



MODURBAN

FP6 Project: TIP4-CT-2005-516380

EC Contract n°: 516380

MODSYSTEM SUBPROJECT

– DELIVERABLE REPORT –

Deliverable ID:	D128
Deliverable Title:	Risk assessment based on human factors
Responsible partner:	UVAL
Contributors:	UVAL, KITE, JRC, LUL, RATP

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: Risk assessment based on human factors
Document ID: D128
Revision: Version 6
Revision Date: 15/04/2008
Author: Chaali, A., Vanderhaegen, F., Cassani, M.

Approvals

	Name	Company	Date	Visa
<i>Technical Management Committee</i>	B. VON WULLERTSORFF P. TEILLET / G. P-RIVIÈRE D. DIMMER G. LEGOFF L. LINDQVIST A.PRICE / U. HENNING M. NOCK JP RICHARD/D. COINEAU Y. AMSLER C. GOUTORBE	UNIFE ALSTOM THALES ANSALDO STS BOMBARDIER SIEMENS KNORR BREMSE RATP UITP ALMA	17/07/08	OK
<i>Coordinator</i>	B. VON WULLERSTORFF	UNIFE	17/07/08	OK
<i>Subproject Coordinator</i>	JP. RICHARD	RATP	17/07/08	OK
<i>Quality Manager</i>	B. VON WULLERSTORFF C. GOUTORBE	UNIFE ALMA	17/07/08	OK

Document history

Revision	Date	Modification	Author
Version 1	01/10/2007		UVAL
Version 2	09/11/2007		UVAL
Version 3	15/01/2008		UVAL, KITE
Version 4	31/01/2008		UVAL, KITE
Version 5	31/03/2008		UVAL
Version 6	15/04/2008		UVAL



The scope of the document applies to:

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

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



SECTION I – DELIVERABLE SUMMARY

Risk assessment based on human factors	
Deliverable ID , associated WP & Subproject	D128 MODSYSTEM/WP23
Type of Deliverable	Report
Input / Starting stage	<i>D87 of MODURBAN, WP23 meetings, Outputs of the Workshop on Human Factors of the WP23 in Valenciennes, the 11-12 of January 2007</i>
Output / Final stage	<i>Report D128</i>

Lead partner(s)	UVAL
Achievement to date (%)	
Expected date of achievement	
Type of exploitation	
Exploitation potential	
Protection	
Protection date	

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

Associated Risk analysis	Type, solution envisaged, action, actors	Actual Reduction
Before start		
During task implementation		



Risk assessment based on human factors

Deliverable Abstract

This report entitled ‘Risk assessment based on human factors’ is the second step of the WP23.2 on human factor impact on functional and technical specifications. It concerns risk assessment process related to the human factor. It presents some human error probabilities evaluation. This report is initially based on the D87 of the MODURBAN project and on the outputs of the workshop of WP23 on Human Factors in Valenciennes, the 11th and 12th of January 2007. These outputs concern the medium term perspectives related to the feasibility of the human factor integration into the safety analysis process of an urban guided transport system.

This reports contains these complementary parts:

- The first part of this report reminds the human error related concepts and methods and their consequences evaluation with the Benefit, Cost and Deficit (BCD) model.
- The second part presents a human error probability evaluation method: THERP.
- The third part presents some examples of human error probability evaluation with THERP.
- The fourth and the fifth parts apply THERP to evaluate some human error probabilities in normal and degraded mode of urban train driving, without and with barrier removals.
- The last part of this report proposes extended perspectives for human error related risk evaluation in urban guided transport system.

Associated Milestone (if relevant):

Contribution to MODURBAN Objectives as mentioned in the Description of Work

Objective Definition	Comments	Quantification
Objective 1 -		
Objective 2 –		
Objective 3 ...		
Objective 4 ...		

SECTION 2 – DELIVERABLE DETAILED DESCRIPTION

Table of contents:

Table of contents:	6
Figures and Tables:	7
Figures:	7
Tables:	7
1 Introduction: Risk analysis in a Human-Machine System	8
2 Terms, definitions and abbreviations	9
3 The human errors in the Human-Machine System	10
3.1 The human error definition and analysis	10
3.2 Barrier design and barrier removal	11
4 Technique for Human Error Rate Prediction: THERP	13
4.1 The choice of THERP	13
4.2 The THERP process	14
5 Examples of human error probability assessment with THERP	16
5.1 The doors procedure, example 1	16
5.2 The doors procedure with sound signal, example 2	18
5.3 The red light procedure, example 3	20
5.4 The red light procedure with external intervention, example 4	22
6 Examples of the probability of failure of barrier removals	24
6.1 The example of an Express Regional Network: RER A (France)	25
6.2 The task driver	27
6.3 Probability assessment without and with barrier removal	28
6.4 THERP use in transport domain	30
7 Perspectives for an integrated approach for human-machine system safety design	31
7.1 The barrier removal expected utility	32
7.2 Simple illustration	32
7.2.1 Hypothesis:	33
7.2.2 The train driver error consequences evaluation with the BCD model	33
7.2.3 The train driver error probability evaluation with THERP	33
7.2.4 The train driver error utility evaluation	33
7.3 The barrier removal expected utility based prediction method	34
8 Conclusion	34
9 References	36

Figures and Tables:

Figures:

Figure 1 - Risk analysis in a Human-Machine System	8
Figure 2 - Human Error Classification (Reason, 1990)	10
Figure 3 - Barriers of prevention, of recovery and of containment.....	12
Figure 4 - The BCD model.....	13
Figure 5 - The THERP event tree.....	15
Figure 6 – The doors procedure: THERP tree.....	17
Figure 7– The doors procedure: example 1	18
Figure 8 – The doors procedure with sound signal: THERP tree	19
Figure 9 – The doors procedure with sound signal: example 2	20
Figure 10 – The red light procedure: THERP tree	21
Figure 11 – The red light procedure: THERP Tool results	22
Figure 12 – The red light procedure with external intervention: THERP tree.....	23
Figure 13 – The red light procedure with external intervention: THERP Tool results.....	24
Figure 14 - Nature of the risked events	25
Figure 15 - Events at risk connected to the human factors	25
Figure 16 - Events at risk connected to the human factors	26
Figure 17 - Some signs involved in the degraded train driving procedure	26
Figure 18 - Human task analysis example	27
Figure 19 - Example of THERP event tree	27
Figure 20 – The speed procedure in normal mode: THERP Tool results	29
Figure 21 – The speed procedure in degraded mode: THERP Tool results.....	30
Figure 22 - The BR decision-making process.....	32
Figure 23 - Risk analysis in Human-Machine System.....	35

Tables:

Table 1 - Comparison of the standard HF methods	14
---	----

1 Introduction: Risk analysis in a Human-Machine System

Risk analysis in Human-Machine Systems (HMS) generally and in transportation specially has to take into account the human errors in order to improve both the risk analysis and the safety of the design. In fact, in some transportation domain such as aviation or railway, human error is the cause of more than 70% of the observed accidents (Amalberti, 90).

In Human-Machine Systems, malfunctions can be caused by technical failures, human failures, or any combination of both types of failures (see Figure 1). Risk analysis consists in forecasting such undesirable events in order to reduce their frequency or consequences.

Traditionally, quantifying the risk of an undesirable event involves a combination of occurrence probability and consequence evaluation (see Figure 1).

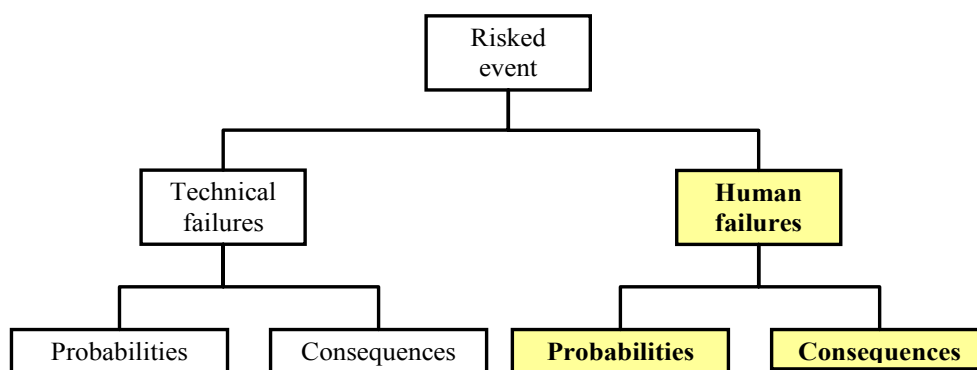


Figure 1 - Risk analysis in a Human-Machine System

This report entitled ‘Risk assessment based on human factors’ tries to give solutions to integrate human factors into the safety analysis process of urban guided transport systems. In fact, the aim of this report is to present a methodology that evaluates the probabilities of human errors in urban train driving procedure using the Technique for Human Error Rate Prediction (THERP) (Swain and Guttmann, 1983). The consequences are evaluated by the so-called Benefit-Cost-Deficit (BCD) model (Polet et al., 2002; Vanderhaegen, 2004). The report illustrates the probabilities evaluation with some examples related to urban guided train driving procedures.

This report focuses on the risk assessment process related to the human factor and presents some examples of human error probability evaluation. It is initially based on the D87 of the MODURBAN project and on the outputs of the workshop of the MODURBAN WP23 on human factors held at Valenciennes the 11th and 12th of January 2007. It is divided into several parts:

- The first part of this report reminds the definition and analysis of human errors.
- The second part presents the human error probability evaluation method: THERP.
- The third part presents some examples of human error probability evaluation with THERP.

- The fourth and the fifth parts apply THERP to evaluate some human error probabilities related to the achievement of procedures of urban train driving on both normal and degraded mode of functioning, and with or without barrier removals.
- The last part of this report proposes perspectives for future human error related risk evaluation in urban guided transport system.

Notes:

- The repartition between the human part and the technical part in the safety demonstration is not developed in this report.
- Probability assessment of the human action might be advised and applied when human operators are considered as protections to control degraded modes.
- The probability assessment used the basic failure probability of elementary tasks given by the THERP method. These basic elementary tasks probabilities were initially identified for nuclear power plant application. Future works might verify that these elementary tasks and their associated probabilities of failure are also suitable for being applied to urban guided transport.
- The procedures proposed in this report are simplified. The feasibility study might be extended in order to analyse more realistic and complex procedures.
- The probability assessment results might be compared for validation with those obtained with databases or expertises from urban guided transport operators.

2 Terms, definitions and abbreviations

The abbreviations used in this report are defined below.

APJ	Absolute Probability Judgement
BCD	Benefit / Cost / potential Deficit
BR	Barrier Removal
ET	Event Tree
FT	Fault Tree
HCR	Human Cognitive Reliability
HMS	Human-Machine System
HRA	Human Reliability Analysis
IDA	Influence Diagram Approach
MAPPS	Maintenance Personnel Performance Simulation
NBR	No Barrier Removal
OAT	Operator Action Tree
PC	Paired Comparison
SLIM	Success Likelihood Index Methodology
TESEO	Tecnica Empirica Stima Errori Operatori
THERP	Technique for Human Error Rate Prediction
U	Expected utility

3 The human errors in the Human-Machine System

3.1 The human error definition and analysis

System components are considered to have failed when they do not run as they should. Specifically, the human components of the Human Machine System—the human operators—are considered to have failed when their behaviour deviates from the prescribed behaviour. Given that human errors can cause more than 70% of the accidents in certain domains (e.g., aeronautics) (Amalberti, 2001), Human Machine System risk analysis cannot afford to neglect the human factor.

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 of human reliability and is related to the probability that an error will occur while the human operator is performing the allocated task. However, the general concept of human failure is a bit more complex because when operators deviate from reliable behaviour, their actions can be either intentional or unintentional. Unintentionally deviate behaviours (i.e., slips, lapses) are indeed called "errors". Even if mistakes are intentional deviate behaviours, the human operators who perform them think they behave correctly. Other intentionally deviate behaviours that are expected to cause specific consequences are called "violations" (see Figure 2).

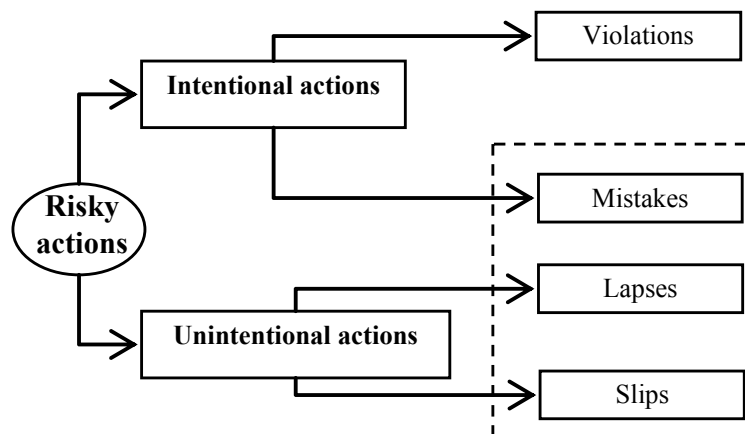


Figure 2 - Human Error Classification (Reason, 1990)

Actions are erroneous related several characteristics such as (Hollnagel, 1998):

- Erroneous goal, e.g. the achievement of an action related to a wrong target or a wrong objective.
- Erroneous sequence, e.g. the achievement of an action relates to an omission, an interruption, an inversion, a repetition, an intrusion.
- Erroneous duration, e.g. the processing time of an action is too large or too small.
- Erroneous time, e.g. the action is omitted or achieved too early or too late.
- Erroneous distance, e.g. the achievement of an action is too far away from the target or too close to the source.

- Erroneous speed, e.g. the action is realized too quickly or too slowly.
- Erroneous space, e.g. the direction, the movement or the orientation associated to an action is wrong.
- Erroneous intensity, e.g. the effort done to achieve an action is too high or too low.

A given erroneous action can also be assessed in terms of consequences. The so-called Benefit-Cost-Deficit (BCD) approach developed in (Polet et al., 2002; Vanderhaegen, 2004) analyzed intentional or unintentional human errors using three distinct consequences on several evaluation criteria such as safety, service quality, workload or production quantity:

- The acceptable costs due to the occurrence of the erroneous action. The human error occurrence may require additional behaviours to recover or control the situation.
- The possible benefits due to the occurrence of the erroneous action. The knowledge of the controlled system behaviour in terms of safety and performances may increase with the management of the human errors.
- The unacceptable possible deficit related to the occurrence of the erroneous action. A human error may lead to unacceptable and unrecoverable situations.

The BCD model is able to assess the benefits and the acceptable cost of a given action in case of successful human error control and the potential unacceptable deficits or dangers in case of failed human error control. Objectively, these BCD parameters may be combined with others ones in order to assess an expected utility level noted $U(s)$ of an erroneous action s :

$$U(s) = p(s)[\alpha.B + \beta.C] + (1 - p(s))[\lambda.D] + \varepsilon$$

The parameters B, C and D are the benefits, the costs and the potential deficits or dangers ponderated by α , β and γ respectively, occurring after the task achievement noted s for which a probability of success of the error control process is given by $p(s)$. Error assessment ε on all the parameters BCD can occur.

Means to achieve these human errors are both internal and external defenses that aim at protecting human operators from the occurrence or the consequences of a miss-controlled event. Internal defences relate to the intrinsic capacities of a human operator to control an event. External defenses are external means such as barriers that provide human operators with protection from dangers.

3.2 Barrier design and barrier removal

In order to inhibit human deviate behaviour and/or to reduce its consequences, Human-Machine System designers provide the system with barriers.

A barrier is a technical or human support that protects 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 (see Figure 3).

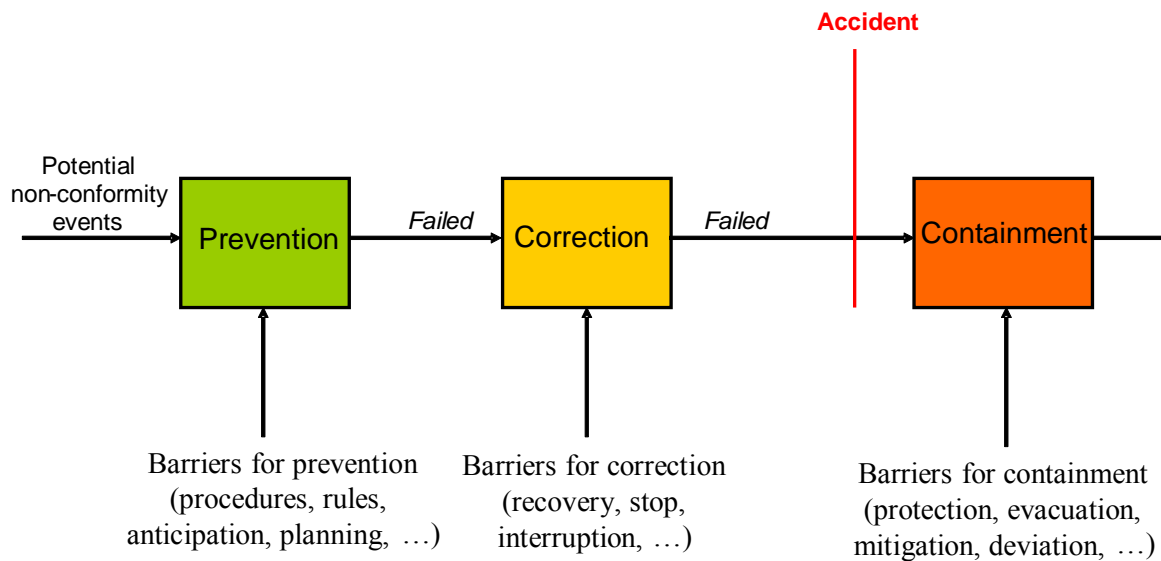


Figure 3 - Barriers of prevention, of recovery and of containment

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, functional barriers, symbolic barriers and immaterial barriers.

Generally, the risk analysis in Human-Machine System done by the designer is a mono-criterion analysis based essentially on the safety analysis. While, the online risk analysis done by the human operator is a multi-criterion analysis.

Specially, the barrier removal is usually the result of a multi-criterion risk analysis. These criteria may be such as the human operator Workload, the Safety, the Productivity, the Quality, the Time, etc. (Polet et al., 2002). It may result from a compromise between many criteria analysis. This compromise may be illustrated by the benefits, the costs and potential deficits established by the BCD model presented above (Polet et al., 2002; Vanderhaegen, 2004).

The BCD model was designed to remedy the lack in existing methods by evaluating one of the possible “other” tasks, the Barrier Removal. BR is interpreted as a compromise between the three attributes of the BCD model (see

Figure 4):

- Benefits (ΣB): Barrier-removal is a goal-driven behaviour offering an immediate benefit that is seen to outweigh the cost.
- Costs (ΣC): In order to remove a barrier, the human operator must sometimes modify the material structure and/or the operating mode. Such modifications have a cost, usually an increased workload and/or negative consequences on productivity, quality or both.
- Deficits (ΣD): Because removing a barrier introduces a potentially dangerous situation, such actions create a potential deficit due to the related risk.

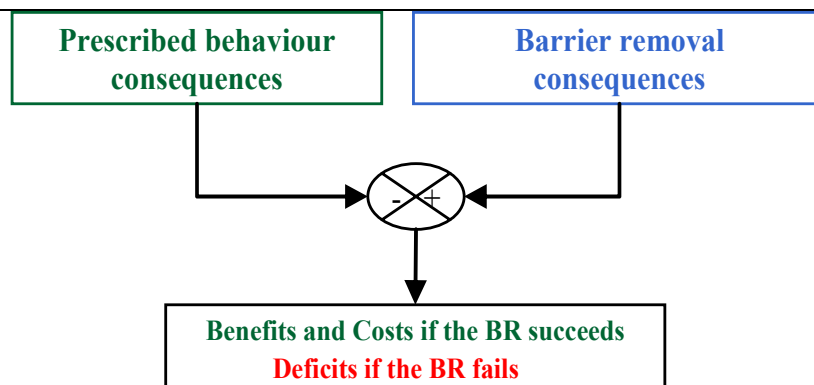


Figure 4 - The BCD model

Two complementary approaches for safety analysis integrating human factors can then be followed:

- The first one consists in analyzing of the success or failure of prescribed behaviours.
- The second one consists in analysing the success or failure of deviate behaviours.

Both approaches can be done with the THERP method.

4 Technique for Human Error Rate Prediction: THERP

In order to evaluate the human error probabilities, it is necessary to:

- analyse the working environment to be studied,
- identify the possible human errors; and
- evaluate the identified human errors by a probability or consequence based measures.

4.1 The choice of THERP

The most commonly used methods and techniques for human factor analysis are presented on the deliverable D87 of MODURBAN (Vanderhaegen et al, 2006). Table 1 compared the following methods:

- 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).

Table 1 - 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 modelling; **1** = insufficient modelling, etc.

However, the THERP approach is the most commonly applied because it offers two very important advantages (Cacciabue, 1996):

- the direct access to the data base contained in its handbook; and
- the immediate integration of its output data into a Fault Tree type approach.

4.2 The THERP process

The Technique for Human Error Rate Prediction (THERP) is a predictive method that assesses human error probabilities and estimates the possible degradation of a given human-machine system caused by human errors with or without interaction with equipments such as barriers. It is basically a hybrid approach because it models human errors using probability trees and models of dependence, but also it considers all factors affecting operator actions.

THERP goals are:

- to forecast the human error probability,
- to evaluate the HMS degradation due to the human error, alone or associated to an equipment dysfunction.

THERP steps for actions are:

- definition of the weak points of the system,
- list and analysis of the tasks, the possible errors which are connected with them and recovery modes,
- estimation of the errors probabilities which relate to tasks,
- estimation of the human error effects on the system (consequences),
- recommendations to modify the system (or barriers) and new probability calculation of failing of the system (or barriers).

In order to describe and analyze these human errors, THERP uses the Human Reliability Analysis (HRA) Event Tree (ET) as its basic tool. By the use of HRA-ET a graphical description of the procedural step in a task is set out in a logical framework, which implies that, at each node of the tree, there is a binary decision point, representing the failure or the success of the current action.

These trees are compatible with conventional system event trees. Moreover they are evaluated in the formal mathematical sense and, consequently, once the success or failure probability of each particular task step in a procedure is known, the overall reliability of the procedure can be calculated.

In particular, THERP uses the event tree method to assess the probability of success and failure of serial and parallel tasks (Cacciabue, 2004) (see Figure 5).

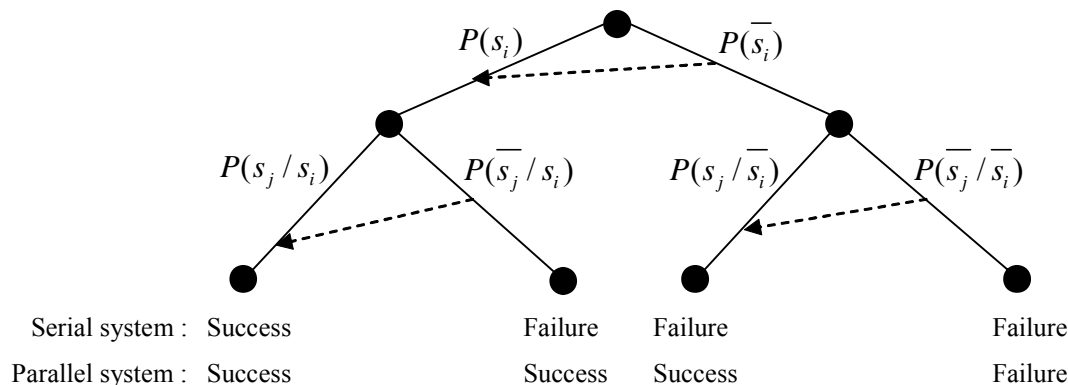


Figure 5 - The THERP event tree

The tasks involved in an event tree are serial if in the system all human activities must be performed correctly for procedure success to be achieved.

The tasks involved in an event tree are parallel if the system fails only if all of the human activities in a set are performed incorrectly.

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 :

$$P(s_j / s_i) = P(s_j) + P(\overline{s_j}).rate$$

An erroneous task may depend on a recovery task 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 and failure probabilities.

For the examples that will be developed below, the THERP trees have been created and calculated by utilizing the THERP Tool.

The THERP Tool has been conceived and developed by KITE Solutions and it is an automated computerized version of the THERP method.

In the below clauses, the probability of success of a given procedure will be noted $p(S)$ and the probability of failure of a given procedure will be noted $p(F)$.

5 Examples of human error probability assessment with THERP

In order to explain the THERP technique, some simplified examples of human tasks in urban guided system have been chosen and their probabilities of failure and success have been evaluated with the THERP Tool.

5.1 The doors procedure, example 1

The first example is based on the task according to which train drivers have to open the train doors when they see a yellow aspect of the signal in the driver cab. Opening the doors necessitates that the train drivers push a special button.

As specified in the previous clause, in order to assess the driver error probability with THERP, the following steps must be performed:

- to identify the elementary tasks of the human operator prescribed task,
- to evaluate the probability of failure of the elementary tasks,
- to calculate the probability of failure of the complete activity of the train driver.

THERP Tool helps to evaluate the probabilities of success and failure of each elementary task. Then it calculates the final probabilities of success $p(S)$ and failure $p(F)$ of the whole human operator task.

In the case of the doors procedure, the elementary tasks are the following:

- to see the yellow aspect of the signal: elementary task noted A,

- to interpret the yellow aspect of the signal: elementary task noted B,
- to action the door button: elementary task noted C.

The corresponding THERP tree is the following one (see Figure 6):

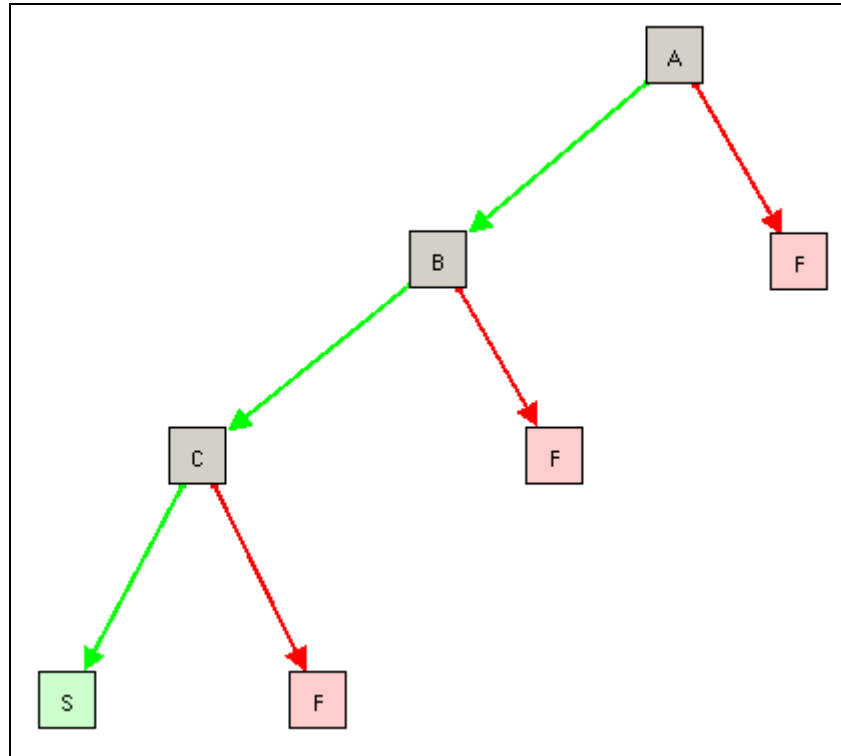


Figure 6 – The doors procedure: THERP tree

The evaluation of the probabilities of failure of the elementary tasks and the calculation of the final probability performed with the THERP Tool are illustrated in the following figure (see Figure 7):

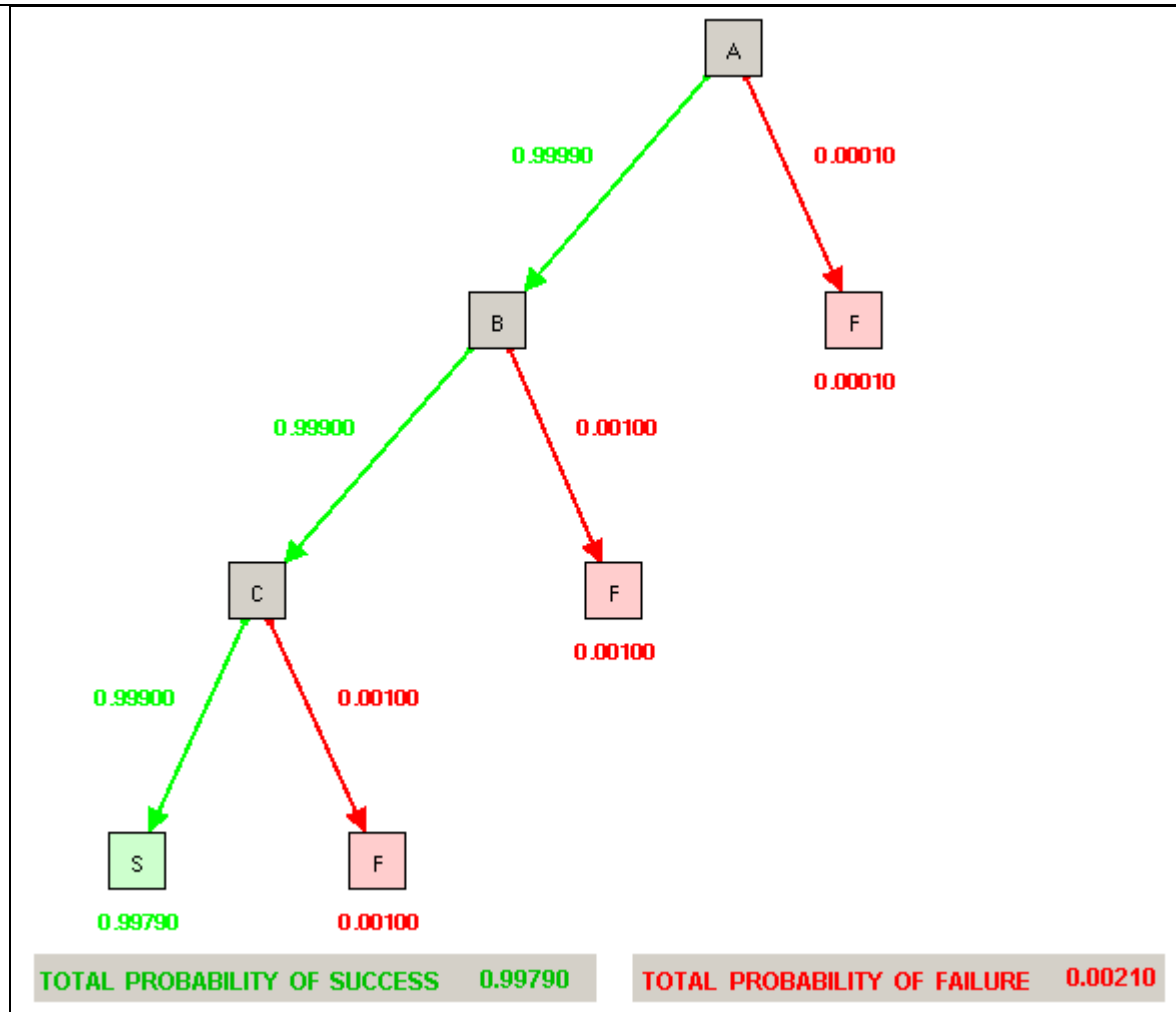


Figure 7– The doors procedure: example 1

The evaluation of the probabilities of these elementary tasks takes into account the experience of the human operator and the level of his stress. The variation of these two criteria influences the probabilities values. Generally, in all examples provided in this Deliverable, the hypothesis is that the driver has a good experience of his activity and his level of stress is medium.

As it can be seen from the Figure 7, the probabilities of success and failure calculated by the THERP Tool for this train driver procedure are:

$$p(S) = 0.99790 \quad \text{and} \quad p(F) = 0.00210$$

5.2 The doors procedure with sound signal, example 2

The previous example of THERP procedure can be changed by taking into account a recovery factor.

In general a recovery factor is any element of a system that acts to detect and correct an incorrect task performance in time to avoid undesirable consequences. For instance an erroneous task may depend on a recovery task that has to be achieved before a given delay. The event tree must be modified considering a supplementary task and its success and failure.

The specific procedure of the example 1 can be modified by taking into account the recovery factor represented by a sound signal. In fact, generally, if the train driver does not see or does not correctly interpret the yellow aspect of the signal, then a sound signal is heard. Hence in the doors procedure, the sound signal is a mean that recovers the train driver activity by advertising him when he does not action the button.

In this case, the elementary tasks are the following:

- to see the yellow aspect of the signal: elementary task noted A,
- to interpret the yellow aspect of the signal: elementary task noted B,
- to hear the sound signal if the train driver does not see or does not interpret the yellow aspect of the signal: elementary task noted C,
- to interpret the sound signal: elementary task noted D,
- to action the door button: elementary task noted E.

The THERP tree corresponding to this door procedure becomes the following one (see Figure 8):

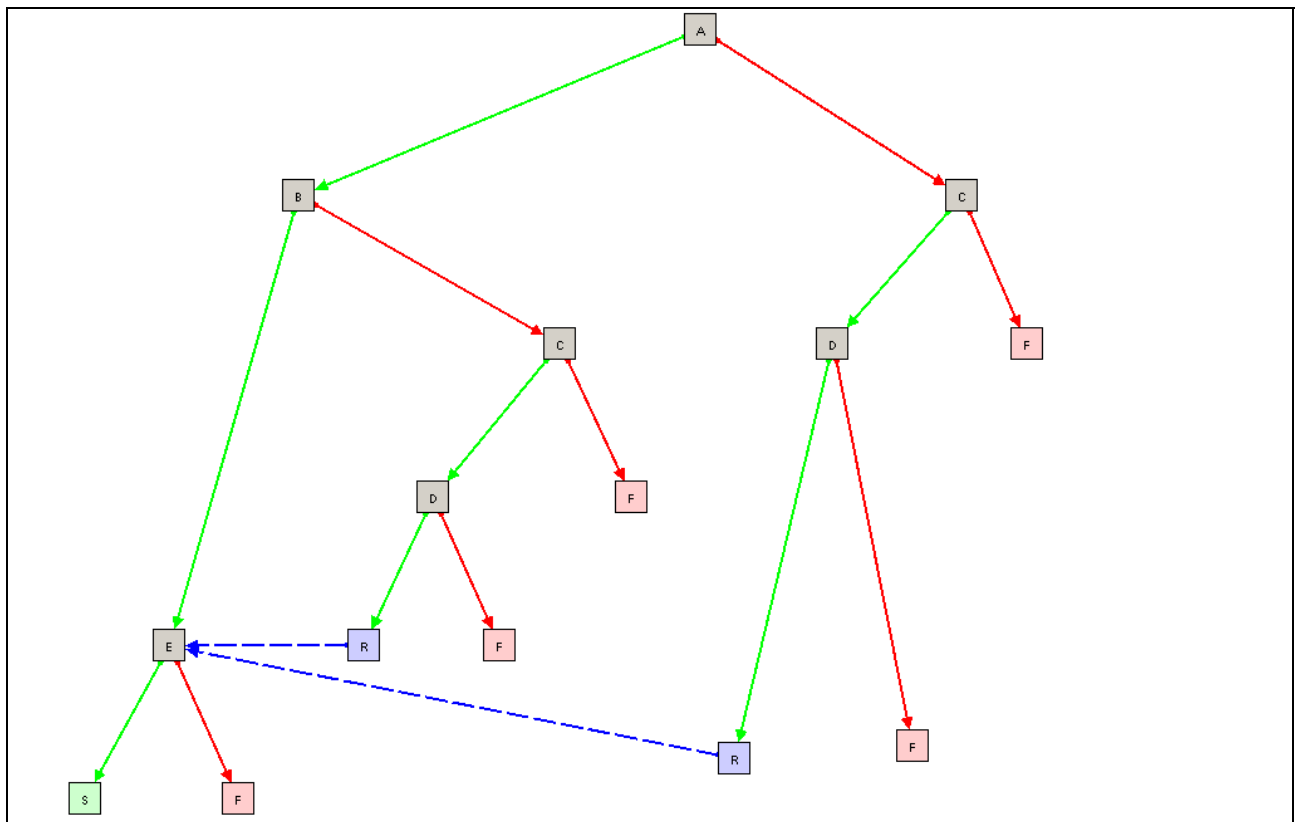


Figure 8 – The doors procedure with sound signal: THERP tree

The evaluation of the probabilities of failure of the elementary tasks and the calculation of the final probability performed with the THERP Tool are illustrated in the following figure (see Figure 9):

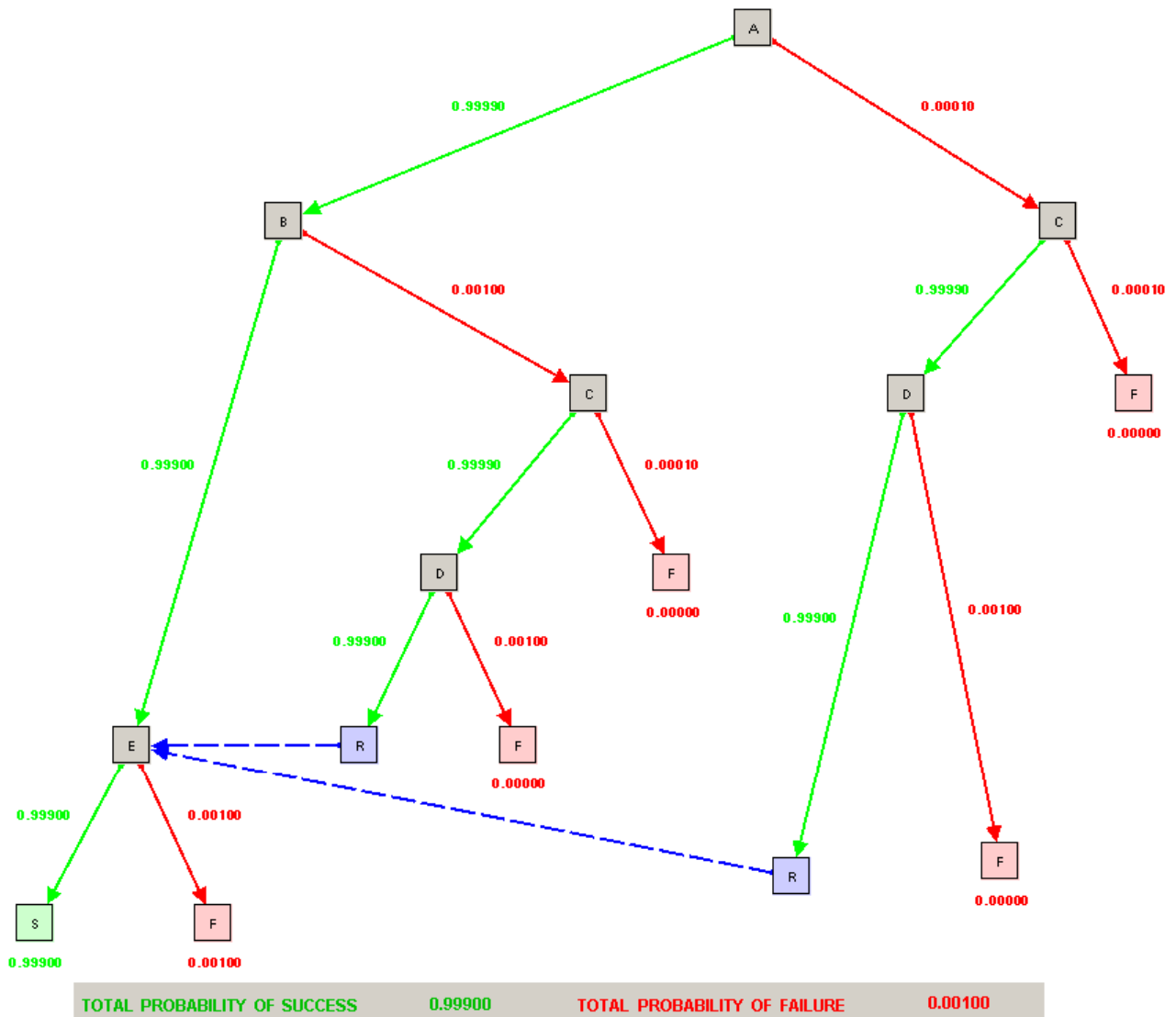


Figure 9 – The doors procedure with sound signal: example 2

As it can be seen from the Figure 9, the probabilities of success and failure calculated by the THERP Tool for this train driver procedure are:

$$p(S) = 0.99900 \quad \text{and} \quad p(F) = 0.00100$$

5.3 The red light procedure, example 3

This example is concerned with the respect of a red aspect of the signal by the train driver. In fact, when faced to this signal, the train driver has to stop the train by pressing a special button.

In this case, the elementary tasks are the following:

- to see the red aspect of the signal: elementary task noted A,
- to interpret the red aspect of the signal: elementary task noted B,
- to action the button to stop the train: elementary task noted C.

The corresponding THERP tree is the following one (see Figure 10) and is similar to the tree of example 1:

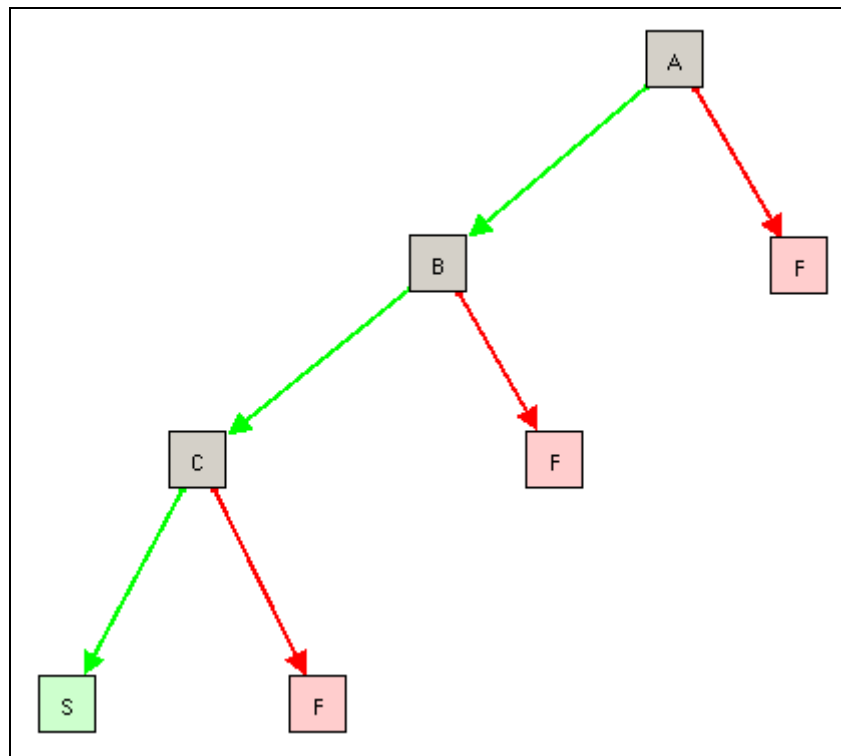


Figure 10 – The red light procedure: THERP tree

The evaluation of the probabilities of failure of the elementary tasks and the calculation of the final probability performed with the THERP Tool are illustrated in the following figure (see Figure 11):

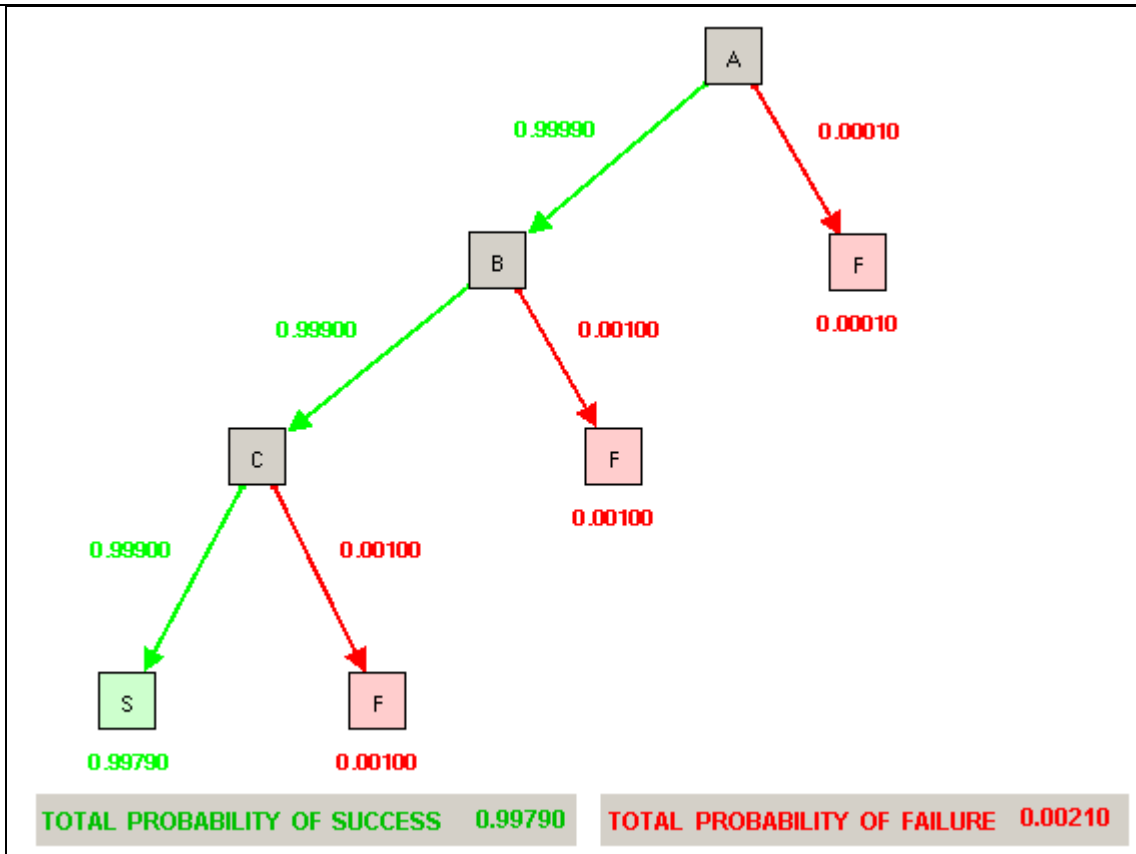


Figure 11 – The red light procedure: THERP Tool results

As it can be seen from the Figure 11, the probabilities of success and failure calculated by the THERP Tool for this train driver procedure are:

$$p(S) = 0.99790 \quad \text{and} \quad p(F) = 0.00210$$

5.4 The red light procedure with external intervention, example 4

Also the example 3 can be changed by introducing a recovery factor. In fact, in general, if the train driver does not stop the train, then the train is stopped by an external intervention. Hence the external intervention can be seen as a recovery factor, i.e. a mean that recovers the train driver activity by stopping the train.

In the red light procedure with external intervention, the elementary tasks are the following:

- to see the red aspect of the signal: elementary task noted A,
- to interpret the red aspect of the signal: elementary task noted B,
- to action the button to stop the train: elementary task noted C,
- to stop the train (external intervention) if the train driver does not see the red aspect of the signal or does not interpret it: elementary task noted D.

The corresponding THERP tree is the following one (see Figure 12):

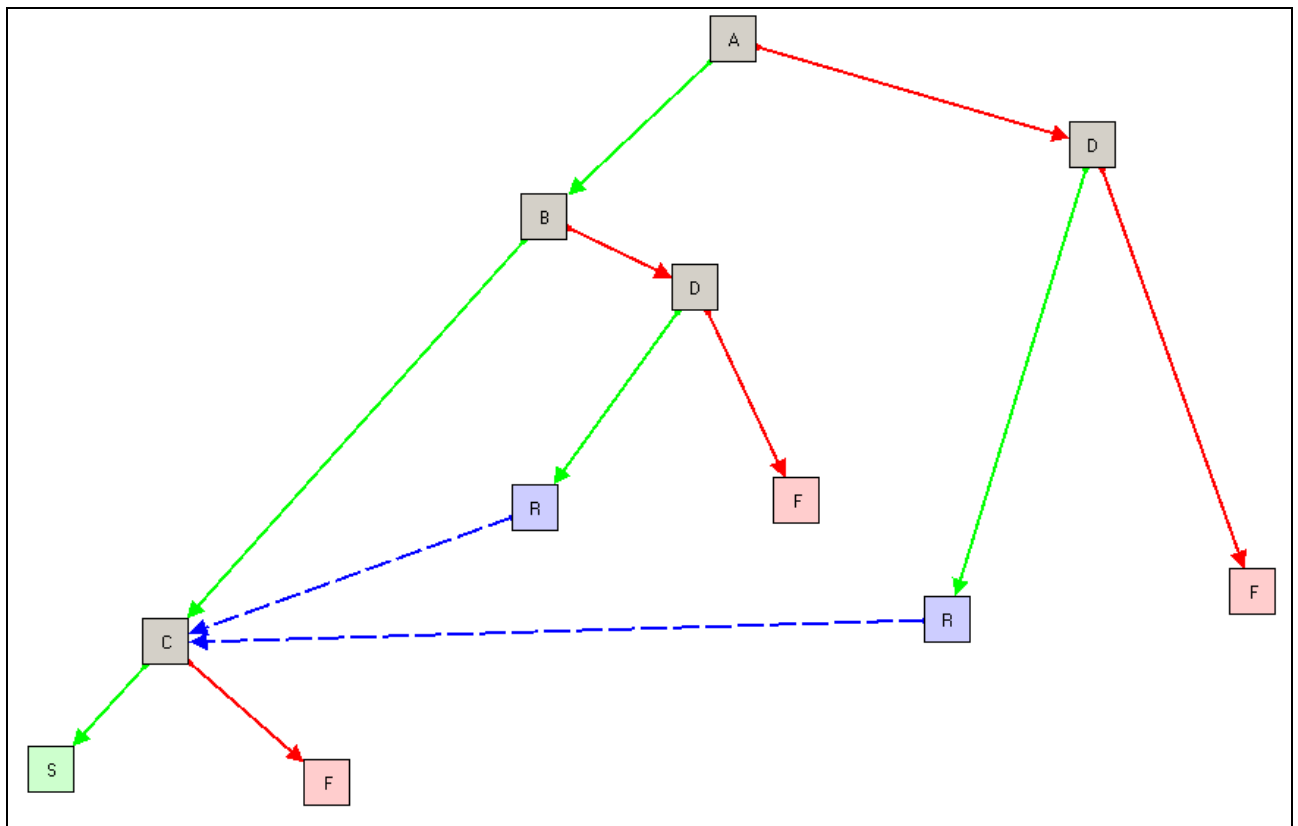


Figure 12 – The red light procedure with external intervention: THERP tree

The evaluation of the probabilities of failure of the elementary tasks and the calculation of the final probability performed with the THERP Tool are illustrated in the following figure (see Figure 13):

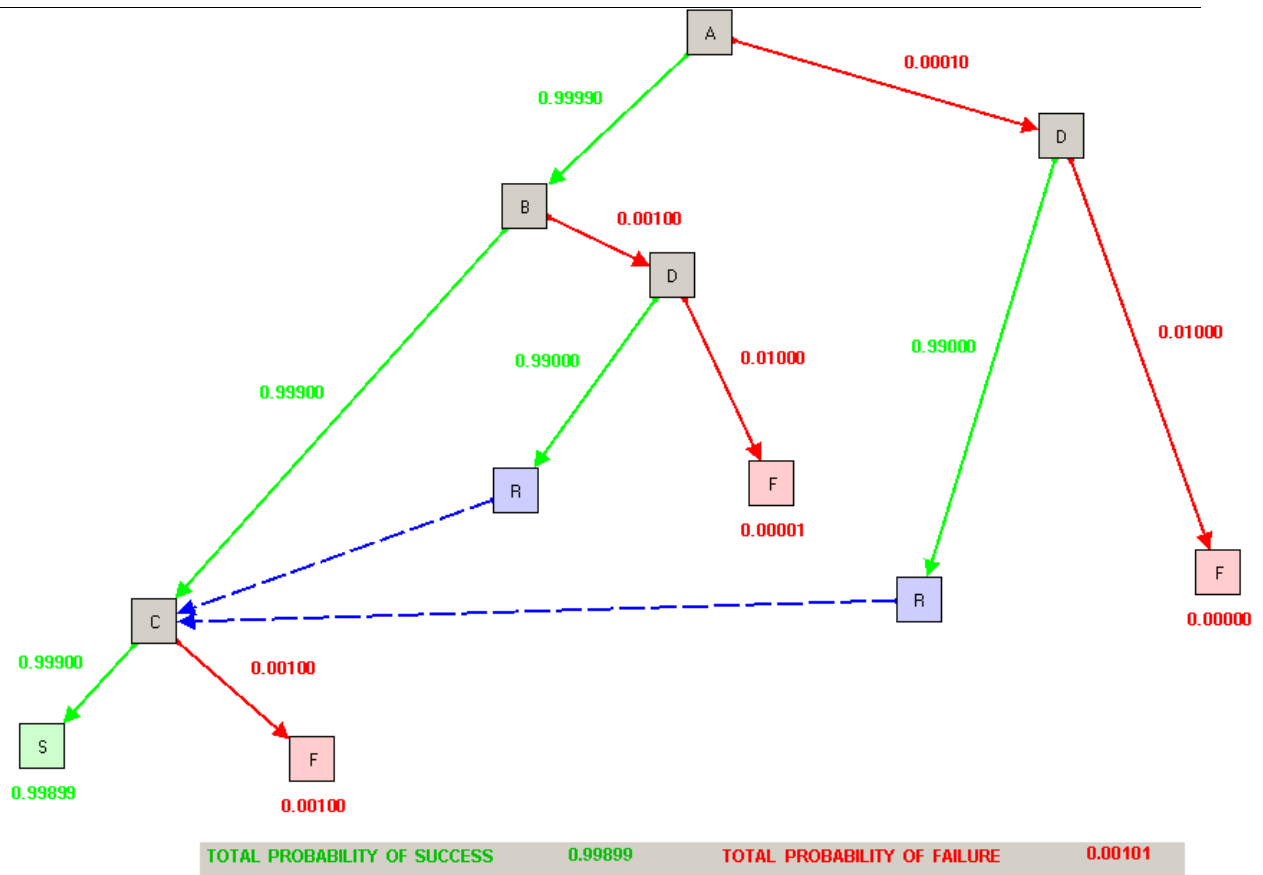


Figure 13 – The red light procedure with external intervention: THERP Tool results

As it can be seen from the Figure 13, the probabilities of success and failure calculated by the THERP Tool for this train driver procedure are:

$$p(S) = 0.99899 \quad \text{and} \quad p(F) = 0.00101$$

Now that the THERP technique and some examples to explain its use have been presented, it is possible to reconsider the aim of this report which is the evaluation of human errors probabilities in the urban guided transport systems for both normal and degraded mode of functioning with or without barrier removals.

6 Examples of the probability of failure of barrier removals

Now that we have presented the THERP process, we can apply it to evaluate human error probabilities to an urban guided transport procedure: the manual train driving. But, before specifying this procedure, we would like to take an idea on human factor impact in rail guided system safety and introduce the studied urban guided train driving context.

6.1 The example of an Express Regional Network: RER A (France)

The nature of observed risked events in the urban guided train context may be classified to six classes (see Figure 14). There are many risked event related to the human factors such as incidents of exploitation. These incidents may be caused by the drivers and related to the non respect of the operating rules, the stop points or the non respect of the rules of the train driving (see Figure 15 and Figure 16).

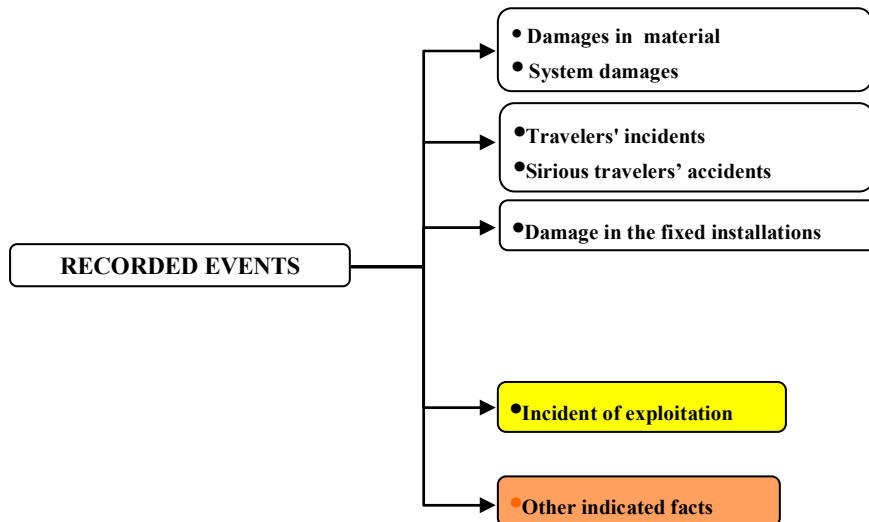


Figure 14 - Nature of the risked events

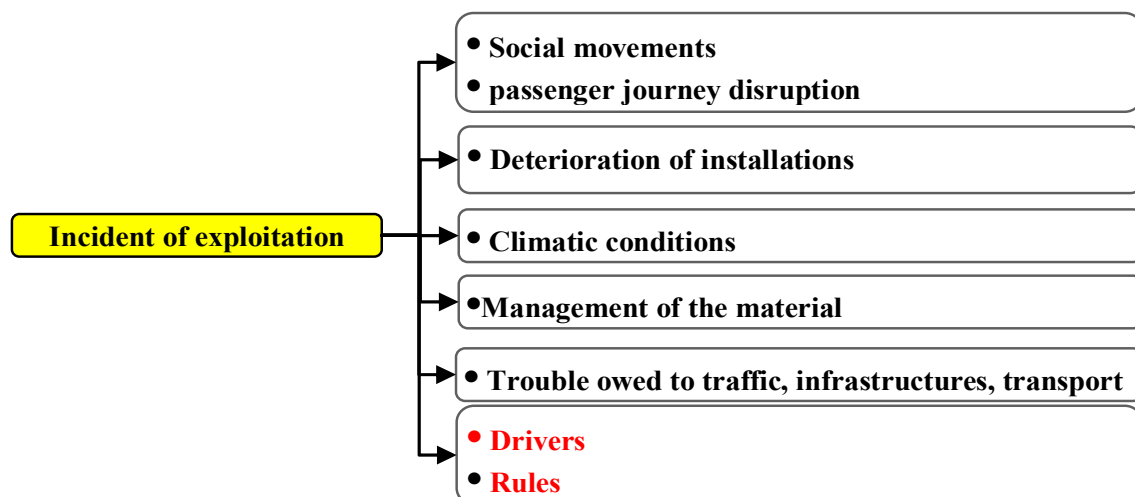


Figure 15 - Events at risk connected to the human factors

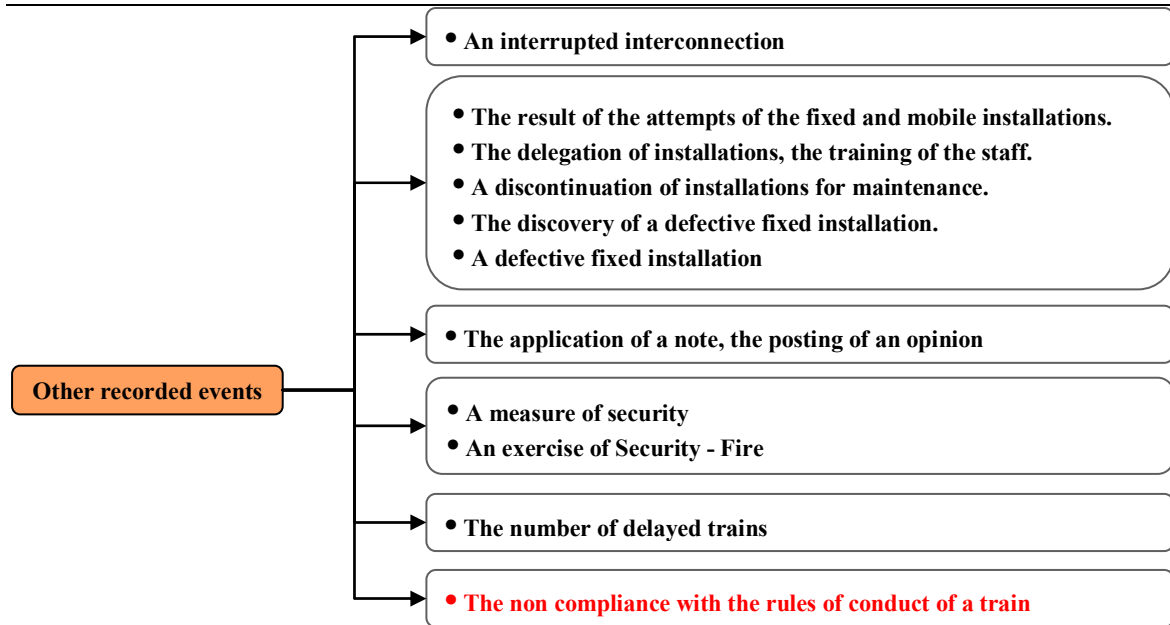






Figure 16 - Events at risk connected to the human factors

These driving rules are related to the aspects (red, yellow, green) of the signals or speed limit signs. The respect of these signals is very important to ensure the infrastructure, the train and the passenger's safety. In automatic driving mode, these signals are always respected. But in degraded mode (manual or semi-automatic mode) application of the train driving rules and the respect of these signals may be allocated to the train driver (see Figure 17). The disregard of the signals by the train driver may be non-intentional or intentional human error.

	Board speedometer (TIV) : indicates to the train which speed it will have to observe from the next board Z.
	Board Z : indicates the beginning of the speed zone.
	Board R : indicates the end of the speed zone and the resumption of the speed references of the line.
	Pancarte G : indicates the beginning of a zone of garage.

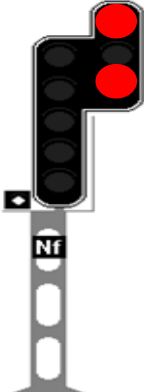


Figure 17 - Some signs involved in the degraded train driving procedure

We present in the following subclauses a detailed study and assessment of the non-intentional and intentional human error probability in degraded mode.

6.2 The task driver

Before studying the driver task it is important to notice that this subclause presents only an example. This procedure is interesting to assess probability in residual scenario (for a solicitation) and not to cover all the operating delay. In fact, this procedure depends on the number of solicitations, including continue controls.

The prescribed tasks to be followed by a train driver are identified as shown on Figure 18.

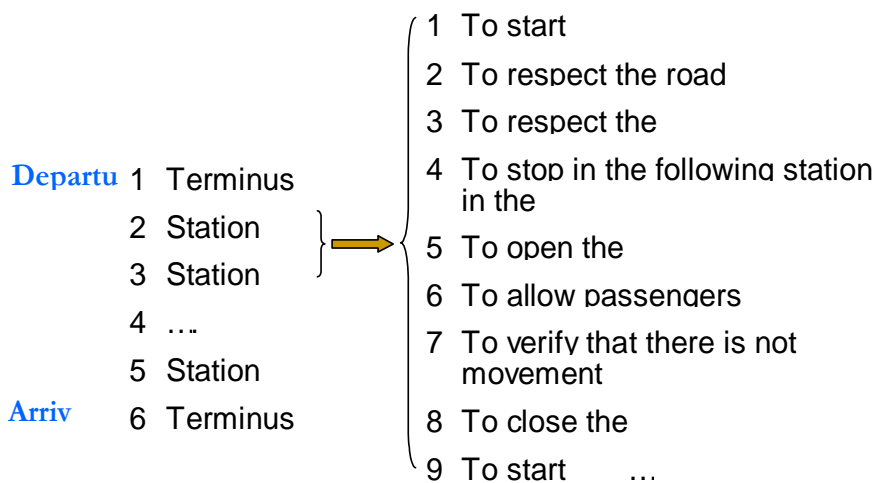


Figure 18 - Human task analysis example

Figure 19 is a possible associated THERP event tree, including possible recovery processes at each level of human activities.

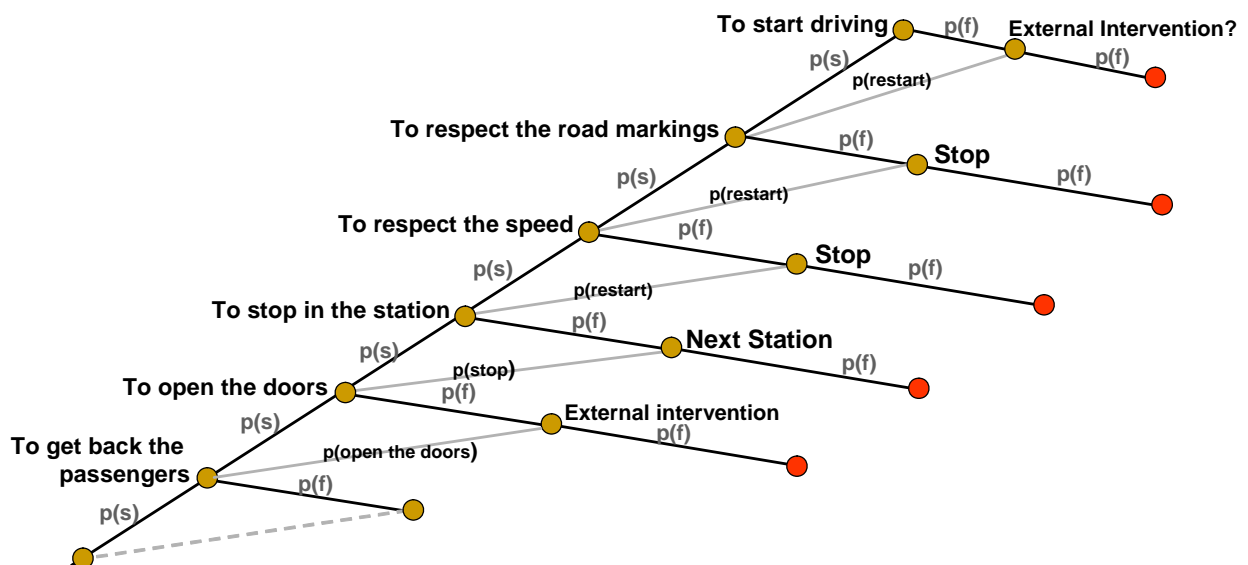


Figure 19 - Example of THERP event tree

In order to assess non-intentional and intentional human error in a degraded train driving procedure at a shunt point, we studied two procedures applied in LUL (London) and RATP (Paris). These procedures detail the role of the train driver when he has to drive the train in a degraded mode. These procedures present some common points. In fact, in both, the driver has to:

- wait for the permission or authority to drive the train,
- drive the train in restricted manual, ready to stop short of any obstruction,
- respect a given speed limit
- continuously drive until the next spacing signal or the end of an opened station.

Between these elementary tasks we will study specially the probability of failure when performing the prescribed procedure and when performing the degraded one. The procedure concerns the respect of speed limit. This study will be done first considering that this disregard is non-intentional then it will be studied as an intentional act.

6.3 Probability assessment without and with barrier removal

This subclause reports a result developed in (Chaali-Djelassi et al., 2007).

The studied example is related to the respect of the speed limit and its three corresponding barriers: the Speed signal (80), the Zone signal (Z) and, if necessary, the sound signal.

According to THERP, it is necessary to define the elementary driving tasks and evaluate their elementary success and failure probabilities. Then the THERP Tool calculates the success and failure probability of the whole driving activity (i.e., $p(S)$ and $p(F)$) in normal and degraded modes.

The elementary tasks of the train driver activity when he respects or not the barriers can be represented by the same tree. The only difference between these two procedures is the probability assigned to each specific elementary task.

The elementary tasks of the speed procedures are:

- Speed signal (80) perception: elementary task noted A,
- Speed signal (80) interpretation: elementary task noted B,
- button action (slowing down): elementary task noted C,
- Sound perception if the speed is not respected: elementary task noted D,
- Sound interpretation: elementary task noted E,
- Zone signal (Z) perception: elementary task noted G,
- Zone signal (Z) interpretation: elementary task noted H.

In the normal mode, the train driver respects all these proposed barriers. In this case the probability assessment of failure and success is given in Figure 20.

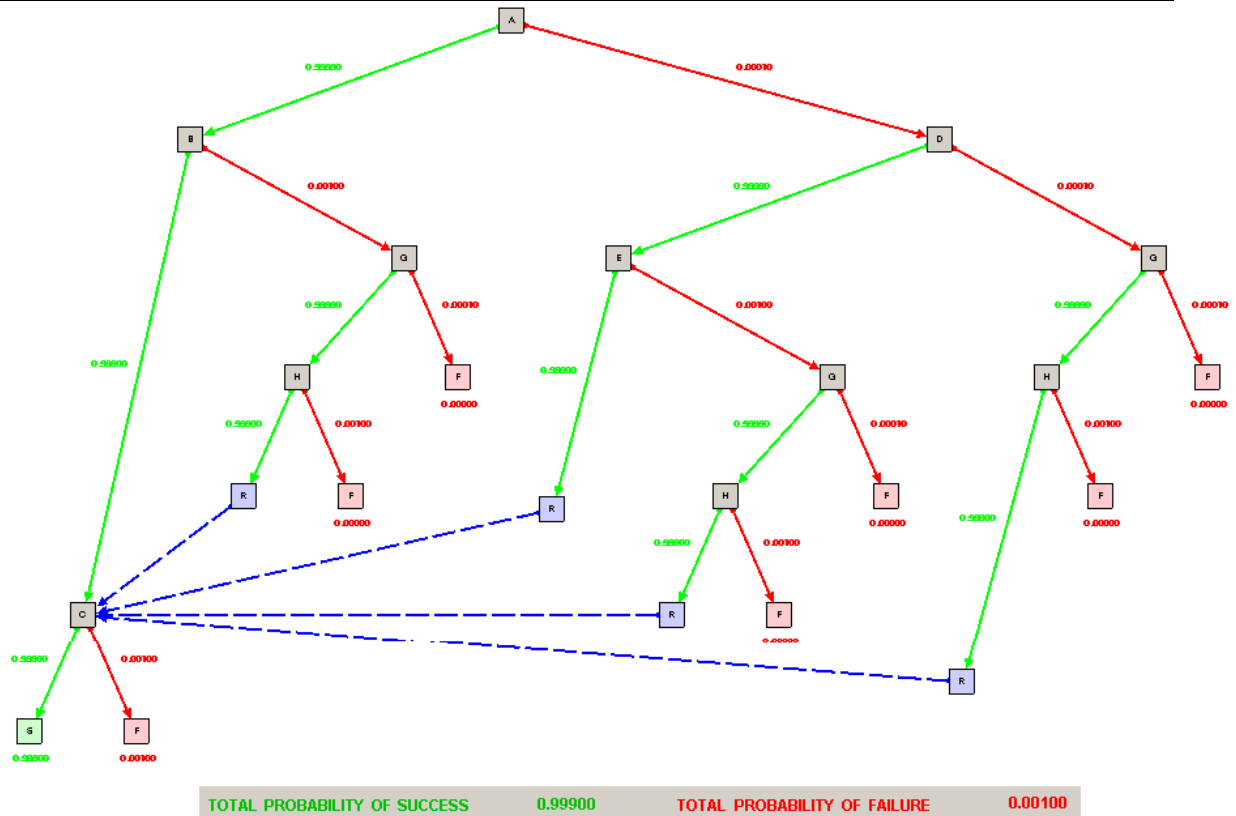


Figure 20 – The speed procedure in normal mode: THERP Tool results

On the other hand, a possible degraded mode for speed limit can be that only one barrier is respected (the zone signal) and the other two barriers (the speed signal and the sound signal) are not respected.

In this case, the assessment of probabilities of failure and success when performing the deviate procedure with barrier removals is given in Figure 21.

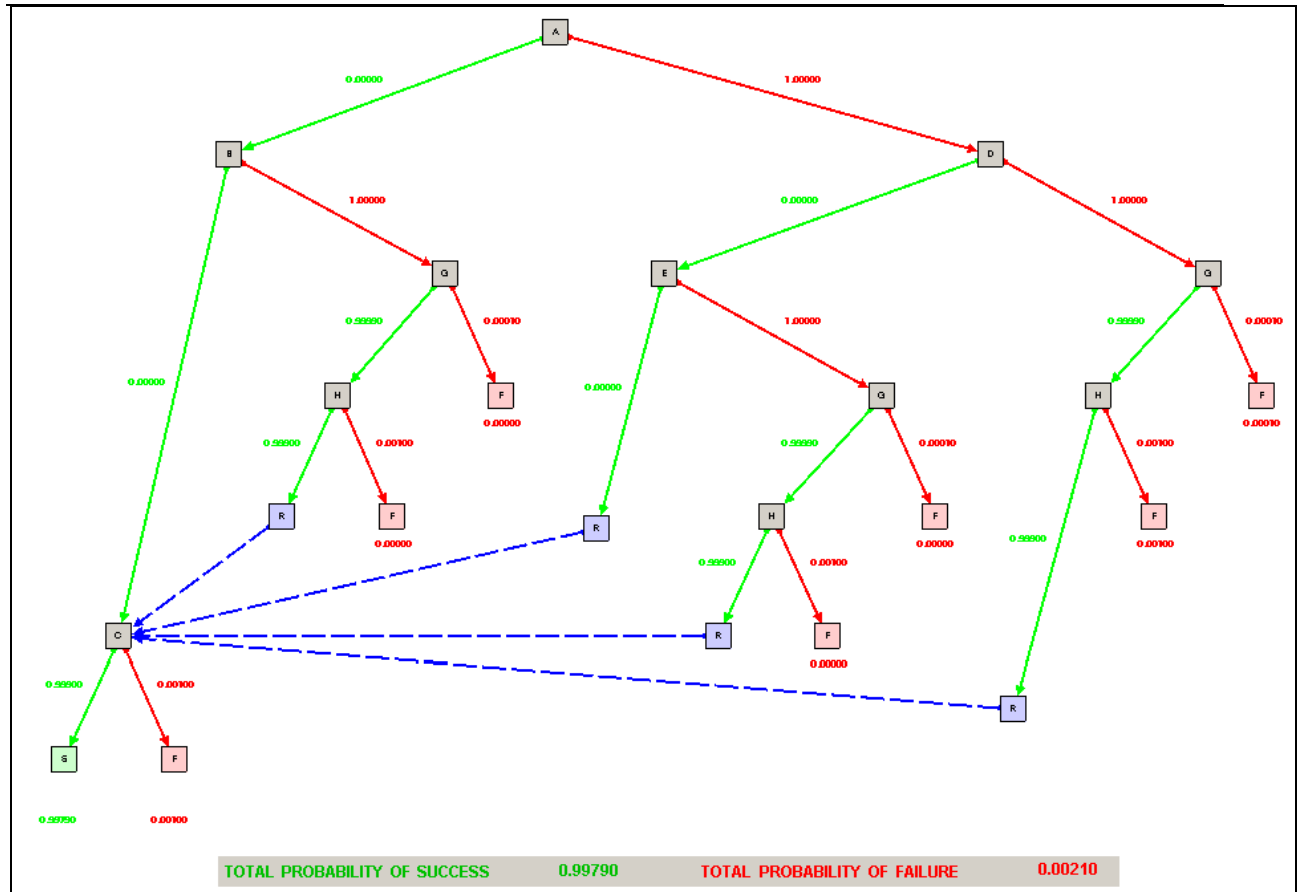


Figure 21 – The speed procedure in degraded mode: THERP Tool results

As it can be seen from the Figure 20, the probabilities of success and failure calculated by the THERP Tool for the speed procedure in normal mode are:

$$p(S) = 0.99900 \quad \text{and} \quad p(F) = 0.00100$$

As it can be seen from the Figure 21, the probabilities of success and failure calculated by the THERP Tool for the speed procedure in degraded mode are:

$$p(S) = 0.99790 \quad \text{and} \quad p(F) = 0.00210$$

6.4 THERP use in transport domain

The probabilities utilized in the THERP trees contained in this Deliverable have been obtained from the Handbook associated to the Technique for Human Error Rate Prediction (Swain and Guttman, 1983). These probabilities are the result of fields observations and experiments carried out by the authors of the Handbook in the domain of Nuclear Energy production.

There are three aspects that must be highlighted with respect to these probabilities values:

- 1) They are basic probabilities, i.e. probabilities for which the influences of factors, other tasks and events have not been considered.
- 2) They are very old and they reflect a technology and design of control systems and human interfaces that is nowadays abandoned. Consequently, a more up-to-date set of data should be identified and applied in order to resolve this issue. These data should be found in specific areas of rail transport.
- 3) In addition to the adequacy of the “age” of data, the domains of application, i.e., nuclear and transport, are rather different, both in terms of technology of control systems and complexity of tasks to be carried out by operators. As an example, the delays and response time of safety critical processes are very different between nuclear and rail systems. Moreover, the amount and typology of automatic control are also very different, with commonalities related mainly to some aspects of autonomous safeguarding and protection systems. Therefore, in order to resolve this issue, a more dedicated set of data should be developed for the domain of urban guided transport.

As consequence of the above discussion, it is essential to consider the results obtained in this Deliverable as propedeutical to the application of a methodology for risk assessment of human aspects, rather than a practical and realistic application of a safety study associated to a specific problem in the domain.

7 Perspectives for an integrated approach for human-machine system safety design

In this report we have:

- described how the human error consequences can be evaluated with the Benefit Cost Deficit (BCD) model;
- described how the human error probabilities can be assessed by using the Technique of Human Error Rate Prediction (THERP),
- evaluated the probabilities of the success or failure of the achievement of some manual driving procedures.

At this level of the report we have shown that it is possible to evaluate the consequences and the probabilities of the human errors and thus we can propose a new risk analysis approach that integrates the human errors into the design process of an urban guided transport system. This approach is based on the prediction of these human errors combining the Benefit Cost and potential Deficit (BCD) model and the THERP model.

The evaluation of the consequences in terms of benefits, costs and potential deficits and the probability of the failure or success of a human error allows us to evaluate the associated risk on one hand and on the other hand allow us to predict the future human operator action. The prediction of the human error is obtained by the evaluation of the utility of the human error.

7.1 The barrier removal expected utility

Barrier removal decision-making is the simplest form of decision-making (see Figure 22). In fact, it involves a choice between two possible actions: barrier removal (BR) and barrier respect (NBR). The barrier removal decision depends on:

- the Benefits and the Costs if the barrier removal is successful. These Benefits and Costs are multiplied by the probability of success of the barrier removal,
- the potential Deficits if the barrier removal fails. These potential Deficits are multiplied by the probability of failure of the barrier removal.

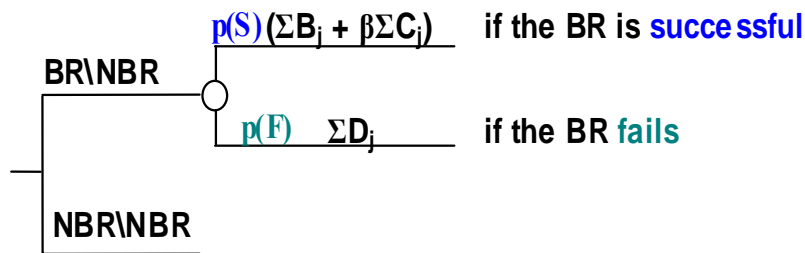


Figure 22 - The BR decision-making process

Where:

- BR\NBR is the BR referred to the barrier respect,
- NBR\NBR is the barrier respect referred to the barrier respect,
- p(S) and p(F) are respectively the probabilities of success and failure of the barrier removal.

This decision making process allows us to translate the barrier removal utility $u(\text{BR}\backslash\text{NBR})$ in the following model:

$$u(\text{BR}\backslash\text{NBR}) = p(S) [\sum B_j + \sum C_j] + p(F) [\sum D_j]$$

7.2 Simple illustration

Let's see again the last example in which the train driver has to respect the train speed limit. In this example (and in order to give a very simple example) we can consider that the train driver takes into account two criteria while he is faced with a the red signal. The two criteria are the train security and the time.

7.2.1 Hypothesis:

For this simple example, we suppose that:

- the train driver has to respect a giving timing,
- he is late comparing to his timing,
- the train driver is trying to win time by not stopping the train at the red signal but only by slowing down.

7.2.2 The train driver error consequences evaluation with the BCD model

For instance, suppose that a given non-compliant action related to speed limit procedure leads to these benefits, costs and potential deficits:

- the Benefits in time are about 7* (i.e., $\sum B_j = 7$)
- the Costs in security are about 1* (i.e., $\sum C_j = -1$)
- there is no potential Deficit if he only slows down the train (i.e., $\sum D_j = 0$).

7.2.3 The train driver error probability evaluation with THERP

After the evaluation of the consequences of the train driver errors, we can add the probability of failure of this driver procedure based on the THERP and the previous example. The probability of failure of the speed control procedure is then equal to 0,04993.

7.2.4 The train driver error utility evaluation

The evaluation of the utility of the disregard of the red signal $u(BR \setminus NBR)$ might be the following :

$$u(BR \setminus NBR) = p(S) [\sum B_j + \sum C_j] + p(F) [\sum D_j]$$

$$u(BR \setminus NBR) = p(S) [7 + (-1)] + p(F) [0]$$

$$u(BR \setminus NBR) = 6 \times 0,95007 = 5,70.$$

This utility value will be used to illustrate the human error and/or the barrier removal prediction method.

* Suppose that, in this simple case, the evaluation may be based for example on a ten-unit scale and given subjectively by expert judgements – The BCD parameters may also be determined by objective indicators to be defined (e.g. response time of the driver, number of movements of the driver, number of physical actions by the drivers, complexity level of the tasks of the driver, etc.)

7.3 The barrier removal expected utility based prediction method

This new prediction method is based on a major hypothesis. In fact because, on one hand, the prescribed task is the barrier respect, then its utility is equal to a given initial value $u(NBR \setminus NBR)$:

$$u(NBR \setminus NBR) = \text{initial value or interval of initial value}$$

On a second hand, between two actions, the one with the higher utility level will be the selected action. This means that if several alternatives are possible, the alternative with the bigger utility level might be chosen.

For example:

- if the utility of the respect of the red signal is considered as nul ($u(NBR \setminus NBR) = 0$),
- if the utility of the non respect of the red signal is equal to 5,70 ,
- if the previous hypothesis is used,
- as the utility of the respect of the red signal in the previous example is lower than the utility of the non respect of the same signal, according to the previous subclause (see subclause 7.2.4),

then we may consider that this driver may not respect the red signal.

This prediction method was applied to simple driving task context. It did not integrate the assessment of probabilities of failure of barrier removals, but it gave acceptable prediction results (Chaali-Djelassi et al, 2006).

This is a very simple way to present the human error prediction method. It does not integrate the totality of the criteria that can be taken into account by the human operators while they are driving a train. It does not integrate also the weights associated to the Benefits, Costs and potential Deficits according to the human operator's characteristics.

8 Conclusion

This report entitled 'Risk assessment based on human factors' tried to help the design or operational levels to integrate human factors into the safety analysis process of the urban guided transport systems. In fact, the aim of this report was to present a methodology that evaluates the probabilities of human errors in urban train driving procedure using the Technique for Human Error Rate Prediction (THERP). It illustrated the probabilities evaluation with some examples related to guided urban train driving procedures. The consequences are evaluated by the Benefit Cost Deficit (BCD) model. Of course the process of safety demonstration has to include a phase to analyse the procedures and the effect of the errors in their application.

The issue of this report is the proposition of the integration of the human errors in the Human-Machine Systems risk analysis. The evaluation of the risk related to the human components can be ensured by the evaluation of the human error probabilities with Technique for Human Error Rate Prediction (THERP) and the human error consequences using the Benefit Cost potential Deficit (BCD) model (see Figure 23).

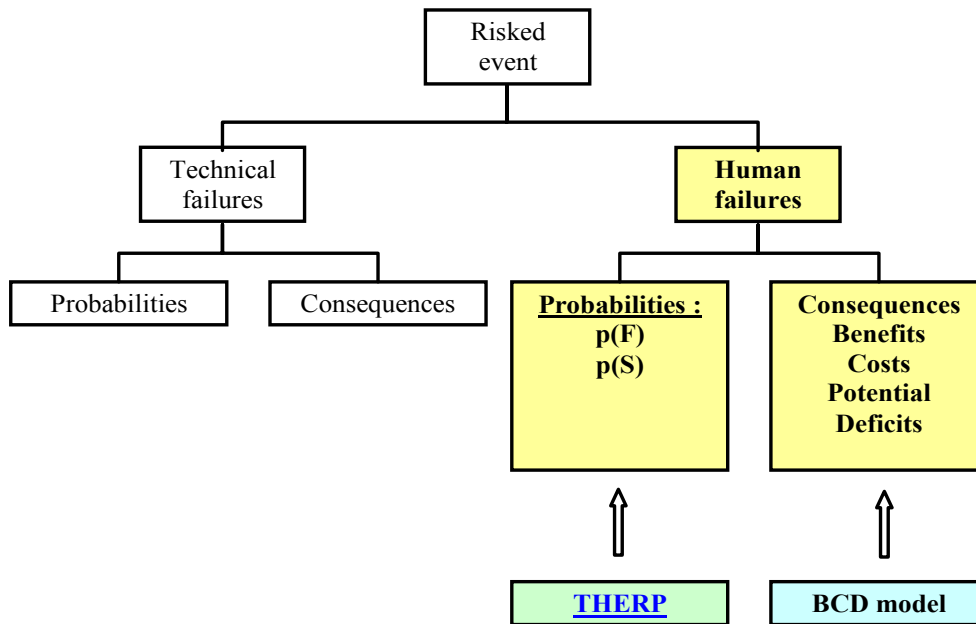


Figure 23 - Risk analysis in Human-Machine System

The integration of the human errors in the risk analysis or safety analysis of a given Human-Machine System can improve its design and its control on operation or maintenance.

Complementary approaches such as THERP and BCD may be integrated in a global human-machine safety assessment logic. It was a long term perspective decided during the workshop on human factors organized by the WP23 in Valenciennes : the SAFE-SADT formalism for example may be an original framework to formalise such human-machine safety analysis applied to urban guided transport system (Vanderhaegen et al., 2007). Future discussions are then required in order to assess the feasibility of this kind of analysis.

The approach developed in this report will be referenced into the deliverable D126 that describes proposals for the safety plan of future urban guided transport systems. Such feasibility study for assessing human error probability or for analysing human erroneous actions might be used for managing a global risk analysis process integrating both technical and human factors. This might concern different system life-cycle steps and might be applied not only for operational tasks such as driving or supervisory tasks but also for maintenance tasks.

9 References

- (Amalberti, 2001). Amalberti, R. The paradoxes of almost totally safe transportation systems, *Safety Science*, Volume 37, Issues 2-3, March 2001. Pages 109-126.
- (Chaali-Djelassi et al, 2006). Chaali-Djelassi A., Polet, P., Vanderhaegen, F. A Method for Predicting Human Behaviour based on the Expected Utility of Barrier Removal and the Iterative learning Control. Application to the Car Driving Task. *IEEE Transactions on Systems, Man, and Cybernetics. Part A Systems and Humans* SMCA06-04-0105. (Revue accepted).
- (Chaali-Djelassi et al, 2007). Chaali-Djelassi, A., Vanderhaegen, F., Cacciabue, P-C. and Cassani, M.. Barrier Removal prediction based on a new approach. Application to a degraded train speed procedure. *EAM* juin 2007. Copenhagen.
- (Polet et al., 2002). Polet, P., Vanderhaegen, F., Wieringa, P. Theory of safety related violation of system barriers. *Cognition Technology & Work*, 4, 171-179.
- (Reason, 1990). Reason, J. *Human Error*. Cambridge University Press, Cambridge, UK.
- (Swain and Guttman, 1983). Swain, A. D. and Guttman, H. E. *Handbook of Reliability Analysis with emphasis on Nuclear Plant Applications*. NUClear REGulatory Commission, NUREG/CR-1278, Washington D.C.
- (Cacciabue, 2004). Cacciabue P-C. *Guide to Applying Human Factors Methods: Human Error and Accident Management in Safety Critical Systems*. Springer. Verlag. London Limited. 2004.
- (Hollnagel, 1998). Hollnagel, E. *Cognitive Reliability and Human Analysis Method CREAM*. Oxford, Elsevier Science Ltd.
- (Hollnagel, 1999). Hollnagel, E. Accident and barriers. 7th European Conference on Cognitive Science Approaches to Process Control, Villeneuve d'Ascq, France, pp. 175-180.
- (Vanderhaegen, 2004). Vanderhaegen, F. The Benefit-Cost-Deficit (BCD) model for human analysis and control. *Proceedings of the 9th IFAC/IFORS/IEA symposium on Analysis, Design, and Evaluation of Human-Machine Systems*, Atlanta, GA, USA, 7-9 September 2004.
- (Vanderhaegen et al., 2006). Vanderhaegen, F., Chaali, A., De Grandis, E., Cacciabue, P.-C. Human factors and system design – Integrated system for “Auditing” safety levels of urban guided systems. Deliverable D87 of MODURBAN.