# Preliminary Hazard Analysis Generation integrated with Operational Architecture – Application to Automobile

Pierre Mauborgne[1,2], Samuel Deniaud [3], Eric Levrat [4], Eric Bonjour[2], Jean-Pierre Micaëlli [5] and Dominique Loise[1]

**Abstract.** We are witnessing evolution of standards (as the functional safety one) and increasing of complexity. This implies to perform safety studies efficiently and earlier in the context of Model-Based System Engineering. So, in this article, we will propose an evolution of the Preliminary Hazard Analysis (PHA) method in order to comply with the overall safety requirements in the automotive domain. To demonstrate its usefulness, we apply this method to an industrial case which concerns the hazard analysis of unintended acceleration of a vehicle.

**Keywords:** MBSE, Safety, Operational Architecture, PHA, ISO 26262

## 1 Introduction

Currently, automotive functional safety standards require manufacturers to demonstrate vehicle safety. Moreover, cars are increasingly complex due to the integration of innovative functions and the respect of regulations related to emission, safety, etc. Activities that aim at evaluating safety properties are often performed separately from design activities. Model-Based Systems Engineering is an opportunity to integrate safety analysis efficiently with Systems Engineering. The expected results are more efficient development. However Systems Engineering and Safety activities have specific methods and tools but also some similar concepts. In order to bridge the gap towards Safe Systems Engineering, a common terminology is required.

[1] PSA Peugeot Citroën – route de Gisy, 78140 Vélizy-Villacoublay, France – {pierre.mauborgne,dominique.loise}@mpsa.com

[2] Université de Lorraine/ENSGSI, ERPI, EA no 3767, 8, rue Bastien Lepage, Nancy, 54010, France – {pierre.mauborgne, eric.bonjour}@univ-lorraine.fr

[3] IRTES-M3M, UTBM, Université de Technologie de Belfort-Montbéliard, 90010 Belfort Cedex, France – samuel.deniaud@utbm.fr

[4] Université de Lorraine, Centre de Recherche en Automatique de Nancy (CRAN) - CNRS, UMR 7039, Campus sciences, BP 239, 54506 Vandoeuvre-lès-Nancy Cedex, France – eric.levrat@univ-lorraine.fr

[5] Université de Lyon, INSA Lyon, Centre des Humanités, 1, rue des Humanités, 69621 Villeurbanne Cedex, France – jean-pierre.micaelli@insa-lyon.fr

In this article, we will focus on the activity initiating the Safety analysis process, which is the Preliminary Hazard Analysis (PHA). It is possible to retrieve the content of this activity as "Hazard and Risk Analysis" in the functional safety standards (1), as "Aircraft (or System) PHA" in aeronautical standards (2) or as "Hazard Analysis and Risk Assessment" in the automotive standard (3).

For Desroches et al. (4), this activity is used to determine a classification of hazardous situations. This is very important because it influences further activities of the safety process.

This article proposes a conceptual model of safe systems engineering with concepts relevant for the PHA. After defining the process of the Concept of Operations and Requirements Analysis, we will explain a method related to the "Preliminary Hazard Analysis" process. Two kinds of PHA are identified: functional PHA, threat-related PHA. Finally we will apply this method to a specific case that concerns an automotive vehicle. As this method is applicable in other domains, we will indicate when the concepts are specific to the automotive domain.

## 2 Background on links between Safety and Systems Engineering

Clear relations between systems engineering and safety is a prerequisite for an efficient integration of engineering and safety analysis.

We can distinguish two types of approaches that deal with these relations: model transformation (5), (6) and processes.

Yakimets et al. (5) selected several target languages as AltaRica (7) or NuSMV (8) which are Safety languages to perform safety analysis. After annotation of functional SysML diagrams, they realize a translation of SysML models to the target model.

Papadopoulos et al. (6) choose to focus on the generation of fault trees and FMEA from structure diagrams such as SysML (9) Internal Block Diagrams (IBD). The enrichment of blocks by "local" analysis and the links between these blocks enable to propagate failures and to get reports.

Regarding process approaches, Systems Engineering standards as ISO 15288 (10) indicate additional activities regarding safety, however these activities are realized in parallel of other activities of the process.

David et al. (11) has identified a method to perform FMEA by determining the necessary information either in the functional model or in a specific database (i.e. generic failure modes). By extending this approach, Cressent et al. (12) integrated it into a design process.

However, we can note that the standards evocate very few links. Moreover, we have found no work concerning a better integration of PHA and systems engineering. For this reason, we choose to focus our contribution on this key activity for the safety analysis.

Regarding "Preliminary Hazard Analysis" methods, the automotive functional safety standard (3) specifies inputs (item definition report), a sub-process and deliver-

ables. It doesn't clarify the links between functional analysis and PHA. We may conclude that in ISO 26262 (3), this activity is subsequent to the functional analysis.

Desroches et al. (4) set out three steps to achieve a PHA: identifying dysfunctional scenarios, assessing them and proposing a risk coverage (or mitigation) that could be avoidance scenarios.

The objective of our contribution is to propose a process that integrates Systems Engineering and Safety activities but it does not concern transformations of model or language. We will present a process in detail which meets the objectives of PHA based on Systems Engineering models.

# 3 Conceptual Model of Safe Systems Engineering – Requirement Analysis View

## 3.1 Introduction

According to Rausand (13), there is no systematic process to realize a PHA. A cause of this statement is that different domains have their own concepts and different definitions for the same concept.

We also agree on the fact that some concepts have relative definitions and their perimeters are not necessarily well defined. It motivates the definition of the conceptual model of safe systems engineering. Table 1 defines 5 major requirements for this conceptual model.

**Table 1** Requirements for the conceptual model of safe systems engineering

| **Reference** | **Requirement.** The conceptual model shall |
|---|---|
| 1 | show the links between system engineering and safety. |
| 2 | be simple |
| 3 | enable to verify the correct application of a safety process. |
| 4 | provide a shared common language between the different stakeholders (experts, systems architects, safety engineers) |
| 5 | be compliant to the state-of-the-art methods of safety analysis |

There are existing conceptual models that do not meet these requirements. The conceptual model in Chalé et al. (14) deals with links between systems engineering and ISO 26262 (3) but it is too generic to satisfy requirements 3 and 5. There is a unique view and concepts are not classified according to the processes. Moreover dependability concepts are in the same group of concepts and are not distribute in systems engineering groups.

The conceptual model in Deniaud et al. (15) contains some relevant concepts but we cannot rely a process on this model: Safety concepts are linked to systems engineering concepts. Conceptual model structure separates design and specification concepts. Due to that, it will be the basis for our conceptual model.

As Chalé et al. (14) or Deniaud et al. (15), the conceptual model we propose in this section is based on the analysis of key standards: IEEE 1220 (16), ISO 15288 (10) for

Systems Engineering concepts and ISO 26262 (3) for safety concepts. In order to fulfill the above requirements, the model is divided into three views corresponding to the three main processes of system design (Requirements Analysis, Functional Architecture Design and Physical Architecture Design). In this article, we only present a partial view of the conceptual model of the first process, Concept of Operations and Requirements Analysis (Figure 1). It represents safety concepts and links to systems engineering concepts.

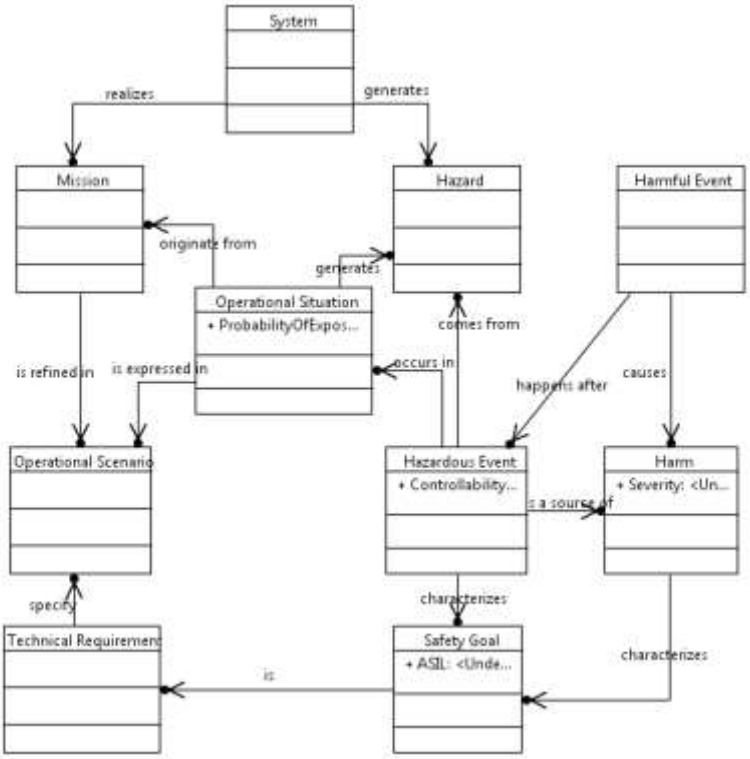


**Fig. 1.** Conceptual Model of Safe Systems Engineering –Requirement Analysis View

### 3.2 Safety concepts definition

If we cut the figure 1 into 4 columns, the two first columns are associated to the main concepts of systems engineering. We focus here on defining the concepts of the two last columns.

We can distinguish concepts to define the dysfunctional scenario and those for the assessment of the scenario.

**Determination of dysfunctional scenario**

Figure 2 presents the sequence of concepts about dysfunctional scenario.

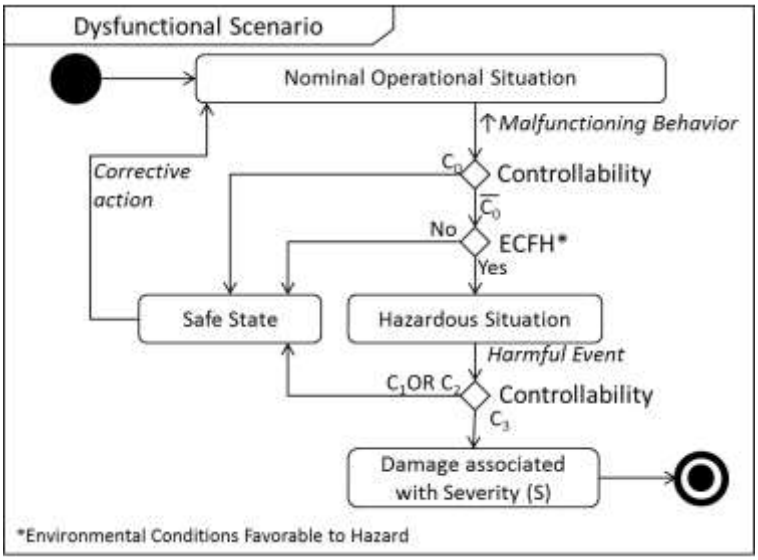


**Fig. 2.** Proposal for determining and assessing dysfunctional scenario

As defined in ISO 26262 (3), the hazard is a potential source of harm caused by a malfunctioning behavior of the system.

The apparition of these hazards (within environmental conditions favorable to hazard (ECFH) corresponds to a hazardous event, that generates a hazardous situation. A harmful event (such as a shock) triggers the transition from a hazardous situation to harm (damage associated with severity).

**Dysfunctional scenario assessment**

As stated before, we use ISO 26262, automotive functional safety standard (3) as a reference but most of the concepts are also present in other standards.

As Desroches et al. (4) defined, one step of the PHA concerns the assessment of dysfunctional scenario.

The probability of apparition of hazardous event is determined either qualitatively or quantitatively depending on the domain. If the qualitative criterion is used, the probability of apparition is defined by 4 classes in automotive domain.

Similarly, the severity of damage is evaluated for each situation, a level of severity can be associated.

Finally, in the automotive field, the controllability determines whether the driver can control the vehicle once he perceives the hazardous event. There are 4 levels to characterize this criterion (C0, C1, C2, C3).

The combination of these three criteria enables to define a Safety Integrity Level named ASIL in ISO 26262 (3). There are similar Safety Integrity Levels in other domains as SIL in IEC 61508 (1) or DAL in ARP 4761 (2) but there are different criterions to determine it.

From this analysis, we can specify a high level safety requirement. The safety integrity level is associated to the requirement. In automotive domain, these requirements are called Safety Goal in ISO 26262 (3) associated with ASIL.

# 4 Our proposal concerning the integration of PHA and MBSE

The proposed conceptual model enables to have a common language between system architects and safety engineers. In this section, we present a process that integrates PHA and systems engineering models.

## 4.1 Inputs and outputs of the PHA

PHA will be linked to the process of Concept of Operation and Requirements Analysis defined in ISO 15288 (10). There are similar processes in other references such as IEEE 1220 (16) or SEBoK (17).

The aim of PHA is to identify and classify hazardous events that can then be expressed as a safety goal. The objective of this activity is to provide the necessary inputs for the next activities of safety related to the functional and physical architectures.

These requirements are derived from the dysfunctional scenario, its assessment and possible avoidance scenarios. To define the dysfunctional scenario, events and situations must be defined (figure 2).

In the following sections, we will explain the global approach which is the most commonly used one. This approach is based on hazards which are deviations of output flows of the system to its environment.

After, we will adapt it to complete this analysis by taking into account the threats of the system towards the environment. Identification of hazards from this approach is based on the determination of emerging and abnormal flows.

## 4.2 Global approach

Figure 3 shows an overview of the global approach.

First we have to find the possible beginnings and ends of the dysfunctional scenario.

With the diagram defining services of the system, we can have flow deviations for services output. Services explicit principal mission of the system. To complete the identification of hazards, the context diagram defining interfaces and flows between system and its environment is necessary. The deviation flow can be associated with the abnormal modification of a performance of a system service. This association allows having a clear and measurable safety requirement.

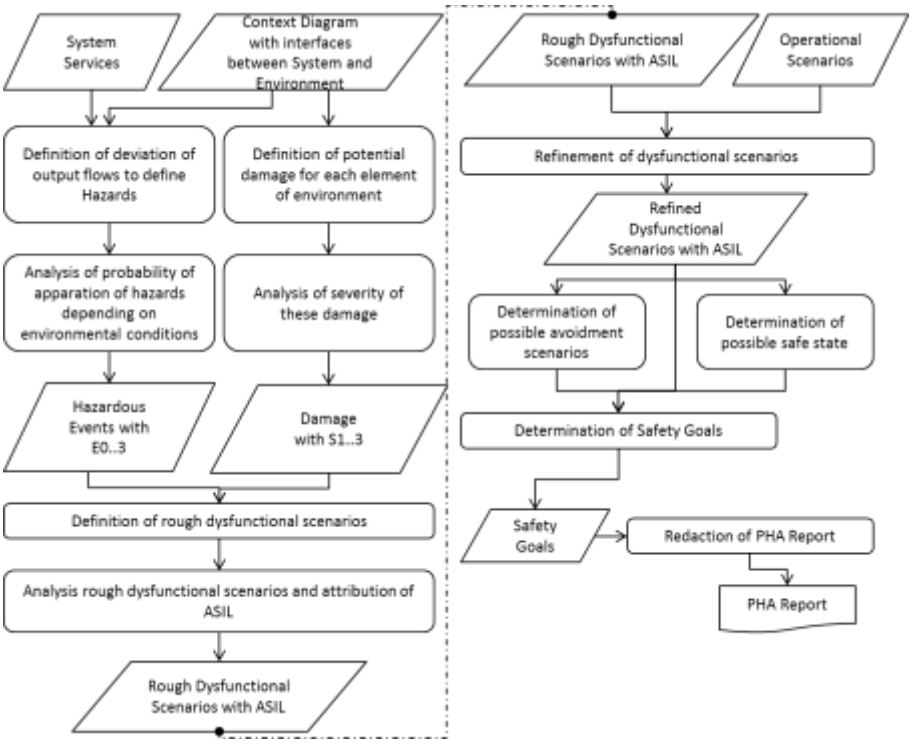


**Fig. 3.** Flowchart of the proposed approach

We identify the possible operational state of each element of the environment of the context diagram. For example, for a pedestrian, possible operational states are injured, safe or burnt. Possible damage is obtained by combinations of these states and events which trigger to damage.

We can evaluate them with ASIL parameters which are severity for the damage and probability of apparition of hazard in a defined environment.

Rough dysfunctional scenarios can then be defined by instantiating for each flow deviation the diagram presented in figure 2. By analyzing these rough scenarios, we can identify critical ones and select them for further analysis.

By refining these critical scenarios, we can determine possible avoidance scenarios or safe states (nominal or degraded states of the system which are safe for the driver).

Finally, we have to conclude by determining a safety requirement that is useful to further design the system.

### 4.3 PHA approach related to threats

The approach of Preliminary Hazard Analysis related to threats of the system on the environment is close to the global approach.

The main distinction concerns the determination of the hazard. It is not as systematic as in the global approach. Indeed, hazards due to threats are new abnormal flows

that didn't exist before. For example, if we consider oil leak, there is no normal flow between vehicle and road.

# 5 Application to an example

## 5.1 Determination of the scenario

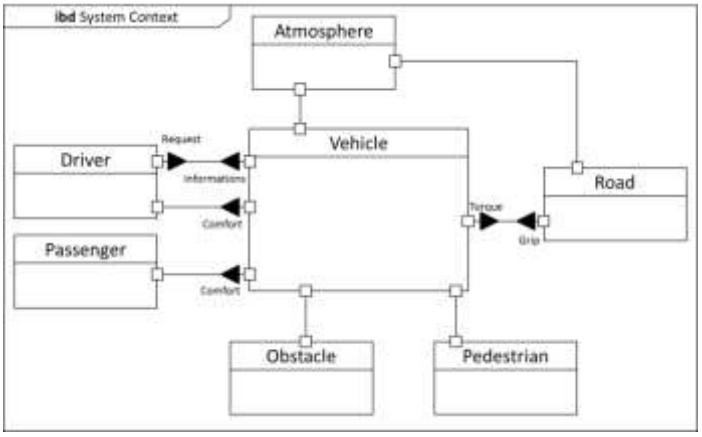


**Fig. 4.** Context Diagram

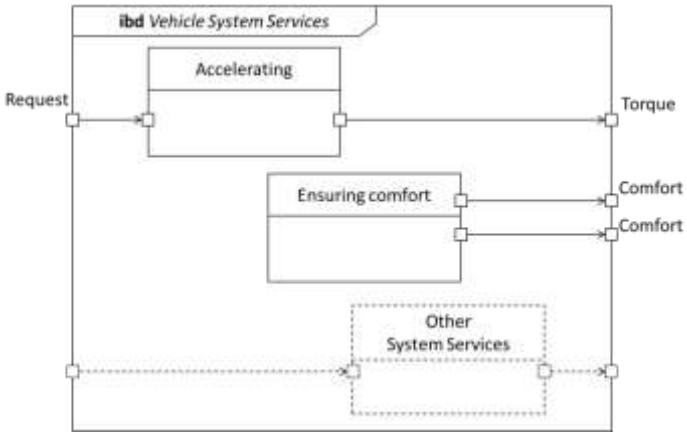


**Fig. 5.** Partial view of vehicle system functions

Diagram in Figure 5 identifies the flow between the vehicle and the road for the system service called "Accelerating". A deviation of the output flow is an "Unintended Acceleration". Now, we have to analyze whether there are potential damage due to this hazard.

Thanks to the diagram on figure 4, we can determine that the worst case of damage is critical injuries of the passenger or pedestrian due to a collision.

So, we can have a scenario thanks to this information described as a diagram in Figure 6. We have environmental conditions favorable to hazard which is "presence of obstacle".

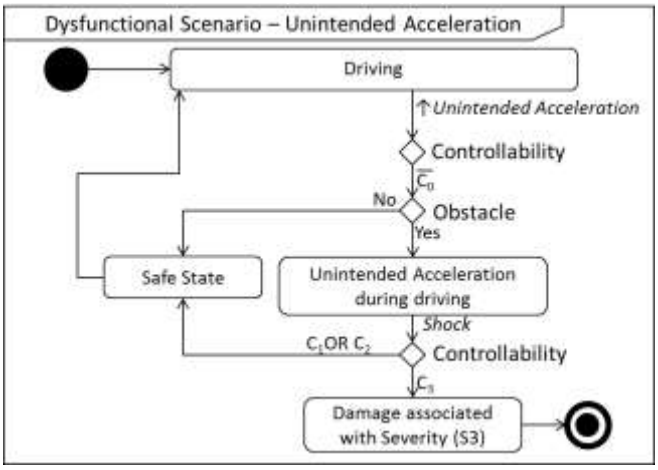


**Fig. 6.** Rough dysfunctional scenario of Unintended Acceleration

By analysing operational scenarios associated to the system service "Accelerating", this rough scenario can be linked to some operational scenarios. Moreover, we choose the one which has the worst consequences, i.e. critical injuries as we analyzed previously. In our case, the operational scenario is obstacle avoidance during driving in normal operation (Figure 7).

After short studies (like the determination of the perception time), we can modelize this dysfunctional scenario (Figure 8). A sequence diagram is chosen because we want to see interactions between the system and its environment.

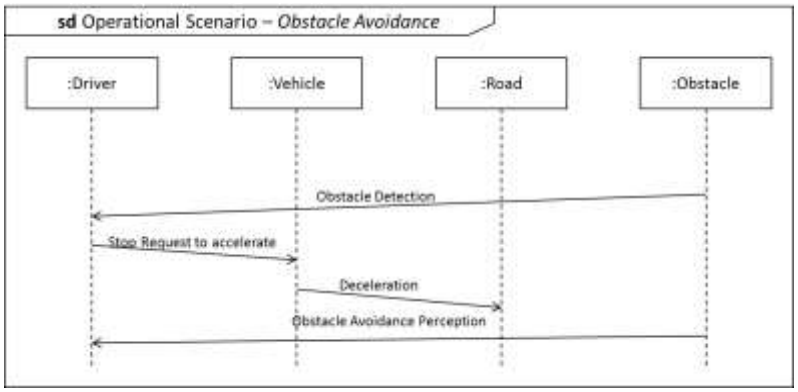


**Fig. 7.** Operational Scenario of Obstacle avoidance in normal operation

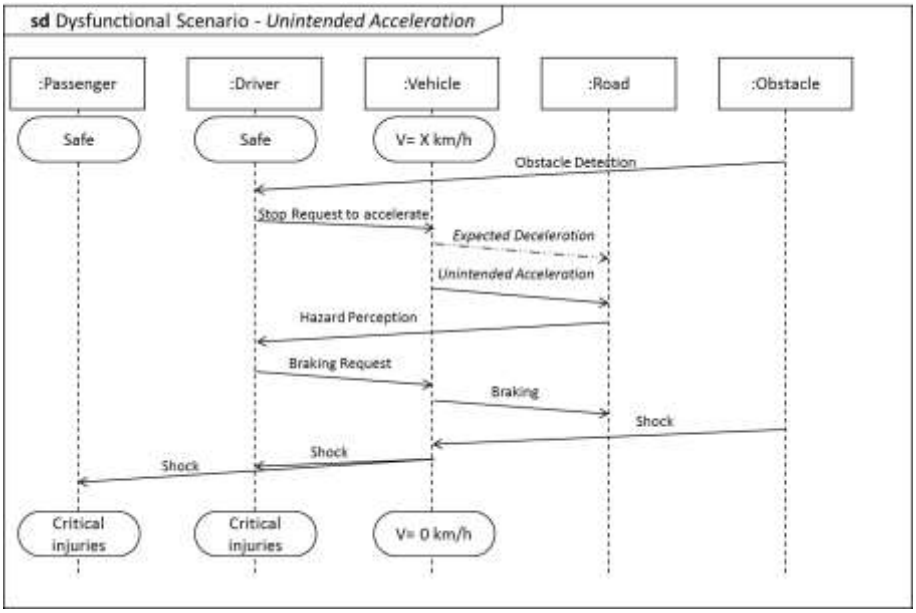


**Fig. 8.** Refined dysfunctional scenario of Unintended Acceleration

### 5.2 Assessment of the dysfunctional scenario (example used in ISO 26262)

Safety standards as ISO 26262 (3) contain tables to attribute a level for each criterion.

In our case study, driving is one of the basic phases of life cycle of the vehicle and accelerating is one of the main system services of the vehicle. So, thanks to the table of definition of this criterion in ISO 26262 (3), unintended acceleration during driving is E4 (E is for exposure and 4 is the highest exposure level).

Since the damage to the passengers are severe, the level for Severity is S3 (3 is the highest severity level) as it is defined in the table of severity in ISO 26262 (3).

Controllability is the most subjective criterion. It can be represented using the dysfunctional scenario modelized in figure 8. In our case study, we consider that 90 % or more of all drivers can react by braking if there is an unintended acceleration, so the level for Controllability is C2 (2 is the medium controllability level). ISO 26262 gives examples to define this criterion in a table.

### 5.3 Proposal of risk coverage

In the case study, the hazard corresponds to the output of the vehicle. So, possible avoidance scenario is to, either limit or reduce this performance. It leads to a safe state "without an unreasonable level of risk" (3).

### 5.4 Result of the PHA

As shown on table 2, the results can be synthesized for the corresponding Safety Goal. For reasons of readability in this article, it is presented into 2 parts. In the first one, there is the description of the dysfunctional scenario. In the second part, there is the assessment of the scenario and the proposal of risk coverage.

**Table 2.** PHA of "Unintended acceleration during driving"

| System | Phase | Considered Flow | Hazard | Hazardous Event | Harmful Event | Operational Situation with Harm |
|---|---|---|---|---|---|---|
| Vehicle | Driving | Mechanical Energy to Road | Unintended Acceleration | Unintended Acceleration during driving | Shock | Critical Injuries of the driver |

| Probability of Exposure | | Severity | Controllability | ASIL | Possible Avoidance Scenario | Safety Goal |
|---|---|---|---|---|---|---|
| X % | E4 | S3 | C2 | C | Reduction of performances | the difference between driver's intend and the acceleration of the vehicle must be less than Y% |

## 6 Conclusion & Outlook

After having defined the various terms used to define a preliminary hazard analysis, we have defined a PHA process that is linked to the process of concept of operation and requirements analysis. Moreover, similar concepts have emerged from the conceptual model like mission and hazard. This emergence proves that systems engineering and safety activities can be done in osmosis and not separately like definition of operational and dysfunctional scenarios as it is shown in this article. The aim is to take into account the requirements of ISO 26262 and to better integrate MBSE and safety analysis.

The first outlook we will investigate is to link this work to the failure propagation in the functional architecture.

The second outlook focuses on the refinement of the process according to the design stages (concept, preliminary design and detailed design). In the preliminary design, we have bases of system architecture. So global PHA can be done from the concept stage and refined in further ones.

## Acknowledgments

We want to acknowledge PSA Peugeot Citroën and especially Dominique's Department for helping us to define this method and for the interesting discussions about this.

## References


1. IEC 61508: Functional safety of electrical/electronic/programmable electronic safety related systems. (1998)
2. ARP 4761 - Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. (1996)
3. ISO 26262: Functional safety for road vehicles. (2009)
4. Desroches, A., Leroy, A., Vallée, F.: La gestion des risques: Principes et pratiques. Management et Informatique. (2003)
5. Yakimets, N., Jaber, H., Lanusse, A.: Model-based system engineering for safety analysis of complex systems. In: MBSAW, Bordeaux. (2012)
6. Papadopoulos, Y., McDermid, J. A.: Hierarchically Performed Hazard Origin and Propagation Studies. In: Computer Safety, Reliability and Security. (1999)
7. Batteux, M., Prosvirnova, T., Rauzy, A., Kloul, L.: The AltaRica 3.0 project for model-based safety assessment. In: Industrial Informatics (INDIN), 2013 11th IEEE International Conference on, pp. 741-746. (2013)
8. Cimatti, A., Clarke, E. M., Giunchiglia, E., Giunchiglia, F.; Pistore, M.: Nusmv 2: An open-source tool for symbolic model checking. In: Computer Aided Verification, pp. 359-364. Springer Berlin Heidelberg. (2002)
9. OMG Systems Modeling Language (OMG SysML) V1.3. (2012)
10. ISO 15288 Systems Engineering - System life cycle processes. (2002)
11. David, P., Idasiak, V., Kratz, F.: Reliability study of complex physical systems using SysML. In: Reliability Engineering & System Safety, *95*(4), 431-450. (2010)
12. Cressent, R., David, P., Idasiak, V., Kratz, F.: Designing the database for a reliability aware Model-Based System Engineering process. In: Reliability Engineering and System Safety. (2012)
13. Rausand, M.: Preliminary Hazard Analysis. In: System Reliability Theory. Wiley interscience. (2004)
14. Chalé, H. G., Taofifenua, O., Gaudré, T., Topa, A., Lévy, N., Boulanger, J.-L.: Reducing the Gap Between Formal and Informal Worlds in Automotive Safety-Critical Systems. In: 21st Annual INCOSE International Symposium. (2011)
15. Deniaud, S., Bonjour, E., Micaëlli, J.-P., Loise, D.: How to integrate reliability into Systems Engineering framework. A case from automotive industry. In: CRECOS seminar, Helsinki (2010)
16. IEEE 1220 - Standard for Application and Management of the Systems Engineering Process. (2005)
17. Pyster, A., Olwell, D. H.: The Guide to the Systems Engineering Body of Knowledge (SEBoK), v. 1.1.2. In: Hoboken, NJ: The Trustees of the Stevens Institute of Technology. (2013)