# The ERTMS railway signalling system; deals on wheels?
# An inquiry into the safety architecture of high speed train safety

John Stoop (1, 2) & Sidney Dekker (2)
(1) Delft University of Technology, the Netherlands
J.A.A.M.Stoop@tudelft.nl
(2) Lund University, School of Aviation, Sweden
Sidney.Dekker@tfhs.lu.se

**Abstract.** ERTMS is the acronym for European Rail Traffic Management System. ERTMS is the future standard for a European train signaling system, enabling interoperable use of the European network without adapting rolling stock to different national signaling systems. It facilitates crossing national borders with a design speed of 300 km/hour eliminating time-consuming change of locomotives at borders. ERTMS causes the loss of visual detection as a safety separation principle. It applies automatic trajectory clearance by automatic train detection and integrity control and a moving block protection, depending on train characteristics. The driver only has a monitoring task and is no longer in control. Ultimately, train control automation aims at driver free operations by Automatic Train Operations. Such a fundamental change in safety assurance concepts requires a most reliable engineering design, implementation and operational strategy. In this contribution, the potential of resilience engineering in designing an innovative alternative is explored.

## 1 INTRODUCTION

ERTMS is a part of the renovation and upgrading of national railway systems, facilitating interoperability on the EU rail network and fully software controlled train surveillance. ERTMS is a trend shift from technical compatibility across nations towards standardisation and harmonisation on the main EU network corridors. The Dutch HSL is part of Paris-Koln-Amsterdam-London corridor.

For the Dutch ERTMS development several political choices have been made:

- innovation in Public-Private Partnerships in contracting; mixing public and private interests.
- the development and implementation of technology are conducted concurrent instead of sequential. A simultaneous development of standards and software components is taking place, assuming a pragmatic Off the Shelf availability of components from various industrial consortia.

  The Dutch High Speed Line is the first of international High Speed train corridors to deploy ERTMS and is deployed on the corridor Amsterdam-

Antwerp. The level migration from ATP level 1 to full automation level 3 is foreseen in three steps.

| Function allocation | Signalling | Train detection |
|---|---|---|
| Level 1 | track | track |
| Level 2 | train | track |
| Level 3 | train | train |

There have been several disruptions in implementation resulting in software upgrades. ERTMS version 2.2.2 proved to be cross-supplier incompatible but was contractually based deployed, while version 2.3.0 would be the new operational standard. There was no anticipation on necessary, continuous hot upgrades in practice. The level migrations (from level 1 to level 2) were implemented in the Netherlands without fallback options of proven technology such as with the French TVM 430 for the TGV. As a result of time delays and cost increases, the necessity for upgrades and migration and expansion of the testing period was repeatedly discussed in Parliament. These discussions lead to an inquiry into the ERTMS deployment strategy.

## 2 HISTORICAL DEVELOPMENT IN RAILWAY CONTROL

In developing railway signalling 3 historical phases can be discriminated:

1. At the dawn of the railway industry in the early 19th century, the system was modelled after the Napoleonic military organisation. Such an organisational structure served the purpose of compensating the deficiencies in safety technology at the time. A strict compliance with time tables and a scrupulous operation was the dominant safety concept to separate trains in time. Safety technology on the railways developed gradually over 150 years. Before technical fallback options were introduced, safety was dependent on self-disciplining and an almost flawless human compliance with regulations. A strict command and control structure by disciplining a large number of railway employees provided the necessary safety on the railways.

2. Enhanced automation. With the aftermath of a major railway disaster at Harmelen in 1962, the Dutch railway systems entered a second phase of automatic train control by introducing the ATP (Automatic Train Protection) system. The gradual implementation of this ATP system has covered a period of about 40 years since.

This system enabled the railways to establish a more accurately position finding by indication occupancy of a static block by a train on a display at the train control centre. Conflict resolution was enhanced by bringing the trains to an automatic and failsafe standstill if the separation of trains was violated by passing a signal at danger. Because the organisational concept of hierarchical decision making remained, a strict separation was maintained between train control and train capacity management. To avoid conflicting interest in decision making within the organisation conflict anticipation was resolved as a responsibility of the capacity management organisation, while conflict resolution was the responsibility of the train control centre.

3. ERTMS. ERTMS can be considered as the next phase in controlling train driver behaviour by reducing his role to monitoring the system, anticipating intervention in case of disruptions and deviations, evolving into a final driverless train system.

# 3 CONCEPTUAL LIMITATIONS

Full automated control systems however have their conceptual limitations. For reasons of economy of scale and cost reduction, many local train control centres are closed down, replaced by a few large regional centres. A remote situation awareness of such a centralised system under production pressure increases the workload of the controllers in case of traffic flow disruptions and incident handling. Additionally, performance based punctuality demands and financial incentives in maximising track capacity initiates conflicts of interest among the business interests of various privatised stakeholders (WRR 2008). This creates a trade-off between short term economical aspects against competing long term public values, creating a 'multiple principal agent problem' (Steenhuisen and Van Eeten 2008). This puts train controllers in a coping situation in which the specialised functionality of their organisation makes their tasks manageable and clearly demarcates their responsibilities, eliminating competing values from their scope. Meanwhile, however, frontline operators face these conflicting values as they emerge in practice. Automation finally, has its limitations by design. With the increase in intensity, the system is loaded to its design limits. The fault tolerance in hierarchical systems increases quadratically with intensity. About its saturation point, the traffic flow becomes instable. At fault, operator induced oscillation becomes possible; fault handling may cause abrupt and progressive collapse of the overall system. To avoid initiating disturbances, an even stricter task performance of the train driver is required. Increasing the punctuality of the time table under high traffic intensity conditions demands an increasing control effort by the traffic controller and train drivers. This aggravates the tactical and operational cognitive workload of the traffic control centres who are forced to communicate simultaneously with several train drivers. Eventually a gridlock situation occurs due to which all traffic operations must be terminated by a failsafe system breakdown and gradual and safety critical The underlying organizational mechanisms which threat public values such as safety versus private business values can be identified as coping behaviour in order to deal with conflicting values (Steenhuisen & Van Eeten 2008). A simultaneous removing of safety margins and introducing conflicting goals during operations is a process which may has unforeseen consequences for the operators. Does this however mean that they are unpredictable because there were not designed into the technical system and reveal themselves over time in practice as emergent properties in hybrid systems? If so, will it suffice to discipline organisations with advanced contracts and incentives, piling up requirements without clarifying inevitable trade-offs?

Or can we design resilience into the system to cope with the change in nature, and if so, how should we do that?

Two principal strategies are applied:

- recognition of value conflicts and subsequently, a structuring of the process of communication, coordination and cooperation among all stakeholders in their decision making processes, coping between quantifiable private performance indicators and qualitative public values;
- elimination of the human involvement in disguised bad performance due to ambiguous and hybrid decision making values by developing an innovative train control system, based on modern technology and a new generation of signalling systems.

# 4 STRUCTURING DECISION MAKING PROCESSES

During the High Speed Line project development in the Netherlands, several unforeseen project cost increases and planning delays emerged in deploying the train control software. These disruptions caused questions in Parliament on clarification into the reasons for the software upgrade, necessary migration time and the reasonability and fairness of the testing period. During the inquiry, several value judgements became visible dealing with the project organisation and technological scope.

The main conclusions of the investigations into the ERTMS software upgrade were:

- the institutional environment has complicated the development and implementation of the project. The divisions that have been created during the project between design and construct of the hardware components and the contractual arrangements between stakeholders created a necessity for a complex interface management. This interfacing has not been accomplished
- the necessity to create oversight emerged only by the end of the project. There was no role for a systems integrator, responsible for the integral coherence of the overall system. The pivotal role of ERTMS became emergent at the end of the project in the full scale testing phase of the integral system
- the technological development of ERTMS was underestimated. There has been a continuous tension between incremental progress and implementation in an existing railway network on one hand and the ambitions of innovative ERTMS and public-private partnership arrangements on the other hand.

Consequences of several technological design decisions should have been submitted to a pro-active safety assessment procedure. Several Points of No Return in the design process have been passed without oversight of their consequences:

- a choice for a new signalling system which was not yet operational at the time, was not compensated for by a qualified fallback option
- the choice for an innovative ERTMS system in the Netherlands was not in harmony with the more incremental process and evolutionary development of the Belgian signalling system on the same corridor Amsterdam-Antwerp
- the choice for connecting the Dutch and Belgian system manufactured by two different signalling system consortia at the country border forced the project management to develop a gateway causing high costs and considerable delays in delivering the integrated system for testing and operations
- a contractually based testing and deployment of ERTMS version 2.2.2 took place while version 2.3.0 would become the new standard, causing unnecessary complications, costs and delays
- the development of ERTMS was considered a conventional technical engineering effort, enabled by a decomposition of the system components in autonomous position finding and communication subsystems. Development and manufacturing of these components was subcontracted across competitive consortia. Each consortium was assumed to be able to deliver these components ‘off the shelf’ as proven technology
- no precautionary measures were taken to assure a smooth and efficient frequent upgrade of the signalling software during its operational phase.

## 5 TOWARDS FULL AUTOMATION

The process industry applies a design concept in which humans are fallible factors and eliminated by design from the system by automation. Their remaining role is restricted to complying with rules which have been imposed by management. There is no room for the operator in taking critical decisions. This design doctrine has become the role model for modern safety management.

Transport systems however, apply two completely different design principles. First, at the control level the system is designed as a support for the operator; it is a *human centred design* with delegated responsibilities. Second, there is a strict separation between the planning and control level with respect to capacity management and traffic control. It is a distributed responsibility.

First, the delegated responsibility. To prevent accidents and incidents between vehicles, they are separated in time, in distance and by visual detection. This creates a triple redundancy. These three principles are under pressure. High speeds make a direct outside observation impossible. To maximize the availability of capacity and interconnectivity of the network, a maximum traffic density is desirable. Dynamic control opens up the opportunity for maximizing punctuality and minimizing tracking times. Consequently, separation in distance is all that is left. This put high demands on technology and requires good faith of the operator in the supporting technology in case of 'beyond design' situations.

Second, in addition to delegated responsibility there is a distributed responsibility. We speak separately of traffic management in addition to traffic control. This separation is introduced in order to prevent a conflict of interest in an organisation where one individual or authority should be responsible for balancing safety versus economy. This principle also has come under pressure. Full automation eliminates the operator and traffic controller, replacing them by computers, in which a black box defines what experience and expertise should be canned into computer algorithms, complying with predefined rules and procedures. Such a view captures any technological development at a rule based level of decision making. As a consequence non-routine situations will emerge as unforeseen properties when the system has to perform under pressure.

This reductionistic view on full automation denies the operator a possibility to learn from experiences. The collective knowledge of operators represents a capital for the sector which exceeds any company level. By this feedback from practical experience, transport systems could develop into Non Plus Ultra systems because practical experiences were rapidly incorporated in operations. The erosion of both delegated and distributed responsibilities leads to so-called sacrificial decision making. Risk decision making is reduced to a single actor issue. If such safety critical decisions are not explicitly countered in the conceptual design phase or at an institutional level, catastrophic consequences may occur in practice. In long living systems within a global network context, midlife updates create a dilemma from a systems perspective: technological innovation takes place in a saturated and matured system, where performance optimization takes place from an extended single agent perspective due to privatisation and public-private partnerships networks.

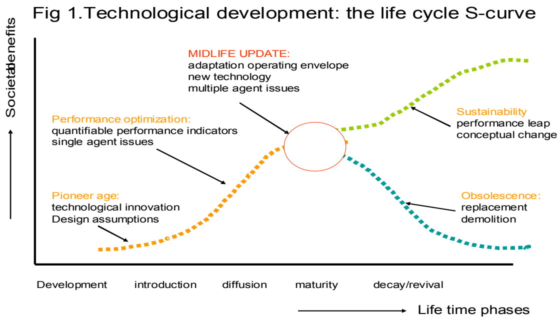


**Fig. 1.** Technological development: the life cycle S-curve

## 6 RESILIENCE ENGINEERING

Safety can be considered a normal consequence of performance variability which should be controlled rather than constrained (Hollnagel 2008). The ability to effectively adjust a systems functioning *prior to* or *following* changes and disturbances can continue its functioning after disruption or mishap, while under continuous stresses. Therefore systems should be able to cope with responses to the critical, potential and factual situations. A transparency in various system states should be available supported by the ability to predict, plan and produce.

But what if such transparency is not possible? What if we cannot cope with system complexity and complex causality or lack self-organising and learning behaviour? If we cannot analyse the complex reality and cannot achieve consensus, are we deemed to restrict ourselves to a battlefield of subjective opinions, submitted to political will and governance resolve (Rosenthal 1999)? Or do we restrict ourselves to a lower systems level of a single agent at the organisational level, accepting sacrificial losses? Resilience has its roots in warfare, where its essence is defined as the ability to make sense of its environment, to generate strategic options and realign its resources faster than its rivals (Hamel & Valikangas 2003).

Secondly, do we accept a pessimistic vision in which engineering design is reduced to a process mixing reuse of known solutions with some new technology and processes, with a sauce of varying thickness of creativity poured over them. Such a concept denies the potential of innovation and technology as a flywheel for progress despite political and institutional controversies (Freer 1949). The potential of offering opportunities in solving complex problems by taking into account the dynamics, multidisciplinarity and complexity of systems enablers a transition into a third systems dimension in applying chaos and complexity theory and a re-introduction of the conceptual design phase in system change (Bertuglia 2005).

This third dimension identifies dynamic systems behaviour beyond the level of linear behaviour. Dynamic properties are identified such as deterministic chaos, emergent behaviour, self-organisation, self-conformity resonance and bifurcations. From a safety perspective, the most interesting parameter is the existence of multiple system states. This eliminates the debate on acceptable and quantifiable system safety performance levels, replacing it by an insight into inherent dynamic properties.

Fig 2. A third system dimension

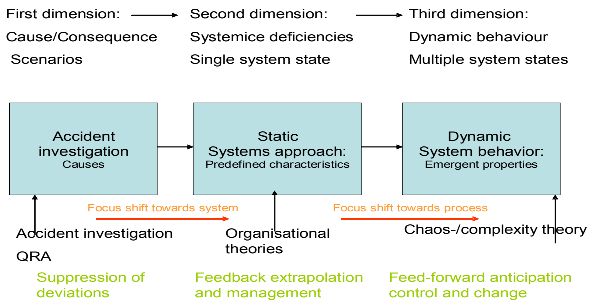


**Fig. 2.** A third system dimension

## 7 TOWARDS A THIRD PHASE IN TRAIN CONTROL

This systems engineering potential has been demonstrate in a feasibility study into the deployment of a new railway concept. A new train control concept was developed in analogy with the Free Flight concept in aviation; the Free Ride concept. Four innovations were incorporated in the Free Ride concept:

- transfer or responsibilities for operational control and safety from traffic control towards the train driver and a transfer from a track to vehicle-bound control
- replacing a strict hierarchical planning of capacity by a dynamic and flexible management of disruptions and faults
- introduction of a self-learning software based on principles of Business Model Driven Engineering, Functional Request Specifications, Use Cases, Operating Envelope and elaboration of a Traffic Management Level
- certification and validation at an integral systems level, replacing a repetitive upgrade and migration of component certification.

The Free Ride concept eliminates the conventional conflict of interest between safety and control, by applying a performance based control strategy instead of a compliance based approach, restricting incident management and handling to the local level of the network.

In analogy with a Harbour Master and Airport Master, a Rail Master is allocated the strategic safety responsibility in the decision making on dealing with other system performance requirements. Finally, a new international, sectorial entity is required in order to assess safety at an integral systems level with respect to systems integration.

Replacing a technological/substantive approach by a process/negotiative approach in which process drives out content, has created disaster, as demonstrated by the introduction of ERTMS in the Dutch railways. Combining three rationalities of a technological construct, a social construct and a local construct facilitates communication, learning and adaptation across actors at all levels and life-cycle phases of a system. Each rationality contributes to the overall systems design: from a technical perspective a dynamic modelling software development is required, from an local operator view, a new cognitive engineering modelling is a prerequisite for delegated responsibilities, from a social perspective new organisational and institutional entities have to be incorporated in the systems concept.

## 8 CONCLUSIONS

In assessing the safety of the ERTMS system development some conclusions can be drawn:

- actors are located at three different phases in S-curve, creating value and control conflicts. A multi-agent process approach is emergent, but not sufficient;
- technological innovation creates major uncertainties: engineering is not a standard technology application which can be bought Off the Shelf: it also contains software design concepts change, system integration, oversight/consequence analysis and integral system certification;
- shifting from a technological perspective in systems development towards a social engineering is not sufficient; there is a need to integrate the technical, human and organisational/institutional design across the various system life phases, taking into account the various system states that may exist in practice.

Resilience engineering consists of three dimensions: technological engineering design, process design and a systems architecture dimension. Without such an encompassing approach, introducing ERTMS is nothing but deals on wheels.

## REFERENCES


Freer (1994). ICAO at 50 years: Riding the Flywheel of Technology. *ICAO Journal Vol.49 No 7, September 1994, pp.19-32*

Rosenthal (1999). International *Conference on the Future of European Crisis management. The Hague, November 7-9th, 1999.* Challenges of crisis management in Europe.

Hamel and Valikangas (2003). The Quest for Resilience. *Harvard Business Review, reprint R0309C, 13 pag, September 2003, wwwhbr.org*

Bertuglia & Vaio (2005). Non-linearity, Chaos and Complexity. *Second edition, Oxford University Press, Oxford*

Stoop et.al. (2007). HSL safety signalling system ERTMS. An independent investigation into the usefulness of adapting the ERTMS safety signalling system. *Commissioned by the Research and Verification Department of the Dutch Parliament.* Delft University of Technology, 23 May 2007 (In Dutch with English summary)

Stoop and Dekker (2007). Are safety investigates proactive? *33rd ESReDA seminar Future Challenges of Accident Investigation. Ispra, Italy, November 13-14*, *2007*

Hollnagel (2008). Remaining Sensitive to the Possibility of Failure. *Ashgate Studies in Resilience Engineering*

Steenhuisen and Van Eeten (2008). Invisible Trade-Offs of Public values: Inside Dutch railways. *Public Money & Management, pp 147-152, June 2008*