4.1 INTRODUCTION

A non-probabilistic approach, which aims at identifying both tolerance and intolerable sets of human behavioral degradations which may affect the system safety. The corresponding scenarios of degradations are characterized by a behavioral model of unreliability including three main factors: acquisition related factors, problem solving related factors and action related factor.

System development methods are usually studied for two life-cycle steps: a design related step and an operation related step. Those steps take into account the results of Probabilistic Risk Assessment methods to determine acceptable and unacceptable risks and to find solutions in order to eliminate or reduce them. Generally, they are Probabilistic Safety Assessment methods because risk analysis concerns system safety. Nevertheless, those methods to usually not
integrate explicitly the possibility to use both human and machine together to guarantee the system safety. Unfortunately, human-machine interaction may also be the cause of incidents or accidents. Therefore, safety analysis has to focus not only on machine interaction but also on human centered analyses. This chapter focuses on Human Reliability Assessment or Analysis methods which integrate human factors on safety analysis, which may be used as a prospective analysis during the design step or as a retrospective analysis during the operation step of the life-cycle. Both prospective and retrospective analysis may guide the design of tolerant and robust operational systems: a robust system is a system on which human error occurrence is impossible or limited during operations, whereas a tolerant system has operational means to recover from human errors that may occur during operations.

When human errors are interpreted in terms of a degradation function, a given task may cause the degradation function, a given task may cause the degradation of another risk or the degradation of the controlled system state. Degradations are deviations, which have negative consequences for either the human behaviour or the system
state. They usually focus on system safety. Two sets of degradations may occur: the set of tolerable degradations, and the set of intolerable degradations. The notion of severity of a degradation can then be introduced. Even if risk is defined as the combination of the probability of the occurrence of a degraded event and the consequences of this event, the use of probabilistic is often inefficient because of the inter-variability and intra-variability of human behaviour.

Therefore, this chapter considers the occurrence frequency and the consequence of degradations separately, and presents a human centered safety analysis approach based on a non-probabilistic human reliability assessment method. This method is called ACIH, a French acronym for Analysis of Consequences of Human Unreliability. It aims at determining both sets of tolerable and intolerable degradations and at specifying adequate error prevention supports. The ACIII method assesses the severity of scenarios of unreliability whereas the frequency of their occurrence may be one of the criteria to filter the scenarios they have to be taken into account on the specification step. This chapter develops the first aspect of the method, i.e. the assessment of both tolerable and intolerable sets of scenarios, integrating both prospective and retrospective analyses, which are applied to the railway domain.
First, both human reliability and human error concepts are defined and some human reliability analysis methods are discussed.

4.2. **Human centered safety analysis methods**

Human reliability and human error can be defined in terms of causes related to human behavioural degradation and/or of their consequences on the system that is being operated upon. Method to assess them are risk assessment based methods or cognitive model based methods. They assess or analyze risks of human behavioural degradation or system degradation due to human erroneous actions.

4.2.1 **Human reliability and error as a degradation function**

Human reliability and human error concepts can be interpreted in terms of degrees of the degradation of human behaviour. They take into account two aspects: the human behaviour degradation that may cause human behaviour degradations and human erroneous action that may cause degradations of the controlled system state.

Human reliability is defined as the probability for a human operator to perform correctly required task in required conditions, and
not to assume tasks which may degrade the controlled system. A human reliability analysis aims at assessing this probability. A human error analysis is the opposite, i.e. it consists of calculating the probability that an error will occur when performing a task. In other words, on the one hand, human reliability is the probability that there is no human behavioral degradation when controlling a system, and that there is no degradation of the system state due to human actions. On the other hand, human error is human unreliability, and is the probability that a human behavioral degradation occurs when controlling a system or a system degradation occurs because of human erroneous actions. Note that human error may occur without degrading the system state and a system state may be degraded independently of the human error occurrence. A human behaviour, which is intended to correct the consequences of degraded one is a human error recovery. Both recoveries and degradations can be operated whatever the state of the controlled system and its evolution.

System state degradations due to human erroneous actions are consequences of human error which many imply several human degradation factors from perception degradations can then be studied: degradation of the task of perception, degradation of the problem solving capacity, degradation of the performed action. For instance, an
error can be caused by the limited human capacity to perceive information and to remain alert for dynamic process evolution. There is then a degradation of perception of information. Moreover, such a degradation of the perception of a situation can relate to the perception of work context. An error is both context and cognition sensitive. It can be the result of a wrong identification of the operational context which guides the human activities. On the other hand a degradation of problem solving capacity relates to human behavioural factors before performing actions on the controlled system. There are factors such as:

- A degradation related to intention. What humans intend to do or obtain may differ from what they do or obtain may differ from what they do or obtain really.

- A degradation related to on-line risk assessment. Humans take risks while performing their tasks but this risk assessment may be wrong.

- A degradation related to workload assessment. Humans behave differently when they feel over-loaded or under-loaded.
A degradation of action can be related to normative action: an error is a deviation of an actual action from that required by the system. Moreover, such a degradation of performed action can be performed too late or too early, or performed too fast or too slow. Degradation of system state are linked with consequences of human actions regarding performance criteria. As an example, the human operators can act successfully and freely on the process only if they remain inside an area limited by three dimensions: admissible states of the controlled process, available resources to achieve goals and human capacity to perform tasks: a human error occurs outside this area. The admissible system states are usually related to system states are usually related to system safety criterion, i.e. state for which consequences on humans, machines and /or the environment are dangerous.

The explanation of human behaviour degradations relates generally to safety criteria. It determines the human causes of unsafe situations, whereas the explanation of system degradation focuses on evaluation the unsafe consequences of human actions. Different methods can then be used: risk model based methods or cognitive model based methods.
4.2.2 Risk assessment and Cognitive methods

Human reliability assessment or analysis methods aim at predicting human error, human reliability or human performance. They can be applied not only for prospective analysis in order to assess a priori human behavioral degradations or system state degradations, but also for retrospective analyses in offer to determine a posteriori the causes of accidents or incidents.

Two main classes of such methods can be considered to analyze human centered safety: the machine centered methods and the human centered methods. Several machine centered methods can be adapted to assess risks of human behavioural degradation focusing on human causes and/or consequences on system. There are methods such as:

- **FMECA (Failure Mode, Effects and Criticality Analysis).** This method analyzes causes of human errors in order to determine their consequences for the process. It aims at assessing a risk level assimilated to a critically of events, i.e. a level of severity combined with occurrence frequency of events.
Fault Tree. This method analyzes consequences of human errors in order to determine their causes, combining logic and probabilities, related to functional properties of system. It aims at identifying scenarios of human erroneous tasks which can lead to an undesirable event and at assessing a probability of the occurrence of all possible scenarios.

Fig. 1 The ACIH method based on a non-probabilistic human reliability analysis
Even though those machine centered methods can in principle be adapted to include human behavioral characteristics, they are difficult to use because they require probabilistic data on human behavior which cannot be tested in the same way as technical components. Other specific methods were developed to analyze human reliability or human error.

Quantitative human centered methods consist of assessing the occurrence probability of human error. The calculation of human error rate is based on combining different values estimated by subjective expert judgment and/or by data bank on incident and accident analyses and/or prescribed probability tables. As an example, the TESEO method (Tecnica Empirica Stima Errori Operatori) gives a probability of error combining five factors: they type of activity, the time pressure factor, the operator's characteristics, the severity of the situation and the environmental ergonomic factor. On the other hand, the THERP method (Technique for Human Error Rate Prediction) evaluates the probability of human error related to a given task, taking into account a corrective coefficient based on a human operators stress level and two probabilities: a probability related to the human operator task characteristics and a probability related to the human error recovery possibility.
Nevertheless, results which are obtained by different quantitative human centered methods often differ from one another. Moreover, some of them require a strong operational database or knowledge on human error in order to assess or estimate the probability of human error occurrence. Most industrial applications cannot use those methods because this database or knowledge does not exist or is incomplete.

Therefore, other methods should be developed. Methods based on cognitive models have been developed. They aim at explaining the cause and/or the consequences of human errors, using human mental models. They are based on taxonomies of error before evaluating human performance. For instance, the SHERPA methods (Systematic Human Error Reduction and Prediction Approach) classified tasks information processing regarding different human behavioral characteristics, adopted from Rasmussen's model: skill based processing, rule based causal processing, rule based action processing, rule based causal processing. On the other hand, the CREAM method) analyzes human errors taking into account other human behavioral aspects: cognitive functions such as observation, interpretation, planning, or execution, and their relations with cognitive activities such as coordination, or regulation.
Those cognitive model based methods confront the problem of ambiguity of interpretation when categorizing human errors. The more complex a cognitive model is, the more important this ambiguity, and validation. The validation problem increases when those methods are combined with quantitative approaches.

Moreover, the use of such cognitive models or quantitative methods remains static, i.e. those methods do not take into account the possibility to repeat human behavioural degradations. Indeed, rather than use those human centered analyzes to specify on-line supports such as the specification of ergonomic workplaces of training programs.

Therefore, a new non-probabilistic approach is proposed in order, to face the problem of reliability of probability assessment of a human error and to treat human errors using a simplified cognitive model. This approach considers the specification of both off-line and on-line prevention supports in order to reduce or recover errors.

4.3 **Design method based on human unreliability analysis**

This global method is called ACIH, a French acronym for Analysis of Consequences of Human Unreliability. It includes both prospective
and retrospective analyses and aims at determining scenarios of human behaviour degradation. Those scenarios depend on a model on a unreliability based on three main behavioural factors: acquisition, problem solving and action.

4.3.1 **Global methodology to analyze unreliable scenarios**

The ACIH method integrates two steps: The APRECHIH step and the APOSCHIH step. The APRECHIH step focuses on prospective consecutive analyses such as vundtional analysis, procedural and contextual analysis, task analysis and consequence analysis. The APOSCHIH step uses retrospective analyses such as activity analysis, incident analysis or accident analysis. Both APRECHIH and APOSCHIH steps are cognitive model based approaches to analyze consequences by determining the causes of human behavioral degradation or system degradation, Fig. 1.

The cognitive model used by the ACIH method is a simplified model that facilitates the classification of human tasks. It is based on three human behavioral degradation factors: acquisition related factors, problem solving related factors and action related factors on the controlled process. The APRECHIH's step aims at focusing on the main
sensitive human factors regarding an a priori analysis of possible unreliable scenarios. The APOSCHIH's step is a complementary step based on an operation feedback analysis that aims at explaining the main sensitive human factors regarding an a posteriori analysis of past scenarios.

The functional analysis aims at identifying the set F of functions, noted \( F = \{F_1, F_2, \ldots, F_j\} \) which includes the system functions allocated to human operators are operational procedures defined regarding the controlled process requirement. A procedure is a list of tasks to be performed when predefined functioning conditions are occurring.

The procedural and contextual analysis is then a complementary step. It consists of identifying the set P of human procedures given a function \( F_j \), noted \( \mathcal{P}(F_j) = \{P_1, P_2, \ldots, P_l\} \) for particular process functioning. This is the identification of the set of work contexts, noted \( C = \{C_1, C_2, \ldots, C_k\} \). The final objective of the procedural and contextual analysis is to determine the list of tasks \( T \) for each procedure \( P_i \) of a given function \( F_j \) for a given context \( C_k \). This list is noted \( T(P_i F_j C_k) = \{T_1, T_2, \ldots, T_n\} \).
The task analysis identifies the possible state S/T_p and the type E/T_p of each T_p. The set of the possible task states S is the list of possible degradation degrees, noted S={d_1, d_2,.....d_m} and the set of possible task types E is composed by the three behavioural factors of unreliability, noted E={acquisition, problem solving, action}. The type of a given task is unique whereas this task may have several possible states. The task analysis aims at determining possible causes of human unreliability which is presented as scenarios combining three behavioral factors: acquisition related degradation, problem solving related degradation and action related degradation.

Finally, the consequence analysis consists of assessing the consequences of degraded procedures on system safety, taking into account possible impact of a given degraded procedure on other procedures. Procedures are then analyzed regarding the scenarios of unreliability with their consequences on the system safety. Three classes of consequence are identified: the first class includes scenarios which have no consequence, the second class is composed by scenarios which are problematic but not catastrophic and the third class integrates possible catastrophic scenarios. This third class represents the set of intolerable human behavior degradations whereas the other classes gather the set of tolerable human behavior degradations.
The list of scenarios of unreliability can be increased by the results of an activity analysis. Those analyses are made with the same scheme of the consequence analysis in order to identify the affected functions and the observed propagation of the human behavioural degradations. An activity analysis focuses on the study of the three classes of scenarios that have occurred in the field, an incident analysis focuses on the study of the second class of scenarios, and an accident analysis focuses on the study of the third class of scenarios.

The ACIH method may guide the specification of prevention support tools to eliminate some scenarios of unreliability from the second and the third classes of unreliability from the second and the third class of consequences, or to reduce the possible occurrence of those scenarios. The specification step will then provide human operators with off-line error prevention supports and/or with on-line error prevention supports because despite a good ergonomic design and an excellent training, the possibility to repeat human errors has to take into account. Therefore, the specification of human error prevention supports aim at designing both robust and tolerant system. Prevention supports have to focus on acquisition, on problem solving and/or, on action, depending on the main factors which are sensitive to the possible occurrence of identified scenarios of unreliability.
**Fig. 2 Model of human unreliability**
4.3.2 **Principles of the model for unreliable behaviour**

Both steps of the ACIH method aims at determining human behavioral degradations determining propagation mechanisms of human error with regard to three behavioral factors: acquisition, problem solving and action, Fig. 2:

- **Acquisition related degradation.** This is often first cause of reduced reliability, because it generates an erroneous perception of the controlled error or dazzle and provoke a lack of information.

- **Problem solving related degradation.** This is a degradation of information processing related to the elaboration of an action plan and concerns both erroneous processing of information and processing of erroneous information. For example, because of lack of attention, the perceived information might not correspond to the real state of the process. In such a way, it is possible to generate an unsafe situation by performing an unrequired action plan according to the real state of the process.
- **Action related degradation.** One must distinguish the execution of an action and its consequences for the process. With regard to humans who perform an action, this action is correct when it corresponds to a required action according to this information (i.e. wrong or correct with regard to the system state), otherwise the action is erroneous. Nevertheless, considering the consequences of an action, a criterion is needed to describe an action as correct or erroneous. Indeed, related to process, an action can be unsafe while human operator who performs it believes that it is correct.

Before acting on the process, human operators may perform several cycles of acquisition related degradation, problem solving related degradation and action related degradation and interact with other human operators and technical tools. Therefore, some relations between components of unreliability can be identified.

The three components of the model can be linked. For instance, the consequence of an acquisition related degradation an erroneous action; an unrequired action can be caused by problem solving related degradation; while an erroneous action can generate an acquisition related degradation.
Several intra-relations can then be distinguished.

- A degradation can generate a degradation of the same kind.
- A degradation can generate another kind of degradation.
- A degradation can generate an omission.
- A degradation can generate serial degradation.
- A degradation can generate parallel degradations.

Feedback

Specification of the demand for rail transport

Needs for rail transport -> Realized mission

Railway Staff
Material

Fig. 3. The main function of railway system

4.4. **Application to railway system**

The method to analyze consequences of human unreliability is applied for a whole railway company. The APPRECIH's analyses are results of a feasibility study made at the University of Valenciennes by the LAMIH and the INRETS (french acronym for National Institute of

4.4.1 **Functional analysis of railway system**

Structured Analysis Design Technique [27] was used to identified the set F of the system functions. In such a representation, the main railway system function is to realize a transport mission by means of a railway material and competent staff, according to the regulation and the demands by passengers or freight companies, Fig. 3.

![Fig. 4 Functional decomposition of railway system](image-url)
The inputs of this function are the real needs required by customers and the feedback when missions are realized. This information can be used to update and optimize the rail transport services. A mission consists of driving passengers of goods from a departure to an arrival point. Different sub-functions can then be identified taking into account the inputs and the outputs for each one, the data flow between them, and the human integration to realize them.

The main railway function can be divided into four interactive functions which evolve from organizational functions to assume the railway system functioning to operational functions to realize movements on rails, Fig. 4. Each function can be divided into other interactive functions. The final set F of functions contains then the main function and its corresponding sub-functions: \( F = \{ F_1, F_{1.1}, F_{1.1.1}, F_{1.1.2}, \ldots, F_{1.2}, F_{1.2.2}, \ldots, F_{1.3}, F_{1.3.1}, F_{1.3.2}, \ldots, F_{1.4}, F_{1.4.1}, F_{1.4.2}, \ldots \} \)

The general functioning organization level (\( F_{1.1} \)) requires development and research services to improve the functioning (\( F_{1.1.1} \)), a management service of human resources to perform if (\( F_{1.1.2} \)), a rule management service (\( F_{1.1.3} \)) and a safety management service to maintain safety during functioning (\( F_{1.1.4} \)). The development and research function aims at organizing the three other functions.
Table – 1

Example of propagation

<table>
<thead>
<tr>
<th>Accident number</th>
<th>Affected Function</th>
<th>Affected Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 1</td>
<td>1.4 (to realized movement on fled)</td>
<td>1.4.2.2. (To pilot)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.4.2.3. (To stop)</td>
</tr>
<tr>
<td>Case 2</td>
<td>1.3 (To manage traffic flow)</td>
<td>1.3.1. (To control flow)</td>
</tr>
<tr>
<td>Case 3</td>
<td>1.3 (To manage traffic flow)</td>
<td>1.3.4.1. (to transfer date)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.3.1. (To control flow)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.3.3. (To shunt)</td>
</tr>
<tr>
<td></td>
<td>1.4 (to realized movement on fled)</td>
<td>1.4.2.1. (To check)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.4.2.2. (To pilot)</td>
</tr>
</tbody>
</table>

Three accidents are presented in term of acquisition related degradation, problem solving related degradation and action related degradation. The first example concerns driving errors on movement on field, the second is errors at the traffic flow management level, and the last one focuses on errors on both realization of movement on field and management of the traffic flow. Explanations related a part of the context of those accidents, which are collisions between trains. The analysis of human activity focuses on the main human factors that caused accidents. Results are a list of human factors that caused accidents, which are collisions between trains. The analysis of human activity focuses on the main human factors that caused accidents. Results are a list of human factors that caused accidents. Results are a list of human unreliable scenarios without
taking into account unreliability of machines. Table–1 relates the affected function and activities of the three accidents. The number of the accident and the failed activity of Table–5 are referenced on the following explanations.

The first case relates an accident 2004 January 11th Western India, 105 Miles South of Mumbai, the very cold weather caused shunting point to freeze, and resulted in trains closing up on each other. There were automatic signaling and blocking system in most of the sections, but in one section there were older signal and switching system which in the event of a blocked line or another dysfunction, required the drivers to phone the signal boxes ahead. Unfortunately, on this day the phone system failed, the rules required drivers to stop if the signals were at red and to proceed slowly if the were at yellow. A train stopped at a red signal after dark in the evening, but in the phones were not working the driver decided (case 1, activity 1) proceed slowly to the next signal (case 1, activity 1) despite knowing the rules. In fact, there was a Second train ahead. As the first train approached it, the next signal went to yellow, allowing the first train to proceed, but the signal light was so bright that the driver did not see the trail light of the second train (case 1 activity 3) and ran into it as about 25-30 km/h. The driver was under the impression the he was running at only about 5 km/h (case 1, activity 4).
The Second accident is another collisions which occurred on 23\textsuperscript{th} June, 2003, Near Sindhudrug, Maharashtra India. The main cause of this human rail operators from two different stations. Regarding the configuration of the single-track line, trains which follow opposite direction have to use a specific crossing area. The first operator informed the second one that a train was arriving without communication the number of the train (case 2, activity 1) and without making acknowledgement of the message (case 2, activity 2). The second operator put a train on the crossing area in order to wait the running of the announced train, saw on the mission scheduling which train is supposed to arrive but he focused his attention on a wrong train (case 2, activity 3). As the train he was waiting did not arrive, taking into account remarks from the driver of the train which was at the crossing area, he verified his mission scheduling, saw he has made an error and selected another wrong train which crosses the waited train at another crossing area (case 2, activity 4). Therefore, he called his colleague to announce him that the train on his crossing area will arrive, without making acknowledgement and refusal of authorization to run (case 2, activity 5).
The third accident is a collision which occurred on 1st June, 2003 Near Buxar, Danapur Division, India. During shift handover, the outgoing. Yard master transferred the information to the incoming and all information was transferred only verbally (case 3, activity 1). Therefore, the second yard master did not develop an adequate situation awareness (case 3, activity 2) and allowed two trains to employ the same track in opposite directions (case 3, activity 3), without realizing that in this way a conflicting situation would arise. Because of the permission given sure that there was no other train on the track. Therefore, they operated at a speed that prevented them from stopping the train before crashing, whereas rules impose them to regulate their speed in order to make such an emergency stop possible (case 3, activity 4). The radio of the locomotive cabin has to be always set at a volume to ensure continuous monitoring, but it was set at a low volume for one train (case 3, activity 5). Therefore, the train crew members did not hear the warning given by the crew of a third train about the presence of another train approaching on the same track when it was too late to avoid the collision, because instead of focusing his attention on the state of the track(case 3, activity 7), he was trying to understand how to operate his new portable radio. These unreliable behaviors caused the collision between two trains.
Both retrospective and prospective analyses identify critical and sensitive factors that facilitate the occurrence of scenarios of unreliability. The specification step has then to study scenarios of the second and the third classes of consequence on system safety in order to provide humans with a set of error prevention support tools such as situation awareness programs or computer bases to. Nevertheless, when support tools are designed such as the train speed control tool or the driver's vigilance control tool analyses have to be reviewed in order to assess possible interactions between humans and the support tools, and their consequences.