Comparative Analysis of US and European Approaches on Risk Analysis in Railway Signaling

Sonja-Lara Kurz – Technical University Braunschweig, Germany
University of Rhode Island, USA
INTRODUCTION

- Transportation systems – railway systems are used for person movement for commute, business, or leisure travel as well as to ship goods or freight

- Industry constantly tries to improve railway safety

- System safety is especially important where current systems are improved by new technology

- Railway signaling safety:
  - Past: traditional rule-base approach
  - Current: risk-base approach

- Different procedures for risk assessment process were developed in the US and in Europe
METHODOLOGY

- Review US and European Regulations for Railway Signaling
- Compare US and European Standards
- Review Risk Assessment Methods
- Introduce Case Study: CBTC for New York City Subway System
- Application of Risk Assessment Methods for Case Study
- Compare Risk Assessment Methods

<table>
<thead>
<tr>
<th></th>
<th>United States of America</th>
<th>Europe</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard</strong></td>
<td>FRA Rule 49, Part 209/234/236</td>
<td>IEC 62278 (EN 50126), EN 50129</td>
</tr>
<tr>
<td><strong>Risk Assessment Method</strong></td>
<td>ASCAP</td>
<td>Risk Graph</td>
</tr>
</tbody>
</table>
US AND EUROPEAN REGULATIONS

- Federal Railroad Administration (FRA)
  - FRA Rule 49 CHR Part 209/234/236
    Standards for Development and Use of Processor-Based Signal and Train Control Systems

- European Committee for Electrotechnical Standardization (CENELEC)
  - IEC 62278 (EN 50126)
    Railway Applications – Specification and Demonstration of Reliability, Availability, Maintainability, and Safety (RAMS)
  - EN 50129
    Railway Applications – Communication, Signaling and Processing Systems – Safety Related Electronic Systems for Signaling
FRA RULE 49

- Subpart H requires the establishment of
  - Railroad Safety Program Plan (RSPP) and
  - Product Safety Plan (PSP)

- PSP requires Risk Assessment to demonstrate that the system of interest will not result in a risk that exceeds the previous condition
  - Mean Time To Hazardous Events (MTTHE) has to be larger for the new system in comparison to the system to be replaced
  - No quantitative safety target is defined

- Risk Assessment Process: ASCAP
CENELEC

- CENELEC standards are a railway-specific adaptation of IEC 61508.

- Risk assessment process is generic and demands the definition of hazards and tolerable hazard rates (THR)

- IEC 62278 (EN 50126): RAMS management
  - System life cycle concept

- EN 50129: System Safety
  - Safety case structure
  - Global Process: First a quantitative safety target is established and then qualitative targets are set based on SILs.

- Both give examples of methods but do not prescribe any particular technique or risk tolerability criterion

- VDV 331: Risk Graph for SIL assignment
### COMPARISON FRA - CENELEC

<table>
<thead>
<tr>
<th>Similarities</th>
<th>Differences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk based</td>
<td>PSP has no specific absolute quantitative safety target, but quantitative risk assessment in terms of MTTHE,</td>
</tr>
<tr>
<td>Safety management</td>
<td>IEC 62278 and EN 50129 set quantitative safety target and then qualitative safety target based on SIL,</td>
</tr>
<tr>
<td>Systematic approach to hazard identification, hazard reduction assessment and</td>
<td>PSP quantitative assessment includes human factors,</td>
</tr>
<tr>
<td>risk assessment,</td>
<td>IEC 62278 and EN 50129 quantitative safety is based on random faults,</td>
</tr>
<tr>
<td>Verification and Validation: Demonstration of safety under various conditions,</td>
<td>FRA Rule is open for the public at no cost, and</td>
</tr>
<tr>
<td>Requirements of third-party assessment and final approval.</td>
<td>IEC 62278 and EN 50129 are better structured and have descriptive figures and tables.</td>
</tr>
</tbody>
</table>
RISK ASSESSMENT METHODS

- ASCAP
  - Axiomatic Safety-Critical Assessment Process
  - Developed at the University of Virginia Center of Rail-Safety-Critical Excellence
  - Supports the US FRA Rule 49, Part 209/234/236
  - Novel Monte-Carlo-based risk assessment simulation

- Risk Graph
  - Common technique used for assigning SILs
  - Qualitative method that uses decision tree approach, considering four risk parameters
  - IEC 61508 mentions risk graph as example method
  - Procedure is explained in VDV 331
ASCAP

ASCAP Risk Assessment Monte Carlo Simulation

Stationary and Mobile Objects
(Switches, signals, trip-stops, work trains, etc.)

Object Model

OP

FUS

FS

Hazard

Failures

Human Factors Model

NY Operating Rules/Procedures

Human Errors

Maintenance

N Train Movement (Exposure)

Movement Model (Davis eqs)

NY Timetable

Agents
(Subways Control Center, Train Operator, MOW Crew, etc.)

Interactions

Train(s) Coincident?

Events Passed At Danger (EPADs)

Train Incidents

Train Accidents

RISK GRAPH

Risk Parameters:

S = Consequence

A = Frequency and Exposure Time

G = Probability of Avoiding the Hazardous Event

W = Probability of Unwanted Occurrence

CASE STUDY

- New York subway system is fifth largest in the world (regarding annual ridership)
- Canarsie Line project represents the basis for long-term, total conversion of NYCT's signaling system
- NYCT Canarsie Line is being upgraded to CBTC technology
- $135 million contract to SIEMENS Transportation Systems to install CBTC system for Canarsie Line

- Canarsie Line:
  - 23 miles double track
  - 24 passenger stations
  - 30 trains

[http://www.mta.nyc.ny.us/nyct/service/lline.htm]
CBTC

ASCAP APPLICATION

- Risk assessment for Canarsie Line is performed per US FRA Rule 49, Part 209/234/236
  - Rule requires demonstration that the risk of the new system is equal or less than the risk of the existing system
  - Although US FRA Rule formally applies only to railroads, NYCT elected to be compliant to the rule

- UVA performs independent risk assessment of Canarsie Line project to support system approval process for CBTC equipment deployment

- Two primary cases are considered:
  - Base Case – Canarsie Line prior to CBTC deployment
  - CBTC Case – Canarsie Line after CBTC deployment
ASCAP APPLICATION

CBTC Case shows 85% risk reduction versus Base Case

RISK GRAPH APPLICATION

- ATP - Automatic train protection
  - speed and distance supervision, usually intervening when the driver of a train neglects to react to optical signals given from the wayside system.
  - ATP receives permitted speed and location information from the track via radio.
  - ATP ensures that trains comply with speed restrictions and prevents them from passing signals at danger

- CBTC ATP functions:
  - Train Detection
  - Safe Train Separation Assurance
  - Overspeed Protection
  - Brake Assurance
  - Traffic Direction Locking
RISK GRAPH APPLICATION

Risk Assessment for ATP:

Consequence = S3
Death of several people

Frequency and Exposure Time = A2
Frequent to permanent exposure in the hazardous zone

Probability of unwanted occurrence = W3
Relative high probability, frequent are likely

⇒ SIL 4
Comparison ASCAP – Risk Graph

Comparison Criteria:

- Transparency
- Adaptability
- Scalability
- Compliance
- Cost-Effectiveness
- Accessibility
- Tool Support
- Reproducibility
- Visual Representation
- Application

- Documentation
- Risk Parameters
  - Usage Profile
  - Hazard Rate
  - Exposure Time
  - Latency Time
  - Risk Reduction Factors
  - Severity Classification
  - Human Factors
### SUMMARY

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCAP</td>
<td>0</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Risk Graph</td>
<td>0</td>
<td>+</td>
<td>-</td>
<td>0</td>
<td>+</td>
<td>0</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

+ positive aspects outweigh negative aspects

0 balanced positive and negative aspects

- negative aspects outweigh positive aspects
## SUMMARY

<table>
<thead>
<tr>
<th>Risk Assessment Method</th>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCAP</td>
<td>Adaptability</td>
<td>Scalability</td>
</tr>
<tr>
<td></td>
<td>Compliance</td>
<td>Cost-Effectiveness</td>
</tr>
<tr>
<td></td>
<td>Reproducibility</td>
<td>Accessibility</td>
</tr>
<tr>
<td></td>
<td>Risk Parameters</td>
<td>Tool Support</td>
</tr>
<tr>
<td>Risk Graph</td>
<td>Adaptability</td>
<td>Scalability</td>
</tr>
<tr>
<td></td>
<td>Cost-Effectiveness</td>
<td>Reproducibility</td>
</tr>
<tr>
<td></td>
<td>Tool Support</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Visual Representation</td>
<td></td>
</tr>
</tbody>
</table>
CONCLUSION AND RECOMMENDATIONS

- US and European standards coincide in many general concepts but differ in details
  - THR and MTHHE concepts are similar with respect to setting safety targets
  - Different verification processes for assuring that safety targets are met

- ASCAP
  - simulation-based approach that replicates the actual behavior of a transportation system from a vehicle-centric perspective

- Risk Graph
  - assigns Safety Integrity Levels (SILs) to achieve a particular system safety target

- Further research: possible combination of ASCAP and Risk Graph based on knowledge of strengths and weaknesses
QUESTIONS?