The Journal of Systems and Software 86 (2013) 1124–1151

Contents lists available at SciVerse ScienceDirect

The Journal of Systems and Software

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

Comparing risk identification techniques for safety and security requirements

Christian Raspotnig[a,b,*], Andreas Opdahl[a]

[a] Department of Information Science and Media Studies, University of Bergen, NO-5020 Bergen, Norway
[b] Software Engineering Department, Halden Reactor Project, P.O. Box 173, NO-1751 Halden, Norway

ARTICLE INFO

Article history:
Received 16 November 2011
Received in revised form 6 September 2012
Accepted 2 December 2012
Available online 8 January 2013

Keywords:
Risk identification
Safety
Security
Technique
Requirement elicitation
Comparison

ABSTRACT

When developing systems where safety and security are important aspects, these aspects have to be given special attention throughout the development, in particular in the requirements phase. There are many similar techniques within the safety and security fields, but few comparisons about what lessons that could be learnt and benefits to be gained. In this paper different techniques for identifying risk, hazard and threat of computer-supported systems are compared. This is done by assessing the techniques' ability to identify different risks in computer-supported systems in the environment where they operate. The purpose of this paper is therefore to investigate whether and how the techniques can mutually strengthen each other. The result aids practitioners in the selection and combination of techniques and researchers in focusing on gaps between the two fields. Among other things, the findings suggest that many safety techniques enforce a creative and systematic process by applying guide-words and structuring the results in worksheets, while security techniques tend to integrate system models with security models.

1. Introduction

The development of computer-based systems, where safety or security are important aspects, follow much the same approach for assessing risk involved with the systems. In the safety field the benefits of a system and its features have to be balanced against the possible accidental harm it might impose, while the security field needs to consider such benefits against possible malicious harm. Although this is the typical way to distinguish the two fields, it also exist another distinction: "Security is concerned with the risks originating from the environment and potentially impacting the system, whereas safety deals with the risks arising from the system and potentially impacting the environment" (Piètre-Cambacédès and Chaudet, 2010). Common for both fields is the risk, which expresses the potential of harm, mostly stated through probability and severity. It is important, both during the system development and operations, to identify, analyse, evaluate and finally deal with as many relevant risks as possible. At the same time there are different techniques used within the fields, especially as safety deals with unintentional hazards and security with intentional threats. Even though there are distinct differences for dealing with the intentional versus the unintentional, we acknowledge that the techniques for identifying hazards and threats build on the same principles. In this paper the focus will be on what the two fields can learn from each other, in particular related to the identification of risk. The term risk is used as a collective term for both hazards and threats, as the focus is kept on techniques for risk identification (ISO, 2009). We will not include analysis of severity and likelihood when referring to the term risk, as it is a subsequent process risk identification referred to as risk analysis (ISO, 2009).

Risk identification can never be left as a straightforward activity, even when the system under assessment has low complexity and is well-known. There are no guarantees that all risks are identified, especially not when a person or a group intentionally wants to harm some assets. This might be the most significant distinction between the security and safety fields, although they can also be distinguished by considering whether the risk originates from the environment or the system, and what it impacts (Piètre-Cambacédès and Chaudet, 2010). Security deals with deliberate attacks causing the malicious risk, while safety is occupied with unintentional behavior or failures causing the accidental risk. We recognize that unintentional behavior or failures are a part of security in the sense that it might leave a system vulnerable to an attack, but at the same time it is important to be aware of the fact that harm can never happen unless somebody or something deliberately exploits these vulnerabilities. This does not mean that risk identification in the safety field is regarded as an easier task. Safety systems are often concerned with hazards related to humans and the potential consequences of harm can often be worse than those of security systems. At the same time safety systems will often have security issues, as there is potential of misusing the system to cause harm to humans as an asset. Nevertheless, the likelihood

[*] Corresponding author at: Software Engineering Department, Halden Reactor Project, P.O. Box 173, NO-1751 Halden, Norway. Tel.: +47 69 21 22 00; fax: +47 69 21 24 60.
E-mail address: christian.raspotnig@hrp.no (C. Raspotnig).

0164-1212/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jss.2012.12.002

of an attacker that deliberately wants and can exploit vulnerabilities in computer-based systems to cause lethal harm to humans is in most cases less than those of unintentional mishaps. That might be one of the reasons for security issues being ignored in the development safety critical computer-based systems. Another reason is the fact that these systems traditionally have been less networked and operated in closed networks, being inaccessible for the public.

This paper focuses on techniques applied in the process of identifying risk during the development of computer-based systems. A technique is regarded as an enabler for fulfilling certain steps in a methodology. Even though there are differences between the safety and security fields, it is apparent that they have common interest in a proactive approach for identifying and handling risk associated with the computer-based system. We recognize that risk identification cannot be totally integrated and performed as one activity for both safety and security, as the two aspects often can conflict each other and these conflicts are important to identify and analyse (Pasquini et al., 1999). However, we see the benefit of integrating the two aspects closer and that our work with assessing the techniques from the two fields can help discover how the techniques can mutually complement each other. This can supplement other work on integration of safety and security, such as (Ibrahim et al., 2004; Schnieder et al., 2010). An assessment framework helps us keep the focus on important criteria, and to obtain an overview of the current state of the fields regarding risk identification. Finally, we also provide feedback on the assessment framework itself, which will be used in the further comparison of techniques for both the safety and security fields. Part of this work originates from an industry project (Raspotnig et al., 2012b).

The paper is structured as follows. Section 2 gives the background for risk identification and discusses related work. In Section 3 the methods for selecting techniques and the techniques selected are presented. Furthermore, the establishment of an assessment framework is described, while in Section 4 the techniques are assessed with the framework. This is followed by a discussion of the assessment results in Section 5. Finally, in Section 6 conclusions and ideas for further work are presented.

2. Background

Computer-based systems alone do not pose any risk. It is when they are put in a total system context that they have the potential of contributing to hazards or threats. This applies to both security and safety, and has to be the basis for any risk assessment.

2.1. A layered view of computer-based systems

Fig. 1 shows a layered view of a computer-based system and its environment. On the right hand side of the figure the different risk-related aspects are shown as to where they arise in the layered view.

Computer-based systems and their software relate to faults, errors and failures as described by Avizienis et al. (2004), which can propagate and become hazards or threats in the total system layer (IEC, 2008). Furthermore, the hazards and threats can in worst case develop to harm in the environment (Schnieder et al., 2010; Firesmith, 2003). Schnieder et al. (2010) relate the term harm to risk for both safety and security based on ISO standards. We define these terms and their relationships as:

- Harm – is the “physical injury or damage to the health of people or damage to property or the environment” (IEC, 2008).
- Hazard – is a “potential source of harm” (IEC, 2008).
- Threat – is the “potential cause of an incident which may result in harm to a system or organization” (ISO, 2005).

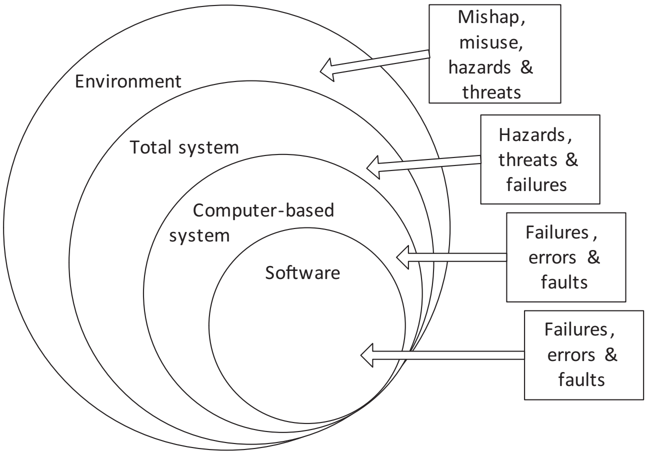
Environment
Total system
Computer-based system
Software
Mishap, misuse, hazards & threats
Hazards, threats & failures
Failures, errors & faults
Failures, errors & faults

Fig. 1. A layered view.

- Failure – is a “termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required” (IEC, 2008).
- Error – is the “discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition” (IEC, 2008).
- Fault – is an “abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function” (IEC, 2008).

Even though not shown in Fig. 1 we recognize that the total system usually consists of Man, Technology and Organisation (MTO) and that the environment is where the total system will operate. The boundary between the total system and environment can often be unclear, just as how comprehensive the environment has to be defined in the development process. Environment and total system is often collectively referred to as domain or context (Kang et al., 1990).

When performing risk identification the layers presented in Fig. 1 have to be considered. From a safety perspective harm will have to be identified in the environment in order to identify the corresponding hazards. From a security perspective it is also important to identify the corresponding harm, but another aspect also has to be considered. This is the identification of the attacker in the environment or in the total system as part of the harm. Harm has to be related to hazards and threats, both in the environment and in the total system. Furthermore, these hazards and threats have to be decomposed and related to different elements in the environment and total system. Finally, decomposition of the computer-based system and its software has to be undertaken by identifying related failures and faults as causes to hazards and threats.

2.2. Requirements elicitation and risk identification

Risk identification activities will support the security and safety requirements elicitation. However, risk identification is also dependent on the requirements elicitation activity, as this activity establishes the domain knowledge needed as input to the risk identification. Fig. 2 illustrates how the requirements elicitation activity on the left hand side generates requirements and models, which are used in the risk identification activities on the right hand side to identify hazards and threats. These are fed back to the requirements elicitation activity as safety and security requirements. In the bottom are the stakeholders, who contribute with domain knowledge as input to the activities. Note that the domain knowledge