Transport
Asset Standards
Authority

# T HR SC 01256 SP

## Telecommunication Transmission Systems for Signalling and Control Systems

Omer Saricilar, Principal Engineer - Control Systems

February 2016

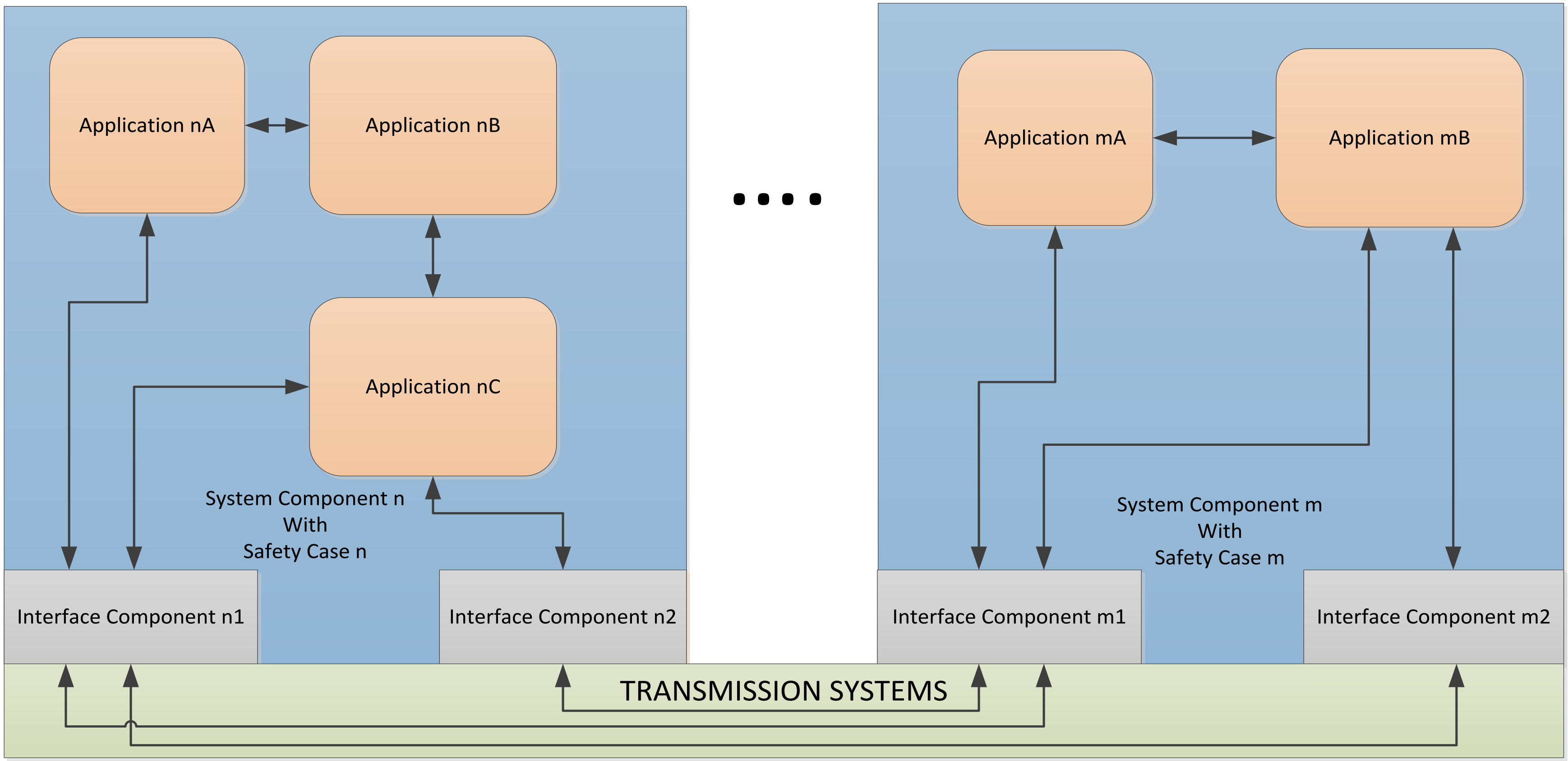
# What is in ‘T HR SC 01256 SP’?

- Replaces SPG 1256 Communication Links for Signalling Control V 1.1
- Aligned with international standards
- Requirements are based on performances
- Apportioned requirements
- Applicable for all signalling and control systems including on board systems
- Applicable to new design
- Context of requirements are explained
- Safety and security aspects expanded
- Provided examples using existing TfNSW assets

# Standards

- **IEC 62278** Ed. 1.0 (Bilingual 2002) Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS) (**EN 50126-1: 1999**)
- **IEC 62425** Ed. 1.0 (Bilingual 2007) Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling (**EN 50129: 2003**)
- **IEC 62279** Ed. 2.0 (Bilingual 2015) Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems (**EN 50128: 2011**)
- **IEC 62280** Ed. 1.0 (Bilingual 2014) Railway applications - Communication, signalling and processing systems – Safety related communication in transmission systems (**EN 50159: 2010**)

# Reference architecture



**Interface Components**
- Serial Interface
- Parallel Interface
- Network Interface
- USB

**Transmission Systems:**
- Any type of cable, including optical cable
- Packet Switching Network
- Circuit Switched network
- Radio or WiFi

**System Components:**
- Server
- Network equipment
- PC or laptop or tablet or mobile device
- Supporting equipment, such as KVMA, convertors
- RBC, IXL, Object Controllers

**Application:**
- Software
- Firmware
- Executive
- Ladder Logic
- Hardware

↔ Communication Path between applications

# What is failure?

- defined at OSI application layer
- The integrity of the message stream is compromised when any one of the following does not fulfil the specified requirements:
  - message order
  - message content
  - timeliness, including throughput and responsiveness
- each protocol may have different parameters for the failure criteria
- The following requirements as a minimum:
  - complete failure criteria of individual message
  - retry criteria
  - timeliness criteria
  - message ordering criteria

# Transmission delays

- Determines:
  - responsiveness - real-time system or not.
  - timeliness
  - staleness.
- Two distinct components:
  - the transmission system’s delays between system component boundaries
  - delays between the application and interface to the transmission systems
- Generic requirements
  - delays in milliseconds
  - number of retries
  - measurement direction
- Delays include redundancy handling

# Diversity and Redundancy

- Apportioned requirement
- Telecommunication cables
  - No diversity,
  - Cable diversity, duct diversity, route diversity
  - Full diversity
- Other links
  - No diversity,
  - Partial diversity
  - Full diversity
- provide full diversity for all communications path between applications
- supported evidence-based risk analysis and industry standard methodologies
- the common cause failure analysis also be a part of the analysis in order to identify such failure

# RAM

| RAM | Functions | | |
|---|---|---|---|
| | Safety related | High availability | Standard |
| Availability | 99.999% | 99.995% | 99.99% |
| Reliability (in hours) | 100000 | 70000 | 50000 |
| Mean down times (in hours) | 1 | 3.5 | 5 |

# Safety

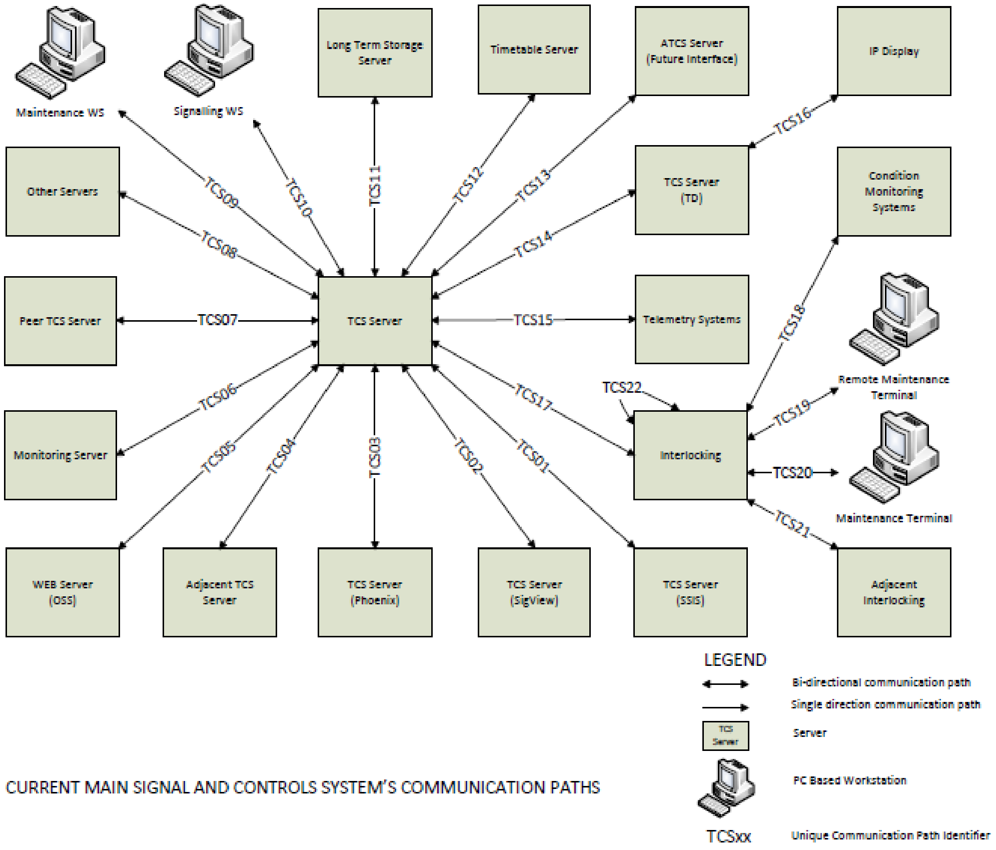
- IEC 62280 based (EN 50159)
- Categories
  - category 1 (closed transmission system) – the transmission system satisfies all preconditions
  - category 2 (open transmission system) – the transmission system satisfies precondition 3, but not precondition 1 or precondition 2
  - category 3 (open transmission system): if the transmission system does not satisfy the precondition 3
- Default is Category 3
- Examples are provided
  - Categorisation
  - Applying defences

# Security

- Physical security
- Encryption
- Defense in depth
  - DMZ
  - Multi Layer strategy
  - VPN
  - Segregation
- No impact on the performance requirements

# Example: TfNSW communication paths

- Only as guideline



CURRENT MAIN SIGNAL AND CONTROLS SYSTEM'S COMMUNICATION PATHS

# Example: Defence analysis

- Only as guideline – transmission system is NOT cat 1
- Encryption on its own does not provide complete protection against repetition, deletion or re-sequencing.

| Threats | Defensive protocol characteristics | Proposed defences |
|---|---|---|
| **Repetition** | None | **Encryption** |
| **Deletion** | None | **Encryption** |
| **Insertion** | Only slave address | **Encryption** |
| **Re sequence** | None | **Encryption** |
| **Corruption** | CRC-16 polynomial check | **None** |
| **Delay** | Timeout | **None** |
| **Masquerade** | **None** | **Encryption** |

# Train management system requirements

- New name: ‘**T HR SC 01257 SP Train Management Systems Requirements”**
- Replaces **ESG 005** Signalling Operator Interface v1.2
- In drafting phase for open discussions
- Generic and planned to use for ATCS
- Performance based requirement specifications
- Context of requirements are explained
- Safety and security aspects are expanded
- Human interface are left to HFA, but guideline will be provided
  - Zooming, combining controlled area
  - Sizes, colours, shapes
- Redundancy, disaster recovery are expanded
- Integrity aspects are detailed
- RAM