Towards compliance assurance for automotive safety-critical development: a model-based approach

Arash Khabbaz Saberi[1], Dennis van den Brand[1], and Mark van den Brand[2]

[1]Dept. of Integrated Vehicle Safety, TNO, Helmond, NL
[2] Dept. of Mathematics and Computer Science, TU/e, Eindhoven, NL
arash.khabbazsaberi@tno.nl, dennis.vandenbrand@tno.nl,
m.g.j.v.d.brand@tue.nl

Abstract. With the advent of automated driving, compliance with safety norms becomes essential for automotive system development. In this paper, we present an approach that supports the development of standard-compliant systems based on model-based techniques. We use a domain model of ISO 26262 that covers both process and product aspects on an object level. We then define constraints that define non-compliance to this standard. We check these constraints before or after related safety activities. This way, we can discover compliance errors at the moment they happen; and depending on the type of fault, we formulate feedback, or apply an automatic fix and inform the user. We believe that detecting design faults in the right moment decreases the chance of human errors to become design errors.

Keywords: Model-Based Engineering, Functional Safety, Constraint.

1 Introduction

Novel technologies such as smart mobility and automated driving are introduced in the automotive and transport industries to achieve better safety [1]. These trends increased the complexity of the systems. The system complexity increases the chance of design errors. It is more difficult to detect these design errors since there are more dependencies among components. Another source of design errors may be the miscommunication among a multidisciplinary development team as the individuals may have a different understanding of the system. An indication of these issues can be seen in the rising number of software-related recalls during recent years.

In the remainder of this paper, we describe the concept of a tool that monitors project artifacts for compliance with ISO 26262 based on a model of this standard and gives feedback to the user.

2 Tool Concept

We model the ISO 26262 with three distinct parts: product, process and constraint aspects. The product part of the domain model provides a classification for all the concepts required for safety analysis. This aspect classifies the information in the domain model into Classes, Attributes, and Relations between Classes. The process aspect consists of activities that have input and output from the product aspect. The inputs and

outputs of an activity denote the needed and produced information, respectively. We define constraints to specify what should hold to comply with the standard. These constraints are defined regarding the product aspect, and each constraint is related to an activity from the process aspect of the domain model. This allocation defines when the constraint must be evaluated.

During the development process, information is generated in various forms. We refer to all the information generated during the system development as well as their specifications as *project artifacts*. As shown in Figure 1, the proposed tool keeps tracking the project artifacts through a defined mapping to the product aspect of the domain model. The tool evaluates the constraints on these project artifacts and provides process guidelines for the user.

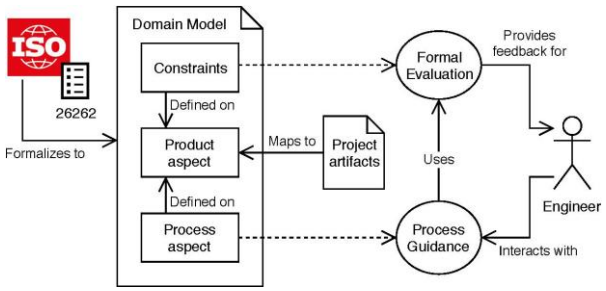

Fig. 1. Overview of the tool concept

3 Conclusions and future work

An increase in system complexity increases the chance of human error during design and the effort required for quality assurance. In this paper, we proposed the use of constraints to detect noncompliance during safety engineering according to ISO~26262. We define constraints based on ISO 26262 and a domain model of this standard. We also describe the concept of a software tool that evaluates these constraints and guides the user through the development process. As we check compliance automatically while the project artifacts are being created, we would be able to provide feedback to the safety engineers promptly. Timely feedback may reduce the impact of possible noncompliance and human errors. By automating certain tasks and detecting noncompliance at an early stage, we make it possible to reduce the overall development time and compliance evaluation effort. The nest steps for our research is to create a proof of concept for our proposed tool and validate the impact through industrial application use cases.

References

1. Meyer, G.: European Roadmap Smart Systems for Automated Driving. EPoSS Eur. Technol. Platf. Smart Syst. Integr. (2015)