Information and Software Technology 73 (2016) 151–163

Contents lists available at ScienceDirect

Information and Software Technology

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

Metrics design for safety assessment

Yaping Luo, Mark van den Brand*

Eindhoven University of Technology, Den Dolech 2 NL-5612 AZ Eindhoven, The Netherlands

ARTICLE INFO

Article history:
Received 1 September 2015
Revised 18 December 2015
Accepted 23 December 2015
Available online 21 January 2016

Keywords:
Safety assessment
ISO 26262
Metrics
Functional safety
Practical Software and Systems Measurement

ABSTRACT

Context :In the safety domain, safety assessment is used to show that safety-critical systems meet the required safety objectives. This process is also referred to as safety assurance and certification. During this procedure, safety standards are used as development guidelines to keep the risk at an acceptable level. Safety-critical systems can be assessed according to those safety standards.

Objective:Due to the manual work, safety assessment processes are costly, time consuming, and hard to be estimated. The goal of this paper is to design metrics for safety assessment. These metrics can, for instance, identify costly processes in the safety assessment process. In this paper we propose a methodology to design metrics for safety assessment from different perspectives. For the demonstration and validation of our method, we focus on safety assessment in the automotive domain (ISO 26262).

Method:Metrics can be identified by answering three questions. Three different sources of information have been identified for obtaining metrics: industrial interests, safety standards, and available data. For each of these sources appropriate methods have been proposed and used for obtaining the relevant metrics. These methods include GQM-based surveys, PSM-based procedure, and brainstorming. For the validation, the ISO 26262 standard has been studied for obtaining safety standard related metrics.

Results:A case study in the context of the European project OPENCOSS is carried out to demonstrate the method. Finally, there are 76 metrics obtained and a validation of these metrics has been done by means of a survey amongst 24 experts from 13 project partners.

Conclusion:It can be concluded that metrics for safety assessment can be derived from three sources. Different methods for designing metrics have to be used for each source. The validation shows that most of the relevant metrics are useful for industry.

1. Introduction

In safety-critical domains, such as the automotive, railway, and avionics domains, failure or malfunction of a safety-critical system may result in death or serious injuries to people, as well as severe damage to equipment. Manufacturers in those domains are expected to deliver continuously-safe products. From the end of 2009 to start of 2010, Toyota recalled millions of vehicles that are potentially prone to uncontrolled acceleration. Toyota announced that the company could face losses around US$2 billion from lost sales worldwide [1]. In July 2011, two high-speed trains collided on a viaduct in the suburbs of Wenzhou, Zhejiang province, China. In total 40 people were killed, at least 192 were injured, 12 of which suffered severe injuries. The accident was caused by a faulty signal system which failed to warn the second train of the stationary first train on the same track [2]. Therefore, with the increasing complexity of software-intensive safety-critical embedded systems, more and more effort is necessary to ensure their safety.

Safety standards, such as ISO 26262 [3], are proposed to guarantee safety risks at an acceptable level. Safety engineers in these domains manually check the development process of safety-critical systems for compliance with the standards. This checking process is referred to as safety assessment or certification. Due to the huge amount of manual work involved, safety assessment is costly and time-consuming [4]. Metrics, such as the time spent on the safety assessment process, can be used to estimate the overall cost and monitor the whole compliance process. They can also help to identify the costly activities related to safety assessment. The process of metric design is an iterative process. Normally metrics are designed and evaluated during the project. However, if incorrect information is identified, wrong decisions can be made. If unnecessary data is collected, it will increase the cost, effort, and reduce the effectiveness [5]. Furthermore, important aspects cannot be

* Corresponding author. Tel.: +31 402472744.
E-mail addresses: y.luo2@tue.nl (Y. Luo), m.g.j.v.d.brand@tue.nl (M. van den Brand).

http://dx.doi.org/10.1016/j.infsof.2015.12.012
0950-5849/© 2016 Elsevier B.V. All rights reserved.

analyzed if data is missing. Thus, we should not only consider what metrics for safety assessment can be designed, but also what data is available to be measured.

A number of methodologies have been proposed for designing metrics. Goal Question Metric (GQM) is a common approach for metric design [6]. It first defines an objective, then refines it into questions. Finally metrics are derived and collected to answer those questions. Based on GQM, a software measurement framework, called Practical Software and Systems Measurement (PSM) [7], has been developed. According to industrial practices and experience, PSM provides a guideline and suggestions for implementing a software measurement program. Moreover, a method to alter PSM to include safety is proposed [8]. This method provides two approaches (top-down approach and bottom-up approach) for designing metrics. However, both of them have disadvantages. Top-down approach does not consider the feasibility of base measures, for example, whether suitable measurable entities actually exist in an area of work. Bottom-up approach does not consider the purpose of measurements. When using this method for designing safety measures, a balance between these two approaches should be found. In this paper, based on the different perspectives (industrial interests, safety standards, available data), we identify three questions (*What do we want to measure? What should we measure? What can we measure?*) for designing metrics for safety assessment. Then different approaches are applied to get answers to these questions. Finally, a number of metrics for safety assessment can be obtained and implemented. For demonstration of our process, we carried out a case study in the context of an FP7 European project (OPENCOSS) [9]. The case study focuses on safety assessment in the automotive domain (ISO 26262) regarding functional safety.

The rest of the paper is organized as follows: Section 2 discusses the background information. Section 3 provides the research methodology used in this paper. In Section 4 questions for the metric design are discussed, as well as methods for getting the answers. Section 5 introduces a case study in the context of the OPENCOSS project. Then, the validation of the final results is discussed in Section 6. Finally, concluding remarks and future work are presented in Section 8.

2. Background

In this section, we first discuss safety assessment and safety standards. Next we describe briefly the Goal Question Metrics method [6] and Practical Software and Systems Measurement framework [7].

2.1. Safety assessment and safety standards

As mentioned before, safety-critical systems are often required to undergo a stringent safety assessment procedure to show that they meet the required safety objectives. Typically, a formal assessment process is carried out by an independent organization. The process of safety assessment or certification always includes reviews of material, testing, and facility inspection [10]. This covers the assessment of the product/system, as well as the processes and personnel involved in the development. The goal of safety certification is to check that the final product/system complies with specific standards for safety, quality or performance requirements that hold for the domain.

A number of international functional safety standards have been developed to provide development guidelines and keep the risk at an acceptable level [11], such as IEC 61508 (multiple domains) [12], ISO 26262 (automotive domain) [3], DO 178C (avionic domain) [13], CENELEC railway standards (railway domain) [14–16]. Those standards are typically large documents containing a huge number of requirements for the system to be developed and the development process used. The safety standards describe generalized approaches for identifying hazards and risks, defining design life-cycle, and prescribing design and analysis techniques. Adherence to such standards is the basis for safety assessment or certification. For each domain, automotive, avionics, railway, etc., multiple standards with different objectives exist. For example, in the automotive domain, ISO 26262 standard is a product-based standard focusing on functional safety, while SPICE(ISO/IEC 15504) [17] is a process-based standard focusing on software process assessment. In the avionic domain, DO 178C focuses on the safety of software used in certain airborne systems, while ARP 4754 [18] focuses on the development processes of aircraft systems. When applying these standards for developing a specific application, a significant degree of interpretation of these standards may be necessary.

ISO 26262. In this study, we focus on the ISO 26262 standard. Functional safety features form an integral part of each automotive product development phase. The safety standard ISO 26262 for Automotive Electric/Electronic Systems [3] is an adaptation of the Functional Safety standard IEC 61508 [12]. Similar to IEC 61508, ISO 26262 is a risk-based safety standard. Based on the V-model [19], ISO 26262 standardizes a safety lifecycle process used in the automotive industry. In the standard the risk of hazardous operational situations is qualitatively assessed. This is done to avoid or control systematic failures, and to detect or control random hardware failures [20].

ISO 26262 consists of ten parts. Parts 3–7 correspond to the product lifecycle. In the case study we will mainly focus on the Concept Phase (Part 3) of the standard, which is the starting point of the V-model. This phase has a few references to Part 6 and Part 8.

2.2. Goal Question Metric and Practical Software and Systems Measurement

The *Goal Question Metric* is a data collection method for evaluating software development methodologies and improving the software development process [6]. It can be used for understanding the fundamentals of measurements, identifying information needs, and defining measurement goals. The GQM is a top-down approach and uses goal-directed data collection. It starts with a set of corporate, division and/or project business goals, then derives questions for achieving these goals, and finally it identifies the metrics to answer the questions.

PSM is based on the *Goal Question Metric* approach, and standardized in ISO/IEC 15939 [21]. This process encourages [8]:

1. the identification of Information Needs (IN);
2. the interpretation of an Information Need as being within an Information Category (Cat);
3. the identification of Measurable Concepts (MC) within each Information Category;
4. the identification of Prospective Measures (PM), associated with each Measurable Concept.

One of the key contributions of the PSM framework is the Information Category-Measurable Concept-Prospective Measures (ICM) Table [22]. This table contains a categorization of concerns, and base measures which can be used to address the corresponding concerns. The mapping between Information Categories, Measurable Concepts and Prospective Measures is recorded in the ICM table. When using the ICM table, a user could follow the recommended process in the PSM to identify their Information Needs, select Prospective Measures, and map these measures to the