Trustworthiness requirements for manufacturing cyber-physical systems

Radu F. Babiceanu*a, Remzi Sekera

aDepartment of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University
Daytona Beach, FL 32114-3900, United States

Abstract

Distributed manufacturing operations include cyber-physical systems vulnerable to cyber-attacks. Long time not considered a priority, cybersecurity jumped to the forefront of manufacturing concerns due to the need to network together legacy, newer equipment, and entire operation centers. This paper proposes trustworthiness solutions for integrated manufacturing physical-cyber worlds, where trustworthiness is defined to complement system dependability requirements with cybersecurity requirements, such that the resulting manufacturing cyber-physical system delivers services that can justifiably be trusted. Acknowledging the inevitability of cyber-attacks, the paper models the cybersecurity component using the resilient systems framework, where system resilience is viewed as preservation of a required state of cybersecurity.

© 2017 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Keywords: cyber-physical systems; trustworthiness requirements; manufacturing cybersecurity; system resilience; denial of service

1. Introduction

The current manufacturing worldwide operations trend imposes the presence of all established requirements in terms of manufacturing design processes and actual operations, combined with an increased safety and flexibility of
operations. In addition, it requires the presence of more recent cybersecurity protection of electronic transactions between distributed operation centers [1].

The high-tech progress in material science research, and the information and communication technologies made the development of manufacturing cyber-physical systems a reality. Not only physical facilities can be linked together through network applications and coordinate their applications, but also physical operations can be simulated in real-time in cyber centers. The resulting benefits are significant, and to name a few, cyber-physical coordination leads to reduced raw material used in testing, prototyping, and actual operations, as well as increased safety of finished products [2]. Moreover, the manufacturing cyber-physical systems include a wide range of sensing devices and data processing capabilities that can provide online monitoring of manufacturing processes, thus further reducing the chances of scrapped lots and increasing the safety of the actual manufacturing operations, through production abort commands, whenever hazardous events, or out-of-specifications environment conditions are detected [3].

Since all good things come with a price tag, the path towards manufacturing cyber-physical systems has one of its own. Just as all other network-based or Internet-based systems, cyber-physical distribution of manufacturing operations include systems vulnerable to cyber-attacks. Long time not considered a priority, cybersecurity jumped to the forefront of manufacturing concerns due to the need to network together legacy, newer equipment, and entire operation centers. Many of the legacy operations are controlled by Supervisory Control and Data Acquisition (SCADA) systems that automatically monitor and adjust process control activities and control physical pieces of equipment [4, 5]. However, many SCADA systems were designed and built in the 1980s without any regard of cybersecurity. Recent research discusses also the need to network traditional stand-alone equipment such as PLC-controlled and CNC machines, which were never designed with any control measure for data security. The newer systems have their cybersecurity problems of their own, as many of the Internet of Things devices embedded on physical manufacturing equipment, such as sensors and data processing and communication hardware, are reported to be easily hacked and become the port of entry for intruders to the manufacturing network data centers [6, 7].

Given all the above issues, within the manufacturing and cybersecurity fields, the capability of virtualized manufacturing operations to prevent, respond, thwart and/or recover from cyber-attacks is now becoming an active area of research.

This paper proposes trustworthiness solutions for integrated manufacturing physical-cyber worlds, where trustworthiness is defined to complement system dependability requirements with cybersecurity requirements, such that the resulting manufacturing cyber-physical system delivers services that can justifiably be trusted. System dependability, traditionally, includes operational availability, reliability, safety, and maintainability requirements, which can only be enhanced by the advancement of cyber-physical systems in manufacturing operations. Cybersecurity includes aspects such as confidentiality, integrity, availability, authenticity, and assurance of data transactions and/or computer systems, and to a lesser extent anonymity of data records and transactions. Acknowledging the inevitability of cyber-attacks, this paper models the cybersecurity component using the resilient systems framework, where system resilience is viewed as preservation of a required state of cybersecurity [8, 9].

From this point forward, the paper is structured as follows. Section 2 presents the trustworthy manufacturing cyber-physical model, with its dependability and cybersecurity requirements, and introduces the concept of system resilience in the face of cyber-attacks. Next, Section 3 provides insights for the cyber-resilience mechanisms through simulation modeling. The paper concludes with a brief section summarizing the importance of cybersecurity adoption within manufacturing domain and a discussion related to needed further investigation of manufacturing cyber-physical systems.

2. Trustworthy Manufacturing Cyber-Physical Systems

Previous authors’ work identified the framework for the development of manufacturing cyber-physical systems, emphasizing aspects such as complex event processing, virtualization, Internet of Things adoption, Big Data analytics, and cyber-attacks targets and vehicles [1-3]. This current work goes further into modeling aspects by adding to the mix traditional operational requirements such as availability, reliability, safety, and maintainability, many times known as system dependability, and detailing cybersecurity protection mechanisms.
دریافت فوری متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات