한국철도학회논문집
제7권 제3호 2004년 ‖ pp.251-258

A Case Study for Safety Analysis

안전성 분석에 대한 사례 연구

Kwang-Chi Chang[1] · Key-Seo Lee[2]
장광지 · 이기서

Abstract

A systematic methodology to determine safety requirements for railway signalling system and safety requirement allocation into system are presented. THR concept is used for as an interface between Risk Analysis to be performed by railway operator and System Design Analysis by the supplier. This approach is based on Signalling Safety Standard EN50129 by CENELEC.

Keywords : Safety Analysis, SIL (Safety Integrity Level), THR (Tolerable Hazard Rate), FMEA (Failure Mode and Effect Analysis), FTA (Fault Tree Analysis)

1. Introduction

Safety analysis plays a vital part in the development of any safety-critical system. It must be carried at an early project stage, as its results have a great influence on all aspects of the project. Moreover the safety analysis is not a "One-Off" procedure performed at the beginning of the project, and so it will continue through the development process. It also demands a range of techniques, each providing a different insight into the characteristics of the system under investigation. Safety analysis has many purposes according to approaching aspect, but one of the main purposes is to induce safety target and allocate it into system as safety requirement.

Many safety analysis technologies come from reliability analysis technologies and the approach shown in this paper is based on CENELEC standard. Accordingly some information can be known already. But this paper intend to introduce sequential tasks and its procedure necessary for safety analysis, and look at some practices in a railway signalling system for Korean Railway Safety Engineers.

A Level Crossing system (LC) will be assumed and applied to provide practices of safety analysis in order to work out the major safety aspects clearly. Major aim is to present a guidance of safety analysis. The values used in the calculation are arbitrary one.

Finally we will explain how to set a safety target and to allocate the safety target into subsystems by safety analysis.

2. Task of Safety Analysis

It is necessary to set a safety analysis procedure model, which shall be agreed between the safety related parties in the project. In general safety analysis is composed of the risk analysis and the system design analysis, and each analysis includes further analysis or tasks. One of the important aspects in this model is the different roles between suppliers and the railway authority. At the centre of the safety analysis process there shall be a well-defined interface between the supplier and the railway authority. From the safety point of view this interface is defined by a list of hazards and Tolerable Hazard Rates (THR)

1 Siemens, RAMS Manager
2 Kwangwoon Univ. Professor

associated with the system.

Risk Analysis will be performed by the Railway Authority including following tasks;

- to define the requirements of the railway system
- to identify the hazards relevant to the system
- to derive the tolerable hazard rates
- to ensure that the resulting risk is tolerable

The major requirement is that the tolerable hazard rates must be derived taking into account the risk tolerability criteria. Risk tolerability criteria are not defined by standards, but depend on national legislative requirements. Risk tolerability criteria may be explicit or implicit. Explicit criteria demand estimation of the (individual) risk, while implicit criteria demand to demonstrate that a new system is at least as safe as an approved reference system. In this case the tolerable hazard rates may be derived from comparison with the performance of reference systems, either by statistical or analytical methods.

The supplier's task (System Design Analysis or Causal analysis) comprises;

- definition of the system architecture
- analysis of the causes leading to each hazard
- determination of the safety integrity requirements for the subsystems
- determination of the reliability requirements (Failure Rates (FR)) for the equipment

Causal analysis constitutes two key stages. In the first phase the tolerable hazard rate for each hazard is apportioned to the level of system functions. Safety Integrity Levels (SILs) are defined at this functional level for the subsystems implementing the functionality. The hazard rate for a subsystem is then translated to a SIL using a SIL table. During the second phase the hazard rates for subsystems are further apportioned leading to failure rates for the equipment, but at this physical implementation level the SIL remains unchanged. The apportionment process may be performed by any method that allows a suitable representation of the combination logic, e.g. reliability block diagrams, fault trees, binary decision diagrams, Markov models etc. In any case particular care must be taken when independence of items is required. While in the first phase of the causal analysis functional independence is required, physical independence is sufficient in the second phase. Assumptions made in the causal analysis must be checked and may lead to safety-relevant application rules for the implementation.

The risk analysis and the system design analysis have to be approved by the Safety Authority.

3. A Case Study for Safety Analysis

3.1 System Definition

The First step of the safety analysis is to define system and its boundary clearly. The definition of the system is very important because final identification of hazards can not be made before the scope, boundaries and the application conditions of the system are well defined.

One particular type of automatic Level Crossing system (LC), which uses light signals for the road user and a distant signal for the train driver is under analysis. The following table gives a description of the principle function

Table 1. Function of LC Units

No.	Functional unit	Remark
01	Switch on LC	This function is responsible to trigger the LC switch-on when train approaches (usually implemented by train sensors like e.g. axle counters)
02	Switch off LC	This function is responsible to trigger the LC switch-off after the train has left the crossing (usually implemented by train sensors like e.g. axle counters)
03	LC Monitoring	Display of the state of the LC to the train driver or interlocking (usually implemented by a signal), so that the correct operation can be monitored
04	Road Signalling	Display of the state of the LC to road users
05	Normal positioning	The LC is set back to normal position (no protection) if the LC is switched on but not switched off after a certain time (e.g. due to sensor failure or the train stopped before the LC etc.)
06	Power Supply	Usually the normal power network. As a fallback LCs have a battery, which can operate the LC for a certain time, e.g. 2 hours. The battery voltage is usually remote controlled by the interlocking
07	Controller	Programmable electronic device, which operates and controls the LC, with application SW, site-specific data etc.

units of the LC under consideration.

A functional description of the fault-free operation of the example LC is shown in the picture below.

1) An approaching train is detected by the switch-on element (01) and is being reported to the controller unit (07).
2) The controller gives the command to switch-on the road signals (04). The controller waits until successful switch-on is reported back.
3) LC controller gives the command to switch-on the distant signal. Default position is off. If the distant signal is off, an approaching train has to stop at the LC and the LC could be manually operated as a fallback mode.
4) When a train leaves the LC, it is detected by a switch-off element (02) and reported to the controller unit.
5) The controller gives the command to switch off the distant signal. After a certain waiting time the road signals are switched off.

3.2 Hazard Identification

"A hazard is a condition or state that could lead to an accident. In the context of a system safety, a hazard is an unprotected state of the system, which under certain external conditions leads to an accident". The identification of hazards starts with obtaining information about Safety requirements, past Safety performance, identified sources of hazards. It carries on with describing the scope of the system hazard analysis and making preliminary hazard identification. Hazard Identification involves systematic analysis of a system to determine those adverse conditions (hazards), which may arise throughout the life-cycle. Systematic identification of hazards generally involves two phases:

- an empirical phase (exploiting past experience, e. g. checklists)
- a creative phase (proactive forecasting, e. g. structured what-if studies, Hazard and Operability(HAZOP))

The empirical and creative phases of Hazard Identification complement one another, increasing confidence that the potential hazard space has been covered and that all significant hazards have been identified. It should be noted that identification of a single significant hazard might outweigh identification of a large number of less significant hazards. That means that the quality is the essence rather than the quantity.

There are some techniques for hazard identifications. Failure Modes, Effect Criticality Analysis (FMECA) and HAZOP are more frequently suggested. In practice empirical database is quite useful in hazard identification for railway signalling system because of its cumulative experience in well-defined structure. However in case of new product development, creative phase is quite important.

This paper does not perform a complete hazard identification, but considers one major hazard H_1="*Failure of LC to protect public from train*". It covers all situations, where the LC should warn the public (of approaching trains), but does not fulfil this task. Note that in our perspective events like track circuit fails to detect train are not a hazard to be considered at this level, because although this event might lead to an accident when occurring at a level crossing, in our consideration, it is only a cause of a hazard, not a hazard in its own right on system level.

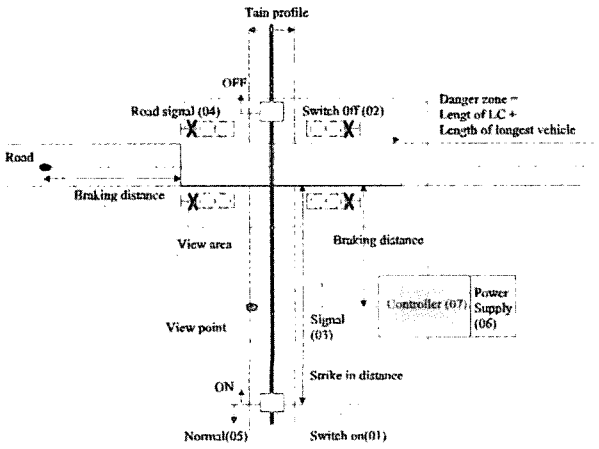

Fig. 1. Level Crossing System Overview

3.3 Risk Analysis

Consequence analysis is started after hazards are identified. The frequency, the likely severity of the consequences, and the risk for each hazard shall be evaluated. The acceptability of the risk associated with each hazard shall be determined and classified. Then the results of the consequence analysis are transferred into the system require-

ment specification as safety function requirements, safety integrity requirements for each function and application environment. Starting from the hazard, all physical, procedural and circumstantial barriers are captured from an expert panel that are familiar with the escalation mechanisms and the existence of various protection measures in the environment of application. A graphical structure is thus produced for representing various escalation scenarios arising from the hazard, depending on the success or failure of each barrier. When no further barriers can be identified, consequences are arrived at situations from safe status to a wide range of incidents and accidents with varying degrees of loss:

- Safe or loss free Consequences
- Consequences primarily entailing Safety Loss
- Consequences primarily entailing Commercial Loss
- Consequences primarily entailing Environmental Loss

The Consequence Analysis results in forecasting a range of incidents and accidents, which arise as a result of the various combinations of success and failures of defensive mechanisms, once a hazard has occurred. Once a Consequence model is developed, the strength of each barrier can be quantified in terms of the probability of failure. In combination of these failure probabilities the probability of a particular accident arising from a hazard can be estimated. For the consequence analysis ETA method are mostly applied.

3.3.1 Quantitative Risk Analysis

An approach to determination of safety risks is pertinent to novel or potentially high-risk hazards. The aim is to systematically and objectively arrive at a quantitative Tolerable Hazard Rates (THR). A mathematical model for the determination of individual risk is given, taking into account the causality leading from hazards to accidents.

An individual *i* uses a technical system (here level crossing (LC)). The usage profile is described by the number of uses N_i (per year). For reference a total exposure per use E_i may be defined (i.e., the duration of a train journey or the time needed to pass a LC).

While operating the technical system the individual is exposed to hazards arising from failure of the technical system. This is described by the list of hazards and the corresponding hazard rates $\{(H_j, HR_j)\}$. The probability that the individual is exposed to the hazard depends additionally on the hazard duration D_j and the exposure time E_{ij} of the individual to the hazards. This probability consists of a sum of the probability that the hazard already exists when the individual enters the system (approximately $HR_j D_j$) and the probability that the hazard occurs while the individual is exposed (approximately $HR_j E_{ij}$). Note that the exposure to the hazard H_j may be shorter or equal than the total exposure: $E_{ij} \leq E_i$.

From each hazard one or several types of accidents may occur. This is described for each hazard by the consequence probability C_j^k, that accident k occurs. This probability stands for the external risk reduction factors derived by consequence analysis. To each type of accident A_k associated there is a corresponding severity (derived by the loss analysis), which from the individual point of view is described as the probability of fatality F_j^k for the single individual.

This causality corresponds one to one to the individual risk of fatality defined by,

IRF_i is

$$\sum_{All\ Hazard\ H_j} N_i \left[(HR_j \times (D_j + E_{ij}) \sum_{Accident\ A_k} C_j^k \times F_j^k \right] \qquad (1)$$

Formula (1) can be calculated either by using mean values or by inserting statistical distributions for the input parameters. If, as a result the individual risk is less than the target individual risk, then the calculated or estimated Hazard Rates (HR) are called as Tolerable Hazard Rates (THR).

3.4 Risk Tolerability

Risk acceptance is a societal and legal issue. Therefore it should be based on generally accepted principles or consensus. As Low As Reasonably Practicable (ALARP) or any similar risk tolerability principle or benchmark figures are frequently used to fix target. In this thesis, benchmark figures from Railtrack's Railway Group Safety Plan (1997/98) are used. There it is said that "*Reasonably practicable schemes will continue to be implemented with the aim of ensuring that automated level crossings expose the individual occupants of road vehicles to a risk of fatality no*

greater than one in 100,000 regular users per annum by the year 2000".

In order to define the "broadly acceptable bound", we take an additional safety factor of 10 into account. This means that the individual risk for a regular user should be less than 10^{-6} per year, which we take as the Tolerable Individual Risk (TIR) value.

3.5 Determination of Individual Risk

We follow the approach summarized by formula (1). For the purpose of our example we look at one particular type of individual: a commuter crossing a railway line regularly, say N_i=1000 times a year. We do not regard other users like pedestrians or cyclists here. We assume that we know from operational experience that hazard H_1, if it occurs, lasts much longer than the individual exposure time, which would be the time for crossing the LC. This means we can disregard the individual exposure time E_{i1} in (1). As a pessimistic estimate we use a hazard duration time D_1=10 hours, which is the time the LC has the wrong-side failure (until negated or repaired).

3.6 Cause Consequence Analysis

Consequence Analysis is aimed at identification, capture and quantification of a range of likely outcomes, arising from a hazard. In this perspective, all events after a hazard has occurred lie in the consequence domain. This analysis corresponds to the determination of the external risk reduction C_j^k in formula (1).

Starting from the hazardous or Critical Event, all physical, procedural and circumstantial barriers are elicited from the expert panel who are familiar with the escalation mechanisms and the existence of various protection measures in the environment of application. A graphical structure is thus produced representing various escalation scenarios arising from the hazard, depending on the success or failure of each barrier. When no further barriers can be identified, Consequences are arrived at which range from safe and benign conditions to a wide range of incidents and accidents each with varying degrees of loss.

Once a Consequence model is developed, the strength of each barrier can be quantified in terms of the probability of Failure. This, together with the rate or probability of the Critical Event, facilitates the computation of the rate or probability for various forecast accidents (Consequences).

The aim of Consequence Analysis is to systematically develop potential scenarios post realization of a hazard and identify a broader spectrum of accidents and incidents than the traditional "worst case". In practice, most consequences associated with a hazard have safety and commercial implications. The loss potential for the hazard is therefore the sum of individual safety and commercial losses pertaining to each forecast accident. In order to determine the consequences of LC we have to look at the scenario that an individual meets hazard H_1, which means we look at one particular occurrence of a driver approaching an unprotected LC. By using ETA method, determination of external risk can be reduced as below. This analysis identifies two types of accident and the external risk reduction factors between the initial hazard and the accident. This is an inductive method of analysis where the hazard under consideration is displayed at the left of a decision-tree structure. Possible protective barriers affecting event escalation are then identified, classified and assessed. The potential outcomes as a result of success or failure of the barriers are presented at the end of right side. Figure. 2 was adjusted from the Consequence Analysis of [7].

3.7 Loss Analysis

Most accidents entail a measure of loss which, depending on the severity and energy, location, materials and the number of people involved would comprise Safety, Commercial and potentially Environmental dimensions. However, objective estimation of each component is dependent on a large number of case specific parameters. The more reliable computed value for THR developed through Quantitative Consequence and Loss analyses primarily addresses the criticality due to the operational environment. It can sub-

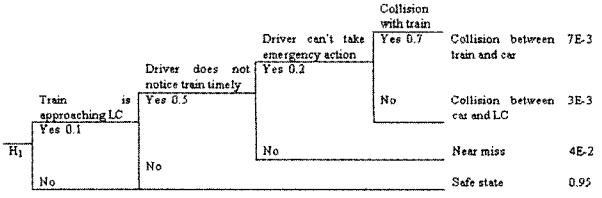

Fig. 2. Causal-Consequence Analysis using ETA

Table 2. Risk Reduction Parameters

No.(k)	Accident(Ak)	Risk reduction factor (C_1^k)	Probability of fatality (F_j^k)
1	Collision between train and car	0.007	0.8
2	Collision between car and LC	0.003	0.05

sequently be employed in the determination of the system architecture and Safety Integrity requirements for systems and subsystems.

As a result we have identified two types of accidents and the external risk reduction factors between the initiating hazard and the accidents. For the purpose of this example we roughly estimate the accident severity as a probability of fatality, which could be derived from the statistics of railway operators. The results are summarized in the following table.

3.8 Determination of THR

We can now determine the tolerable hazard rate THR_1 for H_1 from the input parameters by simplifying formula (1) only for one hazard H_1:

IRF_i is,

$$N_i\left[(HR_1\times(D_1+E_{i1})\sum_{Accident\,A_k} C_1^k\times F_j^k\right]$$
$$=1000\times HR1\times 10\times(0.007\times 0.8+0.003\times 0.05) \quad (2)$$

This results in $HR_1 \cong 1.8\times 10^{-8}$/h, which is now called THR_1. This corresponds to approximately one tolerable hazard per LC per 6300 years. Here we assumed only one hazard, but in case of multi-hazards handling, THR shall be selected after whole calculation of THR_S by using formula (3).

$$THRS = Min\ \{THR_1, THR_2 \ldots THR_n\} \quad (3)$$

where THR_S stands for the subsystems THR and the THR_n for the contributions of the functions.

3.9 System Design Analysis

The Figure 3 below shows the detail procedure in System Design Analysis with intention of setting safety target in terms of Safety Integrity Level. Starting from the

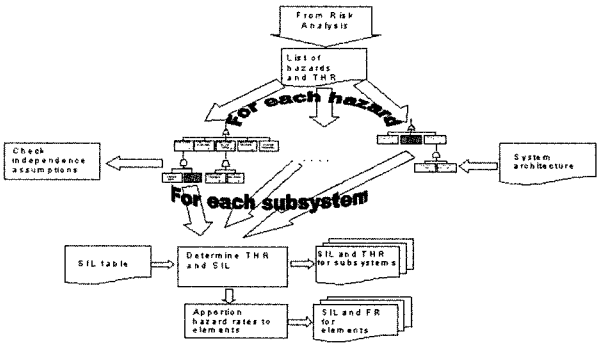

Fig. 3. System Design Analysis

THR for a subsystem S the SIL shall be determined by use of a SIL table T (e. g. IEC 61508 or EN 50129), which gives the correspondence between SIL and THR:

$$SIL_S = T(THR_S) \quad (4)$$

Combination of (3) and (4) leads to

$$SIL_S = Max\ \{SIL_1, SIL_2 \ldots SIL_n\} \quad (5)$$

In our example case of Level Crossing, SIL level of total system will be allocated as 3 according to SIL table from IEC 61508, which specifies THR value $10^{-8} < THR < 10^{-7}$ as SIL 3.

3.9.1 FMEA Analysis

To start system Design Analysis, it is necessary to investigate possible failure effects of each function units defined at system definition phase. FMEA is a useful tool for this purpose.

3.9.2 FTA Analysis

Based on above functional FMEA analysis, we can produce following Fault Tree Analysis (FTA) as a causal analysis. In this case FTA shall be a top-down approach to allocate THR into functional units. The results with suggested THR allocations are shown below.

Allocations of THR at the top level are arbitrary in this study, but it shall be discussed with related engineers in real project case. This allocation task should be carefully treated by concerned people because it has a direct relationship with reliability and safety target of each components. After constructing this system level analysis, next

Table 3. FMEA for Level Crossing

No.	Function	Failure Mode	Effect	Hazard
01	Switch on	Late or no detection of train	Untimely protection of LC	Possible, if additional failure of LC monitoring
02	Switch off	Failure of train detection	Untimely protection of LC	Possible, if train has passed distant signal and LC set back to normal position
03	LC monitoring	Distant signal shows wrong aspect ("green")	Train driver will never stop at distant signal	Possible, if additional strike-in fail
04	Road Signalling	Road signal shows wrong aspect ("green")	A car driver could pass LC.	Possible, if failure of Switch-on functions.
05	Normal positioning	The LC is not set back to normal position after switch-on.	Road user can neglect LC and pass it.	Possible, if additional failure of LC monitoring
06	Power Supply	Complete immediate failure	LC may standstill in an undefined state or remain in a given state	Possible, if road signals are off and distant signals shows "green" aspect
07	Controller	Undetected wrong output	LC might be set in any state	Yes, if command is wrong-side

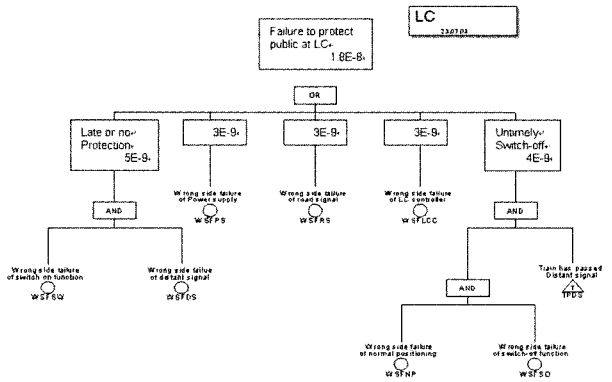

Fig. 4. FTA for Level Crossing

step is to analysis each branch in more detail to allocate safety target up to final functional units or design module.

In this example 5 top-level events shall be investigated, but in this thesis only "Wrong Side Failure of LC Controller" will be considered to provide an example for analysis. In practice there are many considerations in detailed analysis. Looking at the LC controller as one system, an undetected failure of the controller means that the controller itself is unable to detect this failure. Failure means any deviation from the specified function. This means that in case of an undetected failure the controller gives a different output than specified. This may result in a hazard or not, depending on the type of output. Note that undetected failure does not means wrong-side failure always. A wrong-side failure means a dangerous or hazardous failure. In a simple example, where only a single signal is controlled, there are only two possible wrong outputs, which the controller may produce. The failure "red output instead of green" is generally not hazardous, whereas the failure "green instead of red" generally is hazardous. In more complex situations, where more elements are controlled there may be more failure modes. The probability of wrong-side failures may then be approximated by

k = number of hazardous outputs/number of all false outputs

Note that this factor actually depends on the design of the LC Controller (e.g. number and encoding of outputs etc.) and is therefore part of the causal and not of the consequence analysis. In our causal analysis example this may be taken into account as in the following fault tree, where we have used a factor of 1/10 as an example. This requires that LC controller can be designed as SIL 3.

In this entry of the fault tree the fraction factor of the wrong side output is used. It is assumed to be 0.1 (10%) which is justified by the following argument:

We assume that core part of controller is 2 out of 2 fail-safe structured processors, where each processors process data in at least 8bit wide bytes. Upon failure there are at least 2^8=256 possible results, which can be distinguished from each other, including the correct one, which also deviates from a falsified result. Consequently, the proba-

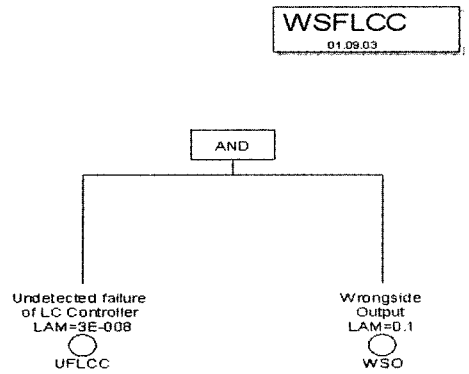

Fig. 5. Undetected and Wrong-Side Failure

bility to yield indistinguishable results from different failures is less than or equal to 1/256. This would support a factor of 0.01 for the hazard rate, however for the worst-case calculation a factor of 0.1 is adopted to provide a significant margin of error on this figure.

4. Summary

Procedure and tasks of Safety Analysis were explained with intention of setting safety target and it allocation into subsystems.

Safety Analysis is divided into two categories. The one is the Risk Analysis, which shall be executed by railway authority. It begins with System Definition followed by Hazard Identification. When hazards are identified clearly based on the defined system definition and boundary, Consequence Analysis is asked to find the risk. By using ETA method, determination of external risk can be reduced. With the result of ETA and TIR, THR are calculated according to formula (1). In case of LC example we could get Safety target THR 1.8×10^{-8} for the top hazard H_1= "Failure of LC to protect public from train".

The other Safety Analysis is called as System Design Analysis, which allocate target THR into subsystems to be designed. For this purpose FMEA and FTA method are applied. FMEA investigates possible failure effects of each function units defined at system definition phase. Based on the functional FMEA analysis, FTA is carried out as a Causal Analysis. In this case FTA shall be a top-down approach to allocate THR into functional units in the end. In this paper FTA suggests LC controller subsystem to be designed as SIL 3 with the wrong side failure rate of 3×10^{-8}.

References

1. "Safety-Critical Computer Systems", Neil Storey Addison-Wesley.
2. EN50129 CENELEC, "Railway Applications: Safety-related Electronic Systems for Signalling", 2000.
3. Braband, J. and Lennartz, K.: "A Systematic Process for the Definition of Safety Targets for Railway Signalling Applications", Signal+Draht 9/99.
4. "Fault Tree Analysis (FTA)", IEC 61025.
5. "Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA)", IEC 60812.
6. "Safety and hazard Analysis", 2-5 March HISE, The University of York. 1999.
7. "Engineering Safety Management", Volume 3, Issue 2.0 Railtrack.