

Understanding vulnerabilities in cyber physical production systems

Azfar Khalid, Zeashan Hameed Khan, Muhammad Idrees, Pierre Kirisci, Zied Ghrairi, Klaus-Dieter Thoben & Jürgen Pannek

To cite this article: Azfar Khalid, Zeashan Hameed Khan, Muhammad Idrees, Pierre Kirisci, Zied Ghrairi, Klaus-Dieter Thoben & Jürgen Pannek (2021): Understanding vulnerabilities in cyber physical production systems, International Journal of Computer Integrated Manufacturing, DOI: [10.1080/0951192X.2021.1992656](https://doi.org/10.1080/0951192X.2021.1992656)

To link to this article: <https://doi.org/10.1080/0951192X.2021.1992656>



© 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.



Published online: 28 Oct 2021.



Submit your article to this journal [↗](#)



View related articles [↗](#)



View Crossmark data [↗](#)

Understanding vulnerabilities in cyber physical production systems

Azfar Khalid^a, Zeashan Hameed Khan^b, Muhammad Idrees^b, Pierre Kirisci^c, Zied Ghrairi^d, Klaus-Dieter Thoben^{c,d} and Jürgen Pannek^{b,c,d}

^aDigital Innovation Research Group, Department of Engineering, School of Science & Technology, Nottingham Trent University, Clifton, Nottingham, UK, NG11 8NS ; ^bDepartment of Mechatronics and Biomedical Engineering, Air University, Islamabad, Pakistan; ^cUniversity of Bremen, Bibliothekstraße 1, 28359, Bremen, Germany; ^dBIBA-Bremer Institut Für Produktion Und Logistik GmbH (BIBA), Hochschulring 20, 28359, Bremen, Germany

ABSTRACT

Development of future manufacturing systems is featured with flexibility, mass customization, intelligence and context based learning to produce smart products. These production systems are characterized through networked, cooperating objects called cyber physical systems (CPSs). From the manufacturing perspective, the ability to communicate data and develop interaction between devices, manufacturing machinery, raw materials, working robots, humans and the plant environment develops the concept of cyber physical production systems (CPPS). Human-robot collaboration is a technology area that will be an integrated part of the future factory floor and the CPPS. With the involvement of human part in the automated system industrial scenarios, practical safety issues are expected to arise in the connected environment due to the use of a large number of devices, sensors, and cloud services causing complex network, IP conflicts, compromised nodes and communication issues. This all may lead to occupational safety issues on the factory floor in different ways and combinations. Overall, the system's physical vulnerability will be increased in the context of compromised connected working space and cyber-security. In this paper, the authors developed a risk assessment based on system vulnerability of a CPPS developed for a use case requirement and performed a simulated approach by launching a cyber-attack and measuring the causal effect to identify implications on human worker safety.

ARTICLE HISTORY

Received 15 September 2020
Accepted 8 October 2021

KEYWORDS

Human robot collaboration;
industrial safety and security;
cyber physical production
systems

1 Introduction

System flexibility is the key in the future manufacturing systems to deliver flexibility in products, generally known as mass customization. Many new technology domains are being integrated in manufacturing to support such systems, which include Internet of things (IoT), cloud computing, sensor networks, cyber physical systems and big data analytics (Gonçalves, de Araujo, and Corazzim 2020). The merger of these ICT technologies in manufacturing enables the system to predict properties in operation, maintenance, product design variation and logistics (Zhang, Yan, and Zhenghua 2020). These futuristic systems are proposed for system flexibility enabling high productivity of customized products and further technology areas to evolve in the umbrella of Industry 4.0. Advanced robotics is also an integrated technology in the future manufacturing systems in which the flexibility of artificial intelligence and positioning accuracy of the robots can be beneficial for the

industrial manufacturing systems (Thames and Schaefer 2017). For this reason, the workspace envelope of robots is expected to rise in future smart factories. These self-learning, self-decision-making manufacturing systems and robots may limit the future industrial roles for the humans to some extent. It does not mean that the human absence is the future of the manufacturing systems. Human presence would be inevitable but is restricted to supervisory roles on the shop floor working closely with the robotic counterparts (Khalid and Khan 2014). This has led to the evolution of technologies like human-robot collaboration (HRC) in an industrial scenario. Many industrial robot developers have already built collaborative robots or cobots with flexible capabilities to support manufacturing tasks.

There are almost one million non-collaborative robots installed in the industry worldwide (Knight 2014). Replacement of present-day conventional robots with the newly developed cobots needs

CONTACT Azfar Khalid  azfar.khalid@ntu.ac.uk  Department of Engineering, School of Science & Technology, Nottingham-Trent University, NG11 8NS, Nottingham, UK

© 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

a huge amount of investment by the manufacturing industry (Khan, Khalid, and Iqbal 2018). On the other side, new manufacturing processes or assembly lines can easily be designed to work with cobots and possess a lot of revenue potential for cobot manufacturers (Stadnicka and Antonelli 2019). In order to save the huge replacement cost, there is a development opportunity to transform the conventional robots into intelligent cobots using the integrated working environment of the interconnected sensor network, communication system, data fusion and other technologies (Ore et al. 2020). However, due to worker safety issues, the transformation of conventional robots to cobots is more feasible in small and medium scale payload robots (Weippl and Kieseberg 2017). In order to develop such an interconnected system, a cyber physical system (CPS) is envisaged to incorporate requirements of sensors, safety, security, communication and electronics. It is noted that successful transformation in medium scale robotics will trigger research effort in the case of heavy payload robots to enable collaborative tasks (Khalid et al. 2016; Lasota, Rossano, and Shah 2014).

There are many cobot examples that are developed to work with human workers and have appropriate safety certifications (Knight 2014; Collaborative Robotics Market Exceeds US\$1 Billion by 2015). These are mostly medium payload (0.5 to 14 kg) cobots developed for mobile phone and electronics manufacturing. The regular features of the cobots are human worker avoidance, speed reduction upon violation of workspace, collision detection and instant hold upon collision and the programmable compliance that they can be trained quickly for different jobs on the shop floor (Tsarouchi et al. 2017). There are safety and protection measures that need to be implemented for a cobot-human shared work cell

according to the ISO 15066–2016 (ISO 2016). However, the safety and security (protection) requirements in the case of heavy payload cobotics are still in the infancy stage (Prinsloo, Sinha, and Basie von 2019). Human robot collaboration (HRC) is discussed in (Stadnicka and Antonelli 2019), but no safety/security aspect is analyzed, in case of fault. Similarly, in another research, body gestures are utilized for HRC in an automotive assembly line jointly instrumented by robots and humans assuming fault-free scenario (Tsarouchi et al. 2017).

The present research focuses on the development of CPS in which conventional robots or cobots are connected with the intelligent manufacturing environment. Together with the other intelligent plant modules, the cyber physical production system (CPPS) (Khalid and Khan 2014; Pirvu, Zamfirescu, and Gorecky 2016; Monostori 2014) is composed of the necessary communication and sensor network, the cyber component (CC), physical component (PC) and the human component (HC). The HC integration is an extension in the initial conceptual framework of CPPS in which different adaptors (HMI technologies, gesture control, tracking sensors) have made it possible for production employees to be part of the CPPS (Uhlemann, Thomas, Lehmann, and Steinhilper 2017). In the future manufacturing systems, there will be a seamless integration of humans and machines and passive safety fencing will be removed (see Figure 1). The increased level of connectivity in future manufacturing systems (CPPS) will affect the concepts of safety and security. Safety and security (Plósz, Schmittner, and Varga 2017) are both system level properties and must be considered concurrently. As safety physically protects humans from the systems, the security essentially protects the systems from humans as attackers (Rehman et al. 2020). Cyber-

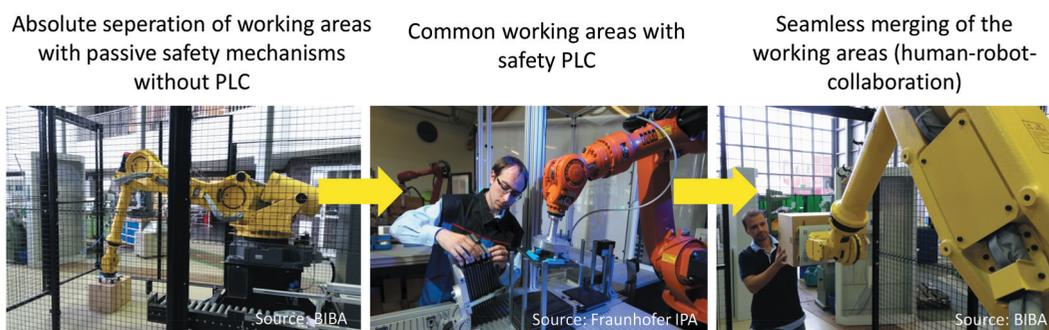


Figure 1. Human–robot interaction in cyber-physical work environments.

attacks as a safety threat in joint tasking by a human co-worker and cobot in the present framework is a novel analysis for the assessment of vulnerability in CPPS. This analysis will be helpful in ensuring reliability in future automated industrial manufacturing.

In this paper, the objective is to systematically identify the risk sources and highlight hazards from the integrated safety and security aspects. The considered heavy payload robot is installed in an automobile manufacturing plant as a vital physical module and works intelligently by developing an external CPPS that enables it to exhibit HRC. The outcome of the paper may contribute towards the development of future HRC capable of integrated manufacturing systems in the context of Industry 4.0. The next section of the paper introduces a use case of an assembly scenario in the automobile industry proposed for an active HRC. The third section explores the CPPS model for the use-case and the technology requirements according to the designed framework. The fourth section investigates risks based on the integrated concepts of safety and security in a CPPS. [Section 5](#) considers the simulation benchmark based on KUKA youBot and two-conveyor platform to study the system vulnerabilities based on the identified risks due to cyber-attack resulting in compromised safety and failure issues. [Section 6](#) concludes the discussion and findings.

2. Use case

Traditional work environments lack the ability to respond intelligently to adapted processes and therefore do not allow dynamic modifications. While this leads to new and improved ways of interaction and collaboration, it places challenges on safety and protection systems. Contemporary protection systems separating the worker from the machine (e.g. through safety fences; see [Figure 3](#)) pose a serious limitation for realizing an efficient HRC. Context-based systems are required, which have to provide active, integrated and omnipresent protection for the human worker. The CPPS work environment needs real time adaptation to situations and working conditions. This is an



Figure 2. The assembly scenario (courtesy of thyssenkrupp System Engineering).

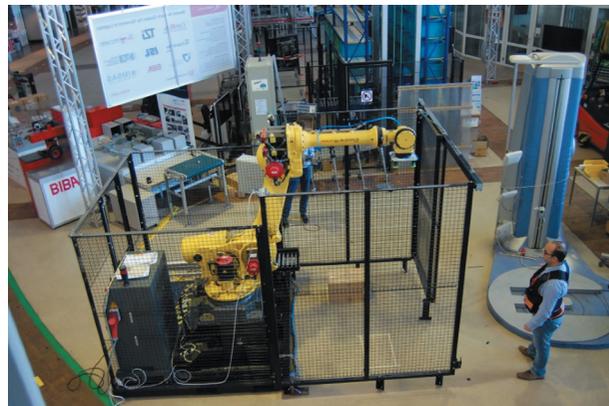


Figure 3. Conventional heavy payload robot as PC in CPPS (passive safety measures to be removed).

active protection concept in addition to the passive protection of injury avoiding construction of robots and machines.

As a representative industrial HRC scenario, an assembly process from the automotive industry is chosen, as shown in [Figure 2](#), where the workspace of an industrial robot and a human worker substantially overlap. The tasks are related to the assembly of motors and gear drives. Under consideration of customer requirements, several potential assembly scenarios were identified. These were analyzed according to qualitative criteria and weighting and thus were narrowed to eight scenarios. The eight scenarios were subject to a task and cost analysis in order to highlight which of the processes possess the highest economic potential.

In this manner, a semi-automatic assembly process focusing on motor and gear drive assembly is chosen.

Table 1. Detailed phases of the assembly scenario.

No.	Operation sequence
1	Workpiece in the workpiece carrier is moved discontinuously on the conveyor belt and moved to the default position.
2	Robot removes the workpiece from the workpiece carrier by clutching it with gripper.
3	Robot moves the workpiece into the assembly position.
4	Workman removes the assembly component cover from the default position.
5	Workman positions the assembly component cover on to the workpiece.
6	Workman removes assembly component screws at the default position and moves them to the assembly position.
7	Workman mounts the assembly component screw on the assembly component cover and workpiece.
8	Robot moves the assembled workpiece to the pneumatic screw driver.
9	Pneumatic screw driver tightens (screws on) the assembly component cover and assembly component screw to the workpiece.
10	Robot moves the workpiece to the workpiece carrier and gripper declamps the assembled workpiece.
11	Robot moves to the default position.

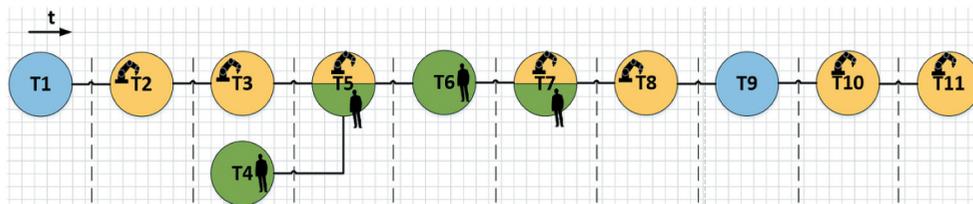
The main advantage of this particular process lies in the fact that the type and sequence of the tasks significantly comprised of the generalized assembly processes in manufacturing. This process is an exemplary HRC reference scenario, which is based upon the semi-automatic assembly of the seal ring upon an automobile motor. A heavy payload robot with a gripper lifts a motor from a workpiece carrier. The motor is then forwarded to the assembly worker and presented in an ergonomically convenient position. The task of the assembly worker consists of screwing on a seal ring on the front end of the motor with a pneumatic screwdriver. This process step can be considered as the intermediate HRC (Khalid et al. 2016), since the working areas of the assembly worker and the robot overlap synchronously. The robot is supposed to reduce its speed in the presence of trackable production employees and present the workpiece to the worker for further operation. Table 1 shows the detailed operation sequence of the representative scenario. Figure 4 shows the phase wise HRC identification for better understanding of the process.

It is clear that HRC is exhibiting at two collaborative phases (T5, T7) out of the 11 phases marked as separate activities in the process.

3. Cyber physical production system model

To develop an effective HRC system, a continuous speed or distance monitoring between the human and robot is a way that is combined with the context of the work setup. From this industrial assembly scenario, technical measures can be derived for the appropriate behaviour of HRC safety systems. It became evident that the minimum safety distance within the HRC scenario should be incorporated when choosing the appropriate CPPS components (Khalid et al. 2017). It has been shown that the integration of virtual commissioning (VC) for CPS-based HRC is an excellent complimentary technique for accompanying the realization of HRC safety concepts and thus for evaluating the functional-safety and interoperability of CPPS components. However, there is a need of more sophisticated data models for describing and visualizing the behaviour of a CPPS-based industrial scenario. For example, the integration of real sensor data from motion tracking systems is possible in visualization tools, which are suitable for VC. In this respect, it has to be noted that in HRC settings, the HC is a vital part of the CPPS in addition to the other technical components.

In the basic CPS definition, [shown in Figure 5(a)], it is evident that it is a smart system in which the computational and physical systems are integrated to control and sense the changing state of real-world variables (Sunder 2012). However, the extended CPPS concept [shown in Figure 5(b)] involves the vital HC interaction with other components of the CPPS to exhibit HRC. There are certain adaptor technologies playing an important role between the main components of the CPPS. These adaptors work according to the industrial scenario

**Figure 4.** The assembly scenario – phase-wise HRC identification.

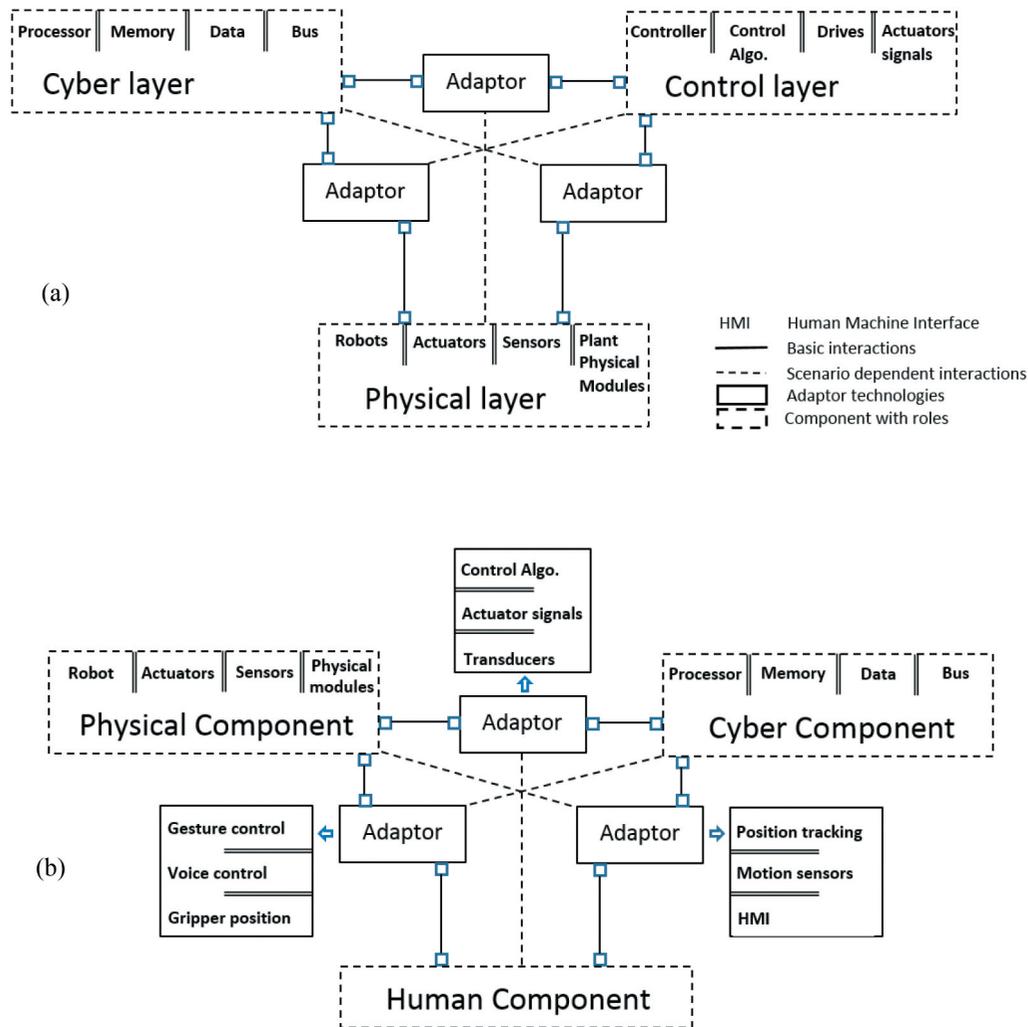


Figure 5. (a) Basic CPS definition. (b) CPPS framework for HRC (legend given is common).

requirement. Figure 6 shows different adaptor technologies in order to work out the safe HRC. For instance, a human worker is equipped with a body suit and helmet that comprised of the motion tracking devices.

A physical research demonstrator of this HRC representative scenario has been implemented with off-the-shelf components. The demonstrator consists of a heavy payload robot from FANUC (R-2000iB 165 F), a robot controller (R30iA), an industrial PC (Siemens) with ProfiNet/ProfiSafe interfaces, as well as two safety laser scanners (SICK S3000), two HD cameras and a wearable 3D motion capturing system. The concept of the demonstrator relies upon a sensor framework, which enables the ad-hoc integration of potential cyber-physical components, whereas the sensor data is collected and sensor fusion takes place in the environment of the industrial-PC. The

laser scanner detects the human presence in the robot cell, whereas the two overhead HD cameras cover the visual surveillance of the cell. The human worker signature is recorded by the inertial measurement unit (IMU) fitted bodysuit, which is a must wearable in this case and communicates data wirelessly to the server. For this purpose, the hardware components such as PLC and sensors are coupled with the simulation environment (hardware-in-the-loop), and robot control and sensor data are used within the simulation for safety distance computation, implementation of human avoidance algorithm and speed reduction upon detection, thereby controlling the system through the cyber component of the CPPS.

Moreover, to verify the industrial HRC scenario in the case study, i.e. only phase numbers 5 and 7 in Figure 4, the virtual commissioning is carried out to test the effectiveness of human avoidance algorithms

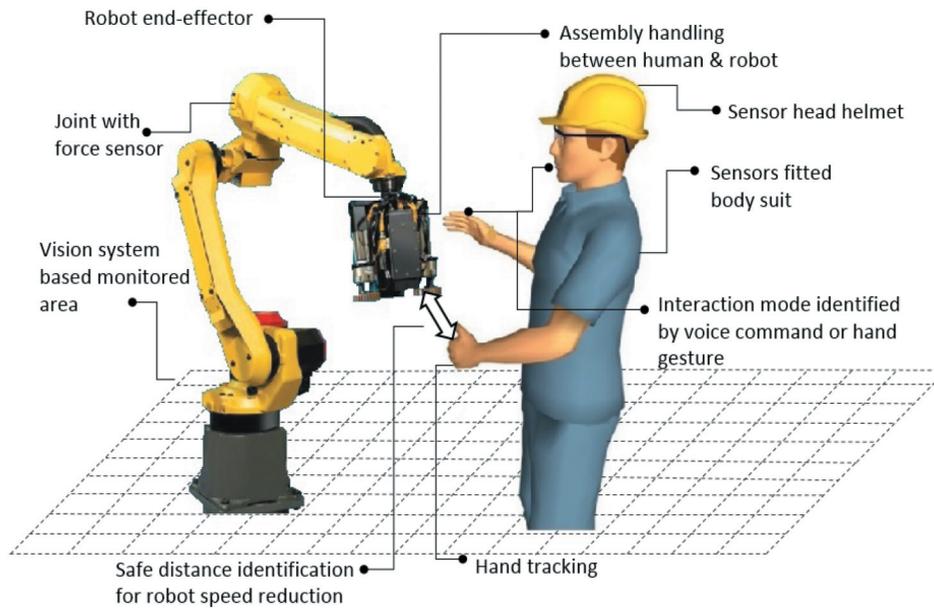


Figure 6. HRC adaptor technologies involved for transforming conventional robots.

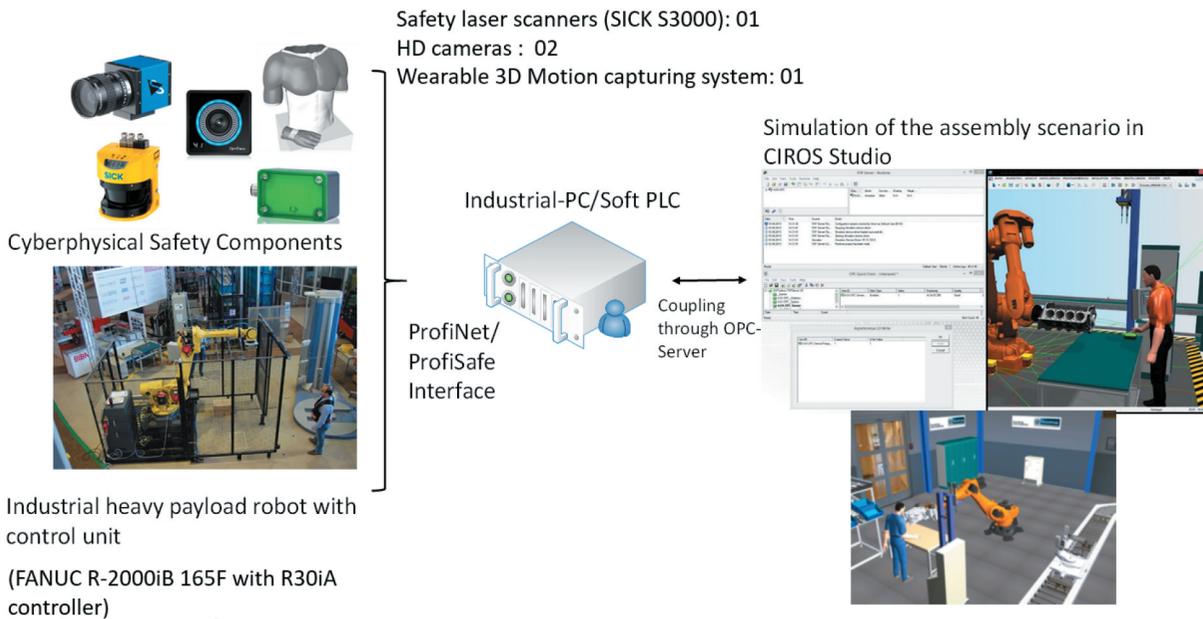


Figure 7. Demonstrator along with virtual commissioning visualization including sensors and communication protocol.

based on the real time safety distance calculations. Figure 7 shows a visualization window for the assembly process and to study safety issues in real time. It is clear from the sequence of operation that a semi-collaborative process is followed in which a heavy workpiece block is presented to the production

employee for further installation of small items on the block. It is necessary for the robot to hold the workpiece for the complete duration of the task and put it back safely to the initial position after the task is finished. The system also has manual control adjustments as the robot position is locked in that case for

an unlimited time unless the manual push button is triggered by the worker to start the next process sequence.

4. Risk identification

Factories of the Future (FOF) represent demonstrative infrastructures, which highlights the fourth industrial revolution strategy implied by 'Industry 4.0'. These environments are characterized by interconnected cyber-physical components. These infrastructures provide technological challenges regarding security and interoperability and, additionally, foster new interaction opportunities for humans with equipment, machines and tools. HRC is a descriptive paradigm and comprises a manifold of technological challenges. As such, an increasing number of industrial customers of this industrial domain dealing with automatic and semi-automatic assembly processes are highly interested in leveraging their assembly processes to a stage to enable seamless HRC.

The challenges related to an industrial HRC scenario are manifold from a technical point of view but uniquely address the safety and security aspects. On one hand, the CPPS is designed to meet a single objective of 'CPPS-safety', but on the other hand, 'CPPS-security' is also an equally vital issue to comprehend. Mitigation approaches for CPPS-security challenges seriously lack the ability to detect and actively react to the cyber-attack that can advance without restriction once the cyber layer is compromised. Currently, all the development focus is on the design side of intelligent security cyber-attack that includes the penetration enhancement of such

attacks through in-depth understanding of the target (CPS) control system (Tuptuk and Hailes 2018). Figure 8 shows a list of potential attack methods, targets, effects and interdependencies between the different CPPS layers.

A CPS possesses different system layers, and thus, potential attacks are executed at targets placed at diverse system layers. Due to the great amount of reliance and interdependencies amid CPPS components at different strata, ancillary effects can follow at CPPS elements, which have not been openly confronted. These prompted effects can happen at components placed in diverse layers or even linking to different (cyber or physical) domains. Such cross-layer and cross-domain assaults on CPPS are very complicated and hardly understood so far.

The selection of technology for the implementation of defined CPPS for HRC has many technical challenges. The biggest challenge is the computation of real time safety distance, which the robot must establish to avoid the human working in the production cell. Tight specifications on safety distance will be translated as the technology limit in terms of sensor specifications. Other challenges may include the use of reliable components to develop such a CPPS and a cyber security mitigation plan to counter intelligent cyber-attacks in the connected environment. This security plan must ensure the safe HRC and the security of PC even in the case of a compromised cyber layer of the system.

To build on the human avoidance approach, the physical challenge is to cover all parts of the robot to avoid humans using the safety distance approach (Khalid et al. 2016), meaning that sensors need to be

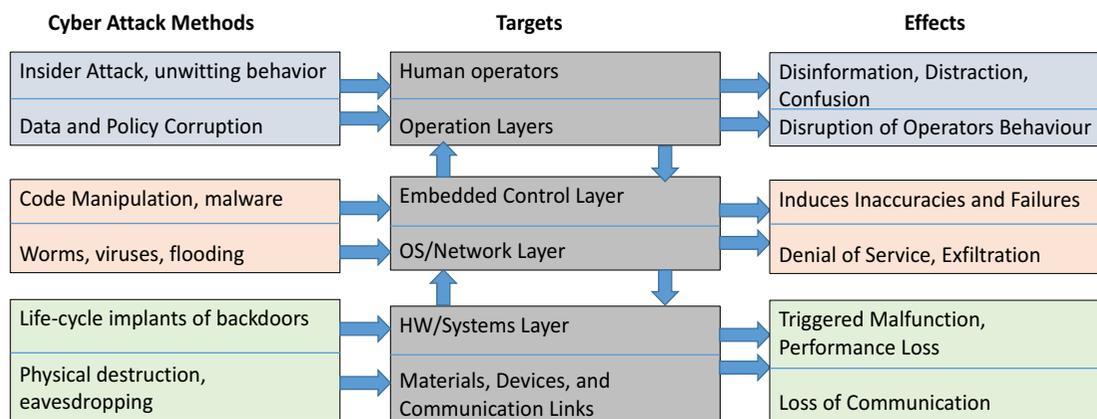


Figure 8. Potential cyber attack methods, targets, effects, and interconnections between the CPS layers (Elder 2008).

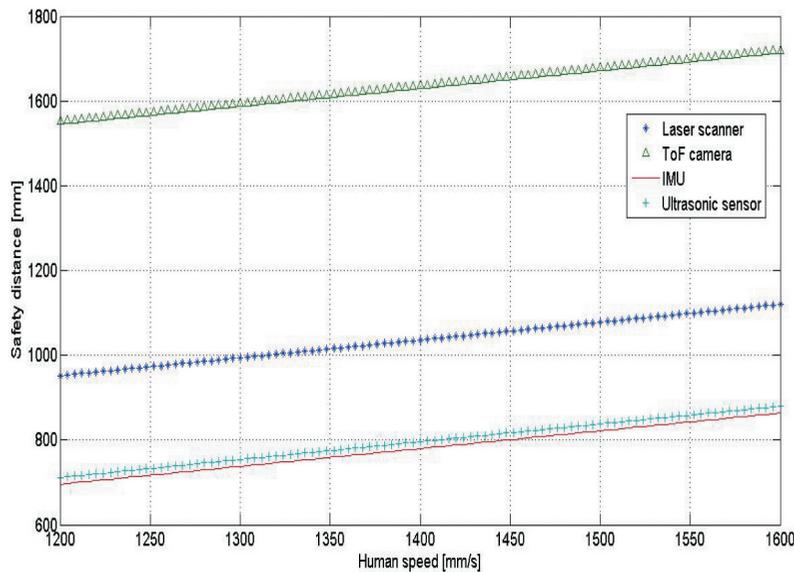


Figure 9. Safety distance versus human worker speed assessment on four different sensors.

installed on multiple links and joints. Figure 9 shows the safety distance calculations with four technology component sensors selected for CPPS application. The data shows that camera systems are the slowest and hence need the largest safety distance. Also, increased human worker speed results in large safety distance. Additionally, the data delay rate of the individual sensor output and communication over the network can cause undesirable results for HRC. Using multiple sensors from different makes can cause 120–150 ms delay using the present day sensor technology and requires sensor fusion techniques to reduce the delay time. The authors believe that the sensor fusion approach is more appropriate to reduce this delay instead of using only visual feedback (Islam et al. 2019).

A complete CPPS may have many sources of potential hazards due to which the system can malfunction and compromise on safe HRC. The list of these hazards can come from different sources. The three identified hazard sources are due to the collaborating robot, the industrial process, and the CPPS control layer malfunction. Detailed lists of hazards from these sources are given in Table 2.

All the three hazard sources are fully effective to those phases of the selected industrial scenario in which the HRC is established in the use-case (see

Figure 4). The hazards identified above can affect the HRC at any scale, as the focus in this work is on medium to heavy payload robots. The involved (hazards) variables at different magnitudes (low, medium, high) during collaboration can be further studied to see the effects on the human worker health and safety, industrial process effectiveness, quality of collaboration and the safety and security of the collaborative system. These domains can be further expanded to incorporate robustness in the HRC process.

5. Vulnerabilities in CPPS – A simulated study

The cyber-physical security challenges need to be addressed for successful collaborative tasking in the HRC segment. This requires access control to all interconnected devices in the CPPS. However, wireless networks are vulnerable to security threats, and secure communication protocols need to be utilized in order to ensure fault proof HRC. Moreover, in case an eavesdropper gains access to any component, the cyber security checks should act fast enough to mitigate the possible damage, as listed in Figure 8. It is challenging to counter zero day vulnerabilities (ZDV), which are unknown to the CPPS and can result in fatal consequences if not detected timely. On the other hand, most of the other types of cyber attacks have

Table 2. Hazards during collaboration.

From Robot	From Industrial Process	From robot control system malfunction
Robot characteristics, i.e. speed, force, torque, acceleration, momentum, and power.	Ergonomic design deficiency for operation and maintenance.	Due to operator's (reasonable and foreseeable) misuse of the system.
Operator dangerous location of working under heavy payload robot.	Time duration of collaboration in the process.	Control layer malfunction and misuse of collaborative system by the attacker under a cyber-attack in a connected environment.
End-effector and work part protrusions	Transition time from collaborative operation to other operation.	Physical obstacles in front of active sensors used in the collaborative workspace. (e.g. obstacle in front of a camera)
Sensitivity of the parts of the operator body that can come in contact in case of collision.	Potential hazards from the industrial process (e.g. temperature and loose parts).	Non-provision of transition from collaborative operation to a manual system in case of system malfunction.
Mental stress to operator due to robot characteristics (e.g. speed and inertia).	Mental stress to the operator due to a collaborative industrial process.	Multiple workers involvement in the collaborative process.
Trajectory taken by the robot.	Work material routing during the process.	Due to wrong perception of industrial process completion by the robot.
Physical obstacles against robot operation.	Physical obstacles tackled by the worker in order to accomplish process requirement in a collaborative workspace.	Obstacles against unobstructed means of exiting the collaborative workspace at any instant.
Fast worker approach speed and robot's slow reaction time.	Task complexity in a collaborative workspace.	Visual obstruction for the robot in collaborative workspace due to the vantage point of the operator.
Tight safety distance limit in the collaborative workspace.		

detectable signatures and their patterns are known to the security experts. For zero day vulnerabilities, complex artificial intelligence and machine learning algorithms are needed to detect and encounter these attacks (Wegner, Graham, and Ribble 2017; Khalid et al. 2018).

The VC scenario presented in Figure 7 is followed further for the simulation, in which a heavy workpiece is presented to the worker. The worker install items, and then, the robot safely pulls the workpiece to the carrier. The scenario during the installation task is extended as the involved CPPS is

compromised under a cyber-attack and the robot controller receives false signals and subsequently reduces the gripper force, primarily required to grip the heavy workpiece. The failure of operation results in a serious safety issue and failure of HRC. To evaluate the system's vulnerabilities and appraise the hazard from control system failure that could be faced by CPPS, a simulation setup of an automated collaborative control of the robotic system is presented for software in the loop simulation using the Matlab/Simulink platform. The kinematics and dynamics of the manipulator are based on youBot

**Figure 10.** KUKA youBot used for pick and place task on two conveyors (Robot 2018).

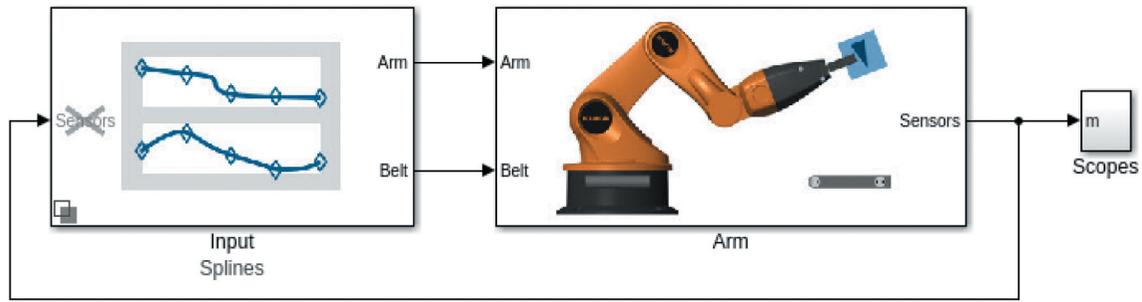


Figure 11. Simulation model of the youBot manipulator.

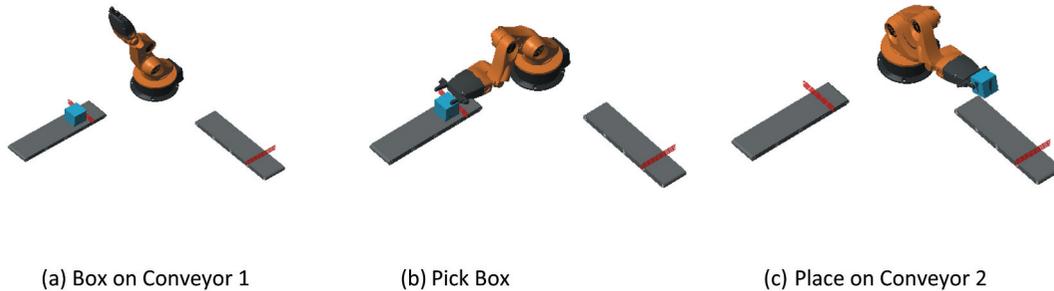


Figure 12. (a)–(c) Manipulator with two conveyors for pick and place task.

specifications from KUKA robotics (Miller 2020). The youBot mobile robot (see Figure 10) is composed of an omnidirectional base and a KUKA arm with 5 degrees of freedom. The weight of the robot is 5.3 kg with a payload capacity of 0.5 kg (Robot 2018). This robot has been designed for teaching, research and experimentation (Krasňanský, Tóth, and Huertas 2013). The implemented simulink model is used to demonstrate a benchmark example for the collaborative control in CPPS and its vulnerability in case of a cyber attack on the EtherCAT real time communication for the control of manipulator (2020). The Simulink model of the youBot manipulator is shown in Figure 11.

A) Normal operation

In a simplified scenario, the task of the collaborative control is coordinated with the help of two conveyors placed in a simulated industrial environment. The workflow for the simulation is sequenced in three steps, as shown in Figure 12. In the first step, the manipulator detects the box at the end of conveyor 1. It then picks the box using a parallel gripper with two-fingers. Next, the controller executes a safe trajectory for youBot to move from conveyor 1 to

conveyor 2. Finally, it places the box on conveyor 2 to finish the job. The handling, gripping and holding of the box between the two conveyors are seen as the simplified representative of the actual scenario explained above. The participating worker in the collaboration is assumed to be present in/or near the robot working area.

The joint angles for the pivot, bicep, forearm and wrist are shown in Figure 13 under normal conditions. The finger position shown in the same figure depicts the gripping action of the manipulator while picking the box from conveyor 1 and placing it on conveyor 2. The radial and axial forces for all axes are shown in Figure 14.

B) Cyber attack scenario

The typical scenarios of cyber-attack on the collaborative CPPS in an industrial setting may include man in the middle (MIM) attack, down sampling attack, control parameter attack or a coordinated attack, which maybe a combination of two or more basic attack mechanisms in order to disrupt the desired functioning of a CPPS (Wan, Canedo, and Faruque 2015; Khalid et al. 2018). For our case, the intruder is able to penetrate through the firewall and execute

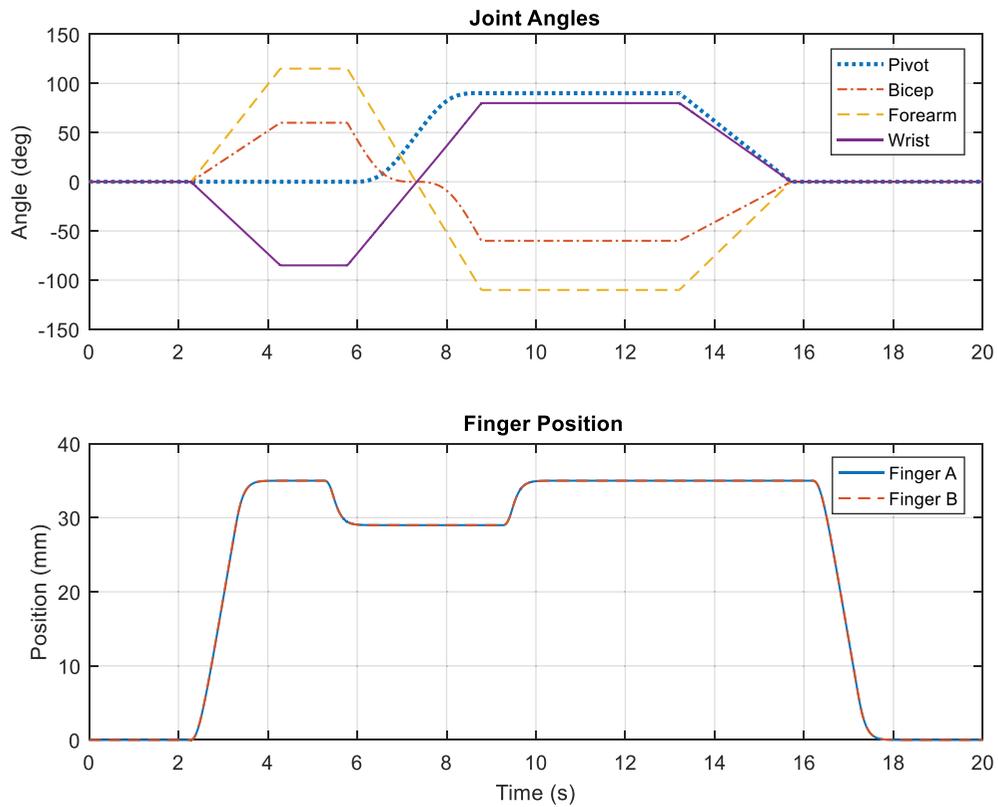


Figure 13. Manipulator joint angles and finger position for pick and place task under normal conditions.

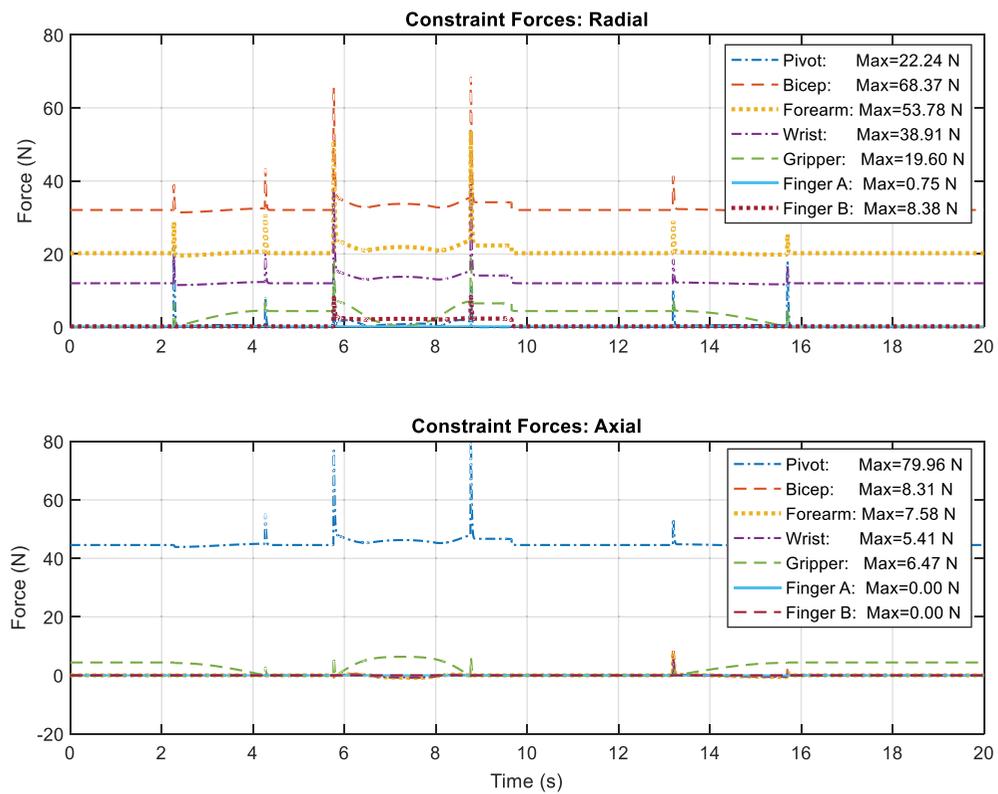


Figure 14. Manipulator radial and axial forces for pick and place task under normal conditions.

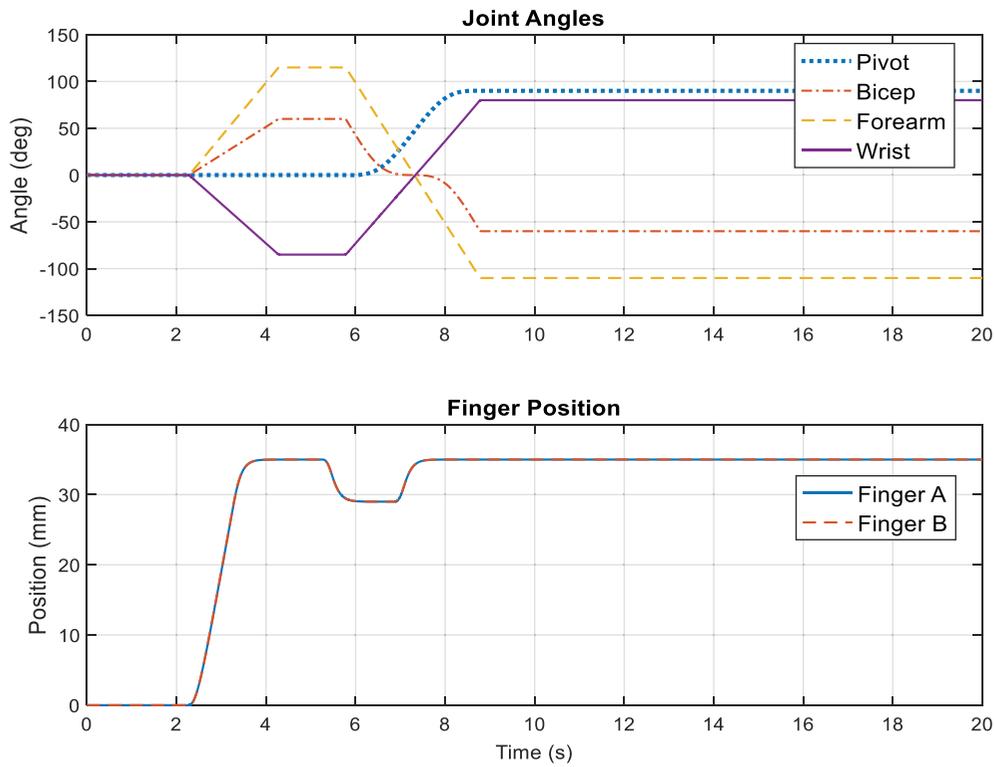


Figure 15. Manipulator joint angles and finger position for pick and place task under cyber-attack at $t = 7s$.

a control parameter attack at $t = 7s$, resulting in modification of the gripper filter time constant from 0.1 to 1. This results in the failure of the finger position to maintain the grip on the box, resulting in dropping

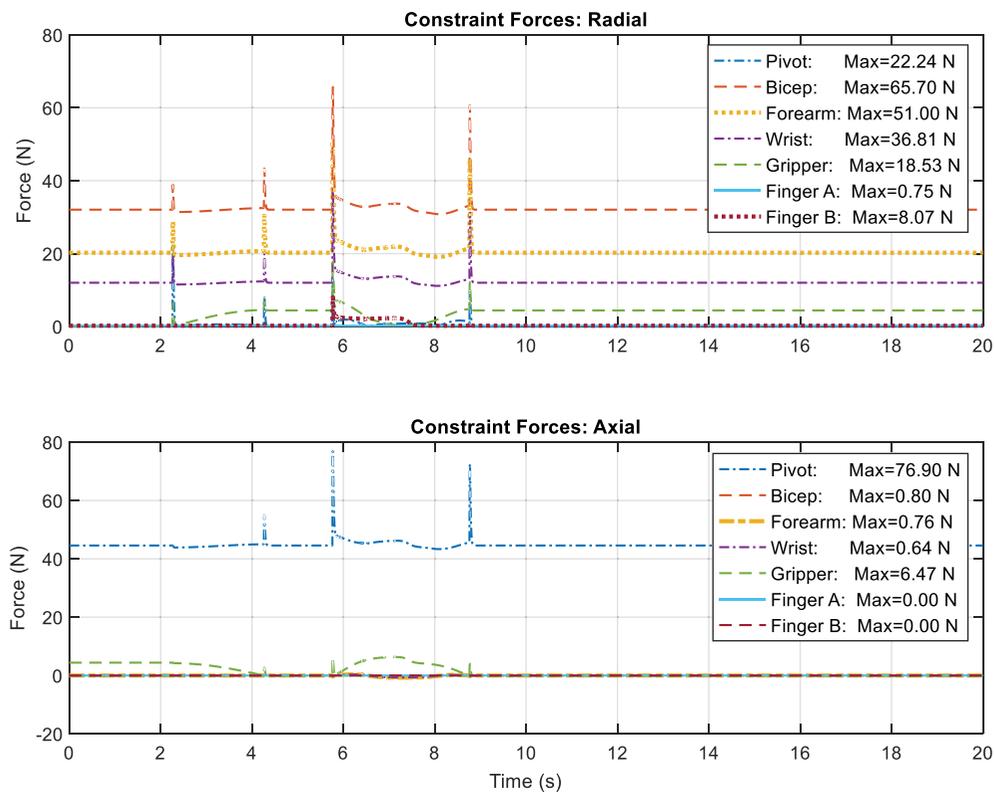


Figure 16. Manipulator radial and axial forces for pick and place task under cyber-attack @ $t = 7s$.

the box at $t = 7s$, and thus, the pick and place task is not successful. The joint angles and finger positions for the cyber-attack scenario are shown in Figure 15. The radial and axial forces along all axes in this scenario are shown in Figure 16. The maximum radial force of the gripper has changed to 18.53 N, which was previously 19.6 N under normal execution of pick and place operation.

As is evident from the above figures, in case of cyber attack resulting in malfunctioning of the control layer, the industrial operations may be hazardous for surrounding operators due to uncontrolled action of the robot. In our case, the manipulator missed to grip the box and therefore was unable to complete the task. A heavy payload dropped in such events can damage the equipment or hurt an operator within the collaborative robot workspace. In a worst case scenario, the malfunctioned manipulator or conveyor system could result in a total disaster for the plant.

6. Conclusion

The manuscript proposed an integrated CPPS for the flexible manufacturing industrial environment. The new definition in the CPPS includes the HC that interacts with other CPS components in a fully interconnected system with the robotic component as part of the futuristic manufacturing systems. In order to see the feasibility of the proposed system, an industrial scenario is selected to visualize an industrial assembly process using a heavy payload robot. The technology selection phase in the CPPS revealed the real challenges that can seriously encumber the HRC. The challenges are highlighted from the standpoint of the used robot scale, industrial process complexity, safety distance computation based on the existing sensor technology and the malfunction of the control layer in case of cyber-attacks. It is evident from the simulation that a security compromised physical asset can cause a serious safety issue in the CPPS due to the high connectivity. Our prime objective is to emphasize on a flexible cooperative framework of hybrid team players in a CPPS to provide relief to the human workers in ergonomically hard jobs or injurious activities. Overall, it is suggested that any such design activity for such a HRC system must include the

integrated concepts of safety and security. As in the interconnected environment, both concepts merge to affect the overall quality of HRC, the industrial process itself and the health and safety of the human operator working with the cobot in the context of Industry 4.0.

Acknowledgments

The authors would like to acknowledge the support of the cLINK (Centre of excellence for Learning, Innovation, Networking and Knowledge), the Erasmus Mundus Programme of the European Union, the InSA Project, sponsored by the German Federal Ministry for Economic Affairs and Energy (project register number: HRB 24505 HB), and the thyssenkrupp System Engineering GmbH.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the German Federal Ministry for Economic Affairs and Energy [project register number: HRB 24505 HB].

ORCID

Klaus-Dieter Thoben  <http://orcid.org/0000-0002-5911-805X>
Jürgen Pannek  <http://orcid.org/0000-0001-5109-9627>

References

- 2015. Collaborative Robotics Market Exceeds US\$1 Billion by 2020. ABI research.
- Elder, R. 2008. "Defending and Operating in a Contested Cyber Domain." In *Air Force Scientific Advisory Board, Winter Plenary*.
- Gonçalves, L. R., P. R. M. de Araujo, and M. Corazzim. 2020. "In-process Machine Vision Monitoring of Tool Wear for Cyber-Physical Production Systems." *Robotics and Computer-Integrated Manufacturing* 61. doi:10.1016/j.rcim.2019.101859.
- Islam, S., O. Bin, W. A. Lughmani, W. S. Qureshi, A. Khalid, M. A. Mariscal, and S. Garcia-Herrero. 2019. "Exploiting Visual Cues for Safe and Flexible Cyber-physical Production Systems." *Advances in Mechanical Engineering* 11 (12): 1687814019897228. doi:10.1177/1687814019897228.
- ISO. 2016. Robots and robotic devices – Collaborative robots. ISO/TS 15066: 2016

- Khalid, A., P. Kirisci, Z. Ghairi, J. Pannek, and K.-D. Thoben. 2017. "Safety Requirements in Collaborative Human-robot Cyber-physical System." In *Dynamics in Logistics*, 41–51. Springer.
- Khalid, A., P. Kirisci, Z. Ghairi, K.-D. Thoben, and J. Pannek. 2016. "A Methodology to Develop Collaborative Robotic Cyber Physical Systems for Production Environments." *Logistics Research* 9 (1): 1–15. doi:10.1007/s12159-016-0151-x.
- Khalid, A., P. Kirisci, Z. H. Khan, Z. Ghairi, K.-D. Thoben, and J. Pannek. 2018. "Security Framework for Industrial Collaborative Robotic Cyber-physical Systems." *Computers in Industry* 97: 132–145. doi:10.1016/j.compind.2018.02.009.
- Khalid, A., and Z. H. Khan. 2014. "Multi-objective Optimization for Error Compensation in Intelligent Micro-factory CPS." In Zeashan H Khan A. B. M. Shawkat AliZahid Riaz (eds.), *Computational Intelligence for Decision Support in Cyber-Physical Systems*, 67–103. Singapore: Springer.
- Khan, Z. H., A. Khalid, and J. Iqbal. 2018. "Towards Realizing Robotic Potential in Future Intelligent Food Manufacturing Systems." *Innovative Food Science Emerging Technologies* 48: 11–24. doi:10.1016/j.ifset.2018.05.011.
- Knight, W. 2014. "How Human-robot Teamwork Will Upend Manufacturing". MIT Technology Review, Business Report, Breakthrough Factories.
- Krasňanský, P., F. Tóth, and V. V. Huertas. 2013. "Basic Laboratory Experiments with an Educational Robotic Arm". International Conference on Process Control (PC). Strbske Pleso, Slovakia.
- Lasota, P. A., G. F. Rossano, and J. A. Shah. 2014. "Toward Safe Close-proximity Human-robot Interaction with Standard Industrial Robots". 2014 IEEE International Conference on Automation Science and Engineering (CASE). New Taipei, Taiwan.
2020. "MathWorks Student Competitions Team, Designing Robot Manipulator Algorithms, GitHub". accessed April 16. <https://www.github.com/mathworks-robotics/designing-robot-manipulator-algorithms>
- Miller, S. 2020. "Robot Arm with Conveyor Belts, MATLAB Central File Exchange". accessed April, 14. <https://www.mathworks.com/matlabcentral/fileexchange/61370-robot-arm-with-conveyor-belts>
- Monostori, L. 2014. "Cyber-physical Production Systems: Roots, Expectations and R&D Challenges." *Procedia Cirp* 17: 9–13. doi:10.1016/j.procir.2014.03.115.
- Ore, F., J. L. J. Sánchez, M. Wiktorsson, and L. Hanson. 2020. "Design Method of Human-industrial Robot Collaborative Workstation with Industrial Application." *International Journal of Computer Integrated Manufacturing* 33 (9): 911–924. doi:10.1080/0951192X.2020.1815844.
- Pirvu, B.-C., C.-B. Zamfirescu, and D. Gorecky. 2016. "Engineering Insights from an Anthropocentric Cyber-physical System: A Case Study for an Assembly Station." *Mechatronics* 34: 147–159. doi:10.1016/j.mechatronics.2015.08.010.
- Plósz S., Schmittner C., Varga P. (2017) Combining Safety and Security Analysis for Industrial Collaborative Automation Systems. In: Tonetta S., Schoitsch E., Bitsch F. (eds) *Computer Safety, Reliability, and Security. SAFECOMP 2017. Lecture Notes in Computer Science*, vol 10489. Springer, Cham. <https://doi.org/10.1007/978-3-319-66284-81616>
- Prinsloo, J., S. Sinha, and S. Basie von. 2019. "A Review of Industry 4.0 Manufacturing Process Security Risks." *Applied Sciences* 9 (23): 5105. doi:10.3390/app9235105.
- Rehman, M., U. Muneeb, H. Z. U. Rehman, and Z. H. Khan. 2020. "Cyber-attacks on Medical Implants: A Case Study of Cardiac Pacemaker Vulnerability." *International Journal of Computing and Digital Systems* 9 (6): 1229–1235. doi:10.12785/ijcds/0906020.
- Robot, G. 2018. "KUKA youBot, robot mobile omni-directionel avec bras". accessed April, 10. <https://www.generationrobots.com/en/402093-kuka-youbot-robot-mobile-omni-directionel-avec-bras.html>
- Stadnicka, D., and D. Antonelli. 2019. "Human-robot Collaborative Work Cell Implementation through Lean Thinking." *International Journal of Computer Integrated Manufacturing* 32 (6): 580–595. doi:10.1080/0951192X.2019.1599437.
- Sunder, S. 2012. *Foundations for Innovation in Cyber-physical Systems*. Chicago, IL, USA: Proceedings of the NIST CPS Workshop.
- Thames, L., and D. Schaefer. 2017. Industry 4.0: An Overview of Key Benefits, Technologies, and Challenges. In: Thames L., Schaefer D. (eds) *Cybersecurity for Industry 4.0*. Springer Series in Advanced Manufacturing. Springer, Cham. https://doi.org/10.1007/978-3-319-50660-9_1
- Tsarouchi, P., A.-S. Matthaikis, S. Makris, and G. Chryssolouris. 2017. "On a Human-robot Collaboration in an Assembly Cell." *International Journal of Computer Integrated Manufacturing* 30 (6): 580–589. doi:10.1080/0951192X.2016.1187297.
- Tuptuk, N., and S. Hailes. 2018. "Security of Smart Manufacturing Systems." *Journal of Manufacturing Systems* 47: 93–106. doi:10.1016/j.jmsy.2018.04.007.
- Uhlemann, Thomas, H.-J., C. Lehmann, and R. Steinhilper. 2017. "The Digital Twin: Realizing the Cyber-physical Production System for Industry 4.0." *Procedia Cirp* 61: 335–340. doi:10.1016/j.procir.2016.11.152.
- Wan, J., A. Canedo, and M. A. A. Faruque. 2015. "Security-aware Functional Modeling of Cyber-physical Systems". IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA). Luxembourg.
- Wegner, A., J. Graham, and E. Ribble. 2017. A New Approach to Cyberphysical Security in Industry 4.0. In: Thames L., Schaefer D. (eds) *Cybersecurity for Industry 4.0*. Springer Series in Advanced Manufacturing. Springer, Cham. https://doi.org/10.1007/978-3-319-50660-9_3
- Weippl, E., and P. Kieseberg. 2017. "Security in Cyber-physical Production Systems: A Roadmap to Improving IT-security in the Production System Lifecycle". 2017 AEIT International Annual Conference. Cagliari, Italy.
- Zhang, H., Q. Yan, and W. Zhenghua. 2020. "Information Modeling for Cyber-physical Production System Based on Digital Twin and AutomationML." *The International Journal of Advanced Manufacturing Technology* 107 (3–4): 1927–1945. doi:10.1007/s00170-020-05056-9.