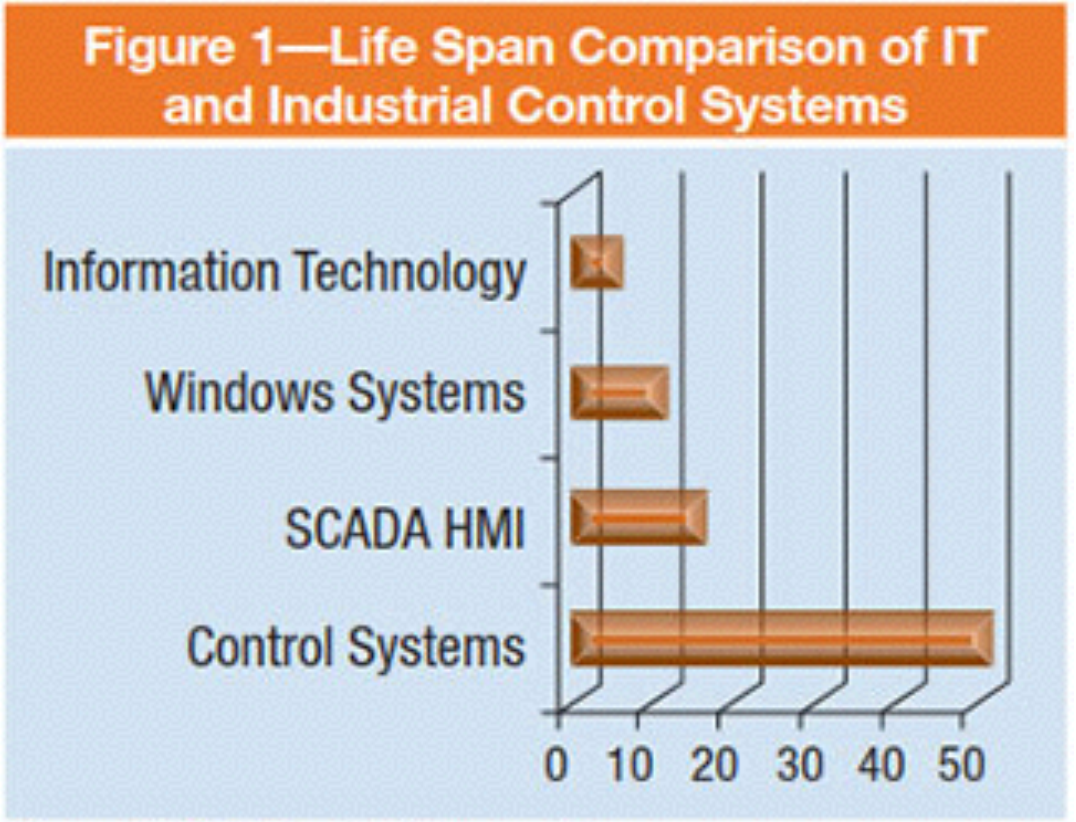


Railway Business Fragmentation

- Railway Engineering (CCS)
  - Focusing on signalling
  - Onboard and Trackside equipment
- Railway Operations
  - Traffic Management
  - Train Scheduling
- Corporate
  - Ticketing system
  - Passenger Information

Challenges in the Railways

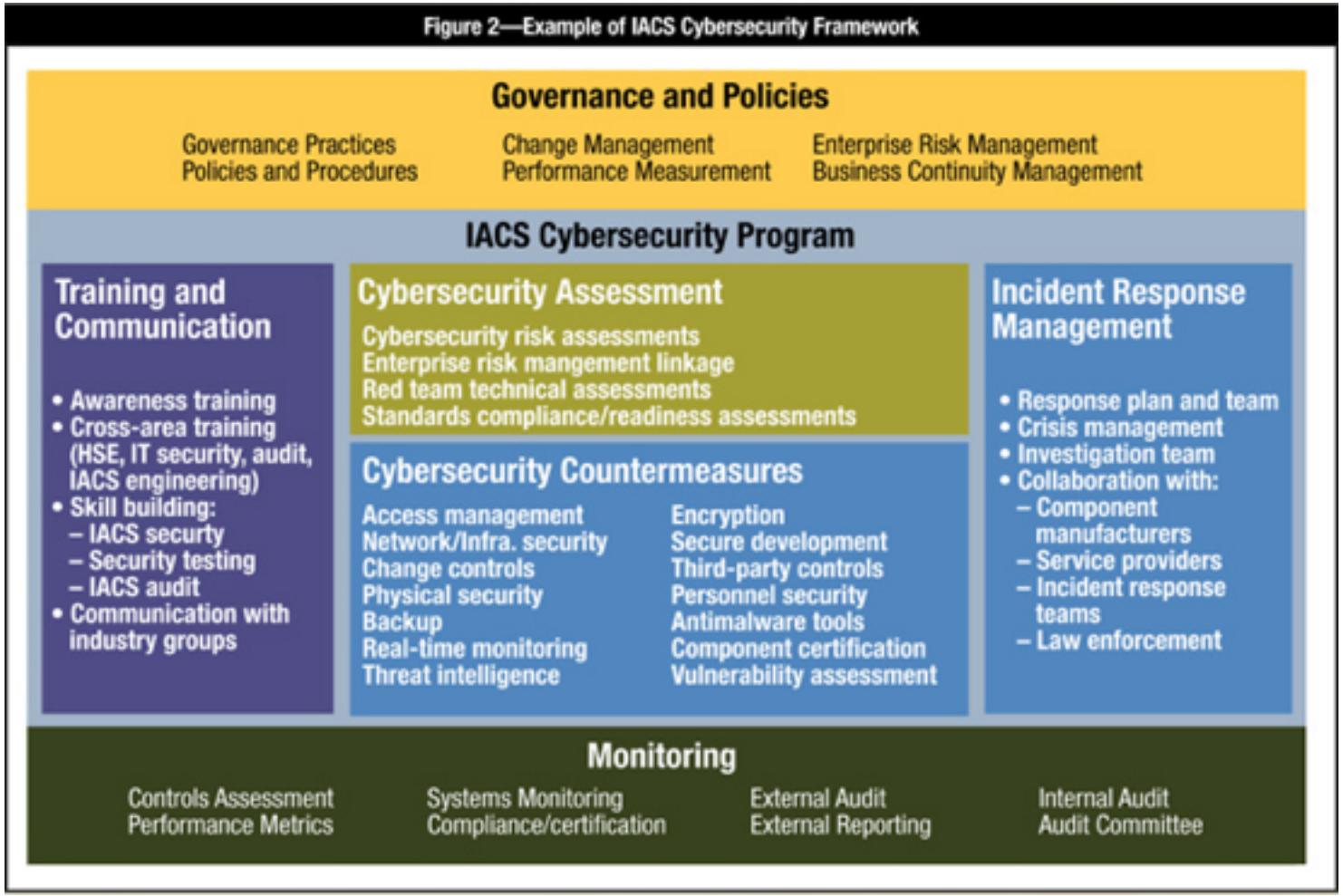
- Shifting from proprietary technologies to Off-the-shelf
- Manage the difference in lifecycle of control systems and IT
- Long amortization period for ICS investment



More Challenges

- The Awareness Level
  - Lack of awareness of the cyber security criticality in ICS environment
- The People Mindset
  - People thinking of ICS has no relation with ICT stuff, no need to deploy cyber security in ICS environment
- The Professionals Availability
  - Lack of capable professionals that has ability to cover Automation Control engineering and Information Communication Technology disciplines to deal with the Cyber Security Management and Compliance in ICS
- Business Driven
  - Business driven is not seeing the critical requirement of having cyber security assurance for their ICS environment
- The Systemic Framework
  - Standards/policy/procedures/manuals not in place or inadequate
- Organizational Culture
  - The organizational culture that still lack of cyber security compliance, the security culture should be developed from the security practice and behaviour in personal level. It also requires governance from the systemic framework

IACS CyberSecurity Framework



IACS Security Lifecycle

Take Away

- IACS cybersecurity is not a 1 man show (1 team show)
- The whole organisation has to engage into a IACS Cybersecurity Programme
- Top Management buy-in is key
- Many IACS security standards and framework exist and can be valuable when establishing an IACS cybersecurity Programme
- No “one size fit all” approach to IACS Security

Thank you for your attention

www.ertms.be

Co-financed by the European Union
Connecting Europe Facility