Security Framework for Industrial Collaborative Robotic Cyber-Physical Systems

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.

Keywords Cyber Physical System, Cyber Security, Human-Robot Collaboration

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 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 'Collaborative Robotic Cyber-Physical System' (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.

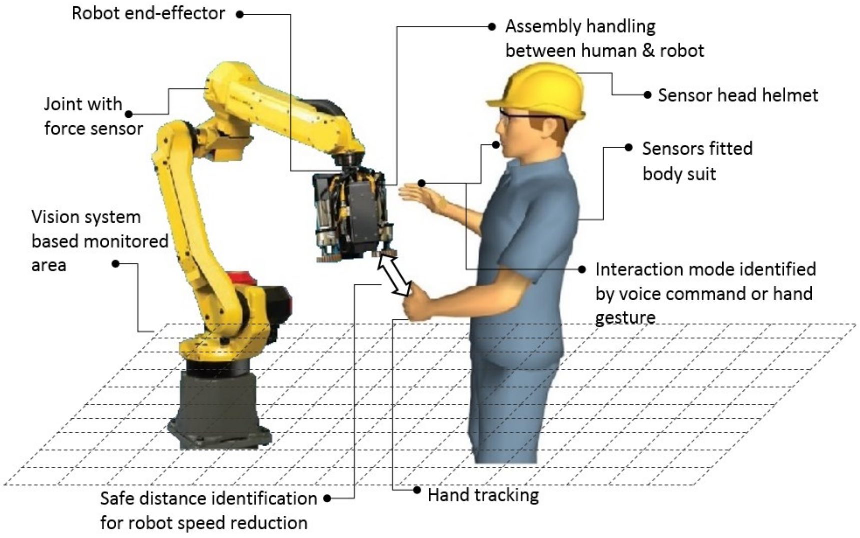

Robot end-effector
Assembly handling between human & robot
Joint with force sensor
Sensor head helmet
Sensors fitted body suit
Vision system based monitored area
Interaction mode identified by voice command or hand gesture
Safe distance identification for robot speed reduction
Hand tracking

Fig. 1 HRC, technology modules

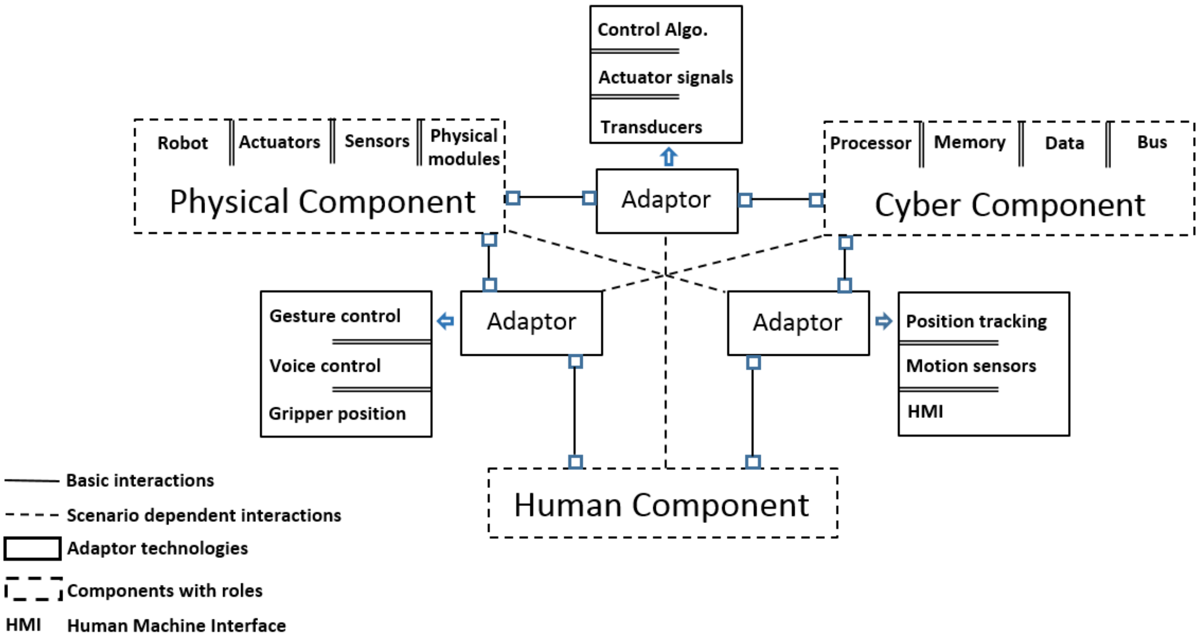


Fig. 2 CRCPS structure: Modules, components, adaptor technology modules and interconnected links.

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 focus on security aspects of CRCPS and the protection measures needed for implementation. In CRCPS, the functional modules are interconnected through wired systems and/or wirelessly to converse with the same type of devices [26, 27]. Using human-machine interactive (HMI) systems, machines connect and cooperate with humans through a network. Hence, the disposition of a complete CPS interprets the human collaborator as a vital system component. In defining CRCPS, there are a few main interconnected components in the model (See Fig. 2). These modules are the human component (HC), the physical component (PC) and the computational component (CC) [28]. The communication midst the three entities is subjected to the advent of the enabling adaptor technologies in CPS. To define a CRCPS, the basic modules of HC, PC, and CC interact through adaptors while the system possesses all the inherent characteristics of CPS like integrity, sociability, locality, irreversibility, adaptability, autonomous and highly automated [10, 28]. For CRCPS, the PC must be a robot. The human component is coupled through diverse adaptor technologies, e.g., worker position tracking is crucial adaptor in the CRCPS either through overhead cameras or IMU. The CRCPS is an automated system as it eliminates the limits amid the multiple components, thus favoring their operating communications.

There are numerous HMI technologies that are dependent on acoustics, vision, and haptics. The planned CRCPS has employed vision system for detection and tracking of operator position. The collaborative robot command system can also use gesture recognition of operator and acoustics like voice control. Furthermore, a diversity of actuators and sensors can deliver the communication among PC, HC and CC. There are regular connections revealed amid the components contributing a role. Adaptor technologies are situation dependent (plug and play) devices. There are discretionary situation reliant connections among the adaptors and regular components in CRCPS. In CRCPS, the controller node of the PC (robot system) performs the intelligent control part to compute precise positioning and rate commands. PROFINET/ProfiSafe in real time protocol provides up to 1 ms cycle time for PROFINET IO applications cascading real-time communication concept for distributed component models. It is used in CRCPS and the communication system is designed through wireless or wired networking and information. This specific application is analogous to such instrumentation in which sensor measurements to a supervisor application are communicated through a network that renders the important information like safety distance calculation in real time.

The system communication requirement aims to present machine to machine (M2M) and human to machine (H2M) communication integration. Mostly, the information runs from a machine (sensor or a physical module) connected through a network and then arrives at a system using a gateway where it can be looked over and proceeded on. The H2M communication in CRCPS initiates through gyro output and sent over the network so that it can be analyzed for the safe distance computation and other considerations. The selection of an appropriate protocol is determined by the secure communication, range and data rate. ZigBee or wireless HART-based 802.15.4 protocol is normally selected for the moderate range. A time division protocol is exploited for real time communication in wireless HART as it practices channel blacklisting for interference avoidance. Due to the service quality, certain communicating nodes are employed as a preferred choice for time/resource allocation. However, Bluetooth protocol is suitable in CRCPS due to close area proximity communication with high security.

3. Challenges of Cyber Security for CRCPS

A secure CRCPS framework can only be constructed if there is an awareness about the intelligent knowledge driven (of the target) cyber-attacks. The cyber-attack can come from both internal and external sources. Raya et al. [15] have described an attacker according to three ways of classification, i.e., active vs. passive, malicious vs. rational and outsider vs. insider. As shown in Fig. 3, a cyber-attack may arrive from an external source like outside communication channels, wireless transmission or from an internal attacker by physically accessing a data port, e.g., by a worker involved in HRC in a given industrial scenario. The active attacker initiates the attack directly while passive attacker has the tendency to observe/eavesdrop from the control or cyber component of the target CPS [29]. The passive attacker's function is to do reconnaissance about the target's physical asset through the control or cyber layer and bring back the valuable information to aid in the design of an intelligent active cyber-attack. An active attacker uses the network authority, but bounded by its inherent intelligence, can only significantly harm the target's physical assets, if well-equipped with the required knowledge. A malicious attacker aims for destruction at a larger scale while rational attacker specifies the target. Here, the job of the CRCPS mitigation security framework is to stop all classes of attackers.

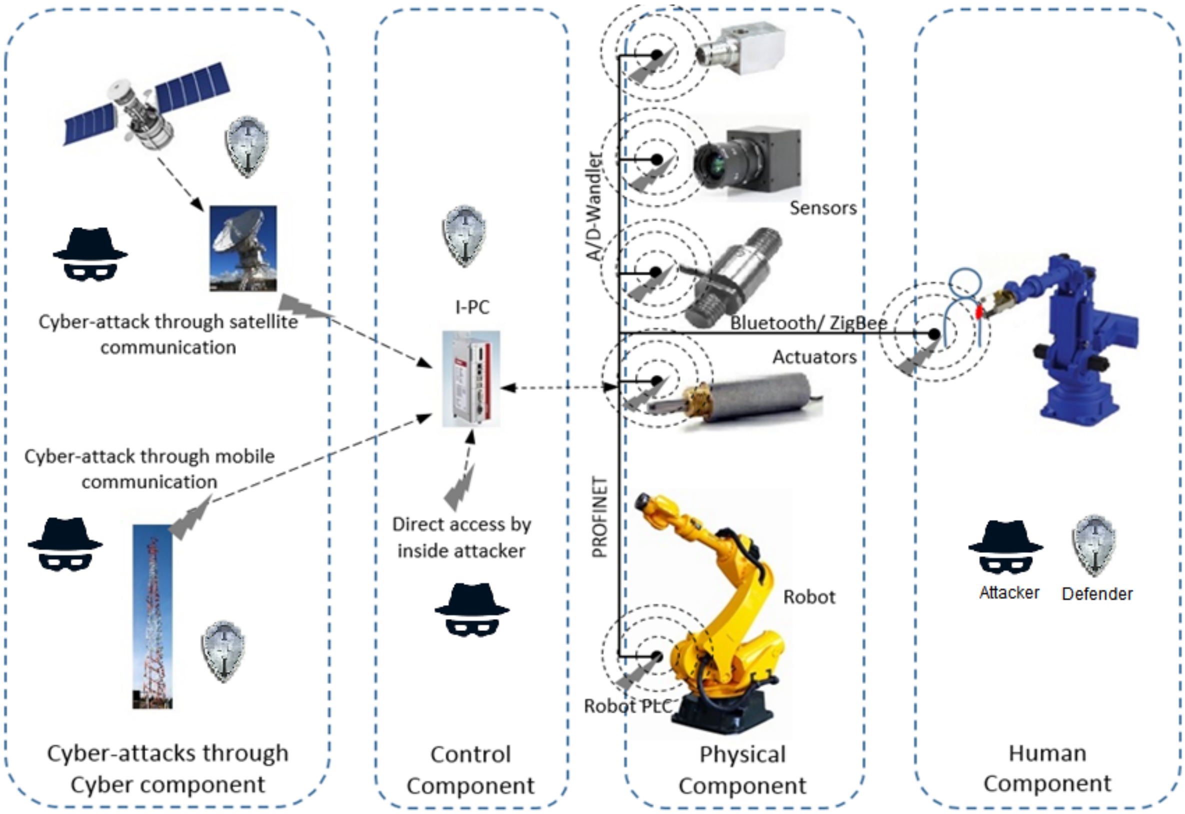
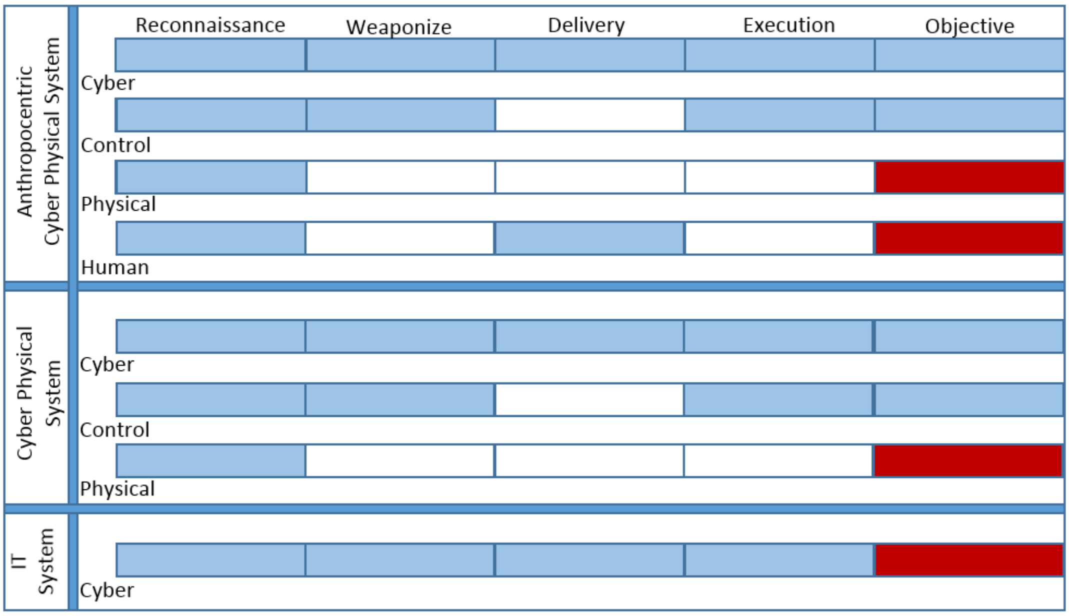

Cyber-attack through satellite communication
Cyber-attack through mobile communication
Cyber-attacks through Cyber component
I-PC
Direct access by inside attacker
Control Component
A/D-Wandler
Sensors
Bluetooth/ ZigBee
Actuators
PROFINET
Robot
Robot PLC
Physical Component
Attacker
Defender
Human Component

Fig. 3 Cyber-attack routes in CRCPS and logical causal effect diagram for HRC.

A security concept in an IT system is different from the one in CPS, mainly due to the fact that a PC is integrated and controlled by a CC in CPS. In the CPS scenario, it is a necessary requirement to safeguard PC, even in the case of a security compromised CC. If in the CRCPS case, the cyber component is compromised by a cyber-attack, the PC comprised of the robot, human, actuators, and sensors may come under direct attack and may result in a system failure like unsafe HRC or occurrence of an accident while HRC in operation in any given industrial scenario.

To design a security concept in CPS effectively, it is advantageous to analyze how cyber-attacks work in such a system. Fig. 4 introduces the conceptual difference of a cyber-attack mechanism on a CPS, an IT system and an anthropocentric CPS (ACPS). ACPS is an extension of a CPS in the social domain [13, 21, 28, 30, 31], in which human is an integrated part of the CPS. The CRCPS structure shown in Fig. 2 is a logical derivative of the ACPS.

In an IT system, all the phases of a cyber-attack, i.e., from planning to meeting final objective are conducted in a cyber-layer. However, in a CPS, these tasks are divided according to the role played by each layer. For example, the attack planning phase is comprised of all layers to gather the information of the target system [32]. Here, the reconnaissance part of the cyber-attack is conducted as a passive attacker to aid in designing a sophisticated attack for an active attacker. In the next phase, a cyber-attack weapon prepares itself in order to gain control of the target system and achieve the final objective. The delivery phase is only possible through the cyber layer and the attack execution is to overcome the control part of the target system using the obtained information from the passive attacks. Though, the objective of a cyber-attack in an industrial CPS is to destroy costly physical assets, the cyber and control components can also be part of objective depending upon the target system application and control structure. In an ACPS case, the additional role of the human in the cyber-attack mechanism is at three places, i.e., in the planning phase for the system information, in the delivery phase of the attack through USB port or other inside ways and also the human can be a final objective to be harmed in a CRCPS. Therefore, it is evident that a cyber-attack mechanism for an IT system, CPS, and an ACPS has different means and concepts. Similarly, a mitigation plan against such sophisticated attacks should also follow a different approach.



		Reconnaissance	Weaponize	Delivery	Execution	Objective
Anthropocentric Cyber Physical System	Cyber	🟦	🟦	🟦	🟦	🟦
	Control	🟦	🟦	⬜	🟦	🟦
	Physical	🟦	⬜	⬜	⬜	🟥
	Human	🟦	⬜	🟦	⬜	🟥
Cyber Physical System	Cyber	🟦	🟦	🟦	🟦	🟦
	Control	🟦	🟦	⬜	🟦	🟦
	Physical	🟦	⬜	⬜	⬜	🟥
IT System	Cyber	🟦	🟦	🟦	🟦	🟥

Fig. 4 Cyber-attack mechanism: A comparison of ACPS, CPS and an IT system

4. Cyber-attacks categorization criteria in CRCPS

In order to cater for a variety of cyber-attacks, it is important to see the node characteristics in the network. Once the attack enters the CRCPS through the cyber layer, it can conduct a variety of attacks like broken nodes or data falsification. The horizon of such attacks may span from cyber to control layer to perturb the physical objective. A decentralized CPS architecture is preferred as compared to a failure at the unique node that a foe can aim. The execution phase attacking the target's control action attempts to achieve specific properties guided by operational requirements and the cyber layer properties (confidentiality, integrity, and availability) must be secured in the face of cyber-attack. Overall, it is the goal of cyber-attack that determines the extent gained of the particular properties of different CPS components. The goal may range from the degraded performance of some aspects of the physical operation of CPS up to the complete disruption or destruction of PC in a CPS. Figure 5 shows the guideline list of attack methods and the interconnections of possible targets and effects in different CPS layers. In line with excessive interdependencies among CPS functional components and adaptors, secondary effects can follow during individual element interactions which needs to be confronted. These second order effects can occur at components engaged in different layers or even involving other (cyber or physical) domains.

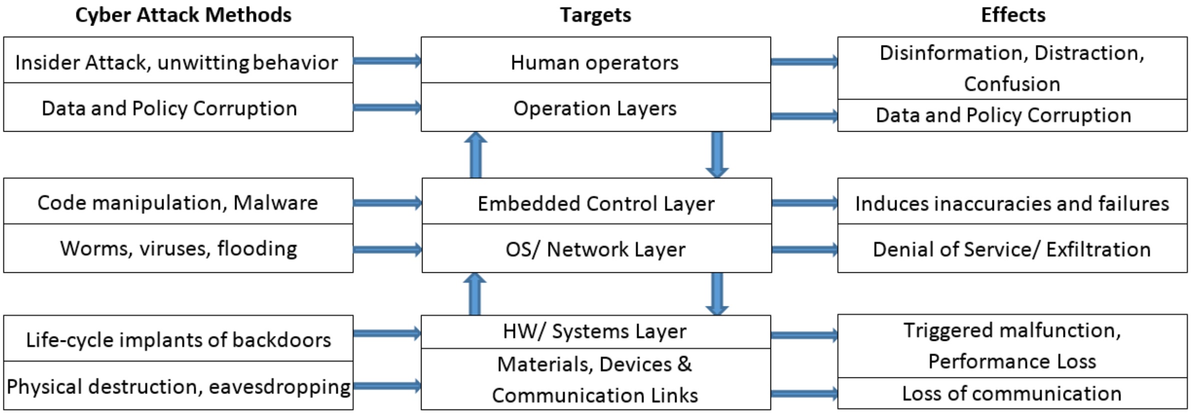
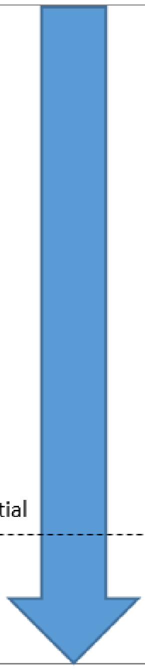

Cyber Attack Methods
Targets
Effects
Insider Attack, unwitting behavior
Data and Policy Corruption
Human operators
Operation Layers
Disinformation, Distraction, Confusion
Data and Policy Corruption
Code manipulation, Malware
Worms, viruses, flooding
Embedded Control Layer
OS/ Network Layer
Induces inaccuracies and failures
Denial of Service/ Exfiltration
Life-cycle implants of backdoors
Physical destruction, eavesdropping
HW/ Systems Layer
Materials, Devices & Communication Links
Triggered malfunction, Performance Loss
Loss of communication

Fig. 5 The methods of cyber-attacks guideline: an interconnectivity of targets and involved CPS layers [33]

The execution phase of cyber-attack effects the control and cyber components as shown in Fig. 4. The possible effects and the extent of the attack on controllability of CPS should be assessed [1, 11]. It is important to categorize and assess the impact of the particular type of attacks in the context of CRCPS. The control component's properties are controllability and observability of internal states of the system [32-34]. A control algorithm for a controllable system is designed to render a stable system. An observable system employs a state estimator or an observer that for given sensor measurements, can track the system state precisely [9]. In CRCPS, sensors for human position information are an example of observability. The two properties are mathematical duals. Any compromise on system controllability or internal control variables can effect on CRCPS physical outcome in terms of system stability and efficiency. The scale (from low to serious attack) is developed according to the CRCPS physical outcome. Based on the three categories of cyber-attack, (authentication, availability, and confidentiality) the possible effects may range from low to high. Low to medium range effects mean short period control loss to reduced sensor efficiency, while high risk is gauged by the false sensor output under attack [9]. As an example, if the worker safety is disturbed due to the false sensor output, the extent gained by the attacker crosses the line from partial to full attack. The proposed framework is designed keeping in mind that the attacker has a strong understanding of the system stability, efficiency, safety and resource constraints.

Table 1 shows criteria based assessment on cyber-attack effect on CRCPS physical outcome. Low to serious cyber-attacks are categorized and assessed based on the degradable cyber properties of the CRCPS, i.e., node authentication, node availability, data confidentiality, and integrity. The level of attacks on CRCPS is considered low if the control is lost for a short period. In table 1, the low category authentication attacks include tempering, position faking and message suppression in a close area network [35]. These are forms of false authentication techniques an attacker can follow to disturb the system. Sensor node authentication is measured as a vital security prerequisite in networks and the most involved system component is, in fact, the network user. A CRCPS operator may act as a malicious attacker or an eavesdropper by violating security as a legitimate network user.

Table 1 Assessment & categorization of cyber-attacks on CRCPS

Attack intensity on CRCPS	Authentication	Availability	Confidentiality	Extent of attack on controllability	Possible effects
Low	- GPS spoofing/ Movement tracking/ position faking - Tunnelling - Message tempering - Message suppression - Non-repudiation	- Jamming - Greedy behaviour - Grey hole - Sink hole - Broad cast tempering - Spamming	- Non-repudiation		Short period control loss
Medium	- Sybill - Node impersonation - Key/Certificate replication - Masquerading - Unauthorized pre-emption	- DOS - Jamming - Black hole - Worm hole - DDoS - Malware		Partial	Effect on sensor node efficiency
Serious or high risk	- Replay		- Eavesdropping	Full	Data falsification from sensor output node

The availability attacks in the same category describe many attacks pertaining to node non-availability. The node availability condition infers that information traffic through all nodes in a network at any time is possible. Attacks on availability disturb the performance features of threads and processes, such as memory access delays, data transfer features of buses and troublesome communication. Grey hole and sinkhole attacks are a type of Denial of Service (DoS) attacks in which packets drop and fake routing update are possible and can cause launch of other attacks. Broadcast tempering is another type of attack that may lead to the accident by hiding safety related messages from legitimate nodes [11]. To design a protected CPS network, authentication, data integrity, privacy, confidentiality, and availability are important. Out of these parameters, authentication, availability, and confidentiality are relevant to CRCPS, mainly due to the safety application of the human worker [24]. A confidentiality attack allows the foe to collect system information and use such information when the user is not aware of the information leak. A repudiation attack occurs when a system does not implement controls to correctly monitor user activities, therefore, compromising industrial data protection and worker anonymity in the case of CRCPS.

The medium risk for CRCPS is defined due to decreased sensor efficiency. The medium risk authentication attacks include Sybil attack [36, 37], masquerading and also the type of attacks in which cheating with positioning information and ID disclosure are common. The CPS system must be able to identify the untrusted sender and ignore signals from such sensors within the CPS. The availability attacks in the medium category include the black hole, worm hole, DoS, and Jamming attacks [38]. Black holes are formed in interconnected nodes due to a broken node. In the CRCPS network, a broken node from an important sensor, e.g., laser scanner responsible for area monitoring, can cause the collaborative system to be less efficient. All of these attacks are categorized as having low to medium scale effects on cyber security of CRCPS [39].

An attack on the CRCPS is considered serious when the sensor data is false. By influencing sensor output, the state estimates can be corrupted by an attacker that cause wrong control signals to actuators. A replay attack [40, 41] is like sending previously received information in the network again, leading to a failure to signal propagation. A false functioning of such sensors in the network may jeopardize the system safety. In CRCPS, the worker's location information is coming either from vision system or from the motion sensors. A replay attack, i.e., false information update about the worker location, can make the system unsafe. Another goal is to acquire information about the control algorithms, sensors and actuators and how they are used to monitor and control the CPS. An attack on confidentiality can compromise the system state information that is necessary for a cyber-attack to perturb the PC of the CPS. Eavesdropping [18] deals with the illegitimate collection of messages by the attacker and enhance the attacker's ability to influence the physical operations of the system.

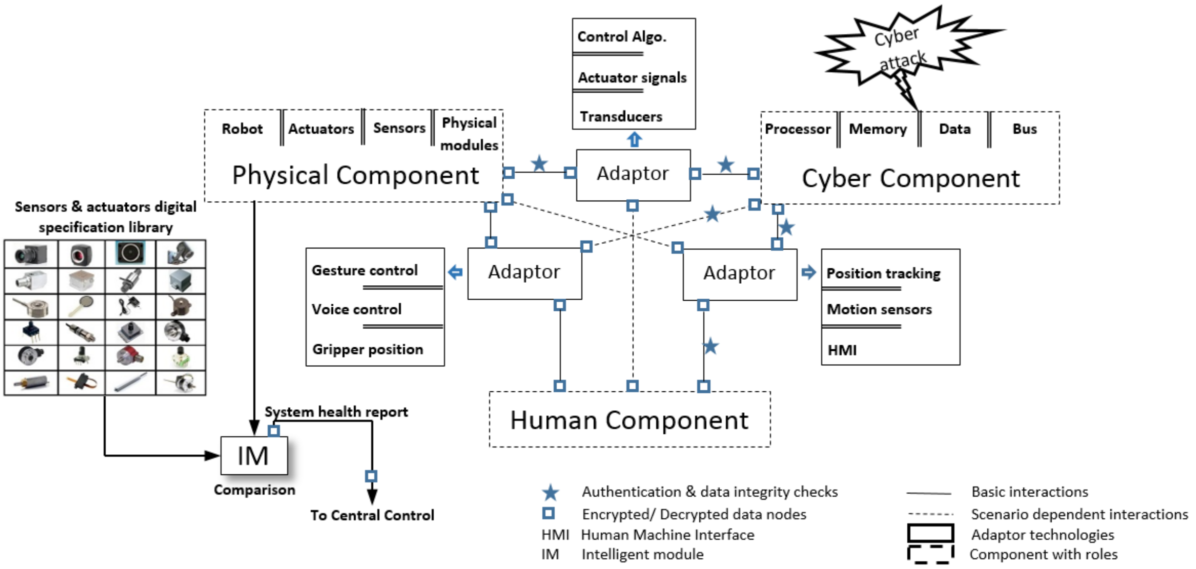


Fig. 6 Collaborative Human-Robot CPS under Cyber-attack and the two-pronged strategy as a mitigation plan

CRCPS is comprised of a (vital) sensor network which keeps the HC safe. The network must not be compromised because of the associated physical outcomes of stability, efficiency, and safety. The security of the cyber layer comprised of attacks based on integrity, availability, and confidentiality that can effect adversely on access, performance and other qualities of the CRCPS. The quantification of risk methods in CPS is studied [42] about integrity, availability, and confidentiality. In response to an attack, challenges and influence on the security principles of confidentiality and integrity are identified. Detection of high-risk nodes in a network can be identified effectively by a security framework to sort appropriate responses with the fundamental principles of security. Effective categorization of cyber-attacks in the context of CRCPS revealed the possibility of risk according to the extent of the attack on controllability. As system stability disturbance for a short period is linked with the low level of attacks, reduced system efficiency can be caused by the attacks categorized at the medium level in CRCPS. This is based on the assumption that the human avoidance algorithm and safety distance computations in CRCPS cannot be disturbed in real time. The serious types of attacks are considered by which HRC safety become compromised.

5. Proposed Secure Framework for CRCPS

Communication channel security is fundamental for the deployment of the safe network. Providing authenticity in a short distance CPS network involves protecting legitimate nodes from attackers penetrating the network through fabricated identity. For CRCPS application, the trustworthy secure data update is required especially for the interface adaptor nodes between CC and PC in real time and with a limited overhead. The idea is to develop a security framework (See Fig. 6) by evolving a two-pronged defense strategy. The strategy allows developing secure adaptors through strict cyber security procedures comprising of authentication, availability and confidentiality requirements by choosing proper nodes for solution implementation. The second component of the strategy has an independent intelligent module that may provide calibration support and comparison in real time from the reference library of sensors and actuators stored elsewhere in the system.

In the event of a cyber-attack on a CPS designed for HRC, the effects of cyber perturbations reach ultimately to the human working with the robot. It is required to make a mitigation plan based on a protective architecture that can support the CPS under attack. To build a secure CRCPS, we are proposing a two-pronged strategy in which the first part will take care of the interconnected nodes and the enhanced data security at important adaptor nodes. The node authentication and data integrity check procedures are adopted for all the adaptor nodes between the CC and other components such that in the case of a compromised CC, the remaining CPS can be secured and take decision for its survival. The second part of the strategy is to develop an intelligent module to see the health check of the costly PC and reporting it to the main control room in the industrial scenario, for making decisions on further options if a compromised CC is detected.

In cyber security schemes, the concept of physical status checks reflects information from the physical execution, rather than theoretical flaws in the algorithm. This concept can be used for a preventive security strategy based on physical parameter checks to identify whether the system is under attack. The original concept is to cater against ‘side channel attacks’ [43, 44]. Some examples are timing information, power consumption or electromagnetic leaks. Moreover, heat dissipation measurement from a chip and acoustic signals can be exploited for target system disruption. Based on such information, side-channel attacks are developed based on statistical tools [40]. In the CRCPS security strategy, the side channel attack theory is used to conceptualize the physical parameter measurement at key nodes, devices, and PC which can diagnose the system under attack [45].

The proposed security framework is based on the assumption that a cyber-shield installed at CC acts as a standard IT system security protection that will comprehend the cyber-attack. A designed cyber-attack for CPS can arrive only through CC, but actually, perturb the control layer to cause damage to PC. So, this is a pre-assumption that CC and any further secure modules in the CRCPS having similar shields can also be compromised. An incoming cyber-attack has the possibility to effect the important basic functionality of the CPS if the layers after CC come under control by the attack. A redundant control system to run such basic system functionalities of PC can be proposed in the event of CC under attack, but its switching mechanism is hard to conceive. Again, an independent, intelligent module is required to find out the system status in real time. One such technique would be the comparison of real-time physical parameters of sensors with the pre-stored specifications information. There must also be an option in the case of CRCPS to come to a manual industrial scenario if the independent module (IM) reports of a less efficient system due to an attack. On the physical aspect, the collaborative system is designed for safe and secure working of humans near functional industrial robots. The goal of a possible cyber-attack on such a system is to break the system security, get the control of a possible sensor and actuator nodes, corrupt the data and then disturb the CRCPS functionality. A cyber-attack scenario on CRCPS is shown in figure 5 and the possible ways and means to infiltrate into the system are discussed. Additionally, the defense strategy framework is highlighted in the face of a cyber-attack.

As shown in Figure 6, node authentication and data integrity check procedures are installed at the adaptor nodes adjacent to CC in order to avoid the spread of cyber-attack beyond CC and to safeguard the costly PC. The node authentication checks include the handshaking procedure followed by the security key parameters identification and then generation, exchange and verification of a security certificate. An encryption algorithm can also be proposed especially for the nodes where confidentiality is required, e.g., system health report generated by the IM needs a confidential path to the HC or to any centralized place for human notice and further intervention. The routing for the IM can be checked for man-in-the-middle (MiM) type of attack. In MiM attack, the attacker modifies the communication among parties who trust the channel for communication with each other. Active eavesdropping is an example of MiM attack in which the attacker develops self-directed connections with the targets. The attacker transmits signals among the parties and the whole exchange is organized by the attacker. A similar MiM check can be introduced for the nodes between CC and PC. The IM is proposed as a strategy to find out the CRCPS health and efficiency under a cyber-attack. The IM consists of a system comparator to compare the real-time sensors and actuators parameters with the pre-stored specifications library. Any reduction in the efficiency of PC can be monitored by IM and report directly to a central control for human intervention for further decision making.

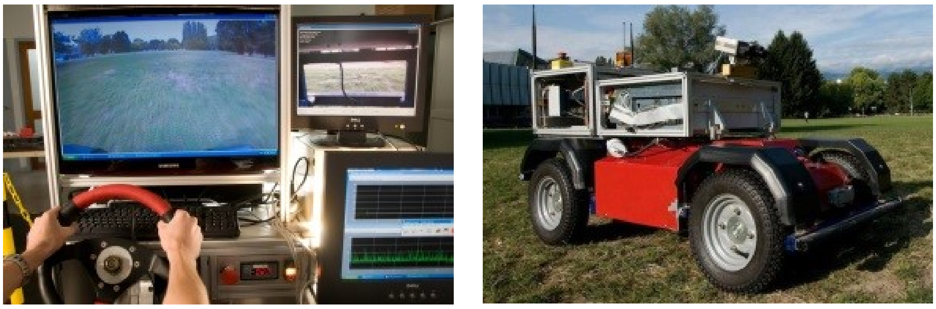
However, there exists a fundamental issue to be unsolved about the cause of such unusual behavior in physical parameters or in readings of IM. The reasons can be identified in two ways. One may be due to the cyber-attack and the other may be due to the erroneous behavior of the sensor, chip or a machine due to some malfunction. The important point is to differentiate between the system under cyber-attack versus the erroneous behavior of the system. There are protocol verification methods in which both hardware and software verification is conducted through system simulation in advance of the system operation. However, to ensure system reliability during operation, the machines must be enabled to do the verification process on their own. Self-verifying or self-learning machines may also make use of the adjustment algorithms to cater for the aging of the physical systems, may look for the intentional and unintentional faults and better predict and alarm in an accurate way against cyber-attacks.

There are self-verification approaches like building multi-compartment [46, 47] or container modules [48]. Such methods can be valuable in tackling with strange system performance within modules and to search for the real source of the malfunction. For example, the container approach is a system integration strategy that takes the individual modules and components from different unverified and potentially malicious sources and constructs a safe and correct overall system. The container approach encapsulates intellectual property (IP) blocks in verifiable modules. Every IP component is placed inside a container, which actually implements the required protection mechanisms. Every container has multiple layers of verification arrangements and protection checks that depend on the acceptable overhead. The integration of such containers ensures the surrounding system to work securely.

6. Benchmark Setup for demonstration of CRCPS

We aim to discuss a scenario where we can simulate the proposed scheme on a real time system. Since, the full-scale implementation of a highly precise, multi-DOF robotic platform is under development, we have demonstrated a simplified version of the proposed algorithm on a network is driven teleoperation setup. As mentioned above, the proposed security framework is a two-step methodology based on the enhanced data security for interconnected nodes and an intelligent system health monitor for real-time mitigation of cyber-attacks.

A teleoperation setup for drive by the wireless application is considered as a generalized CRCPS for simulation of the proposed strategy. Such systems are very popular in applications involving operation in dirty, dangerous and difficult to access places [49, 50]. For long range teleoperation, wireless networks are preferable; however, control over a wireless network presents some challenges due to inherent communication link issues [48]. The classical configuration of Master/Slave parts is retained in our demo while improving the position control algorithm for real-time implementation. A fuzzy controller is used to accommodate the degrading quality of service (QoS) of the control and video flows by varying the packet rate of the video frame. Moreover, the adaptive scheme implemented on this test bench permits to improve the telepresence even in the presence of delays and packet losses up to an acceptable level based on the subjective quality of service. The proposed scheme is successfully incorporated on a benchmark setup where the passivity-based controller with adaptive neuro-fuzzy monitoring loop for QoS control is implemented.



(a) (b)

Fig. 7 Drive by Wireless – (a) Driver at remote station using stereo vision (b) Teleoperation test bench Vehicle

A drive-by-wireless system is a collaborative CPS in which the mechanical linkages and transmissions are replaced by electronic systems and electrical wires. Multisensory data is passed to a data acquisition and computational platform, which transfer the electrical energy into mechanical motion. There are different types of drive-by-wire systems, so more generally, it is referred to as ‘x-by-wire’ [51]. This paper describes a drive-by wireless teleoperation application in which the test vehicle is designed to be remotely teleoperated from an active steering wheel platform (Mater station) which is equipped with a 3D stereo vision system as shown in Fig. 7. Bilateral teleoperation is performed using wheel contact torque measurements and feedback for force deflection; whereas, the wireless connection allows to test coding algorithms in the presence of packet loss and transmission delays.

The scattering based transformation is supplemented with a packet loss strategy by an observer to choose between the hold last sample (HLS) and zeroing. The gain of position control loop is time-varying with respect to delay while ensuring the passivity-based stability condition [52]. The system block level diagram is shown in Fig. 8, where the nominal teleoperation loop is supplemented by a feedback loop which keeps a track of network performance for the control of QoS [53].

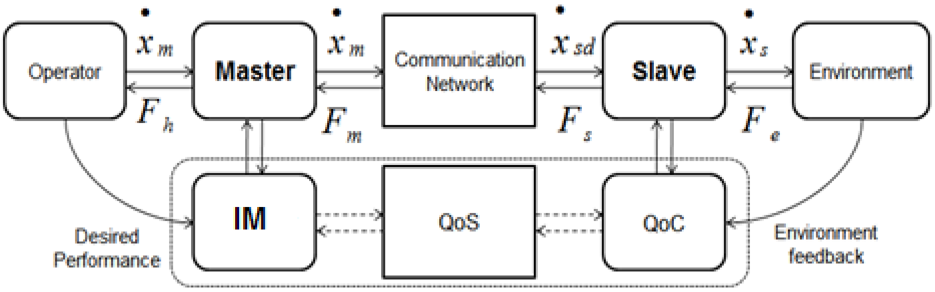


Fig. 8 Teleoperation architecture with Master/Slave stations and intelligent module (IM)

Requirements and Challenges: The position control loop of the master/slave tracks the position and force commands as shown in Fig. 8. In [54], a detailed survey of techniques in bilateral teleoperation is presented. The single degree of freedom (DOF) master/slave dynamics with position control loop in standard notation are given as:

$$M_m \ddot{x}_m + B_m \dot{x}_m = F_h + F_m \qquad (1)$$

$$M_s \ddot{x}_s + B_{s1} \dot{x}_s = F_s - F_e \qquad (2)$$

Where, x_m is the velocity of the steering command at the master station; F_h and F_m establish the force pair applied to the motors at the master/slave; M_m, M_s are the inertias; B_m, B_{s1} are the viscous frictions of master and slave; F_h, F_e are the reaction couple from the operator and the environment; while the x_m, x_s are the respective positions. $F_{feed} = K(x_m(t-\tau)-x_s)$ and $F_{back} = K(x_s(t-\tau)-x_m)$ are the position controllers for the slave and master stations respectively. Instead of transmitting original force and velocity variables, the scattering transformation based passivity control algorithm is used under the assumption of a constant time delay (τ). Following transformation is used to calculate the scattering variables [55]:

$$U_m = \frac{1}{\sqrt{2b}}(F_m + b\dot{x}_m), \;\; V_m = \frac{1}{\sqrt{2b}}(F_m - b\dot{x}_m) \qquad (3)$$

$$U_s = \frac{1}{\sqrt{2b}}(F_s + b\dot{x}_{sd}), \;\; V_s = \frac{1}{\sqrt{2b}}(F_s - b\dot{x}_{sd}) \qquad (4)$$

Where, 'b' is the virtual impedance of the transmission line. These scattering variables (u_m, u_s, v_m, v_s) are transferred across the wireless channel instead of the original forces and velocities. The transient error is delay dependent whereas, the steady state position tracking $e(t) = x_m(0)-x_s(0)$ depends on the position difference at the start up even without any packet loss.

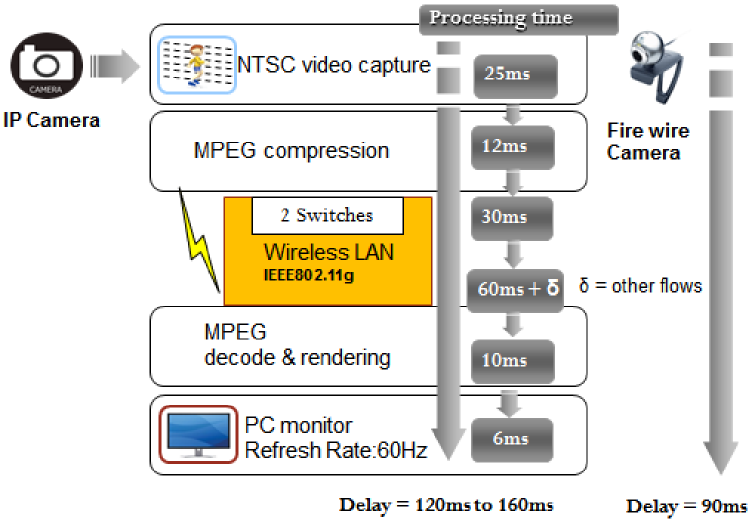


Fig. 9 Delay comparison with IP camera (25 fps with MPEG compression) and FireWire Camera (33 fps with JPEG compression)

Nevertheless, the performance of the control loop deteriorates even further with packet losses. The position tracking error is defined as e = $x_m(t-\tau)-x_s(t)$, where $x_m(t-\tau)$ is the delayed master position received on the slave side. To ensure stability, we assume that the human operator and the environment model are passive systems, bounded by known functions of the master and the slave velocities. All signals are assumed to belong to the extended l_{2e} space and x_m, x_s = 0 for t < 0. For the identification of the vehicle model (J_s, B_{s1}) between the wheel angular position θ_v and the motor torque τ_{mot}, a pseudo random binary signal (PRBS) is injected to the steering motor in open loop. As a consequence, the steering wheel starts to oscillate with a variable angular speed. Assuming a first order model, the transfer function in a closed loop with proportional gain k_α is given as:

$$G_0(s) = \frac{\dot{\theta}_v}{\tau_{mot}} = \frac{k_\alpha}{1+T_p s} = \frac{1}{B_{s1}+J_s s} \qquad (5)$$

Thus, the parameters to identify correspond to $J_s = T_p/k_\alpha$ and $B_0 = 1/k_\alpha$. Using the system identification toolbox of Matlab, the resulting values for the inertia and the viscosity are J_s = 0.0325 kg.m^2 and B_s = 0.072 N.m.rad^{-1}s respectively.

Fault Scenario: We are considering a medium intensity attack on CRCPS operated over IEEE 802.11b/g (WLAN) i.e. a distributed denial of service (DDoS) such that the controllability of the closed loop teleoperation is threatened because of the unavailability of the network resources for some specific period. It is assumed that the attacker is able to breach the security and is capable to add multiple network traffic flows thus congesting the wireless network. This results in significant if not complete loss of command data from the operator's station. The attack pattern severely affects the QoS and consequently the QoC of the teleoperator.

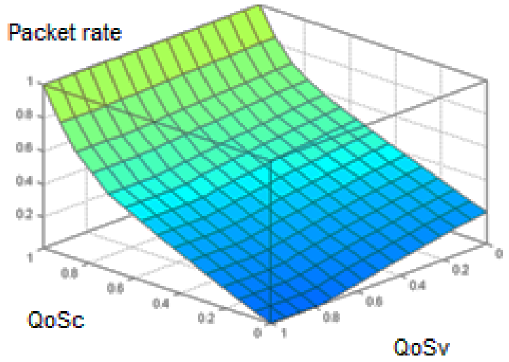


Fig. 10 Fuzzy Packet rate surface with varying QoSc and QoSv

Prototyping and results: Dual cameras and compression schemes were compared in an effort to reduce the video feedback delay as much as possible. As shown in Fig. 9, the IP-camera with 25 frames per second (fps) is found to give an end-to-end delay of 120-160 ms inclusive of communication retard; whereas, the Firewire camera is found to provide a delay around 90 ms with JPEG compression while using the same rest of the hardware as in the first scenario. In a saturated network, keeping frame rate constant if we increase packet rate, it will increase the delay. So, it is important to see the relationship between the driver performance and packet rate and always find the global minimum on this curve. We designed a fuzzy controller for ensuring the quality of service of video flow (QoS_v) as well as the control flow (QoS_c) by varying the packet rate of the video as a controlling parameter in our teleoperation application. Neuro-fuzzy approaches are found popular in such applications recently as found in [56, 57]. The real-time control algorithm is implemented on the NeCS-Car benchmark located at the Department of Control Systems, GIPSA-lab, France. Detailed design steps are discussed in [58].

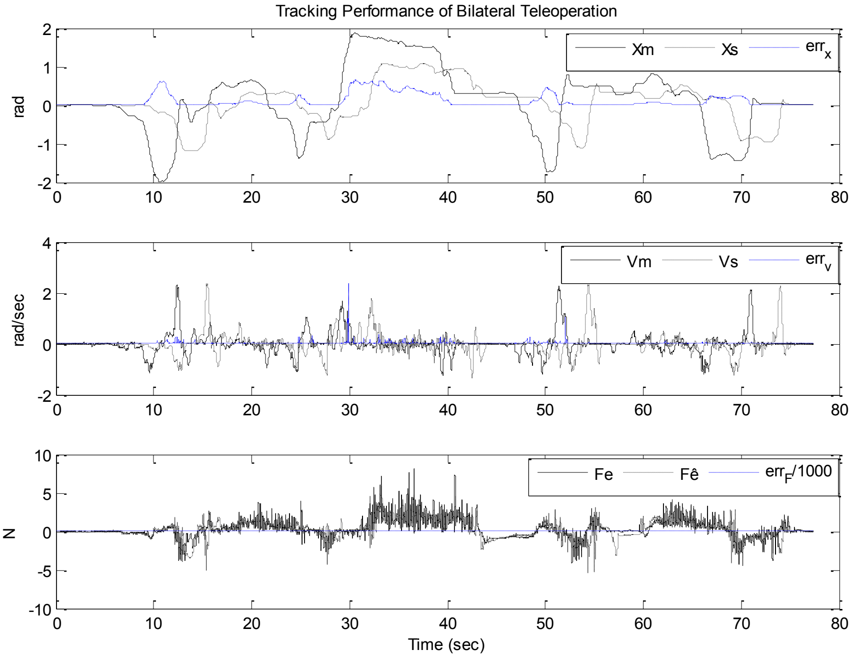


Fig. 11 Evolution of tracking performance with changing QoS

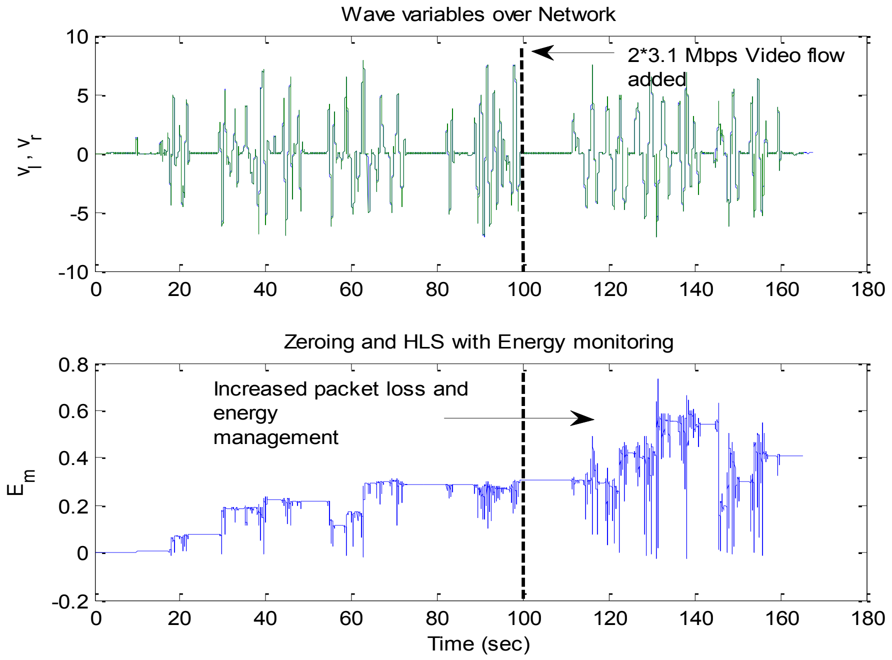


Fig. 12 Wave variables over network with energy monitoring

A fuzzy controller is used to real time evaluation of the QoS for control and video flows. Fig. 10 shows a 3D surface showing the distribution of packet rate w.r.t. the quality of service mapping for video and control flows. The variables with subscript ‘m’ and ‘s’ show the master and slave displacement, velocity and forces respectively. The errors namely err$_X$, err$_X$ and err$_F$ depict the errors in these measurements when the NeCS car is teleoperated on a zigzag track. The results in Fig. 11 show the tracking performance of the teleoperation variables with error signals in position, velocity and force variable. The packet loss effect on the system stability is pronounced in terms of energy injection into the system as it can violate the passivity criteria of the control loop. In this energy monitoring strategy, the input wave energy $\sum_k u_l^2(k)$ is sent over the forward path and $\sum_k v_r^2(k)$ for the backward path of the network. The Same data packet is used for the energy data transmission as the one used to exchange the wave variable information to minimize the network traffic.

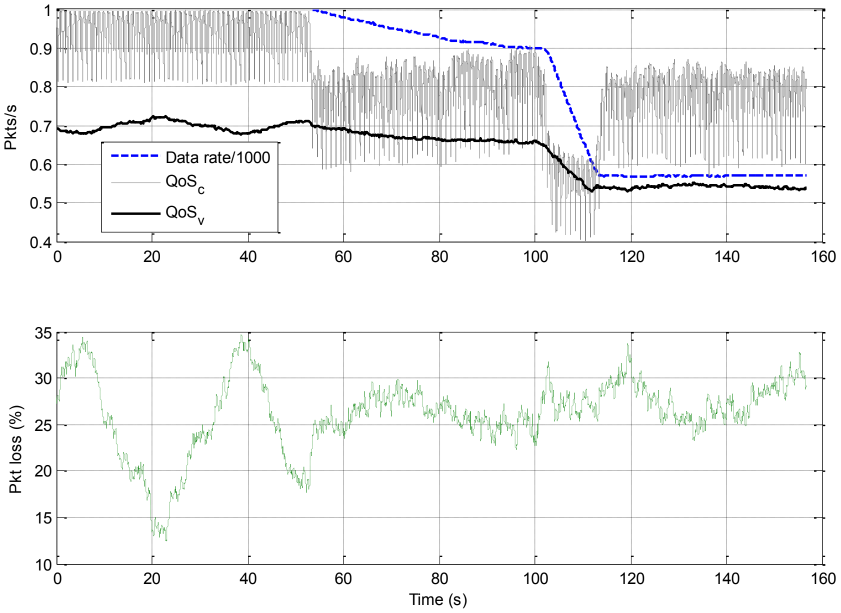


Fig. 13 Reconfiguration scenario with varying QoSv and QoSc

The forward and backward virtual energies are $E_{v,f}(N)$ and $E_{v,b}(N)$ respectively which is defined as the difference of the consecutive intervals of wave energy input as follows:

$$E_{v,f}(N) = \sum_{k=0}^{k*} u_l^2(k) - \sum_{k=0}^{N} u_r^2(k) \qquad (6)$$

$$E_{v,b}(N) = \sum_{k=0}^{k*} v_r^2(k) - \sum_{k=0}^{N} v_l^2(k) \qquad (7)$$

It is known that keeping both $E_{v,f}(N)$ and $E_{v,b}(N)$ as non-negative, the passivity condition can be satisfied. Energy supervised data reconstruction provides an easy approach to keep the system stabilized while selecting between the zeroing and HLS based on the sign of the criteria as shown in Fig. 12 after implementing the following criteria.

$$E_{c,in}(N) = \sum_{N}^{k=0} u_l^2(k) - u_r^2(k) + v_l^2(k) - v_l^2(k) \geq 0 \qquad \forall N \in \mathrm{Z} \qquad (8)$$

As shown above, the QoS requirements are managed by controlling the QoS of the communication network, the benchmark setup still have vulnerabilities e.g. “teardrop”, which is a UDP attack and “overlapping fragment” which can bypass the MAC layer to gain access of the victim node [59]. Thus, the malicious intruder can carry out a DoS attack by either UDP or TCP flooding to deliberately block the communication between the master and slave station which is crucial for the control of the electric vehicle. Based on the detection of a simulated DoS attack by adding video flows over the network at 55 s and 100 s, the reconfiguration logic deliberately reduces the QoSv to maintain QoSc as much as possible as demonstrated in Fig. 13. However, in case, the delay exceeds 500 ms, it is assumed that the fault has developed in a communication failure, thus an emergency stop command is released from the slave system to apply immediate braking sequence. This emergency action is independent of the Master station. Fig. 14 demonstrates the timing diagram for the real time control of the teleoperator. The diagnosis is based on the estimation from the force, velocity and position sensors which results in loss of transparence as the QoS deteriorate.

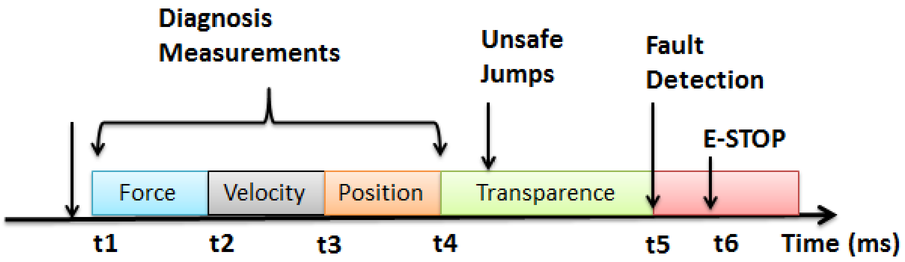


Fig. 14 Timing sequence for emergency stop

The paper demonstrates a security framework for collaborative CPS based on a two-pronged strategy where the impact of this methodology is demonstrated on a teleoperation benchmark (NeCS-Car). Previously, a collaborative CPS is only visualized in theoretical perspective and the CPS literature lacks in a possible secure mitigation plan with a real industrial perspective. The generalized application framework can be easily applied to any other industrial system with higher complexity, thus it is hoped to provide enlightened vision and multidirectional future horizons.

7. Conclusion

A secure CPS is required in order to protect the costly physical elements. The security of CPS is challenged by ever increasing intelligent cyber-attack developed with the target's structural insight. The paper highlighted the fact that the key to the development of an effective mitigation plan for the security of CPS requires the knowledge of the structure of cyber-attack and cyber-physical interconnection properties of the system. The previous work in this domain covers the intelligent cyber-attacks on CPS, but the comprehensive mitigation strategies are missing so far. Cyber-security measures are mostly limited to cyber layer of the CPS, whereas industrial protection systems are rigid, less intelligent and resilient against dynamic disturbances caused by the cyber-attacks. In this context, the CRCPS is proposed with the aim to avoid critical life threatening situations for the worker collaborating with heavy payload industrial robots. The method in the CRCPS design is the merger of security and safety strategies in a single framework. The resulting security framework is also based on a CRCPS structure in which the HC is well linked through diverse adaptor technologies with PC and CC.

One of the important functions of cyber-attack is the reconnaissance of the target physical asset through the control or cyber layer that reveals valuable information. The CRCPS's controllability is affected by the attacker's ability to design a cyber-attack that challenges explicit characteristics directed by functional necessities. The extent gained by the attacker depends upon the damage on the cyber layer properties by the confidentiality, integrity and availability attacks. We proposed the scalability of cyber-attacks towards the system's physical outcomes as stability disturbance for a short period and reduced sensor efficiency poses low to medium level threats. The problem in defining the exact categories of attacks is a difficult estimate, as the threat ability of these attacks is always on the rise due to continuously advancing attack algorithms. In that case, an attack considered as a low level may harm the target to a serious effect. A security approach or a mitigation plan against cyber-attacks must have robust characteristics. The robustness is required specifically for controllability of the CRCPS. As a non-linear system, the controllability and observability properties can jeopardize in the case of attacker gain and defender loss of the system. The security framework highlighted the risk hotspots and the type of attacks possible. It may also lead up to the quantification of risk metrics derived from the scalable extent of the attack. We reduced the number of cyber properties and identified authentication, availability, and confidentiality as important ones to CRCPS. The paper presented the detailed security requirements of CRCPS before proposing a security mitigation plan against cyber-attacks on such systems.

The paper analyses cyber vulnerabilities in CRCPS and demonstrated cyber-attack impact on different elements of a control loop. The elements that can be impacted include sensor measurements, actuator signals, controllers and reference signals. The system vulnerability in terms of controllability and security attributes show the relevance of SISO and MIMO systems in designing CPS. MIMO systems are preferable as decentralized control can perform better for cyber-security. For designing countermeasures in such systems, the system must exhibit an attack detection feature. The paper emphasizes on intelligent physical parameter check; e.g. side channel attacks in cryptography, to identify whether the system is under attack. However, the strategy cannot differentiate the system under attack status from the aging effects on a system. To preserve the confidentiality within a CRCPS, the use of an encrypted data bus is considered to be useful, as the attacker reads data without a decryption key. This may specifically provide a benefit for system security if the physical access to a data port is made. A lightweight demonstration is presented over NeCS-Car teleoperation test-bench. Moreover, it has been demonstrated that controlling the QoS alone to improve the QoC is not sufficient without securing the intelligent communicating nodes of the overall architecture. It is recommended to consider using IP security protocols (IPSec) or its improved versions to enhance the security of CRCPS further. In future, we will develop the validated design guideline for security framework of the complex multi-degree of freedom collaborative CPS, with quantifiable risk analysis and follow a robust approach towards security framework design by dealing with the drawbacks of IPSec protocol for CRCPS implementation.

Acknowledgments: The authors would like to acknowledge the support of the cLINK (Centre of excellence for Learning, Innovation, Networking and Knowledge), Erasmus Mundus Programme of the European Union, the InSA Project, sponsored by the German Federal Ministry for Economic Affairs & Energy (Project register number: HRB 24505 HB) and the NeCS team at GIPSA-lab/INRIA, Grenoble, France for their support in experimentation over teleoperation test-bench.

References

[1] E. A. Lee, "Cyber physical systems: Design challenges," in *Object Oriented Real-Time Distributed Computing (ISORC), 2008 11th IEEE International Symposium on*, 2008, pp. 363-369.

[2] L. Monostori, "Cyber-physical production systems: Roots, expectations and R&D challenges," *Procedia CIRP,* vol. 17, pp. 9-13, 2014.

[3] V. VDE. Industrie 4.0 Wertschöpfungsketten, Statusreport [Online].

[4] S. Sunder, "Foundations for innovation in cyber-physical systems," in *proceedings of the NIST CPS Workshop, Chicago, IL, USA*, 2012.

[5] J. IQBAL, Z. H. KHAN, and A. KHALID, "Prospects of robotics in food industry," *Food Science and Technology (Campinas),* pp. 0-0, 2017.

[6] A. A. Khan, S. A. Khan, and Z. H. Khan, "Distributed Control of Multiple Plants over Embedded Network," *Int. J. Com. Dig. Sys,* vol. 6, 2017.

[7] M. Foehr, J. Vollmar, A. Calà, P. Leitão, S. Karnouskos, and A. W. Colombo, "Engineering of Next Generation Cyber-Physical Automation System Architectures," in *Multi-Disciplinary Engineering for Cyber-Physical Production Systems*, ed: Springer, 2017, pp. 185-206.

[8] S. Plósz, C. Schmittner, and P. Varga, "Combining Safety and Security Analysis for Industrial Collaborative Automation Systems," in *International Conference on Computer Safety, Reliability, and Security*, 2017, pp. 187-198.

[9] A. Hahn, R. K. Thomas, I. Lozano, and A. Cardenas, "A multi-layered and kill-chain based security analysis framework for cyber-physical systems," *International Journal of Critical Infrastructure Protection,* vol. 11, pp. 39-50, 2015.

[10] A. Khalid, P. Kirisci, Z. Ghrairi, K.-D. Thoben, and J. Pannek, "A methodology to develop collaborative robotic cyber physical systems for production environments," *Logistics Research,* vol. 9, p. 23, 2016.

[11] A.-S. K. Pathan, *Securing cyber-physical systems*: CRC Press, 2015.

[12] S. H. Khan, M. A. Akbar, F. Shahzad, M. Farooq, and Z. Khan, "Secure biometric template generation for multi-factor authentication," *Pattern Recognition,* vol. 48, pp. 458-472, 2015.

[13] C. B. Zamfirescu, B. C. Pirvu, J. Schlick, and D. Zuehlke, "Preliminary insides for an anthropocentric cyber-physical reference architecture of the smart factory," *Studies in Informatics and Control,* vol. 22, pp. 269-278, 2013.

[14] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," *Reliability Engineering & System Safety,* vol. 139, pp. 156-178, 2015.

[15] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security,* vol. 15, pp. 39-68, 2007.

[16] N. Falliere, L. O'Murchu, and E. Chien, "W32. Stuxnet dossier (version 1.4). Symantec," ed, 2011.

[17] M. Zeller, "Myth or reality—Does the Aurora vulnerability pose a risk to my generator?," in *Protective Relay Engineers, 2011 64th Annual Conference for*, 2011, pp. 130-136.

[18] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommunication Systems,* vol. 50, pp. 217-241, 2012.

[19] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: requirements and challenges for the 21st century," *International journal of critical infrastructure protection,* vol. 8, pp. 53-66, 2015.

[20] A. Pichler, S. C. Akkaladevi, M. Ikeda, M. Hofmann, M. Plasch, C. Wögerer*, et al.*, "Towards shared autonomy for robotic tasks in manufacturing," *Procedia Manufacturing,* vol. 11, pp. 72-82, 2017.

[21] A. Khalid, P. Kirisci, Z. Ghrairi, J. Pannek, and K.-D. Thoben, "Safety Requirements in Collaborative Human–Robot Cyber-Physical System," in *Dynamics in Logistics*, ed: Springer, 2017, pp. 41-51.

[22] A. Riel, C. Kreiner, G. Macher, and R. Messnarz, "Integrated design for tackling safety and security challenges of smart products and digital manufacturing," *CIRP Annals-Manufacturing Technology,* 2017.

[23] T. B. Rasmussen, G. Yang, A. H. Nielsen, and Z. Dong, "A Review of Cyber-Physical Energy System Security Assessment," in *12th IEEE Power and Energy Society PowerTech Conference*, 2017.

[24] A. A. Nazarenko and L. M. Camarinha-Matos, "Towards collaborative Cyber-Physical Systems," in *Young Engineers Forum (YEF-ECE), 2017 International*, 2017, pp. 12-17.

[25] I. Zinnikus, A. Antakli, P. Kapahnke, M. Klusch, C. Krauss, A. Nonnengart*, et al.*, "Integrated Semantic Fault Analysis and Worker Support for Cyber-Physical Production Systems," in *Business Informatics (CBI), 2017 IEEE 19th Conference on*, 2017, pp. 207-216.

[26] H. Chao, Y. Chen, and J. Wu, "Power saving for machine to machine communications in cellular networks," in *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, 2011, pp. 389-393.

[27] Z. H. Khan, J. M. Thiriet, and D. Genon-Catalot, "Wireless network architecture for diagnosis and monitoring applications," in *Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE*, 2009, pp. 1-2.

[28] B.-C. Pirvu, C.-B. Zamfirescu, and D. Gorecky, "Engineering insights from an anthropocentric cyber-physical system: A case study for an assembly station," *Mechatronics,* vol. 34, pp. 147-159, 2016.

[29] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya*, et al.*, "Secure vehicular communication systems: design and architecture," *IEEE Communications Magazine,* vol. 46, 2008.

[30] D. Gorecky, R. Campos, and G. Meixner, "Seamless Augmented Reality support on the shopfloor based on cyber-physical-systems," in *Proceedings of the 14th International Conference on Human-computer Interaction with Mobile Devices and Services*, 2012.

[31] M. Schmitt, G. Meixner, D. Gorecky, M. Seissler, and M. Loskyll, "Mobile interaction technologies in the factory of the future," *IFAC Proceedings Volumes,* vol. 46, pp. 536-542, 2013.

[32] A. Chattopadhyay, A. Prakash, and M. Shafique, "Secure Cyber-Physical Systems: Current trends, tools and open research problems," in *2017 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2017, pp. 1104-1109.

[33] R. Elder, "Defending and operating in a contested cyber domain," *Air Force Scientific Advisory Board, Winter Plenary,* 2008.

[34] I. Akkaya, P. Derler, S. Emoto, and E. A. Lee, "Systems engineering for industrial cyber–physical systems using aspects," *Proceedings of the IEEE,* vol. 104, pp. 997-1012, 2016.

[35] A. Caruso, S. Chessa, S. De, and A. Urpi, "GPS free coordinate assignment and routing in wireless sensor networks," in *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, 2005, pp. 150-160.

[36] J. R. Douceur, "The sybil attack," in *International Workshop on Peer-to-Peer Systems*, 2002, pp. 251-260.

[37] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *Proceedings of the 3rd international symposium on Information processing in sensor networks*, 2004, pp. 259-268.

[38] A. Perrig, R. Canetti, D. Song, and J. D. Tygar, "Efficient and secure source authentication for multicast," in *Network and Distributed System Security Symposium, NDSS*, 2001, pp. 35-46.

[39] M. Moghaddam and S. Y. Nof, "The collaborative factory of the future," *International Journal of Computer Integrated Manufacturing,* vol. 30, pp. 23-43, 2017.

[40] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Annual International Cryptology Conference*, 1996, pp. 104-113.

[41] Y. Sung-Ming and L. Kuo-Hong, "Shared authentication token secure against replay and weak key attacks," *Information Processing Letters,* vol. 62, pp. 77-80, 1997.

[42] N. Kheir, N. Cuppens-Boulahia, F. Cuppens, and H. Debar, "A service dependency model for cost-sensitive intrusion response," in *European Symposium on Research in Computer Security*, 2010, pp. 626-642.

[43] S. Chen, R. Wang, X. Wang, and K. Zhang, "Side-channel leaks in web applications: A reality today, a challenge tomorrow," in *Security and Privacy (SP), 2010 IEEE Symposium on*, 2010, pp. 191-206.

[44] J. Ambrose, A. Ignjatovic, and S. Parameswaran, *Power Analysis Side Channel Attacks: The Processor Design-level Context*: VDM Publishing, 2010.

[45] J. Giraldo, E. Sarkar, A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "Security and Privacy in Cyber-Physical Systems: A Survey of Surveys," *IEEE Design & Test,* 2017.

[46] J. Porquet, C. Schwarz, and A. Greiner, "Multi-compartment: a new architecture for secure co-hosting on SoC," in *System-on-Chip, 2009. SOC 2009. International Symposium on*, 2009, pp. 124-127.

[47] J. Sepúlveda, G. Gogniat, R. Pires, W. Chau, and M. Strum, "Security-enhanced 3D communication structure for dynamic 3D-MPSoCs protection," in *Integrated Circuits and Systems Design (SBCCI), 2013 26th Symposium on*, 2013, pp. 1-6.

[48] R. Drechsler and U. Kühne, "Safe IP integration using container modules," in *Electronic System Design (ISED), 2014 Fifth International Symposium on*, 2014, pp. 1-4.

[49] H. Zhong, J. P. Wachs, and S. Y. Nof, "A collaborative telerobotics network framework with hand gesture interface and conflict prevention," *International Journal of Production Research,* vol. 51, pp. 4443-4463, 2013.

[50] H. Zhong, J. P. Wachs, and S. Y. Nof, "Telerobot-enabled HUB-CI model for collaborative lifecycle management of design and prototyping," *Computers in Industry,* vol. 65, pp. 550-562, 2014.

[51] A. Mechraoui, Z. H. Khan, and J.-M. Thiriet, "Effect of packet loss on the quality of control of a networked mobile robot," in *30th IFAC Workshop on Real-Time Programming and 4th InternationalWorkshop on Real-Time Software*, 2009, pp. 97-101.

[52] S. Hirche and M. Buss, "Packet loss effects in passive telepresence systems," in *Decision and Control, 2004. CDC. 43rd IEEE Conference on*, 2004, pp. 4010-4015.

[53] Z. H. Khan, J.-M. Thiriet, and D. Genon-Catalot, "Drive-by-wireless teleoperation with network qos adaptation," *International Journal of Engineering Science and Technology,* vol. 2, pp. 160-169, 2011.

[54] T. Hatanaka, N. Chopra, M. Fujita, and M. W. Spong, "Scattering Variables-Based Control of Bilateral Teleoperators," in *Passivity-Based Control and Estimation in Networked Robotics*, ed: Springer, 2015, pp. 51-70.

[55] N. Chopra, M. W. Spong, R. Ortega, and N. E. Barabanov, "On tracking performance in bilateral teleoperation," *Robotics, IEEE Transactions on,* vol. 22, pp. 861-866, 2006.

[56] Z. Li, W. Wang, and Y. Jiang, "Managing quality of control and requirement-of-bandwidth in networked control systems via fuzzy bandwidth scheduling," *International Journal of Control, Automation, and Systems,* vol. 7, pp. 289-296, 2009.

[57] Y. Yang, C. Hua, and X. Guan, "Adaptive fuzzy finite-time coordination control for networked nonlinear bilateral teleoperation system," *Fuzzy Systems, IEEE Transactions on,* vol. 22, pp. 631-641, 2014.

[58] Z. H. Khan, "Wireless Network Architecture for Long range Teleoperation of an Autonomous System," Institut National Polytechnique de Grenoble-INPG, Grenoble, France, 2010.

[59] A. A. El Kalam, A. Ferreira, and F. Kratz, "Bilateral Teleoperation System Using QoS and Secure Communication Networks for Telemedicine Applications," *IEEE Systems Journal,* vol. 10, pp. 709-720, 2016.