A PHA based on a systemic and generic ontology

Mohamed Habib Mazouni, Jean-François Aubry

IEEE/INFORMS International Conference on Service Operations and Logistics, and Informatics (SOLI'2007), Loews hotel, Philadelphia, Pennsylvania. USA – August, 26-29 USA

A PHA based on a systemic and generic ontology

Mohamed-Habib MAZOUNI
CRAN - UMR 7039 , Nancy-Université, CNRS /
ESTAS - INRETS
20, Rue Elisée Reclus
Villeneuve d'Ascq, 59666 - France
mohamed-habib.mazouni@inrets.fr

Jean-François AUBRY
CRAN - UMR 7039 , Nancy-Université, CNRS,

2, Avenue de la Forêt de Haye
Vandoeuvre, 54506 - France
jean-francois.aubry@isi.u-nancy.fr

Abstract - *This communication addresses the "Service Design, Engineering, Operations, & Innovations" topic. It is oriented towards the "Security & safety-related services and management" and deals more precisely with the Preliminary Hazard Analysis (PHA) practiced in high risk industrial fields: nuclear, chemical, military, and among others, guided transport.*

The PHA was developed at the beginning of the sixties in the aeronautical and military fields. Almost five decades later, the practice of the PHA remains not less problematic and completely far from any harmonization optics. Moreover, the European lawful and international normative contexts remain very pragmatic in that sense.

In order to meet the ceaseless needs of generic methodologies allowing to harmonize the PHA, we consider that the divergences between the various actors are rather of a semantic nature then syntactic and that it wouldn't be enough to write and than distribute a glossary of concepts, but to model them in a dedicated ontology.

Indeed, our objective is to conceive a "systemic ontology based generic methodology" in order to exploit efficiently the exchange of PHA know-how, of course without concession on results' coherence and completeness .

Keywords: Ontology, Methodology, Systemic, PHA, Hazard, Risk, Dependability, Safety, Railway.

1 Introduction

The PHA is usually used first and very early in the design process of a Safety Management System. It aims at identifying the various hazardous elements which could be internal or external for the studied system. Then, each element shall 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.

The objectives of the safety evaluator can be to [13]:

- Classify the functions according to their severity, then to be able to process them according to the acceptable risk level,
- Define the system specifications,
- Refine the hazard covering methods.

The various actors involved in the development and the acceptance of industrial systems (project superintendents, customers, appraisers and administrations) still have currently a problem of vocabulary divergence [4]. Consequently, that last handicap slows down seriously the European harmonization processes of common safety methods engaged by the European Union Commission. Concerning the railway field, the transposition of the directives 2004/49/EC and 2001/16/EC related respectively to safety and to interoperability is considered as a significant step [1], [2], [3].

2 State of the art of PHA practice

According to the multitude of "confidential" Preliminary Hazard Analysis files we studied, we had immediately noticed that the PHA is practiced in various ways by the different concerned actors (e.g. Siemens Transportation System, Alstom, Faiveley, SNCF, RATP, Bombardier, etc.).

In any case, we have noticed that the whole of the studied PHAs allows mainly to highlight:

- A list of potential accidents,
- A list of hazardous events,
- A risk calculation,
- A list of risk reduction measures.

Nevertheless, many important points haven't been taken into account. For example:

- The allowance of the responsibilities to various interveners,
- The covering of the risks through an a posteriori assessment of severity and frequency.

3 A proposal of a generic system of systems for PHA

The collocation of the term system might seem inappropriate, since this term has a very generic meaning. However, the definition of system we adopted is quite specific: "A system is a set of interacting components for achieving common objectives".

The systemic approach applied to a complex system takes into account the internal interactions between the whole of its components. In other words, the total system is, in fact, not equal to the sum of its components, because quite simply, each one of them is indissociable from the whole [17].

The interactions System/Human, System/Environment and Human/Environment shall be carefully studied. However, disposing of a dependable technological system, a perfect personnel and an adapted environment,

doesn't guarantee the achievement of the safety and dependability targets. Consequently, a complete analysis of the interaction's trip-type between these entities must be performed (fig. 1).

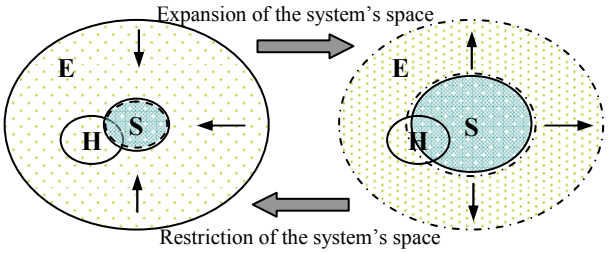

Figure 1: Human/System/Environment boundaries

System vs. Environment:

The expansion of the system on the environment's space (notice the new border beyond the limit of the two arrows on the Figure 1) lead to consider new humans and new subsystems being, indeed, inside the new system boundaries. For example, the infrastructure or the agents of maintenance intervening on its rail track can either be regarded as subsystems or parts of the environment.

3.1 Socio-technical system

A socio-technical system is an organized total unit of interrelationships between elements, actions or individuals [16].

3.1.1 Technological System

It concerns rather the equipments entities than the functional aspects allowing to manage them.

However, defining a generic system means being able to describe the following characteristics:

- The general description of the system and its boundaries,
- The description of its various mission profiles,
- The functional description including a structural breakdown of the system into lower level sub-systems and components.

In order to be consistent with European Railway directives [1] [2] [14], a generic railway system must be separated into two main subsystems:

- Structural subsystem: is the physical railway transport system. This system basically comprises infrastructure and trains:
  - Track infrastructure: track bed, tracks, points and crossings, civil works (bridges, tunnels, viaducts, level crossings, etc.), station infrastructure such as platforms,
  - Energy: power supply, overhead catenary supply, pantographs, etc,
  - Signalling and train control systems,
  - Rolling stock,
  - Operation and regulation.

- Functional subsystem:
  - Maintenance (procedures and mandatory corrective and preventive tasks),
  - Operations (normal and degraded modes),

3.1.2 Human - workforce

This entity includes the whole of the management and technical staff and training facilities implicated in the project life cycle between the specification and the dismantling phases.

For example, the following workforce groups could be affected by the operation and maintenance of a railway system:

- Railway workers on trains, at stations, on or near the lines,
- Railway companies subcontractors.

The human error is defined in standard IEC 50(191) as: "a human action that produces an unintended result". The standard gives a generic definition of the concept of "Error": "(an error is) a discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition" [9].

J. Reason has classified human errors in three categories [11]:

- Error at the behavioural level: the error is imputed directly to the individual,
- Error at the contextual level: "to err is human", but it is necessary to investigate and deduce the related causality,
- Error at the conceptual level: here, the assumptions on the cognitive mechanisms are explored by distinguishing error types (Intentional, Unintentional) and forms (Violation/Fault, Mistake/Slip).

3.2 Environment

L. GOFFIN [12] defines the environment as a dynamic system characterized by the physicochemical, biological and cultural interactions, perceived or not, between the man, the other alive beings and all the surroundings elements, which can be natural, transformed or created by the man.

The environment of the major industrial systems (nuclear, chemical, military, transport, etc.) is primarily defined through three types of risk: the first one could be grouped as a part of the public risks, the second one as a part of the technological risks and the last one as a part of the natural risks.

In the Railway field, the environment is perceived as a composition of a whole of entities, which are not under the control of any railway organization, but could be targets or suppliers of hazards.

3.2.1 Human - members of the public

It can be approached as members of the public behaving in either legitimate or illegitimate manner and not being under the organization control.

In the railway system, the following groups can be distinguished:

- Passengers on trains or at stations,

- People legitimately on railway property (e.g. on level crossings),
- People living or working outside the physical boundaries of the railway,
- Emergency services (fire services, police, emergency medical services, etc.).

3.2.2 Technological environment

The technological environment can be composed of:

- Neighbouring technological systems providing services with potentially to be either hazardous or vulnerable entities towards the organization's global system,
- Building and factories with potentially hazardous processes,
- Roads, airports, harbours,
- Electromagnetic environment.

3.2.3 Natural environment

The natural environment can include the meteorological, hydrological, geological, seismic conditions, etc.

4 Proposal of a generic systemic ontology for PHA

4.1 Introduction

The ontology we propose takes into account the possibility of several Vulnerable Target Entities (VTE) to be in implication with one Hazard Supplier Entity (HSE) in the same accident scenario.

4.2 Ontology's elementary entities

The standard IEC 50 (191) defines the concept of entity as follow: "Any part, component, device, subsystem, functional unit, equipment or system that can be individually considered. It may consist of hardware, software or both, and may also in particular cases, include people" [9].

4.2.1 Hazard Supplier Entity (HSE)

Any entity (natural or created by man) or adopted provision comprising one or several hazards; in the field of the technological risks, a "hazard potential" corresponds to a technical unit necessary to the envisaged operation of a given process.

4.2.2 Vulnerable Target Entity (VTE)

Any entity such as people, goods or various environment components likely to be threatened in certain circumstances of exposure in the hazard space.

4.2.3 Threat of HSE on VTE

Refers to implicit consequences in a hazardous situation, but more precisely describes its realization circumstances and its imminent propagation into an accident situation.

4.3 Ontology's elementary events

An event is the dual concept associated with the concept of state of an entity; in other words it can produce or be produced by a change of that state. An event is characterized by its occurrence (date, frequency, number, etc.) and it can be deterministic or stochastic (random).

4.3.1 Exposure Event (EEv)

Event, running or abnormal, internal or external for the system allowing to expose a VTE in a hazard space. In other words, to put it in a hazardous situation.

4.3.2 Initiating Event (IEv)

Event, running or abnormal, internal or external for the system, located upstream the hazardous event in the kinetic sequence, having the capacity to excite a HSE which becomes generator of a hazardous phenomenon.

4.3.3 Hazardous Event (HEv)

An incidence of a hazardous phenomenon in a context of exposure situation. Conventionally defined, within the framework of a hazard analysis, as in the heart of the accidental process. Generally, it acts as a loss of containment for the fluids or as a physical loss of integrity for the solids.

4.4 Ontology's elementary situations

4.4.1 Initial situation

It is the phase considered to be normal where the whole of the entities belongs to their specification. The VTEs are beyond the range of the hazard space, then protected from any HSE's threat.

4.4.2 Exposure situation

The Exposure event announces the entry of one or several VTEs in the hazard space. A passenger being on the rail track is regarded as a VTE in exposure to several hazard fields (electrocution, crushing by a train, legal proceeding (another dimension of the hazard space)…). A scientist (VTE) who's working in a laboratory with radiation effects (Hazard) is considered in exposure while he's intervening inside.

4.4.3 Hazardous situation

It is characterized by the development of a hazardous phenomenon as soon as appears a stimulating "Initiating Event". A hazardous phenomenon is a release of whole or part of a hazard potential. This concretization produces undesirable effects (dispersion of a pollutant gas cloud, skid of a car, etc).

4.4.4 Accident situation

This phase succeeds like a logical continuation for the hazardous and exposure situations when the hazardous phenomenon intensity reaches one or several vulnerable

targets. This stampede phase is announced by the first impact.

4.5 Ontology's risk governance and corollary

4.5.1 Hazard

Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment [7].

4.5.2 Hazardous phenomenon

An incidence due to the exposure of a HSE to an Initiating Event (IEv). It is a release of a whole or a part of a hazard's potential through the hazardous situation (see above, section 4.4.3).

4.5.3 Risk

The concept of risk is very badly understood and differently defined:

HMSO [5]	A combination of the probability, frequency, occurrence of a definite hazard and amplitude of the related consequences.
BARBET [6]	The risk is a contingent and detrimental event for the people, goods and organizations. Contingent: It can occur or not according to the realization of one or several causes.
INERIS Working Group : Methodology [8]	The risk is regarded as the possibility of supervening of a damage resulting from an exposure to the effects of a dangerous phenomenon. It is an expectation of losses in human lives, wounded, damage to the goods and nuisance to the economic activity during a reference period and a given area, for a particular hazard.
IEC 61508, ISO 300-3-9, ISO/CEI 51	Combination of the probability of a damage and its severity.

The risk is a measurement of the occurrence of an undesirable event and its associated effects and consequences. We can admit that the risk is the measurement of the hazard expressed by a relation between several factors (Severity, Occurrence, Exposure, Avoidance possibilities, etc).

4.5.3.1 Risk calculation

a. Severity assessment

According to the systemic classification (cf. section 3), we take into account the harm caused to the system's and environment's people, the damage caused to the technology constituting the system and that localized in the environment's space, and finally, we integrate the potential threats on the organization's issues.

Severity	**Impact on the socio-technical System**		**Impact on the Environment**			**Organization's issues being potentially threatened**
	Human	**Technology**	**Human**	**Technology**	**Natural Environ-ment**	
Minor	No wounded	Minor damage	No wounded	No effect	No effect	Technical
Import-ant	Minor wounds	Important damage	Minor wounds	Minor damage	Significant threat	Commercial, Financial, Technical
Critical	Critical wounds, or one dead	Loss of the system	Critical wounds, or one dead	Important damage	Localized damage	**(Localized crisis)** Judicial, Commercial Financial, Technical
Catast-rophic	More than one dead	X	More than one dead	Loss of systems	Important damage	**(Important crisis)** Economic, Media effect, Judicial, Commercial, Financial, Technical, etc.

b. Occurrence assessment

An accident frequency is the measurement of the number of awaited events occurring in a given lapse of time under given conditions.

Generally, the occurrence classes are selected in a qualitative way with giving indications on the corresponding qualitative values per a given duration:

Qualitative label	**Quantitative correspondence (/hour)**
Unlikely	Extremely incredible to occur during the life of the system (<= 10^{-9} occurrence per hour)
Rare	Incredible to occur but possible during the life of the system (> 10^{-9} occurrence per hour)
Occasional	Probable that it occurs during the life of the system
Frequent	Probable that it occurs frequently during the life of the system

c. Risk ranking through the criticality matrix

The approach of risk level's classification per interval allows to engage the risk reduction decisions with a priority to the protective actions aiming at reducing the severity (primary safety). Graphically, the purpose of the committed actions is to bring back the risk level towards the most possible clearest colour (i.e. the up-left case):

	Minor	**Important**	**Critical**	**Catastrophic**
Unlikely	Negligible	Negligible	Negligible	Negligible
Rare	Negligible	Tolerable	Undesirable	Intolerable
Occasional	Tolerable	Undesirable	Intolerable	Intolerable
Frequent	Undesirable	Intolerable	Intolerable	Intolerable

Negligible risk: Accepted without agreement of the Official Authority. It refers to a level of risk whose occurrence is unlikely (i.e. about 10^{-6} per year in the railway field [13]) and the possibility of realization does not affect the everyday life [5].

Tolerable risk: Accepted with the implementation of an adequate control and the agreement of the Official Authority. However, it is accepted in a certain context based on the current values of the society [4] [7] [10].

Undesirable risk: Shall only be accepted when its reduction is impracticable. It requires an agreement of the Official Authority. It's a residual risk remaining after the application of the measures of prevention and whose reduction is impossible or insufficient.

Intolerable risk: Shall be eliminated/insulated at least to obtain a tolerable level.

b. Risk control policy

A risk is either accepted if it is lower than the risk already incurred or tolerable if there is a counterpart.

It is noticed that the railway casualty data, and therefore safety targets, may not be comparable between countries adopting different safety principles [14]:

The GAME principle: A new system acceptance depends on the proof that it reaches at least the state of the art or the same degree of safety of an existing referential system.

The ALARP principle: The ALARP principle defines a first range where the risk is so small that it appears to be broadly acceptable and a second range where the risk is so high that it cannot be accepted. Between these two intervals there is a width band where it is possible to put into relationship the additional costs for risk reduction and the benefits.

The MEM principle: MEM is based on the endogenous mortality caused by natural reasons e.g. illness or natural defects.

Risk management:

It's a risk covering phase, while engaging the appropriate risk reduction actions allowing to avoid the causes, to mitigate the effects or to limit the consequences. Also, it is suitable to reduce the exposure factor.

4.6 Modelling of the proposed ontology

The identification of the accident scenarios would be based on the state/transition based accidental process:

Transition condition	Input State	Output state	Causes	Principles of Defence in-depth
EEv: Exposure Event	Initial Situation	Exposure Situation	Internal or external for VTEs	Limitation of exposure, remedy for the VTEs' vulnerability
IEv: Initiating Event	Initial Situation	Hazardous Situation	Internal or external for a HSE	Reduction of the HSE's sensibility, limitation of HEv's occurrence
HEv: Hazardous Event	Hazardous Situation + Exposure Situation	Accident Situation	Hazardous phenomenon intensity + VTEs' Vulnerability	Mitigation of effects + Limitation of consequences

The figure below (Figure 2) shows a sketching-out of the proposed PHA's ontology:

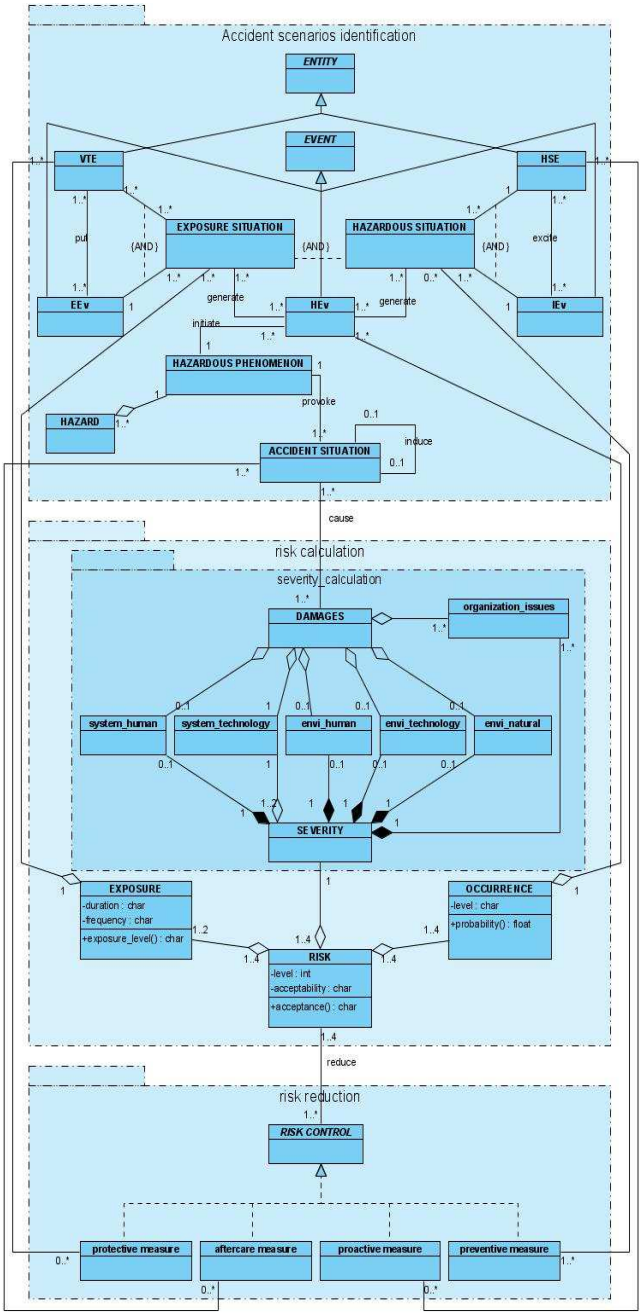

Figure 2: UML Class Diagram Modelling of the PHA's Ontology

4.7 Proposal of a PHA's methodology based on the systemic ontology

The methodology we proposed is mainly composed of six primary and complementary phases [4]:

1. Development of the Potential Accident Tree,
2. Hazard study: identification of the hazardous elements (VTE, HSE) and the resulting hazardous

situations. Here, the analyst would be guided by the elaborated checklists (tree) of Potential Accidents,

3. First Phase: deductive identification of the HSEs and the corresponding VTEs,
4. Second phase: inductive identification of the accident scenarios from each HSE identified through the first phase. Indeed, the analyst tries to develop the different ways inducing potentially an hazardous event,
5. Risk calculation,
6. Risk management:
   - Pro-active measures: to eliminate HSEs.
   - Preventive measures: to prevent of HEvs.
   - Protective measures: to mitigate impacts reaching VTEs.
   - Aftercare measures: to go back to the normal (initial) situation before a HEv's apparition.

5 Conclusion

The paper intends to show the difficulties noticed in the practice of the PHA, which is the starting point of the definition of any SMS (Safety Management System).

The preoccupation with genericity led us to widen our investigation with various fields. Henceforth, we are persuaded that an accident develops semantically according to the same process, only the specificity of the circumstances and the consequences characterizes it differently.

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

Defining the environment helps define the system interfaces. Therefore, a harmonized PHA's methodology based on a systemic ontology constitutes an interesting step towards a decision-making aid system allowing to:

- Organize the defence in-depth lines by establishing barriers suitable with each elementary entity, situation or event of the ontology.
- Inter-connect the different subsystems PHAs (generally elaborated by subcontractors) in order to constitute the PHA of the whole system by identifying if the effects of an accident relative to a subsystem doesn't represent immediate causes of a new accident scenario implying the whole system.
- Inter-communicate the similar system's PHAs via experience feedback similarity mechanisms on already studied, and better known existing systems. This will undoubtedly optimize the practice of the safety principles *GAME* and *ALARP*.

Currently, we are working on the development of an Interactive System of Decision-Making Aid for drafting, editing and checking the PHAs'output documents.

6 References

[1] *Directive 96/48/EC on the interoperability of the trans-European high speed rail system*, Commission of the European Communities, Brussels, July 23, 1996.

[2] *Directive 2001/16/EC of the European Parliament and of the Council on the interoperability of the trans-European conventional rail system*, Commission of the European Communities, Brussels, March 19, 2001.

[3] *Directive 2004/49/EC on safety on the Community's railways*, L164 p44-113, 29 April 2004, Official Journal of the European Union (2004).

[4] M.H. MAZOUNI, D. Bied Charreton, J.F. AUBRY, "Proposal of a generic methodology to harmonize Preliminary Hazard Analyses for guided transport", IEEE – SMC international conference: system of systems engineering , San Antonio-Texas - USA, April 2007.

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

[6] J.F. BARBET, *Maîtriser les risques* , Préventique / Sécurité, Journal, March - April 1996.

[7] IEC 61508, *Functional safety of electrical / electronic / programmable electronic safety-related systems*, International Electrotechnical Commission, 2000.

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

[9] IEC 50(191) *International Electrotechnical Vocabulary, Chapter 191: Dependability and quality of service*, International Electrotechnical Commission, 1990.

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

[11] J. REASON & D. PARKER, *Managing the Human Factor in Road Safety*, The Hague: Shell International Petroleum Maatschappij, 1993.

[12] L. GOFFIN, 1976, *Environnement et évolution des mentalités*, PhD Thesis, FUL, Arlon-Belgium, 1976.

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

[14] SAMRAIL Consortium, D 2.1.1 report: *Analysis of existing approaches*, European Commission and SAMRAIL partners, September 2003.

[15] SAMRAIL Consortium, D 2.3 report: *common safety methods*, European Commission and SAMRAIL partners, September 2004.

[16] E. MORRIN, 1980, *La Méthode, 1 : la nature de la nature ; 2 : la vie de la vie,* Le Seuil Edition.

[17] F. GALLOU & B. BOUCHON-MEUNIER, 1992, *Systémique : Théorie & Application,* Lavoisier Edition.