Computers in Industry 97 (2018) 132–145

Contents lists available at ScienceDirect

Computers in Industry

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

Security framework for industrial collaborative robotic cyber-physical systems

Azfar Khalid[a,b,*], Pierre Kirisci[b], Zeashan Hameed Khan[d], Zied Ghrairi[c], Klaus-Dieter Thoben[b,c], Jürgen Pannek[b,c]

[a] Department of Mechanical Engineering, Capital University of Science & Technology (CUST), Islamabad Expressway, Zone-5, Islamabad, Pakistan
[b] University of Bremen, Bibliothekstraße 1, 28359, Bremen, Germany
[c] BIBA-Bremer Institut für Produktion und Logistik GmbH (BIBA), Hochschulring 20, 28359, Bremen, Germany
[d] Department of Electrical Engineering, Bahria University, Shangrilla Road, Sector E-8, Islamabad, Pakistan

ARTICLE INFO

Article history:
Received 16 February 2017
Received in revised form 12 January 2018
Accepted 22 February 2018
Available online xxx

Keywords:
Cyber physical production system
Cyber security
Human-robot collaboration

ABSTRACT

The paper introduces a security framework for the application of human-robot collaboration in a futuristic industrial cyber-physical system (CPS) context of industry 4.0. The basic elements and functional requirements of a secure collaborative robotic cyber-physical system are explained and then the cyber-attack modes are discussed in the context of collaborative CPS whereas a defense mechanism strategy is proposed for such a complex system. The cyber-attacks are categorized according to the extent on controllability and the possible effects on the performance and efficiency of such CPS. The paper also describes the severity and categorization of such cyber-attacks and the causal effect on the human worker safety during human-robot collaboration. Attacks in three dimensions of availability, authentication and confidentiality are proposed as the basis of a consolidated mitigation plan. We propose a security framework based on a two-pronged strategy where the impact of this methodology is demonstrated on a teleoperation benchmark (NeCS-Car). The mitigation strategy includes enhanced data security at important interconnected adaptor nodes and development of an intelligent module that employs a concept similar to system health monitoring and reconfiguration.

1. Introduction

Future industrial manufacturing systems are most likely based on the cyber-physical production systems (CPPS) to produce smart products with larger flexibility [1–3]. This intelligent manufacturing concept evolved from the collaborative cyber-physical system (CCPS) definition in which integration of physical and computational components result in sensing and control of state variation in real world parameters [4,5]. Such a system is comprised of the physical hardware, sensor network as well as information, computer and communication technologies with human machine interface (HMI). These infrastructures provide technological challenges and foster new interaction opportunities for humans with equipment, machines and tools in the environment. CPS integrates computation and physical processes to optimize resource usage and system performance. These systems can be connected to the internet or an external secure network [6]. The physical hardware can be a robot, actuators or a manufacturing plant and can be termed as the physical component (PC) in the CPS. The cost of the physical component can be very high and varies from one application area to the other [7].

For smooth functioning of such collaborative robotic system, a secure CPS is required in order to protect highly sophisticated and costly physical elements [8]. The security of such systems can be compromised by cyber-attacks through the network or internet connectivity [9]. It is certain that such attacks enter the CPS through the cyber component (CC) and hit the PC (Industrial computer, PLC, robot etc.) which is mainly controlled by the CC. The increased connectivity to external networks is a threat to the security of CPS [10]. If attackers develop means to enter the control systems and modify the system behavior, this may cause irreversible damage to the PC. Cyber attacks on IT systems has resulted in the evolution of anti-virus shields for the security of computer networks [11,12]. The CPS domain is different in this context as the security of an IT system only serves the CC and there is no mechanism in it to protect PC. Moreover, the causal effect of cyber-attacks from cyber layer all the way to the PC is inherent. In

* Corresponding author at: Department of Mechanical Engineering, Capital University of Science & Technology (CUST), Islamabad Expressway, Zone-5, Islamabad, Pakistan.
E-mail address: azfar.khalid@cust.edu.pk (A. Khalid).

https://doi.org/10.1016/j.compind.2018.02.009
0166-3615/

this context, development of mitigation plans against such intelligent cyber-attacks is a novel area of research. It involves identification of novel frameworks for analyzing the cyber-attacks on CPS [13–15].

The most important aspect regarding the security of a CPS is the design knowledge of a cyber-attack. The critical aspect of an effective mitigation plan for the security of CPS is to know the structure of such a cyber-attack. To study this, a number of cyber-attacks were designed against CPS components, and its effects on cyber, physical and collaborative control components were evaluated. Stuxnet [16] and Aurora attack [17], have created awareness and widespread concerns about physical infrastructure damage through cyber-attacks. As stated, existing security measures were mostly developed for cyber-only systems and they cannot be effectively applied to CPS in a collaborative network directly. Therefore, new approaches to prevent CPS failure are necessary. The difference in the properties of physical and cyber layers within CPS has made the interface a very important node where cyber components render a large variety of attacks possible. In contrast to that, the PC are inflexible and simple with relatively low possibilities of attacks.

Security features in networks [18] are essential for the protection of key infrastructure. For today's industrial control systems, new intelligent network architectures [19] are an essential requirement. The present research aims to develop an industrial security framework for safe and secure human-robot collaboration (HRC) in an industrial connected manufacturing environment [20], known as 'Collaborative Robotic Cyber-Physical System' (CRCPS) [21]. There is an increasing interest in industrial customers of 'collaborative robot manufacturers' dealing with automatic and semi-automatic assembly processes in leveraging their assembly processes to a stage to enable seamless human-robot-collaboration. This is particularly valid for semi-automatic processes in the automotive industry which are characterized by the fact that some tasks are done manually by the human worker. The security of network in the industrial CRCPS is crucial as this system is aimed to avoid any critical life threatening situation for the worker working with the heavy payload industrial collaborative robots. In addition to worker safety, it is imperative that important information within CRCPS remain secure and must not be compromised due to a malicious attack [22]. The secure CPS must have the ability to determine the accountability of human workers while maintaining their safety and privacy. The problem becomes complex due to the increasing interactions in the modules of CPS and also due to the increasing complexity of the design of cyber-attacks. Raya et al. [15] classified cyber-attacks based on three dimensions. These attributes are related to the type of attacker as insider or outsider to the system, attacker's aims and objectives and the attack mode with which the attack is launched. An active mode attacker attempts to disturb the CPS node availability and authentication and directs the attack towards physical damage, whereas passive mode attack retains itself in the network to extract valuable system level and control information like a reconnaissance mission [23]. By avoiding information from untrusted senders and by constructing a trust network, the secure CPS network can reduce the threat. The untrusted sender can be a sensor already under cyber-attack that is sending misleading information.

This research paper focuses on the CPS components and the interfaces connecting different components specifically at the interactive nodes of physical and cyber components. The architecture is developed on a module based defense strategy framework and by securing the interfaces. In this paper, we are proposing a systematic solution of intelligent secure physical modules to prevent cyber-tempted physical destruction even when the cyber layer is compromised. In this context, self- secured intelligent adaptors are employed between physical and cyber components that preserve the prevailing reliability in control and data flow. A decentralized architecture approach is adopted for the CRCPS structure so that the system may not have a single node of failure that an attacker can mark. However, against such architecture, the foe attacks sub-systems, and the security model design has to include the interdependent interactions between modules.

In this paper, Section 2 introduces the CRCPS technological components and a CPS structure. The CPS structure further supports the development of a novel framework to safeguard CRCPS against (incoming intelligent) cyber-attacks. Section 3 deals with the concepts of cyber-attack on CPS, the differences of cyber-attack mechanism on an IT system, CPS in general and a special case of CRCPS. Section 4 discusses the attack properties in different layers and a categorization of attacks in the context of possible effects on CRCPS is explained. Section 5 reveals the mitigation plan of the proposed framework for a secure CRCPS and a safeguard against the physical objectives of an intelligent cyber-attack. Section 6 demonstrates a teleoperation benchmark to show the effectiveness of the strategy by simulating a distributed denial of service (DDOS) attack on the NeCS-Car communication network. Section 7 concludes the paper by identifying the strengths and weaknesses of the proposed strategy.

2. Collaborative robotic CPS

The HRC for a given industrial scenario is suggested by exhibiting safe interaction without any fencing. This application area in CPS research is a perfect example where safety and security, are integrated and need to be addressed in the CPS architecture [24]. The merger of security and safety issues in the CRCPS design is similar to the concept followed in the design and risk assessment of industrial facility and control that reflect both facets [14]. Security is closely associated with safety as both of these characteristics have to be addressed synchronously. The safety aspect tangibly guards industrial workers against the machines whereas security shields the systems from persons as foes.

Based on such integrated approach, technology selection for such a system can have multiple challenges. As an example of HRC, a speed or separation monitoring collaborative system is illustrated in Fig. 1. The concept employs several networked integrated sensors and the HRC is taking place in the area under monitoring for accomplishing an industrial task. In the collaboration type of speed and separation monitoring, the system incorporates cameras or other sensors for the real-time worker positioning. Moreover, robot speed is reduced or a probable break is applied in the case, the operator move in the hazardous area. The overhead cameras are installed to track the real-time human position with the help of markers. A laser scanner or a light curtain can be installed to cover any violation of monitored area and to signal the robot for human presence. Additionally, there is another system for human location signature acquisition through the inertial sensors. The operator has to wear a vest (or a body suit) during collaboration that comprises of several IMU built-in at different body positions, so providing rate and position data to the CRCPS. Gyro sensor data is communicated through a safe protocol to the physical and cyber components for further real-time analysis and decisions made are then rerouted into the system. The IMU fitted helmet for head position and rate data is another device used for a similar purpose.

As the basic aim for the development of CRCPS is to maintain worker safety while HRC is in operation, we assume a safe HRC system is in place. Detailed safe HRC system requirements, CPS structure, safety classifications, industrial scenarios and development methodology are studied for CRCPS in [10,25]. Here, we