MOST PRESSING ISSUES FACING SYSTEM SAFETY

A BRIEFING ON SYSTEM SAFETY IN THE RAIL INDUSTRY for ISSS Conference 2015
SYSTEM SAFETY AS PRACTICED IN THE PASSENGER RAIL INDUSTRY

- Historical Perspective
- Standards and Practices in USA
- Recent Developments
- Future Considerations
- International Standards for Railway RAMS
HISTORICAL TIMELINE

- System Safety Applications in Passenger Rail in USA

1972: First Rail Transit SSPP
1981: MIL STD 882
1987: Industry Adoption
1996: FRA Regulation of SSPP
2012: FTA SSO 49CFR659
2012: SMS, Risk Reduction, Positive Train Control
STANDARDS & PRACTICES

• General System of Operations (FRA)

• Mass Transit (FTA)

• Operating by Waivers or Under Rule of Particular Applicability (Shared or Exclusive Use)
CHARACTERISTICS OF THE GENERAL SYSTEM
CHARACTERISTICS OF MASS TRANSIT
CHARACTERISTICS OF HIGH SPEED RAIL
RECENT DEVELOPMENTS

• High Profile Events
• Legislative Actions
• Positive Train Control
• State of Good Repair
• High Speed Rail
FUTURE CONSIDERATIONS

• Strong Trend Towards High Technology Solutions to Human Performance Limitations.

• Development of PTC into fully autonomous train operations or ATO. (Google trains)

• Magnetic Levitation technology
INTERNATIONAL
TYPES OF FAULTS

- **Inherent in the system**
  - Quality & safety management, organization

- **Safety-Significant Function**

- **Systematic Faults**
- **Random Failures**
- **Human Interactions**
- **External Influences**
  - EMI, temperature, vibration
  - Systematic, random or human error
  - Action causing a failure or unintended behaviour
  - O&SHA, FMECA, manuals

- **Result of deterioration**
  - Inherent in the system
  - Quality & safety management, organization

- **Reliability prediction, maintenance**
STRUCTURE OF EN50129 SAFETY CASE

System Requirements Specification

Safety Requirements Specification

Safety Case
- Part 1: Definition of System
- Part 2: Quality Management Report
- Part 3: Safety Management Report
- Part 4: Technical Safety Report
- Part 5: Related Safety Cases
- Part 6: Conclusion

Safety Assessment Report
Section 1: Introduction
- Describes the safety design, technical safety principles

Section 2: Assurance of correct functional operation
- Under fault-free normal conditions

Section 3: Effects of faults
- In the event of random hardware faults or systematic faults

Section 4: Operation with external influences

Section 5: Safety-related application conditions

Section 6: Safety Qualification Tests
CROSS-ACCEPTANCE OF GENERIC SAFETY CASES

- Must address safety-related application conditions

- System A
  - Subsystem 1
  - Subsystem 2
  - Subsystem 4

- System B
  - Subsystem 3

- Equipment a
- Equipment b
- Equipment c

Specific Applications → Generic Applications → Generic Products
THANK YOU

Bill Grizard
BGrizard@APTA.com

Sue Cox
Sue.Cox@SafetyWright.com