Paper from: *Computers in Railways VIII*, J Allan, RJ Hill, CA Brebbia, G Sciutto and S Sone (Editors).
ISBN 1-85312-913-5

Qualitative and quantitative safety assessment of ERTMS operating rules

E. El Koursi[1] and B. Kampmann[2]
[1]*INRETS-ESTAS, Villeneuve d'Ascq, France.*
[2]*SNCF, France.*

Abstract

This paper deals with the common operating rules assessment approach developed during the HEROE (Harmonisation of European Rail Rules for Operating ERTMS) project. This approach is based on the qualitative and quantitative analyses using a common operational diagram to represent each rule. After a brief presentation of the ERTMS (European Rail Traffic Management Systems) concepts and the HEROE project, the description of the assessment method will be made. The assessment will be specified and the phases of this assessment process will be detailed. The results of the qualitative and quantitative safety assessment of set of rules will be given and the finding will be discussed in the last section.

1 Introduction

The increasing need for railway competitiveness to extend the traffic flow beyond the borders between European states urge the railway authorities, the railway operators and the train operators to make the system interoperable, instead of mixing together national control-command systems. The technical interoperability is no sufficient to avoid the necessity for the driver to use a lot of operational regulations on different national railway networks where the rules applied can be very different from one network to another. To harmonise the

Paper from: *Computers in Railways VIII*, J Allan, RJ Hill, CA Brebbia, G Sciutto and S Sone (Editors).
ISBN 1-85312-913-5

technical and operational systems, the European Union launched in 1989 an integrated programme of research and development, in railway sector, to set up a common, coherent and consistent transport policy regarding safety and operational procedures. The objective is to develop a harmonised European railway network in order to fulfil the interoperability requirements and to improve and optimise the rail operation with high level of safety. The work, under this research programme, aimed at developing the ERTMS (European Rail Traffic Management Systems) with a generic control command system.
In the scope of ERTMS, the HEROE (Harmonisation of European Rail Rules for Operating ERTMS) project was launched in 1998. The main objectives of the European HEROE project were the development, harmonisation and assessment of rules and regulations for the new ERTMS control-command system in normal and degraded modes by taking into consideration the experiences gained from European High Speed Train: Eurostar and Thalys.
The common assessment approach of operating rules developed during the HEROE project approach is based on **the qualitative and quantitative analysis** by using a common operational diagram to represent each rule. Each operating rule in the operational diagram is split up in a series of essential exchanges between various system and environment elements (actors) including Driver, Train, Onboard systems, Trackside, Operators, Signalmen and others. This diagrammatic representation facilitates comprehension, correction and consistency checking for a given scenario. Once the total system exchanges and functions are mapped and captured in this graphical and simple notation, it is possible to identify specific actions, scenarios and circumstances requiring performance enhancement, risk mitigation, design changes, rules and procedural control.
After a brief presentation of the ERTMS concepts and the HEROE project, the description of the assessment method will be made. The assessment will be specified and the phases of this assessment process be detailed. The results of the qualitative and quantitative safety assessment of set of rules will be given and the finding will be discussed in the last section.

2 ERTMS concepts

The European Union launched in 1989 an integrated program of research and development in the railway sector, to set up a common, coherent and consistent transport policy regarding safety and operational procedures and to develop a harmonised European railway network in order to fulfil the interoperability requirements and to improve, and optimise the rail operation with a high level of safety. The work, under this research program, aimed at replacing the European Rail Traffic Management System/European Train Control System (ERTMS/ETCS) [1] with a generic system based on on-board command/control and safe radio communication (Global System Mobile for communication-Railway: GSM-R). The advantages of an international interoperable system can

Paper from: *Computers in Railways VIII*, J Allan, RJ Hill, CA Brebbia, G Sciutto and S Sone (Editors).
ISBN 1-85312-913-5

be summarised as:

- Cross border interoperability,
- Improvement of the safety of national and international train traffic,
- Improvement of international passengers and freight train traffic management,
- Shorter headway on heavily travelled lines,
- Possibility of step-by-step introduction of the new technology,
- Enabling Pan-European competition between the manufacturers of ERTMS/ETCS components; thus strengthening the position of the European railway industry on the world market.

The ERTMS system [2], a future unified standard European Train Control System (ETCS), can be divided into 5 progressive levels. The ERTMS/ETCS system is partly on the trackside sub-system (interlocks, control centres, etc.) and partly on the on-board sub-system (train and driver interface, ATP and ATC). A train equipped with ERTMS/ETCS on-board equipment always co-operates with the ERTMS/ETCS trackside equipment in a defined ERTMS/ETCS level. All transitions between levels are performed according to well-specified rules. ERTMS/ETCS [3] can be configured to operate in one of the following application levels:

- ERTMS/ETCS Level 0 means that the train is equipped with ERTMS/ETCS on-board and is operating on a line without ERTMS/ETCS or a national system.
- ERTMS/ETCS Level STM means that the train is equipped with ERTMS/ETCS on-board operating on a line equipped with a national system with which it interfaces by use of a Specific Transmission Module,
- ERTMS/ETCS Application Level 1 means that the train is equipped with ERTMS/ETCS operating on a line equipped with Eurobalise (non continuous transmission). Optionally, also with in-fill transmission, using Euroloop, or Radio in-fill,
- ERTMS/ETCS Application Level 2 means that the train is equipped with ERTMS/ETCS operating on a line controlled by a Radio Block Centre and equipped with Eurobalises (for reset of odometry) and Euroradio (continuous transmission). The integrity proving is performed by the trackside.
- ERTMS/ETCS Application Level 3 is similar to level 2 without track circuits. Train location and train integrity supervision are based on the information received from the train.

It is possible to superimpose several application levels in parallel on the same track. For example, trains can operate without a train integrity device in level 2 and in parallel with trains equipped with train integrity device in level 3.

Paper from: *Computers in Railways VIII*, J Allan, RJ Hill, CA Brebbia, G Sciutto and S Sone (Editors).
ISBN 1-85312-913-5

3 HEROE project

The implementation of the unified ERTMS, encouraged by the European Commission, allows the Railways to approach global interoperability if they can set up common rules and regulations in accordance with their safety Law. In order to achieve this essential objective under the management of the European Economic Interest Group (EEIG), the HEROE project was launched in 1998. It was aimed at harmonising the operating rules and simplifying the safety regulations specific to signalling and rail traffic management on the networks where ERTMS is to be implemented. The HEROE project [HER.00] involves 14 European partners: EEIG (B), NS_Railned (NL), Railtrack (UK), DB (G), RENFE (SP), FS (IT), GEC_ALSTOM (F), INRETS (F), TÜV EURO RAIL (G) TIFSA (SP), DITS (IT), SNCF (F), ERRI (NL) and UIC (F). Principally, the HEROE project aims at elaborating the common rules and regulations for ERTMS and to set a strategy for managing the period of co-existence between old systems and ERTMS. The HEROE project is structured in order to:

- Draw up appropriate rules to ERTMS operation to allow an operational interoperability as broad as possible and to harmonise rules and regulations for the new ERTMS control-command system in nominal and degraded situations,
- Ease a fair competition by fixing common levels of safety particularly for degraded situations which means to agree with a common risk analysis method,
- Establish a pre-standardised set of rules and regulations in regard to each operating situation.

The project was dedicated to the development of harmonised rules and to the demonstration that they are coherent with the ERTMS/ETCS system design. The assessment team was independent from the one in charge of producing the rules and the procedures. The rules for operating ERTMS, as developed by operators, were assessed with regard to safety aspects. The assessment of the rules and procedures takes into account normal operating conditions as well as degraded modes. The qualitative assessment first checks to assure that the rules will be adequately safe when applied. Then the assessment performs a quantitative analysis, evaluating the probability that the operators made errors in applying the rules.

4 Assessment of the operating procedures and principal rules for operating ERTMS

The operating rules have been developed using the experience and the expertise of European railway operations specialists. The rules are based upon the functionality described in SRS (System Requirement Specification) document agreed between ECSAG (ERTMS Core SRS Assessment Group) and UNISIG [2 and 3] in early 1999. These rules refer specifically to the use of ERTMS and are provided to complement any existing national railway rulebook. The rules are designed with the purpose of allowing interoperability throughout Europe where

Paper from: *Computers in Railways VIII*, J Allan, RJ Hill, CA Brebbia, G Sciutto and S Sone (Editors).
ISBN 1-85312-913-5

ERTMS has been implemented. Each rule described within the HEROE is structured within the following framework:

- Status,
- Reference,
- Situations in which the rule is used,
- Definition of the operational rule,
- Rationale/fundamental,
- Addenda,
- Links with other subjects,
- Assumptions/system behaviour,
- Questions to be solved,
- Problems with existing national rules,
- Recommendations to solve problems with existing national rules,
- Operational test scenarios.

In principle, ERTMS operational rules are elaborated by the Work Package Group A [4] and assessed by an independent group within the context of Work Package Group B [5] with other groups providing support services. In this task, the rules for the operation of ERTMS, as elaborated by a panel of experts, are assessed with the view to safety. The evaluation of the rules and procedures takes into account normal operating conditions as well as degraded modes. The global approach is based on three items:

The qualitative assessment [6] checks that the safety will be fully effective if the rules are applied correctly. In order to perform an impartial and objective assessment of the rules and procedures, the members of the assessment group (Work Package B :WPB) are independent from those in Work Package Group A who are in charge of producing rules.

The quantitative assessment [7] consists of evaluating the probability that the operators made errors in applying the rules (due to their complexity or to human errors) and evaluating the relevant consequences from the safety viewpoint.

The tests of the rules through simulation [8] are used to detect incoherence and inconsistency of defined operational rules. The simulation is particularly adapted to test the driver's behaviour in normal and degraded situations.

5 Assessment Template of qualitative and quantitative assessment

The proposed methodological and systematic framework for assessment comprises a number of diverse processes. It synthesised to satisfy the requirements of a systematic and efficient environment for Qualitative and Quantitative assessment of ERTMS/ETCS operational rules. This view of the operational railway is applicable to any particular configuration (Level) of ERTMS. Each state in the operational diagram is divided into a series of essential exchanges between various system and environment elements (actors)

Paper from: *Computers in Railways VIII*, J Allan, RJ Hill, CA Brebbia, G Sciutto and S Sone (Editors).
ISBN 1-85312-913-5

including Driver, Train, Onboard systems, Trackside, Operators, Signalmen etc. Figure 1 depicts one such schematic diagram. This diagrammatic representation facilitates comprehension, correction and consistency checking for a given scenario. It also lends itself to a hierarchical decomposition of complex problems until adequate level of detail and simplicity is arrived at while still maintaining the big picture. The same environment and style of system representations have been employed to identify potentially hazardous scenarios likely to lead to accidents and incidents which underpin the safety analysis of ERTMS/ETCS. Once the total system exchanges and functions are mapped and captured in this graphical and simple notation, it is possible to identify specific actions, scenarios and circumstances requiring performance enhancement, risk mitigation, design changes, rules and procedural control.

5.1 Qualitative assessment

The assessment approach is depicted in a template, split into 5 key parts as shown below. The subdivisions of the template are intended to aid simplification, record keeping and modularity for work sharing. The process necessitates each and every rule to be assessed in accordance to Parts 1-4, broadly corresponding with the qualitative approach. Part 5 is reserved for rules considered critical or with significant potential to cause harm should it fail or be misapplied. Part 5 therefore broadly corresponds with the quantitative assessment requirements.

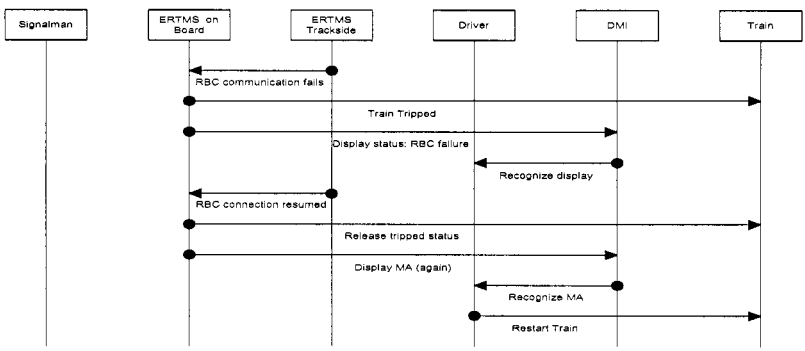
5.1.1 Part 1- Rule Definition

It contains fields that provide tractability, clarity and describes the aims/objectives of a given rule. The following elements are defined:

- The railway circumstances for which the rule is derived (Scenario),
- The specific aspect of the scenario (scene),
- Why a rule is needed for the given scenario-scene (rationale),
- The title and definition of the rule (Rule),
- What the rule is expected to achieve (Purpose).

5.1.2 Part 2 – Task Analysis

This reflects the first and most fundamental aspect of analysis carried out by assessor team. The input rule from Part 1 is analysed in detail and represented in UML format (Figure 1).



Paper from: *Computers in Railways VIII*, J Allan, RJ Hill, CA Brebbia, G Sciutto and S Sone (Editors).
ISBN 1-85312-913-5

Figure 1: Task analysis of the relationship between actors involved of a rule

The analysis involves identification of all the key players (actors) involved in the application of a given rule, the time sequence of actions to be taken and the expected responses. This would generally include people, procedures and the technical system (automation). All actors are depicted in boxes and the required series of actions and responses shown as arrows starting from the top of the diagram. Each arrow indicates the source of the action or response and the destination/intended recipient. The specific cases of conditional actions and responses may be depicted by decision diamonds, which leads to different actions/responses.

5.1.3 Part 3 – Performance Analysis

This part is intended to provide an environment for recording of the specific concerns (hazards) and a measure of effectiveness for every rule. The hazards are identified through scrutiny of the Task Analysis depicted in Part 2. For each adverse context, a number of brief descriptions are required. The following fields are defined for Part 3:

- A particular action/exchange with a potential to cause an accident (Hazard),
- The probability that the hazard will occur (Likelihood) [table1],
- Any possible cause for the occurrence of the hazard (Cause(s)),
- The likely accident(s) which may arise from the hazard (Consequence(s)),
- How often is the rule likely to be applied to attain its objectives/purpose (Effectiveness) [table 1].

The allocation of the hazards occurrence is based on the classification given in the table 1. Five levels are determined: frequent, not rare, almost rare, rare and extremely rare. The effectiveness of a given rule can be measured in terms of successful application of the rule [table 1]. Five levels are identified : zero, low, medium, high and almost full.

Part 3: Performance Analysis - Likelihood (probability that the hazard will occur)		
Level 1	< 0.0001	Extremely rare: order of magnitude of critical failures in safety technical devices
Level 2	0.001 - 0.0001	Rare: order of magnitude of human errors in normal situations
Level 3	0.01 - 0.001	Almost rare: order of magnitude of human errors in particular (stressed, critical, etc.) situations
Level 4	0.01 - 0.5	Not rare: higher than any order of magnitude of human errors
Level 5	> 0.5	Frequent: more likely than it will not occur

Paper from: *Computers in Railways VIII*, J Allan, RJ Hill, CA Brebbia, G Sciutto and S Sone (Editors).
ISBN 1-85312-913-5

Table.1: Classification of the performance and the effectiveness of the rule

Part 3: Performance Analysis - Effectiveness (how often is the rule likely to be applied successfully)		
Level 1	0%	Zero: problems will sure happen (e.g. the problems are caused by the rule)
Level 2	0% - 50%	Low: in the most cases problems will occur
Level 3	50% - 95%	Medium: occurrence of problems should be considered in normal operation
Level 4	95% - 99%	High: usual accepted standard for problems in not safety critical situations
Level 5	> 99%	Almost full: occurrence of problems will be exceptional

5.1.4 Part 4 – General Feedback

This part applies to recommendations for rule enhancement/correction in the light of the Task Analysis (Part 2) and the Performance Analysis (Part 3). The fields in this part essentially carry proposals for correction or enhancements as identified by the assessor team. They give an overall feel (score) about the key features of the rule and its status. The essential fields in this part are as follows:

- Any suggested correction or improvement in a rule and what is the nature of correction/improvement *(enhancement option)*
- What does the option relate to *(which hazard ?)*,
- What would the correction/enhancement achieve *(Value/Impact)*,
- Judgement on overall clarity of the rule *(Clarity)*,
- Judgement on overall complexity of the rule *(Complexity)*,
- Judgement on the overall relevance of the rule to the scenario/scene *(Relevance)*.

5.2 Quantitative assessment

5.2.1 Part 5 – Quantified Analysis

This part is intended to provide a diagrammatic and more thorough analysis of the rule, culminating in the prediction of accidents and incidents. Quantification of the structures in the analysis will enable a probability to be computed for :

- Each accident type predicted through analysis,
- Each incident,
- Rule being effective.

The information fields for the Quantitative Assessment must accommodate as many Barriers, Channels and Consequences as appear within the diagrammatic

Paper from: *Computers in Railways VIII*, J Allan, RJ Hill, CA Brebbia, G Sciutto and S Sone (Editors).
ISBN 1-85312-913-5

assessment. The reference, description, numerical value and rationale for each Barrier, Channel, Consequence are given to globally assess the rule. The description and the total accident frequency forecast in Scientific Format are also defined for the assessment.

5.2.2 Acceptance Criteria of quantified analysis

The quantitative analysis, in terms of per demand likelihood to lead to a safety related accident resulting from the misunderstanding or misapplication of rules is the basis of the quantitative acceptance criteria for each operating rule. The quantified criteria for acceptance or rejection of a rule are determined by the expert panel representing the main partners of the project (Railway operator, industrials and safety experts). The agreed probability for accident cause is defined. The Rule Integrity Level (RIL) is used to asses the potential of a given rule leading to the accidents generated by misapplication of a rule (Table.2). The RIL classification from 1 to 4 (High being most critical) establishes the level of vigilance needed for successful application of a rule.

Table.2: Rule Integrity Level for Quantitative classification

Rule Integrity Level (RIL)	Accident probability per demand	Classification	Guidance
1	$<=10^{-7}$	Routine	Can used as defined
2	$<=10^{-6}$	Exceptional	Requires vigilance
3	$<=10^{-5}$	Critical	Requires independent double checking
4	$<=10^{-4}$	Catastrophic	Should not be applied except in extraordinary circumstances and with multiple diverse supervision and checking

5.3 Tools

The proposed approach and template are captured in the form of a database application to support the systematic qualitative and quantitative analysis and assessment of ERTMS rules. A computer application, HAT (HEROE Assessment Tool) [9] has been specified and developed to facilitate consistency and systematic approach to the analysis.

5.4 Computational results

The computational results are presented in the table 3.

Table.3: Results of assessment

Assessment activities	Rules examined by assessors	Quantitative analysis	Qualitative analysis	Tested on simulator
Number of rules	*49*	*30*	*20*	*15*

Paper from: *Computers in Railways VIII*, J Allan, RJ Hill, CA Brebbia, G Sciutto and S Sone (Editors).
ISBN 1-85312-913-5

6 Conclusion

The qualitative assessments have been made for 39 rules of ERTMS and involved a panel of European experts in railway sectors. The template, supported by a HAT tool, increases the quality of work among experts by using the same data base. Using two assessment passes, the expert panel realised that some rules are inconsistent and incoherent and have to be refined. The quantitative assessment activities were focused on the rules identified by the qualitative assessment as very critical. Twenty (20) rules have been quantified and the safety barriers identified to cope with the hazards related each rule. Taking into account the result from the qualitative analysis, some rules have been identified as inconsistent. The testing of the 15 rules through simulation was carried out by three drivers from SNCF, NS and RENFE in order to check the applicability and the suitability of the rules. Such tests were used for evaluating the ergonomic and the linguistic issues and for integrating the stress and the high speed factors to detect incoherence and inconsistency of defined operational rules. The simulation was particularly adapted to test the driver's behaviour in normal and degraded situations.

7 References

[1] AEIF, The Trans-European High-Speed Rail System, Technical Specification for Interoperability Control-command and Signalling Subsystem, V2.07, May 8, 2000.
[2] ERTMS, Functional Requirements Specification, A200/FRS, Version 4.27, 17 November. 1999
[3] HEROE project WPA, ERTMS Users Group, Operational Principles and Rules, 30 October 2000, version OT.
[4] UNISIG System requirement Specification, ERTMS/ETCS-Class 1 Subset 026, Issue 2.0.0, 22 December. 1999.
[5] HEROE project WP group "the ERTMS Users Group, HEROE project WPB, Final report" , ref 00TA115, 10.01.2001, 19p.
[6] HEROE project WP group "the ERTMS Users Group, HEROE project WPB, Report task 3.1, Qualitative Analysis" , 00TA112, 09.01.2001, 21p.
[7] HEROE project WP group "the ERTMS Users Group, HEROE project WPB Quantitative Assessment", ref 00TA113 1 04.01.2001, 27p.
[8] HEROE project WP group "the ERTMS Users Group, HEROE project WPB Report on simulator tests in Madrid", 00TA111, 04.01.2001, 27p.
[9] HEROE project WP group "the ERTMS Users Group, HEROE project WPB HAT database. Qualitative and Quantitative Assessment », 00TA114, 04.01.2001, 203p.