



MODURBAN

FP6 Project: IP 516380

EC Contract n°: TIP4-CT-2005-516380

MODSYSTEM WP23 SUBPROJECT

– DELIVERABLE REPORT –

Deliverable ID:	D87
Deliverable Title:	Human factors and system design – Integrated system for “Auditing” safety levels of urban guided systems
Responsible partner:	UVAL
Contributors:	UVAL, KITE, JRC

PROPRIETARY RIGHTS STATEMENT

This document contains information, which is proprietary to the MODURBAN Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the MODURBAN consortium.



Document Information

Document Name: Human factors and system design – Integrated system for “Auditing” safety levels of urban guided systems

Document ID: UVAL-D87-FirstDraft-V1

Revision: Version 2

Revision Date: 060621

Authors: Vanderhaegen, F., Chaali, A., M. Bacchi, De Grandis, E., Cacciabue, P.-C

Security: Consortium only

Approvals

	Name	Company	Date	Visa
<i>Technical Management Committee</i>	B. VON WULLERTSORFF J. CAPEY/L. DURET G. JACQMIN G. LEGOFF A. PETERS U. HENNING M. NOCK JP RICHARD/D. COINEAU Y. AMSLER E. MACRON/S. GAMEZ	UNIFE ALSTOM ALCATEL CSEE BOMBARDIER SIEMENS KNORR BREMSE RATP UITP ALMA	11/09/2006	OK
<i>Coordinator</i>	Bernard VON WULLERSTORFF	UNIFE	15/09/2006	OK
<i>Quality Manager</i>	Bernard VON WULLERSTORFF Etienne MACRON	UNIFE ALMA	15/09/2006	OK

Documents history

Revision	Date	Modification	Author
Draft 1	28th April 2006	First version proposed by UVAL-KITE-JRC	See above
Version 2	21st June 2006	Comments of the WP23 consortium taken into account	See above

PROPRIETARY RIGHTS STATEMENT

This document contains information, which is proprietary to the MODURBAN Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the MODURBAN consortium.



The scope of the document applies to:

Metro systems only	Metro and Light Rail		Light Rail only
	<i>With no differentiation</i>	<i>With specific adaptation(s)/recommendation(s) (1)</i>	
		<i>For metro</i>	

(1) – Put a [D] if these adaptations/recommendations are present in the document and a [L] if they will have to be detailed later.

PROPRIETARY RIGHTS STATEMENT

This document contains information, which is proprietary to the MODURBAN Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the MODURBAN consortium.



SECTION I – DELIVERABLE SUMMARY

Human factors and system design – Integrated system for “Auditing” safety levels of urban guided systems

Deliverable ID , associated WP & Subproject	MODSYSTEM/WP23
Type of Deliverable	Report
Input / Starting stage	<i>D6 and D10 of UGTMS, WP23 meetings, inputs from others MODURBAN Subprojects and WPs</i>
Output / Final stage	<i>Report D87</i>

Lead partner(s)	UVAL
Achievement to date (%)	100%
Expected date of achievement	30th of june
Type of exploitation	<i>Internal to the project for the time being</i>
Exploitation potential	-
Expected budget	<i>See MODSYSTEM Budget</i>
Actual costs	See MODSYSTEM actual costs
Expected costs to completion	-
Protection	<i>None</i>
Protection date	Not relevant

IP's	Partners, (type, identification, date)
Pre-existing Know-How	
Exploitation Rights	

Associated Risk analysis	Type, solution envisaged, action, actors	Actual Reduction
Before start	Not relevant	
During task implementation	Not relevant	

PROPRIETARY RIGHTS STATEMENT

This document contains information, which is proprietary to the MODURBAN Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the MODURBAN consortium.



Human factors and system design – Integrated system for “Auditing” safety levels of urban guided systems

Deliverable Abstract

This report entitled “Human factors and system design – Integrated system for “Auditing” safety levels of urban guided systems” is the first step of the WP23.2 on human factor impact on functional and technical prescriptions. It concerns the human factor risk assessment process and it is initially based on the D10 of the UGTMS project. It is divided into four parts:

- The first part focuses on the interest of human factors for the system design.
- The second part is a comparison between several human factor based methods.
- The third part concerns the proposed method to be applied for considering human factors within a safety perspective.

The last part is the perspective of the proposal considering an integrated human-machine assessment analysis method.

Associated Milestone (if relevant):

PROPRIETARY RIGHTS STATEMENT

This document contains information, which is proprietary to the MODURBAN Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the MODURBAN consortium.



SECTION 2 – DELIVERABLE DETAILED DESCRIPTION

**Human factors and system design –
Integrated system for “Auditing” safety
levels
of urban guided systems**

**Authors: F. VANDERHAEGEN, A CHAALI (UVAL), M.
BACCHI (KITE), E. DE GRANDIS and P.-C.
CACCIABUE (JRC)**

PROPRIETARY RIGHTS STATEMENT

This document contains information, which is proprietary to the MODURBAN Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the MODURBAN consortium.



Abbreviations

Acronym	Meaning
ACIH	Analysis of Consequences of Human Unreliability
APJ	Absolute Probability Judgement
ATC	Automatic Train Control
ATHEANA	A Technique for Human Event Analysis
ATP	Automatic Train Protection
BCD	Benefit / Cost / potential Danger
CA	Consequence Analysis
DET	Dynamic Event Tree
DYLAM	Dynamic Reliability Assessment Method
FTA	Functional Task Analysis
GEMS	Generic Error Modelling System
HCR	Human Cognitive Reliability
HERMES	Human Error Risk Management for Engineering Systems
HF	Human Factor
HITLINE	Human Interaction Time Line
HRA	Human Reliability Analysis
IDA	Influence Diagram Approach
MAPPS	Maintenance Personnel Performance Simulation
OAT	Operator Action Tree
PC	Paired Comparison
PDA	Preliminary Danger analysis
PHA	Preliminary Hazard Analysis
PRA	Preliminary Risk Analysis
PSA	Probabilistic Safety Assessment
QRA	Quantitative Risk Assessment
SAFE-SADT	SAFE Structural Analysis Datagramme Technic
SHA	System Hazard Analysis
SHARP	Systematic Human Action Reliability Procedure
SLIM	Success Likelihood Index Methodology
TESEO	Tecnica Empirica Stima Errori Operatori
THERP	Technique for Human Error Rate Prediction

PROPRIETARY RIGHTS STATEMENT

This document contains information, which is proprietary to the MODURBAN Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the MODURBAN consortium.



1	Introduction	9
2	Human factors for system design	9
2.1	Safety based design principle	9
2.2	The role of human factors in system safety control	11
3	A comparison of human reliability assessment methods	14
3.1	Methodologies for Human Factors analysis	14
3.2	Standard methods and techniques for human factor analysis	14
3.3	Advanced methods for human factor analysis	16
3.4	Computer Aided Methods	17
3.5	Discussion	17
4	Human factor based non-conformity event assessment	19
4.1	Generic human factors based risk analysis process	19
4.2	The THERP process	21
4.3	The ACIH process	23
4.4	Sources of data on human factors	25
5	Toward an integrated approach for human-machine system safety	26
6	Conclusion	27
7	References	29

PROPRIETARY RIGHTS STATEMENT

This document contains information, which is proprietary to the MODURBAN Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the MODURBAN consortium.



1 Introduction

This report entitled “Human factors and system design – Integrated system for “Auditing” safety levels of urban guided systems” is the first step of the WP23.2 on human factor impact on functional and technical prescriptions. It concerns the human factor risk assessment process and it is initially based on the D10 of the UGTMS project. It is divided into four parts:

- The first part focuses on the interest of human factors for the system design.
- The second part is a comparison between several human factor based methods.
- The third part concerns the proposed method to be applied for considering human factors within a safety perspective.
- The last part is the perspective of the proposal considering an integrated human-machine assessment analysis method.

2 Human factors for system design

2.1 Safety based design principle

The concept of serial defence or defence in depth to control system safety is usually guaranteed by barriers, Figure 1. A barrier is a technical or human support to protect the human-machine system from the occurrence or the consequences of an undesirable event. Three main events of safety may be controlled: events to be prevented, events to be recovered and events to be contained.

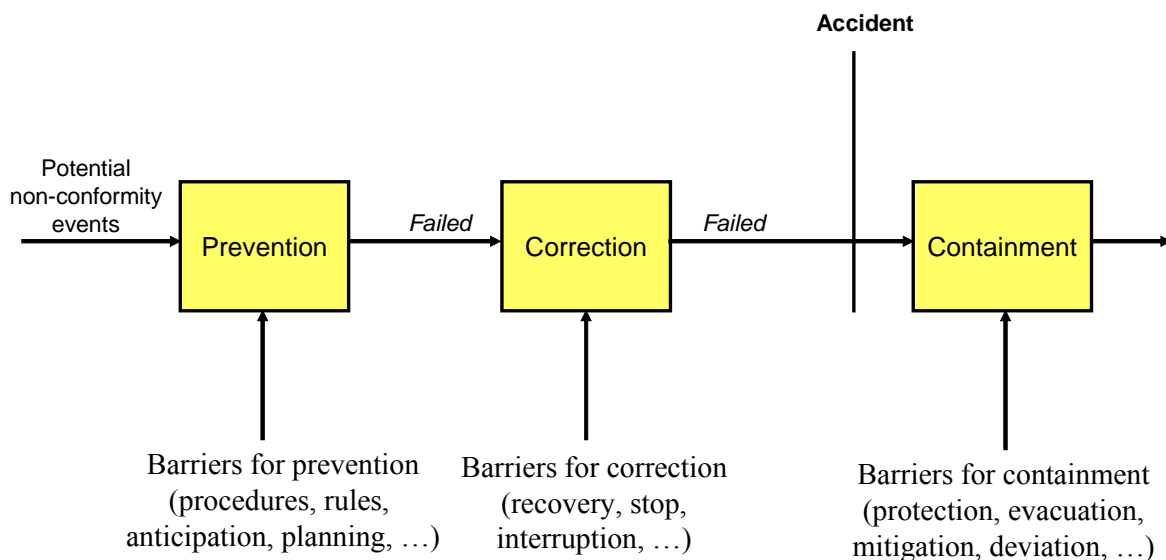


Figure 1. Barriers of prevention, of recovery and of containment

Hollnagel (1999) defines a barrier as an obstacle, an obstruction, or a hindrance that may either (1) prevent an action from being carried out or a situation to occur, or (2) prevent or lessen the severity of negative consequences. He distinguishes four classes of barriers:

- Material barriers (*e.g.*, grid of protection, air bags) physically prevent an action from occurring or limit the negative consequences of a situation.
- Functional barriers (*e.g.*, sensors, keys) logically or temporally link the occurrence of actions with events.
- Symbolic barriers (*e.g.*, panels, signals) require interpretation.
- Immaterial barriers (*e.g.*, rules, procedures) are not physically in the work situation.



A barrier can belong to more than one of these classes. Material and functional barriers are operational means whereas symbolic and immaterial ones are situational. A barrier is characterized by its source, i.e. who is the designer of the barrier and its target, i.e. who will use this barrier. Three levels of barrier design process can be defined (Polet et al., 2002). The designers of a given machine equip it with barriers with respect to the norms or risk analysis results. The employer who installs and operates this machine on an industrial site defines other barriers on field with respect to the implantation environment. Finally, the human operators who use this machine may modify some existing barriers or create new ones. The choice of the barriers of the first level (i.e. the designers of a machine) are the result of a risk analysis process. At the second level (i.e. the company that installs and operates the machine), additional barriers are linked to the operational conformity to be followed. However, the possible behaviours of human operators on field who face technical barriers or who are considered as barriers are not formally assessed.

Therefore, the risk analysis process of a system is done at this three levels, Table 1:

- For the designers, the objective of risk analysis is usually limited to a quantitative assessment of risk on safety. This evaluation is a mono-criterion and an off-line process. Its validation stops evolving when the machine is on field operation and is quite stable because it concerns a common decision. Nevertheless, this process of risk evaluation is external because it is usually made independently of the users and focuses on the factors related safety non-conformity events in order to define tools such as barriers or user manual.

Table 1. Risk analysis principles: main differences between the designers, employers and the users processes, completed and adapted from /D10-UGTMS, 2004/.

<i>Actors</i>	Designers	Employers	Users
<i>Objective</i>	Risk evaluation	Conformity assessment	Risk control
<i>Criterion</i>	Mono-criterion	Mono-criterion	Multi-criterion
<i>Processing</i>	Off-line	Off-line	On-line
<i>Validation</i>	Static	Dynamic	Dynamic
<i>Integrity</i>	Stable	Variable	Variable
<i>Source</i>	External	External	Cognitive
<i>Content</i>	Factors related to non-conformity events	Factors related to non-conformity events	Factors related to all field events
<i>Output</i>	Barriers User manual	Barriers Training	Barriers Learning Competences

- The company that installs and operates this machine has to demonstrate the on-field safety conformity. It is an off-line and external process focusing only on the safety criterion. Its validation and its integrity is not constant because it can take into account data from feedback of experience that may change initial prescriptions, adding barriers or improving training.
- Regarding the users, the risk analysis is much more a multi-criterion and on-line risk control process. Users have to control risks associated to operational situations evaluating them after their detection and intervening on the piloted process to avoid the occurrence or limited the consequences of a given event. This control is multi-criterion because it takes into account not only the system safety but also economical criteria such as production or quality or social criteria such as motivation or workload.



Depending on the variability of the operational situations to be controlled and on the inter-individual and intra-individual differences, the risk control process is dynamic and variable. Moreover, it can concern all factors related to whatever field events and support the definition of new individual or collective barriers, the increasing of the learning on the system behaviour, the improvement of the human competences.

Human factors have to take into account at the upper level of a system design such as a urban guided transport system design. On the one hand, a barrier can mask technical failures and make them undetectable by humans. It can also fail and this requires the presence of humans to solve the current problem. On the other hand, some field studies have shown that sometimes users do not respect barriers for different reasons /Polet et al., 2003/: the barrier is not really adapted; the users prefer repair themselves a problem instead of calling the maintenance service that obliges them to stop the machine they operate on; they modify the function of a barrier allocating it other operational objectives, etc.

In order to take into account human factors into the system design process, the so-called human centred automation concept may then be applied to make the safety barriers more intelligent and interactive with their users. Gathering the principles of redundancy and cooperation, systems such ATC or ATP and human staff of a given urban guided transport system may interact jointly in order to manage the allocation and the understanding of the achievement of the system functions or tasks. For instance, the allocation management may be useful to:

- To improve the system performance.
- To facilitate the activity of a decision-maker.
- To confront the results of the activity of a decision-maker with those of another one.
- To recover the human or technical errors.
- To generate new objectives in order to face with the impact of these errors.

2.2 The role of human factors in system safety control

Swain and Guttman (1983) have defined the human reliability as the probability that humans perform correctly their allocated tasks in given conditions, and that they do not assume any additional tasks which may degrade the human-machine system. Human error is the opposite concept and relates to the probability that an error occurs when performing a task.

An internal human cannot be observed and depends on the occurrence of external and internal factors that may affect human performance, Figure 2.

Internal factors relate to human behavioural factors whereas external ones depend on other factors such as environmental or technical factors. An internal error is supposed to be combined with an intention to act on the process. When human operators act on the process, an external error may occur. An external error is observable and can lead with a slip, a lapse, a fault or a violation (Reason, 1990). An action on the process and the presence of an internal error may lead to an external error.

A potential dangerous situation can be caused by an organisational error, a technical error or an external human error. Unadapted barriers may provoke the occurrence of an incidental situation for which unadapted recovery process may lead to an accident (Van der Schaaf, 1995).



The genesis of an internal human error and the consequence of a dangerous situation can be controlled either by human operators defences or by technical defences. These defences are called barriers that are designed to support human error prevention or recovery, taking into account each step of a given problem solving from the process state perception to the real action on the process. Two ways of human error evaluation can then be identified: the way of the designer of a machine integrating such barriers and the way of the users if these barriers.

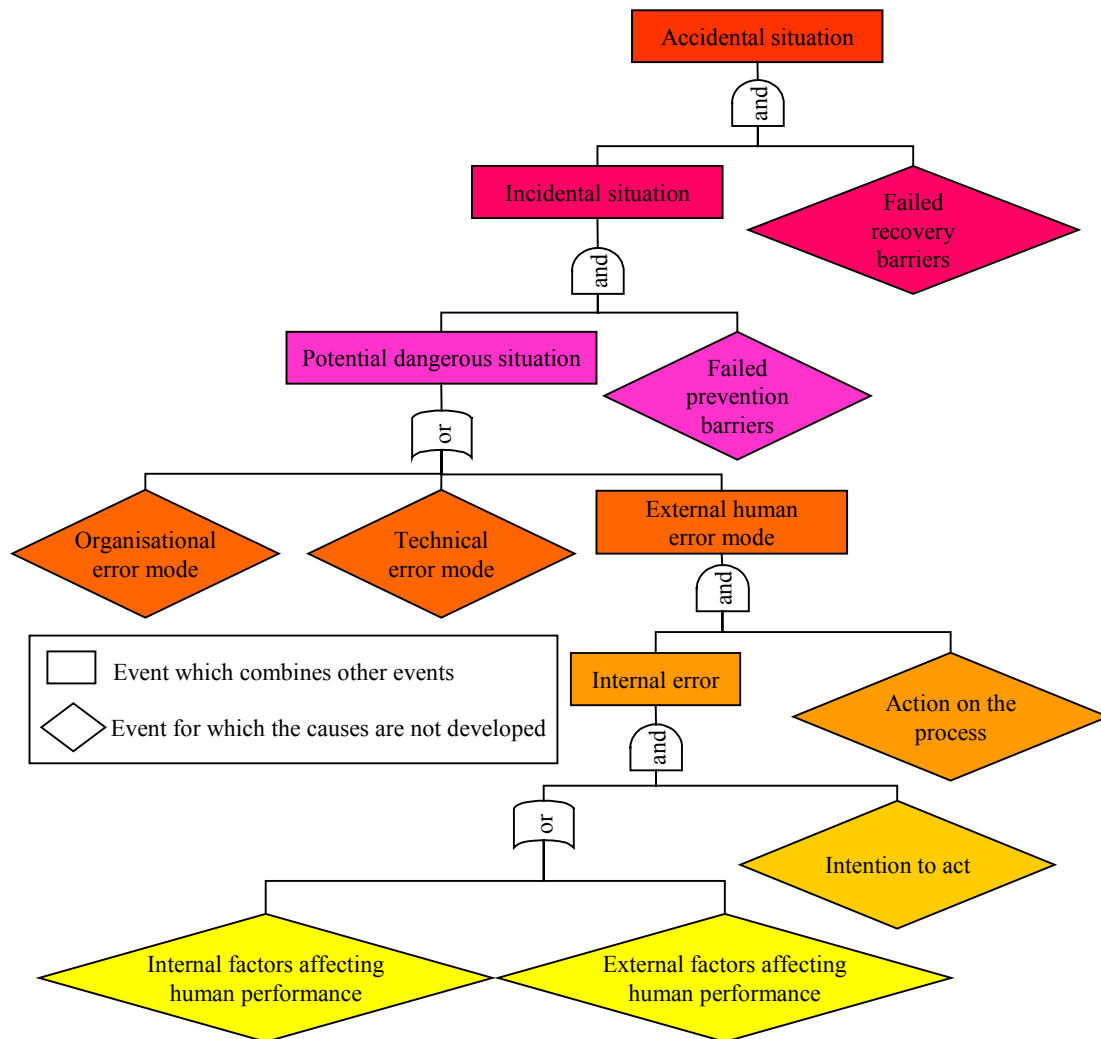


Figure 2. Genesis of an accidental situation due to human factors.

A lot of performance shaping factors have been identified in /Swain and Guttman, 1983/. Some factors that may affect human performance can also maintain an optimal level of performance. For instance, human factors such as stress, workload or task demand can generate positive or negative stimuli when controlling a given system /Wiener et al., 1984; Schonpflug, 1985; Chignel et al., 1985/, Figure 3.

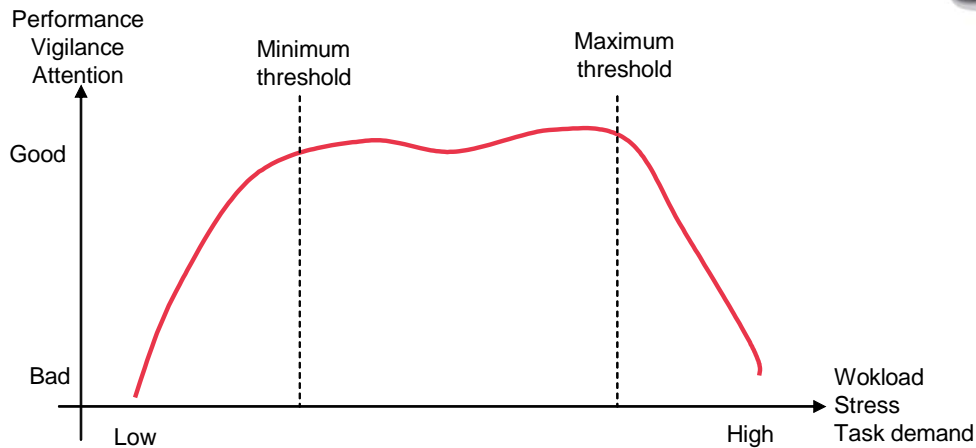


Figure 3. Hypothetical effects of stress or workload levels on human performance

A low or a high level of stress, workload or task demand may lead to a degradation of the human performance, vigilance or attention whereas a medium level may maintain an acceptable level of performance, vigilance or attention. This hypothetical view also consider temporal and functional factors integrating the control of particular situations such as emergent or complex ones.

The integration of human factors into the design process requires adapted methods. In an approach for hazard quantification (Quantitative Risk Assessment, QRA), the combination of event trees and fault trees analyses, performed for a vast number of initiating events, provides a complete description of the possible accidental paths. These include also the events related to human erroneous behaviour. The “human factor” techniques developed over the past years have well matched in accuracy and in formalism with the corresponding “system reliability” methods to which they have been coupled for the performance of hazard studies. Since the original work of Swain and Guttman /Swain, Guttman, 1983/, a number of Human Reliability Assessment (HRA) methods have been developed with a dual aim:

- of ameliorating the scope of HRA, for example by including new aspects of human behaviour connected with the changing role of the operators; and
- of maintaining the basic connections with the hazard evaluation approaches for the system reliability.

There is a high number of methods developed over the last decade on HF with these aims. These methods can be categorised according to their ability to treat dependent and dynamic conditions typical of the functions of operators in modern plants and to their ability to interface their input-output with the other methods adopted for the overall hazard analysis. In particular, the 3 following criteria for comparison can be used:

1. ability to account for cognitive vs. behaviouristic human activities;
2. ability to include dynamic vs. static human-machine interaction;
3. availability of data source, either from data bases, or from expert judgement, or from direct observation.



3 A comparison of human reliability assessment methods

3.1 Methodologies for Human Factors analysis

Prior to the review of the tools available for evaluating and quantifying the human error probability, it is important to understand the methodological approach by which all the steps needed to carry out a HF study are described. A methodology is a body of methods and techniques organised in a certain way in order to achieve the expected result. By applying a methodology for human reliability assessment, the safety analyst can properly structure and perform three essential steps, namely:

- the analysis of the working environment under study;
- the quantification of the possible human errors; and
- the evaluation, by a probabilistic measure, of the procedures and of the consequences of human errors.

There is a limited number of methodologies for HRA and they bare a strong similarity with each other /Embrey, 1992/. Therefore, it will be sufficient to describe here only one of them and, then, to focus our attention on the actual methods and techniques which can be applied to perform each step of the methodology itself. The SHARP (Systematic Human Action Reliability Procedure) methodology of Hannaman and Spurgin /Hannaman, 1984/ is one of the most representative and complete example.

In particular, SHARP develops in seven distinct steps: 1) identifying human interactions (Definition), 2) stating key assumptions (Screening), 3) focusing on key interactions (Breakdown), 4) describing in detail key interactions (Representation), 5) integrating them with the hardware description (Impact Assessment), 6) quantifying the impacts (Quantification), and 7) documenting the results (Documentation). No specific methods or numerical technique is specified for SHARP.

3.2 Standard methods and techniques for human factor analysis

The most commonly used methods and techniques are:

- Technique for Human Error Rate Prediction (THERP);
- Operator Action Tree (OAT);
- Maintenance Personnel Performance Simulation (MAPPS);
- Absolute Probability Judgement (APJ);
- Paired Comparison (PC);
- Tecnica Empirica Stima Errori Operatori (TESEO);
- Success Likelihood Index Methodology (SLIM);
- Influence Diagram Approach (IDA); and
- Human Cognitive Reliability correlation (HCR).

The first three methods cover more than one step of the methodological framework described in the previous section, while the last six techniques are specifically dedicated to the evaluation of data on human error probabilities. These latter methods use mainly the approach of expert opinion elicitation, coupled with the statistical treatment of the information retrieved from different sources.



While the detailed description of these methods is outside the scope of the present work, the comparison between them is shown in Table 2 below /Cacciabue, 1996/. In column 5 of the table, the applicability of each method is clearly identified with the reference to the methodological framework of SHARP. From the table it results quite obvious which is the best suited method for different specific HF analyses. As an example, if several steps of the methodology are to be performed, like in a hazard quantification analysis, the methods THERP, OAT and/or MAPPS should be preferred. THERP and OAT are almost equivalent as far as the human factor representation technique and the consideration for human behaviour aspects are concerned.

However, the THERP approach is most commonly applied because it offers two very important advantages over all other methods, namely:

1. the direct access to the data base contained in its Chapter 20; and
2. the immediate integration of its output data into a FT type approach.

Table 2. Comparison of the standard HF methods

	Models		Interaction		Data			Methodological steps
	<i>Beh.</i>	<i>Cog.</i>	<i>Sta.</i>	<i>Dyn.</i>	<i>Data base</i>	<i>Exp Jud.</i>	<i>Direct Ob.</i>	
THERP	4	2	4	1	X		X	Breakd. - Repres. - Impact As. - Quant.
OAT	4	2	4	2	X			Breakd. - Repres. - Impact As. - Quant.
MAPPS	2	0	2	0	X		X	Breakd. - Repres. - Impact As. - Quant.
APJ	n.a.		n.a.			X		Quant.
PC	n.a.		n.a.			X		Quant.
TESEO	0	2	1	0	X			Quant.
SLIM	n.a.		n.a.			X		Quant.
IDA	n.a.		n.a.			X		Quant.
HCR	3	4	2	1		X		Quant.

Where:

X denotes the type of data used

n.a. stands for not-applicable

0 - 4 level of detail of approach: **4** = full modelling; **0** = no modell.; **1** = insuff. modell., etc.



3.3 *Advanced methods for human factor analysis*

A first generic conclusion that can be drawn from examining the above Table is that, while a very good degree of accuracy can be obtained in the treatment of the data, a less detailed accuracy is adopted in modelling human behaviour, in particular the cognitive components to the root causes of human error. Moreover, the dynamic aspects of man-machine interactions are almost completely neglected.

The reasons for these deficiencies shown by the standard approaches are:

- a) the intrinsic difficulty and complexity of accounting for dynamic (human) interactions and cognitive processes; and
- b) the existence of an equivalent inadequacy in the systemic approaches of plant safety study.

The solution of the first problem can be achieved by the new developments of models of cognition based on new types of computer architectures and software tools. Methods of this type can be found in the literature, but have mainly academic characteristics and have only been developed for simple decision processes. Moreover, they do not show any direct interfaces with hazard evaluation techniques like FTA. Examples of this kind are the methods GEMS (Generic Error Modelling System) and the “Latent Failures” developed by Reason /Reason 1987, 1990/. These approaches are very well suited for auditing and classifying working environments and organisational structures from the human factors viewpoint.

The second deficiency is of methodological nature, as the systemic approaches related to the HF methods have always been substantially static and thus, in practice, there has never been a real need to develop dynamic HF methods. Nowadays, the issue of dynamic dependence is, eventually, becoming of high relevance also in the domain of system analysis and the terminology “dynamic reliability” or “dynamic PSA” (Probabilistic Safety Assessment) is becoming a topic of research. This will certainly give new emphasis to the development of dynamic HF methods. Along this line of development, new methods have been proposed.

Examples of these methods are:

- Human Interaction Time Line (HITLINE) /Macwan, Mosleh, 1993/
- A Technique for Human Event Analysis (ATHEANA), which is a fully structured methodology developed for the US-Nuclear Regulatory Commission to respond to the needs of new HRA approaches oriented on cognitive behaviour of operators as well as performances and actions /Barriere et al., 1998/; and
- Human Error Risk Management for Engineering Systems (HERMES) /Cacciabue, 2004/.

These techniques attempt to combine the concepts of dynamic reliability typical of methods like DYLAM and DET and advanced human behaviour simulation /Cojazzi et al, 1993; Siu, Acosta, 1991/.

Once again, as for the case of dynamic reliability methods, the critical aspects of these latter approaches consists in the difficulty of identifying reliable and sound data for the risk assessment and for the definition of the dependencies. In practice, the input data of these methods rely heavily to expert judgement, which is always difficult to obtain and to assess.



3.4 Computer Aided Methods

The performance of hazard analysis of complex systems leads inevitably to rather complex and time consuming calculations, independently of the method adopted. In practice, manual calculation of FT for example, has become impractical since many years and the use of computerised tools is now an unavoidable process in the performance of hazard analysis.

To date, the majority of fault tree analytical programmes have been developed for mainframe computers and are dedicated to the calculation of minimal cut sets, fault tree reduction processes and top event probabilities. Similarly, computerised calculation of uncertainties associated with the consequences of unwanted faults has been developed on the bases of Monte Carlo methods combined with techniques like Response Surface Methodology.

In more recent times, the development of tools has been focused on the application of the computerised techniques for PCs and for Workstations, using advances programming languages and modelling techniques. In particular, Object Oriented programming and expert systems techniques are applied for the inclusion of engineering experience and data in methods aiming at integrating the whole sequence of process applied for the Preliminary Hazard Analysis (PHA), the System Hazard Analysis (SHA), and the Consequence Analysis (CA).

This is an important effort and needs to be promoted further as it allows to include in the computerised tools the theoretical knowledge of risk analysis and systematic safety which is necessary for hazard evaluation, but which demands a background of advanced statistical and mathematical knowledge not. In practice, in this way this expertise is made transparent to the user of such tools and their application can be carried out by experts in the engineering and technological domain in which they are to be applied, generating the conditions for maximum exploitation of their potentiality.

3.5 Discussion

The occurrence of an given event noted $event_i$, and more precisely of an undesirable event, is linked to the occurrence of one or several factors noted $factor_j$ identified upon the number m of causal factors:

$$Cause(event_i) \equiv \{factor_k / \bigcup_{j \in \square} (\bigwedge_{1 \leq k \leq m} factor_k) \rightarrow event_i\}$$

The difficulty is the identification of the pertinent factors that may affect human performance, or to select the primary causal factors and the secondary ones to focus the design on the analysis and the control of a minimum number of causal factors. Undesirable event can lead to individual factors, organisational ones and technical ones. Its occurrence can be related to several scenarios of different or joint causal factors. By applying abductive reasoning, when these scenarios are identified, all the incriminated factors may be analyzed. For example, if a human error can occur because of a lack of motivation and a underload or of an overload, a monotoneous situation and a loss of location, then the list of factors to be treated may be: {lack of motivation, underload, overload, monotony, loss of location}. Nevertheless, the risk analysis has to treat an isolated factor such as underload or overloaded or to treat them knowing the occurrence of other factors such as lack of motivation or monotony and loss of



location. The first solution remains partial whereas the second is complex to achieve because it requires the identification of the interdependency between factors. For instance the identification of functional links between factors can be limited to a static analysis defining logical links between tasks such serial or parallel achievements whereas temporal ones require a dynamic representation of the system behaviour.

Violations are not systematically unconscious behaviour. As example, different classes of violation may be considered, /Hudson et al., 98/:

- Non-intentional violations occur when human operators do not know or do not understand the prescriptions to be followed. The occurrence of these violations are not conscious.
- Skill-based violations are new behaviours that usually replace the prescribed ones. For instance, when human operators decide that a given procedure is not adapted anymore, they do not respect it and this new practice becomes the new reference communicated to the other operators.
- Exceptional violations occur punctually facing to solve emergency situations or technical failures.
- Optimizing violations aim at improving work conditions.
- Organisational violations occur when human or technical resources are not sufficient or are unadapted to face work demands.

As a matter of fact, the design of protection systems such barriers has to be taken into account all the life-cycle steps of a given system taking into account field and technical constraints and human task demands /Valancogne, Nicolet, 02/. The control the possible migration of the use of the system then requires the definition of a prospective, retrospective and on-line risks analysis applying both quantitative and qualitative measures.

Two other classes of protection can be done: passive barriers are waiting external stimulus to be activated active barriers are continuously activated to control unsafe events. These active protections depend usually on three main classes of measures : measures directed at the element cause of the hazard (i.e., source of danger), measures directed at the hazard itself (i.e. risk calculation) and measures directed to the element facing the danger (i.e., target of danger). Regarding risks associated to human action, human factor based assessment measures can lead to these three classes of measures. For instance, a human operator's underload measure can relate to the source of a danger, or to a consequence of a risk or to a consequence for another human operator's behaviour. The main difficulty of such factor measure is its location and its interpretation into the accident process. Moreover, same causal factors (such underload for example) may make maintenance agents some errors when repairing or verifying active protections: this can have dangerous impact on field during operation activities. Therefore, the defence-in-depth concept usually used for system design has also to be applied for operation and maintenance design in order to avoid such unintentional hazardous migrations of system use.

As shown on the /D10-UGTMS, 2003/, results about probabilistic based human reliability analysis are not homogeneous when an analyst uses several methods or when several analysts use the same method (Kirwan, 1997). Most of them require a sufficient operational feedback or knowledge to assess probability or severity. Moreover, the use of qualitative methods confronts the problem of the pertinence or the difficulty application of the error taxonomy (De Keyser, 2003). Other studies have tried to classified the pertinence level of these human error analysis methods in terms of utility, validity, accuracy or maturity for example (Humphreys,



88; Swain, 89; Reason, 90; Kirwan, 97), but there is not homogeneous results except for the THERP method that seems the more completed one.

The first important conclusion that can be derived from this comparison is that the use of THERP is the most appropriate approach that can be initially applied when a quantification is required for the risk associated to human factors. The reason for this conclusion is that THERP offers direct access to the data base contained in its Chapter 20 and an immediate integration of its output data into a FT type approach.

The existence of a very detailed description of THERP and the associated database is a further factor favouring the use of such methods. In fact, the development of a computer supported approach for guiding the user to the implementation of the method and its association with the reference set of data contained in Chapter 20 of THERP manual, can be quite easily implemented.

The application of more sophisticated techniques can however be implemented when very specific and detailed studies are necessary that requires the contribution of field studies and observations on factual working contexts in order to achieve a relevant set of data that can support advanced and detailed methods such as for example ATHEANA.

Researches are then required in order to improve the development and the application of these human factor based analysis approaches. This report proposes to assess human factors applying two main approaches: the THERP one because it is well-known and well-accepted by the engineering community on human error and reliability, and the ACIH one to complete the first one and define an on-line model of human behaviour.

4 Human factor based non-conformity event assessment

4.1 Generic human factors based risk analysis process

Normal versus abnormal human behavioural models and off-line barrier design versus on-line barrier removal have to be foreseen into the future design process of an urban guided transport systems, Figure 4.

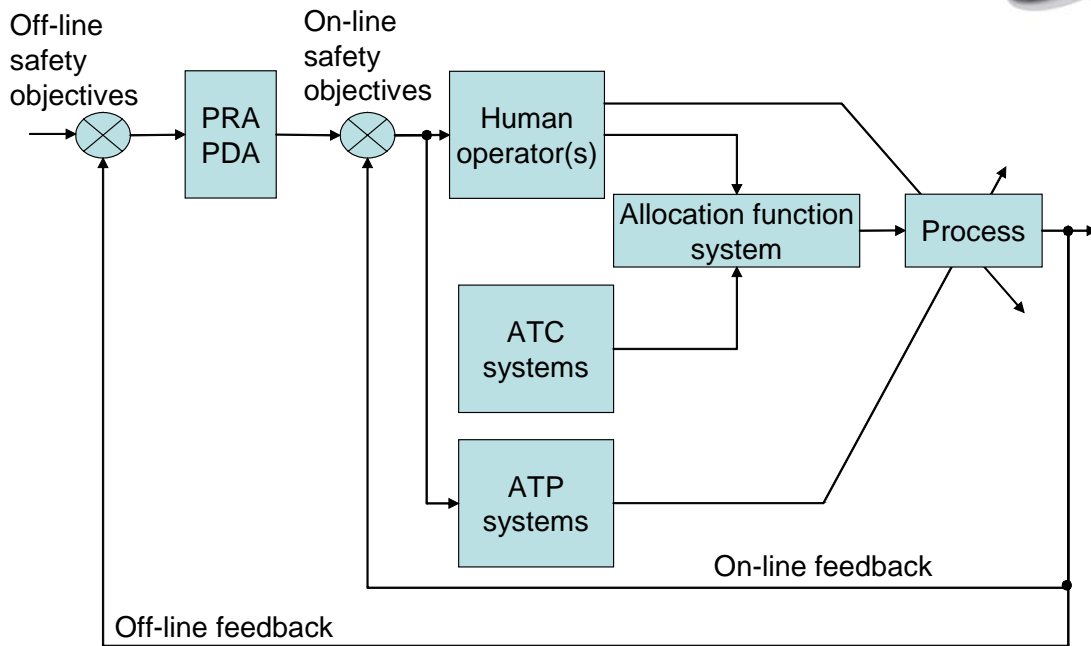


Figure 4. Off-line and on-line risk analysis process

Technical or human control actions have to be planned in order to recover human errors and technical failures. Such human control actions are integrated into prescribed safety procedures and such technical control actions are the ATP systems. ATC systems and other procedures are required to control on-line the given process depending on a predefined allocation of function or tasks between humans and machines. This allocation and human-machine control system are defined regarding off-line results of the PRA or PDA integrating safety based objectives. The off-line safety assessment process can be assessed using appropriate technical analysis methods combining human ones in order to take into account human-machine interactions and complementarities.

An off-line human error risk analysis process usually includes standard steps, Figure 5:

- The definition of the objectives and the constraints to be followed.
- The structural and functional analysis related to the objectives and constraints defined above.
- The task analysis including function allocation between humans and machines.
- The identification of potential human errors and their control modes in terms of prevention and recovery.
- The human error occurrence assessment process in order to evaluate qualitatively or quantitatively the probability of human error occurrence.
- The human error consequence assessment if required. This step combined with the previous step aims at assessing the risks of human error.
- The specification of human-machine system if the residual risk of human error is acceptable.
- The possible modification of task description and allocation in case of unacceptable residual risks of human error.
- The possible proposal for other solutions such as training programme definition.

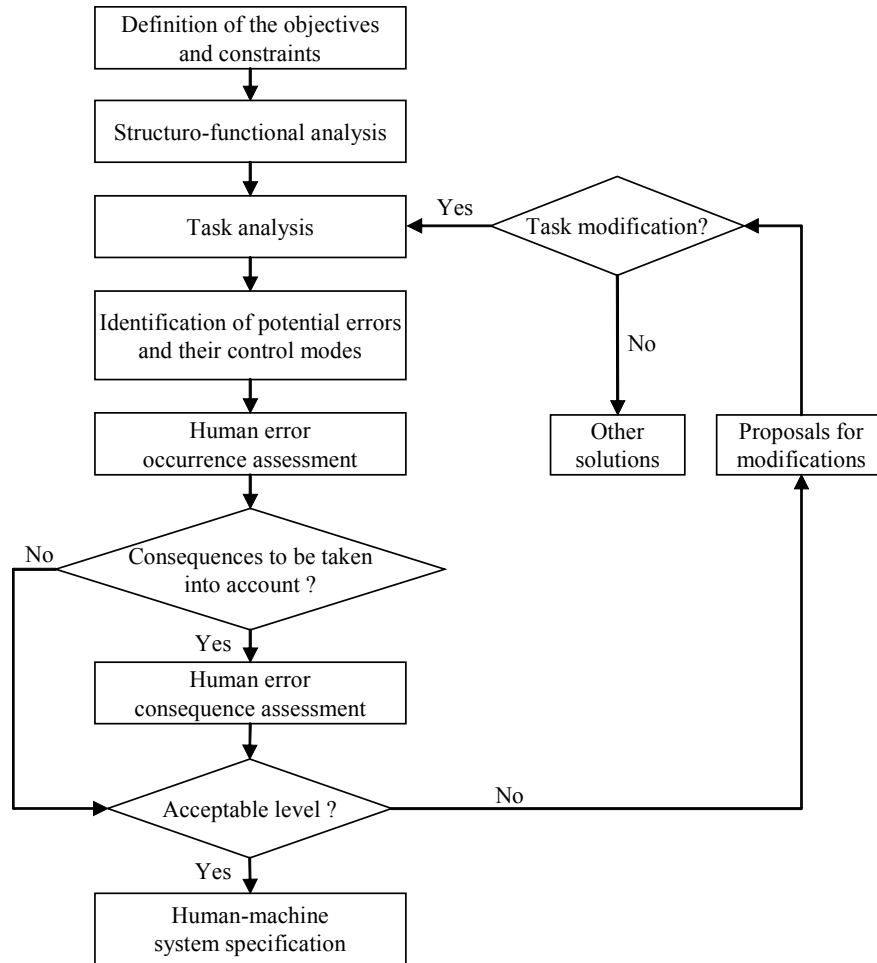


Figure 5. Human error analysis for system design, adapted from /Gerdes, 1997/

Future research works will focus on the feasibility to develop an off-line integrated method that can take into account technical and human factors assessing human-machine system safety and compromises between safety and availability criteria. Regarding the human factor based method, two methods will be studied: the THERP and ACIH analysis presented hereafter.

4.2 The THERP process

THERP (Technique or Human Error Rate Prediction) is a predictive method that assess human error probabilities and estimate the possible degradation of a given human-machine system caused by human errors with or without interaction with equipments such as barriers. It uses the event tree method to assess the probability of success or failure of serial or parallel tasks, Figure 6.

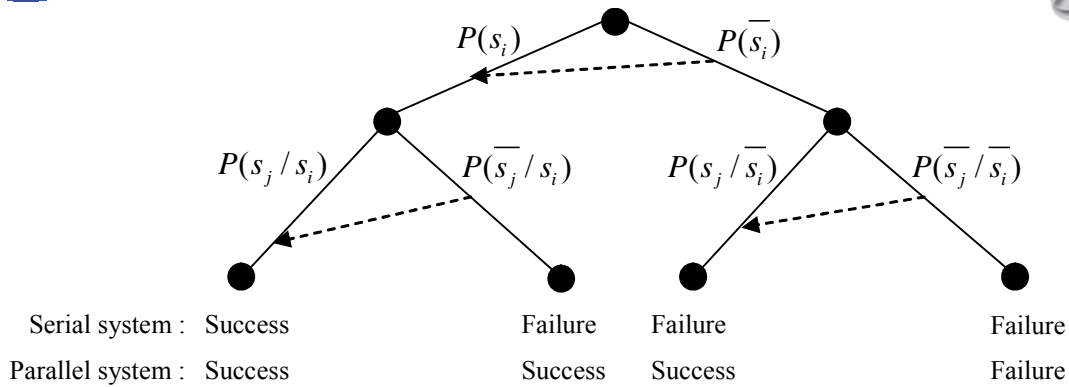


Figure 6. The THERP event tree

For serial tasks, dependency may be taken into account. Several approaches can be used and a dependency rate is required (rate=0 for no dependency or rate=1 for a total dependency). Conditional probability are then assessed using dependency this rate For instance, the probability $P(s_j/s_i)$ is equal to $P(s_j)$ if there is no dependency between s_j and s_i otherwise it is ponderated by the rate. For a total dependency between s_j and s_i , the success of s_j depends entirely of the success of s_i :

$$P(s_j / s_i) = P(s_j) + P(s_j)\cdot rate$$

An erroneous task may depend on a recovery tasks that has to be achieved before a given delay (i.e. 10 seconds, 30 seconds, 5 minutes, 30 minutes, etc.). The event graph has to be modified considering a supplementary recovery task and its success.

The prescribed tasks to be followed by a driver are identified as shown on Figure 7.

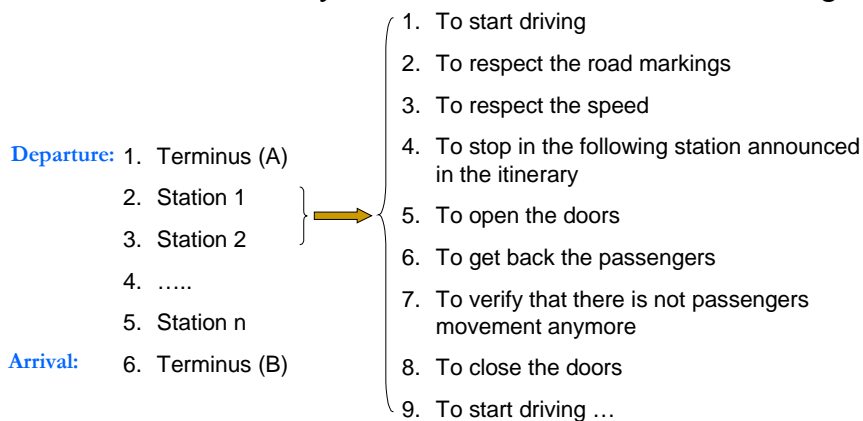


Figure 7. Human task analysis example

Figure 8 is a possible associated THERP event tree, including possible recovery processes at each level of human activities.

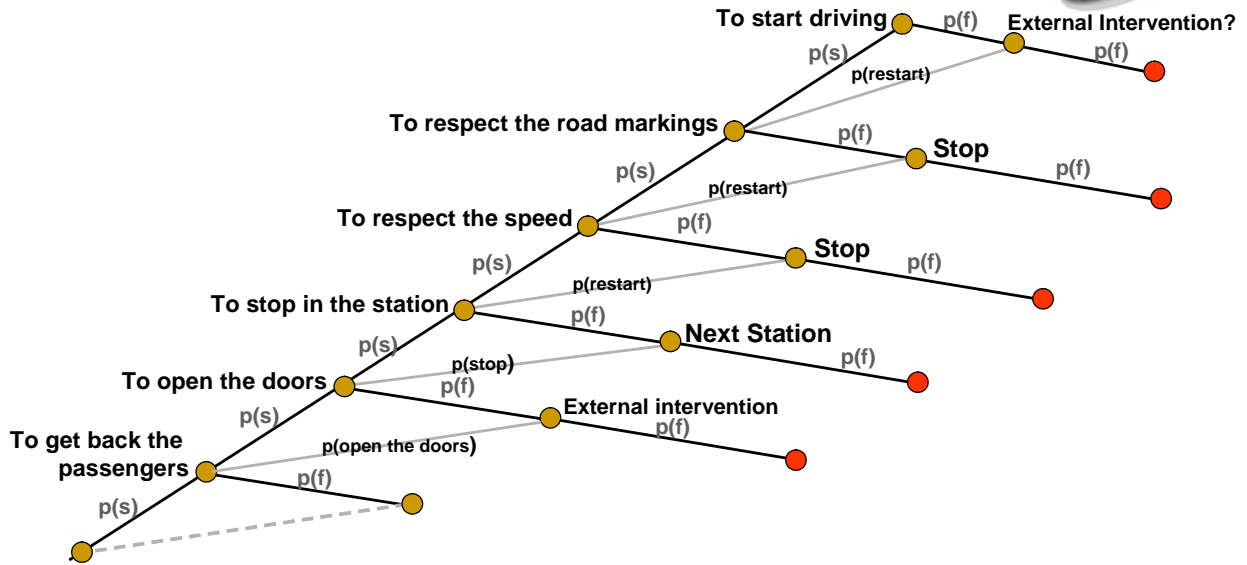


Figure 8. Example of THERP event tree

THERP focuses only on the analysis of the tasks allocated to human operators, i.e. the prescribed tasks, without evaluating possible additional tasks such as the removal of existing barriers or the creation of new barriers by human operators on field. The ACIH approach is a complementary one: it takes into account violation.

4.3 The ACIH process

The ACIH method (French acronym for Analysis of Consequences of Human Unreliability) aims at comparing prescribed task with observed ones by observations, simulations or inferences /Vanderhaegen, 2001/, Figure 9.

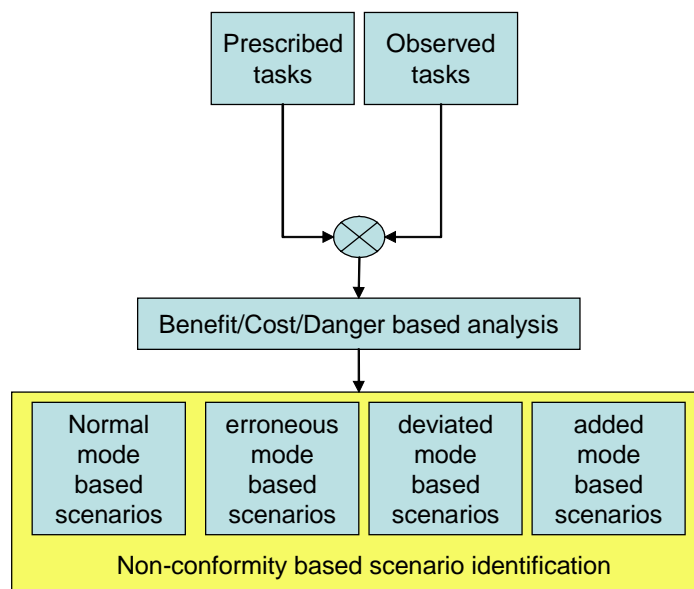


Figure 9. The ACIH process

This comparison identifies different modes of functioning of the human operators: normal modes, added modes, deviated modes, erroneous modes. Erroneous modes includes non-intentional hazardous acts such as attention and memory based failures and intentional ones



such as rule or knowledge based failures. Deviated modes concerns intentional violations such as barrier removals. The taxonomy is then based on the Reason’s classification /Reason, 1990/ of non-conformity events related to hazardous human tasks, Figure 10.

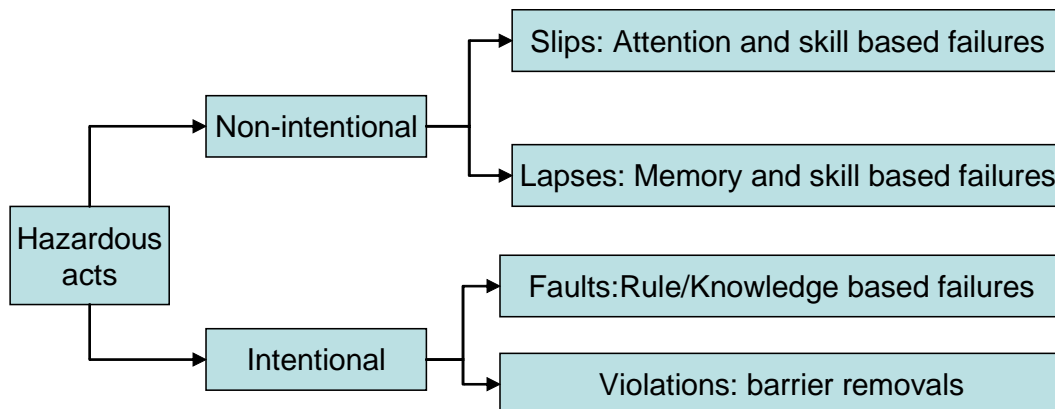


Figure 10. The Reason’s taxonomy of human error, /Reason, 1990/

The comparison between prescribed and observed tasks is based on the so-called BCD model taking into account several criteria such as safety, workload or quality. For a given human action, this model is able to assess the immediate benefits and the acceptable and immediate cost of a given action in case of success and the potential unacceptable deficits (or dangers) in case of failure. These BCD parameters can be combined with others ones in order to assess the utility level of an action:

$$Utility(s) = p(s)[(\alpha \sum B_j) + (\beta \sum C_j)] + (1 - p(s))[\gamma \sum D_j] + \epsilon.$$

B, C and D are the Benefits, the Costs and the Potential Dangers ponderated by α , β and γ respectively, occurring after the task achievement s that a probability of success is given by $p(s)$. Error assessment ϵ on all the parameters BCD can occur.

This utility function is presently tested using different tools: case-based reasoning tool /Polet et al., 2005/, neural network based tool /Zhicheng et al., 2004/, and an iterative learning control based tool /Chaali et al., 2005/. This study aims at comparing the results of the prediction tool in order to identify the technical and human factors for which each tool is the more sensitive on, and to determine the operational context and the pertinent factors for which the prediction is better. Figure 11 gives a example a such a comparative study : the neural network based model takes into account the factors of utility separately whereas the iterative learning control based model gathers these factors into the global assessment of the utility level /Chaali et al., in submission/. Results are obtained using data from simulation of a car driving platform of the university of Valenciennes. Similar study will be done for a guided transport system simulation.

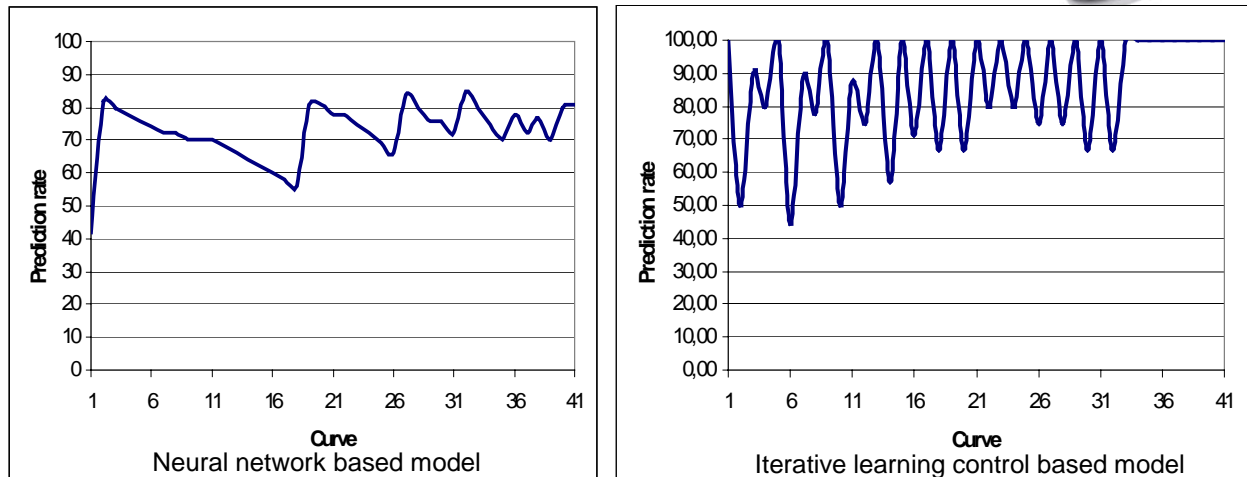


Figure 11. Comparison of prediction capacity of a neural network based tool and an iterative learning control based tool.

An Iterative Learning Control based method will also be defined in order to study the feasibility to define an on-line human error control support tool for human operators on field.

Regarding a particular violation called a barrier removal, several tasks may be identified: the perception of the current environment, the physical action to remove to barrier, the control of the new current situation without the protection, an additional action to put the removed barrier back. THERP is then able to assess the global probability of success and failure of a given barrier removal. This probability could be used into the ACIH approach to described this success or potential failure in terms of benefits, costs and/or potential dangers.

These human factor based analyses require data in order to assess probability of success or failure and to identify consequences such as benefits, costs or dangers.

4.4 Sources of data on human factors

The main challenge of THERP to assess the probability of success or failure of a given human action is availability of sources of data related to non-conformity events involving human factors. These data can be obtained by field observation, expert judgements, data based system, non-conformity event reports or simulation, Figure 12. Such data collections are off-line processes that will support the definition and the validation of human behaviour models.

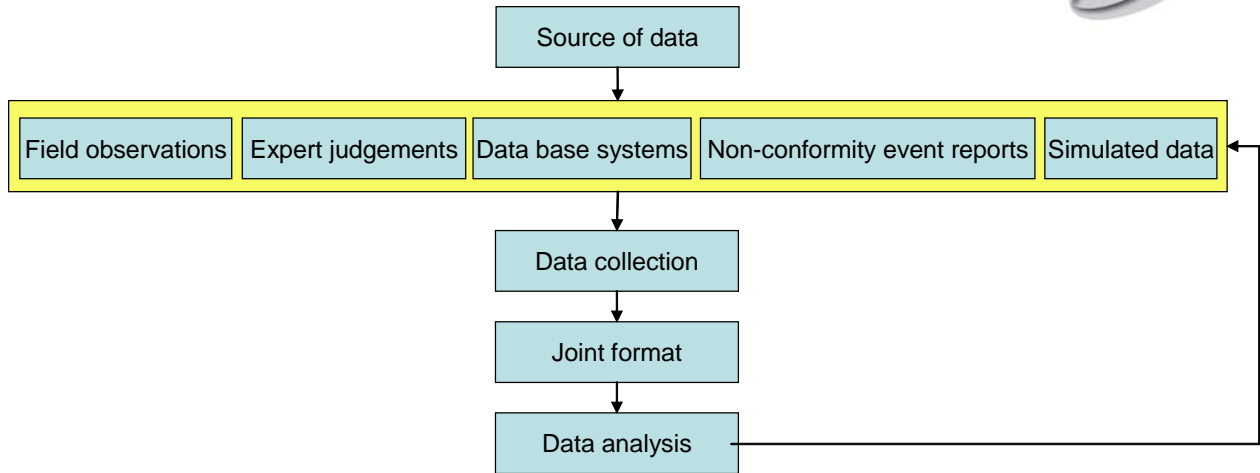


Figure 12. Sources of data on human factors

The models of human behaviour such as the utility based model of the ACIH method will be used for supporting the design of new barriers or the demonstration of the safety conformity of the global system.

5 Toward an integrated approach for human-machine system safety

The main perspective of this research work consists in defining relations between each step of the assessment method of non-conformity events, involving organisational, human and technical factors.

Regarding the human factor based design approach, the THERP and the ACIH methods will be used in order to assess probability of human error and an utility level of human action. Both positive and negative impact of human factors will be then taken into account in the control process of the system safety.

The integration of such complementary approaches in a integrated human-machine safety assessment is required. A new state of the art is then required to identify the methods that are able to take into account this human-machine safety assessment, Figure 13. For instance, such an integration will be discussed around the so-called SAFE-SADT formalism /Renaux et al., 2005/.

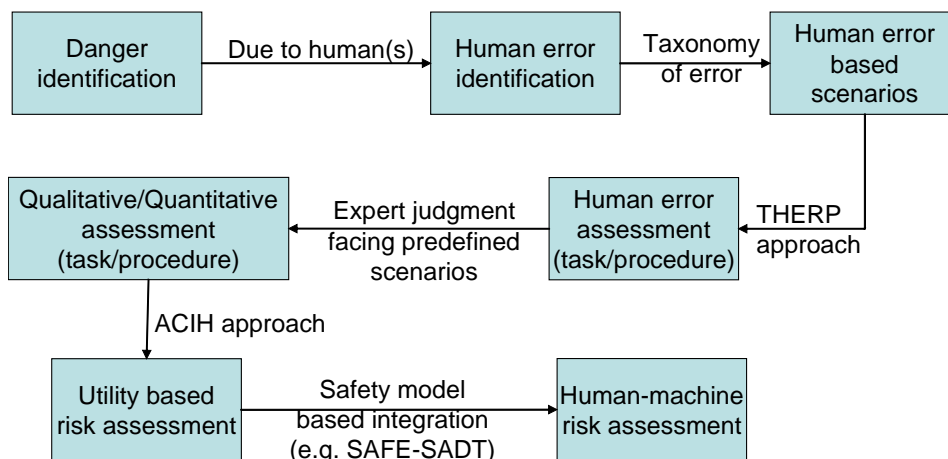


Figure 13. The integration of the human factors into the system design process



The proposed SAFE-SADT process concerns, Figure 14:

- The state and the complexity level of the global system to be assessed
- The integration of technical components assessed according the classical RAMS process where the Safety can be interpreted in terms of SIL (i.e., RAMSiL).
- The integration of human factors assessed via the THERP and ACIH methods to adapt the BCD values for the utility assessment in terms of RAMSiL.
- The interoperability between subsystems.

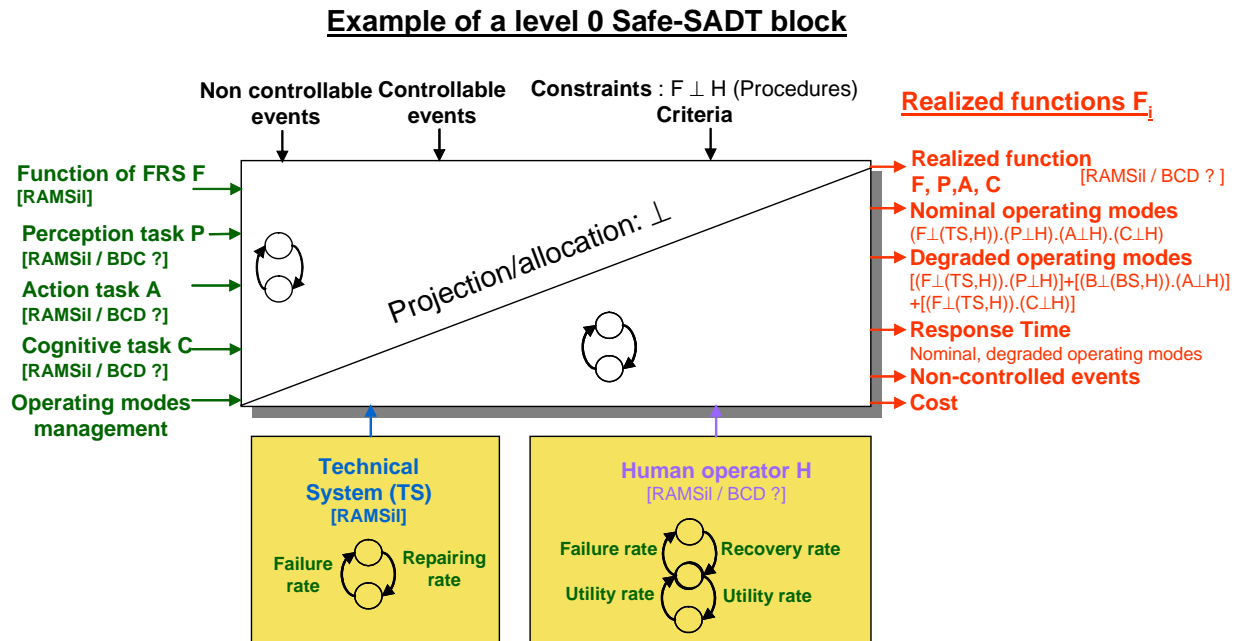


Figure 14. The SAFE-SADT process for an integrated safety, adapted from /Renaux et al., 2005/

6 Conclusion

The report has presented the advances of the works done one the WP23.2 of the MODSYSTEM project. Facing the large panel of human factor based risk assessment analysis methods, two approaches were developped: the THERP method that helps the designers of a system to assess the probability of a human error, and the ACIH method that supports them to determine the consequences of human behaviour.

The THERP method is based on the event tree and is able to take into account dependent or independent tasks, recoverable or unrecoveralbe tasks. The probability assessment of failures when performing elementary tasks requires expert judgements or databases. The probability of a combination of tasks is assessed following classical rules of conditional probabilities taking into account serial or parallel tasks.

The ACIH method aims at defining the consequences of a human behaviour considering several criteria assessment. Three classess of consequences can be identified: the immediate benefits and costs in case of success and the potential dangers or deficits in case of failure. Whatever the human behaviour (i.e. normal or deviated), costs and dangers are distinguished



when the concerned behaviour is under control and generates acceptable costs or is over control and may generate dangers.

An integrated approach for assessing human-machine safety was then evoked. It concerns the SAFE-SADT formalism for which the human factors may integrate results from the THERP and the ACIH processes.

Future short-term researches will focus on two main works: the development of a computer based tool for applying the THERP method and the feasibility study of combining the THERP and the ACIH approaches.



7 References

/Barriere et al., 1998/. Barriere M. T., D. C. Bley, S. E. Cooper, J. Forester, A. Kolaczowski, W. J. Luckas, G. W. Parry, A. Ramey-Smith, C. Thompson, D. W. Whitehead, and J. Wreathall, 1998. Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA). NUREG - 1624, US-NRC, Washington DC.

/Cacciabue, 2004/. Cacciabue P.C., 2004. Guide to Applying Human Factors Methods. Springer-Verlag, London, UK.

/Cacciabue, in press/. Cacciabue P.C., in press. Human Reliability Assesement: Methods and Techniques. In F. Redmill and J. Rajan (Eds) Human Factors in Safety Critica Systems, Butterworth-Heinemann, to appear.

/Chaali et al., 2005/. Chaali, A., Polet, P., Vanderhaegen, F., 2005. Human error based learning method. Paper presented to the 11th International Conference on Human-Computer Interaction. HCII International. 22-27 Juillet 2005. Las Vegas, Nevada. USA. ISBN 0-8058-5807-5.

/Chaali et al., in submission/. Chaali, A., Polet, P., Vanderhaegen, F., in submission. Predication of violations in road transportation system. Paper submitted to the IEEE SMC review.

/Chignell and Hancock, 1985/. Chignell, M., Hancock, P., 1985. Knowledge-based load leveling and task allocation in human-machine systems. Proceeding of annual conference on manual control. Vol. 21, pp 9.1-9.11. 1985.

/Cojazzi et al., 1993/. Cojazzi G., Cacciabue P.C., Parisi P., 1993. DYLAM-3. A Dynamic Methodology for Reliability Analysis and Consequences Evaluation in Industrial Plants. EUR 15265 EN

/Gerdes, 1997/. Gerdes, V., 1997. Identification and analysis of cognitive errors – Application to control room operators. Doctorate thesis, University of Technology of Delft, The Netherlands.

/De Keyser, 2003/. De Keyser, V., 2003. Les systèmes de report d'incident. Communication présentée lors du 3e séminaire sur le risque de défaillance et son contrôle par les individus et les organisations dans les activités à hauts risques, 12-13 Mars, Gif-sur-Yvette, France.

/D6-UGTMS, 2003/. Safety conceptual approach & guideline. Deliverable D6 of the UGTMS european project. September 2003.

/D10-UGTMS, 2004/. Confirmity assessment, human factors issues & guidelines for FRS. Deliverable D10 of the UGTMS european project. January, 2004.

/Embrey, 1992/. Embrey DE, 1992. Managing Human Error in the Chemical Process Industry. Proceedings of Int. Conf. on Hazard Identification and Risk Analysis, Human Factors and Human Reliability in Process Industry. Orlando Florida, January 15-17, Amer. Inst. of Chem. Eng., New York, 399-413, 1992



/Hannaman, Spurgin, 1984/. Hannaman GW, Spurgin AJ., 1984. Systematic Human Action Reliability Procedure (SHARP). EPRI NP-3583, Project 2170-3, Interim Report, NUS Corporation, San Diego, CA, US.

/Hollnagel, 1999/. Hollnagel, E., 1999. Accident and barriers. 7th European Conference on Cognitive Science Approaches to Process Control, Villeneuve d'Ascq, France, pp. 175-180.

/Hudson et al., 98/ Hudson, P.T.W., Verschuur, W.L.G., Lawton, R., Parker, D., Reason, J.T., 1998. Bending the rules II – Why people break the rules or fail to follow procedures and what can you do about it? The violation manual, version 1.3, Leiden University.

/Humphrey, 1988/. Humphrey, P., 1988. Human reliability assessors guide. In Human Factors and Decision Making – Their Influence on Safety and Reliability - B. A. Sayers (ed.), (Elsevier : Amsterdam), pp.71-86.

/Kirwan, 1997/. Kirwan, B., 1997. Validation of human reliability assessment technique: part 2 – Validation results. Safety Science, 27, 43-75.

/Macwan, Mosleh, 1993/. Macwan A. P., Mosleh A., 1993. A Simulation Based Approach to Modeling Errors of Commission during Nuclear Power Plant Accidents: Application to PRA. Proc. of Int. ANS/ENS Topical Meeting on Probabilistic Safety Assessment, PSA 93, Clearwater Beach, FL, Jan. 26-29, 1993.

/Polet et al., 2002/. Polet, P., Vanderhaegen, F., Wieringa, P., 2002. Theory of safety related violation of system barriers. Cognition Technology & Work, 4, 171-179.

/Polet et al., 2003/. Polet, P., Vanderhaegen, F., Amalberti, R., 2003. Modelling border-line tolerated conditions of use (BTCUs) and associated risks. Safety Science, 41, 2-3, 111-136.

/Reason, 1987/. Reason J., 1987. Papers in New Technology and Human Errors. J. Rasmussen, K. Duncan and J. Leplat (Eds.). pp. 5-14, 15-22, 45-52, 63-86, J. Wiley and Sons, NJ.

/Reason, 1990/. Reason, J., 1990. *Human Error*. Cambridge University Press, Cambridge, UK.

/Renaux et al., 2005/. Renaux, D., Cauffriez, L., Beugin, J., Benard, V., 2005. SAFE-SADT methodology. Presentation of the MODSYTEM WP23 meeting, 6th June 2005.

/Schonpflug, 1985/. Schonpflug, W., 1985. On the role of psychophysiological recording in stress research. In F. Klix, R. Naatanen, K. Zimmer (Eds), Psychophysiological approaches to human information processing. Elsevier, North Holland, 1985.

/Siu, Acosta, 1991/. Siu N., C. Acosta, 1991. Dynamic Event Tree Analysis - An Application to Steam Generator Rube Rupture, In Apostolakis, G.E. (Ed.), Proc. of the Int. Conf. on Probabilistic Safety Assessment and Management (PSAM) 4-7, February 1991, Beverly Hills, California, 413-418.



/Swain, 1990/. Swain, A. D., 1990. Human reliability analysis: need, status, trends and limitations. *Reliability Engineering and System Safety*, 29, 301-311.

/Swain and Guttman, 1983/. Swain, A. D. and H. E. Guttman, 1983. *Handbook of Reliability Analysis with emphasis on Nuclear Plant Applications*. Nuclear Regulatory Commission, NUREG/CR-1278, Washington D.C.

/Valancogne, Nicolet, 02/ Valancogne, J., Nicolet, J.-L., 2002. Defence-in-depth : a new systematic and global approach in socio-technical system design to guarantee better the timelessness safety in operation. *European Conference on System Dependability and Safety*, March 19-21 2002, Lyon, France, pp. 298-305.

/Van der Schaaf, 1995/. Van der Schaaf, T., 1995. Human recovery and error management. *Proceedings of the 5th IFAC/IFIP/IFORS/IEA, Symposium on Analysis, Design and Evaluation of Man-Machine Systems*, June 27-29 1995, Boston, USA, pp. 91-96.

/Vanderhaegen, 2001/. Vanderhaegen, F., 2001. A non-probabilistic prospective and retrospective human reliability analysis method – application to railway system. *Reliability Engineering and System Safety*, 71, 1-13.

/Weiner et al., 1984/. Weiner, E. L., Curry, R. E., Faustina, M. L., 1994. Vigilance and task load: in search of the inverted U. *Human factors*, 1984, 26(2), 215-222.