Tool-based Safety Analysis of Operational Rules

Katrin Hartwig (DLR), Georg Mandelka (Bombardier)
Overview

- Background
- Challenge
- Approach
- Method for Analysis
- Example – Telephone Block Operation
- Findings of the Example
- Conclusions
Background

- Complex systems integrated for the operation of railways
- Complex operational rules used
- Systems consist of various sub-systems, some of them are safety-related
- High safety requirements for railways
  - High-quality components required
  - High life cycle costs
- New systems often based on structures of existing systems
- Existing systems get modified (to fit new requirements, to be employed in different environment)
- Modifications in complex systems cause high effort for the reassessment of the system’s safety / assessment of the consequences to safety
Challenge

Reduction of LCC
\[\text{e.g. for acquisition, operation, maintenance, ...}\]

Increase of Safety
\[\text{e.g. increase of reliability, decrease of forces}\]

By means of
- Utilization of most suitable components (low-cost ⇔ highly reliable)
- Implementation of safety functions
- Use of safe rules for operation

⇒ Analysis needed to show the possibilities for optimization
Approach

* Assessment of all elements and communication flows between the elements of the system

- Computer-supported system analysis for design* and rules

* here: control technology, not structure / material
Method and Tool for Analysis

Method

- Assessment of interactions with system environment
- Allocation of acceptable risk or similar
- Assessment of each sub-system generating interactions with environment
- Assessment of information influencing the interactions
- Assessment of sub-systems generating the information
- Assessment of sensors generating the information

The requirements on the output influence the requirements on the input!

SW Tool SALT

- Automatic allocation of safety relevance to each element (sub-system, information, sensors, ...)

Institute of Transportation Systems > Aerospace technology for road and railway
Method and Tool for Analysis

How to include rules for human (Instructions on how to act)?

Approach:
- Consider driver as a sub-system receiving and generating information
- Validation
- Transformation from technical system to written rule and vice versa

 Hardware logic  

\[ \text{PB1} \quad \text{PB2} \quad \text{R1} \quad \text{R2} \]

Software logic

\[ \text{PB1\_active} \quad \text{PB2\_active} \quad \text{Lamp\_active} \]

Written rule

"If pushbutton 1 is active and pushbutton 2 is not active then Lamp active"
Example – Telephone Block Operation

Instructions on how to act

Functions & Information flow

Activity diagram

Sub-systems & Information flow

Analysis

Representation

Advice

Split-up
Findings of the Example

- Information on track occupancy is important
- Information on track occupancy is stored twice (train report book in offering and accepting train reporting point)
- **But**: Information on track occupancy must be checked only once (when train shall be offered, but not for acceptance)
- In „Instructions on how to act“ the rule for the train acceptance is ambiguous („accept when no conflict exists“ – but what are the conflicts?)

**General findings**

- Rules must be formulated in a way that it can be checked against compliance unambiguously ⇒ no fuzzy formulation
- Rules must use clearly defined, unambiguously input and output
Conclusions

- The tool presents components and information paths of a system
- The tool highlights the safety-related components and information paths
- Human involvement and weaknesses in the rules for operation can be identified
- With this knowledge ways to support the staff in its tasks can be developed
  - staff can be relieved from safety-related tasks / replaced by more reliable systems and deployed in other services
- For analysis of further characteristics of the system more attributes can be assigned to the system elements (e.g. kind of processing unit, communication channel, ...)
- Computer supported analysis using a database ⇒ Assessment after modification of system / rules easy; only modified parts have to be updated
Thank you for your attention!

Contact

Dipl.Ing. Katrin Hartwig
Deutsches Zentrum für Luft- und Raumfahrt e.V.
Lilienthalplatz 7
38108 Braunschweig
Germany
Tel.: +49 (531) 295-3467
Email: katrin.hartwig@dlr.de