Methodological Approach for Performing Human Reliability and Error Analysis in Railway Transportation System

Fabio De Felice [#1], Antonella Petrillo [#2]

# Department of Mechanism, Structures and Environment - University of Cassino
G. Di Biasio street N° 43 – 03043 Cassino (FR) – ITALY
1 defelice@unicas.it
2 a.petrillo@unicas.it

Abstract—**Today, billions of dollars are being spent annually world wide to develop, manufacture, and operate transportation system such trains, ships, aircraft, and motor vehicles. Around 70 to 90 percent of transportation crashes are, directly or indirectly, the result of human error. In fact, with the development of technology, system reliability has increased dramatically during the past decades, while human reliability has remained unchanged over the same period. Accordingly, human error is now considered as the most significant source of accidents or incidents in safety-critical systems. The aim of the paper is the proposal of a methodological approach to improve the transportation system reliability and in particular railway transportation system. The methodology presented is based on Failure Modes, Effects and Criticality Analysis (FMECA) and Human Reliability Analysis (HRA).**

Keyword-Human Error, Incidents, HRA, FMECA, Railway, Transportation

I. INTRODUCTION

The safety of staff, customers and of the general public in general viewed as one of the most important requirements in industry and is of particular importance in the railway industry, where passenger rightly expert vary high standards of care. Identifying the errors that frequently result in the occurrence of rail incidents and accidents can lead to the development of appropriate prevention and/or mitigation strategies. There is little doubt that human error contributes to the majority of incidents and accidents which occur within complex systems, including the railway system [1, 2]. To prevent and/or reduce the number of accidents and incidents which occur we must work towards reducing human error or making the system/organisation more error tolerant. Human error and accident management involves the prevention of human errors, the recovery from errors, and the containment of the consequences that result from error occurrence [3]. The first step in this process is error identification. Identifying the errors that frequently result in the occurrence of incidents and accidents may allow appropriate prevention and/or mitigation strategies to be developed.

We note that the objective difficulties of governing the human factor and the human error, have made many experts believe that the conduct of preventive and safety were related to intrinsic characteristics of the person, as the traits of personality. Another explanation of the phenomenon credited accident is based, on the contrary, on the search for extrinsic causes, such as research productivity. In other words, the accident can be determined on one side by unsafe behaviour and on the other, by structural conditions and inadequate instrumentation technique. From this point of view several methods have been developed to control the behaviour of safety or methods for safety management based on better behaviour critical to the safety of workers with the aim to drastically reduce accidents For risk analysis have been developed several techniques including: Safety Review, Checklist Analysis, Relative Ranking, What-if Analysis, Preliminary Hazard Analysis, Hazard and Operability (HAZOP), Failure Modes, Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Cause-Consequence Analysis (CCA). In particular in our work we will analyse:

- The Human Reliability Analysis (HRA), a recently spread method which focuses its attention on the responsibility of the “human factor”;
- The Failure Modes, Effects and Criticality Analysis (FMECA), methodology designed to identify potential failure modes for a product or process, to assess the risk associated with those failure modes, to rank the issues in terms of importance and to identify and carry out corrective actions to address the most serious concerns.

It is evident that the inherent complexity of the study of human factors requires the implementation of multi-criteria approach. The aim of this work is to develop a methodological approach to improve the reliability of transportation system and in particular of railway transportation system starting from identification of possible sources of risk and through the integration of HRA and FMECA [4]. The paper is structured in the following sections: Section II in which we analyse principles of Human Reliability and Human Factors; Section III that describes methods to perform human reliability (we focus our attention on HRA and FMECA); Section IV in which we propose a model for improve accident causation and finally Section V in which we summing up results of our study.

II. Human reliability and human factors

The filed of human factors exists because humans make errors in using systems or machines. The history of human factors may be traced back to Frederick W. Taylor who in 1898 conducted various studies to determine the most effective design of shovels [5]. In 1924, the national Research Council initiated a study concerned with examining various aspects of human factors at the Hawthorne Plant of Western Electric in the State of Illinois. By 1945, human factors became to be recognized as specialized discipline, and in 1972 the United States Department of Defense released a document on human factors (MIL-H-46855, Human Engineering Requirements for Military Systems, Equipment, and Facilities) that contained requirements for manufacturers or contractors engaged in developing equipment to be used by the service.

A. Fundamental aspects of human factors

The need to include human factors (HF) considerations in the design and safety assessment processes of technological systems is nowadays widely recognised by almost all stakeholders of technology, from end-users to providers and regulators. There are many objectives of human factors. They can be divided into four categories as show in Fig.1.

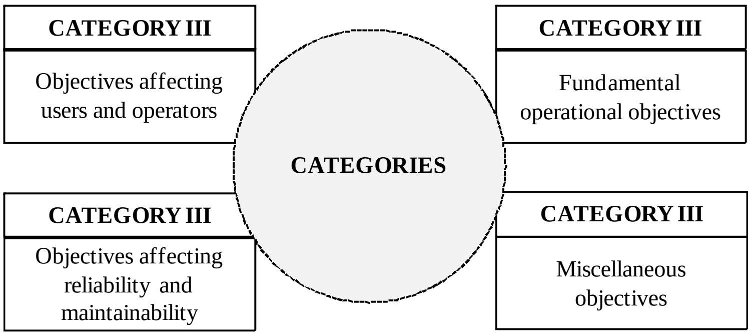
CATEGORY III
Objectives affecting users and operators
CATEGORY III
Fundamental operational objectives
CATEGORIES
CATEGORY III
Objectives affecting reliability and maintainability
CATEGORY III
Miscellaneous objectives

Fig. 1. Human factors objective categories

Human factors is a multidisciplinary field. There are many disciplines that contribute to it. Some of these disciplines are: psychology, engineering, anthropometry, industrial design, environmental medicine, operation research. From this point of view HRA aims to assess and help prevent the negative effects of human factors/error on system performance and safety, and is usually applied in the context of the risk assessment of complex and potentially hazardous systems such as transportation system [6].

As we note past experiences indicate that human behaviour plays a crucial role in the success of an engineering system. Some of the typical behaviours are as follow [7]:

- Human are often quite reluctant to admit mistake;
- Humans often overlook or misread instructions labels;
- Most people fail to recheck specified procedures for mistakes;
- Humans frequently respond irrationally in emergency situations;
- Humans normally carry out tasks while thinking about other things;
- Humans are normally poor estimators of clearance, distance, and speed;
- A significant proportion of humans become quite complacent after successfully handling hazardous or dangerous items over a long period time;
- People frequently use their hands first to test or explore;
- People get easily confused with unfamiliar things;
- Generally, people regard manufactured items as being safe;
- Usually humans tend to hurry at one time or another.

Other important factor in the reliability of an individual performing is the stress. There are basically the following four types of occupational stressors: occupational change-related stressors; occupational frustration-related stressors; workload-related stressors; miscellaneous stressors. The relationship between human performance and stress has been studied by various researcher over the years. They conclude that such relationship can be described by the curve shown in Figure 2:

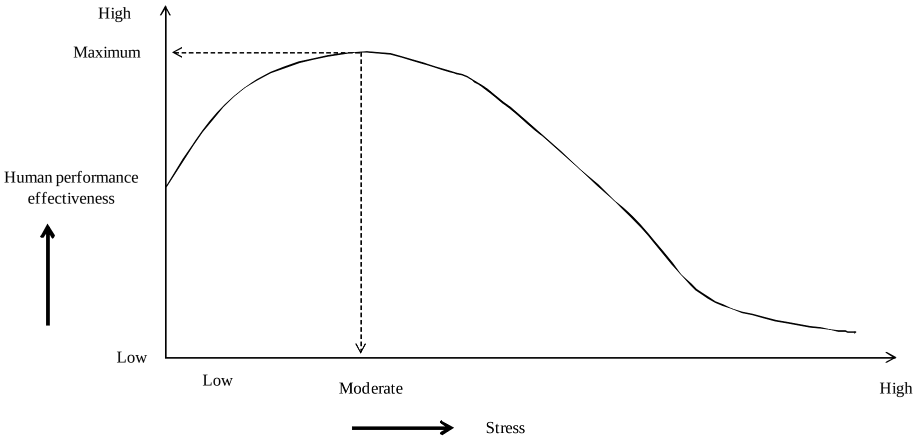

Fig. 2. Human performance effectiveness versus stress curve

B. *Human Error in Railways*

Baysari [1] analyzed the distribution of railway incident applying above classification that took place in Australia over the period of 1998–2006. Three hundred and thirty contributing factors emerged out of the 40 investigation reports, resulting in 360 errors being identified. An equipment failure was identified as the primary cause of 17 incidents (43%). The most common non-organizational influence to contribute to these incidents was that of the physical environment, with high ambient temperature proving to be the most widespread problem. Interestingly, all incidents triggered by an equipment failure were derailments and all were associated with inadequate equipment or equipment in poor condition. In all but four incidents, an organizational oversight was identified, that of inadequate monitoring or checking of equipment/resources. Here below is describe in detail the errors associated with these "human failure" incidents.

- *Unsafe acts.* The most common error types were skill-based errors. Of these skill-based errors, most were the result of an attention failure;
- *Preconditions for unsafe acts*. The most common problem was the formation of an incorrect expectation/assumption;
- *Unsafe supervision.* The most frequent problem was found to be inadequate supervision, specifically a failure of supervisors to track worker performance;
- *Organisational influences.* The most common problem was inadequate equipment design.

The global analysis of "human failure" investigation reports revealed that skill-based errors were the most common errors.

From this point of view many models of accident causation have acknowledged the contribution of human error in accident occurrence [8]. The most influential of these is that proposed by Reason [9] that defined two broad categories of error: *active and latent failures*. Active errors, whose effects are felt almost immediately, are associated with the front-line operators of the system, while latent errors, whose adverse consequences may lie dormant within the system for a long time, only become evident when they combine with other factors to breach the system's defences. Identifying what errors (both active and latent) contribute to accident occurrence can be difficult because there is no well defined start of the causal chain of an accident and exactly the same events can lead to widely different consequences [10].

The type of framework used for error identification in accident analysis or investigation is dependent on the theoretical approach, or perspective, to human error adopted. Common perspectives on human error include cognitive, ergonomic, behavioural, individual, psychosocial, and organisational [11]. A framework capable of accounting for the full range of human errors possible in a complex system would be one that identifies all latent and active failures included in Reason's model of human error. The Human Factors Analysis and Classification System (HFACS) appears to be one such framework because it encompasses the entire range of system errors, from the sharp end (e.g. operator) to the blunt end (e.g. management). It describes four levels of failure, as shown in Table I:

TABLE I
The HFACS framework (Wiegmann and Shappell, 2003)

The HFACS framework		
I Level	**II Level**	**III Level**
Organisational Influences	Resource management	
	Organisational Climate	
	Organisational Process	
Unsafe Supervision	Inadequate Supervision	
	Planned Inappropriate Operations	
	Failed to Correct a Problem	
	Supervisory Violations	
Precondition for Unsafe Acts	Environmental Factors	Physical Environment Technological Environment
	Condition of Operators	Adverse Mental States Adverse Psychological States Physical/mental Limitations
	Personnel Factors	Crew/Resource Management Personal Readiness
Unsafe Acts	Errors	Decision Errors Skill-bases Errors Perceptual Errors
	Violations	Routine Exceptional

III. METHODS TO PERFORM HUMAN RELIABILITY

Over the years, many new methods and techniques have been developed in this area. Here below we analyse fundamental principles of HRA and FMECA,

A. *Human Reliability Analysis (HRA)*

The term “human reliability” is usually defined as the probability that a person will correctly performs some system-required activity during a given time period (if time is a limiting factor) without performing any extraneous activity that can degrade the system. The historical background for the development of the set of methods that are commonly referred to as Human Reliability Analysis (HRA) was the need to describe incorrect human actions in the context of Probabilistic Risk Assessment (PRA) or Probabilistic Safety Analysis (PSA) [12].

The practice of HRA goes back to the early 1960s, but the majority of HRA methods were developed in the middle of the 1980s – mainly as a consequence of the concern caused by the accident in 1979 at the nuclear power plant at Three Mile Island. Partly due to the conditions under which it was developed, HRA methods from the beginning used procedures similar to those employed in conventional reliability analysis. The main difference was that human task activities were substituted for equipment failures and that modifications were made to account for the greater variability and interdependence of human performance as compared with that of equipment. The traditional approach is first to determine the human error probability (HEP), either by using established tables, human reliability models, or expert judgement. The characterisation of human failure modes is usually very simple, for instance in terms of “error of omission” and “errors of commission”. Since human actions clearly do not take place in a vacuum, a second step is to account for the influence of possible

In the search for a way of describing and understanding the failure of human actions, several classes of models have been used. In brief, HRA methods seem to include one of the following types of operator model.

- *Behavioural*, or human factors, models that focus on simple manifestations (error modes). The error modes are usually described in terms of omissions, commissions, and extraneous actions, and the methods aim at deriving the probability that a specific manifestation will occur. Since causal models are either very simple or non-existent, the theoretical basis for predicting performance failures is inadequate. Behavioural models are therefore also weak in accounting for the influence of context.
- *Information processing models* that focus on internal “mechanisms” for, e.g., decision making or reasoning. The methods aim at explaining the flow of causes and effects through the models. Causal models are therefore often complex, but with limited predictive power, and little concern for quantification. Error types typically refer to the cause as much as the manifestation (e.g., slips, lapses, mistakes, violations), or to the malfunctioning of a hypothetical information processing function. Context is not considered explicitly, at most in terms of the input to the operator, and information processing models are better suited for retrospective analysis than for predictions.

- *Cognitive models* that focus on the relation between error modes and causes, where the latter refer to the socio-technical environment as a whole. Unlike information processing models, cognitive models are simple and context is explicitly represented. Cognition is the reason why performance is efficient - and why it is sometimes limited - and the operator is seen as not only responding to events but also as acting in anticipation of future developments. Cognitive models are well suited for both predictions and retrospective analyses. There are, however, only a few HRA approaches that pay more than lip service to this type of model.

The purpose of human reliability analyses is to estimate the likelihood of particular human actions (that may prevent hazardous events) not being taken when needed, or other human actions that may cause hazardous events (by themselves or in combination with other conditions) occurring. Failures to take action to prevent hazardous events, and actions that cause hazardous events, are commonly called "human errors" in HRA. This term does not imply that people are necessarily personally responsible or culpable in some way, just that an action was omitted (or taken) that adversely influenced safety. Figure 3 shows a top-level representation of human performance, how human errors can create weaknesses in safety, and how those human errors are conditioned by the environment in which people work.

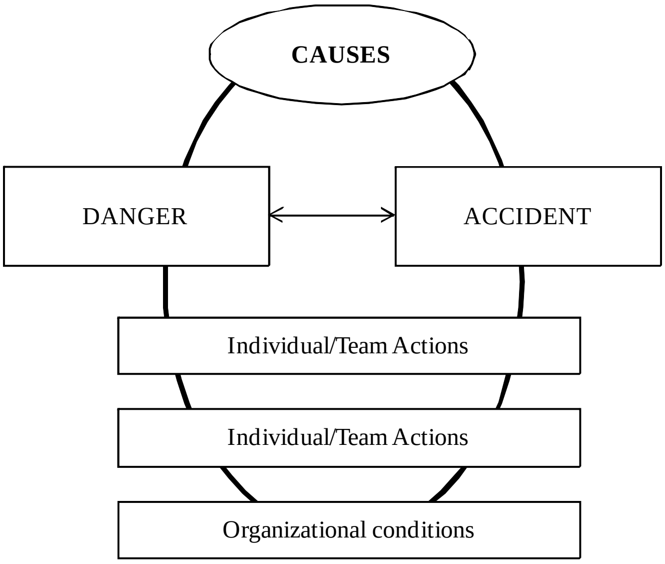

Fig. 3. Relationship of Safety, Human Errors, and Their Influences

Definitely the purpose of the HRA task to estimate the probabilities of human errors that can potentially fail the safety. However, this estimation needs to take into account the work environment and task conditions under which the work is done, since these can provide an important influence on the likelihood of error. An important aspect of the human reliability analysis process is to identify the contributing factors that may cause an unsafe action to be made. Contributing factors can be external (to the person) conditions like poor radio equipment or signals, or a train that is "difficult to control," or internal (to the person) conditions like fatigue or boredom, which we know lead to paying reduced attention to the track ahead.

B. Failure Modes, Effects and Criticality Analysis (FMECA)

The identification and choice of a suitable risk assessment model has been considered as a crucial issue for decades. So far, models used in the practice were developed for different applications and adapted for health and safety at work (Hazards and Operability Study – HAZOP, Failure Methods and Critical Analysis- FMECA, Fault tree analysis, Events tree, etc.) [13].

In our work we focused attention on the FMECA technique. FMECA has been widely standardized, as MIL-STD-1629A, MIL-HDBK-217 in the USA and as BS 5760 in the UK. Industrial users have reported significant benefits from these design tools. Successful users have achieved a 15–45% improvement in quality, and reduction in cost and time to market [14].

FMECA is a systematic analysis of the potential failure modes of a component of a system [15]. It includes the identification of possible failure modes, determination of the potential causes and consequences and an analysis of the associated risk. It also includes a record of corrective actions or controls implemented resulting in a detailed control plan. Typically, a FMECA is performed at the component level, starting with potential failures and then tracing their effects up to the ultimate consequences. The FMECA allows the identification of the most critical components and the likely failure mechanisms, thus leading to the specification of system parameters to be monitored.

This technique is a well known assessment tool used to identify the components of an equipment most likely to cause failures, and to enhance the reliability of a system through the development of the appropriate corrective actions [16, 17]. FMECA is important for directing maintenance tasks and identifying more efficient operational methods and for allocating the recommended actions at those points with higher damage potentials.

The main problem faced in the utilization of this technique is the necessity to help management to consider different parameters simultaneously. Thus, it is useful to adopt multi criteria techniques. From this point of view in a recent article, Kjellen pointed out the importance of risk of accidents as a criterion in decision making [18]. Amongst many factors, maintenance practice will also affect the occurrence of accidents.

IV. Methodological Approach: Human Factors Process Failure Modes and Effects Analysis

The railroad industry is developing a new generation of processor-based signal and train control systems to improve safety and enhance operations. From this point of view, as we said, humans play a very important role in ensuring safety. So, it is necessary to develop a methodological approach to evaluating the reliability of human actions that are modeled in a probabilistic risk assessment of train control operations. The aim of the paper is the proposal of a methodological approach to improve the reliability of transportation system and in particular of railway transportation system. The methodology presented is based on Failure Modes, Effects and Criticality Analysis (FMECA) and Human Reliability Analysis (HRA). In fact the most important and well known standard for the system design of railway technical components EN 50126-1 (CENELEC, 1999) [19] requires integration of human factors. Figure 4 shows that human factors particularly appear in the design and construction, operation and maintenance phases.

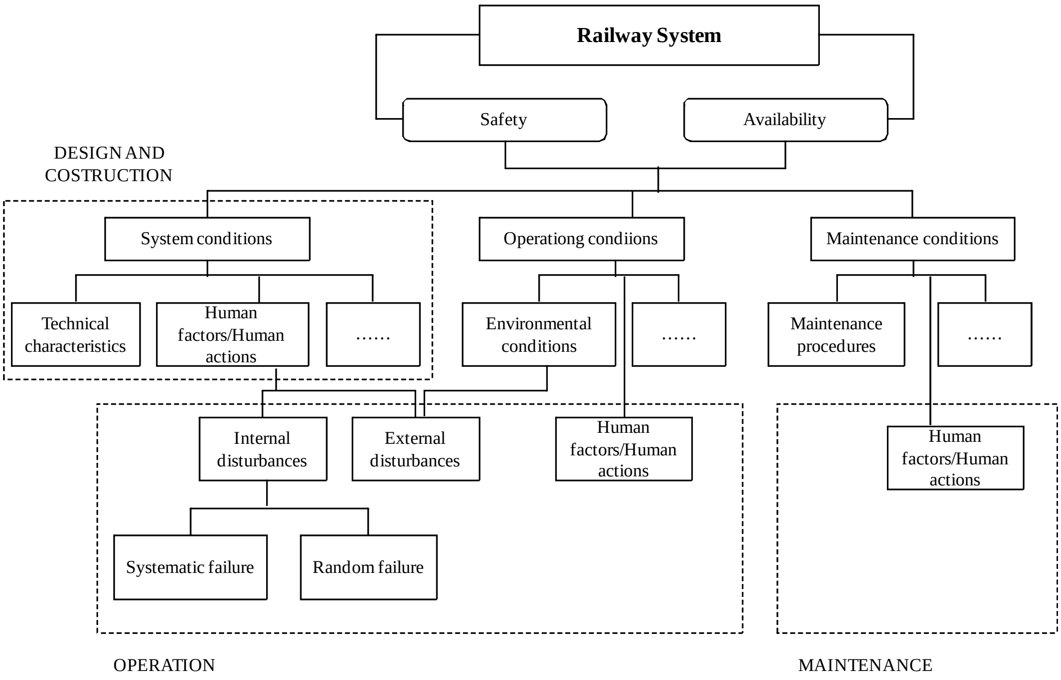

Fig. 4. Human factors in the railway system safety life cycle

Steps of methodological approach are:

- *STEP 1 – Analysis of the system and Evaluation of failure.* This activity mainly consists of the identify failure that could characterize the system.
- *STEP 2 - Evaluation of Human Factors*. This task requires study of operating rules, procedures, available data, as well direct observation of the work environment and interviews of individuals involved in the work. The goal is to identify the major sources of human risk and reliability with and without the new system as well as to understand the factors in the current environment that enable errors to be caught and recovered. This step requires following phases:
  1. Qualitative Human Factors Analysis;
  2. Quantitative Analysis;
  3. Human Failure Events to be Estimated.
- *STEP 3 - Identification of failure modes – FMECA.* This activity mainly consists of the identify failure modes: the aim is to integrate information coming from operational fields with global level effects.

- *STEP 4 - Identification of FTA.* A fault tree structure is proposed to analyze undesired events with different levels of operation quality.
- *STEP 5 - Make recommendations for reducing error.* To permit review and later understanding of the details of the quantification, all results and processes must be well documented, providing the bases for all estimates.

Figure 5 shows methodological steps.

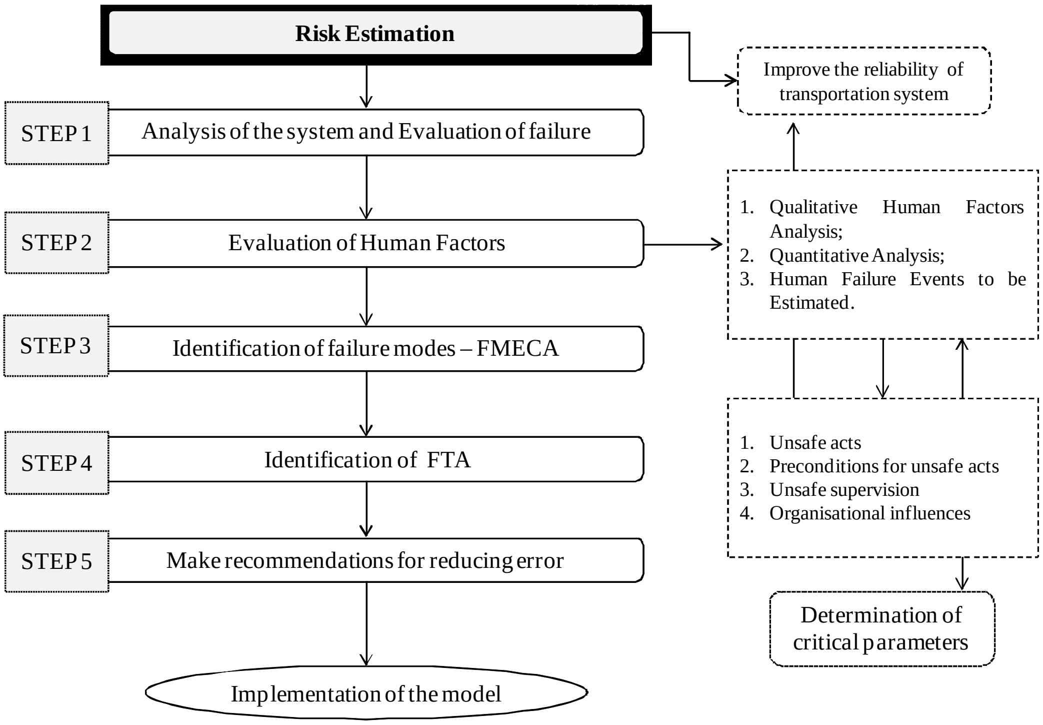
Risk Estimation
Improve the reliability of transportation system
STEP 1
Analysis of the system and Evaluation of failure
STEP 2
Evaluation of Human Factors
STEP 3
Identification of failure modes – FMECA
STEP 4
Identification of FTA
STEP 5
Make recommendations for reducing error
Implementation of the model
1. Qualitative Human Factors Analysis;
2. Quantitative Analysis;
3. Human Failure Events to be Estimated.
1. Unsafe acts
2. Preconditions for unsafe acts
3. Unsafe supervision
4. Organisational influences
Determination of critical parameters

Fig. 5. Methodological steps

A. Case Study: Radio Block Center (RBC)

The approach has been validated in a real case study concerning the European Train Control System - E.T.C.S.. We focused our attention on a particular component that is the Radio Block Center (RBC).

STEP 1 – Analysis of the system and Evaluation of failure.

RBC is a vital part of a ERTMS System (European Rail Traffic Management System) that is responsible for sending ETCS equipped trains the information they need to perform speed and distance supervision, according to the physical characteristics of the line (such as gradients and line speed limits), the conditions of the traffic (train spacing) and of others subsystems (Interlocking, adjacent RBC, Control Traffic Centre …). The main functions of the RBC are:

- Handle the radio communication with trains;
- Handle the protocol for data exchange with the Interlocking and the neighbouring RBCs;
- Handle the train spacing logic in accordance with ERTMS/ETCS.

The RBC system is composed of two cabinets and a desk PC:

- The NS2G (2nd Generation Safety Nucleus) Cabinet. Safety Nucleus of the RBC; it manages the RBC functions in their entirety while at the same time guaranteeing availability and safety;
- The ART2G (2nd Generation Remote Control and Recording Alarm Subsystem) Cabinet dedicated to the management of alarms, recording of events. It is also used for the interface with CTC and interface with the D&M (Diagnostic & Maintenance) PC;
- The Diagnosis and Maintenance desk.

Main RBC functionalities are:

- managing radio communication with the trains;
- managing the protocol and the respective connections for data exchange with the adjacent RBC and the IXLs used for line logic control;
- managing the Block/Distancing Logic.

RBC system shall comply with the EN 50126:1999 Railway applications standards.

Figure 6 shows Central Vital Processing Unit (NS2G) – Front Panel and ART2G – Front Panel.

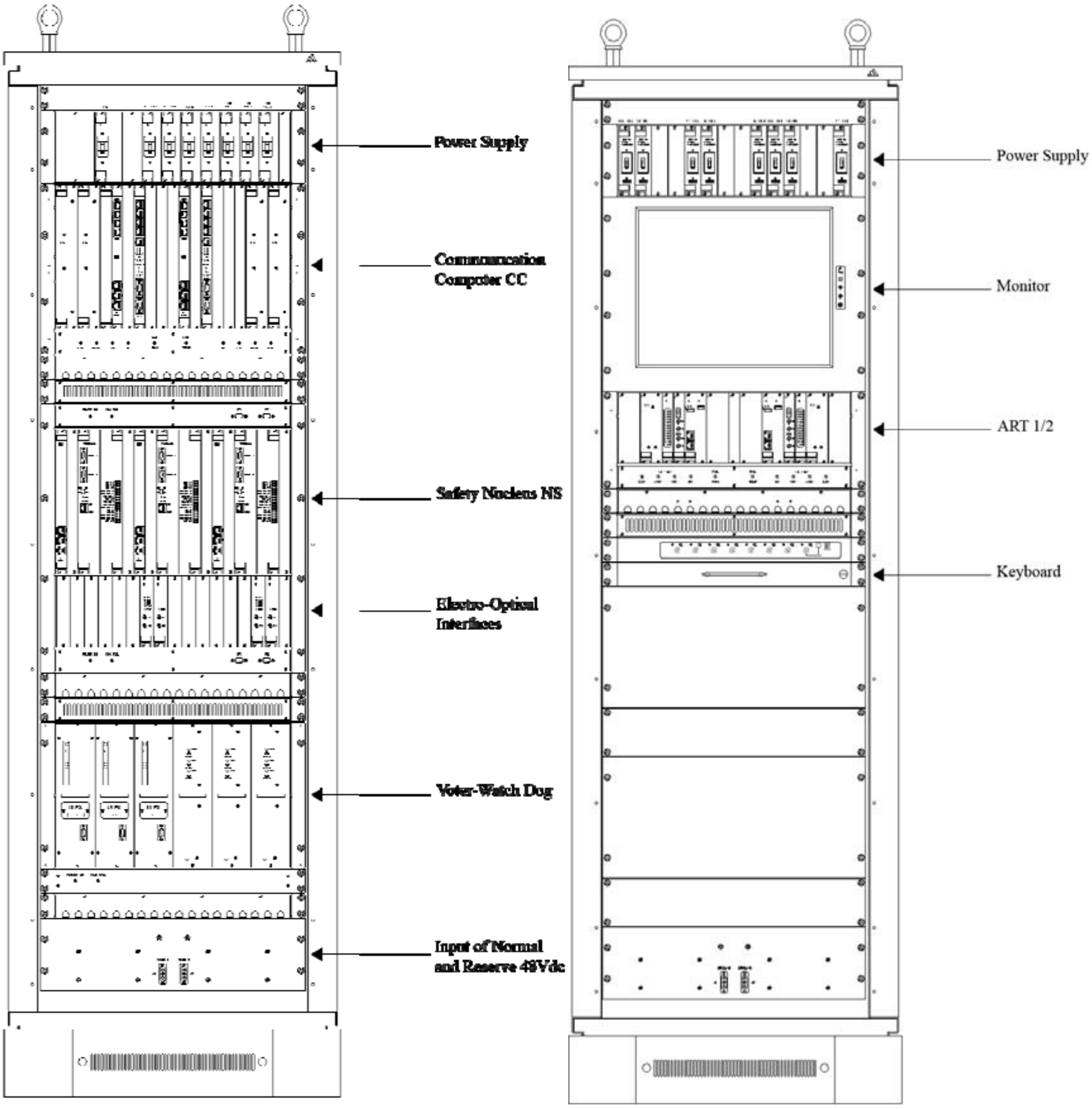
Power Supply
Communication Computer CC
Safety Nucleus NS
Electro-Optical Interfaces
Voter-Watch Dog
Input of Normal and Reserve 48Vdc
Power Supply
Monitor
ART 1/2
Keyboard

Fig. 6. Central Vital Processing Unit (NS2G) – Front Panel and ART2G – Front Panel

STEP 2 - Evaluation of Human Factors.

1. Qualitative Human Factors Analysis. The first step was to perform a qualitative human factors analysis. This involved two aspects: (1) An analysis of the current work environment to understand the types of errors that can arise and the factors that contribute to those errors; (2) An examination of the system, its user interface, and proposed human-system interaction, to assess its potential impact on human performance and human reliability.

Site visits were conducted in support of the qualitative analysis. The focus of the interviews and observations addressed the following questions:

- What are the most likely forms of unsafe actions?
- What are the factors that are most likely to contribute to those actions?
- What recovery mechanisms do humans provide that contributes to a robust, high-reliability system?
- What impact would RBC likely have on human reliability and overall safety?

2. Quantitative Analysis. The primary tasks in the quantitative analysis of the HRA were:

- Identification of relevant data sources;
- Identification their limitations and gaps;
- Application of the expert elicitation process to compensate for these limitations and gaps.

Overall process is shown in Figure 7.

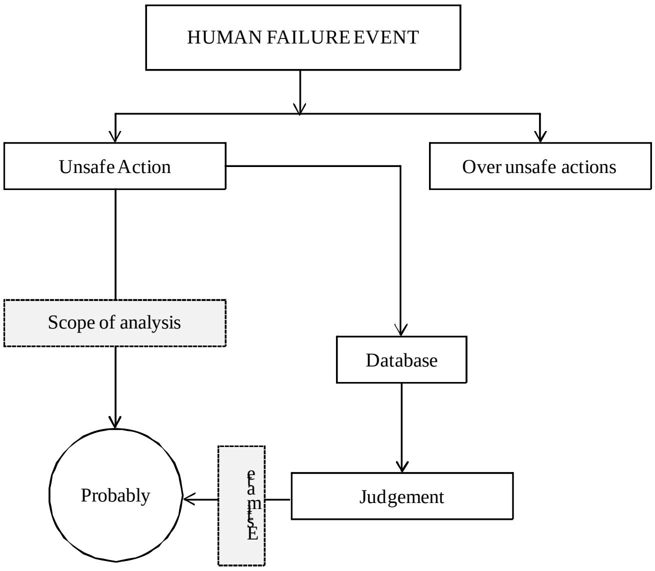

Fig. 6. Overall Analytical Process

3. Human Failure Events to be Estimated. Errors happen every day at work and whilst most are harmless, some can result in fatalities, injury or plant damage. Errors can occur in operations, maintenance or emergency tasks. The requirements of this study were to analyse the probabilities of specific unsafe actions representing potential contributors to the risks. We identified these ‘critical’ errors through: probabilistic safety assessment (PSA); by ‘brainstorming’ and by behavioural safety observation [20]. Summary of Data Associated with Each Human Failure Event is shows in table II.

TABLE II
Example of Human Failure Event

Event	Unsafe actions	Unsafe action data
Train fails to stop at boundary of authority	Train crew fails to stop at block boundary at end of authority: - block sign present - block sign missing	Employee disciplinary actions database
	Train crew mishears dispatcher as to limit of authority (location, train ID)	Estimates (e.g., estimates obtained from train crews or dispatchers)
	Dispatcher mishears train crew request for authority (location, train ID)	Estimates (e.g., estimates obtained from train crews or dispatchers)
Train exceeds speed restriction	Train crew exceeds speed restriction - permanent speed zone - sign present - sign missing - temporary speed zone - sign present - sign missing	Employee disciplinary actions database
Train runs over wrongly positioned switch	Previous train crew leaves switch in wrong (“reverse”) position without agreement from dispatcher Train crew does not recognize switch in wrong position and stop – target not OK	Employee disciplinary actions database Employee disciplinary actions database

STEP 3 - Identification of failure modes – FMECA.

A FMECA analysis is carried out for each LRU/sub-system, in order to determine, by implementing a bottom-up approach, the effects of every single fault on the system’s functional character.

The FMECA analysis is carried out according to IEC 60812 standard - Analysis techniques for system reliability – Procedure for failure mode and effects analysis. The analysis helps to identify, for each LRU, the effects of its failure on the sub-system and on the train service, identifying the criticality level:

- Severity level I (Significant failure): A failure that prevents the system from maintaining normal conditions for all traffic on more than one “Station area”. A failure on a line that only affects traffic conditions on the line and not the adjacent stations, is not regarded as a significant failure;
- Severity level II (Major failure): A failure that prevents the system from maintaining normal conditions for traffic within one “Station area”. A failure on a line that only affects traffic conditions on the line and not the adjacent stations, is regarded as a major failure;
- Severity level III (Minor failure): A failure that is neither significant nor major, i.e. a failure that doesn’t affect traffic conditions neither on the line nor on the adjacent stations.

In appendix (Table III) we show an example of FMECA.

STEP 4 - Identification of FTA.

For modeling fault we used the technique FTA (Fault Tree Analysis), deemed appropriate to highlight the dependencies between logical and functional components of the subsystem that can lead to abnormality determination of exercise (Top Event) and to quantify the probability of occurrence. FTA analysis assumes that the subsystem at the beginning of the mission is fully efficient, that every component is in good working condition and that all redundancies planned are active.

A realistic analysis must consider:

- FR that is failure rate. FR is based on the field measured data;
- MTBF that is Mean Time Between Failures (see Equation 1). MTBF shall be Significant failures (50 years); Major failures (0,2 years); Minor failures (0,05 years);

$$\text{MTBF} = (\text{Total up time}) / (\text{number of brekdowns}) \qquad (1)$$

- MTTR that is Mean Time To Repair (see Equation 2). MTTR shall be less than 0.5 hour for centralized equipments.

$$\text{MTTR} = (\text{Total down time}) / (\text{number of breakdowns}) \qquad (2)$$

Examples of Failure Rate are show in Table III.

TABLE III
Example of Failure Rate

Description	Unit FR [h^{-1}]	Unit MTBF [h]	MTTR [h]
Vital CPU card	5.50E-06	168550	0.50
Non vital CPU/Carrier card	5.84E-06	163237	0.50
Module IP36	2.46E-06	364000	0.50
ISC2 card	2.12E-06	465050	0.50
COM4 card	1.38E-06	655676	0.50
COS4 card	1.19E-06	619224	0.50
Exclusion logic backplane	1.00E-07	10000000	0.75
Exclusion logic unit	4.02E-06	222718	0.50
DC/DC converter	8.03E-06	112048	0.50
Power supply boards backplane	1.00E-07	10000000	0.75
…..	…..	….	….

The mission time was assumed to be 24 hours, or equal to the time of daily use of the subsystem. Here below (Figure 8) is an example of FTA.

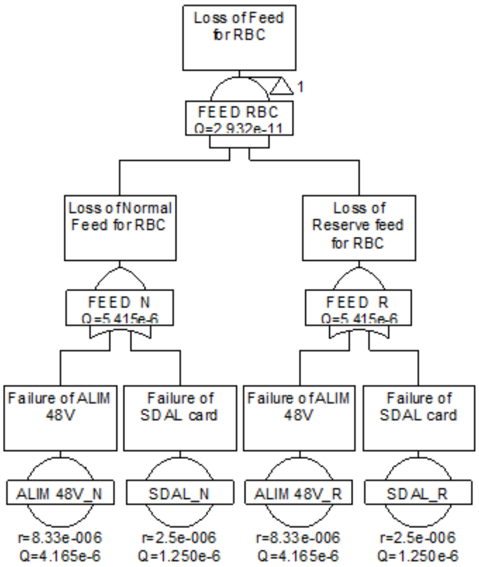

Fig. 8. FTA example for "loss of feed for RBC"

STEP 5 - Make recommendations for reducing error.

The errors included in the previous analysis were judged by the analysis team. In fact, on our opinion, one of the important elements to the success of a human factors quantification project is to assemble an interdisciplinary team to conduct the quantification that jointly possess experience and expertise in:

- Human Reliability Analysis;
- Probabilistic Risk Assessment;
- FMECA Analysis.

Summing up the following error forms were identified:

- Fails to recognize location due to weather and lack of experience;
- Misunderstands authority (Distracted while receiving authority, Expected to get greater number of blocks than actually issued, Boundary relocated, Mishears authority);
- Distraction or over-reliance by one crew member on the other;
- Unconscious (Highly fatigued, Environment (e.g., chemical release), Drug and alcohol).

V. Conclusion

Historically, the evaluation of train control systems has been design-based. That is, components of a train control system were evaluated based on engineering performance criteria taking into account operability, reliability, and maintainability criteria. With the advent of recent changes in electronic technology the railroad industry felt that new and better train control systems might be adopted more quickly using a performance-based approach, assuming that safety could still be assured. The complexity of these technologies (communication and information technology) requires additional safety considerations that current safety evaluation methods do not address. This study focused on:

- The development of an approach to assess the human failures in train control systems;
- The use of that approach to estimate probabilities of human failures;
- Estimation of likely human failure probabilities under a new and different type of system; and

The purpose of human reliability analyses is to estimate the likelihood of particular human actions (that may prevent hazardous events) not being taken when needed, or other human actions that may cause hazardous events (by themselves or in combination with other conditions) occurring. Advantages of human reliability analysis are: Provides a logical comprehensive analysis of factors influencing human performance; Leads to recommendations for improvement; Supports the safety case: forces attention on safety critical tasks.

Further developments could be oriented in applying the approach in several fields (automotive, aeronautic, etc.).

References

[1] M. T. Baysari, A. S. McIntosh, J. R. Wilson, Understanding the human factors contribution to railway accidents and incidents in Australia. *Accident Analysis and Prevention* 40 (2008) 1750–1757.

[2] D. Gaur, 2005. Human factors analysis and classification system applied to civil aircraft accidents in India. Aviation, Space, and Environmental Medicine 76 (5), 501–505.

[3] P. C. Cacciabue, P.C., *Human error risk management methodology for safety audit of a large railway organisation.* In: Wilson, J., Norris, B., Clarke, S., Mills, A. (Eds.), Rail Human Factors: Supporting the Integrated Railway. Ashgate Publishing Limited, Cornwall.

[4] F. De Felice, A. Petrillo, Development of a model for the improvement of safety in the work place through the Analityc Network Process. *Proceedings of the International Symposium on the Analytic Hierarchy Process (ISAHP)*, Pittsburgh (PA – USA), July 29–August 1, 2009

[5] Chapanis, Man-Machine Engineering, Wadsworth Publishing Company, Belmont, California, 1965.

[6] Kirwan. VALIDATION OF HUMAN RELIABILITY ASSESSMENT TECHNIQUES: PART 1 - VALIDATION ISSUES Safety Science Vol. 27, No. I, pp. 25-41, l997.

[7] W. E. Woodson, Human Reliability with Human factors, Pergamon Press, Inc., new York, 1981

[8] O'Hare, D., 2000. The 'Wheel of Misfortune': a taxonomic approach to human factors in accident investigation and analysis in aviation and other complex systems. Ergonomics 43 (12), 2001–2019.

[9] J. Reason, 1990. Human Error. Cambridge University Press, Cambridge.

[10] S.T., Shorrock, 2007. Errors of perception in air traffic control. Safety Science 45, 890–904.

[11] Wiegmann, S.A. Shappell, 2003. A Human Error Approach to Aviation Accident Analysis: The Human Factors Analysis and Classification System. Ashgate Publishing Limited, Bodmin, Cornwall.

[12] Hollnagel, *Cognitive reliability and error analysis method*. Oxford: Elsevier Science Ltd., 1998.

[13] De Felice, A. Petrillo, A Decision support tool based on ANP and FMEA to determine cause failures. *Proceedings of the International Conference on Modelling & Applied Simulation*, Fez (Marocco), 13-15 October, 2010.

[14] Q. Huang, J. Shi, K. L. Mak, 2000. Failure Mode and Effect Analysis (FMEA), *International Journal Adavanced Manufacturing Technoly*, 16 603–608.

[15] P. García Màrqueza, F. Schmid, J. C. Collado, A reliability centered approach to remote condition monitoring. A railway points case study, *Reliability Engineering and System Safety 80 (2003) 33–40*.

[16] Q. Hung, M. Nie, K. L. Mark, 1999. Web-based failure mode and effect analysis, *Computers and Industrial Engineering*, Vol. 37, pp. 177–180.

[17] Atkins, 2003. Research programme management rail-specific HRA technique for driving tasks user manual. Rail Safety and Standards Board Research Catalogue.

[18] U. Kjellen, G. Motet, A. Hale, 2009. Resolving multiple criteria decision making involving risk of accident loss. *Safety Science* 47, 795–797.

[19] CENELEC (ed.) 1999, EN 50126-1, Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS). Basic requirements and generic process.

[20] N. Hickling, 2007. An Independent Review of a Rail-Specific Human Reliability Assessment Technique for Driving Tasks (No. T270). Rail Safety and Standards Board, London.

FMECA Analysis for RBC2G Generic Product for Ester Project	**Rev: 00**	**Date: July 2011**
	Filled by: X	

ID	**Sub-system**	**Equip.**	**LRU** **Line Replaceable Unit**	**Function**	**Cause and Failure Mode**	**Effects**			**Diagnostics**	**Compensation Means**	**Severity**
						Local	**Sub-system**	**Service**			
1	RBC	Safety Nucleus	BTMR-VME	Hosting processing sections and optic interface sections	Failure of BTMR-VME	No connection between processing sections and optic interface sections	NS is out of service with consequent loss of RBC functionality	Traffic conditions affected on more than one Station Area	Alarm on D&M Desk	Immediate substitution of failed component	I
2	RBC	Safety Nucleus	MVME 6100-NS	Performing logic and diagnostic vital functions of the NS	Out of service of MVME6100 CPU	Exclusion of the failed processing section	NS works in a 2/2 processing logic	None	NS Internal diagnostic tests and communication to ART and D&M	Substitution of failed card to enable the 2/3 working logic of the NS	III
3	RBC	Safety Nucleus	TVME 8240 A	Performing Fast LAN interface with Communication Computers and hosting the 4 IP modules	Out of service of TVME8240 A	Exclusion of the failed processing section	NS works in a 2/2 processing logic	None	NS Internal diagnostic tests and communication to ART and D&M	Substitution of failed card to enable the 2/3 working logic of the NS	III
4	RBC	Safety Nucleus	IP36	Managing the serial communication interfaces for internal and external links	Out of service of IP36	Exclusion of the failed processing section	NS works in a 2/2 processing logic	None	NS Internal diagnostic tests and communication to ART and D&M	Substitution of failed card to enable the 2/3 working logic of the NS	III

APPENDIX

TABLE IV
FMECA Example.