Safety Analysis and Methods in a Railway Signalling System

Kwang-Chi Chang*, Key-Soe Lee and Jong-Ki Kim*****

Abstract - This paper intends to provide practical safety analysis methods and the criteria for method selections. A careful choice of safety analysis techniques will enhance the efficiency of the safety case process. A couple of recommendations are provided from practical experience.

Keywords: Markov, Railway Signalling, Safety analysis

1. Introduction

Safety analysis is not one, but a range of techniques, each providing a different insight into the characteristics of the system under investigation. Some methods have evolved within particular industries and have limited use in other areas. Other methods, even though they have originated from various specialized areas, have broad acceptance throughout many industrial sectors.

In this paper we will explain the safety-related tasks in a railway signalling project to provide the background of safety analysis, and look at several analysing methods associated with railway signalling systems. Finally, we will develop criteria in selecting a safety analysis method and suggest recommendations for proper analysis methods according to application purposes.

2. Safety Tasks in a Railway Signalling Project

Safety tasks are not simple tasks that are limited to a single phase of a project. Rather, safety tasks are performed on a continual basis and should normally extend throughout all project phases. The main features of the safety tasks over the project life cycle are summarized as follows:

Design Phase The main hazard identification, safety analysis work and risk assessments are undertaken at the design stage. Control measures are identified to ensure that the risk is tolerable and reduced to ALARP. The hazard log is established and this remains as a live document for the entire life of the Project.

Manufacturing Phase Design change control measures are established to ensure that the safety of the signalling system installation is not compromised by proposed changes to the design. A reporting system will be established by the manufacturer such that any hazards identified during the manufacturing of the signalling system are entered into the hazard log and acted upon.

Installation Phase A reporting system will be established by the manufacturer such that any hazards identified during the installation, maintenance and de-commissioning of the signalling system are entered into the hazard log and acted upon.

Testing Phase The testing phase is essential to verify that the safety and performance requirements of the customers have been met. The acceptance test results will be reviewed against the design safety case to ensure that all of the arguments presented are validated.

Operational Phase The O&M Manual will be provided so that the signalling system will be operated and maintained in a safe manner. Once the signalling system has been accepted for operation, continued safety will rely on correct maintenance, control of spare parts, and a proactive approach in identification of and systematic treatment of potential hazards. To this end, a Failure Reporting and Corrective Action System (FRACAS) will be established. This will provide a systematic framework for reviewing incidents so that their impact on safety can be quickly assessed and any corrective action taken. Again the hazard log is central to this process.

As briefly explained above, safety lifecycle and management is to be defined and integrated into the engineering process lifecycle. These tasks will be implemented by the following safety activities.

Safety Management Planning is the initial activity. Following nomination of a safety manager, a safety plan is defined. Usually the document is approved and endorsed by the customer and the responsible railway safety authority, if one exists. Hazard and Risk Analysis are carried out as the next activity. The purpose of this is to identify critical functions and their safety requirements. When the system architecture has been developed, safety integrity and RAM requirements for components of the architecture can be apportioned. All safety management

* Siemens AG, Germany (chang.kwang-chi@siemens.com)
** Kwangwoon University, Korea (kslee@daisy.kwangwoon.ac.kr)
*** Korea Railroad Research Institute (jkkim@krri.re.kr)

Received May 6, 2003 ; Accepted March 31, 2004

activities, hazards identified, decisions made and solutions adopted are recorded or referenced in a safety log. The adequacy and efficiency of safety management is verified by safety audits. Then, a strategy for satisfying the safety requirements is developed and documented in a safety case concept. The necessary evidence for the fulfilment of the safety requirements is prepared during the design and implementation phase, in particular by safety validation activities. The evidence is integrated in the safety case.

An independent safety assessor agreed upon by the customer and the responsible railway safety authority reviews the safety case. Details of the safety assessment are planned and approved by the railway authority as part of the project safety plan.

3. Overview of Safety Analysis Methods

There exist too many analysis methods and techniques for safety analysis (see e.g. Ref. [5] for an overview of 101 techniques). Some of them are required by international standards, but others are used only in limited applications. CENELEC EN 50129 provides general guidance on the usage of methods (refer to Table 1), which has been taken from EN50129, Table E.6. CENELEC EN50129 is a unique standard for railway application for safety related electronic systems for railway signalling. Even though this standard is a European standard, it is becoming a more international standard in railway industries. Accordingly it could be reasonable to select analysis methods, which will be investigated in this chapter, based on this standard.

4. Studies of the Methods

4.1 Preliminary Hazard Analysis (PHA)

The preliminary hazard analysis phase takes the hazards identified in the Preliminary Hazard Identification (PHI) phase and subjects them to a detailed study using HAZOP or certain other systematic techniques. Each hazard is considered in association with the functional requirements of the system to identify safety implications and to evaluate design alternatives. All the hazards identified are recorded in the hazard log, which represents an ongoing record of the safety issues of the system. The findings of the PHA are documented in the preliminary hazard analysis report. This provides a great deal of background information on the system and its hazards, including:

- a brief description of the system and its environment;
- an overview of the system's function and its safety features;
- the safety objectives of the system;
- justification of the risk and integrity level assignments made;
- target failure rates and safety level;
- sources of any data used within the analysis;
- a bibliography of all documents used.

Table 1 Guidance on safety analysis techniques from CENELEC EN 50129

Techniques/Measures	SIL1	SIL2	SIL3	SIL4
1. Preliminary Hazard Analysis	HR	HR	HR	HR
2. Fault Tree Analysis	R	R	HR	HR
3. FMECA	R	R	HR	HR
4. HAZOP	R	R	HR	HR
5. Cause-Consequence Diagrams	R	R	HR	HR
6. Markov Diagrams	R	R	R	R
7. Event Tree	R	R	R	R
8. Reliability Block Diagram	R	R	R	R
9. Zonal Analysis	R	R	R	R
10. Common Cause Failure Analysis	R	R	HR	HR
11. Historical Event Analysis	R	R	R	R

4.2 Fault Tree Analysis (FTA)

FTA is a very common, broadly used and internationally standardized technique [6]. Fault tree analysis (FTA) is a means of analyzing system failures in terms of combinations of subsystem and lower level faults, and eventually component faults. It is referred to as top-down analysis and identifies the causes of an unwanted top event, starting with a qualitative analysis followed by a quantitative analysis, if data are available. If fault data are available and the structure of the system is not too complex, it is a relatively simple matter to estimate the probability of the top event taking place, as shown in Fig. 1. It is often assumed that the input events are statistically independent. Should this not be the case, for example if a basic event occurs at more than one place in the fault tree, then the cut sets must be calculated. FTA easily deals with any combination of events, but has limitations with respect to modelling time-dependent behaviour. FTA can in this case be combined with Markov sub-models, which can be included as basic events in FTA (also called dynamic FTA).

4.2.1 Benefits

- It gives the designers an insight into the structure of the system.
- It is possible for the analyst to produce a list of all possible serious component fault combinations, some of which may not have been considered by the designers, including any single point failures.
- It permits the effects of external factors beyond the control of the designers to be analyzed.
- When the relevant data are available, the probability of the top event and hence possibly the system

reliability or availability can be estimated.

4.2.2 Limitations

- The analysis can be time consuming.
- It has to be repeated for each top event.
- For these reasons, it is often the case that only those top events that are judged to occur most commonly or those judged to have more important safety implications are analyzed.

4.3 Failure Mode Effects and Criticality Analysis (FMECA)

A failure mode and effects analysis (FMEA) is an inductive technique for establishing the effects of potential failure modes within a system. The analysis can be performed at any level of assembly. FMEA shows the effects of potential failure modes within a system on subassembly, subsystem and system functioning, taking into account the possible degradation of performance and the consequences for safety. FMEA identifies in a bottom-up fashion the effects of faults. It can be used for almost any problem and at any system level, e.g. for processes, functions, software, hardware or human tasks. Just like FTA, it is very common, broadly used and internationally standardised [6].

The analysis should be performed by a group that includes reliability and design engineers, and others who may be able to contribute to the analysis by virtue of their experience or familiarity with the system or similar equipment. Criticality analysis (CA) is an obvious next step after an FMEA. The combination is called an FMECA-failure mode and effects and criticality analysis. CA is a procedure by which each potential failure mode is ranked according to the combined influence of severity and probability of occurrence. The purpose of the criticality analysis (FMECA) is to identify the failure mode and then rank each potential failure effect according to its criticality. Table 2 below shows an example of FMECA in a railway signalling system.

4.3.1 Benefits

- It provides designers with an understanding of the factors that influence the reliability of a system.
- It helps to identify items that place reliability at risk.
- It helps identify potential fault modes whose effects are unacceptable.
- It provides an objective basis for deciding priorities for corrective design action.
- It can be used as a basis for fault diagnosis, and to determine testability parameters.
- It can identify high-risk areas and items where special inspection, test or maintenance requirements are needed.
- It can produce recommendations for production, such as quality of bought-in components, inspection, etc.
- It can establish whether there are any constraints imposed on the user by the design.
- It can be used as a basis for maintenance planning.

4.3.2 Limitations

- FMEA is often expensive and time consuming.
- Only one failure at a time can normally be considered.

4.4 Hazard and Operability Study (HAZOP)

Originally used in chemical industries, HAZOP is a method of team review of the significance of all of the ways a process element can malfunction or be incorrectly operated. The technique is, essentially, a structured brainstorming using specific guidewords. While there are many sector-specific standards, there is also an international, sector-independent one [8]. In identifying the subsystem of the plant that gives rise to an accident initiator, it is useful to list guidewords that stimulate the exercise of creative thinking. A HAZOP (Hazard and Operability study) suggests looking at a process to see how it might deviate from design intent by applying guidewords. For example, more of, less of, none of, part of, reverse, wrong address, other than, as well as, etc. The HAZOP study begins by identifying the interconnection between

Table 2 An example of FMECA according to IEC60128

No	item name	failure mode	failure cause	failure effect		fallback function	failure detection	failure probability	criticality level	remark
				local effect	end effect					
1	VENUS2	faulty data processing	device failure	cut off	loss of supervision	RM1	error message to CTC	3.4E-06	critical	SN VENUS2
2	VESUS3	comparison failure	device failure	none	none	not relevant	no message	1.6E-06	insignificant	SN VENUS-3
3	...									
4	...									
5	...									

Table 3 An example of HAZOP

item	inter-connection	attribute	guide word	cause	consequence	recommendation
1	sensor supply line	supply voltage	No	PSU, regulator or cable fault	lack of sensor signal detected and system shut down	
			More	regulator fault	possible damage to sensor	consider over-voltage protection
			Less	PSU or regulator fault	incorrect temperature reading	include voltage monitoring
		sensor current	More	sensor fault	incorrect temperature reading, possible loading of supply	monitor supply current
			Less	sensor fault	incorrect temperature reading,	monitor supply current
2						

components within the system and determining the corresponding interactions. These interactions may consist of the physical flow of material from one component to another, as in the case of a chemical plant, or may represent the flow of electricity, signal and data. Such flows are referred to as entities. Each entity processes certain properties or attributes that determine the correctness of the system's operation. Deviation from the design values for these attributes may have implications for the correct operation of the system. The study is based on a rigorous and systematic investigation of possible deviations from each of the identified attributes. In order to structure the assessment process, a series of guide words is used to define the particular type of deviation. Table 3 shows an example of HAZOP.

4.4.1 Benefits

- It can be very effective.
- It is very methodical. Use of guide words can give confidence in completeness of analysis.
- Team conclusions may carry more weight than those reached by an individual analyst.

4.4.2 Limitations

- It can produce lots of output.
- Team approach is expensive – must be shown to be cost-effective.
- It is only a qualitative analysis method.
- It relies heavily on expert input.
- It can be very effective but is also very tedious and time consuming.

4.5 Cause-Consequence Diagram (CCD)

CCD (Cause-Consequence Diagram) is an integration of deductive (fault tree) and inductive (event tree) analyses into a single method and notation. It was developed at the Riso Laboratory in Denmark in the early 1970s, initially for nuclear applications. It has been evaluated by French, American and Canadian nuclear industries, but there are few documented examples of its use on real systems outside the nuclear industry. Particularly, it is suited to analysis of systems, which include protective mechanisms. Even though there are some particular expressive notations in this method, it is a combination of the ETA and FTA in principle, where the cause of initiating events of an ETA is basically analyzed by FTA. For this reason, it has not been standardized and is therefore not further discussed here.

4.6 Markov Models

Markov Models are a widely used standardized method [9] for any type of dependability modelling. In contrast to FTA, they can handle time or sequence dependencies. A variant of Markov models are Petri nets, which are often more comfortable for the graphical representation of the model. As both have the same dependability modelling capability, Petri nets are not discussed as a method here. Markov techniques are used mainly to model system repair strategies. The method is based on representing a particular combination of failed and functioning units as states. The failure or repair of a unit is regarded as a transition between the corresponding states. State diagrams are prepared in this way to represent all possible states of system operation from the fully operating state, through partially operating states, to the fully failed state. By calculation of the probabilities associated with each state, system reliability parameters can be obtained. The process of constructing a transition state gives considerable insight into the strength and weakness of the system. The technique is especially useful for the analysis of complex systems and would not normally be applied to systems in which there is no redundancy. The technique of Markov analysis can be used for modelling repair strategies and comparing the resultant system reliabilities and availability to enable an appropriate maintenance option to be selected. Fig. 1 represents an example of a Markov model, which shows 5 states for the communication equipment used in a safety related application. We will not investigate this model in detail because it is not relevant to the scope of this paper.

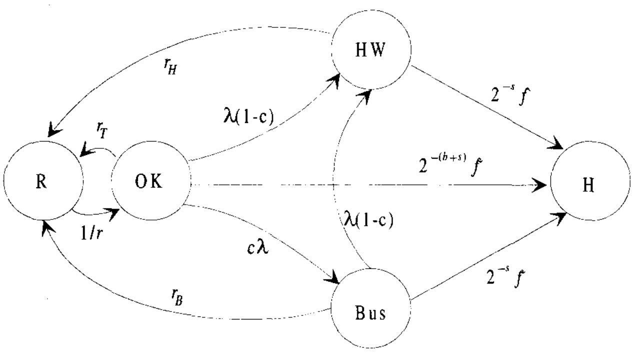
4.6.1 Benefits

- The state diagram gives insight into the consequences of failures and repairs and may provide suggestions for system reliability improvement.
- It provides a probabilistic model for a system state behaviour.
- It provides probabilistic solutions for sub-sets of other models such as RBD and Fault Tree.

4.6.2 Limitations

- It can become very complex for large numbers of states.

It depends normally upon the assumption that transition rates are constant.



Remarks
R: Repair
OK: Normal operation condition
HW: Hardware failure
Bus: Transmission codec failure
H: Hazard
λ : Failure rate
c : Percentage of undetected hardware failure
f : Frequency
r : MTTR

Fig. 1 An example of the Markov model

4.7 Event Tree Analysis (ETA)

ETA is used when it is essential to investigate all possible paths of consequent events, their sequence and the most probable outcome/consequence of an initiating event. ETA is widely used in risk analysis to analyze the consequences of events, which follow after an initial event. However, there is no international standard, but several national standards [12]. ETA is a technique used to identify the possible outcomes and if required, their probabilities, given the occurrence of an initiating event. This analysis is used for facilities provided with engineered accident mitigating features, to identify the sequence of events, which lead to the occurrence of specified consequences, following the occurrence of the initiating event. It is assumed that each event in the sequence is either a success or a failure. ETA is an inductive analysis in which the basic question is "what happens if ..?". An example of ETA is shown in Fig. 2 below.

4.7.1 Benefits

- Provides the relationship between the functioning or failure of various mitigating systems.
- Identifies events that require further analysis using fault tree analysis (FTA); i.e. the top event of the fault trees.

4.7.2 Limitations

- Only success and fault states of a system are dealt with; it is difficult to incorporate delayed success and recovery events.
- There is always a potential for missing some crucial initiating events.

4.8 Reliability Block Diagram (RBD)

RBD [11] is the graphical representation of a system's logical structure in terms of sub-systems and/or components. This allows the system success paths to be represented in the way the blocks (sub-systems/ components) are logically connected. Usually, the application of RBD is limited to non-repairable systems. The purpose of RBD is to present failure criteria pictorially and to use the diagrams to evaluate the system reliability/availability parameters. For these reasons the functional block diagram must be converted into a reliability block diagram. Elementary models (each block should be independent of other blocks) are series, parallel, M out of N and standby. More complex models in which the same block appears more than once in the diagram can be assessed by the use of:

- The theorem of total probability; and,
- Boolean truth tables.

An example of RBD is shown in Fig. 3

4.8.1 Benefits

- The graphical presentations are easily understood and readily interpreted.
- Relationships between the elements of a system can be identified.
- The overall system reliability/availability can be determined by using probability laws.

4.8.2 Limitations

- Systems in which the sequence of failures affects the results cannot be modelled.
- Maintenance strategies for repairable systems cannot be considered.

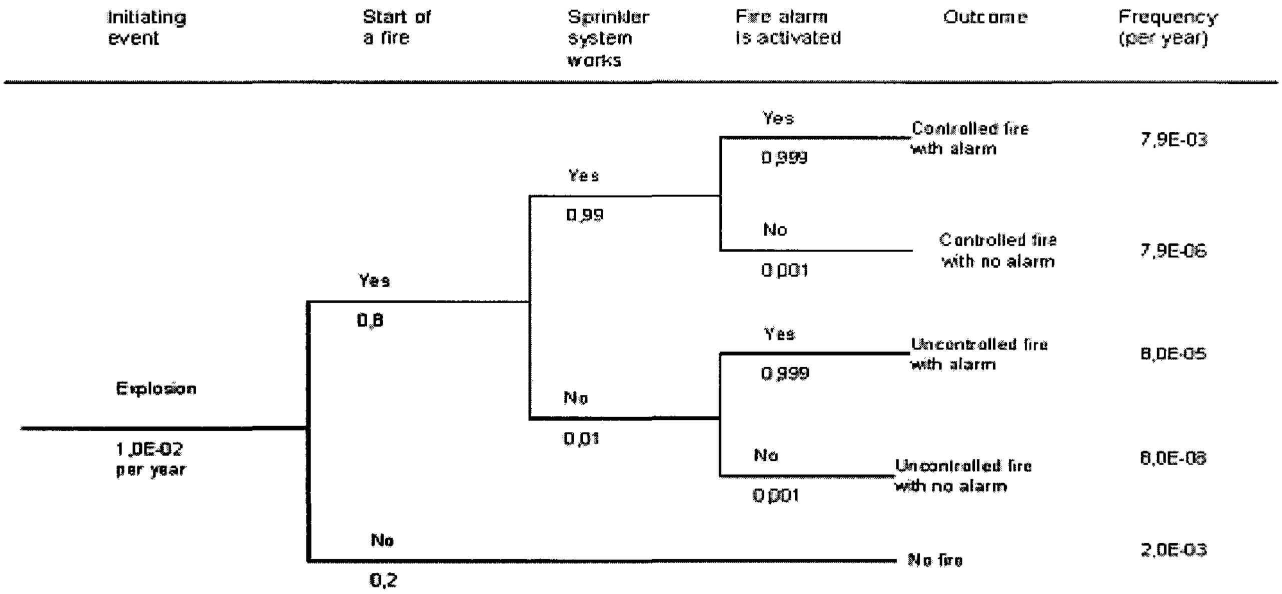


Fig. 2 An example of ETA

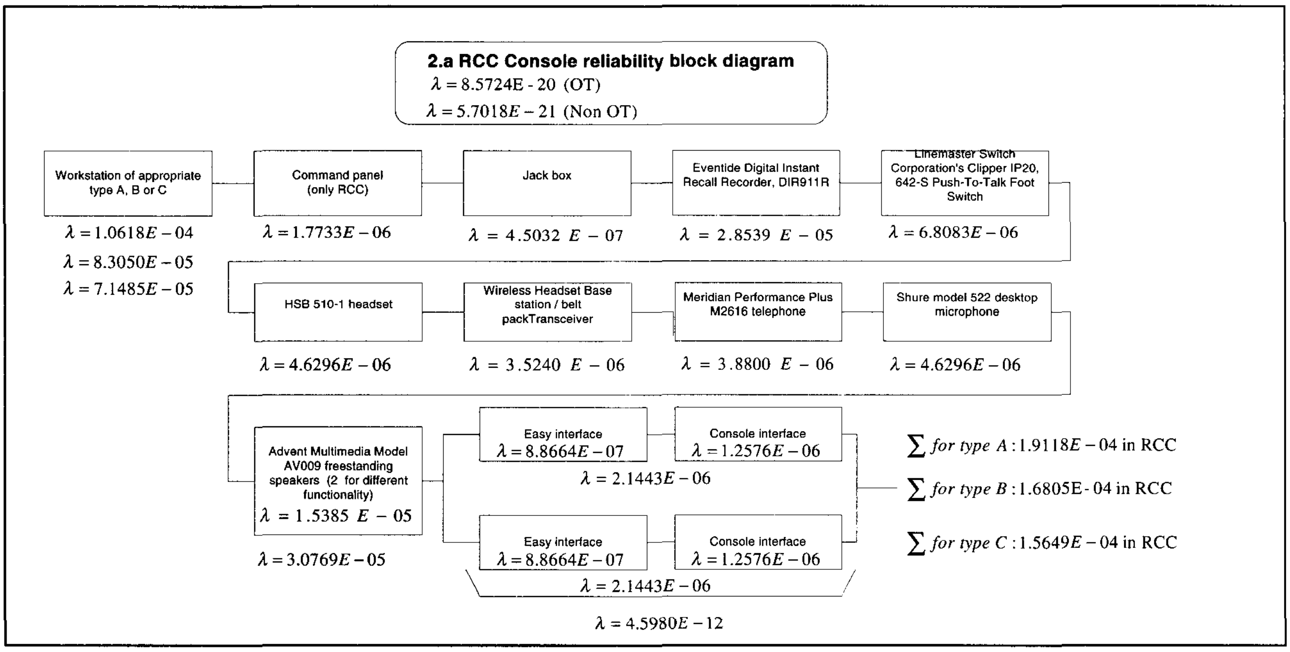

2.a RCC Console reliability block diagram
$\lambda = 8.5724E - 20$ (OT)
$\lambda = 5.7018E - 21$ (Non OT)
Workstation of appropriate type A, B or C
$\lambda = 1.0618E - 04$
$\lambda = 8.3050E - 05$
$\lambda = 7.1485E - 05$
Command panel (only RCC)
$\lambda = 1.7733E - 06$
Jack box
$\lambda = 4.5032\ E - 07$
Eventide Digital Instant Recall Recorder, DIR911R
$\lambda = 2.8539\ E - 05$
Linemaster Switch Corporation's Clipper IP20, 642-S Push-To-Talk Foot Switch
$\lambda = 6.8083E - 06$
HSB 510-1 headset
$\lambda = 4.6296E - 06$
Wireless Headset Base station / belt packTransceiver
$\lambda = 3.5240\ E - 06$
Meridian Performance Plus M2616 telephone
$\lambda = 3.8800\ E - 06$
Shure model 522 desktop microphone
$\lambda = 4.6296E - 06$
Advent Multimedia Model AV009 freestanding speakers (2 for different functionality)
$\lambda = 1.5385\ E - 05$
$\lambda = 3.0769E - 05$
Easy interface
$\lambda = 8.8664E - 07$
Console interface
$\lambda = 1.2576E - 06$
$\lambda = 2.1443E - 06$
Easy interface
$\lambda = 8.8664E - 07$
Console interface
$\lambda = 1.2576E - 06$
$\lambda = 2.1443E - 06$
$\lambda = 4.5980E - 12$
$\sum$ for type A : 1.9118E − 04 in RCC
$\sum$ for type B : 1.6805E- 04 in RCC
$\sum$ for type C : 1.5649E − 04 in RCC

Fig. 3 An example of RBD

- Each failure definition in a given system needs a separate block diagram.

4.9 Common Cause Failure (CCF)

The purpose of CCF analysis is to identify any cause in which two or more events could occur as the result of a common event or causative mechanism. If the probability of a common cause is significantly greater than the probability of two or more events occurring independently, then the common cause could be an important risk contributor. This task is very important e.g. for the proper handling of AND gates in fault trees, where independence is assumed. Common factors, which are typically considered, include:

- physical location;
- manufacturing process; and,
- human error.

This analysis requires generally very detailed knowledge of system.

Table 4 Guidance on safety analysis techniques from CENELEC EN 50129

Method	suitable for complex system	suitable for novel system design	quantitative analysis	suitable for combination of faults	suitable to handle sequence dependence	bottom-up or top-down	suitable for safety integrity allocation	suitable for high safety requirement	mastery required	acceptance and commonality	need for tool support	plausibility checks	availability of tools	International standard
ETA	nr	nr	yes	nr	yes	B-U	nr	nr	high	avg	avg	yes	avg	-
FMECA	nr	nr	yes	no	no	B-U	nr	no	low	high	low	yes	high	60812
FTA	yes	yes	yes	yes	no	T-D	yes	yes	avg	high	avg	yes	high	61025
HAZOP	nr	nr	no	no	no	B-U	no	nr	low	avg	low	yes	avg	61882
Markov	yes	yes	yes	yes	yes	T-D	yes	yes	high	avg	high	no	avg	61165
RBD	yes	nr	yes	yes	no	T-D	yes	nr	low	avg	avg	yes	avg	61078

Index:

Nr may be used for simple system, not recommended as a stand-alone method

T-D Top-Down, B-U Bottom-Up, avg. average

4.10 Historical Event Analysis

This is a very general collective term, which could mean to learn from the past accident sequences and field data. As it does not describe particular techniques on its own, it is not considered further here.

5. Criteria for Selecting Safety Analysis Method

The selection of methods is a highly individualized process so that a general suggestion for a selection of one or more of the specific methods cannot be made. The selection of appropriate methods needs to be done by the joint effort of experts in the safety and system engineering field. Selection should be carried out early in safety program development and should be reviewed for applicability. However, selecting methods can be made easier by using the following criteria:

- System complexity: Complex systems, e.g. involving redundancy or diversity features, usually demand a deeper level of analysis than simpler systems.
- System novelty: A completely new system design may require a more thorough level of analysis than a well-proven design.
- Qualitative vs. quantitative analysis: Is a quantitative analysis necessary?
- Single vs. multiple faults: Are there relevant effects arising from a combination of faults or can they be neglected?
- Time or sequence-dependent behaviour: Does the sequence of events play a role in the analysis (e.g. the system fails only if event A is preceded by B, not vice versa) or does the system exhibit time-dependent behaviour (e.g. degraded modes of operation after failure, phased missions...)?
- Bottom-up vs. top-down analysis: Usually, bottom-up methods can be applied in a more straightforward manner, while top-down methods need more thought and creativity and may therefore be more error-prone.
- Allocation of safety requirements: Should the method be capable of quantitative allocation of reliability requirements?
- Mastery required: What level of education or experience is required in order to meaningfully and correctly apply the method? Is the method easily explained to system engineers so that they can be involved?
- Acceptance and commonality: Is the method commonly accepted, e.g. by a regulatory authority or a customer? Is the method accepted by the system engineers?
- Standardization: Is there a standard, which describes the features of the method and the presentation of results (e.g. symbols)?
- Need for tool support: Does the method need tool support or can it also be performed manually?
- Availability of tools: Are tools available either in-house or commercially? Do these tools have a common interface with other analysis tools so that results may be re-used or exported?

Table 4 provides an overview of various safety analysis methods and their characteristics.

More than one method may be required to carry out a complete system analysis.

6 Conclusions

A careful selection of safety analysis techniques greatly enhances the efficiency of the safety case process. Although there is no magical solution that works in all cases, a couple of recommendations can be made based on practical experience:

- Historical experience or field data should be used wherever possible.

- For hazard identification, FMEA or HAZOP are the recommended techniques.
- For simple serial systems, FMECA may be sufficient.
- For a consequence analysis as part of a risk analysis, ETA is recommended. FMECA should be used for simple systems only.
- For hazard analysis and the safety case of complex systems including redundancy or interacting subsystems, FTA in combination with FMEA is recommended.
- If it is necessary to consider time-dependent properties of systems, FTA should be combined with the Markov method (Markov sub-models for basic events) or the Markov method should be used directly (also in combination with FMEA).
- A CCF analysis is necessary for all systems where the independence of items is claimed.

References

[1] Dr.Lauwers, Generic RAMS process for projects, VT 1 SYS, Siemens 1998,

[2] EN 50126 Railway Applications: The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), CENELEC, May 1998

[3] EN 50129 Railway Applications: Safety-related Electronic Systems for Signalling, CENELEC, November 2000

[4] Braband, J. and Lennartz, K., A Systematic Process for the Definition of Safety Targets for Railway Signalling Applications, Signal+Draht 9/99

[5] System Safety Handbook, System Safety Society, 1999,

[6] Fault Tree Analysis (FTA), IEC 61025

[7] Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA), IEC 60812

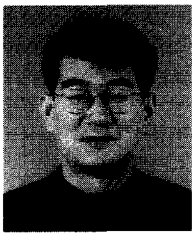
[8] Hazard and Operability (HAZOP) Studies - Guide Word Approach, IEC 61882

[9] Application of Markov Techniques, IEC 61165

[10] Analysis Techniques for Dependability - Reliability Block Diagram Method, IEC 61078

[11] Electronic Components – Reliability – Reference Conditions for Failure Rates and Stress Models for Conversion, IEC 61709

[12] Ereignisablaufanlayse, DIN 25419



Kwang-Chi Chang

He received his B.S. degree from Yonsei University, and his M.S. degree from Kwangwoon University. His research interests are in the areas of railway signalling, RAMS management. He works for Siemens Transportation Group in Germany as a RAMS manager.

Key-Soe Lee

Professor, System engineering Kwang woon University His research interests are in the areas of fault tolerant system design, digital control system, railway signalling and RAMS.

Jong-Ki Kim

He received his B.S. degree from Kwangwoon University and his M.S. degree from Inha University. His research interests are in the areas of railway signalling and RAMS management.