Proposal of a generic methodology to harmonize Preliminary Hazard Analyses for guided transport

Mohamed Habib Mazouni, Dominique Bied Charreton, Jean-François Aubry

Proposal of a generic methodology to harmonize Preliminary Hazard Analyses for guided transport

Mohamed-Habib MAZOUNI
CRAN-ENSEM-INPL/ESTAS-INRETS
2, Avenue du général Malleret
Arcueil cedex, F-94114 France
mohamed-habib.mazouni@inrets.fr

Dominique Bied-CHARRETON
ESTAS-INRETS,
2, Avenue du général Malleret
Arcueil cedex, 94114 France
dominique.bied-charreton@inrets.fr

Jean-François AUBRY
CRAN-ENSEM-INPL,
2, Avenue de la Forêt de Haye
Vandoeuvre, 54506 France
jean-francois.aubry@isi.u-nancy.fr

Abstract - *This communication addresses the "Safety, Reliability & Quality Assurance" topic. It is located very clearly in the field of land guided transport (interurban train, HST, subway, tram).*

The land guided transport systems are mainly composed of four material classes: the infrastructure, the rolling stock, the energy supply chain and all of the signaling and control systems.

This paper deals with different methodologies used to analyze and demonstrate the safety of a control system, but it more especially deals with the Preliminary Hazard Analysis (PHA), which is usually used first and very early in the Safety Management System.

Keywords: Safety, Dependability, Risk, PHA, Guided transport, Control systems.

1 Introduction

The safety demonstration of the transport system can be achieved through a total Preliminary Hazard Analysis (PHA), but especially through the development of files for the specific safety of each subsystem and through the examination of their interfaces. The control systems such as indication, speed control, or automatic piloting have as a task to manage major risks which can induce disasters (collision or derailment).

For a very long time, the engineers who have been working on the design, the homologation or the evaluation of this equipment, have worked in a context where the used methods are very strictly formalized, and where the safety files are structured complying with quality plans that are the bases of the project management. This tendency in the field of indication has increased with the emergence of data processing to manage critical functions. From the middle of the eighties, the equipment became more and more complex, and so the need for rigor and formalization has increased. In this field, control is more advanced than the other transport system components.

This set of safety and fault avoidance demonstration steps led to the drafting of European standards NF EN related to the RAMS aspects of the railway applications[19], their software[20] , their hardware[21] and their environment.

These standards translate a broad consensus in the profession of guided transport and constitute a set of guidelines and credible references concerning safety and availability.

2 PHA quotation in the French regulation [17]

The Safety File (SF), enriched throughout the project, tends to show that the identified risks in the Preliminary Safety File (PSF) are covered and controlled.

The Decree No. 2000-286 of March 30, 2000 related to the safety of the national railway network stipulates that the PSF considers the technical and functional data as well as the objectives of safety stated with the Definition File (DF).

In the decree of January 8, 2002, adopted to enforce the decree No. 2000-286 of March 30, 2000 related to the safety of the national railway network, the output documents which must provide a PHA are specified as follow:

- The functional description of the system,
- The identification of hazardous events,
- The evaluation and classification of the associated risks,
- The proposition of prevention and protection measurements,
- The allowance of safety objectives.

The PSF comprises a document containing the results of the PHA, while the SF contains the conclusions of the safety studies carried out and the certificate that the PHA identified risks are considered and reduced sufficiently to be acceptable.

3 PHA quotation in the standards

"The PHA is a technique to identify and to analyze the hazard frequency, which can be used during the upstream phases of the design to identify the hazards and to evaluate their criticality" [5], [14], [16].

IEC 300-3-9 standard relating to the management of the dependability and more precisely the 3rd part presents a risk generic analysis process, including six steps which can be associated to the PHA [16]:

- The specification of the applicability,
- The identification of the hazards and the initial evaluation of the consequences,
- The risk assessment,
- The checking,
- The documentation,
- The progressive updating as the project develops.

We may conclude that the French national regulation indicates the documents that a PHA should provide without specifying how it should be approached, whereas standard IEC 300-3-9 recommends an analysis process containing several stages but without addressing more precision on the PHA output documents to be provided.

3.1 The PHA as it is considered by NF EN 50126 standard

The French and European railway standard NF EN 50126 proposes a 14 phases life cycle. Each phase contains many tasks linked with the Dependability (Reliability, Availability, and Maintainability) or with the safety. Of course, we will be interested more particularly in this second category. The first phase consists in collecting data on reliability, availability and safety relating to similar systems previously brought into service.

Once phase 2 is completed, the mission profile, the description and the various constraints resulting from the system environment are supposed to be known. During this phase, the RAMS team must undertake the "hazardous situations preliminary analysis".

NF EN 50126 standard has the advantage of positioning very well this type of analysis in the system life cycle. Indeed, this stage is located in phase 3, before the specification of system requirements. It must according to the standard, be carried out after a description of the system and a good knowledge of its environment.

PHA results are presented according to a table with two main columns:

- Hazard investigation : initial events, hazardous situations, final hazardous event,
- Risk management: methods of covering and control.

These are precisely the processes of risk management which will then make it possible (beyond phase 4 of the life cycle according to the standard) to specify the system safety requirements, and to define the safety acceptance criteria. The table of PHA often comprises another column which appoints the actor(s) responsible of each hazardous situation management actions: traveling material, infrastructure, energy supply chain, control, operation or maintenance. Thus, we ensure traceability in the assignment of the responsibilities between the various groups and between the various subcontractors.

The recommendations of the French/European railway standard NF EN 50126 lead to a Preliminary Analysis, since the system is still slightly or badly known. At this stage of the life cycle, PHA is an opportunity to write the specifications of the functional requirements and of the whole system safety aspects.

4 PHA methodology

4.1 Objectives of PHA

The Preliminary Hazard Analysis was developed at the beginning of the sixties in the aeronautical and military fields. Since then, it has been used in many other industries[4], [10].

PHA aims at identifying the various hazardous elements present in the studied system. Then, every element will be studied in order to know how it could lead to an incident or to a more or less serious accident, further to an event causing a potentially hazardous situation.

But term "PHA" also is used by some manufacturers in quite different cases than those quoted by the above mentioned standard. Indeed, the objectives of the manufacturer can be to [6], [18]:

- Classify the functions according to their severity, then to be able to process them according to their SIL (Safety Integrity Level),
- Define the system specifications,
- Refine the hazard covering methods.

The PHA is then carried out on a functional modeling of the equipment to be developed, for which we seek to define with precision the safety requirements.

The various actors involved in the development and the acceptance of a system (project superintendents, customers, appraisers and administrations) still have currently a problem of vocabulary divergence, which slows down the safety methods harmonization [11], [13], [16].

4.2 The principles of causality of the accident scenarios

The preliminary knowledge of the accident concept, its causality mechanisms and its materialization process, guarantees a better identification of the accidents scenarios in order to implement the defensive barriers in a strategic and effective way, so that this materialization

will be avoided, its impact reduced or its repetition frequency limited.

The undesirable phenomena can be Accidents or Incidents (macroscopic approach) or Failures or Faults of subsystem components (microscopic approach).

Theoretically, the causes and effects sets are non-restrictive. Nevertheless, in practice, we consider representative sets containing the most credible elements.

The causal approach is a way to say that nothing is due to chance, and that behind any effect there is at least a possible cause. Indeed, the cause/effect relations can be explored via a link-up Hazardous Event (HEv) in two ways :

- The inductive causal approach: it is the direct approach, starting from some knowledge on the causes and seeking to predict the corresponding effects,
- The deductive causal approach: it is the opposite approach, starting from some knowledge on the consequences and trying to identify the origins of the corresponding causes.

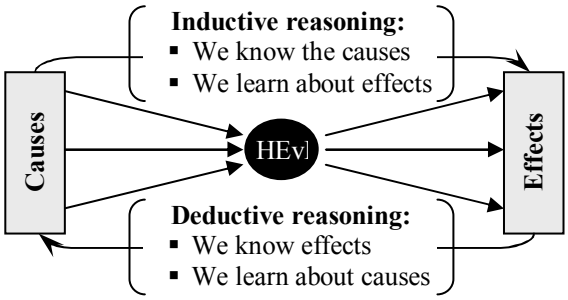

Figure 1. Inductive and deductive causal reasoning loop

4.3 Is the PHA an Inductive or a deductive analysis?

The viewpoints diverge both on the PHA terms, concepts and methodology**:**

"It is (the PHA) traditional inductive approach", quoted by Prof A. Laurent, CNRS-LSGC (sécurité des procédés chimiques, p 367, May 2003) [3],

"*It is (the PHA) deductive analysis***"**, quoted by Prof A. Heurtel, CNRS - IN2P3/LAL (La gestion des risques techniques et des risques de management, p 14, December 2003) [2].

The quality and the quantity of relevant knowledge are determining factors in the choice that will be related to the analysis approach: inductive or deductive.

If this knowledge primarily relates to the consequences, we can thus proceed by deduction in order to identify the possible causes. The mechanisms of learning feedback are largely used in this approach which also seems in perfect harmony with the exercise of accidents reconstitution.

The opposite approach requires a good knowledge of the causes likely to be precursors for undesirable phenomenon materialization. At this stage, we try to release the possible consequences relating to given causes set. This approach thus consists in extracting the various possible accident scenarios.

5 PHA methodologies as practiced in the railway field

5.1 PHA Methodology at ALSTOM Transport [10]

5.1.1 Hazard Identification

This phase can be based on the learning feedback to draw up the preliminary list of hazards.

5.1.2 Textual analysis

This analysis corresponds to a census of the technical provisions guaranteeing safety. These provisions can be classified either by subsystem or by hazard.

5.1.3 PHA results presentation

The deductive preliminary analysis aims at highlighting:

- The list of the hazardous events precursors of potential accident,
- The risk reduction measurements,
- The allowance of the responsibilities to various intervenors,
- The covering of the risks through an a posteriori assessment of severity and frequency.

Table 1. ALSTOM prototype of a PHA results presentation

1	2	3	4	5	6
Potential accident	No.	Phase	Hazardous event	Causes	Consequ-
					Consequences

7	8	9	10	11	12	13
-ences	Measurements taken			Risk assessment		
Severity	Wording	Type	Resp.	Sev.	Freq.	Accept.

- 5: The causes can be external dysfunctions or operational problems,
- 10: A responsibility assignment for the taken measurements application.

5.2 PHA Methodology at the RATP

5.2.1 The identification of the causes and the origins of the hazardous events

The analysis continues according to a deductive approach in order to try to identify the causes and the origins of the hazardous events at this stage.

5.2.2 The proposal of risk reduction measurements

The allowance of measurements to control risks is done according to the evaluation of the consequences related to each hazardous event. The precision of the actors concerned with these measurements is an organizational aspect aiming at defining clearly the responsibilities and to make official the follow-up of the risks.

5.2.3 PHA results presentation

Table 2. RATP prototype of a PHA results presentation

1	2	3	4	5
Potential accident	hazardous event	Place	Potential cause	Elements as cause

6	7	8	9
Severity class	Type	Measurements in risk reduction	Actor concerned

- 1.2: Revealed further to the development phase of the tree hazards,
- 3: Place: in station, in line, etc,
- 4: The possible cause of the hazardous event,
- 5: The involved element in the hazardous event: railway, infrastructure, signals, etc,
- 6: The severity classes of hazardous events are derived from the criticality matrix proposed by NF EN 50126 standard.

6 A proposal of a generic and harmonized PHA methodology

6.1 Development of the Potential Accidents tree

This phase is mainly based on the learning feedback to determine the potential accidents list, and then we try to detect the corresponding hazardous events by a deduction reasoning. The results are put in an analysis elementary table having the following form:

Table 3. Potential Accidents Tree

Potential accident		Hazardous event
1. collision	1.1 with obstacles	1.1.1 Too long stopping distance
		.....
	1.2 with third	1.2.1 Presence of a road vehicle or service on the way (rail)

6.2 Hazard study

To identify the hazardous elements (VTE: Vulnerable Target Entities, HSE: Hazards Supplier Entities) and the resulting hazardous situations, the analyst is guided by the elementary checklists of Potential Accidents (Potential Accidents Tree). These checklists are specific to the concerned study field. As its name indicates, this method is not intended to process the materialization of accident scenarios in details, but rather to highlight the various possible problems encountered during the life cycle of the studied system.

6.2.1 First Phase: Deductive Identification of the HSE and VTEs

Table 4. HSE and VTE investigation phase

1	2	3	4	5
Potential Accident	Hazardous Event	Hazardous Situation	Initial Event	HSE, VTEs

PA: Potential Accident,
HEv: the Hazardous Event(s) causing this PA,
HS: The corresponding Hazardous Situation,
IEv: Initial Event announcing the HS,
HSE: Hazardous Supplier Entity (ies) that is (are) the principal(s) generator(s) of the HS after the IEv emergence,
VTEs: targets could be threatened as a result of the PA materialization.

- 1,2: revealed further to the development phase of the accident scenarios tree,
- 3,4: The possible causes of the hazardous event: the lists of the hazardous situation and of the initial events precursors of the hazardous event,
- 5: The involved element in the hazardous event apparition: human factor, rail, infrastructure, signaling or control systems, etc.

6.2.2 Second phase: Inductive identification of accident scenarios

Table 5. Accident scenarios investigation phase

1	2	3	4
Accident scenarios			
Hazard Supplier Entity	Initial Event	Hazardous Situation	Hazardous Event

- 1,2,3,4: Development of the accident scenarios causality. The causes can be external dysfunctions, operational problems or due to human factor.

From each HSE identified in the first phase, we develop the different ways inducing an hazardous event. We suppose that the apparition of an Initial Event stimulate the HSE that immediately become generator of a hazardous situation considered as a precursor of an hazardous event.

6.3 Risk calculation

The risk calculation covers the following four steps:

- The determination of the possible mishaps for the exposed VTEs,
- The assessment of severity,
- The assessment of the probability of occurrence of a hazardous event,
- The risk calculation as a combination between Exposure, Occurrence and Severity.

Table 5. Risk assessment presentation

5	**6**	**7**	**8**
Assessment			
Mishaps	Severity	Occurrence	Risk

- 5: Mishaps: human death or injury, system or service loss or environmental damage,
- 6,7: The classification of severity and hazardous events occurrence are derived from the criticality matrix proposed by NF EN 50126 standard,
- 8: Risk classification.

6.4 Risk management

In order to reduce or eliminate the risks that have been evaluated as unacceptable, the following categories of measurements can be implemented:

- Pro-active measurements: the elimination of the structural causes (Hazard Supplier Entities) of a hazardous event.
- Preventive measurements: the prevention of the direct causes of a hazardous event and the reduction of its effects.
- Protective measurements: the minimization of hazardous event consequences on the vulnerable targets.

Another type of measurements can be considered, it concerns the aftercare going back to the original situation before a hazardous event apparition.

Risk management can be approached from different angles. It can be considered as the gateway that an organization have to go over to meet its responsibilities for safety. On the other hand it can be considered as the process which demonstrates that a studied system satisfies its overall requirements for safety [9], [15].

Table 6. Risk control policy

9					**10**		
Risk Management					Decision		
Risk Reduction				Desirable gains	Word.	Motive	Resp.
Word.	Type	Tm.	Man.				

- 9: The risk reduction measurements:
  Measurement "Wording", its "Type" (pro-active, preventive...), the "team" and its "Manager" appointed to apply the required control actions (allowance of the responsibilities to various intervenors).
  The "Desirable gain" box is added to assess the margin of risk reduction, which should be obtained further to the taken measurements implementation. This step is covered through an a posteriori assessment of severity and frequency,
- 10: final "decision": to disapprove or to agree the risk reduction actions (step 9).

7 Conclusion

The paper is not intended to be a complete talk about all the methods of safety specification, validation and demonstration in the field of control systems equipped land transports. It first intends to show the place of PHA, which is the starting point of all of the safety activities, and which then enables to specify safety requirements while complying with previously defined specifications.

The practice of PHA is perceived in various ways by the manufacturers of guided transport systems or Control systems.

It should initially be noticed that in the majority of the cases, PHAs are Hazard analyses, because we consider the severity of accidents, but not their occurrence frequencies; thus we should speak about Preliminary Hazard Analysis and not Preliminary Risk Analysis *"Analyse Préliminaire de risques (APR)"* which is the term used by the French specialists.

The PHA thus provides the risks covering directives. These processes are at this stage written in very general terms: constructive provisions, periodic tests in maintenance, operation procedures, calculation note, etc. To be able to write the System Requirements Specifications (SRS), which is the higher level specification document, it is necessary to refine its general provisions in terms of lower level criteria.

The proposed methodology is an interesting framework for the definition of a PHA generic methodology which would comply with the regulation measurements, with the standards recommendation and above all in harmony with various industrial contexts

(ALSTOM, RATP, Siemens Transportation Systems, etc.).

Up to date, we are working on the specification of an Interactive System of Decision-Making Aid for drafting, editing and checking the PHA output documents.

8 References

[1] A. DESROCHES, "L'Analyse Préliminaire des Risques", Qualita, France-Bordeaux, 2005.

[2] A. HEURTEL, *La gestion des risques techniques et des risques de management*, CNRS - IN2P3/LAL, 2003.

[3] A. LAURANT, *Sécurité des procédés chimiques*, Lavoisier Edition, 2003.

[4] A. VILLEMEUR, *Sûreté de fonctionnement des systèmes industriels,* Eyrolles *Edition*, 1988.

[5] IEC, *Guide 300-3-9: Dependability management*, International Electrotechnical Commission, 1995.

[6] IEC 61511, *Functional safety - safety instrumented systems for the process industry sector*, International Electrotechnical Commission, March 2005.

[7] IEC, *61882: Hazard and operability studies (HAZOP studies) – Application guide,* International Electrotechnical Commission, May 2001.

[8] CENELEC, *First edition of the 9th Memorandum: Safety aspects - Guidelines for their inclusion in standards*, European Committee for Electrotechnical Standardization, 1994.

[9] E.M. El-Koursi, S. Fletcher, L. Tordai , J. Rodriguez, *SAMNET synthesis report: safety and interoperability,* February 2006.

[10] GTR 55 Workgroup, *aspects sémantiques du risque*, Collège sécurité, Institut de Sûreté de Fonctionnement, 2000.

[11] HMSO, *A guide to Risk Assessment and Risk Management for Environmental protection*, Her Majesty's Stationery Office, 1995.

[12] INERIS, *Analyse des risques et prévention des accidents majeurs : Synthèse vis-à-vis de l'étude de danger*, INERIS - Direction des risques accidentels, Unité évaluation des risques, 2004.

[13] ISO 14971, *Medical devices - Application of risk management to medical devices*, International Organization for Standardization, 2000.

[14] ISO/CEI Guide 51, *Safety aspects - Guidelines for their inclusion in standards*, International Organization for Standardization / International Electrotechnical Commission, 1999.

[15] L. Tordai, Report *D.1.2.3: Common Safety Targets and Common Safety Indicators*, June 2005.

[16] M.H. MAZOUNI and H. HADJ-MABROUK, "Méthode et formalisme de base pour l'Analyse Préliminaire des Risques appliquée dans le transport ferroviaire", The 6th International Conference on sciences and techniques of automatic control, Tunisia-Sousse, December 2005.

[17] M.H. MAZOUNI, "Concepts et terminologie de base pour l'Analyse Préliminaire des Risques dans le transport ferroviaire", *Actes INRETS*, No. 109: Communiquer, Naviguer, Surveiller et Innovations pour des transports plus sûrs, plus efficaces et plus attractifs, April 2006.

[18] NF EN ISO 12100, *Safety of machinery*, International Organization for Standardization, November 2003.

[19] NF EN 50126, *Railway applications: the specification and demonstration of Reliability, Availability, Maintainability and safety (RAMS)*, AFNOR, December 1999.

[20] NF EN 50128, *Railway Applications: Communications, Signaling And Processing Systems-Software For Railway Control And Protection Systems,* AFNOR, July 2001.

[21] NF EN 50129, *Railway applications: communication, signaling and processing system - safety related electronic systems for signaling,* AFNOR, May 2003.