Consequence analysis of human unreliability during railway traffic control

F. Vanderhaegen & B. Telle

*Laboratoire d’Automatique et de Mécanique Industrielles et Humaines (LAMIH),
University of Valenciennes - URA 1775 CNRS,
Le Mont Houy BP 311 - 59304 Valenciennes Cedex France
Email: {vanderhaegen, telle}@univ-valenciennes.fr

bINRETS-ESTAS (Institut National de Recherche sur les Transports et leur Sécurité - Évaluation des Systèmes de Transport Automatisés et leur Sécurité)
20 rue Elisée Reclus - 59650 Villeneuve d’Ascq, France
INRETS-ESTAS co-finances B. Telle (Ph.D. student)

Abstract

The paper presents a descriptive method to analyse consequences of human unreliability. Unreliability is seen as combining three behavioural factors: acquisition related failure, problem solving related failure, and action related failure. The method is divided into four steps: the functional analyses, the context identification, the task state identification and the consequence analysis of the human unreliability. The functional analysis step aims at determining interactions between the required control process functions and the human tasks. The context identification step lists the required procedures with regard to different work supports and conditions. The task state identification identifies the unreliable tasks which can be due to an acquisition related failure, e.g. data sensor failure, and/or a problem solving related failure, e.g. erroneous processing of information or/and processing of erroneous information, and/or an action related failure, e.g. an unrequired performed action or an omission. Finally, the consequence analysis step identifies catastrophic scenarios due to human behaviour. The whole methodological approach is applied on a practical example: the railway system, and more precisely the railway traffic control system.
1 Introduction

On the one hand, humans contribute to maintain both safety and reliability when controlling systems. On the other hand, they are infallible. Indeed, when process dysfunction appears, safety procedures have to be carried out by human operators. Humans contribute to maintaining the safety level. Nevertheless, even if they are able to prevent, to recover or to manage unsafe situations, they are fallible and can themselves perform unsafe actions. Therefore, knowledge about human dysfunction characteristics is sometimes useful when designing dependable systems. For instance, knowledge of accidents and incidents due to human errors can direct a preventive training programme for human operators.

The consequences of human errors can be considered at different levels. Some of them can damage the process dependability, i.e. the process safety and/or the process productivity. On the paper, the human reliability assessment is assimilated into the identification of the human unreliable parameters which can damage this process safety. Different methods can then be applied. Nevertheless, their use is often limited to design off-line error prevention supports such as training programme, awareness programme, ergonomic improvement and rules modification. The new approach proposed on the paper aims at guiding the design of both off-line and on-line error prevention supports. This approach frees human reliability analysis from a probability based assessment. It is based on a model of unreliability designed to identify unreliable behavioural scenarios when performing tasks.

Firstly, the paper presents the bases of the method to analyse the consequences of human unreliability. Secondly, it applies this method to the railway traffic control system.

2 Consequence analysis of human unreliability

Different methods to assess human error or human reliability and their limits are listed. The new proposed approach aims at evaluating the consequences of the human unreliability with regard to acquisition related failure, problem solving related failure and action related failure.

2.1. Reliability assessment methods

Human reliability is defined as the probability for a human operator (1) to perform correctly required tasks in required conditions and (2) not to perform tasks which may degrade system performance [1]. A human reliability analysis aims at assessing this probability. An human error analysis is the opposite, i.e. it consists of calculating the probability that an
error will occur when performing a task [2]. An error is a deviation related to a reference. Different references can be identified: deviation related to the perception of information [3], deviation related to the perception of work context [4], deviation related to a norm [5], deviation related to the state of a performed action [6, 7], deviation related to on-line risk assessment [8], deviation related to human intention [9], deviation related to performance [10]. Usually, human error analysis is oriented toward safety analysis with regard to the controlled process. Different methods can then be used.

As a matter of fact, different methods to assess human error can be included into the design process. Firstly, machine centred methods can be adapted [11]:

- FMECA (Failure Mode, Effects and Criticality Analysis). This method analyses causes of failures in order to determine consequences for the process. It aims at assessing a criticity of events, i.e. a level of gravity combined with frequency of events.
- Fault Tree. This method analyses consequences of failures in order to determine their causes. It aims at assessing failure occurrence combining logic and probabilities.

Even though those machine centred methods can be adapted for human behaviour assessment, they are difficult to apply because they require data on human behaviour which cannot be tested in the same way as technical components. Other specific methods were built to analyse human reliability or human error. Two main classes can be considered: a quantitative assessment based class and a classification based class:

- Methods from the former class consist of assessing qualitatively the human error occurrence. The calculation of human error rate is based on combining different values estimated by subjective expert judgements and/or by data bank on incidents and accidents analyses and/or prescribed probability tables. As example, the TESEO method (Tecnica Empirica Stima Errori Operatori) [12] gives a probability of error combining five factors: the activity's typologic factor, the temporary stress factors, the operator's typologic factor, the activity's anxiety factor and the activity's ergonomic factor. On the other hand, the THERP method (Technique for Human Error Rate Prediction) [1] evaluates the probability of human error related to a corrective coefficient according the human operator stress level and two probabilities: a probability related to the task characteristics and a probability related to the human error recovery possibility.
- Methods from the latter class aim at classifying the human errors. As example, the classification of the Paired Comparison method [13] consists of classifying tasks from the least risky to the most risky, related to expert judgements. The SHERPA method (Systematic Human Error Reduction and Prediction Approach) [14] is based on a taxonomy of tasks with regard to human behavioural characteristics: skill based behaviour, rule based behaviour distinguishing rule based diagnosis tasks and if-then rule based tasks, and knowledge based behaviour. The CREAM method (Cognitive
Reliability and Error Analysis Method) [7] analyses the human error taking into account a taxonomy of the erroneous action states.

Results which are obtained by different human centred methods often differ one from another [9]. Moreover, some of them require a strong operational data base on human error in order to assess or estimate the probability of human error occurrence. Most industrial applications cannot use those methods because this data base does not exist or is incomplete. Furthermore, rather than use those human centred safety analyses to specify on-line human support tools, they are used to improve off-line error prevention supports such as work environment ergonomics or training. Indeed, despite a good ergonomic design and an excellent training repeat human errors is not taken into account. Therefore, a new approach is proposed in order to consider both off-line and on-line prevention support specification into the global system development during the safety analysis phase.

2.2. Toward a method to analyse consequences of human unreliability

This method analyses consequences of human unreliability and leads to generate a set of design recommendations to increase reliability and safety, taking into account both off-line and on-line error prevention principles. It is divided into four steps, Figure 1:

• Step 1: functional analysis of the system. This step includes different analyses: process analysis, human activity analysis and feedback experience analysis. Those analyses aim at identifying system functions and human tasks. Functions allocated to human operators define the human tasks required by the controlled system. Therefore, the main objective of this step is to identify the matrix which indicates the interactions between human tasks and the system functions. As example, related to the system function F1, F2, F3 and F4, the human operator has to realise the F2 function performing three main human tasks: T1, T2 and T3.

• Step 2: procedural and contextual analysis. It consists in identifying the work contexts and the corresponding human tasks, analysing safety rules and determining human safety procedure related to those contexts. As example, two contexts related to the task T1 have been identified: C1 and C2. For each one, a procedure, i.e. a list of actions, is required.

• Step 3: task feature identification. This step aims at evaluating the possible task state (e.g. correct task, erroneous task) and at analysing causes of unreliability. Those causes of erroneous task are analysed according to possible scenarios of human unreliability which is presented as combining between three behavioural factors [15]: acquisition related failure (i.e. data sensor failure), problem solving related failure (i.e. erroneous processing of information or/and processing of erroneous information), and action related failure (i.e. correct action or erroneous action).
Figure 1. Method to analyse consequences of human unreliability.

- Step 4: consequence analysis. The final step consists of combining human unreliability factors and their consequences on the system. The result is a matrix with the causes of unreliability and the consequences on the system. The more the consequence level is, the more catastrophic the consequence is.

Moreover, the design of such tools related to consequences analysis of human unreliability can be guided by different criteria, e.g. consequence occurrence frequency based criteria, economical based criteria, political based criteria. This method is applying to railway system at the University of Valenciennes by the LAMIH and the INRETS-ESTAS team, taking into account catastrophic consequences of human unreliability. On the one hand, at present, the design process of future railway systems does not integrate criteria and demands related to human factors. Nevertheless, a lot of studies on railways have concluded that human failure is an important cause of accidents [16, 17]. On the other hand, with regard to an operational point of view, even though future railway systems will allocate an important human role for train safety, they have to reinforce this safety role with appropriate on-line support tools.

The method to analyse consequences of human unreliability is then applied for railway traffic control in order to specify error recovery tools.
3. Application to railway traffic control

The railway traffic control domain is a practical example to apply this method to assess the consequences of the human unreliability. This part summarises the steps of the method. The functional analysis and the context identification concern the global railway system. On the other hand, the action step identification related to two configuration contexts and the consequence analysis focuses on the traffic flow management function.

3.1. Functional analysis and contexts of railway system

Structured Analysis Design Technique [18] was used to identify the system functions. In such representation, the main railway system function is to realise a transport mission by means of railway system and competent staff, according to the specification of the demand to transport passengers or goods by train. The inputs of this function are the real needs required by customers and the feedback when missions are realised in order to update the planning of the rail transport services. A mission consists in driving passengers or goods from a departure point to an arrival one. Different sub-functions were then identified taking into account the inputs and the outputs for each one, the data flow between them, and the human integration to realise them. Figure 2 lists some of those sub-functions of the global railway system.

Figure 2. Functions of the railway system.
For each sub-function, the implication of humans can be determined. Figure 3 gives an example of those interactions between traffic flow management functions and some human tasks.

<table>
<thead>
<tr>
<th>Human tasks \ System functions</th>
<th>To prepare traffic flow</th>
<th>To control electrical devices</th>
<th>To shunt</th>
<th>To relieve human operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>To receive a verbal communication</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>To transmit a verbal communication</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>To handle train movement</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>To supervise train during moving</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>To control train arrival</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>To manage routes</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Figure 3. Example of interactions between human tasks and system functions (0: no interaction ; 1: interaction).

The matrix of interactions between human tasks and railway system functions is the matrix related to normal control conditions. The second step of the method aims at identifying different work contexts which may modify the initial human activities.

With regard to contexts, the procedures to be followed to control railway system can differ from the procedures of normal situations. The contexts concern incidents, breakdowns or particular railway configurations which orient the specific operations to be performed.

The incidents can be obstacles on rails, danger or presumption of danger, shock or abnormal movements, wanderings of cattle, problem on level crossing, problem on electrical devices, problems on train during moving. A breakdown can be a problem when realising a route or a problem which makes the establishment of a route or of an authorisation impossible. Different configurations of railway equipments (e.g. of trains, of rails, of shunting equipment) require different tasks to be performed.

3.2. Example of task feature identification and consequence analysis

For instance, two configurations of the shunting equipment can be identified on signal boxes. Indeed, there are unified electromechanical equipments or computerised control relay equipments. The shunting function can be divided into different sub-functions: to control the route establishment, to control movements, to control the occupied route freeing, to control the route protection. For some sub-functions, the human signal box operators have different tasks to perform according to the type of the shunting equipment. With regard to the route establishment control sub-function, an unified electromechanical based shunting equipment implies five main tasks: to take into account information about the route to prepare, to take into account the shunting equipment to be operated, to activate the required shunting devices, to verify their positions and to control signals on rails. On
the other hand, a relay based shunting equipment requires three main tasks: to take into account information about the route to prepare, to control using keyboard the automatic railway route opening and to control signals on rails.

Both contexts imply six tasks A1, A2, A3, A4, A5 and A6, Figure 4. The procedure required by the first configuration context related to the unified electromechanical equipment is: A1xA2xA3xA4xA6. On the other hand, the procedure required by the second configuration context related to the computerised control relay equipment is: A1xA5xA6.

<table>
<thead>
<tr>
<th>Code</th>
<th>Human task</th>
<th>Main human behaviour</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>To take into account information about the routes to prepare</td>
<td>Acquisition</td>
</tr>
<tr>
<td>A2</td>
<td>To take into account the shunting equipment to be operated</td>
<td>Acquisition</td>
</tr>
<tr>
<td>A3</td>
<td>To activate the required shunting devices</td>
<td>Action</td>
</tr>
<tr>
<td>A4</td>
<td>To verify the shunting equipment position</td>
<td>Problem solving</td>
</tr>
<tr>
<td>A5</td>
<td>To control the automatic railway route opening</td>
<td>Problem solving</td>
</tr>
<tr>
<td>A6</td>
<td>To control signals on rails</td>
<td>Problem solving</td>
</tr>
</tbody>
</table>

Figure 4. Task feature identification.

A part of the matrix combining consequences on the controlled system and the human task feature with regard to unreliability factors is proposed on Figure 5. The lower level of consequence is 0 and the higher level of consequence, i.e. the catastrophic level is 3.

<table>
<thead>
<tr>
<th>A1</th>
<th>A2</th>
<th>A3</th>
<th>A4</th>
<th>A5</th>
<th>A6</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 5. Example of task features and consequence analysis (0=correct performed task ; 1=incorrect performed task).

Different scenarios of human unreliability are identified taking into account those equipment configurations. According to the examples given on Figure 5, two scenarios may cause catastrophic consequences on system for
each context. Therefore, this kind of matrix identifies possible human problem sources when controlling traffic flow management. With regard to the first configuration, i.e. with the unified electromechanical equipment, problems may occur when performing the tasks A2, A3 and A4. Problem on A2 is an acquisition related failure, problem on A3 is an action related failure and A4 is a problem solving related failure. With regard to the second configuration, i.e. with the computerised control relay equipment, problem may occur when performing the tasks A1, A5 and A6. Problem on both A5 and A6 is a problem solving related failure and problem on A1 is an acquisition related failure. Failure on A6 may not cause catastrophic consequence because an automatic support usually controls the coherence between the shunting equipment state and the signals on rails. Moreover, a failure on A4 may not cause catastrophic event when A3 is performed correctly.

In order to avoid catastrophic consequences on system, the possible incorrect performed tasks have to be reduced by solving acquisition related failures, problem solving related failures and/or action related failures.

4. Conclusion

The paper has presented the concepts of human error and human reliability with regard to different points of view and assessment methods. A new approach was proposed in order to consider both off-line and on-line prevention of human error during specification phase of a system. It is divided into four main steps and aims at analysing the consequences of the human unreliability on the system safety. Finally, the method was applied for the railway system.

This kind of method is useful to identify the possible system modifications depending on the occurrence of acquisition related failures, problem solving related failure and erroneous actions. Therefore, the last step of the method to analyse the consequences of the human unreliability can guide the specification of some prevention supports such as:

- Ergonomics improvements when acquisition related failure and omission were identified.
- Development of training improvement or awareness programme or course on human resource management when, for instance, erroneous actions were due to problem solving related failures such as non respect of safety procedures.
- On-line error prevention support development to improve data acquisition and/or data processing and/or to filter action.

A simulation of railway traffic control will be developed at the University of Valenciennes in order to study the feasibility of this method use to specify computer based tools to support human error recovery during acquiring data, solving problem and/or performing action.
Computers in Railways

References


