PERIODICA POLYTECHNICA SER. TRANSP. ENG. VOL. 32, NO. 1-2, PP. 123-134 (2004)

SAFETY MANAGEMENT SYSTEMS IN TRANSPORTATION: AIMS AND SOLUTIONS

Géza SZABÓ, Krisztián SZABÓ and Roland ZERÉNYI

Department of Control and Transport Automation
Budapest University of Technology and Economics
H-1521 Budapest, Hungary
Phone: (+36 1) 463 1013, Fax: (+36 1) 463 3087
e-mail: szabo-g@kaut.kka.bme.hu

Received: Oct. 30, 2003

Abstract

The control of transportation, including both the track-side and the on-vehicle equipment involves more and more electronic components, which can make the control more intelligent and more effective. The intelligent vehicle system is one of the most demanding concepts of the present and of the near future. By increasing the complexity of the applied electronic systems, much more attention must be paid to safety. Controlling safety is an integrated set of activities during the product's life-cycle rather than a single point activity during the development. This set of activities is called Safety Management System (SMS). In this paper, the features of the SMSs are summarized including their possible aims and the basic methods ensuring to achieve the aims.

Keywords: safety, safety management, risk, dependability.

1. Introduction

Since the beginnings of human life, man has had to face situations in which his life or his properties could have been lost. The name of these situations is danger which means that there is no safety at that moment. In order to be able to compare two or more dangerous situations, a new term, risk is introduced. Risk is the measure of danger, and often expressed as a function of the frequency of the dangerous situations and their impact.

The deliberate controlling of risk has become more and more important as complex, computer or microprocessor based systems are increasingly used both on vehicles and in track-side equipment [5]. These systems are applied in order to reduce the original (external) risk of a process (e.g. traffic lights at a road crossing), but they may generate new dangerous situations (internal risk) which requires further risk reduction. The necessary external risk reduction was provided earlier by mechanical systems in which the internal risk reduction was reached by over-designed mechanical components: their strength ensured the safety level. This over-design is not useful for electronic systems in some aspects (certainly at the component level it can be a good solution), and due to the complexity, human factors have an enormous impact on the safety of the product. The railway industry

has created the methods applicable to specify and demonstrate safety of the whole railway system as well as its most safety-critical subsystem, the interlocking system [2, 3, 4].

Beside the companies involved in the railway industry, others working in the fields of road and air transportation have to introduce new approaches in order to ensure the safety of the vital functions realized or controlled by electronic subsystems.

The aim of this paper is to describe the basic terms related to safety, the basic methods through which the safety level can be estimated and the methods by which the estimated safety level can be achieved. The structure of the paper is as follows. In Chapter 2 the basic definitions of safety are given. In Chapter 3 we introduce the safety management system and emphasize the methods, which can ensure the determination of the safety level. In Chapter 4 the practice of different transportation sectors is described. Finally in Chapter 5 some conclusions are given.

2. Basic Definitions of Safety

2.1. Basic Definitions

In the following, some basic definitions of the safety management are given [3, 6, 11].

Description	Definition
Risk	The probable rate of occurrence of a dangerous situation causing harm and the degree of severity of the harm.
Dependability	Basic aspect of quality covering reliability, availability, safety and all related notions.
Safety	Freedom of unacceptable risk of harm.
Reliability	The reliability is the probability that the system can perform a required function under given conditions for a given time interval.
Availability	The availability of the system is the probability that the system is functioning at time t.
Maintainability	Maintainability is the probability that a failed system is restored to the functioning state in a given time and in a stated environment, which will include the maintenance resources available.
Safety Integrity	The likelihood of a system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.

Description	Definition
Safety Integrity Level (SIL)	One of a number of defined discrete levels for specifying the safety integrity requirements of the safety functions to be allocated to the safety related systems. Safety Integrity Level with the highest figure has the highest level of safety integrity.

2.1.1. Phenomena Affecting Safety

For the specification of safety we must first separate at least two different causes of dangerous situations (*Fig. 1.a, 1.b*):

1. Component failure, and
2. Danger in a failure-free operation,

and a third, but often forgotten source: the risky situations uncovered by the controller (remaining external risk after risk reduction). This third source is not discussed here.

Component failures are unintentional events which cannot be eliminated, but their rate can be lowered. Component failure is a deviation from one of the specified parameters – this deviation is not necessarily followed by any functional problem. If a malfunction is triggered by the failure, the phenomenon is called fault. Certain techniques can be used to eliminate the consequences of a fault to the whole system (e.g. redundancy, fault-masking, re-configuration etc.). In some cases, the effects of faults can be observed at the system level, and these effects result in dangerous situations. Our goal is to specify the allowed rate of dangerous situations (in the railway technology, this rate is called Tolerable Hazard Rate, THR). The allowed rate is well expressible and quantitative approaches are developed for providing the figures. As component failure rates are also predictable or measurable, it can be proved whether the system (including its components with given failure rates) can meet the allowed rate of dangerous events.

Besides the component failures, we must pay attention to another source of malfunctions: the mentioned malfunctions arise during the failure-free state of the system, because they originate from incomplete or improper human actions – errors made in the specification, development etc. phases. Since we have no information on the probability or the frequency of these errors, it cannot be possible to set quantitative requirements for them. The only way to prevent the errors is to specify certain procedures applicable in different phases of the life-cycle: independent checks (often called as verification and validation), documentation to be prepared, developing and analyzing methods to be used etc. The degree of protection is expressed as a figure and called Safety Integrity Level (SIL) The higher the SIL figure, the higher the degree of protection is and the more rigorous the applicable

procedures are. Certainly, the protection against random failures and the protection against human errors must be balanced (see *Fig. 2*). Thus in some cases, the SIL is determined based on the allowed dangerous situation frequency.

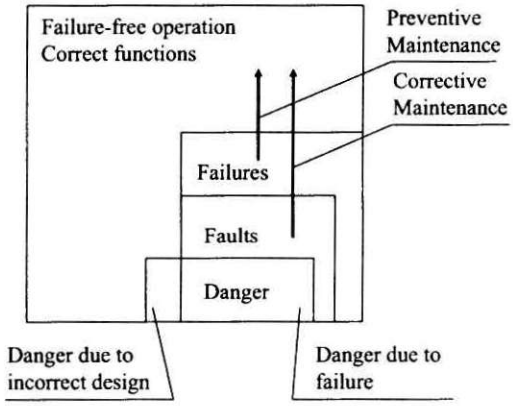

Fig. 1.a. SIL concept

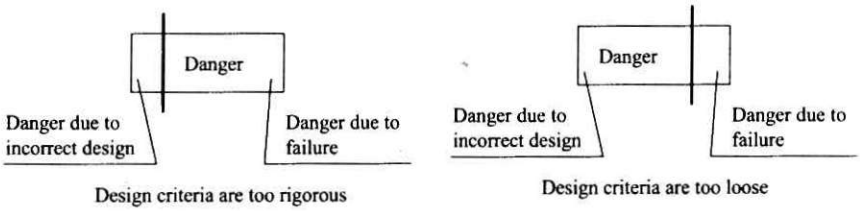

Fig. 1.b. SIL determination

3. Safety Management Systems

Safety Management System (SMS) covers all the activities which are carried out in order to specify and ensure the desired level of safety. We must note that these activities are not limited to the activities during the specification and design phases, but include the activities during the installation, operation and withdrawal. A possible flow-chart is shown in *Fig. 2*.

The basic aims of the SMS can be:

1. To specify and guarantee the level of safety,
2. To simply enhance the safety of the system or
3. To enhance the availability of the system

In the following, the main activities of the process are summarized. Certainly, deviations from the shown SMS structure can be applied, e.g. in some processes, the definition of the safety integrity level is determined after the system structure is finalized and subsystems are separated.

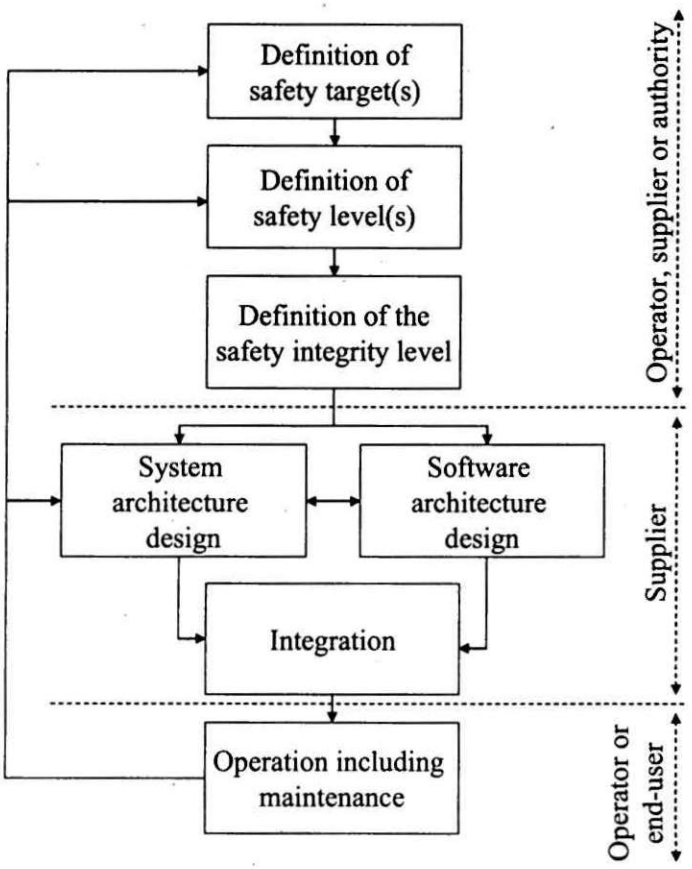

Fig. 2. Basic safety activities during the product life-cycle

3.1. Definition of Safety Targets

The first step in a safety management system is the clarification of the safety related functions. Safety functions (often called as vital functions) are functions which can cause dangerous situations if they are not properly executed. We must note that at this point only functions can be analyzed, since the system corresponding to the

requirements has not been designed.

After the safety-related functions have been determined, all possible hazards, hazardous events and their causes and consequences, like events, situations and effects that potentially cause the system to deviate from normal behaviour must be identified. These hazards and hazardous events should be generated from various viewpoints. For example: an operational viewpoint (what went wrong in the past), a functional viewpoint (failure conditions, human errors), a cognitive viewpoint (operator internal states and strategies, experience, training), an organizational viewpoint (general working conditions, CRM, culture), and a safety management viewpoint (both proactive – to improve the chances to avoid entering the adverse condition at all, and reactive – to improve the chances to escape from the adverse condition prior to its appearance). Hazards may be obtained from incident or accident reports, existing hazard databases, etc. An important activity is to identify sources of statistical information (documents and databases on incidents and accidents) and get the experts' opinion about the frequency of occurrence of the hazards and hazardous events identified.

3.2. Definition of Safety Levels

The tolerable loss of goods (tolerable dangerous situation frequency) can be calculated based on a risk analysis. Risk can be expressed as a function of the frequency of the event to be avoided (the hazard) and the possible consequences of the event. The quantification of risk is a very difficult process and often only categorization is used.

Risk tolerability depends on the tolerability level of the society and the applicable economic resources (See *Fig. 3*) [7]. On the one hand, a certain level of risk cannot be tolerated even when the resources are not sufficient for the reduction – these systems are not allowed to be operated. On the other hand, there is a level of risk which falls below the average risk of the human life, thus no further risk reduction is necessary. The large gap between the two extremities is the ALARP (As-Low-As-Reasonably-Practicable) range, in which the tolerability depends on the cost of the further risk reduction.

The safety level is often determined based on the examination of the existing systems. A good solution is the French GAMAB principle which states that all new systems have to be at least as safe as the existing systems – therefore, the tolerability criteria can be calculated evaluating existing statistical data.

Irrespective of the selected method, the result of this section of safety management is the allowed frequency of dangerous events caused by random failures.

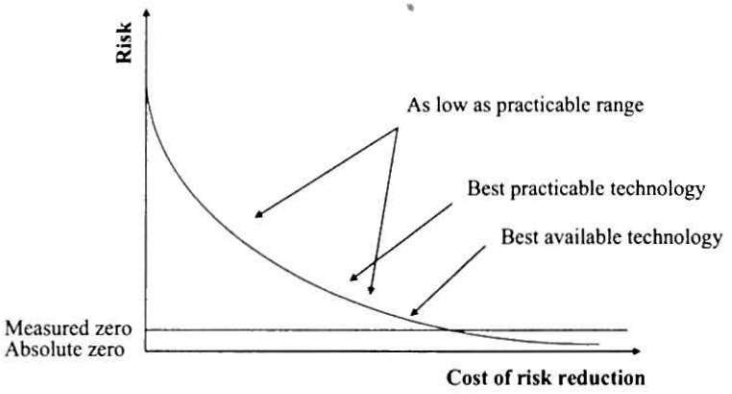

Fig. 3. Risk tolerability estimation

3.3. Definition of the Safety Integrity Level

If allowed frequencies of dangerous events are set, also the required risk reduction for human errors has to be allocated. In some cases, SIL is a simple function of the calculated frequency. The SIL determines the necessary independence of the participants in the project, the required verification and validation phases as well as the documents to be prepared.

3.4. System and Software Architecture Design, Integration

In the design phase it must be ensured that the system under development will meet the requirements. Be careful that SIL requirements can be fulfilled only if the SIL determined actions are taken during the development. Hardware configuration design involves some basic techniques of dependability analysis such as Failure Mode and Effect Analysis (FMEA) or Fault Tree Analysis (FTA). FMEA is a bottom-up method, starting from the individual component failure modes and analyzing their effects and their detection, thus it can support the design continuously. FTA is a top-down method, starting from the pre-defined system malfunctions and examines which failure-combinations can lead to them, thus FTA is useful after a design phase [9].

If FMEA of FTA (or a different method) shows that the current system architecture cannot meet the requirements, some basic dependability techniques must be applied such as adding redundancies to the system, integrating some fault-detection and correction algorithms etc [1, 8, 10]. Some of the applicable methods are hardware related, while others are software related ones. Because of this fact, hardware and software must be developed together – this is called as hardware-software co-design.

The requirements can be met not only by means of design techniques, but by specifying some operational restrictions or some routine tasks. The long-time (life-cycle) dependability is based upon the success of these tasks.

3.5. Operation

The safety requirements concern not only the design phase: it is not enough to prove the safety of the system or a product after the design, the safety level must be maintained during the life-cycle. This requires preventive and/or corrective maintenance activities, as well as training of the users/operators and maintenance staff too.

3.6. Feedbacks

One of the key issues of safety management is the feedback from the real life. Truly successful systems have long time experience which can result the continuous evolution of the safety targets, levels or the system structure. Based on *Fig. 3*, the applicable (practicable) techniques are also in change.

4. Current Status of the Application of Safety Management in Transportation Sectors

4.1. Background

In transportation, two areas are traditionally safety-critical: air and railway transportation. In these areas the safety level can easily be controlled due to the following reasons:

- The number of operators (airlines or railways) is relatively low,
- The personnel involved in the operation are well-educated and trained,
- The number of the manufacturers of main systems is relatively low.

In these areas, the control of safety is necessary since the speed is high and so is the original risk.

The other two main areas of transportation have no significant, widely accepted safety management system as a consequence of the low speed in water transportation, and of the large number of operators and manufacturers in road transportation.

4.2. Air Transportation

In air transportation, definition of safety levels (Tolerable Hazard Rates) is supported by an authorized method. The Joint Aviation Authorities (JAA) has issued the JAR No. 25, in which each failure condition is classified by its severity. (Qualitative definitions of severity are given in *Table 1*.) These definitions are commonly accepted in civil aviation.

Table 1. Definitions of severity categories according to JAR 25

Description	Definition
Catastrophic	Failure conditions which would prevent continued safe flight and landing.
Hazardous	Failure conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be: • A large reduction in safety margins or functional capabilities, • Physical distress or higher workload such that the flight crew cannot be relied upon to perform their task accurately or completely, or • Serious injury or fatal injury to a relatively small number of the occupants.
Major	Failure conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example: • A significant reduction in safety margins or functional capabilities, • A significant increase in crew workload or in conditions impairing crew efficiency, or • Discomfort to occupants, possibly including injuries.
Minor	Failure conditions which would not significantly reduce airplane safety, and which involve crew actions that are well within their capabilities. Minor failure conditions may include, for example: • Slight reduction of safety margins, • Slight increase in crew workload, or • Some inconvenience to occupants.

After the classification of a condition, a classification of frequency or probability of occurrence is given. Qualitative definitions of probability according to the

JAA standard are given in *Table 2*.

Table 2. Definitions of frequency levels according to JAR 25

Description	Estimate of frequency
Probable	Anticipated to occur one or more times during the entire operational life of each airplane.
Remote	Unlikely to occur to each airplane during its total operational life but which may occur several times when considering the total operational life of a number of airplanes of the type.
Extremely Remote	Unlikely to occur when considering the total operational life of all airplanes of the type, but nevertheless, has to be considered as being possible.
Extremely Improbable	So unlikely that they are not anticipated to occur during the entire operational life of all airplanes of one type.

In JAR 25 the terms probable, remote, extremely remote and extremely improbable are also expressed in terms of acceptable numerical frequency ranges for each flight hour, as follows:

Table 3. Qualitative definitions of frequency levels

Probable	Failure condition frequency is more than 10^{-5} per aircraft flight hour.
Remote	Failure condition frequency is between 10^{-7} and 10^{-5} per aircraft flight hour
Extremely remote	Failure condition frequency is between 10^{-9} and 10^{-7} per aircraft flight hour
Extremely improbable	Failure condition frequency is less than 10^{-9} per aircraft flight hour.

JAR 25 allows failure conditions with the following combinations of severity and frequency:

- Minor severity may be probable.
- Major severity must be no more frequent than remote.
- Hazardous severity must be no more frequent than extremely remote.
- Catastrophic severity must be extremely improbable.

According to the rules described above, each airplane manufacturer sets its internal rules for development and manufacturing (system and hardware design and integration in *Fig. 2*). The feedback from operators (airlines) to manufacturers is strong, all events related to safety are recorded and analyzed. An alerting algorithm is introduced to distinguish events caused by random fault or error from the events originating from a common cause such as improper maintenance rules and activities, improper design etc., which require immediate actions.

4.3. Railway Transportation

In railway transportation, new European standards EN 50126 [3], EN 50128 and EN 50129 define the methods which can be applied to specify and set the required safety levels. Application of the SIL levels is obligatory, and the standards establish a link between tolerable hazard rates and SIL levels (see *Table 4* below). SIL0 must be selected if there is no safety relevance.

Table 4. THR and SIL in railway transportation

THR [1/hour]	Required SIL
$THR < 10^{-10}$	4
$10^{-10} \leq THR < 0.3 * 10^{-8}$	3
$0.3*10^{-8} \leq THR < 10^{-7}$	2
$10^{-7} \leq THR < 0.3 * 10^{-5}$	1

The methods determined by SIL and applicable in the software development are listed in the standards, and the application of the methods must be demonstrated in the approval procedure.

5. Conclusions

In this paper, the aims of the Safety Management Systems were summarized. As shown in this paper, there are fields where the SMS concept has been realized or introduced for the whole industry (e.g railways), but there is a chance to implement the SMS in road transportation or to expand the concept for the whole transportation sector by establishing global safety criteria.

References

[1] BLAKE, M. – FREI, CH. – KRAUS, F. – PATTON, R. J. – STAROSWIECKI, M., What is Fault-Tolerant Control? Preprints of Safeprocess'2000 (Ed. A. Edelmayer), 2000, pp. 40–51.

[2] BRABAND, J., Risk Assessment in Railroad Signalling: Experience Gained and Lessons Learned, *Proceedings of the Annual Reliability and Maintainability Symposium*, 2002. pp. 147–152.

[3] EN 50126: *Railway Applications: The Specification and Demonstration of Reliability, Availability, Maintainability and Safety* (RAMS), 2001.

[4] HAINDL, E. – LÖSER, F., Safety and Availability Analysis for Transrapid Maglev Transportation System, In: *Safety and Reliability*, (Eds. Schueller & Kafka). Balkema, 1999, pp. 415–420.

[5] KAFKA, P., How Safe is Safe Enough? – An Unresolved Issue for all Technologies. *In: Safety and Reliability (Eds. Schueller & Kafka)*. Balkema, 1999, pp. 385–390.

[6] LEITCH, R. D., *Reliability Analysis for Engineers*, Oxford University Press, 1995.

[7] ROWE, W., Risk Assessment Approaches and Methods, *In: Society, Technology and Risk Assessment*, (Ed. J. Conrad), Academic Press, 1980. pp. 3–29.

[8] STÖLZL, S. – ISERMANN, R., Online Supervision of Fault-Tolerant Systems for Safety-Related Applications. *In: Safety and Reliability*, (Eds. Schueller & Kafka), Balkema, 1999, pp. 397–401.

[9] SZABÓ, G. – GÁSPÁR, P., Probabilistic Dependability Analysis of Adaptive Functions: A Fault-Tree Based Approach and Its Application in Transportation. *Periodica Polytechnica Ser. Transp. Eng.*, **26** No. 1–2, (1998), pp. 187–200.

[10] SZÁSZI, I. – KULCSÁR, B. – BALAS, G. – BOKOR, J., Design of FDI filter for an aircraft control system. American Control Conference, ACC2002, Proc. on CD, Anchorage, Alaska, USA, 2002, pp. 4232–4237.

[11] WOLSTENHOLME, L. C., *Reliability Modelling*. Chapman & Hall/CRC, 1999.