Available online at www.sciencedirect.com

ScienceDirect

Procedia CIRP 63 (2017) 207 – 212

www.elsevier.com/locate/procedia

The 50th CIRP Conference on Manufacturing Systems

Concept and Use Case driven Approach for Mapping IT Security Requirements on System Assets and Processes in Industrie 4.0

Yübo Wang[a,*], Oleg Anokhin[a], Reiner Anderl[a]

[a]Technische Universität Darmstadt, Department of integrated Design, Otto-Bernsdt-Straße 2,64287 Darmstadt

* Corresponding author. Tel.: +49 (0)6151 16 21845; fax: +49 (0)6151 16 21793. *E-mail address:* y.wang@dik.tu-darmstadt.de

Abstract

The fourth industrial revolution (Industrie 4.0) is distinguished by a growing network and intelligence of machines, products, services and data. This results in new business models and value chains, but also various risks, e.g. by hacker attacks, data theft or manipulation. Many companies consider Industrie 4.0 much as a security challenge other than an opportunity or enabler for new business models. Therefore, effective security methods to protect the Industrie 4.0 systems and its associated values and assets are needed. One of the aims of Industrie 4.0 is identifying and developing new, appropriate security practices for enterprises and especially for their production systems. Based on the connectivity infrastructure in the shop floor, the diversity in the corporate landscape of the global mechanical and plant engineering ultimately causes that every company has to develop its own way of IT and production security management.

In the context of Industrie 4.0, an integral concept is needed, that connects the requirements from manufacturing automation and mechanical engineering to process engineering with the properties of cyber-physical systems as an Industrie 4.0 component and well-established core elements of IT security descriptions. Standards from industry associations and standardization committees have to be included.

In this paper, a process model is developed, which consults RAMI 4.0 and well-established core elements of safety and IT security considering the standards IEC 61508 and IEC 62443. A use case driven approach is developed with the goal to demonstrate the functionalities and validation of the process model. In different iterations, the dynamic change of the system by mapping IT security requirements on system assets and processes will be presented. The purpose of the developed process model is to assign security measures to vulnerabilities and threats of a system for Industrie 4.0.

Keywords: Industrie 4.0; IT security; Defense in Depth

1. Introduction

The ongoing development in the field of information and communication technology continually increases the capabilities of embedded systems. Although this development enabled digitalization and mobile internet to be a natural component of personal everyday life, this way of communication and data-allocation is yet not often used in the industrial sector, especially not for manufacturing environments of small and medium-sized enterprises (SME). To empower and accelerate the adaptation of new technology for the industrial application, Industrie 4.0 was created as a significant part of the German High-Tech strategy [1]. As presented before [2,3] Industrie 4.0 targets information and communication technologies used for manufacturing to drastically increase the capabilities of current value chains.

The main factor is the communication and data-exchange between all systems. Through that kind of collaboration, a new way of production control and optimization can be achieved. On the one hand, there is an opportunity of small-scale adaptation through ad-hoc connection and data-exchange between nearby machines, on the other hand through data-allocation of specific information and real-time data for higher business levels, i.e. managers can make accurate decisions that have big scale influences [4,12]. Especially the communication beyond the borders of one particular enterprise without having the fear of exposing or losing critical and valuable information will lead to a significant overall improvement.

doi:10.1016/j.procir.2017.03.142

2. Process model for IT security in Industrie 4.0

Besides all the possible benefits, connectivity and communication between autonomous machines and cyber-physical system implicate new challenges and risks, as some good-practices are not applicable for this interconnected environment [4]. According to [5], overall security cannot be achieved by a static system design, as new vulnerabilities and weak points arise and become targets of attackers. Therefore, IT security of a system is a property that has to be analyzed and evaluated continuously.

This ongoing process presents the industry with significant challenges. Especially SME in the manufacturing sector lack the necessary competencies and manpower to establish secure and evolving processes and to manage the complexity while at the same time facing the technological challenges of Industrie 4.0 [11,12,13]. To support the development and implementation of interconnected and autonomous systems for SME, concepts for introducing Industrie 4.0 [17] and introducing IT security have to be simplified and if possible automated.

In [6] a combined secure process and data model for IT security in Industrie 4.0 was presented (Fig. 1). This process model is designed to meet the requirements of manufacturing automation, mechanical engineering, process engineering and the properties of cyber-physical systems under the consideration of five main fields of requirements [6]:

- Diversity of systems and processes (R1)
- Defense in Depth strategy (R2)
- Threat analysis and risk assessment (R3)
- Application-specific security solutions (R4)
- Usability (R5)

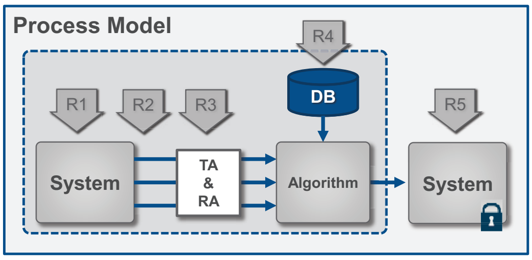

Fig. 1. Process Model [6]

This approach provides a simplified model for SME, which accepts a current system used in the enterprise as input and provides a semi-automated threat and risk analysis. The results of this analysis are committed to an algorithm that semi-automatically chooses appropriate security measures to minimize the risk and improve or eliminate the weak points of the current setting. Core component of this process model is a database, where all significant information about system components, possible threats, previous attacks and applied measures are stored. This kind of information has to be provided by independent security experts, who can provide the necessary maintenance and updates as well as the correlation between new vulnerabilities and security measures accordingly for the algorithm to choose from.

As we consider the database in this process model to be generic, a standardized or at least formalized input is required for the algorithm to work properly and generically for different types of systems. As a result, the algorithm delivers a formalized representation of the improved system that contains the chosen security measures.

3. Formalized representation in the process model

In the long view, Industrie 4.0 initiatives need to assimilate IT security as one of the key design characteristics. To unfold the full potential the possibilities and benefits of Industrie 4.0 applications, on the one hand, resilient and trusted cyber-physical machines have to be developed at the system level [3,15,16]. On the other hand, the challenge is to address on the technology level the topics of secure networks, secure processes, secure services, and secure data – depending on the requirements each system and the process has [3,14].

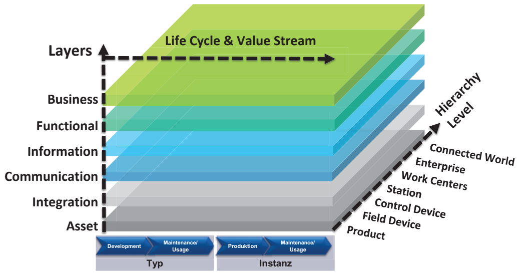

Fig. 2. RAMI 4.0 [7]

Consequently, the Reference Architectural Model Industrie 4.0 (RAMI 4.0) is the necessary common reference point for any system modeling (Fig. 2). RAMI 4.0 is consulted and reflected as the initial system in the developed process model regarding the requirements of diverse systems and processes in Industrie 4.0. In addition, approaches to Standards and IT security design and strategy is also referred to the developed process model to fulfill the assimilation of IT security in Industrie 4.0 and the additional requirements R2, R3 and R4.

3.1. Reference Architecture Model Industrie 4.0

RAMI 4.0 consists of several layers, hierarchical levels and the lifecycle including value chain. This structure is shown in Fig. 2. The hierarchical levels consist of seven levels: product, field device, control device, station, work centers, enterprise and connected world, from bottom to top. All Industrie 4.0 components have the same structure for all hierarchy levels. Each component consists of six layers. Starting with the lowest layer, the structure consists of Asset, Integration, Communication, Information, Functional and Business. The third axis describes the life cycle and the value chain of an