Safety Science 87 (2016) 256–268

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

Operational and System Hazard Analysis in a Safe Systems Requirement Engineering Process – Application to automotive industry

Pierre Mauborgne [a,b], Samuel Deniaud [c], Eric Levrat [d], Eric Bonjour [b,*], Jean-Pierre Micaëlli [e], Dominique Loise [a]

[a] PSA Peugeot Citroën, Route de Gisy, 78140 Vélizy-Villacoublay, France
[b] Université de Lorraine/ENSGSI, ERPI, EA no 3767, 8, rue Bastien Lepage, Nancy 54010, France
[c] IRTES-M3M, UTBM/UBFC, 90010 Belfort Cedex, France
[d] Université de Lorraine, Centre de Recherche en Automatique de Nancy (CRAN) – CNRS, UMR 7039, Campus Sciences, BP 239, 54506 Vandoeuvre-lès-Nancy Cedex, France
[e] Centre de Recherche Magellan, IAE de Lyon, Université Jean Moulin Lyon 3, 6 cours Albert Thomas, 69008 Lyon, France

ARTICLE INFO

Article history:
Received 23 September 2015
Received in revised form 27 February 2016
Accepted 13 April 2016
Available online 26 April 2016

Keywords:
Safety
Systems engineering
Hazard analysis
Safety requirements
MBSE
ISO 26262

ABSTRACT

Automotive engineers have to meet evolving customer expectations, particularly growing concerns for safety, by introducing new sophisticated devices like Line Keeping Assistance, Collision Mitigation Braking System or Pedestrian Detection. These devices are composed of electrical components. They are likely to be subject to failures that may impact automobile safety, which means the safety of the vehicle occupants or pedestrians. Recent standards like ISO 26262 aim at mitigating these safety problems. Automobile engineers must prove that they perform safety studies along the design process. Meanwhile, they have to cope with other changes in their engineering practices. Due to the goals of verifying the satisfaction of all requirements, the design offices have introduced new practices based on Systems Engineering (SE) which are based on models. SE tools or processes are based on a functional approach of the system in which dysfunctional aspects are missing. Thus, there is a need to integrate the safety domain into the SE framework in order to improve safety studies and the collaboration between systems engineers and safety specialists.

This paper analyzes this issue by focusing on the definition of high-level (or vehicle-level) safety requirements. It proposes a Safe Systems Requirement Engineering Process and a method named Operational and System Hazard Analysis (O&SHA) that helps to specify the high-level safety requirements (called safety goals in ISO 26262). It is based on a Model-Based Systems Engineering approach (MBSE) which integrates safety aspects. The added value of the proposed method is illustrated by applying it to two case studies.

1. Introduction

Due to stakeholders' greater demands for safety, automotive engineers have to take into account stringent safety requirements by using specific methods, tools or standards, and performing safety-focused processes or activities. Since 2011, some of them have been also adopting ISO 26262 standard (ISO 26262, 2009) that deals with functional safety of road vehicles. This standard states that car designers perform safety assessment activities and produce specific safety deliverables. Safety activities related to the external view of the system correspond to a rough system definition ("*item definition*" in ISO 26262) and a definition of high-level safety requirements based on hazard analysis ("*Hazard Analysis and Risk Assessment*" in ISO 26262). These requirements are called safety goals in the automotive sector. They are evaluated with a criterion called Automotive Safety Integrity Level (ASIL) being defined as "*one of the four levels to specify the item's or element's necessary requirements of ISO 26262 and safety measures for avoiding an unreasonable residual risk, with D representing the most stringent and A the least stringent level*". In ISO 26262 (2009), a key phase is the "*Concept phase*". It is composed of the "*Hazard Analysis and Risk Assessment*" activity that concludes with the definition of Safety Goals and the Functional Safety

* Corresponding author.
E-mail addresses: pierremauborgne@gmail.com, pierre.mauborgne@univ-lorraine.fr (P. Mauborgne), samuel.deniaud@utbm.fr (S. Deniaud), eric.levrat@univ-lorraine.fr (E. Levrat), eric.bonjour@univ-lorraine.fr (E. Bonjour), jean-pierre.micaelli@univ-lyon3.fr (J.-P. Micaëlli), dominique.loise@systemes-conseil.com (D. Loise).

http://dx.doi.org/10.1016/j.ssci.2016.04.011
0925-7535/

Concept activity. This latter activity derives the functional safety requirements, from the safety goals, and "*allocate them to the preliminary architectural elements of the item or to external risk reduction measures in order to ensure the required functional safety*". To comply with the safety goals, the functional safety concept specifies the safety mechanisms and safety measures in the form of functional safety requirements.

To cope with safety requirements and with the complexity of the electronic systems they induce, car manufacturers also adapt their Systems Engineering (SE) practices defined in standards like ISO 15288 (2002) or IEEE 1220 (2005). The main technical upstream design processes that are identified in ISO 15288 are: the Stakeholder Requirement Definition (SRD), and the System Requirement Analysis (SRA). These processes are focused on an operational view of the system. They aim at providing system requirements to the following architectural design processes. Current SRA and SRD processes include very limited safety activities. For example, they do not take into account any preliminary hazard analysis (PHA), which consists in identifying, assessing and classifying dysfunctional scenarios related to hazardous events (Vincoli, 2014). SRA, SRD, and safety analysis processes and activities are usually performed with silo mentality. Thus safety engineers may misunderstand the system definition and even perform a redundant functional analysis. These issues may induce design errors. Moreover, the safety analysis is not immediate. Hence results may not be applicable by systems engineers. Furthermore, according to Alexander and Maiden (2005), it is necessary during the system design to jointly determine operational scenarios and "*negative scenarios and misuse case*".

The unsatisfactory situation we have depicted shows that there is a need for a better integration of safety activities and SE activities. Our conception of Safe Systems Engineering (SSE) is that system engineers should perform safety activities that do not require expertise whereas safety engineers should lead thorough safety assessments requiring specialized expertise. To bridge the gap toward a SSE, we aim at defining a framework composed of a conceptual model and SE processes. A current trend in SE is to develop Model-Based approaches representing the system from operational, functional, physical "*views*" (defined in (IEEE 1471, 2000)). Model Based Systems Engineering (MBSE) enables designers to define and to simulate the system structure and behavior with interrelated models. Therefore, MBSE could be a relevant basis to integrate safety activities into SE models and processes. It enables to perform traceability of safety requirements, improve safety requirements justification and integrate safety recommendations into system models.

In this paper, the focus is then on Hazard Analysis and Risk Assessment concerning the definition of high-level safety requirements (safety goals) that should be performed by system engineers. This paper deals with a method to determine and classify dysfunctional scenarios in order to define the safety goals based on models compliant with ISO 26262 standard. This method is called Operational and System Hazard Analysis (O&SHA), instead of PHA because there is no determination of requirements and no model-based approach in PHA. After a state-of-art of approaches aiming at linking SE and Safety domains, this paper proposes a conceptual model integrating concepts relevant to Safe Systems Requirement Engineering (SSRE). Then SRD and SRA processes are refined in order to integrate safety aspects. Based on these enriched processes, we shall propose the O&SHA compliant to ISO 26262 and ISO 15288 standards. Then the proposed method is applied to two cases that concern a dysfunctional behavior of the car, i.e. the unintended acceleration of the vehicle and the loss of brake. Finally the value of the proposed method is discussed.

2. Safety and systems engineering, a missing link

The first safety analysis of the system that aims at defining and classifying critical dysfunctional scenarios is known as PHA. Vincoli (2014) sets out three steps to achieve it: identifying dysfunctional scenarios, assessing them and proposing a risk coverage (or mitigation) that could be avoidance scenarios. We can retrieve occurrences of this activity as Hazard and Risk Analysis in the functional safety standards (IEC 61508, 1998), as "*Aircraft (or System) PHA*" in aeronautical standards (ARP 4761, 1996), as "*Risk assessment*" *in machinery standards*" (Hiettiko et al., 2011) or as "*Hazard Analysis and Risk Assessment*" in automotive standards (ISO 26262, 2009). Even if these standards give specifications that are more detailed than the usual PHA, they do not propose any specific framework and methodology to precisely identify dysfunctional scenarios. This activity remains based on engineers' empirical knowledge and projects feedback.

IEC 61508 and ISO 26262 standards provide a framework to implement methodically PHA. The automotive functional safety standard (ISO 26262, 2009) specifies inputs (item definition), a sub-process and deliverables. Unfortunately it does not clarify the links between functional analysis and the hazard analysis. In ISO 26262 (2009), this latter activity is subsequent to the functional analysis. But, as Jang et al. exposed in (Jang et al., 2015), there is no method to fulfill this activity framework. These authors only proposed a method to determine ASIL of a safety. de Oliveira et al. (2014) presented a safety analysis process based on the HipHops software, which takes into account architecture design. The drawback of this process is the weak integration of safety activities which are still performed separately from the mainstream design activities. Another PHA process is proposed by Sinha (2011). Compliant with ISO 26262 (2009), this process includes design activities and may be a relevant basis concerning the determination of dysfunctional scenarios. Kemmann (2015) elaborated a structured approach of Hazard Analysis and Risk Assessment based on the formalization and the assessment of operational situations. However there is no proposal in the related literature concerning the assessment of dysfunctional scenarios and the way of avoiding many analyses of non-critical dysfunctional scenarios.

Since there is no formal process to generate the safety goals of the vehicle functions, another answer would be to adapt a method performed at another stage of the design process or to instantiate a more global approach. Two types of approaches dealing with safety and SE are then distinguished: model transformation-focused ones (Yakymets et al., 2012), (Papadopoulos and McDermid, 1999) vs. process-focused ones (David et al., 2010).

About model transformation approaches, Yakymets et al. (2012) selected several target safety languages as AltaRica (Kloul et al., 2013) or NuSMV (Cimatti et al., 2002) to perform safety analysis. After annotating SysML diagrams (Block Definition Diagram, Internal Block Diagram or IBD, and State Machines), the authors carried out a transformation of SysML models (OMG, 2012) to the target model. Papadopoulos and McDermid (1999) chose to focus on the generation of fault trees and Failure Mode and Effects Analysis (FMEA) from IBD. The enrichment of a component by analysis of its logical dysfunctional behavior and the links between these components enables to propagate failures and to get reports. The authors applied their method for automotive embedded systems with EAST-ADL for functional safety (Chen et al., 2011). However, there are deficiencies with SE standards and there is no method to determine Safety Goals.

About process approaches, ISO 15288 (2002) or IEEE 1220 (2005) standards add activities regarding safety. However these activities are performed in parallel of other activities of the main-