Cybsersecurity Issues in Robotics

Giovanni Lacava[1]*, Angelica Marotta[1] , Fabio Martinelli[1], Andrea Saracino[1],
Antonio La Marra[2], Endika Gil-Uriarte[3], and Víctor Mayoral-Vilches[3]
[1]CNR-IIT, Pisa, Italy
{giovanni.lacava, angelica.marotta, fabio.martinelli, andrea.saracino}@iit.cnr.it
[2]Security Forge Srl, Pisa, Italy
antoniolamarra@security-forge.com
[3]Alias Robotics, Vitoria-Gasteiz, Álava, Spain
{endika, victor}@aliasrobotics.com

Received: March 15, 2021; Accepted: July 8, 2021; Published: September 30, 2021

Abstract

Cybersecurity in Robotics is a rapidly developing area that draws attention from practitioners and researchers. An increase in cyber-attacks, combined with the development of automated processes, introduces new threats that must be addressed to secure information assets and promote trust in robotics systems. Thus, as robotics can be applied to many facets of an organization and adopted in different sectors, it is critical to evaluate cybersecurity risks in robotics platforms and understand how robots will affect tomorrow's cybersecurity strategy. In this paper, we identify existing problems in managing cyber-security in robotics and provide an overview of the critical cyber-security countermeasures in robotics. We also analyze the scientific approaches to managing cyber-attacks in robotics. In particular, we focus on the types of robotic systems that are more prone to cyber-attacks, the main cyber-attacks performed on robots, and their developments. Finally, we offer examples of common attacks and propose directions for further advances in this area. Various approaches and recommendations are discussed in this area to increase and improve the security level of robotic systems. The approach adopted in this work was helpful to understand how to make a robotic system more resilient and reliable from a security perspective.

Keywords: Robotics Security, Cyber-Attacks, Intrusion Detection, Trusted Robot

1 Introduction

In the last decade, the field of robotics has been pervaded by the emerging technologies like Machine Learning and AI (Artificial Intelligence), IIoT (Industrial Internet of Things), human-machine collaboration or autonomous mobile systems [67]. Therefore robots have become "intelligent" and represented a important resource for digitization in the manufacturing industry[1].

As analyzed by IFR (International Federation fo Robotics) the market value for professional service robots increased by 32% to US$ 9.2 billion in 2018 (over 2017), driven by a 60% increase in unit sales of logistics systems. Sales of robot vacuum cleaner are also dominating the rise in the number of personal/-domestic service robots. The majority of these robots are used in non-manufacturing environments, such as warehouses and hospitals, but some are also used in factories or transportation sectors(professional

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 12(3):1-28, Sept. 2021
DOI:*10.22667/JOWUA.2021.09.30.001*

*Corresponding author: IIT - CNR PISA, Research Area CNR, via G. Moruzzi 1, 56124 Pisa, Italia, Tel: +39-3208628060, Web: https://www.iit.cnr.it/giovanni.lacava/

[1]https://ifr.org/img/office/Sales_Flyer_World_Robotics_2019_web.pdf

robotics). The rapid increase in sales of logistics systems is partially due to an expansion in the field of e-commerce; technology advances have, thus, expanded the range of tasks logistics robots, opening avenues to different areas. For example, logistics robots equipped with sensors can be programmed with the help of data from sensors; they can create a map of their environment and elaborate obstacle avoidance strategies through sophisticated algorithms [2].

However, this process of diffusion needs to meet some critical requirements, such as cost of production, ever-changing market demand, and user safety [17]. In this context manufacturers often overlook cyber-security aspects during the design and production phases. Robotic applications, such as autonomous cars, drones, entertainment robots, medical robots, are among the most exposed to cyber-security vulnerabilities [41]. Therefore, it is necessary to have a good understanding of the robotics system to assess security risks and threats. The most critical challenges are those relating to the rapidly changing consumer trends, shortage of resources and skilled workers, aging society, demand for local productions and cyber-security risks looming over the dawn of a yet immature industry.

Although the integration of information technologies (IT) represents an important step towards obtaining more smart and flexible robotic systems, it introduces some critical aspects, especially in the context of cyber-security. As illustrated by the National Institute of Science and Technology (NIST) [93], compromised robots can have a digital and physical impact on the environment in which they operate. Therefore, it is critical to manage security and safety in robotic systems. Usually, to assess the strength of a robotic system in terms of cyber-security, it is possible to adopt the following procedures:

- Threat modeling (Identifying attack vectors);
- Vulnerability assessment (Penetration testing);
- Assignment of level risk of the vulnerabilities;
- Identification of cyber-attacks and the vulnerabilities;
- Prioritization and implementation of related countermeasures.

As for the first step, as suggested by Vilches et al. in [87], we can use a specific set of guidelines to identify vulnerabilities in a system. The author proposed a framework named Robotic Security Framework to assess robotics systems, which is helpful to classify attacks vectors in the following categories: Hardware, Network, Firmware/OS (Operating System) and Application level. Similarly, other cover this topic [17], [44].

Khalil et al. in [41] introduced the Robot Attack Tool (RAT). Using this tool, it is possible to implement risk assessment in a robotic platforms. The author used two mobile robots, respectively Mobile Eyes and arnlServer and through the RAT identified the risks according to CIA -Triad (Confidentiality, Integrity, and Availability).

However, although they explored the impact of cyber-attacks on robotics, they didn't analyze the technologies involved in great details.While new technologies provide the potential for maximizing the capabilities of robots, they also increase the need to pay closer attention to the "safety and security" issues, in particular Kirschgens et al. [44] discussed how the lack of security might cause safety repercussions; they identified three principal areas of conflict: a) Human loss and injuries b) Data theft and privacy issues and c) Reputation issues. These aspects will be discussed in chapters 2 and 4 [80].

Contribution - As mentioned by Kirschgens in [44], "Robots traditionally employed in industry are being replaced by collaborative robots. Moreover, robotics is becoming increasingly intertwined with facets of IT such as the cloud, mobile devices and the Internet of Things (IoT). And, unlike traditional

[2] `https://ifr.org/post/market-for-professional-and-domestic-service-robots-booms-in-2018`

robots, the coming generation of these machines is being envisioned and designed to gain more autonomy." An increase in cyber attacks, combined with the development of automated processes, introduces new cyber risks that must be addressed to secure information assets and promote trust in robotics systems.

As robotics can be applied to many facets of an organization, it is necessary to address cyber security risks in robotics platforms as well as understanding how robots will affect tomorrow's cyber security' strategy. The purpose of this survey is to highlight existing challenges in managing cyber-security in robotics and provide an overview of the critical cyber-security countermeasures in robotics.

In particular we focused on what are the types of robotic systems more exposed to cyber-attacks, what are the main cyber-attacks performed and how they have been developed as regard aforementioned levels (Hardware, Network, Firmware/O.S., Application).

This approach is helpful to understand how the most used attacks evolve and how is important to know robotic system to be able to perform them. Our work emphasizes how to make a robotic system resilient we must keep in mind: Type of robot, type of attack and evolution of the same in the specific system. We present a classification of many attacks in the literature. We also identified the research directions where we believe we should invest to improve the IT security of these systems.

Structure of Survey. This paper is organized as follows Section 2 discussed what is a robotic system e what is changed respect to the last decades. Section 3 shows the current regulatory environment from a safety, security and privacy perspective. Section 4 we analyzes current threats and examples of attacks in robotic systems. Whereas Section 5 defines the current research issues on the topic. Finally, in Section 6, we summarize the main research findings and recommend future research directions.

2 Robotic Systems

With the rapidly increased power of technology, robots have significantly increasing their level of functionality. Robotics is traditionally considered as "the art of system integration" of robots. It's modular nature provides a wide range of usage options. The majority of robots are equipped with the "ability" to sense, process, and act with the world around them. The field of robotics benefit from continued advancements in a variety of disciplines, such as mechanical engineering, computer science, material science, sensor fabrication, manufacturing techniques, etc. [57]. Robots are designed for specific tasks, such as assembling or repairing, which may not be readily adaptable for other applications. Over the last two decades, several authors have attempted to tackle this problem and explain the unusual characteristics of robotic systems.

CPS and Robotic System

Although our research doesn't specifically focus on robotic systems, it is important to clarify the difference between robotic systems and Cyber-Physical Systems (CPS). We propose this distinction to help the researchers to individuate the peculiar aspects of robotic systems: in fact these differences can be useful to analyze the issue in the field of cyber-security:

- *According to Sabaliauskaite et al. [29]"Cyber-Physical System (CPS) is a system that can effectively integrate Cyber and Physical components using the modern sensor, computing, and network technologies".*
- *ISO 8373 define a Robot as electro-mechanical system composed of a multi-axis manipulator, a control system, an "operator interface," and its hardware and software communication interface. Other authors define robots as: "It is a complex system integration composed of heterogeneous hardware and software" [69], a mechatronic device which also includes resourcefulness or autonomy* [3].

[3] `https://www.galileo.org/robotics/intro.html`

The main differences between a CPS and a Robot is that the latter can have a different motion range, number of controllers to perform tasks and end-effector tools ad hoc for each tasks. Conversely, a CPS can't be necessarily designed or structured to move in 2D/3D space. To perform their functions Robots are generally designed (see Fig.n.1) as follow [92]:

- **Sensing** This function helps robots perceive their environment and share information with the other modules or systems or their users.
- **Actuation** This function enables robots to interact physically with the environment.
- **Cognition** This function(computation and coordination) allows robots to anticipate the effects of their actions as well as the activities of the human users around them.
- **Energy** The purpose of this function is to provide power to their system or subsystems.
- **Communication** This function allow robot to connect with other modules or interfaces through (external) communication channels.
- **User Interface (UI)** This function enables robots and their components to be inter-operable and visible during human-robot interactions. Examples include tools, such as joysticks, tactile screens and voice input.

From the analysis of the literature, we identified the robotic systems according to a criteria of inclusion in relation the adoption of digital technologies:

- Articulated arm robots;
- Humanoid and social robots;
- Unmanned Vehicles:
  - Ground Vehicles (UGVs) and other ground robots;
  - Underwater Vehicles (UUVs);
  - Aerial Vehicles (UAVs).

This classification, although relevant for discussion, is very generic and has several limitations, for example, classifying method robots doesn't have to be limited to their mechanical structure, since it is also necessary to identify the general characteristics of robotic systems, their functionalities and their components. Autonomous systems are a type of robot that are not controlled by human ([17], [18]), others scholars examined robots used in tele-operation mode ([65], [80]). In this analysis, we will extend this classification scheme by focusing on the main cyber-aspects of robotics.

In particular, in the context of robotics, cyber security has the purpose of protecting robotic systems from cyber-attacks and minimizing the impact that unavoidable vulnerabilities may have. Often, this task can be challenging, and it is necessary to introduce some specific requirements to be met so that it is possible to develop effective policies and procedures. These requirements are generally grouped within the "CIA Triad"(see Table n.1), which refers to the three pillars cyber security is based on, namely "Confidentiality," "Integrity", and "Availability".

Confidentiality: Confidentiality refers to an individual or an organization's efforts to keep controlled the access to data in order to avoid unauthorized disclosure and ensure that only those who are authorized have access to specific assets. This requirement can be violated in many ways, from direct attacks

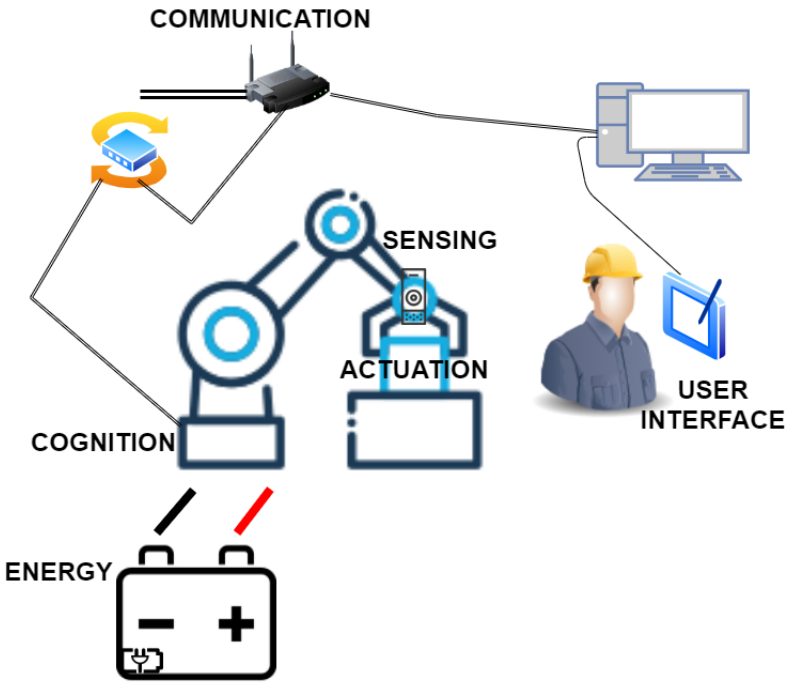


Figure 1: Robot general design

(e.g. man-in-the-middle attacks) to unintentional or accidental violations caused by human errors or inadequate security controls.

Integrity: Another factor that may undermine the security of in a robotic system is the violation of their integrity, which implies the possible modification or deletion of data. It is a risk to which robots are constantly exposed, which can be managed with Intrusion Detection software to prevent and neutralize cyberattacks, or with specific training for those who have different access levels in a company.

Availability: This requirement ensures that authorized users have access to resources in a timely, reliable manner. The inability to access resources that are generally used can be caused by malicious actions, such as DoS (Denial of Service) or DDoS (Distributed Denial of Service) attacks, but also by accidents triggered by events, such as earthquakes, floods, and fires. In addition, software and hardware failures or accidental data removal may also comprise availability. The only way to effectively respond to the risk of unavailability is to have network infrastructures that ensure redundancy between systems. This method ensures that data are continuously accessible without interruption.

Figure 2: CIA-Triad

However while these three principles represent the cornerstone of any organization's security infras-

tructure, a robotic system needs to meet additional requirements [69]:

- *Accuracy:* Robots need to send actuators commands to perform precise operations within acceptable error margins;
- *Safety:* Robots need to make information available to operators. This requirement enable human operator to take safe and informed decisions and perform emergency procedures in safely manner;
- *Integrity:* Robotic controllers need to minimize the impact of potential incidents involving physical parts (e.g. avoiding collisions).

It is necessary to note that the concept of "Integrity" described in this classification has a different focus compared to that illustrated in the CIA Triad. In Robotic systems, any violation of previously mentioned requirements would expose robots to cyber-security threats, potentially compromising the safety and security of the operator and the environment. As observed in [69], these requirements are strongly connected to the concept of safety, i.e. the possibility of robots to injury or harm humans. It is clear that cyber security and safety are strongly interconnected.

Table 1: Security Requirements in Robotics

Security Requirements	Definition	Threats	Solutions
Confidentiality	Confidentiality refers to an individual or an organization's efforts to keep controlled the access to data to avoid unauthorized disclosure and ensure that only those who are authorized have access to specific assets.	• Direct attacks (e.g., man-in-the-middle attacks) • Unintentional or accidental violations caused by human errors • Inadequate security controls	• Improve data usage control • Identity management • Trust • Monitoring and tracking robotic activities, accesses, and the use of privileged accounts
Integrity	Integrity refers to an individual or an organization's efforts to avoid possible modification or deletion of data.	• Lack of security by design • Authentication issues • Manipulation of sensors and cameras	• Intrusion Detection software to prevent and neutralize cyberattacks • Specific training for those who have different access levels in a company
Availability	Availability refers to an individual or an organization's efforts to ensure that authorized users have access to resources in a timely, reliable manner	• Malicious actions, such as DoS (Denial of Service) or DDoS (Distributed Denial of Service) attacks. • Accidents triggered by events, such as earthquakes, floods, and fires. • Software and hardware failures or accidental data removal	Network infrastructures that ensure redundancy between systems.

It is useful to investigate cyber-security in relation to robotics according to a different classification of his components and under a different perspective. In particular, we take as starting point the work of Vilches et al. in [87] that propose the use of a framework based on four levels of analysis to assess the security level of a Robotic system: a) Physical, b) Network, c) FW/Operating System, and d) Application. The work of [87] is mainly focuses on risk assessment methodology. For each of these criteria, the authors identified the following factors: what needs to be assessed (Objective), why it is necessary to perform an assessment (Rationale) and how to systematize an evaluation (Method). As shown in Fig.n.3, the Robot Security Framework provides a methodology that focuses on four layers, which, in turn, cover several security elements[4]. Each *aspect* is analyzed according to three points: 1) *Objective* or description of the evaluation, 2) *Rationale* or relevance of each aspect and 3) *Method* or systematic action plan. In our framework, we use to explain the main potential cybersecurity concerns in robotics.

[4]`https://github.com/aliasrobotics/RSF`

It is worth noticing that not just technical aspects are relevant, also regulatory ones are increasingly attracting the interest of people. In the following section, we will build on this analysis by extending the investigating robotics in the regulatory context.

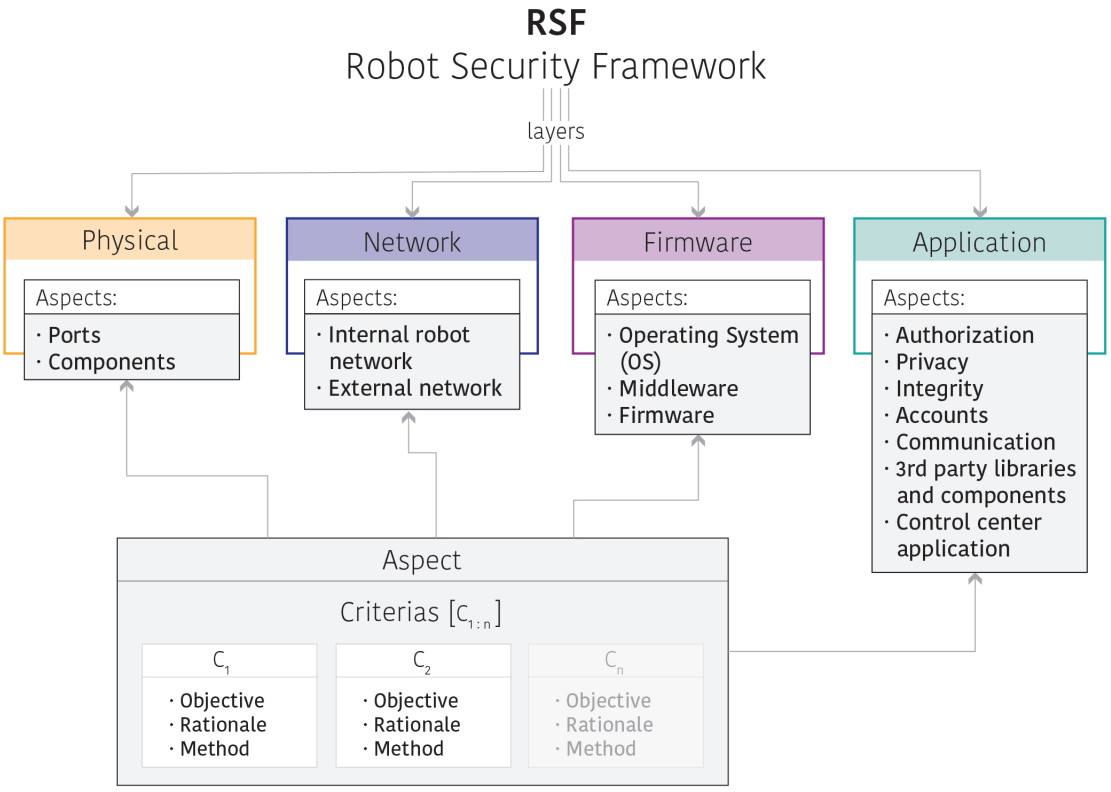


Figure 3: Robot Security Framework introduced by Alias Robotics

3 Regulatory Framework

Robotics continues to open new opportunities and benefits in terms of efficiency and economic convenience. Not only do these advantages encourage improvements in manufacturing and trade, but also in sectors, such as transportation, medical assistance, education, and agriculture [10]. However, despite these advantages, the development of robotics can also lead to severe problems in the legal sphere. For example, some issues may include civil or criminal liability connected to the use of robotic systems. The effort to regulate such a complex subject is, therefore, not exempt, among others, from a part dedicated to the regulation of safety, security, and privacy aspects of robotics.

3.1 Safety and Security in Robotics

Modern robotics systems involve the use of applications, where humans and robots operate collaboratively in industrial or every-day environments. Robot safety is a critical factor in human-machine interactions. This concept refers to the safety of the humans working within a shared human-robot environment. However, safety alone might not be sufficient for developing safe and secure robot applications. One way to guarantee a certain degree of safety is through rules and norms that define the desired and required behaviors.

As robots continue to become more sophisticated and widespread, the need for complete robot safety standards increases exponentially. Robots can be challenging to operate, especially when safety controls are not applied. A robot safety standard is a set of guidelines for specifications and controls concerning robots and their safe operations. Some of the common topics in this area include manufacturing, sales and use of robots [53] and are often created by a diverse group of industry experts to ensure that they provide benefits in different sectors. For example, in some areas, safety has already been addressed, particularly with regards to robotics systems adapted to structured and unstructured environments [53]. The type of environment in which robots operate in may significantly impacts the safety characteristics and capabilities of a robot.

- *Structured environments* - A structured environment is a space that is visibly and accurately defined. Working in this type of environment means that a robot has a defined navigation procedure and a clear perception of potential obstacles or impediments within a space. An example of standards within this category involves industrial robots, which, in Europe, are covered within the scope of the Machinery Directive 2006/42/EC [5];
- *Unstructured environments* - An unstructured environment is a space that is chaotic and undefined. Unstructured environments may be more challenging for a robot to navigate because they must be equipped with advanced capabilities. These may include features aimed at identifying and adapting to unpredictable changes and variables (e.g. people, lighting, humidity, temperature, etc.). Some standards within this category include the General Product Safety Directive 2001/95/EC (GPSD) and the Consumer Protection – Directive 1999/44/EC.

However, with the advancement of new technological systems, lawmakers are making adjustments and updates to these standards. In particular, much of the work of organizations involved in improving robotics safety, such as the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), and the International Electro-technical Commission (IEC) includes harmonizing and creating international robot standards. For example, the following figure shows the connection between standards and the manufacturing system [49], Fig.n.4

3.2 Privacy in Robotics

Privacy within robotics systems involves the personal data of individuals and how that data is stored, collected, used, and shared. According to Rueben (2018) [75], privacy is defined as "the effective setting of boundaries between oneself and other people." The author [53] states that these boundaries define the limits of personal information, personal space, territory, social interaction, relationships, thoughts, feelings, opinions, and decisions. Robots play a crucial role in the establishment of these boundaries as they are capable of collecting and sharing a significant amount of information, moving through personal spaces and distances, and interacting with people. In particular, the social aspect of robots is one of the most controversial issues. Some scholars argue that humans often interact socially with machines, and this phenomenon, also known as "Computers Are Social Actors" (CASA), represents a significant threat to privacy [73], [63], [38]. Also, a recent study [6] has shown that social robots are able to manipulate and trick people into unsafe actions.

This theory suggests that robots are perceived as social actors and, therefore, are included in interactions that typically exist only among people. Calo (2010) [48] and other authors [74] [7], [16] observe that robots are quickly trending towards ubiquity, which involves several privacy implications. Current

[5] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:EN:PDF
[6] https://www.pieterwolfert.com/files/lbr1162-wolfertA_accepted.pdf
[7] https://watermark.silverchair.com/

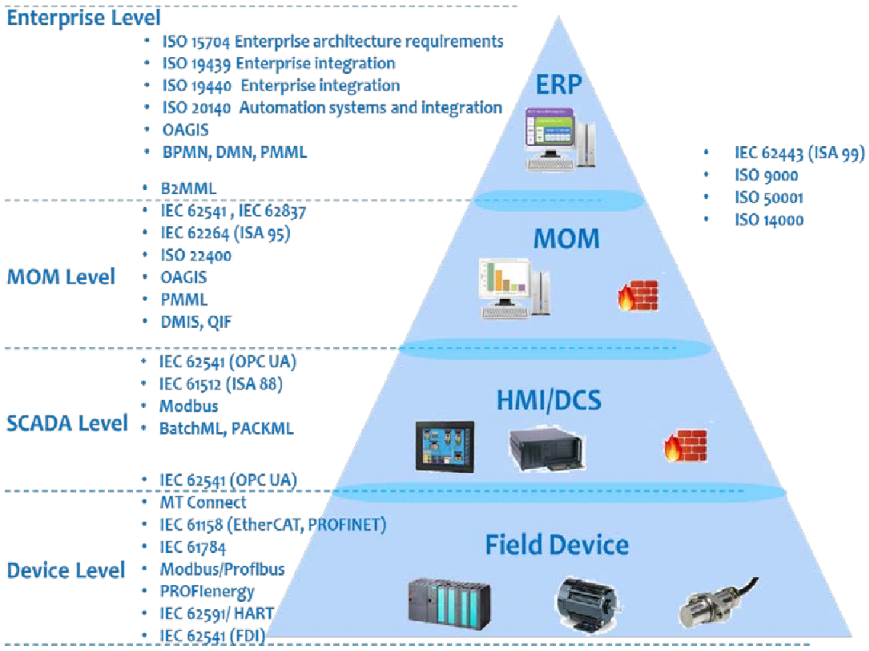


Figure 4: Smart Manufacturing System Pyramid

generations of robots are equipped with microphones, connected sensors, cameras, GPS, rangefinders, accelerometers, etc. (Calo, 2010). The majority of robots collect information about the everyday life of users (Calo, 2010) and their sensitive characteristics, such as emotional, medical, and mental states. For example, the development of robotics applications in the context of healthcare is one of the most discussed in this field. The use of robots to monitoring the clinical and medical parameters of older adults and their transmission to hospitals or doctors in real-time can bring concerns from a data protection perspective. One answer to privacy threats identified in the literature is the concept of "privacy by design" (Calo, 2010; Lutz and Tamò [50], 2015; Sanfeliu, Llácer (Schafer, B., Edwards) [79]).

These authors argue that privacy protection needs to be taken into account from the very beginning of the development process of robotics systems. However, not only is the "privacy by design" concept considered to be effective in the literature, but it is also an essential principle in the regulatory environment surrounding robotics [33]. To this extent, in Europe, the relationship between robotics and privacy has been receiving particular attention over the last few years. For example, on 16 February 2017, the European Parliament passed a resolution with recommendations to the European Commission on civil law rules on robotics (2015/2103(INL)) [8]; following this initiative, the European Parliament (EP) has proposed many principles and requirements for the development of a comprehensive regulatory framework on robotics. Examples of these principles include the concept of reversibility, the inclusion of a protective stop, and the possibility of attributing liability to robots.

For instance, the growing interdependence between robots and cloud services may cause legal and regulatory challenges. Some challenging aspects include applying data protection rules, adapting safety regulations, and attributing responsibility and liability. For example EU's General Data Protection Regulation (GDPR) includes requirements related to automated decision-making processes, fundamental rights concerning data subjects, and data protection by design, which have a significant impact on the distribution of robotics systems.

Other issues arise as to whether robotics systems can be involved in the process of processing the

[8] http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html

data of European citizens, and therefore, take the role of Data Controller. A robot is generally defined as an entity, which is capable of making decisions autonomously (i.e. without the need for human intervention) and interacting with the surrounding environment while processing a considerable amount of data. Following this definition, it is crucial to understand what consequences and regulatory safeguards may come into play in this context. Currently, the GDPR does not link the notion of Data controller to that of a person as a company, or a public authority can generally assume this role. A robot equipped with autonomous decision-making capacity may have the power to determine the purposes and means of data processing. Therefore, it is not excluded that robotics systems could be considered as Data Controllers and be called to fulfill all the obligations placed by the GDPR in relation to this figure. However, an essential factor is that it should always be possible to have control over autonomous systems' decisions (especially if those decisions might cause harm). Given that, for example, most trials of driverless cars have already resulted in several fatal accidents, this issue is still subject to debate in the context of GDPR.

Additionally, GDPR includes specific requirements regarding software medical devices, which are key to addressing challenges such as regulating the liability of all players involved in the robotics production chain (e.g., producers, doctors, users, healthcare centers) [24]. Other works [21] on Collaborative Robotics discuss how and where the data acquired by robots' sensors are stored and used. For example, a collaborative robotic system called YuMi supported hospitals during Coronavirus testing using an application designed at Politecnico di Milano, in partnership with ABB and the European Institute of Oncology in Milan, Italy. YuMi was able to automate up to 77 percent of the testing actions and analyze 450 samples/hour . While these systems present a great opportunity to optimize data collection, they could raise concerns on data accuracy and transparency from a regulatory point of view. However, despite these efforts, the processing of personal data within robotics is still a regulatory goal because, to move forward with privacy regulations, it is necessary for regulators to unify regulatory approaches and address privacy concerns in robotics.

4 Cyber attacks on robotics systems

In this section, we survey attacks on robotics systems (see Tab. 3), by considering the CIA triad (as suggested in [87]) as well as highlighting specific issues and attacks vectors. We then list of the different kind of attacks and their level in the robotics systems (see Tab. 2). Eventually, we present a table linking several aspects together (see Tab. 4).

Confidentiality

During the fabrication phase, as explained in [6], a malicious user can implement a backdoor in general-purpose processors, bypass memory range protection using buffer overflow attacks, or gain access to privileged assets by bypassing control protection mechanisms.

Integrity

Sometimes, Hardware (HW) Trojan, a malicious addition and/or modification to ICs (Integrated Circuits), may cause damages to robots [6]. Malicious users may discover the encryption key of the system and compromise the system (i.e. Malicious off-chip leakage enabled by side channels). Example of attacks may be performed through HW Trojans, attackers could implement the stealth attack by modifying the output values of sensors.

In this context there are two ways to access robotic systems: a) through the network or b) through physical components. An attacker needs network or physical access to a robot controller or robotic set up to implement the attack (e.g access through industrial routers and compromise) robot functionalities, such as sensors reading, executing control logic, making precise movements and ensuring human safety.Specific types of attacks to industrial robots, as described in [69], are listed below:

- Alteration of control-loop parameters;

- Tamper through modification of calibration parameters;
- Tamper through modification of the Production logic;
- Alteration of the user-perceived Robot state;
- Alteration of Robot state.

These attacks can alter the interaction between the robot and the surrounding physical environment. For example in the case of production tampering, an attacker can use a file system or an authentication-bypass vulnerability to compromise the manufacturing process, modify a work-piece or cause the robot to perform wrong task.

Availability

In [30], Gil et al. implemented a Sibyl attack involving swarm-drones. In particular, this attack compromised the drones capabilities and cooperation abilities. This type of attack used a fake member to send a high number of requests to the server node, resulting in drone, degradation or unavailability of the servers. Another critical application field is Medical Robotics. Examples include heterogeneous robotic platforms used in surgery procedures (e.g. Da Vinci - Intuitive Surgical Ltd, Mako - Stryker Corporation, NAVIO - Smith+Nephew). In [9], the authors explained the effects of a DoS (Denial of Service) attack on the RAVEN II robotic system, which uses a master-slave communication between the surgical console and the manipulator. Raven II is based on Linux O.S. and ROS middle-ware, and uses the ITP protocol(Inter-operable Telesurgery Protocol) to control input and robot feedback. In particular, this platform can be used in tele-operation and human operator-robot communication. For example, during hijacking attacks, an attacker may induce the robot to completely ignore the intentions of a surgeon; packets may end up being forwarded towards the wrong part of the network, enter an endless loop, and potentially perform harmful actions.

Other aspects

Robotic system problems are not limited to data management of the system but each part of it can be a source of attack. For example, in [69], the authors described the most common ways in which a robotic system can be compromised:

- Information disclosure: technical materials available on manufacturers website, including software images;
- Outdated software: custom patches applied by manufacturers to update the software, create opportunities for attackers leverage software vulnerabilities;
- Default authentication: remote connections enable attackers to compromise devices through null or ”admin” default password;
- Poor transport encryption: for example, symmetric keys for VPNs or web-based administration are not available on HTTPS;
- Poor software protection: attackers can manipulate software images (e.g. debug information) that are available on manufacturers website.
- Security by obscurity: Poor information about robots may lead to unclear security.

In another study [65], the authors identified two principal attack vector for robotic system: USB physical [55] port (posed on or teach-pendant or robot controller), remote access through the network.

Instead Dieber et al. [21] provide an example of a drone under attack. Simply shutting the drone's system down would not be a good strategy as its basic functionality must be available until it reaches a safe state (e.g., it has landed). According to Clark et al. [17], most of the cyber security issues related to robots derive from the fact the design and manufacture of robots are generally not designed to include cyber security. In fact, development costs and delivering functionality to consumers are the real priorities when building robotics systems.

4.1 Attacks to Robotic Platforms

Table 2: Cyber-Attacks in Robotic Field

Attack	Reference
DoS	[17], [41], [69], [4], [80]
	[60], [21], [59], [67]
	[23], [9], [40], [21]
	[22], [90], [66], [29]
	[70], [85], [82], [12]
	[8], [32], [36], [3]
	[26], [62], [88], [52]
	[11], [72], [35], [51]
Spoofing Attack	[59], [23], [22], [70]
	[85], [39], [42], [13]
	[14], [86], [26], [35]
MitM	[41], [69], [93], [67]
	[85], [82], [39], [8]
	[62], [61], [84]
Eavesdropping Attack	[17], [59], [67], [23]
	[40], [85], [8], [3]
	[26], [61], [35]
Replay Attack	[85], [26], [88], [52], [35]
Tampering Attack	[69], [68], [85], [52]
Fault Injection	[17], [29], [85]
Sybil Attack	[90], [30], [70]
Jamming Attack	[80], [23], [40]
HW Backdoor	[17], [85], [6]
RAT Attack	[64], [85]
Stealthy Attack	[29], [76]
Homing Attack	[90]
Teardrop Attack	[23]
Phishing	[3]
Hijacking Attack	[8]
Masquerade Attack	[26]

When it comes to cyber-security in the field of robotics, there is no single issue that needs to be analyzed to ensure full protection. Given the increasing inter-connectedness of robotic devices, attackers have found ways to perform multiple attacks and overcome traditional barriers. One of the best cyber-security practices lies in creating a comprehensive architecture to mitigate attacks. The table 2 shows the main attacks to which robots are exposed. Some of the most common examples of attacks on robotics systems have been identified and described as follows (summarized in Fig.n.9).

DoS: From January to June 2020, Kaspersky experts reported a 350% increase in Distributed Denial of Service (DDoS) attacks compared to the same period in 2019 [9].

DoS attacks are a type of attack that aims to drain a network until the server crashes. During a Denial of Service (DoS) attack, cyber-criminals attempt to overload the network server with requests until it crashes, causing significant inconvenience to users, including the inability to access services. While DoS attacks involve only one attacking computer, DDoS (Distributed Denial of Service) attacks exploit a "botnet," a series of infected computers capable of carrying out tasks simultaneously DDoS attacks are particularly problematic because they can last from a couple of days to a few weeks, causing disruption of activity and denying people access to important content. In [69], the authors provide a scenario involving DoS attacks applied to robots. They describe a situation where an attacker repeatedly triggers manipulations on the robot's controller at "runtime," leading to a DoS attack. In such a circumstance, the robot persists in the stop status. The following scheme (Figure 5) represents a type of DoS attack described in [21];

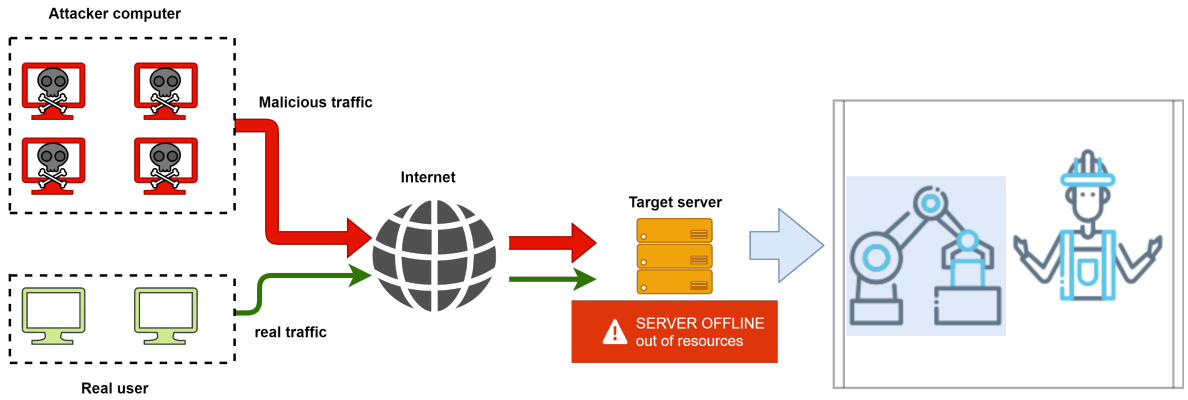


Figure 5: DoS Attack

Spoofing: Spoofing refers to a situation in which an attacker impersonates another device or user on a network. The purpose of using this technique is to steal data, spread malware, or bypass access controls. The most common forms include spoofing an IP address, an email address, or a Domain Name System (DNS) server. In the context of robotics, a spoofing attack may force a robot to behave incorrectly. For example, [86] describes spoofing threats such as GPS spoofing that may cause users to lose control over drones. The technique used by an attacker to perform a GPS spoofing on drones is to transmit fake GPS coordinates to the control system of the drone and change its trajectory. Figure 6 shows how this attack is performed;

MitM: Man-in-the-middle (MitM) is a cyber attack that enables cyber attackers to intercept and manipulate internet traffic. This type of attack often targets robots. As previously mentioned, several studies found that most robots have authentication and authorization problems, use unsecured communications and weak encryption, expose private information, have weak default configurations, and were built using open source frameworks and libraries. Some robots can be controlled by mobile applications or can be programmed with software installed on computers. Other robots communicate through cloud-based services to receive updates and software applications. If the communication channels between these different components are insecure and encrypted, attackers can launch man-in-the-middle attacks and insert malicious software commands or updates that will be executed by robots. Additionally, according to [69], safety features are subject to man-in-the-middle or interface-manipulation attacks. For example, an attacker can cause a denial of service (DoS) by forcefully stopping the robot during normal operation.

[9] `https://tinyurl.com/xauekyx3`

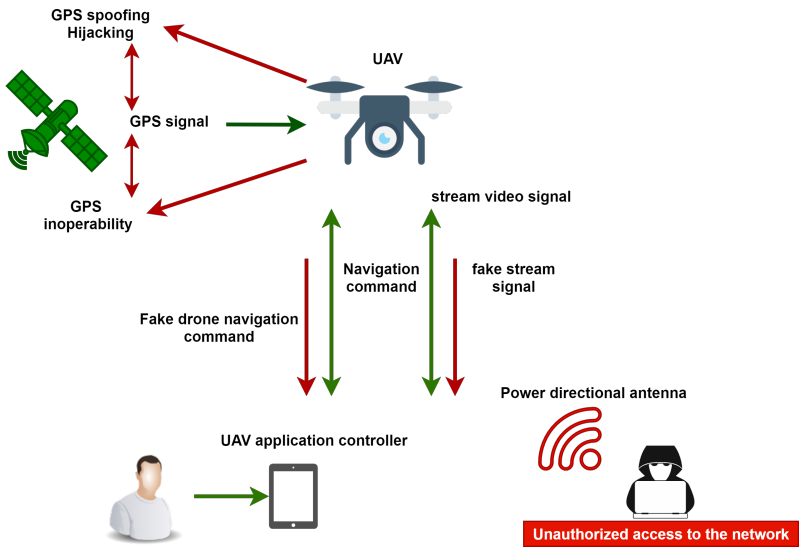


Figure 6: Spoofing Attack

In this context, an attacker can disable safety features, thus preventing legitimate users from activating necessary procedures in case of an emergency. This attack may have significant implications for the safety of the operator. An example is provided by [67] (Figure 7), which described an attack targeting Spykee, a toy spy telepresence robot;

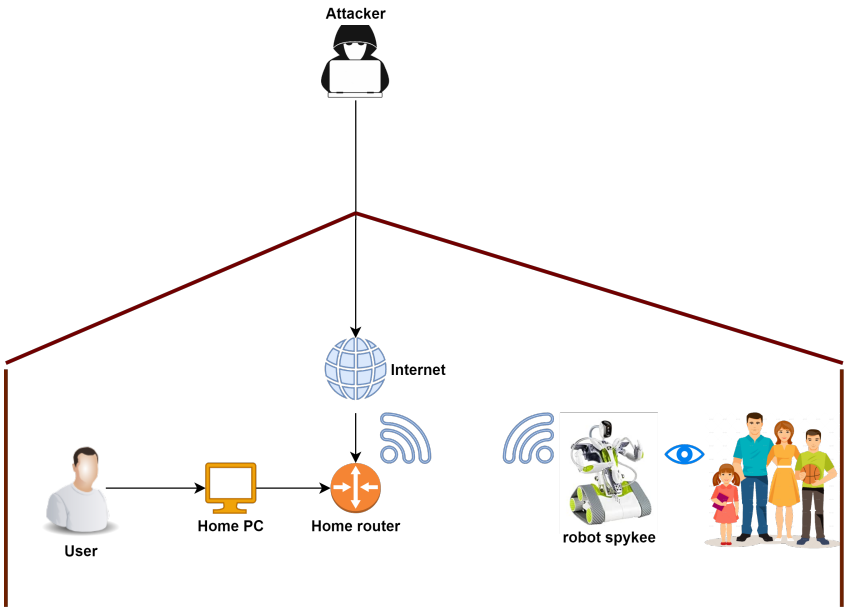


Figure 7: Man in the Middle Attack

An example of a Man-in-the-Middle attack is **Eavesdropping**: The attacker creates independent connections with the victims and re-transmits messages to make them believe they are communicating directly over a private connection. In reality, the entire conversation is controlled by the attacker, who can intercept all the important messages exchanged between the two victims and inject new ones. In many circumstances, this is a simple attack to perform. For example, an attacker can assume the role of

a network observer to eavesdrop on packets between a surgeon and a robot. Thus, an attacker can inject new, malicious packets into the network to impact the surgical procedure [8]. In [5] the authors propose decentralized multi-authority anonymous authentication scheme to avoid the authentication problems, when an entity wants to prove the possession of the attribute credentials to a verifier, it generates a proof of the credentials in a zero-knowledge or witness-indistinguishable way;

Tampering: A Tampering attack generally involves manipulating parameters exchanged between client and server to modify and compromise application data. Examples of data targeted by this type of attack include user credentials and permissions, etc. In [69], [68], the authors offer an overview of different types of tampering attacks, such as Tampering with Calibration Parameters where the attacker attempts to change the calibration to make the robot move unexpectedly or inaccurately. In this case, there may be robot damages, and safety, integrity, and accuracy issues. Another attack described in this work is Tampering with the Production Logic. In this case, the attacker manipulates the program executed by the robot to maliciously introduce a flaw into the work piece. The following example(Figure 8) shows a type of tampering attack described in [69];

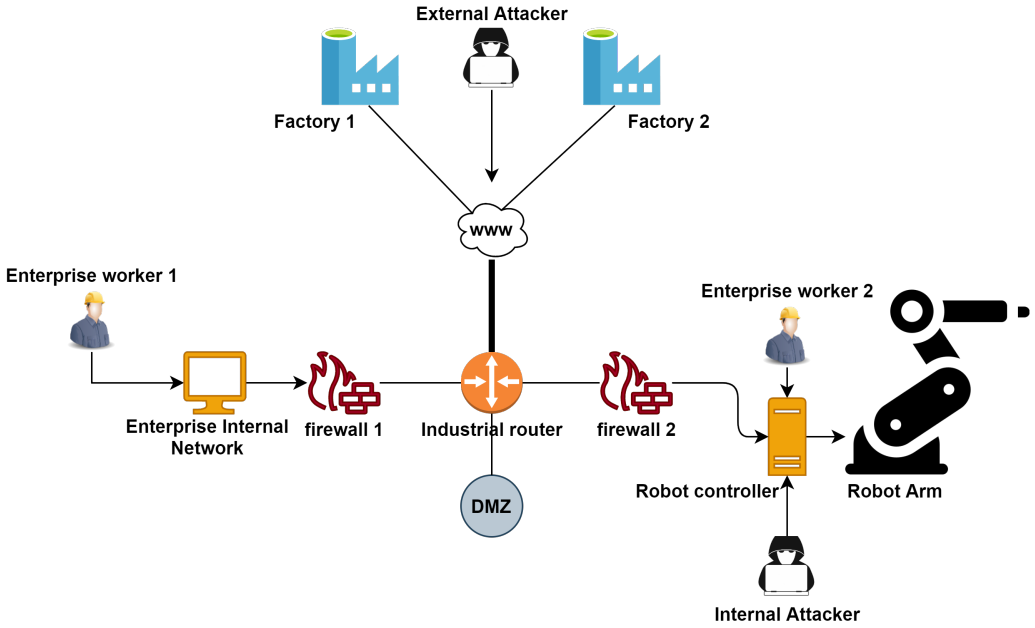


Figure 8: Tampering Attack

Replay attack: ([85], [26])Replay attack is performed how a network attack in which a valid data transmission is maliciously repeated or delayed. In particular the malicious operator intercepts the data among users and re-transmit it (sniffs hash and replays hash), this type of attack is a version of the Man in the middle(MiM), while MiM is in real-time the Replay attack can be execute in asynchronous way when the communication among users it's ended ([88], [52], [35]);

Fault Injection attack: Fault Injection is a physical attack on the data and behavior of an Integrated Circuit([17]). Therefore, Fault Injection is a physical attack with the goal to bypass secure boot mechanisms, acquire a secret key, disrupt a program counter,etc. It can be implemented also via software and be developed using data injection in the embedded code ([29], [85]);

Sybil Attack: The Sybil attack is performed to Network Layer (ISO/OSI), in particular this attack use multiple false identities ([30], [70]) to deny the information passing procedure. It can damage the distance-based/location-based routing protocol([90]);

Jamming Attack: The Jamming attack is a type of DoS attack on wireless network. This attack pre-

vents other nodes to communicate by occupying the channel, usually transmitting on the same frequency and modulation of the signal prevented ([80], [23], [40]). To avoid this problem, different solutions are being studied, including the development of detection algorithms, for example in [37] the authors developed a machine learning based technique to detect and classify different type of jamming attacks on RF channel, focusing on the importance of classifying the type of attack to be able to implement the necessary countermeasures;

HW Backdoor attack: Usually, an backdoor is a method to bypass the authentication procedure or encryption in a PC/System ([17], [85]). It can be create directly through the manufacturing process of ICs (integrated circuits), it is activate from a event (trigger) hardware (tun on of component) or software (execute code after the hardware trigger, i.e. [6]);

RAT Attack: The Remote Access Trojan is a malware that permit at the malicious user to obtain the administrative control over the target device. This type of attack use a backdoor to introduce in the target system or downloaded with a user-requested program or sent as an email attachment ([64], [85]). So, from the target device compromised the malicious user can send RATs toward the other vulnerable devices to create a botnet;

Stealthy Attack: The Stealth attack is type of attack in which the cost and visibility of the attacker have to be minimized. To perform it, it's necessary a good knowledge of the target system or device, based on type of target the stealth attack is composed of different stages of actuation (communication, execution and propagation).In particular in [29], [76] is described the technique to compromise values of sensors with a code-injection approach;

Homing Attack: It's an attack in which the attacker analyze the network traffic to identify particular cluster heads or base station, once done, the attacker can performs the attack toward the critical nodes to compromise or destroy the entire network ([90]);

Teardrop Attack: This is a DoS attack, in particular operate on the sending mangled IP fragments with overlapping, oversize payloads to the target device. Therefore a server vulnerable is unable to reassemble the packets, in [23] is used to compromise the communication between User and tele-operated device;

Phishing: It is an attempt used to acquire user sensitive informations like password, credit card details, etc. In [3] is used how entry point onto a hospital network to compromised personal information of patients, in this case anatomy of the patients treat with a surgical device;

Hijacking Attack: Hijacking is a type of network security attack in which the attacker takes control of a communication. In particular the attacker first assumes the role of observer to eavesdrop on packets between client and server, after can compromise the session by stealing or predicting a valid session to gain unauthorized access([8]);

Masquerade Attack: In this attack a malicious user uses a fake identity, to gain unauthorized access to information resources of the target device through legitimate access identification. In [26] it's used to acquire informations from autonomous vehicle. In a Wi-Fi network can compromise all aspects of security.

4.2 Attack levels

The previous analysis provides an overview of the attack to Robotic systems described in literature. We extended this analysis by, investigating these attacks in the Hardware, Network, Firmware/OS, Application domains (summarized in Fig.n.9).

Table n.3 summarizes the types of threats affecting robots and the related areas of vulnerability.

The majority of the authors [15, 41, 44, 69], addressing this issue argue that the lack of security by design may generate the following categories of threat:

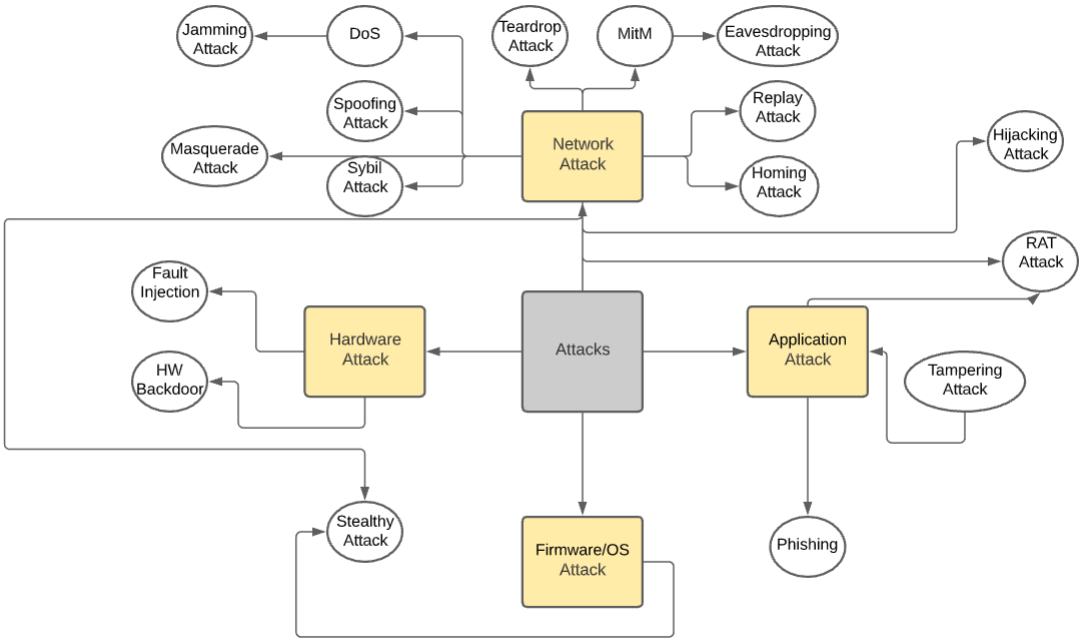


Figure 9: Attacks Overview

- **Insecure communications:** issues between users and robotics systems may encourage a verity of cyber security risks. Kumar et al. [45] specifically addressed this issue in surgical robotics. They argued that there are several ways in which intruders may hack into insecure communication links, especially if robots are connected to public networks. Additionally, some authors claim that plain or poorly encrypted text may enable attackers to obtain a significant amount of data from robotics systems. In particular [15, 40, 41, 44, 67, 69, 87], they argue that the majority of threats related to communications may be caused by the use of libraries or applications connected to the Internet. Another robotics area, which is vulnerable to communication issues is firmware [87], [17], [15], [41], [69], [54], [4], [80], [60], [21], [59], [93], [67], [23], [9], [40], [21], [68], [22], [90], [66]. For example, upgrading firmware online provides ample opportunities for attacks. Finally, since most robots are connected to the Internet via networks, attackers could gain full control of robots by exploiting communication vulnerabilities [87], [15], [65], [69], [44], [80], [60], [59], [93], [67], [21], [68], [22], [90], [66];

- **Authentication issues:** One of the most underestimated threats in robotics is that involving authentication. Some robot applications are designed without the need for username and passwords, allowing anyone to access them remotely. However, even when these services use authentication features, attackers may bypass them [17], [15], [41], [69], [44], [67], [40]. Similarly, most of the networks to which robots are connected networks are not password protected and, therefore, vulnerable. Conversely, when they are protected, authentication mechanisms may not be up-to-date, and unauthenticated users may exploit this vulnerability and access the network [87], [15], [65], [69], [44], [80], [60], [59], [93], [67], [21], [68], [22], [90], [66], [76]. The lack of authentication also means having no verification of whether the physical components of the robot are accessed or not. For this reason, attackers could easily interact with or tamper any components [17], [15], [65], [69], [44], [80], [83], [59], [67], [68], [22];

Table 3: Cyber-Security Threats in Robotic System

Cyber security Threats in Robotics	**Levels of the Attack**			
	Hardware Attack	*Network Attack*	*Firmware/OS Attack*	*Application Attack*
Insecure communications	[70], [71], [43], [6]	[87], [15], [65], [69], [44], [80], [60], [59], [93], [67], [21], [68], [22], [90], [66], [70], [82], [39], [42], [13], [81], [12], [14], [78], [31], [57], [56], [91], [8], [7], [32], [27], [36], [3], [34], [20], [18], [26], [43], [62], [58], [88], [28], [52], [11], [19], [35], [51]	[87], [17], [15], [41], [69], [54], [4], [80], [60], [21], [59], [93], [67], [23], [9], [40], [21], [68], [22], [90], [66], [89], [85], [82], [39], [42], [13], [12], [14], [32], [36], [34], [20], [18], [26], [43], [62], [88], [52], [25], [11], [72], [19], [35]	[87], [15], [41], [69], [44], [67], [40], [70], [85], [82], [39], [13], [14], [8], [3], [62], [61], [19]
Authentication issues	[17], [15], [65], [69], [44], [80], [83], [59], [67], [68], [22], [2], [89]	[87], [15], [65], [69], [44], [80], [60], [59], [93], [67], [21], [68], [22], [90], [66], [76], [86], [61]	[64], [81], [84]	[17], [15], [41], [69], [44], [67], [40], [26]
Missing authorization	[17], [15], [65], [69], [44], [80], [83], [59], [67], [68], [22], [85]	[87], [15], [65], [69], [44], [80], [60], [59], [93], [67], [21], [68], [22], [90], [66], [85], [52]	[17], [15], [41], [69], [54], [4], [80], [60], [21], [59], [93], [67], [23], [40], [21], [68], [22], [90], [66], [78], [8], [11], [72]	[17], [15], [41], [69], [44], [67], [40], [71]
Privacy issues	[64]	[87], [47], [15], [65], [69], [44], [80], [60], [59], [93], [67], [21], [68], [22], [90], [66], [64]	[47], [15], [41], [69], [54], [4], [80], [60], [59], [93], [67], [23], [40], [21], [68], [22], [90], [66], [70], [71], [52], [61]	[47], [15], [41], [69], [44], [67]
Weak default configuration	[17], [15], [65], [69], [44], [80], [83], [59], [67], [68], [22], [42], [14], [6]	[15], [65], [69], [44], [80], [60], [59], [93], [67], [21], [68], [22], [90], [66]	[15], [41], [69], [54], [4], [80], [60], [21], [59], [93], [67], [23], [9], [40], [21], [68], [22], [90], [66], [3]	[15], [41], [69], [44], [67], [40], [88]

- **Missing authorization:** Only authorized users should have access to robotic devices and their resources. Failing to manage unauthorized access properly may enable attackers to easily and remotely use certain robotic features and control the robot. At the application level, [17], [15], [65], [69], [44], [80], [83], [59], [67], [68], [22] most threats involve the ability to access robotic remotely by Internet services, software, mobile applications, etc. Additionally, because these applications communicate via networks, which may be the weakest links during an attack [87], [15], [65], [69], [44], [80], [60], [59], [93], [67], [21], [68], [22], [90], [66]. Anyone within the same network can gain access to the robot and send commands. In case of failed authentication, robots could also be attacked during the maintenance process of its firmware [17], [15], [41], [69], [54], [4], [80], [60], [21], [59], [93], [67], [40], [21], [68], [22], [90], [66]. For example, some robot manufacturers make firmware available online for updates, leaving the device vulnerable. However, making firmware available to the public becomes an issue only if the firmware is modifiable. Finally, unauthorized physical access to a robot may lead to availability issues. The intruder may attack the device hardware and use it to manipulate its data or change its behavior [17], [15], [65], [69], [44], [80], [83], [59], [67], [68], [22];

- **Privacy issues:** Some researchers are concerned that robots could raise privacy concerns, giving companies tremendous access into people's life. For example, robots' mobile applications can send private information to remote servers without user consent [47], [15], [41], [69], [44], [67]. At the firmware level, one of the major risks is that attacker get into the robot through firmware

and then steal information, such as sensitive IP, logs, and other content [47], [15], [41], [69], [54], [4], [80], [60], [59], [93], [67], [23], [40], [21], [68], [22], [90], [66]. Similarly, attacks that are performed at the network level may provide a vehicle for threats to users' privacy [87], [47], [15], [65], [69], [44], [80], [60], [59], [93], [67], [21], [68], [22], [90], [66];

- **Weak default configuration:** When robots include insecure features in their original configuration, they may easily be disabled or accessed. Generally, attacks exploiting these features operate at the hardware [17], [15], [65], [69], [44], [80], [83], [55], [59], [67], [68], [22]] and network level [15], [65], [69], [44], [80], [60], [59], [93], [67], [21], [68], [22], [90], https://arxiv.org/abs/1912.07714 [66], but there may also be applications accessible through default passwords or built using vulnerable open source code and libraries [15], [41], [69], [44], [67], [40]. Additionally, attacks may also be performed to corrupt firmware that is not properly configured or has an outdated configuration [15], [41], [69], [54], [4], [80], [60], [21], [59], [67], [23], [9], [40], [21], [68], [22], [90], [66].

4.3 Overview of attacks

The table 4 shows the types of cyber-attacks most commonly described in the literature. Looking at the literature, it is clear that this type of attack is the most common in robotics because of their severe impact on robots and their resources. Another reason for this is that DoS attacks are easy to execute; they can even be performed through the use of publicly available tools, which allow attackers to create malicious code, such as bots. Conversely, Stealthy and Sybil attacks are the least popular because they require sophisticated techniques and skilled attackers. The network layer is the most critical due to a number of availability issues. It represents the backbone for all communications in a robotics system. The firmware layer is also one of the most critical areas of cyber-security as it presents more vulnerabilities and defenses are often weakest in this part of the system.

Table 4: Perspective of Cyber-Attacks in Robotics System

Robot	Type	Reference	Attack								Level			
			Dos	MitM	Tampering	Fault Injection	Sybil	Sthealty	Eavesdropping	Spoofing	HW	Network	FW/O.S.	Application
Care-O-Bot	*Medical*	[3]	*1*			*1*			*1*				*1*	*1*
PeopleBot	*Mobile*	[6]	1	1									1	1
ABB IRB 140	*Industrial*	[7]	1	1	1						1	1	1	1
PeopleBot	*Mobile*	[9]	1										1	
Erector Spykee	*Toys*	[17]	1	1							1	1	1	1
Raven II	*Surgical*	[19]	1									1	1	
Kuka liwa	*Collaborative*	[23]	1									1	1	
ABB IRB 140	*Industrial*	[24]			1						1	1	1	
Amigobot	*Mobile*	[28]	1			1		1				1	1	1
AscTec Hummingbird, iRobot Create	*Drone/Autonomous, Mobile*	[29]					1			1		1	1	1
Raven II	*Surgical*	[57]	1	1					1			1		
Jacobs Robot	*Mobile*	[58]	1									1		
Parrot AR Drone 2.0	*Drone/Autonomous*	[62]								1		1		
Raven II	*Surgical*	[63]	1						1			1	1	1
CHIMERA	*Mobile*	[65]										1	1	
NPS ARSENIL	*Drone/Autonomous*	[80]		1								1	1	
			11	5	2	2	1	1	3	2	3	13	13	7

5 Current research issues

The increasing dependence of businesses and customers on robotics devices and applications is leading to an exponential growth in terms of cyber risk. Cyber-attacks exploit any type of vulnerabilities concerning robotics systems, whether they are come in the form of software or hardware, or are dependent on the person who uses them. Thus, because cyber-attacks are on the increase in this field, several scholars and experts are bringing cyber security into much prominent focus when trying to find methods to mitigate

cyber threats in robotics (see Fig.n. 10). Several research areas should be further investigated. Below we give some examples.

Figure 10: Countermeasures adopted in Robotic field

- **Security by design** - Implementing security by design means reducing vulnerabilities in software / hardware. This procedure requires a proper consideration of security properties from the very beginning in the requirements phase of the development. In particular, it is necessary to consider security requirements engineering for robotics applications, including privacy and safety aspects. Also, the evolvement of requirements through the whole SDLC (systems development life cycle) and the socio-economic impact of this evolvement should be taken into account. Similarly, it is necessary to develop security support in programming environments. This research area covers new programming platforms that deliver development and runtime environments for trustworthy application that is executed in complex robotics scenarios. The purpose of this discipline is to implement language based security, as well as to secure coding principles and practices. Code signatures and instrumentations, are also an important component of this area;

- **Security and safety co-engineering** - Developing a system that is safe and secure is one of the headrest challenges. Depending on the context, these two concepts could be contrasting and potential solutions need to meet specific risk factors related to both fields;

- **Monitoring** - Monitoring and tracking robotic activities, accesses, and the use of privileged accounts can be an effective way to detect and mitigate the impact of some attacks preventively. According to Alemzadeh et al. [3], detection mechanisms can dynamically estimate the consequence of the attacks before their effect manifests in the systems. Intrusion detection and preven-

tion systems should be adopted. Specific anomaly detection mechanisms, able to behaviourally fingerprinting robots behaviour could be also investigated;

- **Data usage control** - sensing is one of the main activities of robotics systems. Those often collaborate with humans and the collected data should be controlled, where shared and disseminated to other digital systems;
- **Identity management** - robotics systems are often composed of several devices that have their own input output capabilities. Considering how to identify the robotic systems is paramount for the consideration of trust issues related, for instance, to collaborative aspects;
- **Trustworthiness** - Trust is an essential concept in human-robot interaction and their "secure relationship." Trust, defined as "an attitude involving beliefs and expectations of a trustee's trustworthiness," [46] is often connected to vulnerability since the "trustor is dependent on the trustee," and there is always a certain degree of uncertainty about relying on the trustee. Recent studies have proved that trust in social/professional robots is lost when functionalities and operation misbehaves and does not meet expectations. Trust is, therefore, a critical factor to consider when the goal is trusting that robotics systems behave securely (e.g., trusting that the information users get from the robotic device is secure and reliable). One example of developing trust in robotics is implementing security by design and default when building robotics systems. Knowing that robot manufacturers and developers apply cyber security considerations throughout the design and development stages could help create a more operating framework for robots and their users as a warrant for the whole robotics industry;
- **Robustness** - Organizations operating in the robotics field, especially those that have suffered from the effects of cyber attacks, have strengthened perimeter security controls, adopted firewalls, and other protection systems. Although necessary, such security methods are still not enough to protect companies from large-scale cyber threats. For this reason, several authors [8] discussed the importance of strengthening the robustness of communications rather than focusing on enhancing other areas. According to Priyadarshini, [67] the transmission medium is one of the most vulnerable components. The author argues that ensuring that adding a layer of security to reinforce communications would reduce probable insecurities.

More generally, other authors [1] argue that it is critical to have extensive knowledge and be aware of the contemporary and existing cyber-attacks and countermeasures that are specific to robotics systems. The growing shortage of trained cybersecurity employees and the constant pressure to manage and reduce costs make it harder for companies to maintain robotics systems secure or improve their cybersecurity posture more efficiently.

6 Conclusion

Cybersecurity Robotics is a multidisciplinary research domain that is growing in relevance and importance due to the persistent growth of robotics systems and the related cybersecurity and safety risks and challenges. In this work, we reviewed the literature concerning the following topics: Robotics, IT technologies used in Robotics and related fields. Firstly, we discussed the current cybersecurity scenario in robotics; then, we classified and summarize the modules composing the robotic systems with the aim to analyze them in relation to their vulnerabilities.

In particular, we examined the connection between issues in robotics and other domains, such as security and safety. We provided an overview of the regulatory environment surrounding robotics, which helped us frame the current situation in robotics systems.

Secondly, we discussed the problems derived from the interconnection between Robotics and IT technologies and the cybersecurity vulnerabilities affecting robotic systems in industrial contexts and other sectors (i.e. house, autonomous vehicles, unstructured environment). Thirdly, we analyzed potential and actual cyber-attacks, provided a classification according to the CIA triad concept, and divided them into categories of threats. The outcome of this analysis suggests that Robotics faces prominent challenges on security in the following areas:

- Collaborative Robotics;
- Autonomous vehicles;
- Autonomous Robotic platform;
- Regulation and regulatory frameworks.

Finally, we noticed that, in the last decades, the research and development in the robotics field shifted from a focus on industrial robots to a focus on intelligent robotics. This shift created methods of easier integration to create robotics systems, which are capable of providing promising results in different areas of robotic research, such as artificial intelligence, cognitive robotics, human-robot interaction, multi-agent systems for mobile robot collaboration, etc. [77]. In particular, the use of AI and ML algorithms led to new security and safety challenges. The introduction of mandatory regulatory requirements will probably slow down the pace of progress in robotics, but the current advanced robotics systems have enormous potential to transform many aspects of people's lives. This paper aims to bring together the most relevant studies in this domain and to identify the most common risks, threats, and vulnerabilities. This work will serve as a body of knowledge and reference tool to help guide cybersecurity experts, users, manufacturers, and scholars to further understand the threats surrounding this field and create awareness about the topic.

Acknowledgment

This work has been partially supported by E-CORRIDOR project.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] C. Abdullahi, K. Gour, and K. Joarder. *Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches*, pages 284–299. IGI Global, 2017.

[2] A. M. Ahmad Mizher Al-Jabbar and R. Sulaiman. Robotic movement encryption using guaranteed cellular automata. In *Proc. of the 2018 Cyber Resilience Conference (CRC'18), Putrajaya, Malaysia*, pages 13–15. IEEE, November 2018.

[3] H. Alemzadeh, D. Chen, X. Li, T. Kesavadas, Z. T. Kalbarczyk, and R. K. lyer. Targeted attacks on teleoperated surgical robots: Dynamic model-based detection and mitigation. In *Proc. of the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'16), Toulouse, France*, pages 395–406. IEEE, September 2016.

[4] A. AlMajali, A. Y. Khalil, B. J. Mohd, W. Dweik, S. A. Ghalyon, and R. Hasan. Semi-quantitative security risk assessment of robotic systems. *Jordanian Journal of Computers and Information Technology*, 4:185–200, December 2018.

[5] H. Anada. Decentralized multi-authority anonymous authentication for global identities with non-interactive proofs. In *Proc. of the 2019 IEEE International Conference on Smart Computing (SMARTCOMP'19), Washington, DC, USA*, pages 25–32. IEEE, June 2019.

[6] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan. Hardware trojan attacks: Threat analysis and countermeasures. *Proceedings of the IEEE*, 102(8):1229–1247, August 2014.

[7] A. Birk, S. Schwertfeger, and K. Pathak. A networking framework for teleoperation in safety, security, and rescue robotics. *IEEE Wireless Communications*, 16(1):6–13, March 2009.

[8] T. Bonaci, J. Herron, T. Yusuf, J. Yan, T. Kohno, and H. J. Chizeck. To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robots. `https://arxiv.org/abs/1504.04339` [Online; accessed on September 15, 2021], May 2015.

[9] T. Bonaci, J. Yan, J. Herron, T. Kohno, and H. J. Chizeck. Experimental analysis of denial-of-service attacks on teleoperated robotic systems. In *Proc. of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems (ICCPS'15), Seattle, Washington, USA*, pages 11—-20. ACM, April 2015.

[10] J. Borenstein and Y. Pearson. Robot caregivers: Harbingers of expanded freedom for all? *Ethics and Information Technology*, 12(3):277–288, July 2010.

[11] B. Breiling, B. Dieber, and P. Schartner. Secure communication for the robot operating system. In *Proc. of the 2017 Annual IEEE International Systems Conference (SysCon'17), Montreal, Quebec, Canada*, pages 1–6. IEEE, April 2017.

[12] E. Byres and D. Hoffman. The myths and facts behind cyber security risks for industrial control systems. `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.579.3650&rep=rep1&type=pdf` [Online; accessed on September 15, 2021], December 2004.

[13] R. Candell, K. Stouffer, and D. Anand. A cybersecurity testbed for industrial control systems. In *Proc. of the 2014 Process Control and Safety Symposium (PCS'14), Houston, Texas, USA*, pages 1–16. Springer-Verlag, October 2014.

[14] R. Candell, T. A. Zimmerman, and S. K. A. An industrial control system cybersecurity performance testbed. `https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf` [Online; accessed on September 15, 2021], December 2015.

[15] C. Cerrudo and L. Apa. Hacking robots before skynet. `https://ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf` [Online; accessed on September 15, 2021], March 2017.

[16] A. Chibani, Y. Amirat, S. Mohammed, E. Matson, N. Hagita, and M. Barreto. Ubiquitous robotics: Recent challenges and future trends. *Robotics and Autonomous Systems*, 61(11):1162–1172, 2013.

[17] G. Clark, M. Doran, and T. Andel. Cybersecurity issues in robotics. In *Proc. of the 2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA'17), Savannah, Georgia, USA*, pages 1–5. IEEE, March 2017.

[18] G. W. Clark, T. R. Andel, and M. V. Doran. Simulation-based reduction of operational and cybersecurity risks in autonomous vehicles. In *Proc. of the 2019 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA'19), Las Veges, Nevada, USA*, pages 140–146. IEEE, April 2019.

[19] N. DeMarinis, S. Tellex, V. Kemerlis, G. Konidaris, and R. Fonseca. Scanning the internet for ros: A view of security in robotics research. In *Proc. of the 2019 International Conference on Robotics and Automation (ICRA'19), Montreal, Quebec, Canada*, pages 8514–8521. IEEE, May 2019.

[20] B. Dieber and B. Breiling. Security considerations in modular mobile manipulation. In *Proc. of the 2019 Third IEEE International Conference on Robotic Computing (IRC'19), Naples, Italy*, pages 70–77. IEEE, February 2019.

[21] B. Dieber, B. Breiling, S. Taurer, S. Kacianka, S. Rass, and P. Schartner. Security for the robot operating system. *Robotics and Autonomous Systems*, 98:192–203, December 2017.

[22] G. Dini and A. L. Duca. A secure communication suite for underwater acoustic sensor networks. *Sensors*, 12(11):15133–15158, November 2012.

[23] D. I. Dogaru and I. Dumitrache. Cyber security in healthcare networks. In *Proc. of the 2017 E-Health and Bioengineering Conference (EHB'17), Sinaia, Romania*, pages 414—-417. IEEE, June 2017.

[24] Z. Dolic, R. Castro, and A. Moarcas. Robots in healthcare: A solution or a problem? : Workshop proceedings. `https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/638391/IPOL_IDA(2019)`

638391_EN.pdf [Online; accessed on September 15, 2021], April 2019.

[25] A. Elkady and T. Sobh. Robotics middleware: A comprehensive literature survey and attribute-based bibliography. *Journal of Robotics*, 2012:1–15, May 2012.

[26] Y. Eray, G. Cemal, and A. Ziya. A study on cyber-security of autonomous and unmanned vehicles. *The Journal of Defense Modeling and Simulation*, 12(4):369–381, October 2015.

[27] J. Fink, A. Ribeiro, and V. Kumar. Robust control for mobility and wireless communication in cyber–physical systems with application to robot teams. *Proceedings of the IEEE*, 100(1):164–178, September 2011.

[28] P. Fraisse, R. Zapata, W. Zarrad, and D. Andreu. Remote secure decentralized control strategy for mobile robots. *Advanced Robotics*, 19(9):1027–1040, April 2005.

[29] S. Giedre, S. N. Geok, R. Justin, and M. Aditya. A comprehensive approach, and a case study, for conducting attack detection experiments in cyber–physical systems. *Robotics and Autonomous Systems*, 98:174–191, December 2017.

[30] S. Gil, K. Swarun, M. Mazumder, D. Katabi, and D. Rus. Guaranteeing spoof-resilient multi-robot networks. *Autonomous Robots*, 41(6):1383—-1400, August 2017.

[31] S. L. Gregory and T. Bhavani. Cyberphysical systems security applied to telesurgical robotics. *Computer Standards and Interfaces*, 34(1):225–229, January 2012.

[32] F. Higgins, A. Tomlinson, and K. M. Martin. Survey on security challenges for swarm robotics. In *Proc. of the 2009 Fifth International Conference on Autonomic and Autonomous Systems (ICAS'09), Valencia, Spain*, pages 307–312. IEEE, April 2009.

[33] C. Holder, V. Khurana, F. Harrison, and L. Jacobs. Robotics and law: Key legal and regulatory implications of the robotics age (part i of ii). *Computer Law and Security Review*, 32(3):383–402, June 2016.

[34] M. Horton, L. Chen, and B. Samanta. Enhancing the security of iot enabled robotics: Protecting turtlebot file system and communication. In *Proc. of 2017 International Conference on Computing, Networking and Communications (ICNC'17), Silicon Valley, California, USA*, page 662—666. IEEE, January 2017.

[35] F. J.Rodríguez-Lera, V. Matellán-Olivera, J. Balsa-Comerón, Ángel Manuel Guerrero-Higueras, and C. Fernández-Llamas. Message encryption in robot operating system: Collateral effects of hardening mobile robots. *Frontiers in ICT*, 5(2):1–12, March 2018.

[36] A. A. E. Kalam, A. Ferreira, and F. Kratz. Bilateral teleoperation system using qos and secure communication networks for telemedicine applications. *IEEE Systems Journal*, 10(2):709–720, May 2015.

[37] G. Kasturi, A. Jain, and J. Singh. Detection and classification of radio frequency jamming attacks using machine learning. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 11(4):49–62, December 2020.

[38] Y. Katagiri, C. Nass, and Y. Takeuchi. Cross-cultural studies of the computers are social actors paradigm: The case of reciprocity. https://web.ics.purdue.edu/~duffy/IE486_Spr07/ComputersAsSocialActor.pdf [Online; accessed on September 15, 2021], August 2001.

[39] B. Kehoe, S. Patil, P. Abbeel, and K. Goldberg. A survey of research on cloud robotics and automation. *IEEE Transactions on Automation Science and Engineering*, 12(2):398–409, January 2015.

[40] A. Khalid, P. Kirisci, Z. H. Khan, Z. Ghrairi, K.-D. Thoben, and J. Pannek. Security framework for industrial collaborative robotic cyber-physical systems. *Computers in Industry*, 97:132–145, May 2018.

[41] A. Y. Khalil, A. AlMajali, S. A. Ghalyon, W. Dweik, and B. J. Mohd. Analyzing cyber-physical threats on robotic platforms. *Sensors*, 18(5):1643:1–22, May 2018.

[42] F. Khorrami, P. Krishnamurthy, and R. Karri. Cybersecurity for control systems: A process-aware perspective. *IEEE Design&Test*, 33(5):75–83, July 2016.

[43] M. Kinzler, J. Miller, Z. Wu, A. Williams, and D. Perouli. Cybersecurity vulnerabilities in two artificially intelligent humanoids on the market. In *Proc. of the 2019 Workshop on Technology and Consumer Protection (ConPro '19), held in conjunction with the 40th IEEE Symposium on Security and Privacy, San Francisco, California, USA*, pages 1–7, May 2019.

[44] L. A. Kirschgens, I. Z. Ugarte, E. G. Uriarte, A. M. Rosas, and V. M. Vilches. Robot hazards: From safety to security. https://arxiv.org/pdf/1806.06681.pdf [Online; accessed on September 15, 2021], September 2019.

[45] R. Kumar, P. K. Pattnaik, and P. Pandey. *Detecting and Mitigating Robotic Cyber Security Risks*. IGI Global, 2017.

[46] A. Langer, R. Feingold-Polak, O. Mueller, P. Kellmeyer, and S. Levy-Tzedek. Trust in socially assistive robots: Considerations for use in rehabilitation. *Neuroscience and Biobehavioral Reviews*, 104:231–239, September 2019.

[47] R. F. Lera, F. Camino, A. Guerrero, and V. Matellan. *Cybersecurity of Robotics and Autonomous Systems: Privacy and Safety*, chapter 5. InTech Open, George Dekoulis, 2017.

[48] P. Lin, K. Abney, and G. Bekey. Robot ethics: Mapping the issues for a mechanized world. *Artificial Intelligence*, 175(5-6):942–949, April 2011.

[49] Y. Lu, K. Morris, and S. Frechette. Current standards landscape for smart manufacturing systems. `https://www.nist.gov/publications/current-standards-landscape-smart-manufacturing-systems` [Online; accessed on September 15, 2021], February 2016.

[50] C. Lutz and A. Tamò. Robocode-ethicists: Privacy-friendly robots, an ethical responsibility of engineers? In *Proc. of the 2015 ACM Web Science Conference (WebSci'15), Oxford, UK*, pages 1–12. ACM, June-July 2015.

[51] A. Marotta, F. Martinelli, S. Nanni, A. Orlando, and A. Yautsiukhin. Cyber-insurance survey. *Computer Science Review*, 24:35–61, May 2017.

[52] F. Martín, E. Soriano, and J. M. Cañas. Quantitative analysis of security in distributed robotic frameworks. *Robotics and Autonomous Systems*, 100:95–107, February 2018.

[53] A. Marty and R. Hartmut. Legal and ethical considerations in the era of autonomous robots, 2018.

[54] V. Matellán, T. Bonaci, and G. Sabaliauskaite. Cyber-security in robotics and autonomous systems. *Robotics and Autonomous Systems*, 100:41–42, February 2018.

[55] V. Mayoral-Vilches, U. A. Carbajo, and E. Gil-Uriarte. Industrial robot ransomware: Akerbeltz. In *Proc. of 4th IEEE International Conference on Robotic Computing (IRC'20), Taichung, Taiwan*, pages 432–435. IEEE, November 2020.

[56] J. Michniewicz and G. Reinhart. Cyber-physical robotics – automated analysis, programming and configuration of robot cells based on cyber-physical-systems. *Procedia Technology*, 15:566–575, October 2014.

[57] J. Michniewicz and G. Reinhart. Cyber-physical-robotics – modelling of modular robot cells for automated planning and execution of assembly tasks. *Mechatronics*, 34:170–180, March 2016.

[58] J. Miller, A. Williams, and D. Perouli. A case study on the cybersecurity of social robots. In *Proc. of Companion of the 2018 ACM/IEEE International Conference on Human-Robot Interaction (HRI'18), Chicago, Illinois, USA*, page 195–196. ACM, March 2018.

[59] S. Morante, J. G. Victores, and C. Balaguer. Cryptobotics: Why robots need cyber safety. *Frontiers in Robotics and AI*, 2(23):1–4, September 2015.

[60] S. Morimoto, F. Wang, R. Zhang, and J. Zhu. Cybersecurity in autonomous vehicles. `http://knowledgecenter.comarch.com/en/?id=56` [Online; accessed on September 15, 2021], May 2017.

[61] M. Mukhandi, D. Portugal, S. Pereira, and M. S. Couceiro. A novel solution for securing robot communications based on the mqtt protocol and ros. In *Proc. of 2019 IEEE/SICE International Symposium on System Integration (SII'19), Paris, France*, pages 608–613. IEEE, January 2019.

[62] A. Munteanu, R. Muradore, M. Merro, and P. Fiorini. On cyber-physical attacks in bilateral teleoperation systems: An experimental analysis. In *Proc. of 2018 IEEE Industrial Cyber-Physical Systems (ICPS'18), St. Peterburg, Russia*, pages 159–166. IEEE, May 2018.

[63] C. Nass, J. Steuer, and E. Siminoff. Computer are social actors. In *Proc. of 1994 Conference Companion on Human Factors in Computing Systems (CHI'94), Boston, Massachusetts, USA*, page 204. ACM, January 1994.

[64] A. Nellis. Hello, friend: Cybersecurity issues in season one of mr. robot. *The Serials Librarian*, pages 203–211, December 2016.

[65] M. Pogliani and M. P. e. a. Davide Quarta. Security of controlled manufacturing systems in the connected factory: the case of industrial robots. *Journal of Computer Virology and Hacking Techniques*, 15:161–175, February 2019.

[66] M. L. Polla, F. Martinelli, and D. Sgandurra. A survey on security for mobile devices. *IEEE Communications Surveys Tutorials*, 15(1):446–471, March 2013.

[67] I. Priyadarshini. *Cyber Security Risks in Robotics*, chapter 61. IGI Global, 2018.

[68] D. Quarta, M. Pogliani, M. Polino, F. Maggi, A. M. Zanchettin, and S. Zanero. An experimental security analysis of an industrial robot controller. In *Proc. of the 2017 IEEE Symposium on Security and Privacy (SP'17), San Jose, California, USA*, pages 268–286. IEEE, May 2017.

[69] D. Quartaa, M. Pogliani, M. Polino, A. M. Zanchettin, S. Zanero, and P. di Milano. Rogue robots: Testing the limits of an industrial robot's security. Technical report, Trend Micro, Incorporated. All rights reserved, 2017.

[70] A. Rasim, I. Yadigar, and S. Lyudmila. Cyber-physical systems and their security issues. *Computers in Industry*, 100:212–223, September 2018.

[71] Y. B. Reddy. Security and design challenges in cyber-physical systems. In *Proc. of the 2015 12th International Conference on Information Technology - New Generations (ITNG'15), Las Vegas, Nevada, USA*, pages 200–205. IEEE, April 2015.

[72] S. Rivera, S. Lagraa, and R. State. Rosploit: Cybersecurity tool for ros. In *Proc. of the 3rd IEEE International Conference on Robotic Computing (IRC'19), Naples, Italy*, pages 415–416. IEEE, February 2019.

[73] M. Rueben, C. M. Grimm, F. J. Bernieri, and W. D. Smart. A taxonomy of privacy constructs for privacy-sensitive robotics. `http://knowledgecenter.comarch.com/en/?id=56` [Online; accessed on September 15, 2021], January 2017.

[74] M. Rueben and W. D. Smart. Privacy in human-robot interaction : Survey and future work. In *Proc. of the 2016 We Robot (WR'16), Miami, Florida, USA*, pages 1–43. University of Miami, April 2016.

[75] M. Rueben, W. D. Smart, C. Grimm, and M. Cakmak. Privacy-sensitive robotics. In *Proc. of the 2017 ACM/IEEE International Conference on Human-Robot Interaction (HRI'17), Vienna, Austria*, pages 425–426. ACM, March 2017.

[76] G. Sabaliauskaite, G. Ng, J. Ruths, and A. Mathur. Experimental evaluation of stealthy attack detection in a robot. In *Proc. of the 2015 IEEE 21st Pacific Rim International Symposium on Dependable Computing (PRDC'15), Zhangjiajie, China*, pages 446–471. IEEE, November 2015.

[77] S. I. Sacala, A. M. Mihnea, A. D. C. I. Munteanu, and S. I. Caramihai. Cyber physical systems oriented robot development platform. *Procedia Computer Science*, 65:203–209, September 2015.

[78] O. Saha and P. Dasgupta. A comprehensive survey of recent trends in cloud robotics architectures and applications. *Robotics*, 7(3):1–7, August 2018.

[79] B. Schafer and L. Edwards. "i spy, with my little sensor": fair data handling practices for robots between privacy, copyright and security. *Connection Science*, 29(3):200–209, September 2017.

[80] R. Shah. Security landscape for robotics. `https://arxiv.org/pdf/1904.03033.pdf` [Online; accessed on September 15, 2021], April 2019.

[81] K. Stouffer and R. Candell. Measuring impact of cybersecurity on the performance of industrial control systems. *Mechanical Engineering*, 136(12):S4–S7, December 2014.

[82] K. A. Stouffer, V. Y. Pillitteri, S. Lightman, M. Abrams, and A. Hahn. Guide to industrial control systems (ics) security. `https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf` [Online; accessed on September 15, 2021], May 2015.

[83] T. Theodoridis and H. Hu. Toward intelligent security robots: A survey. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 42(6):1219–1230, November 2012.

[84] P. Thulasiraman. Study of security primitives for the robot operating system (ros) of uav swarms. `https://calhoun.nps.edu/handle/10945/53348` [Online; accessed on September 15, 2021], 2017.

[85] N. Tuptuk and S. Hailes. Security of smart manufacturing systems. *Journal of Manufacturing Systems*, 47:93–106, May 2018.

[86] E. Vattapparamban, G. İsmail, and A. İhsan Yürekli et al. Drones for smart cities: Issues in cybersecurity, privacy, and public safety. In *Proc. of 2016 International Wireless Communications and Mobile Computing Conference (IWCMC'16), Paphos, Cyprus*, pages 216–221. IEEE, September 2016.

[87] V. M. Vilches, L. A. Kirschgens, A. B. Calvo, A. H. Cordero, R. I. Pisón, D. M. Vilches, A. M. Rosas,

G. O. Mendia, L. U. S. Juan, I. Z. Ugarte, E. Gil-Uriarte, E. Tews, and A. Peter. Introducing the robot security framework (rsf), a standardized methodology to perform security assessments in robotics. `https://arxiv.org/pdf/1806.04042.pdf` [Online; accessed on September 15, 2021], June 2018.

[88] T. Vuong, A. Filippoupolitis, G. Loukas, and D. Gan. Physical indicators of cyber attacks against a rescue robot. In *Proc. of the 2014 IEEE International Conference on Pervasive Computing and Communication Workshops (PERCOM WORKSHOPS'14), Budapest, Hungary*, pages 338–343. IEEE, March 2014.

[89] L. Wang, M. Törngren, and M. Onori. Current status and advancement of cyber-physical systems in manufacturing. *Journal of Manufacturing Systems*, 37:517–527, May 2015.

[90] G. Yang, L. Dai, and Z. Wei. Challenges, threats, security issues and new trends of underwater wireless sensor networks. *Sensors*, 18(11), November 2018.

[91] K. S. Yogesh and A. Bagla. Security challenges for swarm robotics. *International Journal of Information Technology and Knowledge Management*, 2(1):45–48, 2009.

[92] I. Zamalloa, I. Muguruza, A. Hernández, R. Kojcev, and V. Mayoral. An information model for modular robots: the hardware robot information model (hrim). `https://arxiv.org/abs/1802.01459` [Online; accessed on September 15, 2021], February 2018.

[93] T. Zimmerman. Metrics and key performance indicators for robotic cybersecurity performance analysis. `https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8177.pdf` [Online; accessed on September 15, 2021], May 2019.

Author Biography

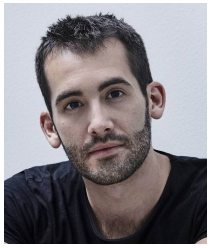
Giovanni Lacava (Ph.D. 2016, M.Eng. 2011) is a Post Doctoral fellow at the Institute for Informatics and Telematics of the National Research Council of Italy (IIT CNR) within the security group. His research topic is trust and security in Robotics System. In [2012-2015] worked on development of control system for Autonomous Underwater Vehicles within ARROWS project (FP7 - EdgeLab srl). In [2016-2018] worked on development of control system for Endocopic Robotic Platform in clinical are within Endoo Project (H2020 - BioRobotics Institute SSSA).

Angelica Marotta (M.Sc. 2017) is a cybersecurity expert with experience working in research and higher education. Forever interested in how cybersecurity intersects with society, Angelica has an interdisciplinary background. She earned a Bachelor's degree in Computer Science from the University of Pisa, a Graduate Certificate in Cyber Security, and a Master's degree in Justice Studies with a specialization in Cyber Security from Southern New Hampshire University. She is also a certified ISO 27001 (Information Security Management Systems) Auditor/Lead Auditor. Her research interests mainly involve cyber insurance, risk management, cybersecurity culture, compliance, and cybersecurity robotics.

Fabio Martinelli is a research director of the Italian National Research Council (CNR). He is co-author of more than four hundreds of papers on international journals and conference/workshop proceedings. His main research interests involve security and privacy in distributed and mobile systems and foundations of security, privacy and trust. He founded and chaired the WG on Security and Trust management (STM) of the European Research Consortium in Informatics and Mathematics (ERCIM) and the WG 11.14 in secure engineering of the International Federation of Information Processing (IFIP). He coordinated the EU NESSoS Network of Excellence in Future internet Security and the EU Training Network on Cyber Security (NeCS). He also served as expert in the EU H2020 Protection and Security Advisory Goup (PASAG) and acts as First Director in the Board of the European Cyber Security Organization (ECSO) and co-chairs ECSO WG6 SRIA.

Andrea Saracino (Ph.D. 2015, M.Eng. 2011) is a Researcher at Istituto di Informatica e Telematica of the National Research Council (IIT-CNR) of Italy. His research is focused on applications of AI for security of mobile and distributed systems, with an emphasis on intrusion and malware detection in Android devices. He is the co-chair of the working group on AI & Cybersecurity of the Italian Association for AI (AIxIA). He is the project coordinator for the H2020 project SIFIS-Home and he is (or has been) involved in a number of EU-project such as EU-H2020 E-Corridor, EU-H2020 C3ISP, EU-H2020 NeCS, EU-H2020 Cybersure, EIT-Digital Trusted Cloud and IoT.

Antonio La Marra (M.Eng. 2015) is the CEO of Security Forge an innovative startup working in data protection and cybersecurity field. Security Forge wants to enable secure and confidential collaboration among different parties, building on top of enhanced data protection. He has an extensive experience in development and exploitation of technologies for access and usage control and has actively participated in the activities of the H2020 project C3ISP and a number of EIT Digital projects.



Víctor Mayoral-Vilches (M.Sc. 2013) is a Robotics architect at Alias Robotics with strong technical background in embedded and deep embedded systems. Víctor has not only experience in functional safety and cybersecurity, but also more than 25 scientific publications and 10 patents filed, mostly in the fields of secure and reconfigurable hardware and software for robots. He spent the last 10 years building robots and interacting with manufacturers and developing strong relationships in the robotics industry. In addition, he experienced to lead research initiatives and projects in the fields of robotics, cybersecurity and artificial intelligence.

Endika Gil-Uriarte (M.Sc. 2014) is the current CSO at Alias Robotics, former CEO. Endika has a background as a researcher with a wide experience in academia (University of Southampton), now devoted to improving the robotics and security intersection know-how. Endika has participated and leaded several research initiatives at EU and national levels. As a contributor to new standards in robotics and well-known speaker in several conferences, he's an advocate for the next generation of secure robots.