A Systems Approach to Safe System Integration in Major Rail Projects

Dr Raden Kusumo
13 October 2019

safe railways for Australia

Presentation

- Complexity in major rail projects.
- RSNL requirements on system integration.
- A systems approach to system integration
- System integration through out system lifecycle
- Case Study

Complexity in major rail projects

- Railways rely on various interdependent systems:
  - operate seamlessly together forming a system of systems of system
- Major projects complexity:
  - implement/change a number of rail systems
  - new and legacy systems
  - variety of complex technologies
  - different suppliers for subsystems
- Rail systems must be safely integrated to ensure safe railway operations

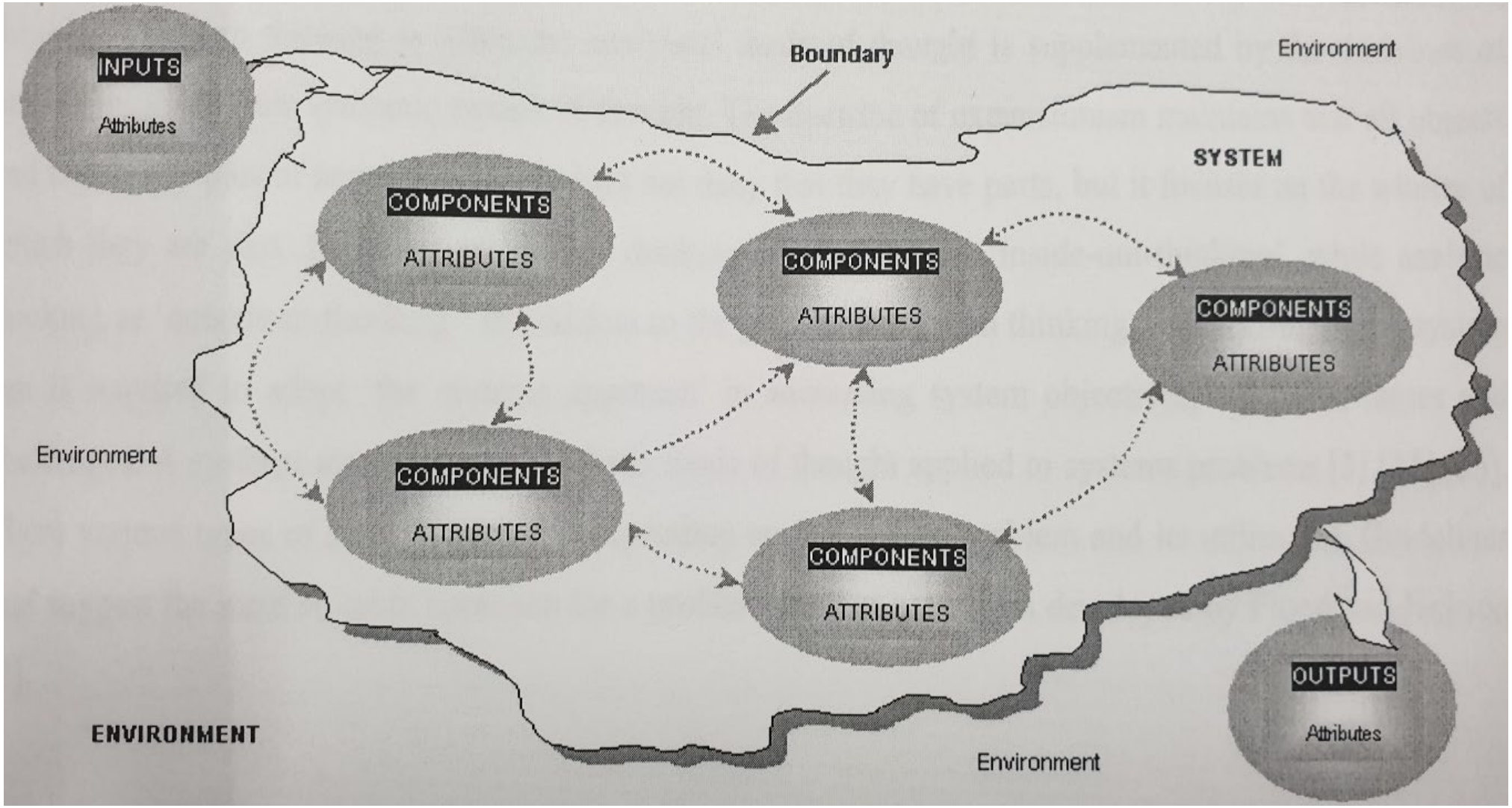
RSNL requirements on system integration

- No specific requirements.
- RSNL related requirements:
  - S.46 – *Management of risks*
  - S.52 – *Duties of rail transport operators*
  - S.53 – *Duties of designers, manufacturers, suppliers, etc.*
- RSNL Regulation related requirements:
  - Sch 1, C.12 – *Management of change*
  - Sch 1, C.19 – *General engineering and operational systems safety requirements*
  - *Sch 1, C. 20 – Process control*

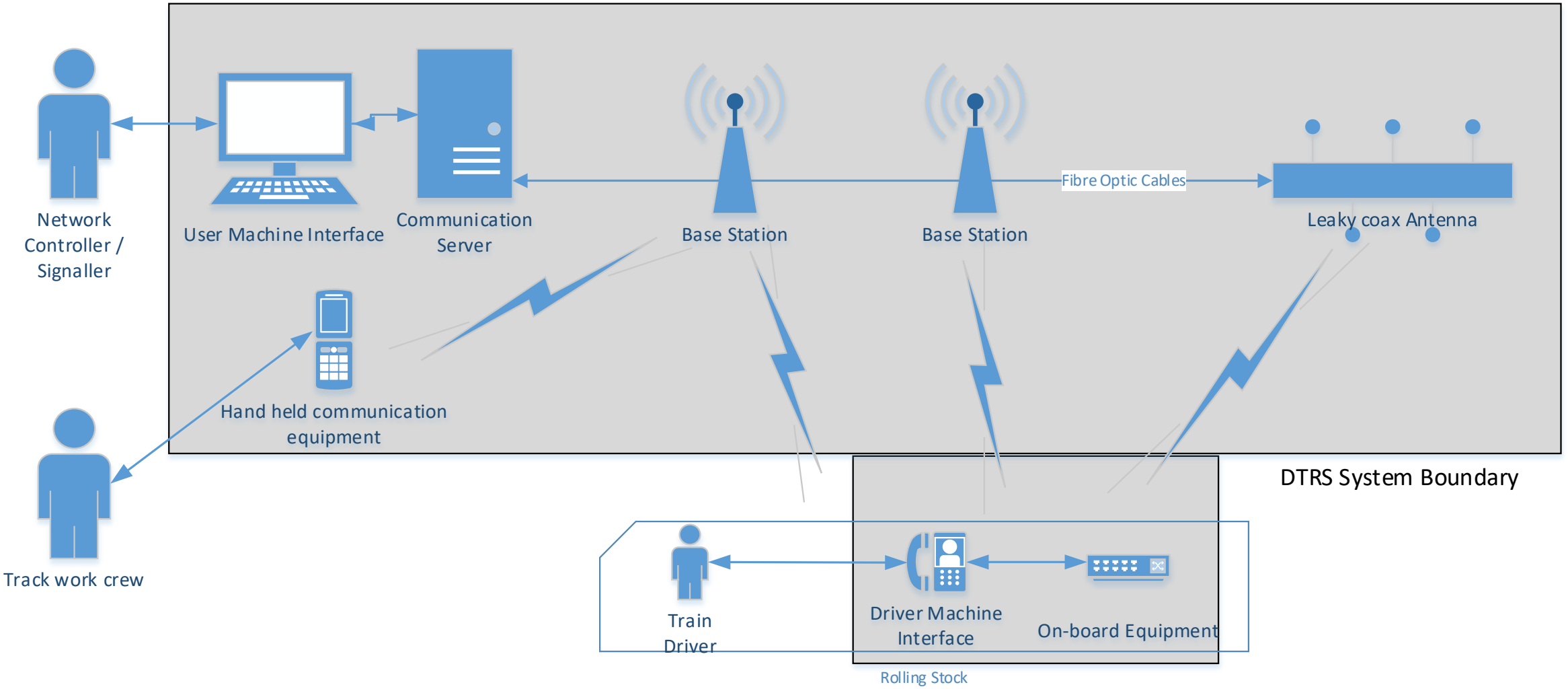
Why adopt a systems approach?

- Allows projects to manage the increasing complexity of railway systems integration
- Ensures projects can meet their safety duties that are stipulated in the RSNL

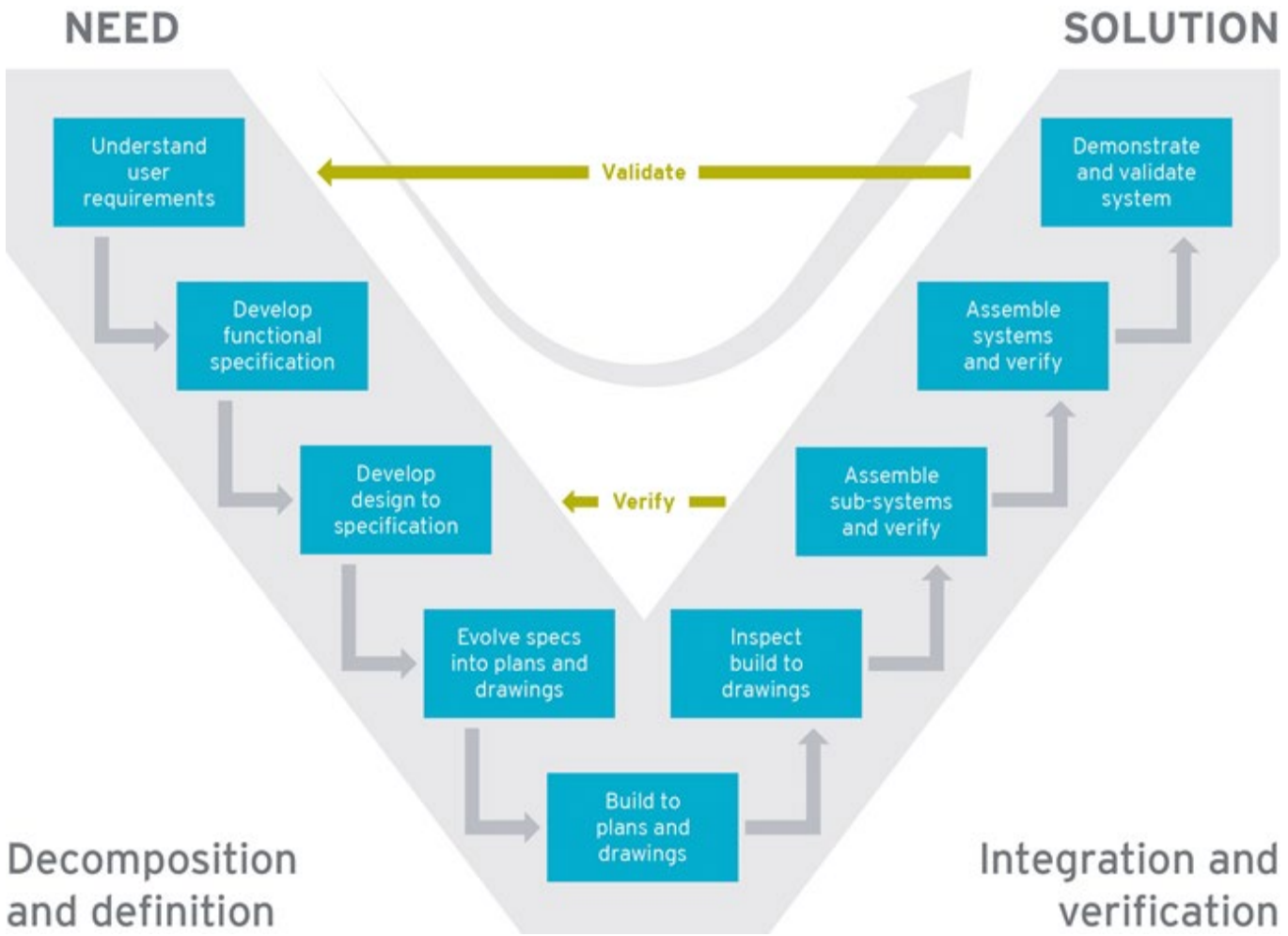
A systems approach



Typical Train Radio System (TRS)



A system life cycle



A systems approach to system integration

At each lifecycle phase determine:

- How the subsystems will be integrated?
- How these subsystems will interface with:
  - Existing railway infrastructure
  - Different types of rolling stock
  - Different types of user

Requirement specification phase

Specify interface requirements:

- Between subsystems
- With legacy systems
- Safety Related Application Conditions (SRACs) on the existing railway systems

TRS interface requirements

- Functional
  - REC management
- Operational
  - DMI interactions
- Physical
  - DMI in-cab position
- SRACs
  - Electromagnetic emission

Design phase

- Interface compatibility between connected railways systems.
- Risk assessment:
  - Interface failures
  - Overall system failures
  - Railway operations safety
- Compliance with SRACS.
- Risk control verification.

TRS design phase

- Interface compatibility analysis
  - Batteries power interface
- Interface hazard analysis
  - UMI interference
- System hazard analysis
  - DMI alarm failure
- SRACs compliance
  - Electromagnetic emission
- Risk control verification
  - Alarms to monitor power supply

Installation phase

- Installation and configuration errors may result in:
  - System failure
  - Wrong side failures of interconnected systems
- System interface verification:
  - Correct implementation
  - Conformance with design
- Risk assessment:
  - Design deviation

System testing phase

- System standalone tests:
  - Factory Acceptance Test
  - Site Acceptance Test
- Include testing system interfaces:
  - Legacy systems interfaces
  - Subsystems interfaces

TRS system testing

- Safely receive the inputs:
  - Clearly receiving emergency voice communication
- Safety functions are not compromised:
  - failure of local power supply
- Safely generate the required outputs:
  - Clearly transmitting emergency voice communication
- Outputs will not compromise interconnected systems:
  - Interference with the signalling systems

System integration phase

- Safety verification & validation:
  - systematically testing the effect of one subsystem on another subsystem
  - changes in the behaviour of subsystems
  - changes in the behaviour of whole integrated system
- Safety verification:
  - safety related system is built right
  - completeness, correctness and consistency
- Safety validation:
  - right safety system is built

TRS system integration

- Function correctly
  - Transmit emergency calls
- Meet operational requirements
  - Transmission delay
- Will not compromise existing systems
  - Interference with signaling systems during testing
- Management of risks associated with:
  - Testing activities
  - Changes in system configuration

System operation & maintenance phase

- Continuously monitor:
  - All faults and corrective actions
  - All residual risks
  - All system SRACs

TRS operation & maintenance phase

- Operational faults:
  - Connectivity with other train communication systems
  - Drop out rates
- Effectiveness of risk controls:
  - Driver training
- Compliance with SRACs:
  - Power monitoring alarm

Case Study

TRS Implementation:

- Modified-of-the-shelf
- SIL 0 according to CENELEC Standards
- Installed in multiple rail corridors and different train types.
- Design, installed and tested as stand alone system
  - Using limited number of base stations

Case Study

- Initial testing shows significantly higher time delay in transmission:
  - Fails to meet operational and safety requirements
- Internal software modification:
  - Optimise base station selection
- Impact of modification:
  - Additional risk assessments on faults and modification.
  - System retesting
  - System SIT retesting for each rail corridor and train type
  - Additional safety artefacts to demonstrate safe SFAIRP.
  - Delays to project.

Questions & Discussion

Thank you