COMPUTERS & SECURITY 72 (2018) 175–195

Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis

H. Abdo [a,*], M. Kaouk [a], J.-M. Flaus [a], F. Masse [b]

[a] Univ. Grenoble Alpes, CNRS, Grenoble INP*, G-SCOP, F-38000 Grenoble, France
[b] INERIS, Parc technologique Alata BP 2, F-60 550 Verneuil-en-Halatte, France

ARTICLE INFO

Article history:
Received 14 March 2017
Received in revised form 5 August 2017
Accepted 8 September 2017
Available online 20 September 2017

Keywords:
Risk analysis
Safety
Cyber-security
Bowtie analysis
Attack-Tree analysis
SCADA

ABSTRACT

The introduction of connected systems and digital technology in process industries creates new cyber-security vulnerabilities that can be exploited by sophisticated threats and lead to undesirable safety accidents. Thus, identifying these vulnerabilities during risk analysis becomes an important part for effective industrial risk evaluation. However, nowadays, safety and security are analyzed separately when they should not be. This is because a security threat can lead to the same dangerous phenomenon as a safety incident. In this paper, a new method that considers safety and security together during industrial risk analysis is proposed. This approach combines bowtie analysis, commonly used for safety analysis, with a new extended version of attack tree analysis, introduced for security analysis of industrial control systems. The combined use of bowtie and attack tree provides an exhaustive representation of risk scenarios in terms of safety and security. We then propose an approach for evaluating the risk level based on two-term likelihood parts, one for safety and one for security. The application of this approach is demonstrated using the case study of a risk scenario in a chemical facility.

© 2017 Elsevier Ltd. All rights reserved.

1. Introduction

Analyzing risks of industrial and complex systems such as those found in nuclear plants, chemical factories, etc., is of crucial importance given the hazards linked to these systems (explosion, dispersion, etc.) (Abdo and Flaus, 2016b). Quantifying and analyzing these major risks contributes to better decision making and ensures that risks are managed according to defined acceptance criteria (Arunraj and Maiti, 2007).

Industrial safety risk analysis aims to evaluate undesirable risk scenarios that can lead to major accidents that affect human and the environment. Traditionally, a systematic risk analysis process is made up of three steps: (i) identification of risk scenarios, (ii) likelihood analysis, (iii) effect analysis (Purdy, 2010). Based on these steps, a level of risk will be given to each scenario to see if it is acceptable or not. If not, safety measures should be added to reduce the level of risk to an acceptable level by diminishing the likelihood or the effects. This work considers the first two steps. Identifying a risk

* Corresponding author.
E-mail address: houssein.abdo@grenoble-inp.fr (H. Abdo).
https://doi.org/10.1016/j.cose.2017.09.004
0167-4048/© 2017 Elsevier Ltd. All rights reserved.

scenario aims to explore how an undesirable hazard can be developed starting from causes and ending with the consequences. Likelihood analysis aims to estimate the likelihood of occurrence of risk scenarios. This estimate can be qualitative or quantitative depending on the available data.

Traditional industries were based on mechanical devices and closed systems (Kriaa et al., 2015). Only safety related risks generated from accidental component failures and human errors need to be addressed during risk analysis of these industries. However, today, industries are influenced by the development of digital technology related to instrumentation and industrial automation (IA). Supervisory Control And Data Acquisition (SCADA) systems are introduced to monitor and control equipment that deals with critical and time-sensitive materials or events. The shift from analog equipment towards technologies has a number of benefits concerning production, but it also presents challenges (Shin et al., 2016). This introduction of automation technology increases the degree of complexity and communication among systems. The use of Internet for connecting, remote controlling and supervising systems and facilities has generated a new type of risk causes that are related to cyber-security. These systems and facilities have become more vulnerable to external cyber attacks. These new security threats can affect the safety of systems and their surrounding environments in terms of people, property, etc. (Johnson, 2012; Kornecki and Zalewski, 2010).

The differences and similarities between safety and security are studied by many authors (Firesmith, 2003; Kriaa et al., 2015). In general, safety is associated with accidental risks caused by component failures, human errors or any non-deliberate source of hazard, while security is related to deliberate risks originating from malicious attacks which can be accomplished physically (which are excluded in this study) or by cyber means. In addition, causes of accidents related to safety are internal and considered to be rare events with low frequency. Causes of security accidents can be internal or external (attacks via insider agents or outsiders) and are classified as common events.

Until today, industrial risk analysis does not take into consideration the cyber-security related risks that can affect the safety of the system and lead to major accidents. Systems are designed to be reliable and safe, rather than cyber secure. In recent years, there has been an increasing number of cyber attacks that target critical facilities (e.g., Stuxnet in 2010 and Flame in 2012). According to Dell's annual threat report (Dell, 2015), cyber attacks against SCADA systems doubled in 2014. Dell SonicWALL saw global SCADA attacks increase against its customer base from 91,676 in January 2012 to 163,228 in January 2013, and 675,186 in January 2014. Many authors have studied the potential impact of security related threats on the safety of critical facilities and highlight the importance of analyzing safety and security risks together (Kornecki and Zalewski, 2010). Thus, concerns about approaches for industrial risk analysis that consider safety and security together are a primary need.

In this paper we aim to analyze and consider the effect of cyber-security on safety risk scenarios that lead to major accidents. As a result, we propose a new global definition of industrial risk and a risk analysis methodology that covers security and safety. The proposed methodology combines Attack tree (AT) for security analysis within bowtie (BT) for safety analysis in order to provide a complete representation of a risk scenario. Then, a likelihood analysis approach with two different scales, one for security and another for safety, is introduced. The likelihood of an event is represented in terms of couples (security, safety) in order to see if higher likelihood is related to either security or safety.

It should be noted that in this study we are interested in cyber-security breaches that can lead to major hazards that have effects on human life and the environment and not on confidentiality, integrity or availability of information.

In order to present the possibilities offered by this study, the paper is structured as follows: Section 2 introduces the concepts of safety risks, security risks and the industrial automation and control system IACS. In Section 3, we highlight the global idea behind this study. In Section 4, we present the proposed methodology for a combined safety/security industrial risk analysis. In Section 5, we present a case study where the proposed methodology is applied for a hazard scenario in a chemical facility. Finally, Section 6 draws a number of conclusions.

2. Preliminary

In this section, we present the definitions of safety and security related risks (Sections 2.1 and 2.2, respectively). These two definitions will be used to generate a new global definition of industrial risk that covers safety and cyber-security related risks. Section 2.3 introduces the concept and design of the industrial automation system.

2.1. *Definition of risks related to safety*

In general, safety related risk is defined or defined as follows (Kaplan and Garrick, 1981):

$$R_{safety} = \{S_{e_i}, P_{e_i}, X_{e_i}\}; \quad i = 1, 2, \ldots, N; \tag{1}$$

where

- R_{safety} – safety related risk which is defined as a set of {};
- S_e – scenario representation of the undesirable event under study (e) by identifying safety causes of e and its related consequences;
- P_e – likelihood of occurrence of S_e;
- X_e – severity of consequences of S_e;
- N – is the number of possible scenarios or undesirable events that can cause damages.

2.2. *Definition of risks related to security*

In the context of cyber-security, risk is defined in terms of likelihood and effects of a given threat exploiting a potential vulnerability (Henrie, 2013; Stouffer et al., 2011):

$$R_{security} = \left\{(tv)_j, P_{(tv)_j}, X_{(tv)_j}\right\}; \quad j = 1, 2, \ldots, M; \tag{2}$$

where

Download English Version:

https://daneshyari.com/en/article/4955400

Download Persian Version:

https://daneshyari.com/article/4955400

Daneshyari.com