Vernez, D. ; Vuille, F. **Method to assess and optimise dependability of complex macro-systems: Application to a railway signalling system.** Safety Science, 47(3):382-394, 2009.

| | |
|---|---|
| Postprint version | Final draft post-refereeing |
| Journal website | http://www.sciencedirect.com/science/journal/09257535 |
| DOI | doi:10.1016/j.ssci.2008.05.007 |

# 1 Introduction

## 1.1 Complex systems and dependability requirements

Achieving a high degree of dependability (safety, reliability, availability, etc…) has obvious human, economic and potentially environmental advantages. In spite of this motivation, such a high-minded objective nevertheless represents a genuine challenge when considering complex macro-systems, for which intuition and experience are not sufficient to comprehend the system in its minute details, while keeping a global understanding of the interaction occurring at system level. Possible deviations and interferences between components are numerous, while the required data is spread amongst a large number of stakeholders involved in the system development and operation. Worse, as systems are becoming more and more specialised and dedicated, the availability of existing dependability data describing the performance of such systems is limited. This is particularly true for innovative systems, for which no accident or incident statistics are available.

Modern transportation systems are good examples of large and complex systems. Due to the development of automation, networking, modal transfer and to the general increase of transportation speed (for improved mobility), the number of interacting components or subsystems has increased drastically over the last 20 years. Several standards and recommendations regarding dependability have been developed over the last decades to cope with the increasing complexity of transportation systems (Høj and Kröger, 2002). Developers of safety critical systems are more and more frequently requested to provide system safety assessments to the regulatory authorities, often referred to as "safety case". Such formal certification procedures exist for instance in aerospace (EUROCAE/SAE aerospace guidelines) and railways (CENELEC railway standards and IEC-61508). In both sectors, safety standards exist at the hardware/software level and at systemic level. However, while the recommendations at the hardware/software level are quite specific in terms of design and performance, systemic recommendations only specify global objectives and generic procedures. Given that the most adequate approach to fulfil the safety objectives of a system depends on its actual characteristics such as size, complexity, level of innovation, etc.,
systemic standards do not require specific methods or assessment tools.

Safety standards in the transportation sector are virtually all based on a similar philosophy (Papadopoulos and Mc Dermid, 1999). Their goal is to provide sound guidelines that help the designers to provide procedural and technical evidence of the system compliance with safety and reliability recommendations. Procedural evidence is achieved by following specific procedures for the system development and safety assessment. Technical evidence is obtained through the quantitative demonstration that the engineered system reaches a required level of integrity. To fulfil the latter requirement in complex systems, a partitioning in sub-systems is usually recommended. Safety and reliability specifications are then allocated to the different sub-systems and system components according to the system break-down. The developers/suppliers are thus usually bound to demonstrate the compliance of their subsystems with these requirements by using specific inductive or deductive analysis methods.

## 1.2 Pitfalls in optimising dependability of complex macro-systems

Complex macro-systems are usually partitioned into smaller sub-systems, the design and production of which are distributed to independent suppliers. Global performance requirements are broken-down and allocated to the individual subsystem.

Optimising the dependability of the global system with such project architecture is difficult and may lead to a dangerous overestimate of its availability or safety. Numerous challenges and pitfalls, of procedural or technical nature, await the system developers. Although the common pitfalls of risk assessment are well known (Gadd et al., 2004), avoiding them in the context of macro-systems remains difficult. Frameworks have been proposed to optimise, in a rational way, the design of such systems (Melchers, 2001; Kââniche et al., 2002; Bate and Kelly, 2003). Three pitfalls are of particular relevance in the context of macro-systems:

- lack of system overview
- conflicting objectives or unclear distribution of responsibilities between the actors involved
- lack of relevant data to assess the system performances

### 1.2.1 Lack of overview

In his review of system design optimisation, Melchers (2001) points out that: (1) the optimisation studies are usually focused on a specific part of the system (a subsystem) and that, (2) the focus is on technical aspects.

The focus on independent subsystems is strongly influenced by system boundaries and partitioning. The development of each subsystem is assigned to distinct groups or specialists, who produce their own safety and reliability data. As each subsystem has its own requirement specifications, their respective performances are usually assessed and analysed individually. The system overview is then built through the “simple” summing-up of the individual sub-system’s performance. Interactions between subsystems (functional interaction, common cause factors) being hence neglected, this may lead to serious overestimates of the global system performance.

“Narrowing” the dependability assessment to technical aspects is also a common tendency. The influence of the system environment is neglected, which may lead to a significant discrepancy between the theoretical and effective performance of the system. This often results from a lack of clarity about the respective responsibility boundaries of the actors involved (operator, suppliers, authorities), leading to situations where each actor tries to restrict as much as possible the scope of its own responsibility, hence implicitly increasing that of the others.

### 1.2.2 Conflicting objectives

The suppliers/developer and the system’s owner (the customer) have divergent needs and objectives. While the suppliers must demonstrate the proficiency of his own subsystem or component, the owner’s responsibility is more contextual. He must ensure that the system, in its physical and organisational environment, will work as expected. The need for global performance indicators is also shared by the Authorities, although their concern is usually limited to safety aspects. Understanding each actor’s goals and responsibilities towards risk and reliability assessment is of utmost importance because it defines the focus and boundaries of their respective work. When these limitations are not perceived, the data exchanged between the various actors can be misused. It is for instance the case when, the reliability data provided by a supplier, which represents the intrinsic performance or "nominal" reliability of his subsystem, is used as such by the customer to assess the global performance of the system in its real environment and with its specific operational processes.

The case of railway switching points illustrates this pitfall. Considered as critical elements, switching points are designed to achieve high levels of safety. This integrity is often achieved at the expense of significant maintenance, which proves necessary to ensure an appropriate level of system availability. (Marquez et al., 2007). Failure statistics tend to indicate that in-situ reliability level up to two orders of magnitude below the actual intrinsic reliability indicated by the suppliers. This discrepancy can be explained by the fact that external elements such as stones from the ballast, snow or chunks of ice falling from the trains are the most common cause for the failure of points. Although the intrinsic performance data given by the supplier/developer may be correct, it does not reflect the effective failure rate of the switching points integrated in the system. Using the suppliers' value to assess the dependability level of the system bears the risk of overestimating the performance of the system considered.

Distinct objectives in terms of reliability and safety are also a potential source of conflict. While authorities and regulations will focus on safety performance, the system operator or system owner will also give emphasis on reliability and availability performances in order to avoid costly operation losses. Both performances are linked, although computing and optimising one of them independently may have adverse effects on the other. In railways, Track Vacancy Proving system (TVP) are, for instance, available on track sections. False alarm may occur, for instance, because of metallic dust accumulated on the track (in case of contact measurement system) or because of small backward wheel motion at low speed (in case of wheel counting systems). Should the line operator be "certain" that no train is actually occupying the track section, he may (depending on the operational procedures) manually override the automatic TVP system. Such a compensating provision has a positive effect on the system availability, but reduces in the same time the safety level.

### 1.2.3 Lack of relevant data

For maximum efficiency, dependability optimisation should accompany the system along all its development stages, starting at the concept phase. However, the common point between all innovative systems under development is a recurrent lack of relevant reliability data, which renders the dependability analysis intricate. Analysts may well rely on available data (for instance coming from test phases), but these statistics usually arrives at a late development stage, when major system modifications are no longer possible.

The situation is hardly better when technical data is available for specific components or subsystems prior to the system development; Although this facilitates greatly the setting of quantitative values during the dependability analysis process, the figures at disposal do rarely consider the real environment and operating conditions of the system, as already mentioned above. Therefore, the evaluation of the system performance based on this data may significantly differ from the real system performance.

Considering the above, relying on expert judgments proves always necessary at some stage of the development process, either to estimate components/subsystems performance or to asses the relevance of the input data used.

However, the relevance of such expert figures is itself a source of concern. Previous studies have proposed recommendations to give a sound basis to expert judgment assessment (Hokstad et al., 1998). Mismatching data format and insufficient data on the system's lifespan are the most commonly reported problems. Insufficient lifespan data occurs recurrently in the design of new systems, for which no past experience is available.

## 1.3 Content of the article

Risk assessment of complex macro-systems in the context of safety certification is discussed in this paper. An original functional approach, based on the Failure Modes, Effects and Criticality Analysis (FMECA) method is presented and applied to a railways signalling

system. As compared to a classical hardware approach, enriching the model with a functional description of the system is thought to overcome some of the pitfalls (lack of overview, conflicting objectives) encountered when addressing dependability assessment of complex innovative macro-systems. This approach is also expected to provide global and comparative performance indicators to highlight further developments priorities and potential vulnerabilities.

## 1.4 General Approach and requirements

Inductive and deductive risk analysis (RA) methods have been known and used since the seventies to address risks in “sensitive“ processes such as nuclear or chemical plants. The well-known Fault-trees (Vesely et al., 1981), Event-trees (U.S. Nuclear Regulatory Commission, 1975), HAZOP studies (Kletz, 1993), FMEA (European Cooperation for Space Standardization., 2001) or even MORT (Johnson, 1980) are now applied in a wide range of domains.

Numerous developments and extensions have been made to cope with the increasing complex nature of technical systems and to overcome the limitations encountered with manual approaches. Software tools are available today for most classical methods, enabling to greatly facilitate data storage, processing and retrieval. Other computer-based methods are also available to assess the system’s dynamic performances. This is for instance the case with Markov's chains, which can cope with time constraints such as concurrency and parallelism encountered in complex systems (Vinod and Vijaya, 1997). These techniques are used for instance to model control systems (Betous-Almeida et al. 2002) or complex automated systems (Bernard et al. 2008). Nevertheless, such advanced computing techniques are mainly used to assess the dynamic performance of systems of known behaviour (degraded modes, failure rates, repair rates) rather than to spot unidentified risks or vulnerabilities of stochastic nature (Vernez et al., 2003).

From a methodological point of view, the choice of a suitable methodology for dependability assessment depends on the specific goals’ analysis and on the system considered. In practice, several other constraints must be taken into account, such as the deadlines, the resources available or the deliverables expected from the study. The requirements considered as relevant in this study to address innovative and complex macro-systems are presented in Table 1~~Table 1~~.

Mis
pt, I

Table 1 about here

From our point of view, the methodology which comes closest to satisfy all of the above requirement is a computer-assisted Failure Mode Effects and Criticality Analysis (FMECA). In the classical FMECA, the considered system is successively broken down into subsystems and components. Failures modes are then induced at components-level in a systematic way. The occurrence probability and potential effects at local (component or subsystems behaviour) and global levels (system behaviour) are then assessed for each failure mode. The purely technical build-up of the FMECA structure is part of the FMECA procedure and can be found in literature (US Department of Defense 1980; European Cooperation for Space Standardization, 2001).

Amongst the classical risk analysis techniques, the choice of a failure mode approach proves necessary because:

(1) the requirement for a systematic object/function oriented approach implies the use of an inductive methodology,

(2) it can be quantified based on failure rates of individual components,

(3) it is widely used and documented and therefore more likely to be accepted by the involved actors (suppliers, operator, authorities).

Furthermore, FMECA appears also to be flexible in the context of a system under development. In a top down approach, one can indeed choose freely the appropriate level of detail. In particular, additional system layers can be added to the FMECA structure at later design stages in order to continuously reflect the status of the system development.

FMECA also considers a hierarchical system in which "vertical" failure propagation predominates. This model of propagation makes sense in large systems, which tend to be structured into hierarchical layers. Such a hierarchy exists for instance between the basic operating components and components or subsystems dedicated to strategic activities (controlling, diagnostic, etc.).

The choice of a computerized tool is mostly motivated by practical reasons. It allows the development of a generic structure which facilitates data implementation at later stages of the dependability procedure: update of quantitative data, design changes, addition of new components. Moreover, it facilitates criticality computation, data retrieval and data processing. The FMECA module of *Reliability Workbench* (version 9.1, 2001, Isograph Ltd.) has been used in this study.

## 1.5 Limitation of the classical FMECA

Several drawbacks of the FMECA have been reported by previous authors. One of these concerns the quantification procedure used to achieve a risk priority ranking. An arbitrary rating is usually given on the quantitative factors involved: severity, failure probability and detection probability. As the rating scales of the various factors are different (linear and non-linear scales) their multiplication generates coherence problems. Different values of these quantitative factors may lead to the same criticality ranking, while the corresponding risks may actually differ significantly. Fuzzy or grey reasoning techniques have been developed to overcome these limitations (Pillay and Wang, 2003). The fact that in FMEA, the failure propagation follows a linear sequence is also a source of concern. It is generally known that FMEA cannot cope with consequences specifically caused by complex multiple failures and that it does not provide a systematic perspective on risk ranking (Pate-Cornell and al., 2002).

In a FMECA analysis, each possible failure is considered in turn. The process is time consuming and usually produces a large amount of documents. Automated generation of FMECA reports have been proposed by previous authors (Price and Taylor, 2002). Algorithms to handle both single point and multiple failures have been developed. The drawback of this approach is that it only concerns failure modes in direct relation with hardware components, for which no interpretation is required. Failures occurring at higher

hierarchical levels (operational failure, alarm failure, etc.), of higher abstraction level (system does not fulfil the mission for which it has been designed) can hardly be managed in an automated way. This may explain why important discrepancies are commonly found between theoretical and effective system performance. It is also a limit of the self-certification approach, which relies on similar paradigm than automatic FMECA generation tools, to provide safe to use equipments.

The classic FMECA approach, which relies on non-evolving (static) documents (paperwork, spreadsheets) is of limited use to support the design (the system safety society, 1997). A tedious review of the FMECA documents must be undertaken for any significant change in the system architecture or in the design of its components. Thus, although the analysis is usually conducted by the supplier itself, he seldom perceives it as a support for decision making. This lack of interest from the supplier has been substantiated by Johnson and Khan (2003) in their investigation of the perceived benefits from Process-FMEA (PFMEA). Their work indicates that the documents produced during the analysis are only considered as a mandatory output for the customer, who will use it to sustain the whole dependability demonstration. This situation raises concerns about the relevance of the analysis, as well as about the output data management and the update. Although classical FMECA has brought satisfactory results in the past, the need for more advanced methodologies is necessary today to support the safe and reliable design of increasingly large and complex systems.

## 1.6 Proposed approach

### 1.6.1 Functional approach

A system may be seen either as a set of components or as a set of functions. Both hardware and functional approaches are possible in a FMECA, with various advantages and drawbacks. The hardware approach may provide more thorough data, assuming that the system is defined at a fair level of detail. In our case, a hardware approach may be for instance suitable to depict a specific subsystem (e.g. track equipment), although it is difficult to implement on components or subsystems dedicated to abstract tasks (e.g. processors).

The functional approach is more suitable to model complex layered systems or abstract tasks such as processor-based tasks, while its results tend to be less specific. For this reason, this approach is often only considered as a preliminary step to be used early in the design phase. This point of view is somehow reductive as the “abstract” nature of the functional approach actually presents significant advantages over its hardware counterpart:

- it greatly facilitates the consideration of the system operating environment (organisation, procedures, recovery means).
- it facilitates the system modelling as it allows the breaking-down into hierarchical functional blocs.

The latter property is of particular interest in regards to modularity. The functional blocs can be easily re-arranged to take into account design evolutions or modifications, or to be re-used in similar systems.

In this study, the system has been modelled following, globally, a functional approach. This approach seems of particular interest in the context of complex macro-systems because of their multiple functional layers. The higher the hierarchical layer, the more conceptual the tasks assigned to the corresponding devices become. In large systems, there is already a strong functional hierarchy between systems - subsystems and operating components layers. This is for instance the case in railways or aviation, where normal operation functions and safety functions (e.g. collision avoidance systems) are usually managed by different hierarchical layers (Durou et al., 2002). A strict segregation is also kept between these layers in order to avoid concurrencies.

Functional system modelling has proven powerful to structure and analyse complex systems. An example of the hierarchical functional representation of an automotive lighting system may be found in Snooke and Price (1998). It should be pointed out that methods and algorithms have been developed to systematise and automatise the functional modelling approach. However, such applications seem to be limited to specific components or small-scale subsystems. An example of automated functional approach for an electrically driven gear pump has, for instance, been proposed by Hawkins and Woollons (1998).

### 1.6.2 Hierarchical layering in complex macro-systems

The construction and use of the hierarchical structure approach is shown in Figure 1. The system is successively split into sub-systems until the level of the basis functions/components is reached following a top-down approach. The bloc at the top represents the global function of the system for which it has been designed (for instance "trains performs safely the optimal route" in the case of a railway line). It is interesting to note that, in the upper part of the hierarchy, the use of a functional approach leads to a significantly different structure from the use of a hardware description. The model reflects the expected behaviour of the system. This principle is similar to recent approaches proposed by other authors such as the success modelling approach used in Hierarchical Holographic Modelling (HHM) to address large hierarchical systems (Haimes et al., 2002), as well as the multilevel modelling (MFM) approach used in the Safe-SADT method for instance (Bernard et al., 2008).

The upper part of the hierarchy is constituted of generic functions, and it becomes more and more specific when moving down along the structure. Choosing the adequate level of detail, namely the lowest hierarchical layer to be modelled, is arbitrary and will mostly depend on the data available for the quantification. Pursuing the top down logic will eventually lead to the level of basic constitutive components (e.g. relays, sensors, valves…). At the component level both the functional and the hardware description are equivalent.

Figure 1 about here

Failures are induced at the bottom level of the structure and propagated upwards through the higher hierarchical layers, until they reach the top level of the hierarchy where they appear as macroscopic consequence at the system level. When using "static" spreadsheets to perform FMECA, the exploitation and updating of analysis data is difficult. These drawbacks are mostly due to the absence of dynamic links between the system hierarchical layers. This limitation may be overcome when using a formal top-down description of the system hierarchy in combination with dedicated software. Dynamic linking is indeed included in recent specialized tools.

It is interesting to note that such functional FMECA requires the successive use of top-down and bottom-to-up approaches, respectively to build the hierarchical layers and to propagate failures. Expressing the expected behaviour in a top-down process ensures a systemic view of the system, while the inductive bottom-up analysis of failure propagation allows a systematic quantitative assessment of the risk.

### 1.6.3 Modelling effects of compensating provisions

Certain failure modes can have compensating provisions, such as redundancies, alarm systems or the possibility for the system operator to perform manual corrective actions. These provisions can either stop the further propagation of the failure mode and thus prevent the occurrence of a dangerous situation at the system level, or reduce the severity of this dangerous situation (mitigation measure). Redundancies are a priori integrated directly in the description of the basic components. However, when a corrective measure is not included at the component level, but is located higher in the system hierarchy, the compensating provision is then considered as a dormant element of the system and is modelled in the following ways in the FMECA structure (see Figure 2~~Figure 2~~):

- as a compensating provision at the corresponding structural bloc level
- as a basic building block of the FMECA hierarchy to account for the possible dysfunction of this compensating provision (false alarm, erroneous corrective action, etc.)

Figure 2 about here

### 1.6.4 Multiple failure propagations

Depending on both the circumstances and the corrective measures possibly taken, certain failure modes can propagate on different paths and thus generate different consequences at the system level (Figure 3~~Figure 3~~). The modelling of corrective actions described above enables to account for multiple propagation paths. In this respect, the proposed representation of compensating provisions resembles the structure of an Event Tree Analysis (ETA).

This combined approach goes therefore beyond a classical single failure analysis as the responses of compensating provisions (alarm systems, corrective actions), together with their respective failure probability, are integrated in the model. In other words, the linear accidental process involving several independent failures can be considered in this enriched FMECA approach, whereas it cannot in the classical FMECA.

Figure 3 about here

### 1.6.5 Extrinsic failures

In order for the analysis to reflect the reality of the system in operation, the failure identification should not only consider internal technical failures, but should also integrate failures caused by external risk factors, such as human failures (direct error or errors due to inadequate operational procedures) and environmental hazards. As discussed above, it is of utmost importance that the risk analysis be able to consider the system in its real environment.

In this respect, the functional model developed does provide a framework that enables external risk factors to be considered. At the level of basic elements, human and

environmental hazards can be directly accounted for as individual failure modes and apportioned according to their respective probability of occurrence.

Operational and organisational sources of hazard can also be accounted for thanks to the functional description of the system. Normal operations (those operations that are required for the system to function properly in a non-degraded mode) appear as basic building block of the system hierarchy. Human errors on normal operations can thus be introduced as failure modes of these expected actions.

Human errors occurring on critical actions such as mitigation provisions have to be treated in a different way, as these actions do not appear as building block of the system hierarchy. The way erroneous compensating provisions have been modelled is described in section 2.2.2 below.

### 1.6.6 System boundaries

The definition of the system boundaries enables to clearly delimit the responsibility of the suppliers. Nevertheless, regardless of how complex the system is, its safe and reliable functioning often relies as well on other external systems with which it is in interaction. For instance the safe flying of an airplane not only depends on the intrinsic functioning of the aircraft, it also relies on the data received from the control tower.

When considering the dependable operation of a system, this interaction with dependant neighbouring systems has thus to be considered. The way it is dealt with in the enriched-FMECA is the following. Two categories of basic building functions have to be considered in the FMECA analysis:

- *The basic blocks belonging to the system*. These are given comprehensive functional descriptions in the FMECA structure: function, failure modes, failure rates, apportionment, beta factors, operating time, etc.
- *The basic functions not-belonging to the system*, but which have a direct functional interaction with it. These functions therefore represent the interfaces with the neighbouring systems. The failure modes relative to these external elements are not detailed in the analysis, but their generic consequences on the system have nevertheless to be considered and propagated through the FMECA structure, similarly to a failure mode belonging to the system.

### 1.6.7 Probability, criticality assessment

The probability p(x) of a direct undesired situation x triggered by the occurrence of a failure mode F, also known as criticality number, is given by:

$$p(x) = \lambda_F t_{op} \alpha_F \beta_F \quad \text{Equ. 1}$$

where

- $\lambda_F$ is the total failure rate of the element/function considered
- $t_{op}$ is the operation time of this element/function
- $\alpha_F$ is the apportionment of the specific failure mode, that is the conditional probability that a given failure mode has occurred, considering the failure of the element/function occurred

- $\beta_F$ is the $\beta$-factor of failure mode *F*, that is the conditional probability that the consequence *x* will occur considering the failure mode *F* did occur.

Since the model can consider both multiple propagations and compensating provisions (see above), this introduces apportionments and $\beta$-factors at intermediate hierarchical levels. Therefore, the probability *p(x)* of the final consequences *x* at the system level (at the top of the FMECA-hierarchy) caused by a given failure mode *F* is given by:

$$p_F(x) = \lambda_F t_{op} \prod_i \alpha_F^i \prod_j \beta_F^j \qquad \text{Equ. 2}$$

where

- $\alpha_F^i$ is the apportionment of failure mode F at hierarchical level i
- $\beta_F^j$ is the conditional probability that the effect of failure mode F at hierarchical level j propagates further.

The criticality number *(Cr)* of the whole system, also called cumulated criticality, is the sum of the specific failure mode criticality numbers in the corresponding severity category.

$$C_r = \sum_{F=1}^{m} p_F(x) = \sum_{F=1}^{m} \lambda_F t_{op} \prod_i \alpha_F^i \prod_j \beta_F^j \qquad \text{Equ. 3}$$

Where *m* is the number of failure modes in the severity category considered

# 2 Implementation on a large innovative system

## 2.1 ETCS L2 : innovative railways signalling and automated system

The new high-speed railway line of the Lötschberg contains a bi-directional 37-km tunnel through the Swiss Alps. Budgeted at 3 billion Euros, this strategic north-south line will absorb some 30'000 trains per year, with an operational start-up foreseen in 2007.

An innovative signalling and automated system is planned for this line. As in any railway system, the numerous track equipments must be coordinated in order to absorb a maximal traffic, while optimising availability and safety. These tasks are usually performed through several hierarchical layers by computers and relay boxes. This complexity has been brought a step further in the case of the Lötschberg line because of the recent development of the ETCS (European Train Control System) of the second level (ETCS-L2), in which classical optical signalling (with trackside optical signals and speed signs) is suppressed and replaced by a GSM-radio-transmission to the trains of centrally computed speed profiles. The onboard processing systems of the trains then match these speed profiles to their route according to a dual odometric system and to their respective characteristics (braking performance, maximal speed, etc.).

Considering that the braking distance of a train running at 200 km/h is about 1.5 km, we understand the critical challenge in introducing such a new signalling system, which must maximise traffic capacity while ensuring a very high safety level. No commercial ETCS-L2 lines exist to date, but this technology will be the future European standard for railway traffic management.

The line is composed of a large number of equipments and highly interactive sub-systems of various nature (see Figure 4) (electro-mechanical, electrical, infrastructure, hard-/software, electro-magnetic) and locations (tracks elements, control centre, embarked systems), most of which are still under development. Finally, although this system is largely automated, the human and environmental risk factors nevertheless impact in a crucial way on the system performances.

All these aspects make the Lötschberg railway line a highly complex and innovative system. Because of the lack of past experience (incidents, statistics on failures and disturbances) with the ETCS level 2 signalling system, the dependability demonstration of the Lötschberg railway line relies heavily on prospective risk analyses. Such an approach is furthermore required by the railways CENELEC standards (e.g. EN50126 and EN 50129) (CENELEC, 1999, 2000).

Figure 4 about here

## 2.2 System modelling

### 2.2.1 Functions and hierarchical layers

The first step in the risk analysis is to elaborate a functional model of the system, which reflects the system considered as a whole. Starting from the top function for which the system is designed ("trains follow successively their optimal route"), the system is successively broken down into sub functions, until the level of individual element/component is reached (see description in section 3.1).

When tackling complex systems, it often proves useful to first draw a preliminary functional bloc-description of the system before going into the details of its functioning. Such a sketch description is illustrated for the Lötschberg railway line in Figure 5, while a portion of the full FMECA structure is given in Figure 6.

Figure 5 about here

Figure 6 about here

### 2.2.2 Compensating provisions

Compensating provisions at component-levels, such as internal redundancies, does not appear explicitly in the system description. They are directly included in the quantitative assessment of their related failure mode occurrence. Compensating provisions including functions of higher hierarchical levels are depicted as such in the model. This is for instance the case when a diagnosis is required (human or computer diagnosis).

Consider for instance a Track Vacancy Proving system (TVP), which is the electro-mechanical trackside element indicating if a track-section is occupied by a train or not. Assume the TVP indicates that a given track section is "occupied", whereas it is actually free (false-positive alarm). In this case, the track section will appear as "occupied" (marked in red) on the remote control monitor of the line operator.

Should the line operator have a good enough reason to believe that the TVP is indeed giving a false-positive information (e.g. through direct view on the track, communication with the train driver, etc.) and that the track is actually free, he has the authority to remotely reset manually the TVP with a critical command to set the track section free. This action avoids the TVP failure to propagate at a higher hierarchical level, where the interlocking (the central safety system that allows train routes to be established) would have prevented any route setting on this track section, resulting in a partial loss of operation at the system level.

Of course, the compensating provision “reset the TVP” also bears its own failure rate, as the operator can set free a track which is actually occupied by a train (which explains why this reset function is considered as a critical command). An incorrect compensating action (a resetting TVP action of an occupied track) must also be considered in the analysis. Quantitatively, the success rate of a compensating provision is introduced in the beta factor, which describes the probability of success of the compensating provision, considering the failure of the TVP has occurred (Figure 7). Beta factors, which may refer to uncommon situation, are difficult to quantify because past experience is (fortunately) scarce. When no data or expert judgment is available, an error probability is estimated using generic data source, such as human error estimates based on cognitive errors theory.

This modelling of the compensating provisions enables to integrate in the analysis the alarm systems and the automated/human corrective actions, which is not possible in the classical FMECA approach.

Figure 7 about here

### 2.2.3 Severity assessment

The consequences at the system level of failure modes can be detrimental to the system itself (loss of operation, damage to equipment) or to the safety (fatal accident, injury, etc.). In order to optimise the performances of the system, it is important that availability and safety aspects are considered jointly, as required by the CENELEC railway norms.

In this view, two different severity scales have been defined (Table 2), based on both the CENELEC norms and on current practices in similar systems. The RAM-scale proposed here considers only operation loss, i.e. availability of the system. Damages to equipment, measured in financial losses, could be complementarily matched on the same scale.

Since each failure mode has a consequence at system level (Figure 7), this consequence can be evaluated both in terms of impact on the availability of the system (A-scale) and in terms of damage to humans (s-scale). Each identified failure mode can thus be associated with two unrelated severity categories, which enables to consider both availability and safety aspects jointly.

Table 2 about here

### 2.2.4 Multiple propagations

The example of the switching-point not reaching its end-position (Table 3~~Table 3~~), illustrates perfectly the modelling process of multiple-propagation. This single failure mode can generate different consequences, of various degrees of severity and probability, depending on the corrective measures undertaken by the operator (distinguished by its apportionment $\alpha$), and by its potential success ($\beta$ factor).

Table 3 about here

### 2.2.5 Interfaces

The system considered is in direct interaction with neighbouring systems, with which data is exchanged (see Figure 4). The system considered is not responsible for the completeness and validity of the data/information produced and transmitted from neighbouring systems, but it still has to deal with it, even though this information might be erroneous or incomplete. It can be differentiated between four different types of interface failures depending on whether the information transmitted is necessary for the functioning of the system (expected data) or appears as complementary information (unexpected data). The way we have modelled these four failure mode categories is described in Table 4.

Table 4 about here

## 2.3 Input data

When considering innovative systems such as the ETCS-L2 railway line of the Lötschberg, the failure modes identified are difficult to quantify. When the first iteration of the risk analysis was performed, many components were under development and operational procedures were not well defined at that stage. No statistical data regarding their reliability was thus available. Furthermore, failure modes initiated by external stressors, such as environmental conditions, natural events, or human actions, are even more difficult to assess. Although mandatory, this quantification procedure represents one of the most intricate and crucial tasks of the entire analysis process. A lot of effort can be put into the building up a thorough model, but this effort will prove vain if the input data is of bad quality or irrelevant.

An iterative data refining approach has been used to tackle this issue. In a first step, all the risks identified have been assessed using conservative failure rate data borrowed from international database for similar equipment and operations.

While no further refining effort was necessary on those risks that already proved acceptable at this stage, a second round of assessment, based on more system-specific data, has been performed on those risks that proved unacceptable after the first iteration. In this second step, the failure rates have been obtained either from operational statistics on similar systems in operation (for operational failures), or from the equipment suppliers (for new components), or from railway experts who were specifically asked to provide conservative figures.

A third and final iteration has then been conducted for those risks that still proved critical after the second step. 2 to 3 railway experts (depending on availability) were asked to provide realistic failure rates or occurrence statistics based on their own expert judgement. Should the different expert's estimates on a given failure rate differ significantly, then these figures and underlying expert arguments would be shared and discussed between the experts until a consensus on a final value could be obtained, similarly to what would be done in a Delphi-type analysis. It is important to mention that the experts who provided data in the second iteration, were interviewed again in the final assessment step to refine their own view, which is also a procedure typical of a Delphi-study.

It should be noted that these 3 iteration steps have been conducted at different development stage of the system, with the third step carried out on the final design. This original approach guarantees to always remain on the safe side of the risk assessment by shifting progressively from a pessimistic to a realistic view of the system. Furthermore, this iterative procedure offers the great advantage to focus only on these risks that still prove critical after each assessment step. Not having to worry any longer about those risks that could prove acceptable after the first iteration does save a lot of time and effort.

## 2.4 Results

For each couple “failure mode-consequence at system level” we have evaluated the corresponding occurrence probability, as well as the impact severity given by both the Availability (A) and Safety (S) rankings. This whole data can thus be represented in two criticality matrices, one related to availability and the other related to safety, as shown in Figure 8. 219 events with potential consequences at the macro-system level have been identified and their individual risk level evaluated.

Except for those few undesired events that affect only the safety or the availability of the line, all data points in the A-matrix have a corresponding risk in the S-matrix. Furthermore, due to possible multiple propagation paths, given data points in the matrix may correspond to a single failure mode with multiple consequences at the system level.

These joint A- and S-risk matrices do not only yield a global view of the risk level of the system, but also enable to identify its individual vulnerabilities, since each point is associated to a specific failure of a system component. Furthermore, the approach also represents a mean to directly compare the global A- and S-performances of the system.

Figure 8 about here

Indicative risk acceptance thresholds are given in both the A- and S-matrices. These thresholds have been established on the basis of risk acceptance criteria previously used by the Swiss railways (following a GAMAB approach) as well as criteria proposed for similar infrastructures (e.g. the French matrix used in the context of safety analysis for the Channel tunnel). This has led to the classical definition of zones in the risk matrices in which the risk level is considered respectively acceptable, tolerable and intolerable (respectively the white, orange and red zones in Figure 8).

This approach enabled ones to identify which failure modes represent an unacceptable risk for the system in terms of either availability or safety. However, it should be stressed that the dependability demonstration (i.e. all risks acceptable) represents an ultimate goal of the system design, and is not as such the primary focus at an intermediate development stage. In this regards, the primary use of the risk matrices during the system development is to spot vulnerabilities of the system that require design changes or further process design and serve as indicators of how mature the current design is in terms of dependability achievement. Figure 8 shows the system performance at an early development stage. The numerous unacceptable risks in the highest severity categories reflect the fact that the risk assessment at this early stage has been based on conservative failure rate data.

Measures should then be taken to reduce the vulnerabilities identified on both A- and S-matrices, either by reducing their occurrence probability, or by reducing their severity. Our systemic and computational approach enables to integrate the proposed technical/procedural modifications directly in the model and assess their impact on the overall system. In particular, measures taken to increase the safety level often impact negatively on the availability of the system, and vice versa. In this sense, the effect of possible compensating provisions can be directly compared and their effectiveness in terms of true risk reduction assessed. This proved an extremely useful design- and decision-making tool in trading-off between availability and safety performances.

Last but not least, reducing the risk associated with individual failures is not sufficient to assess the global dependability performance. It should also be shown that the global criticality in each severity category is low, and ultimately below the risk acceptable criteria given for this severity. This global risk, which is shown by the blue bars in Figure 8 simply represents the cumulative criticality, that is the sum of all the individual event probabilities in each severity category (see equation 3). Iterative implementation of design refinement (e.g.

compensating provisions) should be carried out until the cumulative criticality point in each impact category falls below the acceptance threshold. For the Loetschberg project, three iterations have been carried out, respectively in the development phases of concept, system requirements and system design. The system showed a significantly improved dependability level at each iteration.

### 2.5 Coverage and limits

The combination of the top-down (elaboration of the system hierarchy) and bottom-up (propagation of the failure modes) FMECA procedures yields a global view of the system, while ensuring an adequate level of technical details. In spite of these advantages, this approach cannot, on its own, cover all the requirements of the safety and reliability analysis. In studying complex systems, certain factors can restrict the application of the FMECA approach. In particular, this method is not well suited: (1) to identify hazardous events induced by combinations of independent system failures and particular circumstances; (2) to describe operation of the system functioning in degraded state. Both these limitations have been experienced in our case study on the Loetschberg system.

Furthermore, Suokas and Pyy (1988) have shown that, in general, the efficiency and coverage of any given analysis method is limited, and that a significant number of hazardous situations remain undetected when a single approach is used. In order to enhance the coverage of the analysis, complementary studies have been performed using the FTA (Fault-Tree Analysis) and ETA (Event Tree Analysis) methods. These studies have been used to investigate specific safety critical scenarios such as “Reversing”, “Crash of the Radio Block Center”, “Loss of GSM connection”, “Collision linked to odometric failure”, etc. It must be pointed out that ETA and FTA have their own limitations. FTA for instance can cope with complex combination of failures but is coverage is limited to a specific, previously known, hazardous situation. For this reason, FTA and ETA approaches should be considered as complementary, rather than a substitute, to the bottom-up FMECA.

## 3 Conclusions

An integrated approach, based on a classical Failure Mode Effect and Criticality Analysis (FMECA), has been developed to perform risk analysis and risk management of large and complex innovative systems. This approach is based on a functional rather than hardware description of the system, which enables for the various procedures and operational processes to be integrated in the analysis. This is an important value-added feature of the method as those operational aspects often prove critical, if not deciding, when optimising system performances.

The classical FMECA method has been enriched with different computational and analysis features offering a more realistic modelling than that of classical FMECA, without losing the benefits of a systemic approach. In this approach, failure modes may have multiple propagation channels, which enables to account in the risk analysis for compensating provisions (alarm systems, corrective actions). This feature also enables to go beyond single-failure analysis (as normally done in classical FMECA), as the possible failure of these compensating provisions are also considered, similarly to an Event Tree Analysis. Further computational developments are still needed to better integrate the possibility of having apportionment at intermediate hierarchical levels to account for the different propagation paths. This work was carried out manually in this study.

Furthermore, both availability and a safety severity scales have been proposed so that the consequences of system of failures (technical or human) can be assessed jointly. The impact on the availability performance of the system of any mitigation measures meant to improve the system safety can then be directly assessed, and vice versa. This, in turn, enables engineers and decision-makers to optimise the system by taking more informed trade-off decisions between the safety and reliability performances.

Some further computational developments are still needed in this direction to allow for a better (more automatised) link between analysis and presentation of the results, as no such computational tool exists to date. In particular, it would ultimately be very powerful to be able to visualise directly the impact of such or such compensating provision or the effect of the reliability improvement of any given component on the global availability and safety of the system, that is to create a direct link between the evolutionary core data and the representation of the risk matrix.

Finally, being based on a computational structure, this enriched-FMECA approach is both modular and flexible allowing for successive implementations of the model, yielding a permanent up-to-date view of the system performances all along its development, from concept design to operational start-up. This goes in line with the more and more widely recognised fact that dependability analyses should start as early as the concept phase of a project for maximum (cost and performance) benefits.

The proposed approach has been implemented on an innovative railway signalling and automated system. It did yield a global and joint view of the Availability and Safety performances of the system and did successfully highlight existing vulnerabilities in different phases of the system development. However, as it is always the case with innovative systems, the lack of relevant reliability data proved limiting for assessing certain aspects of the system.

To try and overcome these difficulties, an original iterative approach based on expert judgement has been developed, which bears certain similarities with Delphi-type studies in which experts are asked to review their own judgement based on the arguments from other experts. One further key aspect of this approach is that it enables ones to follow the system development while always remaining on the conservative side of the risk assessment. Although relatively convincing, this approach would nevertheless necessitate further investigation, in particular to guarantee that no risk are under-estimated in the first iteration.

With regards to the large discrepancies observed between intrinsic and effective reliability of existing systems, further developments are required in this field, where expert judgment should, to our opinion, play a more important role in such assessment, in particular so far as the operational aspects are concerned.

This study has addressed some of the pitfalls pointed out in the literature (lack of system overview, conflicting objectives) and brings some solutions to partly overcome these difficulties. The methodology developed in this study proved a promising risk assessment (joint evaluation of the dependability performances, identification of vulnerabilities) and risk management (impact assessment of mitigation measures) approaches to support the development of complex macro-systems.

## Acknowledgment

We are indebted to the Swiss Federal Railways (SBB) who allowed us to publish the application to the Loetschberg Railway line.

## References


Bate, I., Kelly, T., 2003. Architectural considerations in the certification of modular systems. Reliability Engineering and System Safety 81, 303–324.

Bernard, V., Cauffriez, L., Renaux, D., 2008. The Safe-SADT method for aiding designers to choose and improve dependable architectures for complex automated systems. Reliability Engineering and System Safety 93, 179-196.

Betous-Almeida, C., Kanoun, K. 2004. Dependability modelling of instrumentation and control systems A comparison of competing architectures. Safety Science, 42(5), 457-480

CENELEC, 1999. Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), EN50126.

CENELEC, 2000. Bahnanwendungen – Sicherheitsrelevante elektronische Systeme für Signaltechnik, prEN 50129.

Durou, O., Godet, V., Mangane, L., Pérarnaud, D., Roques, R., 2002. Hierarchical fault detection, isolation and recovery applied to COF and avionics. Acta Astronautica 50, 547–556.

European Cooperation for Space Standardization, 2001. Failure modes, effects and critically analysis, ECSS, Noordwijk.

Gadd, S.A., Keeley, D.M., Balmforth, H.F., 2004. Pitfalls in risk assessment: examples from the UK. Safety Science 42, 841-857.

Haimes, Y., Kaplan, S., Lambert, J., 2002. Risk filtering, ranking, and Management Framework Using Hierarchical Holographic Modeling. Risk Analysis 22, 383-397.

Hawkins, P.G., Woollons, D.J., 1998. Failure modes and effects analysis of complex engineering systems using functional models. Artificial Intelligence in Engineering 12, 375-397.

Høj, N., Kröger, W., 2002. Risk analyses of transportation on road and railway from a European perspective. Safety Science 40, 337-357.

Hokstad, P., Oien, K., Reinertsen, R., 1998. Recommendations on the use of expert judgment in safety and reliability engineering studies: two offshore case studies. Reliability Engineering and System Safety 61, 65-76.

Johnson, W.G., 1980. MORT Safety Assurance Systems, Marcel Dekkern Inc., Basel.

Johnson, K.G., Khan, M.K., 2003. A study into the use of the process failure mode and effects analysis (PFMEA) in the automotive industry in the UK. Journal of Materials Processing Technology 139, 348–356.

Kââniche, M., Laprie, J.-C., Blanquart, J.-P., 2002. A framework for dependability engineering of critical computing systems. Safety Science 40, 731-752.

Kletz, T., 1993. HAZOP and HAZAN: identifying and assessing process industry hazards,3rd ed., Institution of Chemical Engineers, Rugby.

Marquez, F.P.D., Weston, P., Roberts, C., 2007. Failure analysis and diagnostics for railways trackside equipment. Engineering Failure Analysis 14, 1411-1426.

Melchers, R.E., 2001. Rational optimization of reliability and safety policies. Reliability Engineering and System Safety 73, 263-268.

Papadopoulos, Y., McDermid, J.A., 1999. The potential for a generic approach to certification of safety critical systems in the transportation sector. Reliability Engineering and Systems Safety 63, 47–66.

Pate-Cornell, E., 2002. Finding and fixing system weaknesses: probabilistic methods and application of engineering risk analysis. Risk Analysis 22, 319-334.

Pillay, A., Wang, J., 2003. Modified failure mode and effects analysis using approximate reasoning. Reliability Engineering and Systems Safety 79, 69-85.

Price, C.J., Taylor, N.S., 2002. Automated multiple failure FMEA. Reliability Engineering and Systems Safety 76, 1-10.

Snooke, N., Price, C., 1998. Hierarchical functional reasoning. Knowledge-Based Systems 11, 301–

309.

Suokas, J., Pyy, P., 1988. Evaluation of Four Hazard Identification Methods with Event Descriptions, Technical Research Centre of Finland, Espoo.

The System Safety Society, 1997. System Safety Analysis Handbook, 2nd ed, System Safety Society, Albuquerque NM.

US Department of Defense, 1980. Procedures for Performing a Failure Mode, Effects and Criticality Analysis, MIL-STD-1629A .

US Nuclear Regulatory Commission, 1975. Accident Definition and Use for Event Trees, National Technical Information Service, Springfield.

Vernez D., Buchs D., Pierrehumbert G., 2003. Perspectives in the use of coloured Petri nets for risk analysis and accident modelling. Safety Sciences 41, 445-463.

Vesely, W. E., Goldberg, F. F., Roberts, N. H., Haasl, D. F., 1981. Fault Tree Handbook, National Technical Information Service, Springfield.

Vinod, C., Vijaya, K., 1997. Reliability and safety analysis of fault tolerant and fail safe node for use in a railway signalling system. Reliability Engineering and System Safety 57, 177-183.

# Figure legends

**Table 1.** Methodological Requirements

**Figure 1.** Nature of the blocs at different level of the hierarchical model

**Figure 2.** Modelling of compensating provisions

**Figure 3.** Multiple propagation paths are accounted for in the Enriched-FMECA method

**Figure 4.** Signalling and automated system, together with its neighbouring systems.

**Figure 5.** Synthetic FMECA hierarchy for the Lötschberg railway line.

**Figure 6.** Portion of the full FMECA structure. It contains 141 blocks; amongst which 92 represent basic building functions, for which a total of about 230 failure modes have been identified.

**Figure 7.** Modelling of compensating provisions (alarm systems and corrective actions).

**Table 2**. Severity scales A and S for the joint evaluation of the availability and safety aspects of hazardous situations.

**Table 3.** Example of multiple propagation.

**Table 4.** Possible data transmission failures at the system interface.

**Figure 8.** A- and S-risk matrix of the Lötschberg railway line at an early development stage. 219 events with potential consequences at the marcro-system level were identified and their risk level evaluated. The red zone represents unacceptable risks, while the orange patches define the ALARP zone of the LBL project

# Tables

| Method requirement | Objective |
|---|---|
| allow a systematic analysis of the deviations and potential hazards | Meet the requirements of normative standards dependability in a complex system (railroad, nuclear,…) |
| allow a quantification of the risks | Meet the requirements of normative standards dependability in a complex system (railroad, nuclear,…) |
| be generic | facilitate data storage, use and retrieval |
| enable an inductive analysis by elements or by functions of the system considered | meet the "systematic analysis" requirement while ensuring compatibility with the system partitioning |
| be standardised and/or be internationally recognised | facilitate acceptance from authorities and coordination with suppliers/developers |
| to consider jointly availability and safety aspects | Meet the requirements of normative standard dependability in a complex system (railroad, nuclear,…), avoid the "conflicting objectives" pitfall |
| be modular and extendable to neighbouring systems | avoid the "lack of overview" pitfall |
| be systemic, | |
| o to yield a global view of the system, | avoid the "lack of overview" pitfall, |
| o to integrate the technical, human and operational aspects. | avoid the "conflicting objectives" pitfall |

**Table 1.** Methodological Requirements

| Severity | Class | A-damages | S-damages |
|---|---|---|---|
| Catastrophic | 6 | N/A | Irreversible collective damage |
| Critical | 5 | Total operation loss (days) | Irreversible individual damage |
| Important | 4 | Total operation loss (hours) | Reversible collective damage, major comfort loss |
| Significant | 3 | Total operation loss (minutes)<br>Partial operation loss (days) | Reversible individual damage |
| Limited | 2 | Partial operation loss (hours) | Minor collective comfort loss |
| Negligible | 1 | Partial operation loss (minutes) | N/A |

**Table 2**. Severity scales A and S for the joint evaluation of the availability and safety aspects of hazardous situations.

| Failure mode | Compensating measure | α factor | β factor | Consequence | Severity |
|---|---|---|---|---|---|
| Point does not reach its final position | Operator manages to lock the point by repeated backwards - forwards movements | 20% | 0 | None (failure does not propagate further) | |
| | Operator does not create a route on this point and introduces a blocked section on the corresponding track. | 10% | 1 | Partial operating loss | Limited |
| | Operator allows trains to pass at a reduced speed (10 km/h) on the point | 69.9% | 0.005 | Derailment at reduced speed | Critical |
| | Operator allows trains to pass at a normal full speed on the point | 0.1% | 0.02 | Derailment at full speed | Catastrophic |

**Table 3.** Example of multiple failure propagation.

| n° | Situation | System's reaction | Example in ETCS | Modelling |
|---|---|---|---|---|
| 1 | The interface transmits erroneous expected data | The system normally has a means to check validity, or at least plausibility, and completeness of such data. | The system validates the train data (max speed, braking coefficient, etc.) introduced by the train driver and which is used by the system to compute the train dynamic speed profiles. | The failure is propagated throughout the FMI structure as the erroneous data has a direct influence on the functioning of the system.<br>The possible failure of the data validating pro also considered. |
| 2 | The interface does not transmit expected data | The system always realises that expected data has not been received | A train does not receive its speed profile via the GSM transmission system | The disturbance will be directly propagated t summit of the FMECA hierarchy as no compensating provision is normally possible.<br>However, in certain cases, default data can b by the system, which will minimise the consequences. |
| 3 | The interface does not transmit complementary (unexpected) information. | The system has no means to check that such data has not been received | This is for instance the case for all the alarm systems which are external to the system considered, e.g. undetected flood in the tunnel. | The system cannot compensate for non-rece unexpected information (no compensating provision). The consequences will therefore occur at the system level (summit of the FME hierarchy) |
| 4 | The interface transmits erroneous complementary (unexpected) information. | The system has normally no means to check that the content of such data is erroneous, and will thus consider the information as correct. | This is for instance the case for all the fake alarms transmitted by external alarm systems, e.g. fake fire alarm in the tunnel. | Depending on the system's architecture, it ei can, or cannot, check the validity of the alarm can, then the failure propagates throughout t FMECA structure by considering the compen provision and its possible own failure.<br>If it cannot, then the failure generates direct consequences at the system level, without p corrective action. |

**Table 4.** Possible data transmission failures at the system interface.

## Figures

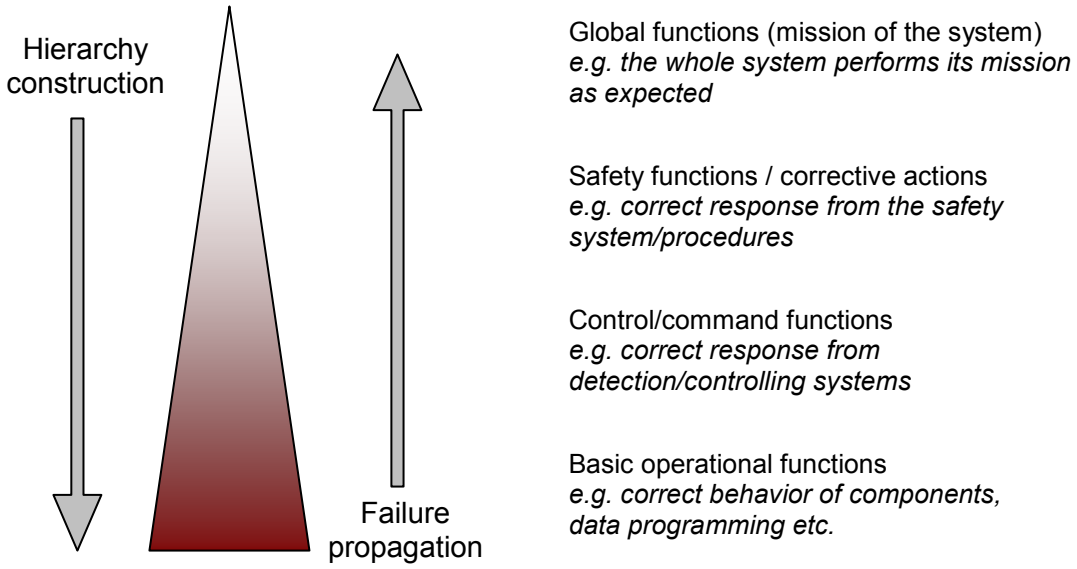
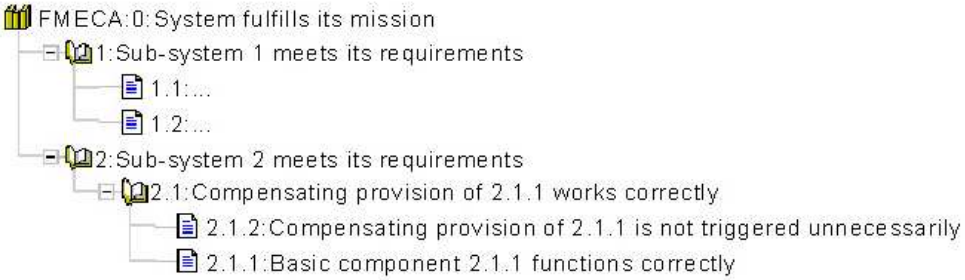



**Figure 1.** Nature of the blocks at different levels of the hierarchical model




**Failure Modes for Block 2.1**

| Effects (Higher Level) | Effects (Immediate) | Up | Apportionment | Description | Down | Contributors |
|---|---|---|---|---|---|---|
| 0.1 System cannot fulfill its mission | Sub-System B fails | ✓ | 100 | Compensating provision of 2.1 fails | ✓ | 2.1.1.1 Component 2.1 fails |
| | | ✗ | 100 | Compensating provision of 2.1 works correctly | ✓ | 2.1.1.1 Component 2.1 fails |
| 0.4 Consequence at system level depends on system configuration and procedures | Consequence on subsystem 2.1 depends on system configuration and procedures | ✓ | 100 | False alarm / faulty action is generated | ✓ | 2.1.2.1 Compensating provision is triggered although component 2.1.1 works properly |

**Figure 2.** Modelling of compensating provisions

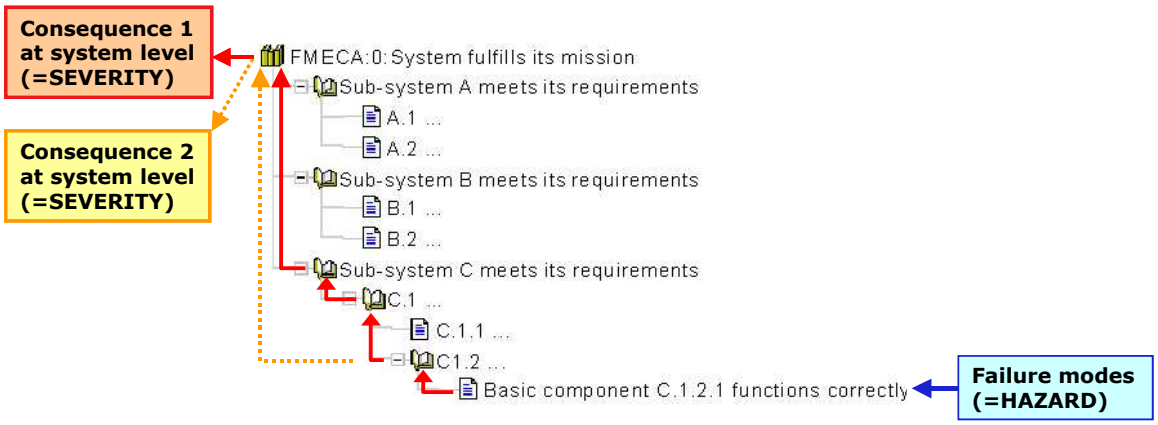



**Figure 3.** Multiple propagation paths are accounted for in the Enriched-FMECA method

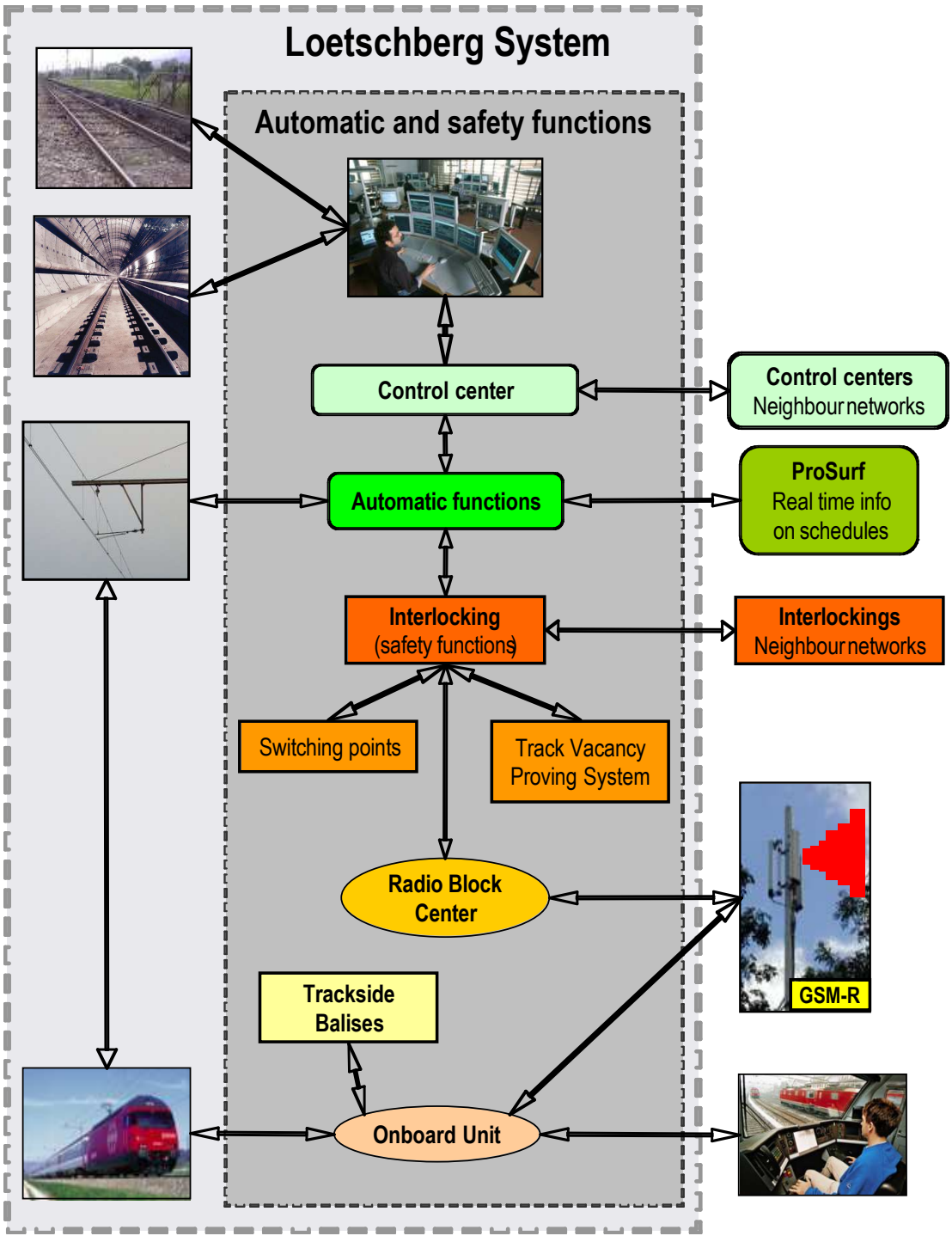



**Figure 4.** Signalling and automated system, together with its neighbouring systems.

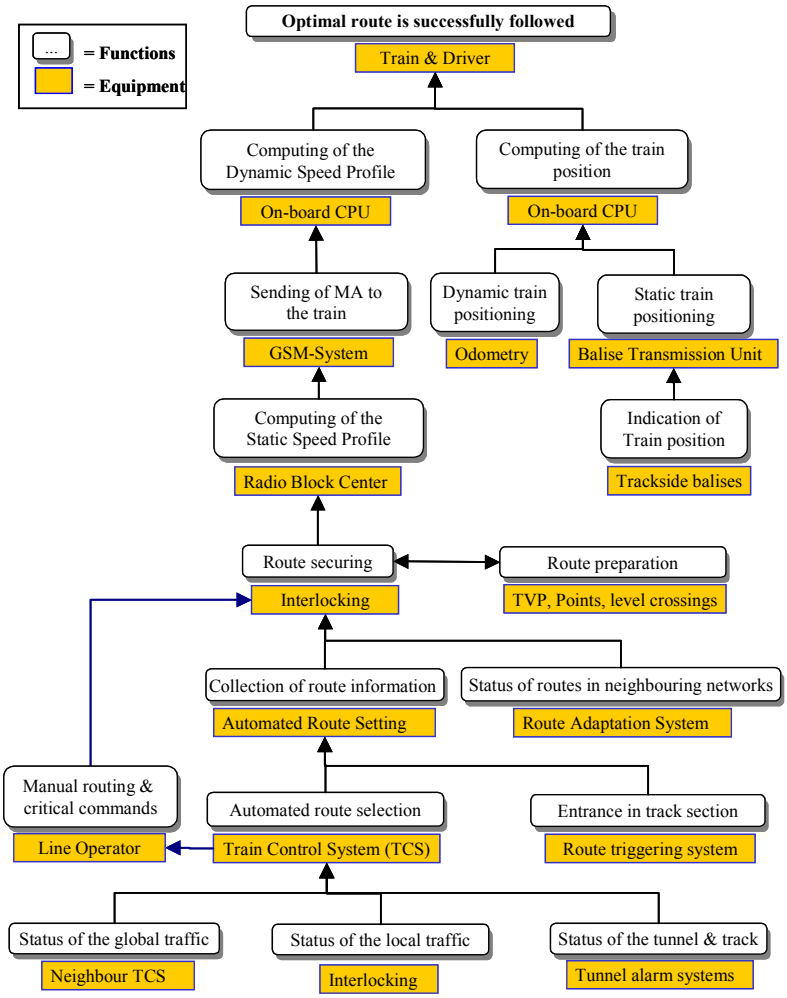



**Figure 5.** Synthetic FMECA hierarchy for the Lötschberg railway line.

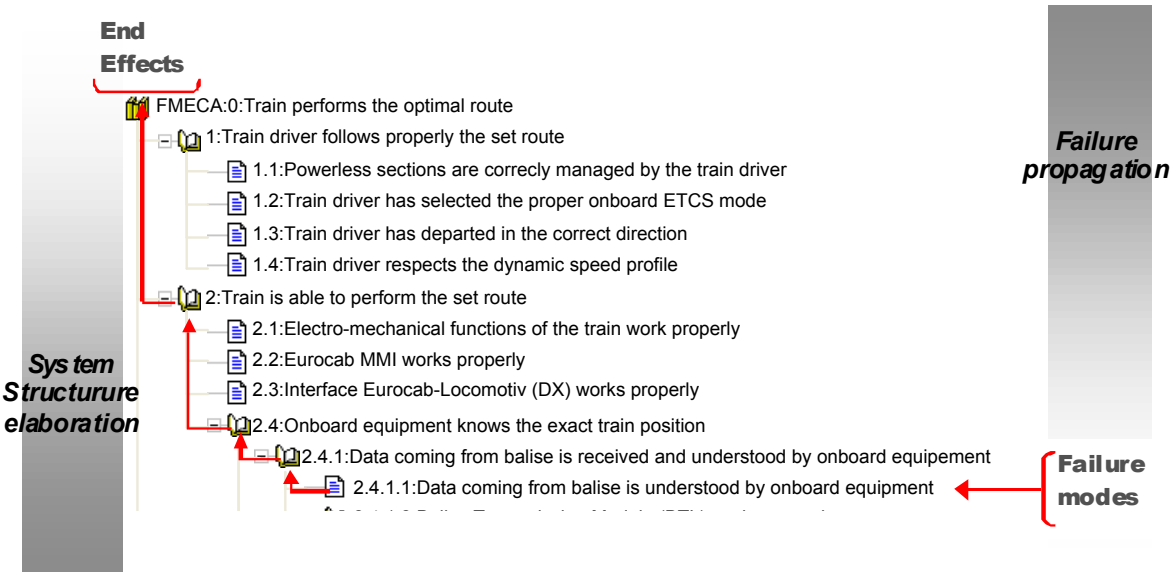



**Figure 6**. Portion of the full FMECA structure. It contains 141 blocks; amongst which 92 represent basic building functions, for which a total of about 230 failure modes have been identified.

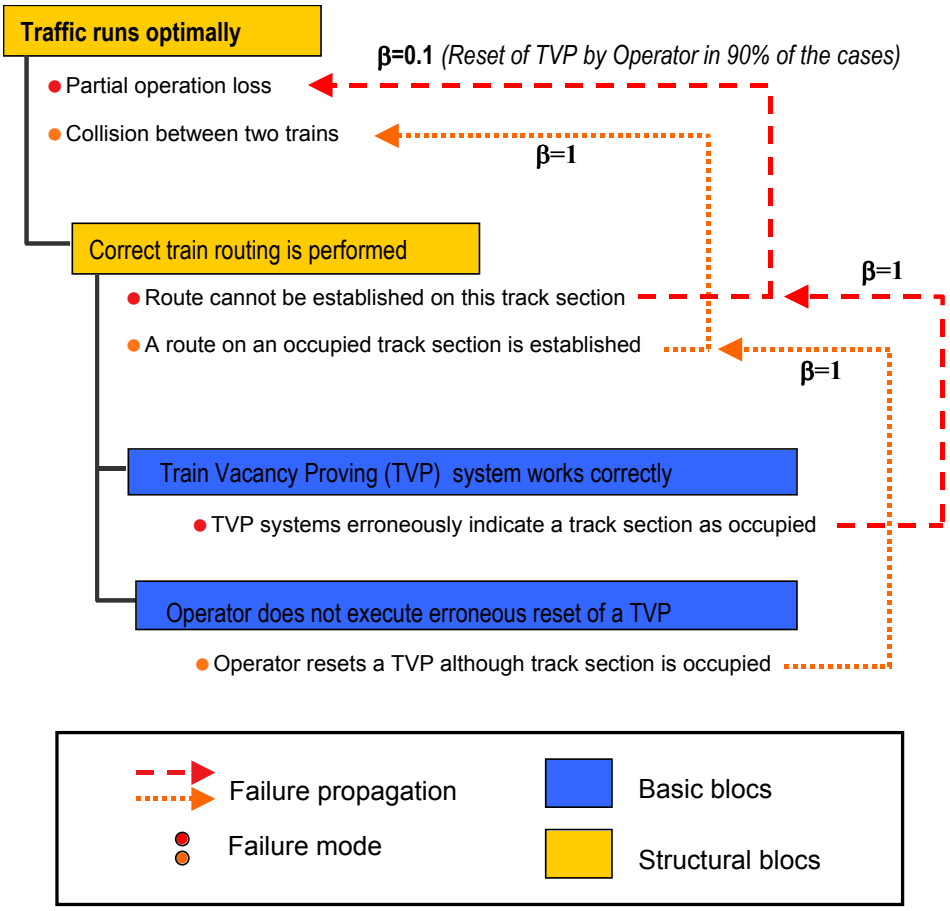



**Figure 7**. Modelling of compensating provisions (alarm systems and corrective actions).

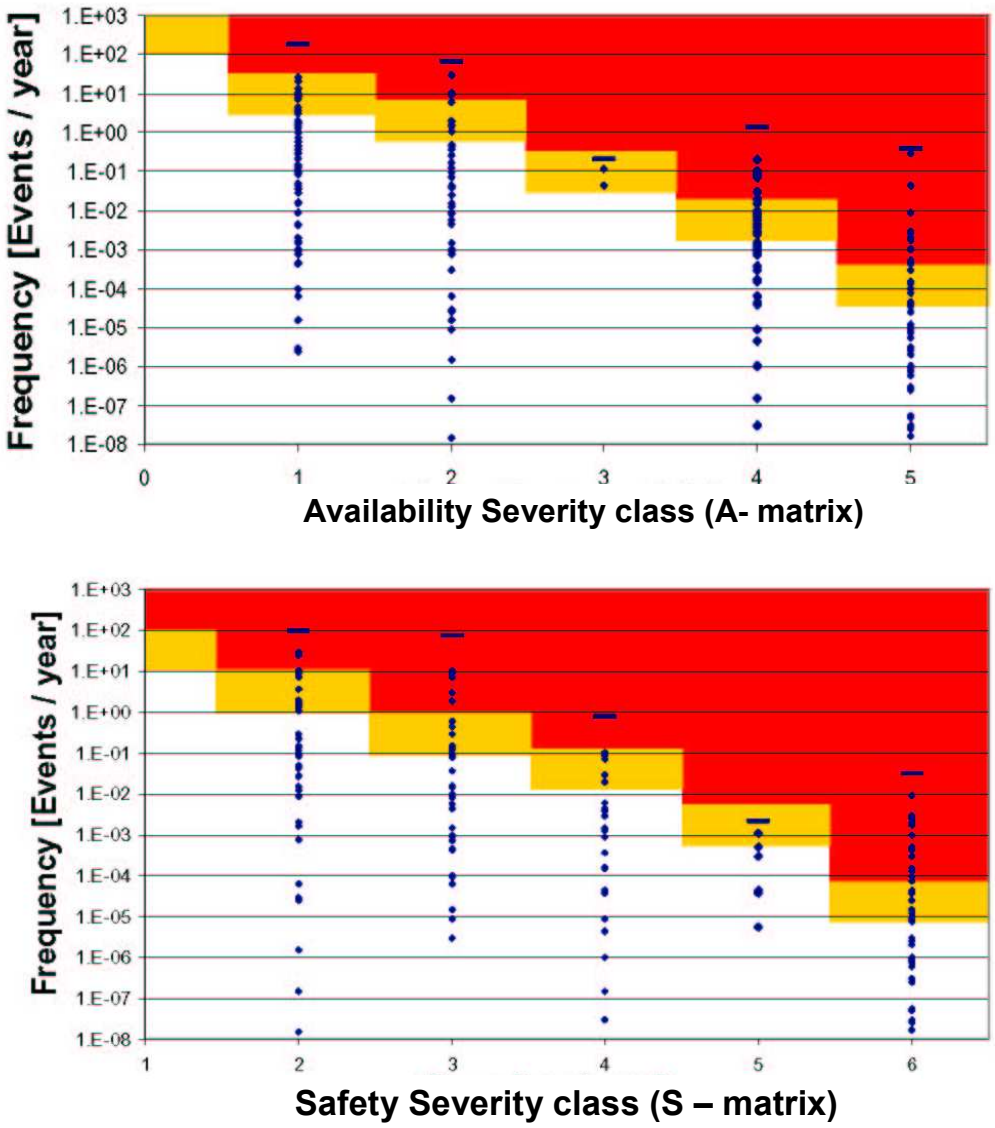



**Figure 8.** Availability- and Safety-risk matrix of the Lötschberg railway line at an early development stage.