electronics

MDPI

Article

Cybersecurity of Robotic Systems: Leading Challenges and Robotic System Design Methodology

Vibekananda Dutta [1,*] and Teresa Zielińska [2]

[1] Institute of Micromechanics and Photonics, Faculty of Mechatronics, Warsaw University of Technology, 00-661 Warsaw, Poland
[2] Institute of Aeronautics and Applied Mechanics, Faculty of Power and Aeronautical Engineering, Warsaw University of Technology, 00-661 Warsaw, Poland; teresaz@meil.pw.edu.pl
* Correspondence: vibekananda.dutta@pw.edu.pl

Abstract: Recent years have seen a rapid development of the Internet of Things (IoT) and the growth of autonomous robotic applications which are using network communications. Accordingly, an increasing advancement of intelligent devices with wireless sensors (that means autonomous robotic platforms) operating in challenging environments makes robots a tangible reality in the near future. Unfortunately, as a result of technical development, security problems emerge, especially when considering human–robot collaboration. Two abnormalities often compromise the basic security of collaborative robotic fleets: (a) Information faults and (b) system failures. This paper attempts to describe the methodology of a control framework design for secure robotic systems aided by the Internet of Things. The suggested concept represents a control system structure using blocks as the components. The structure is designed for the robots expected to interact with humans safely and act connected by communication channels. The properties of the components and relations between them are briefly described. The novelty of the proposed concept concerns the security mechanisms. The paper also categorizes two different modes of network attacks summarizing their causal effects on the human–robot collaboration systems. The issue of standardization is also raised. In particular, the works of the National Institute of Standards and Technology (NIST) and European Parliament (EP) on the security templates for communication channels are commented.

Keywords: cyber physical system; cyber security; networking technologies; autonomous robots; agents; multi-robot systems; Internet of Robotic Things; artificial intelligence

Citation: Dutta, V.; Zielińska, T. Cybersecurity of Robotic Systems: Leading Challenges and Robotic System Design Methodology. *Electronics* **2021**, *10*, 2850. http://doi.org/10.3390/electronics10222850

Academic Editor: George A. Tsihrintzis

Received: 2 November 2021
Accepted: 15 November 2021
Published: 19 November 2021

1. Introduction

1.1. Background

Robots are often listed as typical examples of a Cyber–Physical System (CPS) with computational and physical abilities. The application of robotic platforms in human society is increasing rapidly. The integration of CPS within the networks equipped with advanced communication channels results in enhanced sensing capabilities, efficient control performance, and timely actions according to real-world parameters [1,2]. Accordingly, Machine-to-Machine (M2M) communication is being progressively scrutinized [3] and therefore, the network security of CPSs has become very significant. Moreover, CPSs conventionally include networked robots equipped with Artificial Intelligence (AI) and interact with human beings in professional or public settings [4–6]. In recent years, robotic applications (e.g., networked robots) have widely supported the physical and cognitive capabilities of elderly and disabled persons or everyday human companions [6–8]. Professional service robots and personal service robots are rapidly advancing, and therefore their security enhancement is crucial [3]. Autonomous robots share social spaces with humans in various environments, such as homes, offices, and even critical infrastructures like airports and banks. Therefore, their security and safety are significant, especially when

taking into account that their autonomy is increasing, and they are expected to act without human intervention.

Today, CPS-aided robotic platforms more often use wireless sensory networks and wireless communication channels, particularly applying the IoT concept. The significant components of networked robots usually incorporate cloud computing resources, embedded systems, and various sensory networks [6,9]. An advanced autonomous robot typically incorporates: (a) A control system; (b) physical components: Various sensors, motors, actuators, appendages (wheels, robotic arms, etc.) to sense the surroundings, to manipulate them and to move; and (c) networking elements using a wireless connection, cloud computing or data repositories. Cloud repositories assist the robots in overcoming the limitations of data storage, limitations of real-time processing speed, or data gathering limitations when using the networked sensors. It is relevant that cloud computing enables robots to manage heavy computational tasks such as navigation, speech, or object recognition [10]. Modern applications of cloud-aided robotics concerns professional service robots (in field robots) [11]; industrial robots [12]; and personal service robots [13].

The cybersecurity of a robotic system depends on the control software, so choosing a software platform is essential not only for the quality of work but also for the system's safety.

Beginning in 2007, like other open-source software, the Robot Operating System (ROS) began to be widely used to design control systems. Its first version, ROS1 [14], offered problem-oriented solutions designed to support interaction and communication between devices of various types and from different manufacturers [15]. Unfortunately, ROS1 had several shortcomings in terms of real-time operations. The system's weakness was manifested in time-critical tasks and did not meet the requirements typical for reliable real-time systems. This was especially noticeable in large-scale automated systems. In the case of ROS applications to support large-scale distributed systems, there were problems with timely communication. So, an improved version of ROS was created, namely ROS2 [16]. The data distribution service (DDS), which is the industry requirement for distributed, real-time embedded systems, has been improved here. Mechanisms of various data transmission options have been expanded while, inter alia, keeping in mind timely communication and fault tolerance. Attention has been paid to ensure scalability [17] by making it easier to add processes. The core of the DDS in ROS2 is DCPS (Publish–Subscribe Data-Centric Model). This standard uses a model of publish–subscribe communication considering the needs of real-time, data-critical applications. The data transfer is carried out considering Quality of Service measures (QoS—a set of metrics focused on network performance which can be technically evaluated and are negotiated) [17]. The applied solution also works well in distributed heterogeneous platforms. The interested reader may refer to [15,17] for a more detailed overview of ROS1 vs. ROS2.

Despite increased capabilities, ROS2 still does not fully meet the stringent time constraints. System designers need to fine-tune timing parameters empirically. Many studies are devoted to methods of time delay analysis [18–20]. Unfortunately, they cannot be directly applied to ROS2 due to its specific task management methods [18]. The problems of delays are still discussed in the literature. Overall, ROS2 has not yet achieved a significant advantage over ROS1. There are still many unresolved issues, including: (a) The functions offered by ROS2 are limited, which limits the range of possible applications, (b) the overall performance of ROS2 compared to ROS1 is not much better. The expected benefits of expanded software interfaces to support hardware have not yet been fully demonstrated, and the cost of hardware that can support ROS1 has dropped significantly. This makes the use of ROS2 still limited.

Despite its shortcomings, ROS is expected to play a dominant role in the near future, not only in research applications but also in commercial robotics. Therefore, researchers devote their attention to the security issues of ROS-based robotic controllers [21].

The safe and efficient control process is very significant for networked autonomous robots. Various studies have revealed how critical it can be for robot behavior during the

fault of sensory readings or during networking problems [22]. In contrast to networked robots, many inexpensive semi-autonomous mobile robots are still performing activities using some set of pre-planned tasks, but their abilities are minimal. Considering current technological trends, it is essential to secure skilful autonomous mobile robots starting from their design and implementation stage and taking into account the level of information processing which requires long-term inter-robot communication (communication level) and the reliability of each robot action requiring the temporary communication with sensory networks (behavior level). The main challenge in networked robotics is the integration of the different intelligent capabilities into one overall system that supports the two above-mentioned communication stages [3,23].

Figure 1 illustrates two abstract levels of communication. The behavioral level concerns local communication within a single robot control system. In such a case, the control system may be implemented on one or more computing nodes. The communication level refers to global communication between multi-robot system controllers or between internet repositories and robot controllers. Modern robotics more often uses knowledge and data collected in internet clouds or works as a multi-robot system, increasing the global communication share.

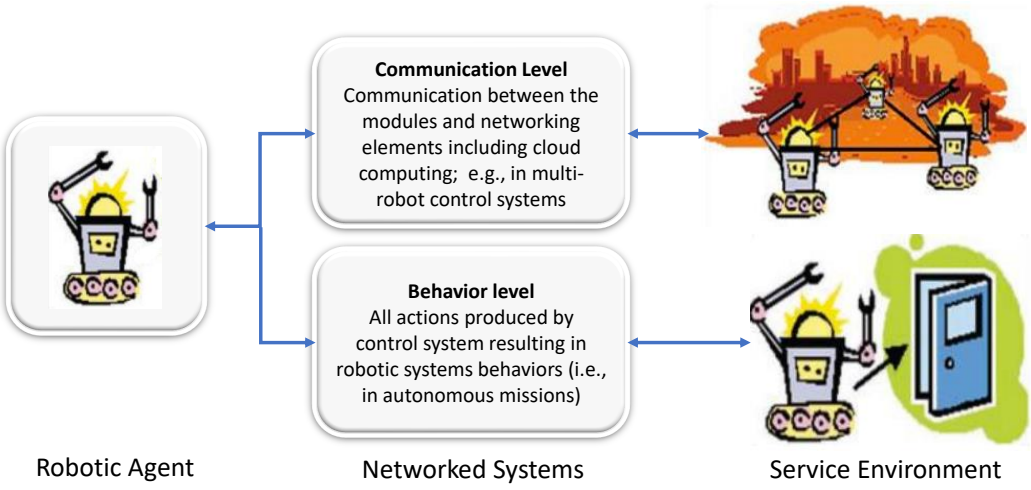

Figure 1. Networked robotic platforms—two levels of communication. Communication level concerns the interaction within the system modules and networking elements. Behavior level delineates local decision making produced by system modules. The idea is adopted from [3].

According to the literature, rapidly developing IoT-aided robotics are now evolving towards the Internet of Everything (IoE), which augments robotic systems with wireless networks, sensory systems, cloud data platforms, open-source middleware, other intelligent devices, and advanced AI technologies. It makes the robotic systems more demanding in the development phase, with security issues being more critical [24,25].

1.2. State of the Art

The security of any CPS (in robots) comprises two elements: (a) Information security; and (b) control security [26]. Information security was first addressed in [27]. Information security is mainly related to data encryption, transmission, and decryption. The safety of the control of the device takes into account attacks on the dynamic performance of that system [28]. That is, its resilience, the stability of its behavior, and the rapid convergence to the action goal are appropriate indicators here.

The security of data and information transmission plays a crucial role in robotic control systems [29]. Complex robotic systems undergo attacks with the aim of [30]: (a) Damaging data and information, (b) violating access rights and system integrity, (c) damaging the logic of their operation. In the works [31,32] the susceptibility to threats and basic types of attacks on robotic systems were discussed. The methods of intrusion prevention are also

presented. In the works [24,33] attention is focused on the role of intelligent connectivity IoRT, on cloud services, and on cloud robotics.

One of the more recent works by Soldatos et al. [34] presents an innovative concept of IoT application for an intelligent system dedicated to assistive robots with social skills. The concept's innovation consists of predicting the correct behavior of robots, which also allows detecting the abnormalities. Radanliev et al. [35] in his latest work, defined a dynamic and self-adapting robotic supply chain system supported by artificial intelligence and machine learning, the system makes predictions of cyber threats. Studies [36,37] are focused on the architecture of the IoT ecosystem, with a view to secure communication. The possibility of repelling the attacks in the IoT system was studied, and their possible impacts were analyzed. These problems were considered using the examples of collaborating robots working in space, on land, and underwater. Machine learning methods were here investigated.

Going farther to this direction, Razafimandimby et al. [38] described how to provide the desired QoS for Internet of Robotic Things (IoRT) by using Artificial Neural Networks (ANNs). Another solution increasing security is presented in [39,40]; it is based on centralized training of cooperating robots and the decentralized execution of their tasks. Guiochet et al. [41] investigated the safety of robotic systems in direct interactions with humans. Jahan et al. [42] reviewed the secure modeling of different autonomous systems, including the robotic ones. Dieber et al. [21] evaluated the security of ROS by applying penetration tests while postulating countermeasures to strengthen security. To Increase robotic control system security, Mayoral-Vilches et al. [43] developed the customized ransomwares.

A lot of research is devoted to communication [44,45]. Intelligent communication is essential for telemanipulation and human-serving robots. Most recently, Bonaci et al. [46] studied safety issues in remotely controlled surgical robots. Quarta et al. [47] empirically analyzed the safety of industrial robots. Such works emphasize the importance of the safety of robots working in factories, in professional, personal services, and so on. Researchers have also analyzed the cybersecurity of robotic systems [48–50] and indicate that security issues should be taken into account at the design stage. On the one hand, this is becoming critical due to the increasing autonomy of modern robots, and the increasing sophistication of attacks that violate the safety of functioning, on the other hand.

Despite their significant advantages and a promising future, networked robotic systems pose serious non-attack resistance problems [51]. Of the relatively limited studies on the cybersecurity of robotic systems, the most common are the theoretical studies of vulnerability to attacks, threats, and risks. The state of the art lacks knowledge of a global understanding of robotics safety. The recommendations are rather limited and point to the need for some general decomposition of system functions in IoT robotics systems. The systematic modularization is not yet applied [29], and there are no methodological recommendations for the design of safe robotic systems.

1.3. Motivation and Objectives

The deployment of robotic systems has been rising significantly over recent years. The corresponding applications are evolving in terms of system configuration, active knowledge or information exchange, system independability, enhanced privacy, and good security protocols [25,52]. In 2000, the National Security Agency (NSA) issued security specifications for IoT implemented in the complex cyber–physical world. It addresses three essential security requirements: (a) Communication, (b) authentication, and (c) cyber security policy development and enforcement [3,53].

Moving forward, the National Institute of Standards and Technology (NIST) and Department of Homeland Security (DHS) distinguished networked and user interfaced robots, e.g., rescue robots, assistive robots, health care robots, caregiver robots, and robots employed for military applications as a class of devices in which the hardware, software, and security functions must be developed simultaneously [54]. The International Federation of Robotics (IFR) [55] predicts the rapid development of service and assistive robots in

the very near future. With this in mind, it should be noted that the issue of IoT ecosystems is still not fully resolved, as legal regulations and security issues vary from country to country. Examples include fragmented, imprecise, and sometimes even contradictory regulations on data access and ownership and on data privacy and protection [56].

The European Parliament (EP) has lately delivered several principles and requirements for cloud robotics [6]. These incorporate the concept of reversibility and inclusion of emergency and protection services. Meanwhile, the General Data Protection Regulation (GDPR) [57] initiated by the European Union (EU) involves: (a) Rules on automated decision-making processes; (b) the right to be forgotten, which means that results should be removed if no longer relevant, irrelevant, or inadequate [33]; and (c) data protection in the design stage [58].

Having explored existing issues raised by different regularity bodies, the motivation for this paper comes from the observation of security enhancement needs in intelligent machines cooperating with humans and using connected networks. We use the term 'robotic things' to refer the IoT robotics. Our particular interest is a collective mechanism that offers services for humans through robotic platforms, embedded sensors, and IoT-aided networks.

This paper attempts to attain several goals of the study: (a) Exploration of the perspective of network design methodology considering communication level and behavior level of robotic systems, (b) scrutinization of the security threats in autonomous robotic systems, and (c) discussion of the lower and higher-level "abilities" of AI applied to robotic communications.

1.4. Problem Statement and Contributions

The inclusion of security mechanisms should ensure an appropriate balance between the efficiency of networked robots and their security levels [31,59]. Taking into account both (a) the state of the art (Section 1.2) and (b) motivation (Section 1.3), the contribution of this work is as follows:

1. Security is discussed, and deliberation given to the categories of robots.
2. The concept of the control system is presented, the semantics of communication are given great consideration.
3. A general concept of the control system decomposition with particular emphasis on network security is given.
4. The role of artificial intelligence techniques in the safety of networked robotic systems is presented.
5. The mitigation of the cyberattack impacts it also addressed.

There are many ways to harm a robotic system, so there are many approaches to making the system more cyber safe. Each of the articles devoted to this issue usually discusses one security problem. This paper aims to provide a general overview of the cybersecurity of robots, taking into account the areas of robot applications and the specificity of robotic control systems. Adequate standards and regulations are also presented. A universal method of decomposition of the control system is proposed by systematizing the safety of robotic systems and introducing the concept of the behavioral and global level of communication in the software system. In this concept, the data/information channels are clearly visible. A data format is proposed that can be easily checked for system intrusions.

1.5. Paper Organization

The remaining part of the paper discusses these contributions in depth. After the introduction, the state of the art, motivation, and objectives, and the authors' contributions are discussed in Section 1. In Section 2, there is a short discussion on IoT-aided robotic systems (Section 2.1) considering the ISO standards with a summary of recent works devoted to Human–Robot Collaboration (HRC) in industry (Section 2.2), professional and personal services (Section 2.3). Section 3 delineates the design methodology of secure Cyber–Physical System-aided robotics considering communication and behavior level

using the concepts of agents. Section 4 discusses the utilization of AI technologies in robotic communications. In Section 5, the authors offer a thorough discussion. Finally, Section 6 ends with conclusions and the possibilities of future directions.

2. Robot Application Domains

2.1. Background

Digital transformation of human society accelerates the development of essential applications in which robotic systems assist, improve, or minimize the continuous human activities [24]. Contemporary robotic systems support additional developments in achieving collaborative human–machine labor tasks. The ongoing development of intelligent systems in the form of collaborative IoT-aided autonomous robotic swarms requires new architectures, new connectivity paradigms, and security mechanisms in industrial domains [24].

When the robots act in an environment close to humans and interact with them, the safety demand tremendously increases. Thus, the human–robot interaction domain has become a growing field of research activities [35]. The contemporary definition of IoT-aided robotic things requires the combination of existing definitions of IoT/IIoT with the terminology used in autonomous systems, collaborative robotics, distributed processing systems, AI, and cloud computing [24].

To address this issue, the denotation of a robotic system issued by ISO 8373 (2012) [60] distinguishes the application areas of robotics considering industrial and service domains. The definition states that the robot is a programmable device which possesses some degree of autonomy and interacts with its environment while performing intended activities. The standard also defines autonomy as the ability to execute the intended tasks without human involvement, taking into account the current state and using the sensing capabilities. In the year 2015 the IEEE 1872 standard provided the set of fundamental definitions. The standard describes the robot as an intelligent system whose purpose is to act in the physical world in order to accomplish one or more tasks. On some occasions, a robot might be subordinate to the actions of other agents, such as humans. Moreover, the robot (or a set of robots) can form robotic systems together with special components to facilitate their work [24].

Moving forward, other standards such as ISO 10218-1, established in the year 2011, provides requirements and guidelines for the essential safety in design methodology and instructions for the use of industrial robots by defining the primary hazards associated with humans and offering preconditions for reducing the dangers associated with these hazards. In addition, ISO 10218-2, established in the same year, specifies safety requirements for the incorporation of industrial robots into industrial systems (defined in ISO 10218-1) and industrial robotic cell(s) by illustrating the possible hazards [24]. This norm offers the requirements to eliminate the risks. The IEEE 1872.1 standard established in 2017 is an extension to IEEE 1872 (2015) that augments the Core Robotics and Automation (CORA) ontology by describing additional ontologies essential for the development of autonomous robotics. The same standard defines an ontology that allows the representation of reasoning about the task in the robotics and automation domain [24]. Table 1 gives the general overview of ISO standards for robotic applications [61].

Following the distinction between the requirements and the features of IoT-aided robotic systems [25], the classification of the robotic system according to application areas is presented in Figure 2. These application areas are in line with the description is given by ISO 8373 (2012) (industrial and service domains) [24].

As shown in Figure 2, the most common applications of industrial robots are the handling operations, followed by welding and assembling. This means that most contemporary industrial robots are still very simple. Operation and welding do not require complicated actions or advanced sensors. No internet resources are needed here either. Professional robots (robots for professional use) are mainly used in logistics services, then in public services and defense. All of these applications require advanced skills and complex

sensory systems and often access to Internet resources. For personal service robots (robots that serve their owners directly), the first most common application is home services (e.g., cleaning), the second is entertainment (advanced robot "toys"), and then other applications. These robots are usually less advanced than professional service robots and use Internet support less frequently. A more detailed description of service robots is provided in Section 2.3. Despite the relative simplicity of most industrial robots, collaborative robots are the future of the industry. These types of robots bring with them new challenges, which will be discussed in the next section.

Table 1. ISO safety standards for robotic solutions.

Type	Name	Description
A	ISO 12100 [62] IEC 61508 [63]	Risk assessment & risk reduction Functional safety of electronic, programmable electronic
B1	ISO 13849-1 [64] IEC 62061 [65]	Safety related part of control systems Functional safety of electronic, programmable electronic
B2	ISO 13850 [66] ISO 13851 [67]	Emergency stop function - Principles for design Two-hand control devices
C	ISO 10218 [68] ISO 10218-1,2 [68] ISO TS 15066 [69] ISO 8373 (2012) [60]	Safety requirements for industrial robots Safety requirements for robot (robot and controller). Describes the basic hazards manufacturers Specifies safety requirements for collaborative industrial robot Autonomy, physical alteration, multipurpose

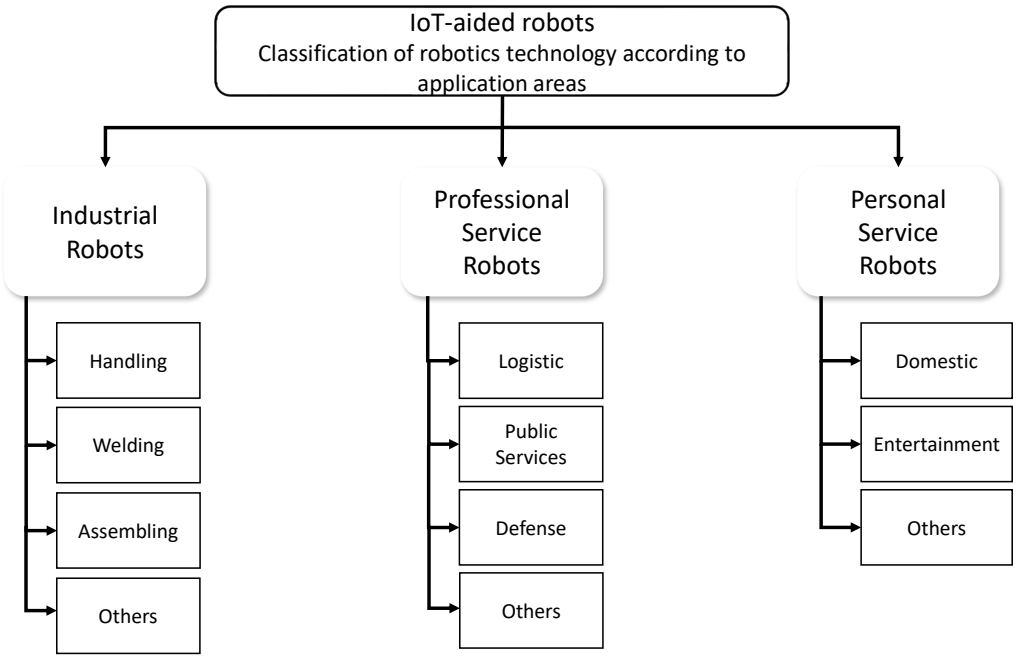

Figure 2. Classification IoT-aided robotic system according to the application areas (top applications are listed first).

2.2. Industrial Robotic Systems

The ongoing 'Industry 4.0' concept [35] incorporates industrial collaborative robots that perform tasks in collaboration with humans in industrial settings. Human factors in an industrial setting also imply the need for the psychophysical and social well-being of operators. Application-driven collaborative robots should facilitate the proper distribution of biomechanical load by assisting the workers in substantial but repetitive tasks.

Following the International Federation of Robotics (IFR) [55] report, between years 2013 and 2019, the installations of industrial robots worldwide increased by 19% per year. Moreover, the stock of operating industrial robots also increased by 13% per year. The majority of industrial robots are employed in the automotive and electrical/electronics industries (approx. 45% of total installations). The first foundation, traditional industrial robots, still plays a significant role in manufacturing automation and continues to operate separately from humans [70]. Lately, the human–robot interaction has been perceived as a fundamental upcoming change in production lines. The ongoing research on human–robot interaction needs the development of: (a) Physical HRI (pHRI) typically associated with robotics technology, (b) novel cognitive HRI (cHRI) using the psychology and cognitive sciences, (c) social HRI (sHRI), which considers the human factor in the complex personal and social relations between humans and robots [71].

In [61], Villani et al. concluded that safety and intuitiveness are two crucial requirements for human–robot collaboration in industrial settings. Concerning Information and Communication Technologies (ICT) in robotics, the ABB controllers should be listed. They offer a Robot Web Service API, an HTTP REST API that allows diverse external program modalities "to speak" to the robot controller [47].

In industrial settings, all systems that interact with robots (including the robot itself) must meet the following requirements: (a) Precision—highly precise sensory measurements are used to optimize robots' movements and to minimize production uncertainties; (b) physical safety—safety of infrastructure and human operators and plant workers must be guaranteed; (c) integrity—the other equipment and robotic controllers must be designed in such a way that logic control faults will not result in equipment damage.

Maurtua et al. [72] explored the semantic approach for multi-modal interaction between humans and industrial robots for enhancing the safety and naturalness of the real-time based human–robot collaboration in an industrial setting [72,73]. A lot of effort has been placed on the implementation of HRC systems in production lines [22]. Human guidance is a crucial feature of contemporary HRC used in production lines, as it allows the robot to be programmed intuitively [74,75].

In modern HRC systems, human operators (guides) offer have better problem-solving skills than the traditional solutions [76]. In recent years safer and more compliant industrial robots have appeared in the market. The communication channels between humans and robots are studied intensely, offering novel, robust solutions [77]. It is interesting that recent development concerns small- to medium-scale payloads leaving heavy-duty robots to become human collaborators in the next stage. Table 2 presents several exemplary robotic systems that work alongside humans in industrial settings without creating hazardous situations.

Table 2. Types of collaborative robotic systems in industrial ecosystems.

Type of Robots	Application Area	Capabilities
Yumi—IRB 14000, ABB [78]	Electronics and small parts assembly lines	Dual arm body, Collision free for each arm
U10, Universal Robots [79]	Packaging, assembly and pick, palletizing	6 DOF single arm robot, collision detection
LBR iiwa 14 R820, KUKA [80]	Measuring, fastening, machine tending	Single arm robot with 7 axis, contact detection
Sawyer, Rethink Robotics [81]	Packaging, kitting, and material handling	Context-based learning, 7 DOF single arm robot

2.3. Service Robotic Systems: Professional and Personal

Over many decades the term service robot had no universal official definition and has been controversial due to different robot structures, abilities, and different applications. For example, the International Service Robot Association (ISRA) addressed the following

working definition of service robots: "machines that observe, sense, think, and extend human capabilities" [82].

Moving forward, the definition of service robot offered by the International Federation of Robotics (IFR) is the following: "a service robot is an agent which acts semi- or fully autonomously to perform service-like tasks beneficial to the well-being of societies and humans, expect industrial operations" [83].

The domain of service robotics has attained significant importance since the end of the last century. However, the effort placed in terminology unification had started already in the 1990s of XXc. by the United Nations Economic Commission for Europe (UNECE) and IFR [83]. Finally, it resulted in a novel ISO-Standard 8373 definition, which became effective in 2012. IFR introduced the classification of service robots according to its intended applications: (a) Professional service robots and (b) personal service robots.

A **professional** service robot is an agent used for commercial activities, usually operated by a properly trained operator in the natural environment, which is fully unstructured. Examples are cleaning robots for public places, delivery robots, rehabilitation robots, and hospital surgery robots. In this context, an operator is a person designated to start, monitor, and stop the intended operation of a robotic system [83].

A **personal** service robot is an agent used for non-commercial activities, usually for the well-being of persons operating in a quasi-structural environment. Examples are: Domestic service robots, automated wheelchairs, and personal mobility assisting robots [83].

In this regard, a significant collection of research works devoted to various branches of service robots, e.g., entertainment, healthcare, nursing, household, natural environment services (field, forest, mountains, etc.), has been published. The existence of "friendly" service robots applying intuitive human–robot interfaces is of great importance. The actions of service robots strongly rely on the information gathered by external sensors. Unlike industrial robots, in service robots, the Human–Robot Interfaces (HRIs) use many modalities. Jones and Schmidlin [84] carried out a thorough review of HRI for personal service robots to facilitate the design requirements. Böhme [85] studied a multi-modal HRI system that allows the service robot to work in a cluttered and crowded environment [73].

Foukarakis et al. [86] explored multi-modal user interfaces for elderly person companions. They proposed the building blocks for creating easy-to-use robotic caregivers. Dutta et al. [87–89] successfully demonstrated an approach for multi-modal human motion intention recognition dedicated for assistive robots. Newman et al. [90] introduced a large multi-modal dataset needed for assisting in eating tasks. Various information was collected for several persons; the data included eye gaze, electromyography signals of the arm, 3D videos. The dataset also contains some other information useful for robot controllers. This dataset allows the researcher to perform multi-modal human behavior analyses. Celiktutan et al. [91] introduced a multi-modal human–human–robot-interaction dataset, intending to study behaviors simultaneously in Human–Human Interactions (HHI) and Human–Robot Interactions (HRI) together with its contextual relation [73].

Today, several commercially available service/assistive systems already incorporate interaction technologies; however, it is still below expectations. Future research will focus on robots for healthcare and clinical applications directly engaged with humans, e.g., when feeding, testing, or health monitoring. Here, enhanced interaction capabilities are needed. An overview of the implementation areas and various examples of the service robotic applications are presented in Table 3.

Table 3. Robotic applications in service areas.

Applications	Implementation Area
Caregiver [92]	Facilitating services to elderly with the help of information, movement of human body, fall detection
Rehabilitation [93]	Support elderly to live independently, reduce possibilities of re-hospitalizations
Clinical Applications [94]	people with chronic diseases to take the appropriate medications
Motor Disorders [95]	Use of vision sensor & wearable sensors which have high ability to detect gait changes
Prevention Assessment [96]	Use of IoT devices in designing fall prevention system for elderly
Human Activity Recognition [97]	Monitoring the daily activities of human, abnormal human activities, prevention of hazards
Elderly Care Monitoring [98]	Monitoring health issues, ambient assisted living

3. Network Interfaces for IoT-Aided Robotic Systems

It should be noted that the security assessment methodology for robotic control systems is still absent. As a result, there are ad hoc solutions that negatively influence the system's robustness against the intrusions and decrease its security.

Out of relatively narrow studies [51,99–102] devoted to the cybersecurity of robotic systems, the most investigated is the safety of networked industrial robots. In the broad considerations given in [99] as some of the prevention mechanisms are listed physical separation of critical functions across different subsystems and appropriately testing the inputs coming from connected components as if they were coming from an untrusted party and taking into account eavesdropping and tampering of the message. Following this line of thinking, we proposed the control system modularization, which allows a more straightforward implementation of such mechanisms.

It should be added that ROS widely used by the robotic community does not force the decomposition of the control system. ROS provides the tools to build a system but does not imply its architecture.

This section proposes a universal architecture for a robotic control system. Transparent structuring taking into account fundamental functions allows for easy monitoring of the operation of each part of the system separately. The data flow is also clearly defined in terms of data type and connecting channels. An additional security mechanism is a dedicated data format (a type of "data protocol") that can be easily checked for fraud and intrusion. Thanks to this concept, the detection of problems is easier because the entire system's malfunction and the failure of each part separately can be detected, for example, as its incorrect or abnormally delayed output. In addition, the reaction to the break-in can be better controlled by the controlled shutdown of the system, starting with its most essential modules (e.g., effector parts) and ending with the less critical (e.g., receptor parts).

The described approach uses the concept of agents [3,103]. The key idea is an architecture of agents (modules) with appropriate connections between them. The system has the ability to monitor its operation. Every agent has an internal control subsystem for the implementation of assigned tasks. It should be borne in mind that the physical environment of the IoT-assisted robotic system is highly heterogeneous. The embodied agents (robots) act in the physical environment while the computational agents (control system modules) act in cyberspace, helping to deal with heterogeneous surroundings [104,105].

Here the IoT is the base of computational agents. It allows easier reconfigurability of the software architecture and supports coordination of the work of multiple devices. Despite that these devices offer different capabilities, they must cooperate closely to achieve a common objective. Unfortunately, the IoT still does not consider the specific needs of IoT-aided robotic systems. Such systems continuously exchange significant data streams while interacting with the physical world. This requirement is fundamental for human–robot collaboration with a shared workspace.

3.1. Design Methodology

The action of a complex robotic system is iterative, and each step can be changed, taking into account the state of the environment. The realization of each task is according to the computational agent's decision, taking into account the environment state [106].

The control system is designed considering: (a) The definition of necessary real receptors and effectors which are essential for the system actions, (b) the decomposition of the system to the agents assigning to them the real effectors and receptors, (c) the determination of individual tasks of the agents, (d) the definition of each system component behavior (often the Finite State Machines (FSMs) are applied for this purpose), and (e) the specification of relevant parameters, i.e., state transition functions, terminal, and error conditions [107]. Each behavior is executed according to the actual tasks.

A design methodology was proposed using the experience gained from developing robotic systems using the real-time operating system QNX and ROS [29,107]. The concept has been proven to be versatile and efficient in various robots and in complex real-time scenarios. The methodology of system design is presented in Section 3.2.

Taking into account the communication reliability and considering the research presented in [108], we applied the concept of data repositories (buffers), which allows the application of data semantics in the communication channels. Thanks to this concept, subsystems can access data in repositories at any time. However, in order to avoid task desynchronization, such an approach requires appropriate coordination of the system activities, which can be ensured by the deterministic FSM system [109].

The general structure considers the postulate of separation of data streaming taken from the list of good practices provided by good practices in software engineering [106].

3.2. General Concept

Scientists and researchers developing robotic applications often design hierarchically organized networked systems. Several European Union research and innovation projects [110] are going in this direction, such as BETAAS and OPENIOT [111,112]. They are focusing on security issues, on context-aware approaches, and on semantic-oriented design (other examples are RELYONIT [113], ICORE [114], EBBITS [115], and VITRO [116]). Our proposition incorporates some elements of hierarchy too.

The robotic networks are the nominal cyber-attack targets [22]. As a result, the robot's sensory readings can be manipulated to misguide the robot control system capabilities; the controller can also be attacked directly or even the data during their transfer to the motors; in all cases, the motor command will be wrong (see Figure 3).

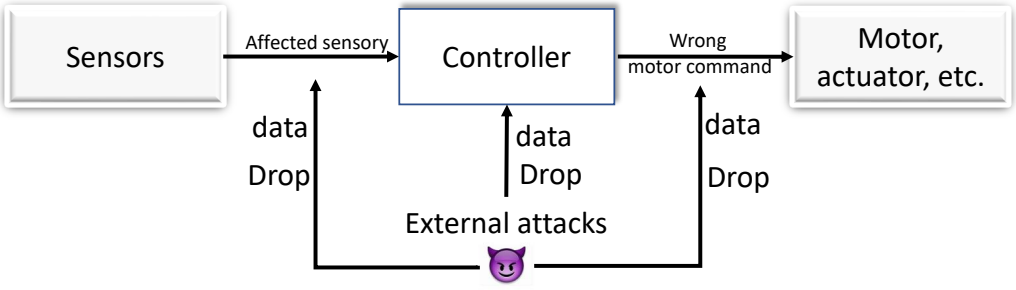

Figure 3. A pictorial representation of typical attacks.

In networked systems, typical communication protocols are used. As their characteristics are widely known, their weaknesses have also been identified, opening the door to cyberattacks. The general methodology of robotic system software decomposition has been deeply studied by Zielinski et al. [117]. This methodology inspired the agent modules of multi-robot systems described in this section. We proposed two mechanisms increasing the system safety: (a) Modular decomposition, (b) introduction of data communication

formats with correctness check before sending from one module and after receiving it in another appropriate module.

Referring to Figure 1 firstly, the behavioral level of communication is considered. The entire control system is divided into subsystems (see Figure 4). This decomposition can be applied to any complex system regardless of the number of actuators and sensors [29,103]. Each subsystem (module) can be easily replaced if necessary. The modular structure allows for its straightforward implementation in the network of processing units.

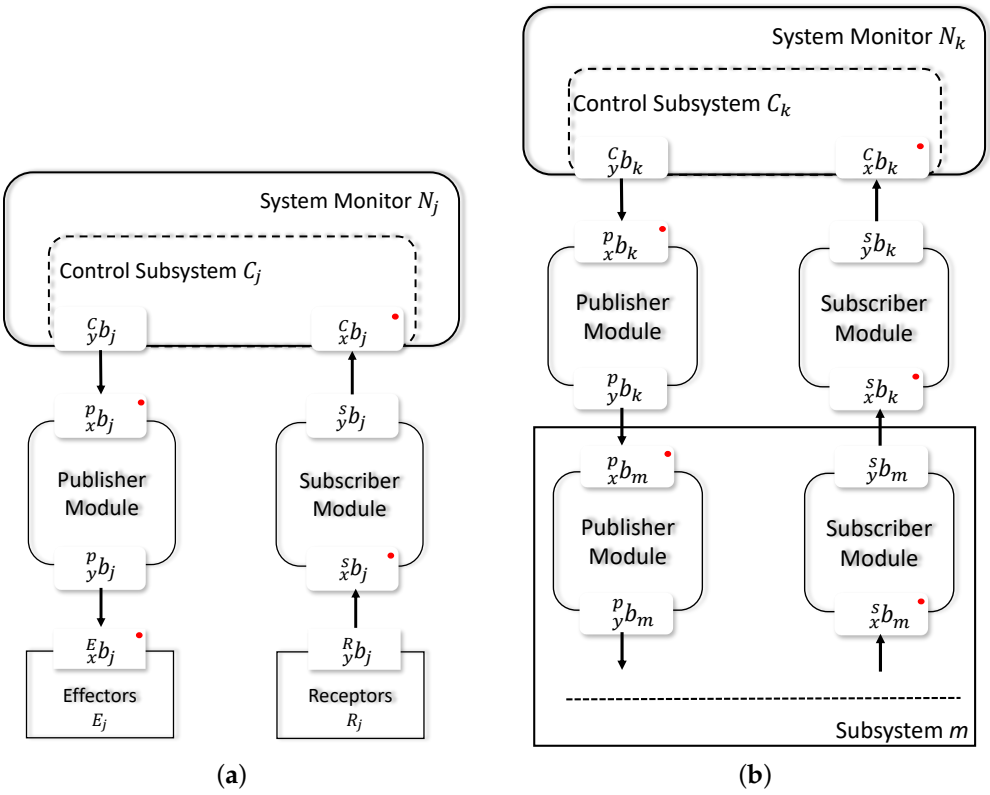

Figure 4. Diagram of control subsystem module communicated with effectors and receptors (**a**); communicated only with other module (**b**). The idea is adopted from [3,107].

Each module is responsible for a logically consistent set of control actions. The subsystem can subscribe to data from some or all of the robot's sensors, the data is pre-processed in the sensor interconnecting sub-module, and the resulting data and information are provided to the control subsystem module for further use (Figure 4a). The subsystem can send motion commands to effectors (e.g., motors), activating the actions of a physical robot. This is done via the effectors' interface. The control subsystem may also be disconnected from the actual effectors and receptors and communicate only with the rest of the subsystems (Figure 4b). Of course, a subsystem can be connected with the effectors and receptors and simultaneously with another subsystem (subsystems). Any combination of these options is also possible. This means that each j-th subsystem can contain the following elements:

- C_j—controller responsible for data processing and decision making;
- N_j—system monitor;
- E_j—effectors receiving commands from the control subsystem via the publisher module in order to influence the surroundings; they can be real effectors (e.g., motors) or virtual effectors, e.g., data or information repositories for the control subsystem;
- s_j—a subscriber responsible for establishing a connection between another subsystem or receptor; the subscriber is the passive side waiting for the data package delivery (it is a receiver according to the QNX philosophy);

- R_j—receptors responsible for collecting information taking into account the task performed; they can be real receptors or virtual receptors, e.g., data repositories holding useful data or information;
- p_j—publisher responsible for establishing a connection between another subsystem or effector; the publisher is an active side in initializing the data packages' sending (it is a sender according to the QNX philosophy).

The system monitor detects anomalies in the control subsystem dynamics. In our notation (x, y) the letter b (denoting buffer) indicates the input or output buffer of the publisher (p), subscriber (s), and controller (C), respectively. These owners are marked with the appropriate letter as the upper right index. The lower right index (j, k, m, etc.) is the identifier of a specific module.

3.3. Communication

The approach to data design format presented in this subsection can be applied to both behavioral and global communication levels (Figure 1). Modular decomposition of control software results in that each module produces the specific data and addresses them to the specific receiver (but not to everyone). The main questions concerning communication are: (a) To what extent typical protocol (e.g., TCP/IP) and Transport Layer Security (TLS) standards can be utilized to deal with complex robotic systems (especially in multi-robot systems) and how effective they are [118]; (b) what are reliable routing mechanisms for network anomaly/intrusion detections [3]; and (c) what is an efficient real-time handling method of the enormous data amount.

We suggest applying a format for transferred data packages that allows checking additionally (besides the protocol's tool) the consistency of communication. To focus attention in Figure 4, red dots indicate the input buffers where such a check proceeds. The data must fit the defined structure.

Each data package consists of a code/command/message saying what to do with data or informing about action status. The next part is the identifiers specifying what subsystem produced this data package and what subsystem is its destination; the next part (optional) is the data itself. They can be numerical or semantical type as is illustrated.

The pseudocode describing the package is given bellow.

```
struct data_package{
  char command; /* a code assisting the data */
  int source; /* source of the message */
  int destination; /* destination of the message */
  struct data; /* data */
}; /* end: message_package */
```

To illustrate the concept in more detail, let us consider the commands and data transferred from the subsystem supervising the progress of walking machine motion (subsystem named *walk_monitor*) to the subsystem responsible for navigation (subsystem named *navigation*). The machine is expected to walk following the straight path trajectory to the destination point given by geographical coordinates. The machine autonomously avoids the obstacles within the given path width and adjusts the gait depending on the terrain. For avoiding often changes of the heading (e.g., occurring due to the terrain unevenness), some range of heading discrepancy towards the target is permissible.

The command codes used in data package:

```
/* command send once at the beginning of work after the navigation
   subsystem communicated the walk_monitor subsystem asking to start
   communication */
#define COMMUNICATION_INITIALIZED 0X01
/* hardware crash, everything must be terminated */
#define HARDWARE_FAULT 0X0E
/* given by navigation subsystem walking distance was passed */
```

```
#define TASK_DONE 0X0A
/* walking machine is on the boundary of a given path (full path width
 locked by obstacles) */
#define ON_BOUNDARY 0X0B
/* machine is walking in order to cover demanded by navigation distance */
#define TASK_IN_PROGRESS 0X0C
```

The example of source and destination codes are:

```
#define NAVIGATION 250 /* set the navigation values to 250 */
#define WALK_MONITOR 101 /* set the walk_monitor values to 101 */
```

The data named for clarity *data_from_walk_monitor_to_navigation* have the following structure:

```
typedef struct{
float distance;  /* walked distance (in meters) */
float side; /* heading drift (angle), positive if the drift to the right,
               negative - if to the left */
char  out_of_path; /* 'Y'-yes, 'N'- no */
char r_obstacle; /* 'Y'- yes, 'N'- no obstacle on the right */
char l_obstacle; /*'Y'- yes, 'N'- no obstacle on the left */
char f_obstacle; /* 'Y'- yes, 'N'- no obstacle on the front */
char blocked; /*'O'- full lock by obstacles (walk is not possible),
                'S'- legs support problem (walk is not possible),
                'I'- terrain inclination is to big for ever available
                     gait (walk is not possible)
                'H'- terrain inclination is to big for ordered gait
                     (walk with this gait is not possible) */
}data_from_walk_monitor_to_navigation;
```

The correctness of the data format is checked in the system buffers. The input buffer of the navigation subsystem receiving data package checks if the command belongs to the list of the above-defined commands. The check is also done for the code of package source and code of the destination. Any inconsistency means that the control system was attacked (under the assumption that the system was previously tested against the software errors). The output buffers are responsible for the appropriate preparation of data packages for further transmission. The multiple checks increase the system's robustness.

Such a concept of data packages was successfully implemented and tested in the control systems of walking machines. The control system was structuralized according to the methodology illustrated in Figure 4. Experience has indicated that data format check goes fast and does not obstruct the real-time performance [29,108]. The main effort is the format design and development of relatively simple software for the format check.

Defense mechanisms applied to data transfers from/to the cloud are crucial in distributed multi-robot systems. Following the proposed decomposition of the control system with the involvement of global communication, Figure 5 illustrates the placement of cloud data in the overall architecture. As is seen, the publisher communicating the data cloud checks the correctness of the data package received from the control system and transfers it to the cloud. In another path, the data obtained by the subscriber from the cloud are checked in the input buffer. The data will be transferred to the controller for the demand. Note: The subscriber takes a passive role and receives the data when they are available, then delivers them farther for the demand. The publisher is active—it receives the data for its demand and decides when to transmit it further. All elements connected to publishers and subscribers are adjusted to this regime. This means that each control subsystem will actively (with its initiative) publish the data (or send the commands) through its publisher while receiving the data passively through its subscriber. The publisher will feed the motors with the following motion data once knowing through the control subsystem from

the receptors (e.g., encoders) that the previous position was reached. In the data cloud communication, the publisher will demand the data from the cloud, and the subscriber will be waiting for it. Besides the clear structure of the system, such a method of data transmission reduces the risks of delays due to the waiting. Assuming that the publisher demanded two sets of data from the cloud, and only one is available at the moment, the subscriber will receive it, and the control subsystem will be able to continue its work assuming that the second set is not so critical at the moment. In the meantime, the following dataset can be prepared.

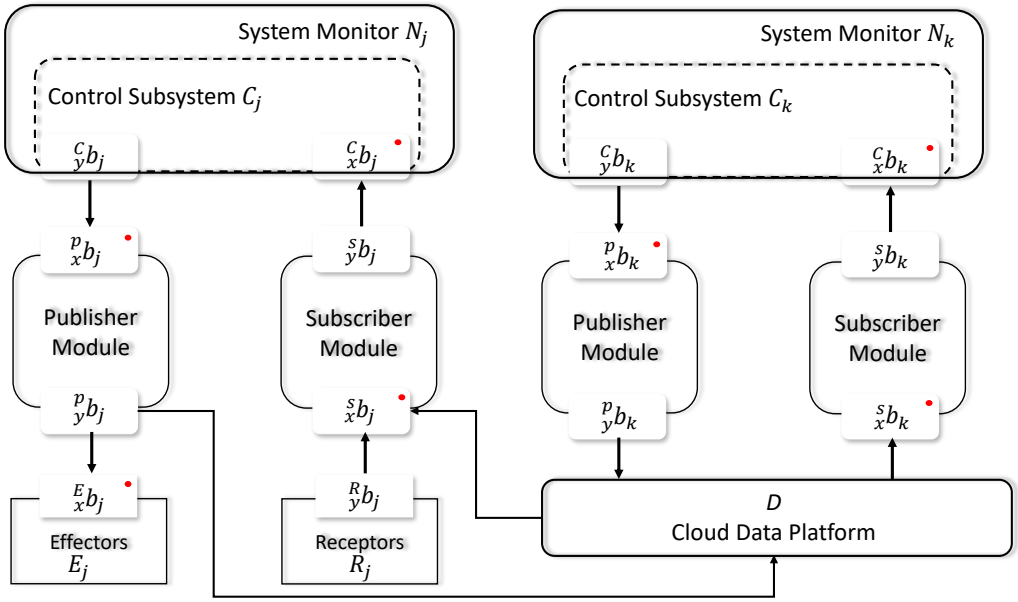

Figure 5. General structure IoT-aided robotic platforms with sample connections.

4. Artificial Intelligence in IoT-Aided Robotic Communication

As is illustrated in Figures 4 and 5, the system Monitor N "surrounds" the control subsystems. The Monitor is responsible for supervising the control subsystem dynamics and its secure activity within the network. Network Intrusion Detection (NID) and Anomaly Detection and Monitoring (ADM) mechanisms should be applied for this purpose. NIDS and ADM are the strategic elements monitoring traffic within the network. For detecting suspicious network activities often the artificial intelligence tools, and machine learning methods are involved. Artificial intelligence also increases the robot's ability.

Artificial intelligence (AI) methods have enhanced robot capabilities supporting sensory data fusion, information processing, environment recognition, and decision-making for many years. New machine learning and deep learning algorithms are improving robotic system capabilities. The continuous advancement of AI algorithms increases: (a) Intelligence of autonomous robots, (b) intelligence of augmented robotic components (increasing robot's or assisted human capabilities), and (c) intelligence of assistive robots at large, as is presented in Figure 6.

The **intelligence of autonomous robotics** aims at the intelligent systems which are offering diverse working capabilities and high redundancy while performing the tasks collectively. The system's scalability, flexibility, and robustness to failures must be assured.

The **intelligence of augmented robotics** focuses on enhancing the sensing, acting skills, and cognitive capabilities of robotics devices. This idea is extended to humans by augmentation of their capabilities, e.g., increase of human force.

Intelligence designed for human **assisting robotics** uses and integrates ideas created by different fields, including: AI, cognitive science, psychology, and sociology. Assistant robots are expected to interact with human beings in a compatible manner. While performing a human support task, they should be predictable.

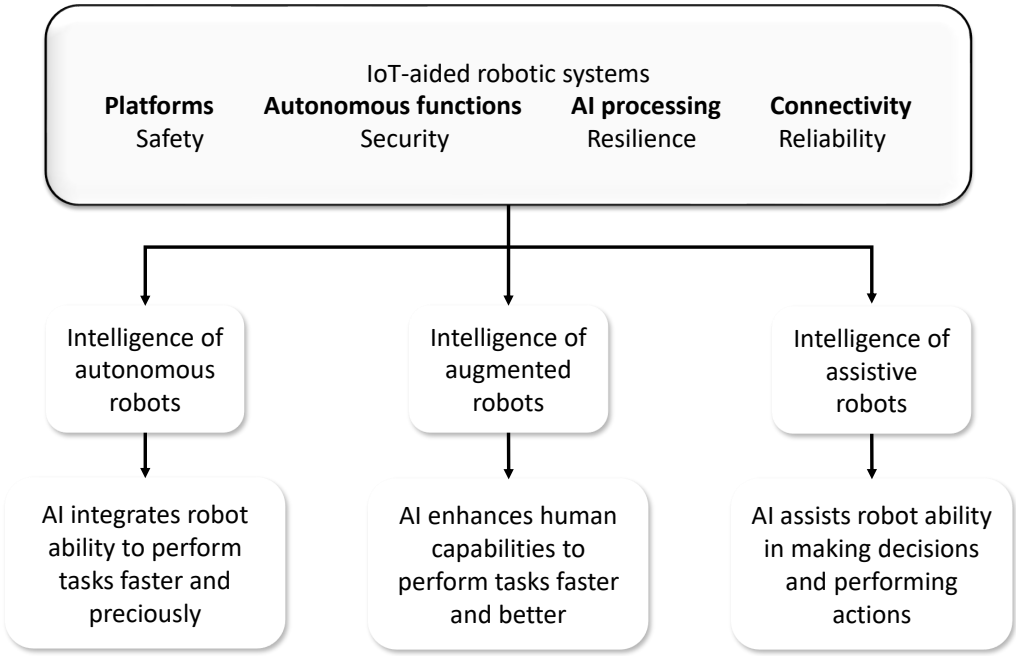

Figure 6. Capabilities implemented at the edge of IoT-aided robotic applications.

Unfortunately, there is a risk that intelligent robots will make wrong decisions. This issue, besides possible intrusions to the control system, also creates a serious security risk. It happens that a system that uses AI sometimes fails or makes a mistake. This causes skepticism towards AI methods and the rejection of such systems by users. It also prevents designers from choosing AI methods [119]. There are inevitable questions about the reliability and objectivity of decisions of the system using AI methods. A demand arises to explain how the AI system comes to a certain conclusion [120].

This need for trust and accountability has led to an increase in research into preventive mechanisms. Explainable Artificial Intelligence (XAI) [121] focuses on understanding and interpreting the behavior of artificial intelligence systems. XAI extracts information to explain how the system draws a conclusion or makes decisions [120,122].

It should be added that artificial intelligence and deep learning methods can also be used to detect and recognize various intrusions by analyzing the software code [51]. A broad study of AI perceived as the target of attacks on one hand and the prevention of attacks on the other can be found in [123].

It is expected that AI methods must not only keep robotic systems safe but also should ensure the necessary accuracy of the work performed and proper adaptation to the task [24]. Secure wireless communication is essential here; it is needed for automated network management with reliable data and knowledge sharing [31].

The conventional IoT-aided robotic system architecture may not be considered sufficient for the application of the contemporary safety mechanisms due to two drawbacks: (a) The frequent changes of these mechanisms and (b) lack of control over the security vulnerabilities [124]. In this regard, machine learning and deep learning methodologies are seen as promising tools for the implementation of defense mechanisms. Besides other things, they are applied for data ownership supervision and ensure data processing and data sharing [125].

The systematic approach for control systems design summarized in this article (see Figure 4) allows the easier introduction of intrusion detection in data management and in access rights supervision.

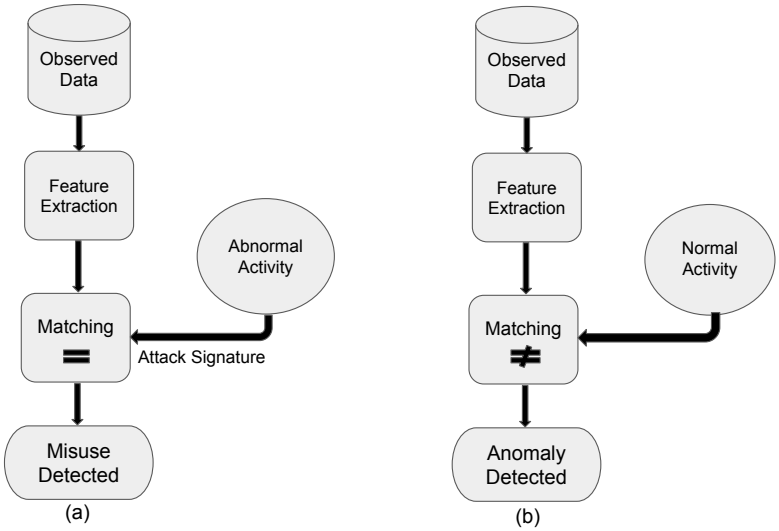

Figure 7. Figure illustrates (**a**) signature-based threat detection, (**b**) behavior-based (or anomaly) detection. The idea is adopted from [124].

Intrusion detection is often based on the known malicious patterns. In this approach, the detection process compares the current event pattern with the stored signatures of an attack (see (a) in Figure 7). If a match is found (that means the bad pattern was identified), an intrusion signal is generated [126,127]. Currently, this constitutes the signature-based industry-standard approach for cyberattacks.

Anomaly detection, another mechanism that acknowledges a malicious or unwanted behavior, uses the set of normal traffic samples for comparison. The advantage of this approach is the ability to detect attacks that did not take place in the past (the so-called zero-day exploits). Therefore, such methods are considered predictive (see (b) in Figure 7). In this approach, the pattern of normal traffic is established, and then it is compared versus the current traffic samples [128,129]. Whenever there is no match, an alarm is raised.

This concludes our overview of the security issues in communication technologies keeping in mind modern robotics that uses IoT capabilities.

5. Discussion

The study presented in this paper focused on intelligent connectivity in IoT-aided robotics [130]. The need to ensure and execute an active and adaptive security mechanism is evident. Internet attacks can maliciously exploit the autonomy of robotic systems. They can take complete or partial control of the robot, which is especially dangerous in autonomous and complex robotics systems cooperating with humans.

The proposed concept of security mechanisms is split into two categories: (a) The data centered, (b) the system centered (e.g., security of control system, cloud data platform) [131].

A defense mechanism associated with the **data-centered** concept addresses the ability to review and delete suspicious data before the system uses them.

The **system-centered** defense mechanism detects adversarial attacks (i.e., wrong threats) in the cloud data and in the control systems as well in order to employ the right security measures.

The holistic approach to the sensory sets and the end devices often fails to work in the open Internet; the real-time QoS measure there is not so high. Several methodologies which allow connecting IoT components in communication networks without human innovation were described. Unfortunately, they still can have limitations in real-time interactions, such as unstable work in the network [132]. Regardless, the Internet or IoT, the advanced communication technologies, and modern AI tools used in robotics have a promising

future [36]. A lot of research effort is still required. The open problem is identifying the fittest network security measures to provide working stability of all robotic network nodes.

- More research is needed to improve Quality of Service (QoS) and Quality of Control (QoC) measures. The communication channels of distributed robotic systems make an attractive object for attacks.
- Another important issue is to elaborate solutions for safe cloud computing considering the communication protocols, the wireless link parameters, and the end-to-end latency, and overall system reliability [24].
- The security of the data transmission should be enhanced in the existing communication models and determine a new set of solutions with a higher level of security.
- Connecting and exchanging information through the networks supports autonomous cognitive decisions [35]. This topic has been recently explored by the cooperation of the IoT and robotics experts.
- The need for real-time safety is highly desired for preventing, after detecting, any anomaly; the robotic system instantly disconnects and/or turns off its elements [31].

As can be seen from the presented material, the problem of cybersecurity in robotics is very broad and covers many issues. In proposing a modular approach to the design of control systems in this article, we focused on communication because incorrect data and information are often used in cyberattacks and manipulate the system's operation. Data and information are the most common and relatively easy targets of attacks. However, we should not forget that there are other possibilities of system corruption, such as the injection of a false system fault or the hijacking of the entire operating system. As the complexity of robots increases, so does the variety and complexity of attacks. Robots are expected to gain full autonomy in the very near future, so the cybersecurity of robotic systems becomes very critical. A widespread application of cybersecurity standards and the robotics software framework is therefore needed. The presented work is an attempt to introduce such a control system framework and data/information package format that allows for better and easier monitoring of the cybersecurity of the system.

In conclusion, it is obvious that the security of intelligent communication in modern robotic systems implemented through various mechanisms is still a bottleneck problem. This issue is still far from being fully resolved.

6. Conclusions

This article provides a comprehensive overview of the challenges involved in intelligent connectivity in IoT-assisted robotics. By discussing security issues, a number of ideas for improvement in terms of network connectivity were given. The methodology of designing robotics control system specification is discussed, taking into account both the system architecture and its activities for network robots.

The main contribution of this work is the formal description of a networked robotic control system using the agent (module) concept, which may be: (a) Helpful in the specification of the safe connection of control and interfaces part; (b) useful for high-level control development using some formal approached (as the finite state machines), preventing logical mistakes, and therefore increasing the system security. We emphasize that detecting and preventing adversary attacks/unauthorized access must be considered when designing a modern robotic system that uses IoT resources. At all times, it must be borne in mind that the infusion to the control systems/cloud data of malicious malware and/or data launches hazards, which may have drastic consequences.

Considering robotic needs [133], the potential directions of future research should include: (a) Requirements analysis and definition taking into account the operation safety of robotic systems which use IoT and/or other commonly accessible resources; (b) introduction of security measures for networked robots taking into account the communication protocols and bearing in mind that in robotic systems timely responses are crucial; (c) study of secure solutions having in mind that, especially in service robotics, system reconfigurability is expected [134] without losing the safety barriers.

Author Contributions: Conceptualization, V.D. and T.Z.; methodology, V.D.; investigation, V.D.; resources, V.D. and T.Z.; writing—original draft preparation, V.D.; writing—review and editing, T.Z.; visualization, V.D.; supervision, T.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding, and the APC was funded by the Institute of Micromechanics and Photonics, Faculty of Mechatronics, Warsaw University of Technology, Poland.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

CPS	Cyber Physical System
IoT	Internet of Things
QoS	Quality of Service
QoC	Quality of Control
NID	Network Intrusion Detection
AD	Anomaly Detection
HRI	Human–Robot Interaction
TCP	Transmission Control Protocol
M2M	Machine-to-Machine
M2C	Machine-to-Cloud
TLS	Transport Layer Security
IPv6	Internet Protocol version 6
FSM	Finite State Machine
HHI	Human–Human Interaction
HRC	Human–Robot Collaboration
ICT	Information and Communication Technology
IFR	International Federation of Robotics
NSA	National Security Agency, USA
NIST	National Institute of Standard and Technology, USA
UNECE	United Nations Economic Commission for Europe
VR/AR	Virtual and Augment Reality
IoE	Internet of Everything
IoRT	Internet of Robotic Thing
GDPR	General Data Protection Regulation

References

1. Khalid, A.; Kirisci, P.; Khan, Z.H.; Ghrairi, Z.; Thoben, K.D.; Pannek, J. Security framework for industrial collaborative robotic cyber–physical systems. *Comput. Ind.* **2018**, *97*, 132–145. [CrossRef]
2. Sunder, S. Foundations for innovation in cyber–physical systems. In Proceedings of the NIST CPS Workshop, Chicago, IL, USA, 13–14 March 2012; Volume 13, pp. 1–12.
3. Dutta, V.; Zielinska, T. Networking technologies for robotic applications. *arXiv* **2015**, arXiv:1505.07593.
4. Dreyer, I.; Stang, G. Foresight in governments–practices and trends around the world. In *Yearbook of European Security*; EU Institute for Security Studies: Paris, France, 2013; Volume 1368, pp. 1–26.
5. Hon, W.K.; Millard, C.; Singh, J. Twenty legal considerations for clouds of things. In *Queen Mary School of Law Legal Studies Research Paper*; SSRN: Rochester, NY, USA, 2016; Volume 216, pp. 1–47.
6. Fosch-Villaronga, E.; Millard, C. Cloud robotics law and regulation: Challenges in the governance of complex and dynamic cyber–physical ecosystems. *Robot. Auton. Syst.* **2019**, *119*, 77–91. [CrossRef]
7. Tapus, A.; Fasola, J.; Mataric, M.J. Socially assistive robots for individuals suffering from dementia. In Proceedings of the ACM/IEEE 3rd Human–Robot Interaction International Conference, Workshop on Robotic Helpers: User Interaction, Interfaces and Companions in Assistive and Therapy Robotics, Amsterdam, The Netherlands, 12–15 March 2008; pp. 1–5.
8. Danaher, J.; McArthur, N. *Robot Sex: Social and Ethical Implications*; MIT Press: Cambridge, MA, USA, 2017; pp. 1–295.
9. Yen, C.T.; Liu, Y.C.; Lin, C.C.; Kao, C.C.; Wang, W.B.; Hsu, Y.R. Advanced manufacturing solution to industry 4.0 trend through sensing network and cloud computing technologies. In Proceedings of the 2014 IEEE International Conference on Automation Science and Engineering (CASE), New Taipei, Taiwan, 18–22 August 2014; pp. 1150–1152.
10. Kohler, D.; Hickman, R.; Conley, K.; Gerkey, B. Cloud robotics. In Proceedings of the Google I/O 2011 Developer Conference, San Francisco, CA, USA, 10–11 May 2011; pp. 21–28.

11. Zacepins, A.; Kviesis, A.; Ahrendt, P.; Richter, U.; Tekin, S.; Durgun, M. Beekeeping in the future—Smart apiary management. In Proceedings of the 17th International Carpathian Control Conference (ICCC), High Tatras, Slovakia, 29 May–1 June 2016; pp. 808–812.
12. Moktadir, M.A.; Ali, S.M.; Kusi-Sarpong, S.; Shaikh, M.A.A. Assessing challenges for implementing Industry 4.0: Implications for process safety and environmental protection. *Process. Saf. Environ. Prot.* **2018**, *117*, 730–741. [CrossRef]
13. Blue Frog Robotics & Robotics. Buddy, the Companion Robot. 2018. pp. 1–7. Available online: www.bluefrogrobotics.com/en/buddy (accessed on 13 September 2021).
14. Quigley, M.; Conley, K.; Gerkey, B.; Faust, J.; Foote, T.; Leibs, J.; Wheeler, R.; Ng, A.Y. ROS: An open-source Robot Operating System. In Proceedings of the ICRA Workshop on Open Source Software, Kobe, Japan, 12–17 May 2009; Volume 3, pp. 5–9.
15. Alzetta, F.; Giorgini, P. Towards a real-time BDI model for ROS 2. In Proceedings of the Workshop "From Objects to Agents", Parma, Italy, 26–28 June 2019; pp. 1–7.
16. Stampfer, D.; Lutz, M.; Schlegel, C. Robot programming. In *Mechatronics and Robotics*; CRC Press: Boca Raton, FL, USA, 2020; pp. 161–194.
17. Maruyama, Y.; Kato, S.; Azumi, T. Exploring the performance of ROS2. In Proceedings of the 13th International Conference on Embedded Software, Chengdu, China, 13–14 August 2016; pp. 1–10.
18. Choi, H.; Xiang, Y.; Kim, H. PiCAS: New design of priority-driven chain-aware scheduling for ROS2. In Proceedings of the IEEE 27th Real-Time and Embedded Technology and Applications Symposium (RTAS), Nashville, TN, USA, 18–21 May 2021; pp. 251–263.
19. Choi, H.; Karimi, M.; Kim, H. Chain-based fixed-priority scheduling of loosely-dependent tasks. In Proceedings of the IEEE 38th International Conference on Computer Design (ICCD), Hartford, CT, USA, 18–21 October 2020; pp. 631–639.
20. Abdullah, J.; Dai, G.; Yi, W. Worst-case cause-effect reaction latency in systems with non-blocking communication. In Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE), Florence, Italy, 25–29 March 2019; pp. 1625–1630.
21. Dieber, B.; Breiling, B.; Taurer, S.; Kacianka, S.; Rass, S.; Schartner, P. Security for the robot operating system. *Robot. Auton. Syst.* **2017**, *98*, 192–203. [CrossRef]
22. Wang, C.; Tok, Y.C. How to secure autonomous mobile robots? An approach with fuzzing, detection and mitigation. *J. Syst. Archit.* **2021**, *112*, 101–129. [CrossRef]
23. Abouaf, J. Trial by fire: Teleoperated robot targets Chernobyl. *IEEE Comput. Graph. Appl.* **1998**, *18*, 10–14. [CrossRef]
24. Vermesan, O.; Bahr, R.; Ottella, M.; Serrano, M.; Karlsen, T.; Wahlstrøm, T.; Sand, H.E.; Ashwathnarayan, M.; Gamba, M.T. Internet of robotic things intelligent connectivity and platforms. *Front. Robot. AI Front.* **2020**, *7*, 104. [CrossRef]
25. Vermesan, O.; Bacquet, J. *Cognitive Hyperconnected Digital Transformation: Internet of Things Intelligence Evolution*; River Publishers: Gistrup, Denmark, 2017; pp. 8–12.
26. Zhao, Z.G.; Ye, R.B.; Zhou, C.; Wang, D.H.; Shi, T. Control-theory based security control of cyber–physical power system under multiple cyber-attacks within unified model framework. *Cogn. Robot.* **2021**, *1*, 41–57. [CrossRef]
27. Shannon, C.E. Communication theory of secrecy systems. *Nokia Bell Labs* **1949**, *28*, 656–715. [CrossRef]
28. Kwon, C.; Liu, W.; Hwang, I. Security analysis for cyber–physical systems against stealthy deception attacks. In Proceedings of the 2013 American Control Conference, Washington, DC, USA, 17–19 June 2013; pp. 3344–3349.
29. Hussain, R.; Zielinska, T.; Hexel, R. Finite state automaton based control system for walking machines. *Int. J. Adv. Robot. Syst.* **2019**, *16*, 814–830. [CrossRef]
30. Dash, P.; Karimibiuki, M.; Pattabiraman, K. *Stealthy Attacks Against Robotic Vehicles Protected by Control-Based Intrusion Detection Techniques*; ACM: New York, NY, USA, 2021; Volume 2, pp. 1–25.
31. Yaacoub, J.P.A.; Noura, H.N.; Salman, O.; Chehab, A. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *Int. J. Inf. Secur.* **2021**, 1–44. [CrossRef]
32. Yaacoub, J.P.A.; Salman, O.; Noura, H.N.; Kaaniche, N.; Chehab, A.; Malli, M. Cyber–physical systems security: Limitations, issues and future trends. *Microprocess. Microsyst.* **2020**, *77*, 103–119. [CrossRef]
33. Villaronga, E.F.; Kieseberg, P.; Li, T. Humans forget, machines remember: Artificial intelligence and the right to be forgotten. *Comput. Law Secur. Rev.* **2018**, *34*, 304–313. [CrossRef]
34. Soldatos, J.; Kyriazakos, S.; Ziafati, P.; Mihovska, A. Securing IoT Applications with Smart Objects: Framework and a Socially Assistive Robots Case Study. *Wirel. Pers. Commun.* **2021**, *117*, 261–280. [CrossRef]
35. Radanliev, P.; De Roure, D.; Page, K.; Nurse, J.R.; Mantilla Montalvo, R.; Santos, O.; Maddox, L.; Burnap, P. Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity* **2020**, *3*, 1–21. [CrossRef]
36. Alsamhi, S.H.; Ma, O.; Ansari, M.S. Survey on artificial intelligence based techniques for emerging robotic communication. *Telecommun. Syst.* **2019**, *72*, 483–503. [CrossRef]
37. Mahapatra, S.N.; Singh, B.K.; Kumar, V. A survey on secure transmission in internet of things: Taxonomy, recent techniques, research requirements, and challenges. *Arab. J. Sci. Eng.* **2020**, *45*, 6211–6240. [CrossRef]
38. Razafimandimby, C.; Loscri, V.; Vegni, A.M. Towards efficient deployment in Internet of Robotic Things. In *Integration, Interconnection, and Interoperability of IoT Systems*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 21–37.
39. Gupta, J.K.; Egorov, M.; Kochenderfer, M. Cooperative multi-agent control using deep reinforcement learning. In Proceedings of the International Conference on Autonomous Agents and Multiagent Systems, Sao Paulo, Brazil, 8–12 May 2017; pp. 66–83.

40. Sunehag, P.; Lever, G.; Gruslys, A.; Czarnecki, W.M.; Zambaldi, V.; Jaderberg, M.; Lanctot, M.; Sonnerat, N.; Leibo, J.Z.; Tuyls, K. Value-decomposition networks for cooperative multi-agent learning. *arXiv* **2017**, arXiv:1706.05296.
41. Guiochet, J.; Machin, M.; Waeselynck, H. Safety-critical advanced robots: A survey. *Robot. Auton. Syst.* **2017**, *94*, 43–52. [CrossRef]
42. Jahan, F.; Sun, W.; Niyaz, Q.; Alam, M. *Security Modeling of Autonomous Systems: A Survey*; ACM: New York, NY, USA, 2019; Volume 52, pp. 1–34.
43. Mayoral-Vilches, V.; Carbajo, U.A.; Gil-Uriarte, E. Industrial robot ransomware: Akerbeltz. In Proceedings of the 2020 Fourth IEEE International Conference on Robotic Computing (IRC), Taichung, Taiwan, 9–11 November 2020; pp. 432–435.
44. Sandry, E. Re-evaluating the form and communication of social robots. *Int. J. Soc. Robot.* **2015**, *7*, 335–346. [CrossRef]
45. Fink, J. Communication for Teams of Networked Robots. Ph.D. Thesis, University of Pennsylvania, Philadelphia, PA, USA, 2011.
46. Bonaci, T.; Herron, J.; Yusuf, T.; Yan, J.; Kohno, T.; Chizeck, H.J. To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robots. *arXiv* **2015**, arXiv:1504.04339.
47. Quarta, D.; Pogliani, M.; Polino, M.; Maggi, F.; Zanchettin, A.M.; Zanero, S. An experimental security analysis of an industrial robot controller. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2017; pp. 268–286.
48. Sabaliauskaite, G.; Ng, G.S.; Ruths, J.; Mathur, A. A comprehensive approach, and a case study, for conducting attack detection experiments in Cyber–Physical Systems. *Robot. Auton. Syst.* **2017**, *98*, 174–191. [CrossRef]
49. Salvini, P.; Ciaravella, G.; Yu, W.; Ferri, G.; Manzi, A.; Mazzolai, B.; Laschi, C.; Oh, S.R.; Dario, P. How safe are service robots in urban environments? Bullying a robot. In Proceedings of the 19th International Symposium in Robot and Human Interactive Communication, Viareggio, Italy, 13–15 September 2010; pp. 1–7.
50. Kirschgens, L.A.; Ugarte, I.Z.; Uriarte, E.G.; Rosas, A.M.; Vilches, V.M. Robot hazards: From safety to security. *arXiv* **2018**, arXiv:1806.06681.
51. Bhardwaj, A.; Avasthi, V.; Goundar, S. Cyber security attacks on robotic platforms. *Netw. Secur.* **2019**, *2019*, 13–19. [CrossRef]
52. Simoens, P.; Dragone, M.; Saffiotti, A. The Internet of Robotic Things: A review of concept, added value and applications. *Int. J. Adv. Robot. Syst.* **2018**, *15*, 172–196. [CrossRef]
53. King, H.; Hannaford, B. *Breaking the Ineroperability Barrier Through Emerging Standards in Teleoperation*; Technical Report; University of Washington: Seattle, WA, USA, 2009; pp. 1–19.
54. Yu, W.; Xu, G.; Pham, K.; Blasch, E.; Chen, G.; Shen, D.; Moulema, P. A faramework for cyber–physical system security situation awareness. In *Principles of Cyber–Physical Systems: An Interdisciplinary Approach*; Cambridge University Press: Cambridge, UK, 2020; pp. 229–238.
55. Robotics, D. *IFR International Federation of Robotics—Service Robots*; International Federation of Robotics: Frankfurt, Germany, 2017; pp. 1–12.
56. Bottalico, B.; Santosuosso, A. *ELS Issues in Robotics and Steps to Consider Them. Part 2: Robotics and Regulations*; ResearchGate: Berlin, Germany, 2016.
57. Voss, W.G. European union data privacy law reform: General data protection regulation, privacy shield, and the right to delisting. *Bus. Lawyer* **2016**, *72*, 221–234.
58. Leenes, R.; Lucivero, F. Laws on robots, laws by robots, laws in robots: Regulating robot behaviour by design. *Law Innov. Technol. Taylor Fr.* **2014**, *6*, 193–220. [CrossRef]
59. Martín, F.; Soriano, E.; Cañas, J.M. Quantitative analysis of security in distributed robotic frameworks. *Robot. Auton. Syst.* **2018**, *100*, 95–107. [CrossRef]
60. Petukhov, V.A. The taxation system in the conditions of production robotization. In *Human and Technological Progress Towards the Socio-Economic Paradigm of the Future*; De Gruyter: Berlin, Germany, 2020; pp. 241–250.
61. Villani, V.; Pini, F. Survey on human–robot collaboration in industrial settings: Safety, intuitive interfaces and applications. *Mechatronics* **2018**, *55*, 248–266. [CrossRef]
62. Main, B.W. Advancing an international standard on machinery safety. *Prof. Saf.* **2009**, *54*, 20–22.
63. Bell, R. Introduction to IEC 61508. In *ACM International Conference Proceeding Series*; Citeseer: State College, PA, USA, 2006; Volume 162, pp. 3–12.
64. Jocelyn, S.; Baudoin, J.; Chinniah, Y.; Charpentier, P. Feasibility study and uncertainties in the validation of an existing safety-related control circuit with the ISO 13849-1: 2006 design standard. *Reliab. Eng. Syst. Saf.* **2014**, *121*, 104–112. [CrossRef]
65. Smith, D.J.; Simpson, K.G. *Safety Critical Systems Handbook: A Straight Forward Guide to Functional Safety, IEC 61508 (2010 Edition) and Related Standards, Including Process IEC 61511 and Machinery IEC 62061 and ISO 13849*; Elsevier: Amsterdam, The Netherlands, 2010; pp. 1–9.
66. Kurkiewicz, J.; Salwa, M.; Majewska, A.; Zylka, L.; Kuciak, A. Radiation shielding swing door drive control system for linear accelerator bunkers. *Lett. Oncol. Sci.* **2020**, *17*, 11–15. [CrossRef]
67. Mariscal Saldaña, M.Á.; González Pérez, J.; Khalid, A.; Gutiérrez Llorente, J.M.; García Herrero, S. Risks management and cobots. Identifying critical variables. In Proceedings of the 29th European Safety and Reliability Conference (ESREL), Helsinki, Finland, 25–29 June 2011; Volume 10218, pp. 1–18.
68. Robla-Gómez, S.; Becerra, V.; Llata, J.R.; Gonzalez-Sarabia, E.; Torre-Ferrero, C.; Perez-Oria, J. Working together: A review on safe human–robot collaboration in industrial environments. *IEEE Access* **2017**, *5*, 26754–26773. [CrossRef]

69. Galin, R.; Meshcheryakov, R. Review on human–robot interaction during collaboration in a shared workspace. In Proceedings of the International Conference on Interactive Collaborative Robotics, Istanbul, Turkey, 20–25 August 2019; pp. 63–74.
70. Kopp, T.; Baumgartner, M.; Kinkel, S. Success factors for introducing industrial human–robot interaction in practice: An empirically driven framework. *Int. J. Adv. Manuf. Technol.* **2021**, *112*, 685–704. [CrossRef]
71. Iglesiasa, I.; Sebastiána, M.; Aresc, J. Overview of the state of robotic machining: Current situation and future potential. *Procedia Eng.* **2015**, *132*, 911–917. [CrossRef]
72. Maurtua, I.; Fernandez, I.; Tellaeche, A.; Kildal, J.; Susperregi, L.; Ibarguren, A.; Sierra, B. Natural multimodal communication for human–robot collaboration. *Int. J. Adv. Robot. Syst.* **2017**, *14*, 189–203. [CrossRef]
73. Berg, J.; Lu, S. Review of interfaces for industrial human–robot interaction. *Curr. Robot. Rep.* **2020**, *1*, 27–34. [CrossRef]
74. Kirchner, E.A.; de Gea Fernandez, J.; Kampmann, P.; Schröer, M.; Metzen, J.H.; Kirchner, F. Intuitive interaction with robots–technical approaches and challenges. In *Formal Modeling and Verification of Cyber–Physical Systems*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 224–248.
75. Liu, H.; Wang, L. Remote human–robot collaboration: A cyber–physical system application for hazard manufacturing environment. *J. Manuf. Syst.* **2020**, *54*, 24–34. [CrossRef]
76. Liu, H.; Wang, L. Gesture recognition for human–robot collaboration: A review. *Int. J. Ind. Ergon.* **2018**, *68*, 355–367. [CrossRef]
77. Liu, H.; Wang, L. An AR-based worker support system for human–robot collaboration. *Procedia Manuf.* **2017**, *11*, 22–30. [CrossRef]
78. Alebooyeh, M.; Urbanic, R.J. Neural network model for identifying workspace, forward and inverse kinematics of the 7-DOF YuMi 14000 ABB collaborative robot. *IFAC-PapersOnLine* **2019**, *52*, 176–181. [CrossRef]
79. Khalid, A.; Kirisci, P.; Ghrairi, Z.; Thoben, K.D.; Pannek, J. A methodology to develop collaborative robotic cyber physical systems for production environments. *Logist. Res.* **2016**, *9*, 23. [CrossRef]
80. Sellami, S.; Respall, V.M. Geometric and stiffness modeling and design of calibration experiments for the 7 dof serial manipulator KUKA iiwa 14 R820. *arXiv* **2020**, arXiv:2006.06314.
81. Bodie, K.; Bellicoso, C.D.; Hutter, M. ANYpulator: Design and control of a safe robotic arm. In Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Daejeon, Korea, 9–14 October 2016; pp. 1119–1125.
82. Pransky, J. Mobile robots: Big benefits for US military. *Ind. Robot. Int. J.* **1997**, *24*, 126–130. [CrossRef]
83. Zielinska, T. Professional and personal service robots. *Int. J. Robot. Appl. Technol.* **2016**, *4*, 63–82. [CrossRef]
84. Jones, K.S.; Schmidlin, E.A. Human–robot interaction: Toward usable personal service robots. *Rev. Hum. Factors Ergon.* **2011**, *7*, 100–148. [CrossRef]
85. Böhme, H.J.; Wilhelm, T.; Key, J.; Schauer, C.; Schröter, C.; Groß, H.M.; Hempel, T. An approach to multi-modal human–machine interaction for intelligent service robots. *Robot. Auton. Syst.* **2003**, *44*, 83–96. [CrossRef]
86. Foukarakis, M.; Antona, M.; Stephanidis, C. Applying a multimodal user interface development framework on a domestic service robot. In Proceedings of the 10th International Conference on Pervasive Technologies Related to Assistive Environments, Island of Rhodes, Greece, 21–23 June 2017; pp. 378–384.
87. Dutta, V.; Zielinska, T. Predicting the intention of human activities for real-time human–robot interaction (hri). In Proceedings of the International Conference on Social Robotics, Kansas City, MO, USA, 1–3 November 2016; pp. 723–734.
88. Dutta, V.; Zielinska, T. Predicting human actions taking into account object affordances. *J. Intell. Robot. Syst.* **2019**, *93*, 745–761. [CrossRef]
89. Dutta, V.; Zielinska, T. Prognosing human activity using actions forecast and structured database. *IEEE Access* **2020**, *8*, 6098–6116. [CrossRef]
90. Newman, B.A.; Aronson, R.M.; Srinivasa, S.S.; Kitani, K.; Admoni, H. Harmonic: A multimodal dataset of assistive human–robot collaboration. *arXiv* **2018**, arXiv:1807.11154.
91. Celiktutan, O.; Skordos, E.; Gunes, H. Multimodal human–human–robot interactions (mhhri) dataset for studying personality and engagement. *IEEE Trans. Affect. Comput.* **2017**, *10*, 484–497. [CrossRef]
92. Chiarini, G.; Ray, P.; Akter, S.; Masella, C.; Ganz, A. mHealth technologies for chronic diseases and elders: A systematic review. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 6–18. [CrossRef]
93. Reeder, B.; Chung, J.; Stevens-Lapsley, J. Current telerehabilitation research with older adults at home: An integrative review. *J. Gerontol. Nurs.* **2016**, *42*, 15–20. [CrossRef] [PubMed]
94. Vickers, N.J. Animal communication: When i'm calling you, will you answer too? *Curr. Biol.* **2017**, *27*, 713–715. [CrossRef] [PubMed]
95. Chen, S.; Lach, J.; Lo, B.; Yang, G.Z. Toward pervasive gait analysis with wearable sensors: A systematic review. *IEEE J. Biomed. Health Inform.* **2016**, *20*, 1521–1537. [CrossRef]
96. Pal, D.; Triyason, T.; Funikul, S. Smart homes and quality of life for the elderly: A systematic review. In Proceedings of the 2017 IEEE International Symposium on Multimedia (ISM), Taichung, Taiwan, 11–13 December 2017; pp. 413–419.
97. Dutta, V.; Zielinska, T. Action prediction based on physically grounded object affordances in human-object interactions. In Proceedings of the 11th International Workshop on Robot Motion and Control (RoMoCo), Wasowo Palace, Poland, 3–5 July 2017; pp. 47–52.
98. de Podestá Gaspar, R.; Bonacin, R.; Gonçalves, V.P. Designing IoT solutions for elderly home care: A systematic study of participatory design, personas and semiotics. In Proceedings of the International Conference on Universal Access in Human-Computer Interaction, Las Vegas, NV, USA, 15–20 July 2018; pp. 226–245.

99. Maggi, F.; Quarta, D.; Pogliani, M.; Polino, M.; Zanchettin, A.M.; Zanero, S. *Rogue Robots: Testing the Limits of an Industrial Robot's Security*; Tech. Rep.; Trend Micro, Politecnico di Milano: Tokyo, Japan, 2017; pp. 1–21.
100. Ferrer, E.C.; Hardjono, T.; Pentland, A.; Dorigo, M. Secure and secret cooperation in robot swarms. *Sci. Robot.* **2021**, *6*, 15–38. [CrossRef]
101. Cerrudo, C.; Apa, L. *Hacking Robots before Skynet*; IOActive Website: Seattle, WA, USA, 2017; pp. 1–17.
102. Fosch-Villaronga, E.; Mahler, T. Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. *Comput. Law Secur. Rev.* **2021**, *41*, 105–528. [CrossRef]
103. Zieliński, C.; Stefańczyk, M.; Kornuta, T.; Figat, M.; Dudek, W.; Szynkiewicz, W.; Kasprzak, W.; Figat, J.; Szlenk, M.; Winiarski, T. Variable structure robot control systems: The RAPP approach. *Robot. Auton. Syst.* **2017**, *94*, 226–244. [CrossRef]
104. Janiak, M.; Zieliński, C. Control system architecture for the investigation of motion control algorithms on an example of the mobile platform Rex. *Bull. Pol. Acad. Sci.* **2015**, *63*, 667–678. [CrossRef]
105. Dudek, W.; Szynkiewicz, W.; Winiarski, T. Cloud computing support for the multi-agent robot navigation system. *J. Autom. Mob. Robot. Intell. Syst.* **2017**, *11*, 67–74. [CrossRef]
106. Kasprzak, W.; Szynkiewicz, W.; Stefańczyk, M.; Dudek, W.; Węgierek, M.; Seredyński, D.; Figat, M.; Zieliński, C. Agent-based approach to the design of a multimodal interface for cyber-security event visualisation control. *Bull. Pol. Acad. Sci.* **2020**, *68*, 1187–1205.
107. Szynkiewicz, W.; Kasprzak, W.; Zieliński, C.; Dudek, W.; Stefańczyk, M.; Wilkowski, A.; Figat, M. Utilisation of embodied agents in the design of smart human–computer interfaces—A Case Study in Cyberspace Event Visualisation Control. *Electronics* **2020**, *9*, 976. [CrossRef]
108. Zielińska, T.; Heng, J. Real-time-based control system for a group of autonomous walking robots. *Adv. Robot.* **2006**, *20*, 543–561. [CrossRef]
109. Estivill-Castro, V.; Hexel, R. Arrangements of Finite-state Machines-Semantics, Simulation, and Model Checking. In Proceedings of the MODELSWARD, Barcelona, Spain, 19–21 February 2013; pp. 182–189.
110. FP7. European Union Research and Innovation Project. 2012. Available online: http://ec.europa.eu/research/fp7/index_en.cfm (accessed on 19 July 2015).
111. Vallati, C.; Mingozzi, E.; Tanganelli, G.; Buonaccorsi, N.; Valdambrini, N.; Zonidis, N.; Martínez, B.; Mamelli, A.; Sommacampagna, D.; Anggorojati, B. Betaas: A platform for development and execution of machine-to-machine applications in the internet of things. *Wirel. Pers. Commun.* **2016**, *87*, 1071–1091. [CrossRef]
112. Kim, J.; Lee, J.W. OpenIoT: An open service framework for the Internet of Things. In Proceedings of the IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, 6–8 March 2014; pp. 89–93.
113. Boano, C.A.; Rmer, K.; Voigt, T. RELYonIT: Dependability for the Internet of Things. *IEEE IoT Newsl. Januray* **2015**, *13*, 20–24.
114. Parodi, A.; Maresca, M.; Provera, M.; Baglietto, P. An IoT Approach for the Connected Vehicle. In Proceedings of the International Internet of Things Summit, Rome, Italy, 27–29 October 2015; pp. 158–161.
115. Furdik, K.; Pramudianto, F.; Ahlsén, M.; Rosengren, P.; Kool, P.; Zhenyu, S.; Brizzi, P.; Paralic, M.; Schneider, A. Food traceability chain supported by the ebbits IoT middleware. In *Dynamics in Logistics*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 343–353.
116. Dillon, E.; Power, G.; Grant, F.C. Experimental testing in the future internet PERIMETER project. In *Future Internet Symposium*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 30–39.
117. Figat, M.; Zieliński, C. Robotic system specification methodology based on hierarchical Petri nets. *IEEE Access* **2020**, *8*, 71617–71627. [CrossRef]
118. Polk, T.; McKay, K.; Chokhani, S. Guidelines for the selection, configuration, and use of transport layer security (TLS) implementations. *NIST Spec. Publ.* **2014**, *800*, 32–35.
119. Linardatos, P.; Papastefanopoulos, V.; Kotsiantis, S. Explainable AI: A review of machine learning interpretability methods. *Entropy* **2021**, *23*, 18. [CrossRef]
120. Wells, L.; Bednarz, T. Explainable AI and reinforcement learning—A systematic review of current approaches and trends. *Front. Artif. Intell.* **2021**, *4*, 4–8. [CrossRef]
121. Dutta, V.; Zielińska, T. An adversarial explainable artificial intelligence (XAI) based approach for action forecasting. *J. Autom. Mob. Robot. Intell. Syst.* **2021**, *14*, 3–10. [CrossRef]
122. Choraś, M.; Pawlicki, M.; Puchalski, D.; Kozik, R. Machine learning–the results are not the only thing that matters! What about security, explainability and fairness? In Proceedings of the International Conference on Computational Science, Krakow, Poland, 16–18 June 2020; pp. 615–628.
123. Fantin, S.; Pupillo, L.; Polito, C.; Ferreire, A. *Artificial Intelligence and Cybersecurity, Technology, Governance and Policy Challenge*; Final Report of a CEPS Task Force; CEPS-Centre for European Policy Studies: Brussels, Belgium, 2021; pp. 1–13.
124. Dutta, V.; Choraś, M.; Kozik, R.; Pawlicki, M. Hybrid model for improving the classification effectiveness of network intrusion detection. In Proceedings of the International Conference on Complex, Intelligent, and Software Intensive Systems, Seville, Spain, 13–15 May 2020; pp. 405–414.
125. Mineraud, J.; Mazhelis, O.; Su, X.; Tarkoma, S. A gap analysis of Internet-of-Things platforms. *Comput. Commun.* **2016**, *89*, 5–16. [CrossRef]
126. Choraś, M.; Kozik, R. Machine learning techniques applied to detect cyber attacks on web applications. *Log. J. IGPL* **2015**, *23*, 45–56. [CrossRef]

127. Dutta, V.; Choras, M.; Pawlicki, M.; Kozik, R. Detection of cyberattacks traces in IoT data. *J. Univers. Comput. Sci.* **2020**, *26*, 1422–1434. [CrossRef]
128. Jain, A.; Verma, B.; Rana, J. Anomaly intrusion detection techniques: A brief review. *Int. J. Sci. Eng. Res.* **2014**, *5*, 1372–1383.
129. Dutta, V.; Choraś, M. A deep learning ensemble for network anomaly and cyber-attack detection. *Sensors* **2020**, *20*, 4583. [CrossRef]
130. Noura, H.N.; Melki, R.; Chehab, A.; Fernandez, J.H. Efficient and robust data availability solution for hybrid PLC/RF systems. *Comput. Netw.* **2021**, *185*, 107–123. [CrossRef]
131. Chigan, C.; Li, L.; Ye, Y. Resource-aware self-adaptive security provisioning in mobile ad hoc networks. In Proceedings of the IEEE Wireless Communications and Networking Conference, New Orleans, LA, USA, 13–17 March 2005; Volume 4, pp. 2118–2124.
132. Finochietto, M.; Eggly, G.M.; Santos, R.; Orozco, J.; Ochoa, S.F.; Meseguer, R. A role-based software architecture to support mobile service computing in IoT scenarios. *Sensors* **2019**, *19*, 4801. [CrossRef]
133. Mazzara, M. Deriving specifications of dependable systems: Toward a method. *arXiv* **2010**, arXiv:1009.3911.
134. Abouzaid, F.; Mazzara, M.; Mullins, J.; Qamar, N. Towards a formal analysis of dynamic reconfiguration in WS-BPEL. In *Intelligent Decision Technologies*; IOS Press: Amsterdam, The Netherlands, 2013; Volume 7, pp. 213–224.