EULYNX

Assuring EULYNX:
Application of CSM-RA to Specification Development

Safety-Critical Systems Symposium 2019

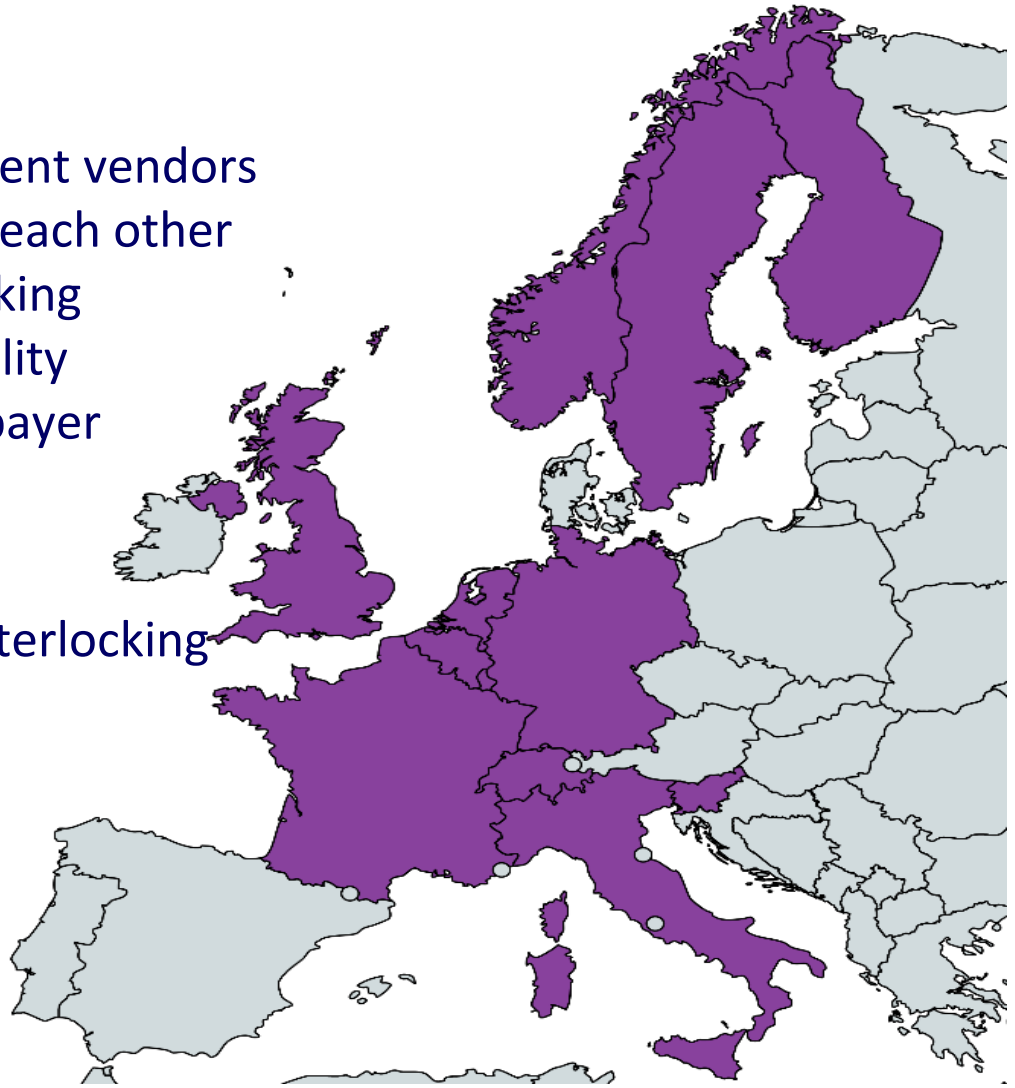
Stephen Bull, Principal Safety Engineer,
Ebeni Limited

David Shipman, Innovations Engineering Manager,
Signalling Innovations Group, Network Rail

Why EULYNX?

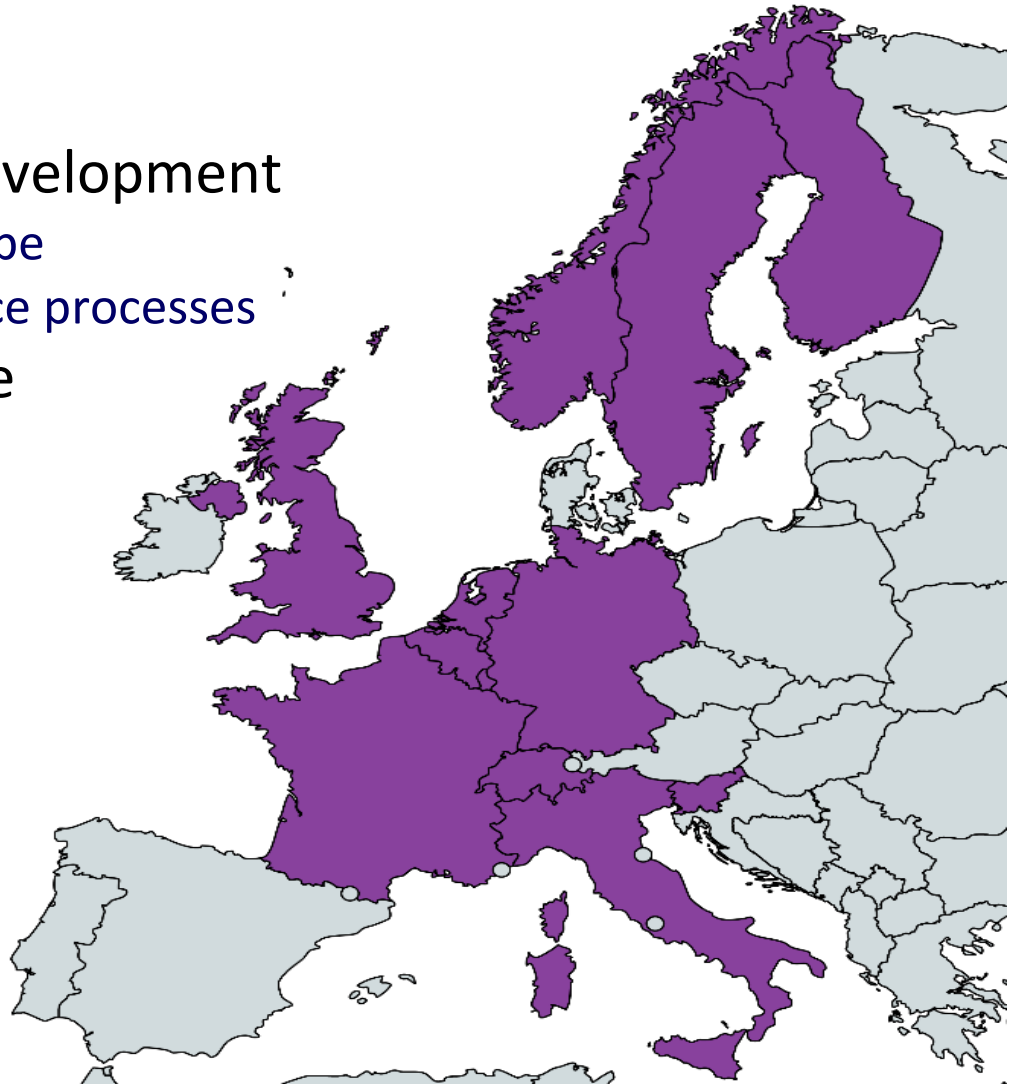
- Conventional signalling systems
  - Wide variety of products from different vendors
  - Safety critical communications with each other
  - Object controllers bound to interlocking
  - Proprietary protocols prevent flexibility
  - Costs to the industry and to the taxpayer

- EULYNX
  - Standardising interfaces between interlocking and object controllers
  - Common communication protocols
  - Separation of component lifecycles
  - Opening markets
  - Accelerating innovation
  - Economies of scale

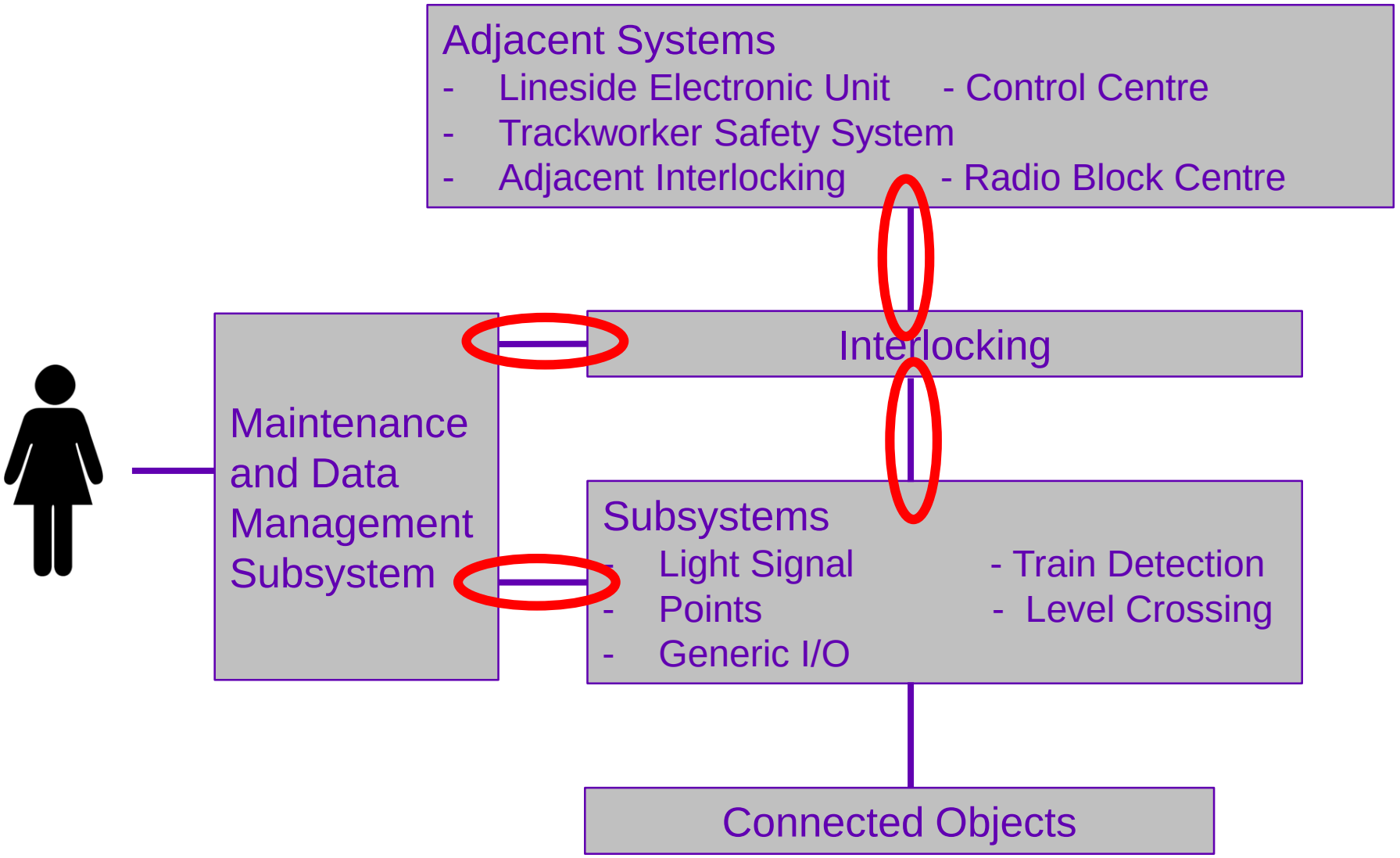


Aims of EULYNX assurance

- Assure interfaces once during development
  - Using method accepted across Europe
  - Consistent with European acceptance processes
- Obtain acceptance across Europe
- Eases
  - product acceptance
  - application safety cases



EULYNX Architecture



EULYNX Clusters

- Light Signal
- Points
- Train Detection
- Level Crossing
- Generic I/O
- Adjacent Interlocking
- Control Centre
- Radio Block Centre
- *Trackworker Safety System*
- *Centralised ETCS L1 Controller*
- System Architecture
- Modelling and Testing
- Data Preparation
- Assurance
- Security

Results Overview

	Process Data Interface	Diagnostics and Maintenance	Specific Subsystem Functions
Hazards	4	2	14
Hazard Causes	9	6	19
Assurance Requirements	17	3	0
Application Conditions	13	3	11

- Also found 14 assurance concerns across the programme

Example findings

- Hazard:
  - Interface does not communicate information correctly
- Cause (one of several):
  - The interface is not capable of passing the message within the timescales required by the application
- Assurance Requirement:
  - Any time critical functions (affecting either safety or availability) associated with each interface shall be identified.
- Application Requirement:
  - The applied system shall identify if there are any time critical safety functions, and establish that the communications protocol and the functional implementation are sufficient to control the risk.

Key Challenges

- Safety and Security
  - Security-Informed Safety Assurance
- Novel Approach
  - driven by development lifecycle
- Understanding system boundary
- Choice of Assurance Standard
  - for acceptability across Infrastructure Managers
- Diversity of Participants

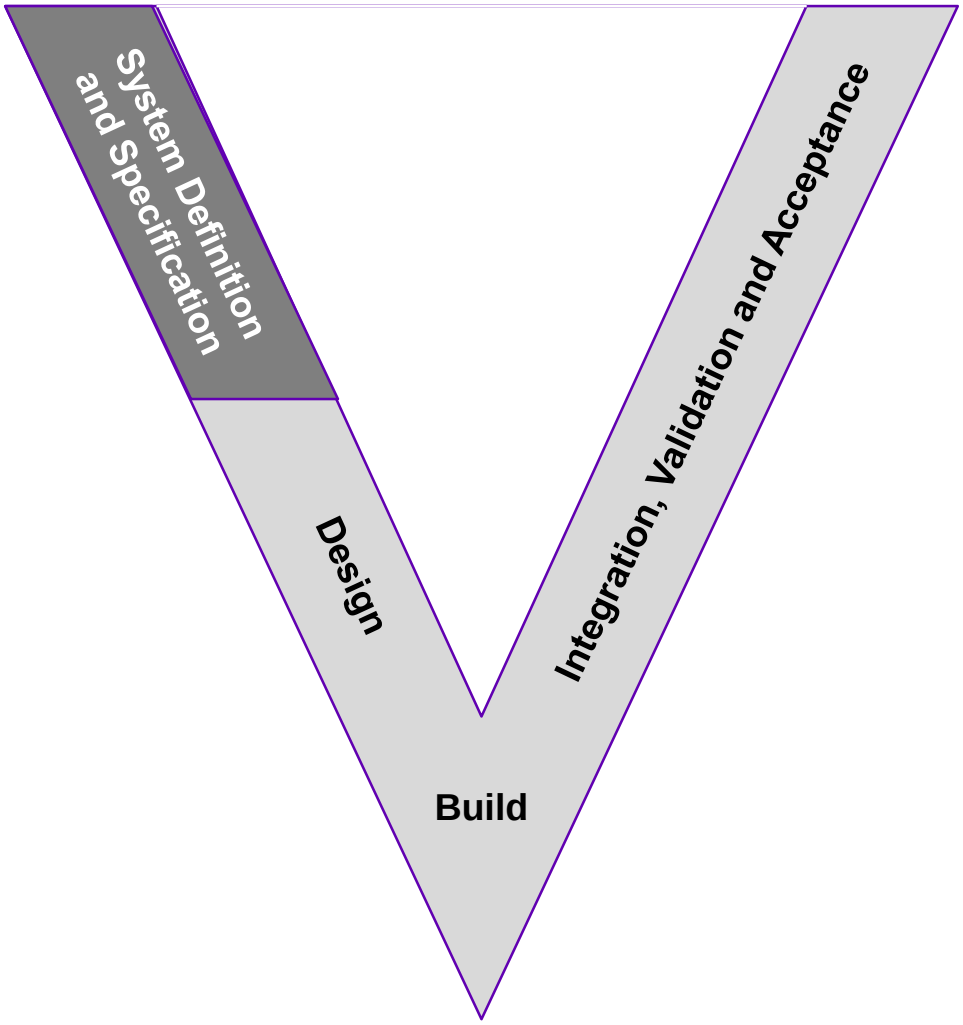
Challenge of Security + Safety

- Safety lifecycle
  - Long lead time (40 year product life)
  - Product acceptance overhead
- Security lifecycle
  - Fast-moving environment
  - Quick response to security threats

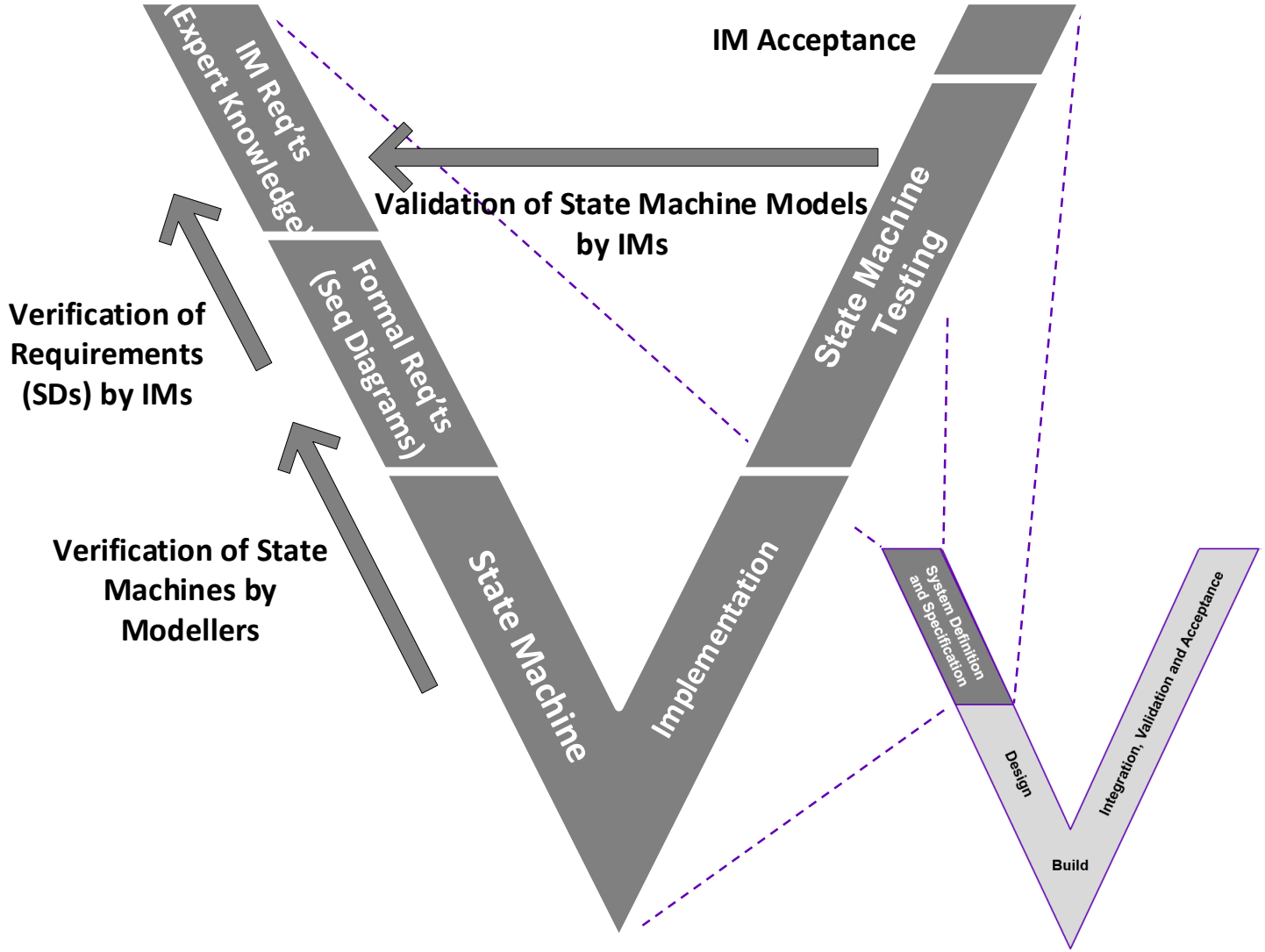
Security-Informed Safety Assurance

- Coupling between safety and security limited
  - RaSTA Protocol (for control interfaces)
  - EN50159 Category 2 network (or equivalent)
  - Assessment of security impact on safety
- Security cluster
  - IEC 62443 as basis
  - Alignment to standards working groups
  - Security concept for IM implementation

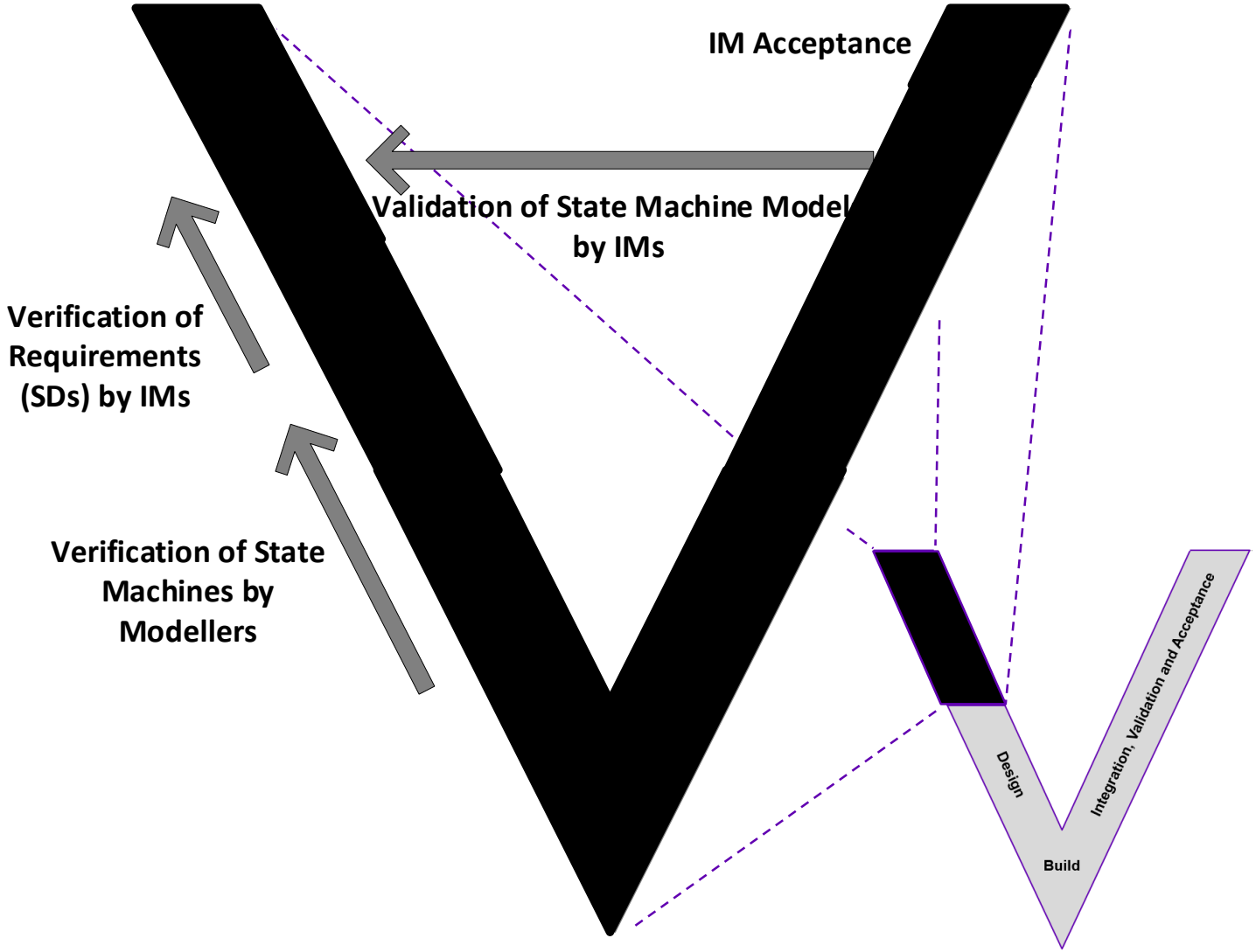
Novel Approach



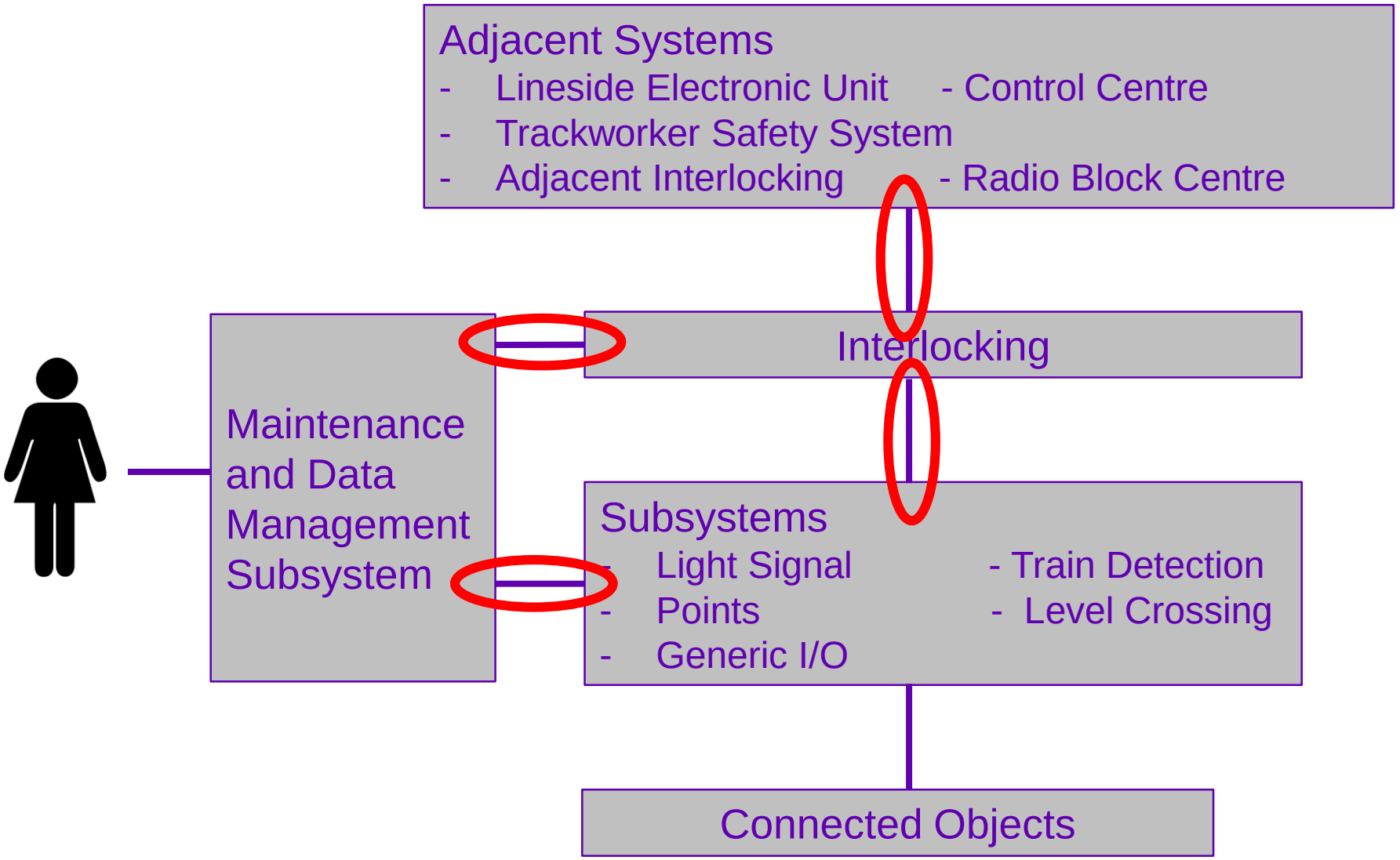
Novel Approach



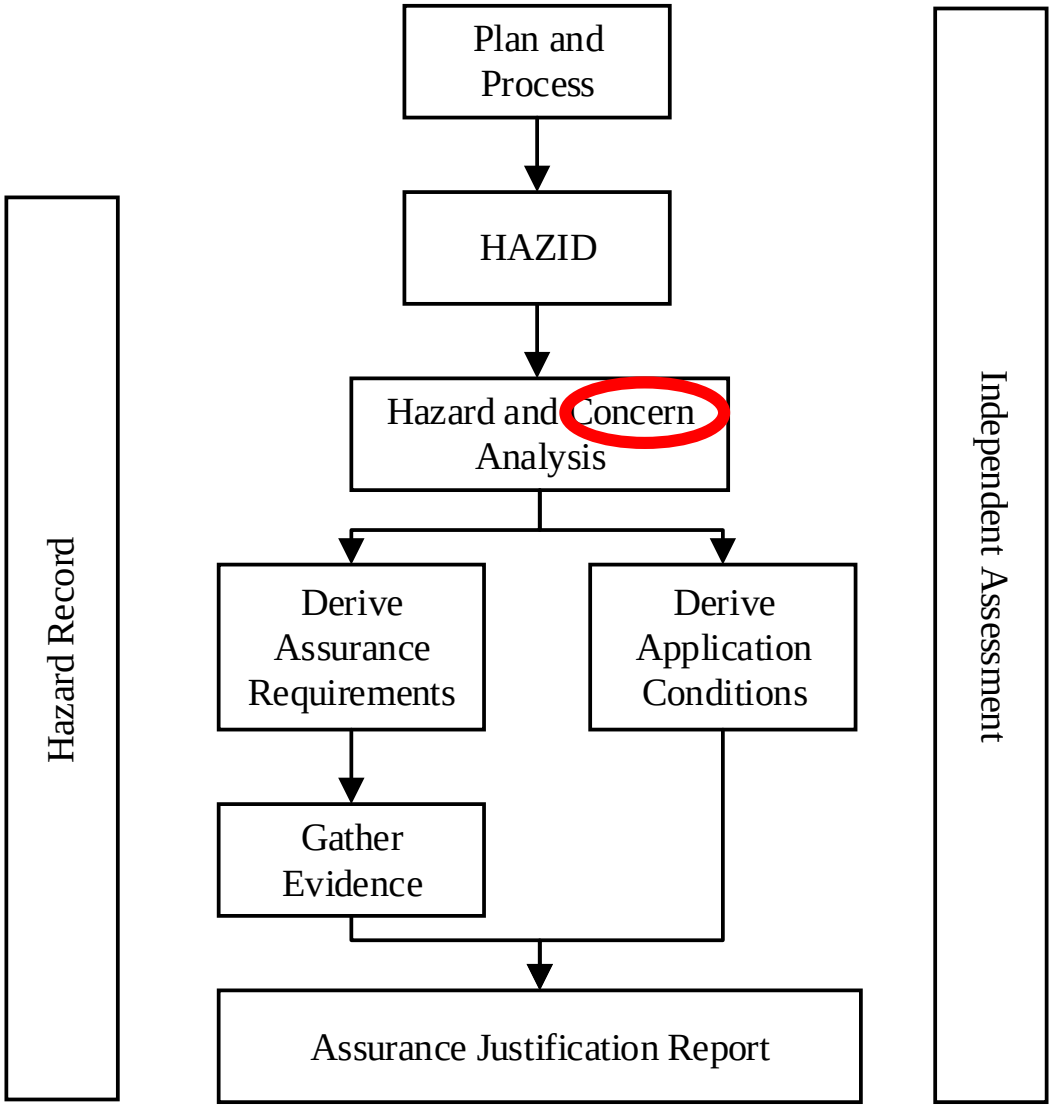
Novel Approach



Understanding System Boundary



Choice of Assurance Standard



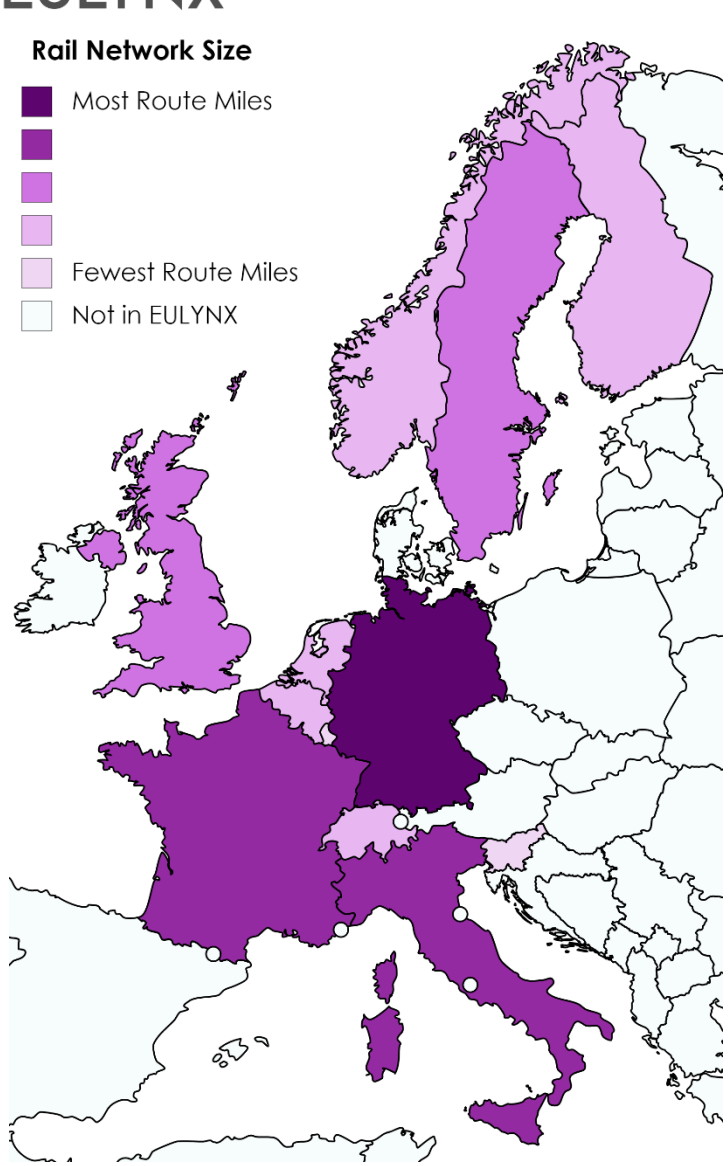
Risk Acceptance Principles

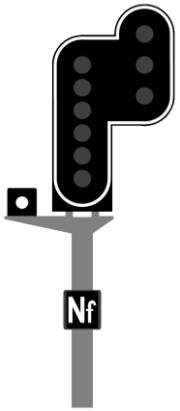
- Codes of Practice
  - EN5012x
  - EN50159
  - IEC 15288
- Reference Systems
  - RaSTA
- Explicit Risk Estimation

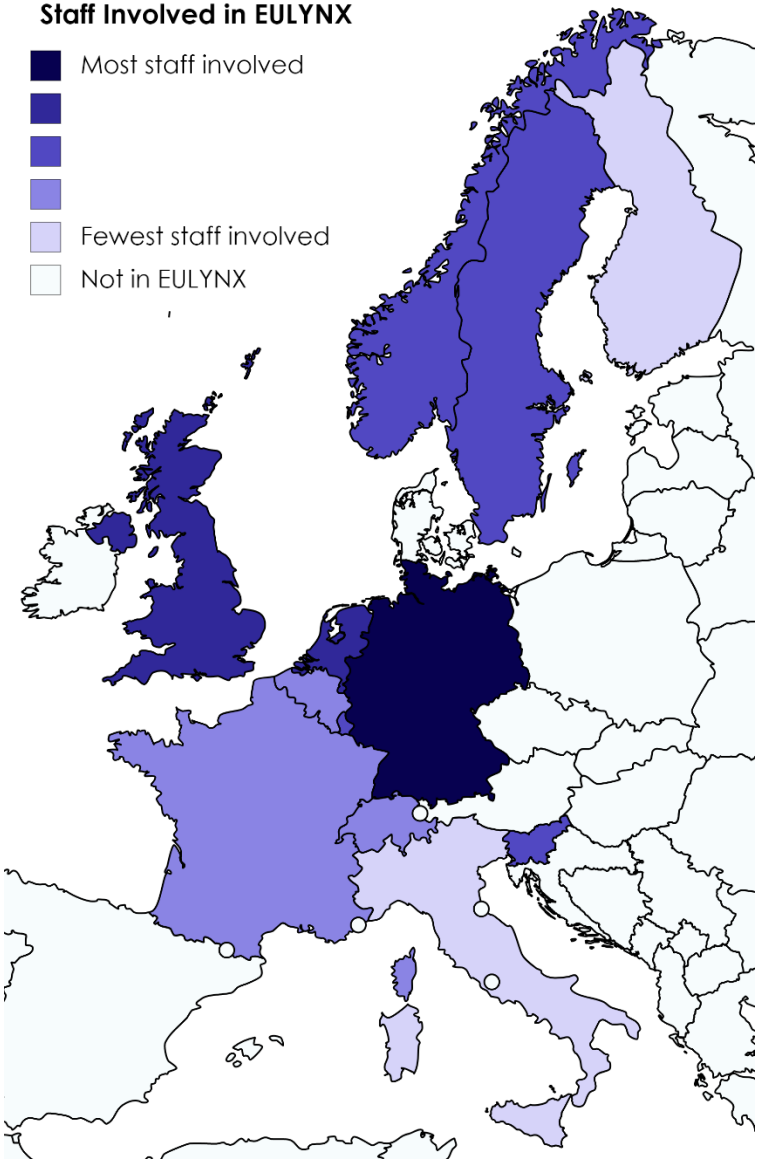
- Engineering Judgment
- Application Requirements
- Architectural Change

NOT REQUIRED

Diversity of Participants







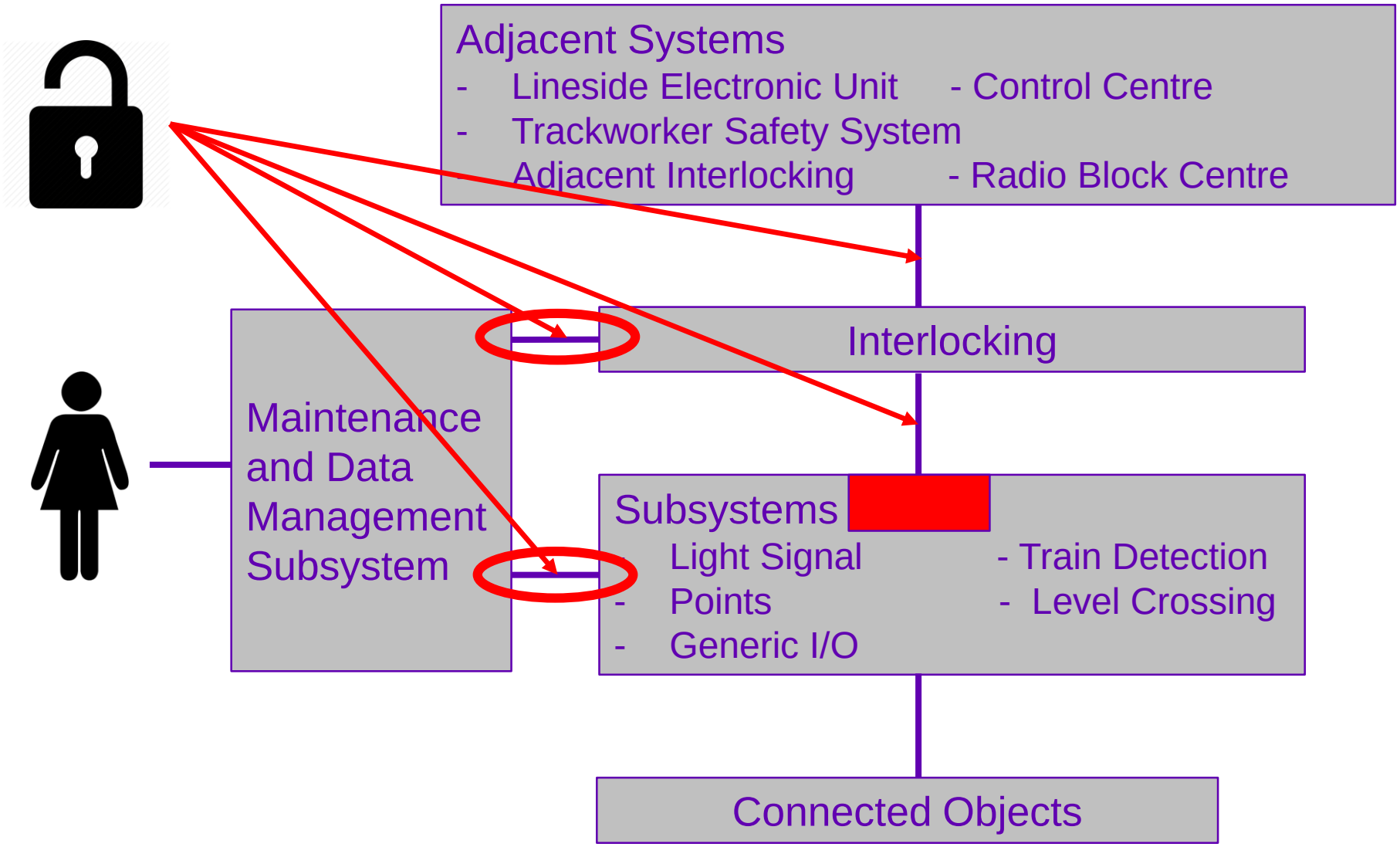
Achievements

- Basis for assuring EULYNX established
  - mapped to CSM; accepted processes and standards
- Interface between safety and security agreed
- Core set of hazards and assurance concerns identified
  - small number
  - significant causes to mitigate
- Mitigations identified
  - within EULYNX
  - for implementation by application projects
- Unified disparate inputs from clusters
  - streamlined process

Conclusions

- CSM works for us
  - Provides Europe-wide assurance
  - Allows us to “close the box” on interface assurance
- Security-Informed Safety
- Assurance is complex
  - despite few hazards, because …
  - … dealing with part of system
    - system behaviour out of scope
    - network architecture out of scope
- Importance of early planning
  - to support gathering of assurance evidence

Next Steps


Adjacent Systems
- Lineside Electronic Unit
- Control Centre
- Trackworker Safety System
Adjacent Interlocking
- Radio Block Centre
Interlocking
Maintenance and Data Management Subsystem
Subsystems
Light Signal
- Train Detection
- Points
- Level Crossing
- Generic I/O
Connected Objects

Further information

- Ask us questions today!
- Visit the project web site: https://eulynx.eu/
- Watch the videos:
  - EULYNX Standardisation of Signalling Interfaces (2017)
  - The Making of EULYNX (2018)
- Contact us:
  - Stephen Bull
    - Principal Safety Engineer, Ebeni Limited
    - stephen.bull@ebeni.com
    - +44 7867 330 843
  - David Shipman
    - Innovations Engineering Manager, Signalling Innovations Group, Network Rail
    - david.shipman@networkrail.co.uk
    - +44 7825 258 429