


Security Reference Architecture for Cyber-Physical Systems (CPS)


Julio Moreno

(NTT Data, Madrid, Spain)

 <https://orcid.org/0000-0001-9974-1199>, jmorgarc@nttdata.com


David G. Rosado

(GSyA Research Group. University of Castilla-La Mancha, Ciudad Real, Spain)

 <https://orcid.org/0000-0003-4613-5501>, david.grosado@uclm.es


Luis E. Sánchez

(GSyA Research Group. University of Castilla-La Mancha, Ciudad Real, Spain)

 <https://orcid.org/0000-0003-0086-1065>, luise.sanchez@uclm.es


Manuel A. Serrano

(Alarcos Research Group. University of Castilla-La Mancha, Ciudad Real, Spain)

 <https://orcid.org/0000-0003-0962-5659>, manuel.serrano@uclm.es

Eduardo Fernández-Medina

(GSyA Research Group. University of Castilla-La Mancha, Ciudad Real, Spain)

 <https://orcid.org/0000-0003-2553-9320>, eduardo.fdezmedina@uclm.es

Abstract Cyber-physical systems (CPS) are the next generation of engineered systems into which computing, communication, and control technologies are now being closely integrated. They play an increasingly important role in critical infrastructures, governments and everyday life. Security is crucial in CPS, but they were not, unfortunately, initially conceived as a secure environment, and if these security issues are to be incorporated, then security must be considered from the very beginning of the system design. One way in which to solve this problem is by having a global perspective, which can be achieved by employing a Reference Architecture (RA), since it is a high-level abstraction of a system that could be useful in the implementation of complex systems. It is widely accepted that adding elements in order to address many security factors (integrity, confidentiality, availability, etc.) and facilitate the definition of the security requirements of a Security Reference Architecture (SRA) is a good starting point when attempting to solve these kinds of cybersecurity problems and protect the system from the beginning of the development. An SRA makes it possible to define the key elements of a specific environment, thus allowing a better understanding of the inherent elements of the environments, while promoting the integration of security aspects and mechanisms. The present paper, therefore, presents the definition of an SRA for CPS by using UML models in an attempt to facilitate secure CPS implementations.

Keywords: Cyber-Physical Systems (CPS); Security Reference Architecture; Secure design; Security patterns

Categories: D.2, K.6.5

DOI: 10.3897/jucs.68539

1 Introduction

Cyber-physical systems (CPS) are intelligent systems that include computing, storage, and communication capabilities with the capacity to track and/or control capabilities of objects in the physical world [Alur, 2015, Maleh, 2020] and provide citizens and businesses with a wide range of innovative applications and services [European Commission, 2013, Walter Colombo et al., 2020]. The CPS cover from Machine-to-Machine (M2M) and Internet of Things (IoT) communications, and the integration of heterogeneous data from multiple sources, in addition to having been integrated into Cloud Computing and Big Data platforms [Jara et al., 2014]. The research related to CPS has recently drawn the attention of academia, industry, and governments owing to their great impact on society, economy, and the environment [Monostori et al., 2016, Lee, 2015, Monostori, 2014]. These highly interconnected and integrated systems provide new functionalities with which to improve the quality of life and allow technological advances in critical areas, such as personalized health care [Suh et al., 2014, Haque et al., 2014, Liu et al., 2018], emergency response [Zander et al., 2015], traffic flow management [Rawat et al., 2015, Xiong et al., 2015, Mihalache et al., 2019], intelligent [Frazzon et al., 2013, Lee et al., 2015, Lee et al., 2013, Wang et al., 2015] defense and national security [Rajkumar et al., 2010, Das et al., 2012], and energy supply [Yu and Xue, 2016, Moness and Moustafa, 2016, Cheng et al., 2019].

While ongoing research work focuses on achieving goals such as the stability, performance, robustness, and efficiency of physical systems [Rajkumar et al., 2010], security and safety within CPS is usually ignored [Kim and Kumar, 2012, Konstantinou et al., 2015, Wang et al., 2010, Tantawy et al., 2020]. Security and safety are, nonetheless, two key properties of CPS [Banerjee et al., 2011, Piètre-Cambacédès and Chaudet, 2010]. They share the same goal: protecting CPS from failures [Novak and Treytl, 2008]. According to NIST, we understand safety as the freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. Security is a condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions in spite of the risks posed by threats to its use of systems. CPS are currently being extensively integrated into various critical infrastructures and industrial control systems, in which hazards include explosions, fires, floods, chemical/biochemical spills and releases, etc., and in which any safety or security breaches to these systems could have catastrophic consequences.

Cybersecurity is a necessary feature of the CPS architecture as regards ensuring that CPS capabilities are not compromised by malicious agents, and that the integrity of the information used, processed, stored and transferred is preserved and kept confidential when necessary [Zacchia Lun et al., 2019]. Cybersecurity is a fundamental discipline that provides confidence in terms such that CPS, their information, and supporting communications and information infrastructures are adequately safeguarded. CPS are increasingly being used in critical infrastructures and other settings. However, CPS have many unique characteristics, including the need for real-time response and extremely high availability, predictability, and reliability, which impacts on cybersecurity decisions [Brewer, 2013]. As advances in technology permit the automatic control of more and more of the functions of physical systems, the opportunity for cyberattacks, including the exploitation of the aforementioned automation capabilities, becomes a greater risk [Horowitz and Pierce, 2013]. Providing cybersecurity to CPS is further complicated by the fact that an ever-expanding array of CPS will be required in order to operate in a wide range of operational conditions, and could be threatened by a plethora of cyberattack

mechanisms and processes.

CPS are, therefore, very complex environments that form an ecosystem in which there is a physical part, with different sensors and actuators, which is in turn controlled by a virtual part that makes decisions based on the analysis of the data generated by the physical part. The complexity of this type of environment makes it difficult to address its security without using a holistic perspective, which considers all the main components of CPS using a high level of abstraction. A global perspective must consequently be followed if their cybersecurity issues are to be properly addressed. One means that has proved to be a valuable solution is that of Reference Architectures (RA) [Avgeriou, 2003, Medvidovic and Taylor, 2010]. There are several RAs that represent different kinds of systems, such as, the Internet of Things [Krco et al., 2014], Cloud Computing [Fernandez et al., 2016a] or Big Data [NIST Group Big Data Public Working, 2018]. An RA can be defined as an abstract software architecture that is based on one or more domains and that does not contains implementation features [Avgeriou, 2003].

An RA is, moreover, usually expressed with a high level of abstraction in order to make it reusable, extendable and configurable for any organization, and it can in consequence be adapted for use in any kind of scenario. Furthermore, when security concepts, such as policies, threats, security patterns or vulnerabilities, are added to the RA, it becomes a Security Reference Architecture (SRA). An SRA is a high-level architecture that incorporates a set of elements that not only provides an abstract view of the different components and elements of a technology, but also facilitates the definition of security requirements and allows a better understanding of security concepts. An SRA is a tool that employs a high level of abstraction in order to identify the most relevant components of a system (in this case, a CPS), and can also help elicit and analyze the security requirements and solutions that suit the inherent characteristics of the system. The SRA should be a central element that is accompanied by multiple techniques such as security patterns and security modeling techniques, and methods for the analysis, design and detailed construction of the system [Fernandez et al., 2016b]. An SRA can, therefore, be used to describe a conceptual security model for a CPS. In a nutshell, SRAs are a good well-known way in which to express an abstract conceptual model of a concrete technology in a way that is accessible to any user.

The scientific community and various standardization companies have described several architectures that attempt to abstract the main components or layers of a CPS. However, as the systematic review of the literature in the Related Work section shows, most of these proposals do not contemplate security as a key aspect when building this kind of environment. We, therefore, reviewed the main proposals in order to create our own SRA for CPS. These proposals were found and analyzed by performing a systematic mapping study (SMS). Once the proposals made by the scientific community had been analyzed, different standards related to CPS were examined. We then discussed all this information with researchers who have extensive experience in the fields of cybersecurity and security architectures so as to eventually create our own proposal for a specific SRA for CPS. This SRA will allow a better understanding of CPS while simultaneously emphasizing the importance of their security concepts. In order to achieve that purpose, our architecture is represented by means of UML diagrams, which allow a more in-depth definition of the connection between the different components and layers of a CPS. UML is a unified language that allows elements, components, software concepts and information systems to be modeled with a semantics and syntax that is easily understood by a variety of stakeholders, including those who are more closely related to the business and its requirements, along with those whose concerns are more technical and are closer to the implementation [Fabian et al., 2010].

The remainder of this paper is organized as follows: Section 2 describes the related work as regards the different proposals made by both the scientific community and the various standardization companies, together with a systematic review of literature carried out with regard to SRA for CPS. Section 3 defines our proposal, including a subsection for each layer of the SRA. Section 4 presents a case study and the SRA resulting from the application of our approach. Finally, Section 5 presents our conclusions and future work.

2 Related Work

As shown later, there are multiple reference architectures for CPS environments that have been proposed by both industry and the scientific community, but not many architectures focus on security. Moreover, some of the proposals are not specifically focused on CPS but are related to this topic, since they contain parts of this kind of environments, such as IoT environments or smart factories. In this section of the paper, a Systematic Review (SR) [Kitchenham, 2004, Kitchenham and Charters, 2007] of the existing literature related to research in the field of *Security Reference Architecture for Cyber-Physical Systems*, which has been adapted to the field of information systems [Barat et al., 2017, Dresch et al., 2015, Marques et al., 2012], will be carried out in order to analyze the most relevant work on security architectures for CPS.

The most relevant proposals for industrial CPS architectures principally RAMI 4.0, IIRA and 5C. RAMI 4.0 [VID/VDE, 2015] is probably the best-known architecture with regard to expressing CPS environments. This proposal shows the peculiarities of this type of system by means of a division into six layers with different levels of abstraction, ranging from the business layer to the assets of which the CPS is composed. Although it includes some security issues, it does not focus specifically on security and cannot, therefore, be considered an SRA. IIRA (Industrial Internet Reference Architecture) [Shi-Wan et al., 2017] is a model that defines the structure of the Industrial Internet of Things (IIoT). IIRA has a structure comprising four layers and five domains, which are based on the study of different use cases. The result is an architecture with a high level of abstraction that does not emphasize security. With regard to 5C [Lee et al., 2015], it is an architecture that defines five levels. This organization is based on the provision of different functions, from the connection of the sensors and actuators to the configuration of the CPS. 5C places no emphasis on data security or environmental safety. A more in-depth analysis of these and other industrial proposals is carried out in [Bunte et al., 2019, Moghaddam et al., 2018]. When comparing the different proposals, one aspect to consider is whether any of these three important architectures are part of any proposal in the studies analyzed in the systematic review.

The first step in any systematic review consists of establishing the object of the question, which is, in this case, that of locating work focused on the development of SRAs in order to permit their application in CPS, Industrial IoT (IIoT) or IoT. This question was defined as follows: *"What work has been carried out to develop Security Reference Architecture for Cyber-Physical Systems?"*. The related words and concepts that were used to formulate this question and that were used during the execution of the review are the following: *"RA: Reference Architecture; SRA: Security Reference Architecture; CPS: Cyber-Physical Systems; IIoT: Industrial IoT, IoT: Internet of Things"*.

In the context of the planned systematic review, it will be noted that several existing proposals on SRAs were found, with particular emphasis on those oriented toward CPS. The most important were extracted and subsequently analyzed and compared.

A comparative framework is, therefore, provided in order to enable the appropriate positioning of new research activities as regards SRAs oriented toward CPS.

The review method was based on the research protocol, and in this phase we, therefore, selected the sources that would be used to carry out the execution of the search for primary studies. The search for primary studies was carried out using web search engines, electronic databases and manual searches, such as searches in a specific journal/conference/book/publication or in research publications recommended by experts in the field.

The search string employed, which was adapted to each specific source search engines, was: [*“Security Reference Architecture” OR “Reference Architecture” AND SRA OR RA AND “Cyber-Physical Systems” OR “Industrial IoT” OR “Internet of Things” AND CPS OR IIoT OR IoT*]. We have limited the search to papers published in the last 10 years (period 2010-2020). Inclusion and exclusion criteria should be based on the Research Question. The inclusion criterion employed herein was mainly an analysis of the title, keywords and the abstract of each document. This criterion was used to locate and eliminate most of the results obtained, which did not contribute to the security reference architecture in the field of CPS.

The exclusion criterion acted on the subset of relevant studies obtained and allowed us to obtain the set of primary studies. In this phase, we focused mainly on reading and analyzing the abstract of the document and its conclusions, and whenever we were unable to identify it as a primary study, we carried out a more in-depth reading of the work in order to verify its relevance for the review. The search carried out using the first chain made it possible to obtain 3,580 papers, 3,181 of which were eliminated because they were not considered to have an impact or because the subject matter was dealt with in a secondary manner. The remaining 399 papers were analyzed, after which 30 of a higher quality or whose content was closer to the subject matter were selected. These were eventually narrowed down to 27 owing to the fact that the subject matter in three of them was duplicated.

Some of the papers eventually obtained are studies that focus on analyzing the problems existing in the current SRA models without proposing new models, and are merely based on the analysis of the current proposals. Some of these final papers focus directly on IoT models [Fortino et al., 2020, Torkaman and Seyyedi, 2016, Guth et al., 2017], while others have analyzed the main problems currently existing in the architectures for CPS (RAMI 4.0, IIRA, IoT-A, etc.), highlighting the need for further progress in their development [Yli-Ojanperä et al., 2019, Butun, 2020, Bader et al., 2019, Weyrich and Ebert, 2016, Monteiro et al., 2018, Weber et al., 2017, Qin et al., 2020, Nowakowski et al., 2018].

Another second group focuses on the development of partial proposals for the development of new SRA models, analyzing the issues of different approaches. Some researchers have proposed new SRA models but focused on IoT and not on industrial environments [Guth et al., 2017, Zibuschka et al., 2019, Dimitrakos, 2018, Syed and Fernandez, 2018, Sabrina, 2019a, Sabrina, 2019b, Addo et al., 2014]. Other researchers have preferred to propose the development of new models based on existing architectures for CPS, in particular RAMI 4.0, IIRA and 5C [Hansch et al., 2019a, Hansch et al., 2019b, Sharpe et al., 2019, Ma et al., 2017, Moghaddam et al., 2018, Baloyi and Kotzé, 2018, Ahmadi et al., 2018]. Finally, another group of researchers has attempted to develop partial proposals for SRA without taking existing architectures into account [Craggs et al., 2019, Romero and Fernandez, 2017, Koziolok et al., 2018, Koziolok et al., 2020, ur Rehman et al., 2018].

The analysis of each of the papers made it possible to create a table summarizing

Papers	Approach	Based on	Domain	Oriented toward	Case study
[Guth et al., 2017] [Fortino et al., 2020] [Torkaman and Seyyedi, 2016]	Generic	–	IoT	analyze SRA problems	NO
[Weyrich and Ebert, 2016]	Generic	IIRA	IoT/IIoT	analyze SRA problems	NO
[Yli-Ojanperä et al., 2019] [Monteiro et al., 2018] [Weber et al., 2017] [Qin et al., 2020]	Generic	RAMI4.0 IIRA	CPS/IIoT	analyze SRA problems	NO
[Bader et al., 2019]	Generic	IIRA	CPS/IIoT	analyze SRA problems	NO
[Nowakowski et al., 2018]	Generic	–	CPS/IIoT	analyze SRA problems	NO
[Blouin and Borde, 2020]	Generic	–	Generic	language specification	YES
[Zibuschka et al., 2019]	Own Model	–	IoT	simplicity and privacy	NO
[Dimitrakos, 2018]	Own Model	–	IoT	life cycle of security controls	NO
[Syed and Fernandez, 2018]	Own Model	–	Generic	containers	NO
[Sabrina, 2019a] [Sabrina, 2019b]	Own Model	–	IoT	use of Blockchain (Ethereum)	NO
[Addo et al., 2014]	Own Model	–	IoT	user reliability	YES
[Li et al., 2020]	Own Model	–	CPS/IIoT	five-tier reference, reuse	YES
[Craggs et al., 2019]	Own Model	–	CPS/IIoT	requirements, attacks vulnerabilities, machine learning	NO
[Romero and Fernandez, 2017]	Own Model	–	CPS/IIoT	interaction between cyber and physical systems	NO
[Koziolek et al., 2018] [Koziolek et al., 2020]	Own Model	–	CPS/IIoT	best practices	NO
[ur Rehman et al., 2018]	Own Model	–	CPS/IIoT	authentication of sensor networks	YES
[Hansch et al., 2019a] [Hansch et al., 2019b]	Own Model	RAMI4.0	CPS/IIoT	communication security requirements for I4.0	YES
[Sharpe et al., 2019]	Own Model	RAMI4.0	CPS/IIoT	representation of security and humans with systems	YES
[Ma et al., 2017]	Own Model	RAMI4.0	CPS/IIoT	models of layered architecture	YES
[Moghaddam et al., 2018]	Own Model	RAMI4.0 IIRA	CPS/IIoT	services	NO
[Baloyi and Kotzé, 2018]	Own Model	RAMI4.0 IIRA	CPS/IIoT	data privacy compliance	NO
[Ahmadi et al., 2018]	Own Model	5C	CPS/IIoT	components for manufacturing based standards	NO
SRA-CPS	Own Model	RAMI4.0 IIRA 5C	CPS	security requirements security patterns	YES

Table 1: Comparison of approaches of the Systematic Review

their main characteristics: i) Approach: “Generic” refers to the fact that the work studies existing generic models without making any concrete proposals. “Own model” means that the authors propose a new model that attempts to improve the problems identified with the existing proposals; ii) “Based on” indicates whether the work has considered the main architectures for currently existing CPS (IIRA, RAMI4.0 or 5C); iii) “Domain” indicates on which environment the work is focused, whether it is for CPS only, or also for IoT or an industrial environment (IIoT), or simply a generic IT environment, or several of them; iv) “Oriented toward” represents the main features to be highlighted in each of the papers analyzed, indicating those that deal specifically with safety and security, and v) “Case Study” indicates whether or not it has been tested or not in a practical manner through the use of case studies, uses cases or specific scenarios.

As shown in Table 1, of the 27 papers identified during the systematic review, 11 of the more generic studies focused on language specification for generic architectures or on the analysis of the problems associated with SRAs, in particular with regard to their orientation towards Industry 4.0 and new technological requirements. These studies

do not taken into account practical validation or case studies, and six of them have considered some of the methodologies associated with Industry 4.0 (IIRA or RAMI4.0).

The remaining papers suggest that there is a need to propose new SRA models, with different orientations. Of these papers, we can distinguish a first group of about 13, which propose new models without taking into account the existing methodologies associated with Industry 4.0. Some of them focus on IoT or generic technologies, while others focus on CPS technologies and industrial environments (IIoT). It is worth noting that in only two out of the ten research works are the results validated through the use of practical cases. The second group of papers, which is made up of seven research projects, focus on developing new models, although based on existing Industry 4.0 methodologies (IIRA, RAMI4.0 or 5C), and four of them carry out validations by means of case studies.

Furthermore, it will be noted that the new proposed models have different orientations and that none of them focus on security or are based on security by design through the use of blockchain, containers, best practices, services, etc. They do not, therefore, focus on security as a central element that serves as the main axis for developing secure systems, such as security requirements or security patterns.

As can be seen from the analysis, none of the research works found provide models that take into consideration the methodologies associated with Industry 4.0, and particularly the three main ones (RAMI 4.0, IIRA and 5C), which share a pure orientation toward CPS, carry out a case study in order to validate the results, or develop a model with an orientation toward security patterns and requirements.

All of these drawbacks led to the conception of our proposal, which will focus on the security and safety aspects from the highest layers of our architecture, which is based on the three most important architectures for CPs (RAMI 4.0, IIRA and 5C); we also provide all the technical details in each of the layers, in addition to the relationships between the components. Our proposal is focused on safety and security requirements in the use of security patterns that will serve as a guide during the whole development process of this kind of system, thus making them more secure, from the outset.

3 SRA for CPS

As stated in the introductory section, an SRA can be defined as an abstract framework that shows the main components of a system while simultaneously emphasizing the understanding of security concepts, such as vulnerabilities or misuse patterns. After identifying the gaps shown in the previous section, we decided to create our own SRA for CPS. Our proposal is based on the main standards or frameworks that define an architecture for CPS, such as RAMI 4.0 or IIRA. The main difference between our proposal and the others is that we created the SRA by following a security-by-design approach. This, therefore, enables the security needs to be incorporated from the first stages of the life cycle of the system, thus allowing robust designs that include appropriate decisions from the security point of view at all the stages of its construction. We also highlight the importance of defining all the elements that a CPS can contain and how they are related to each other. The relations between the different elements of our architecture are made evident through the use of UML diagrams. The use of this kind of diagram also facilitates the application of security patterns, which are usually described as UML models.

Figure 1 depicts the main components of our SRA. As will be noted, our architecture follows a layer structure composed of six different layers that are connected to each other. Moreover, the background of the SRA has a fabric of networks that describes how

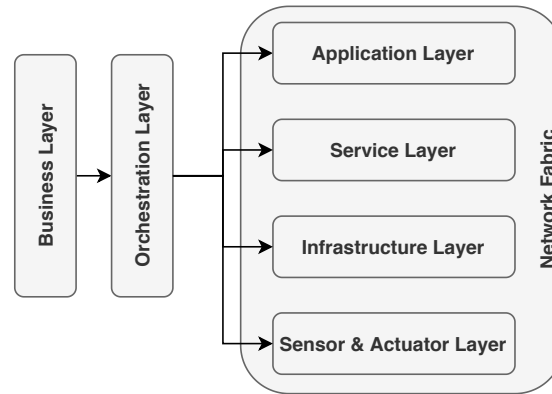


Figure 1: Overview of the SRA for CPS

the different layers communicate with each other. The first two layers of our architecture have a higher level of abstraction than the rest, since their main objective is to perform the governance and management tasks of the CPS architecture implemented, which is why they are connected to the rest of the components of the architecture. In-depth descriptions of all these layers are provided in the following subsections, and an overview of the components and connections between each of the layers is shown in Figure 2.

3.1 Business Layer

The first layer is the business layer. Figure 3 represents the main elements of this component. The main objective of the business layer is to correctly and concisely define the global purpose of the CPS. This CPS goal is usually specified with a high level of abstraction, since it represents the wishes of the company's top management. An example of a CPS objective may be "to provide intelligence and autonomy to an industrial control system". This CPS goal must be aligned with the elements of the organization in which the CPS is to be implemented. These elements include the business policies, the expectation of the company (business goal), how the organization performs its activities (business processes) and what the environment of the organization is (context). All these elements are important, since they should influence the definition of the CPS goal. The realization of a CPS project is not a trivial decision, since it is a complicated system whose implementation may affect different departments of the organization and implies the use of many resources and an important economic cost. The top management must, therefore, be involved in the definition of the CPS goals. The CPS goal defined at this level is divided into more specific requirements in the orchestration layer.

3.2 Orchestration Layer

Once the goal of the CPS has been established, it is necessary to define the different requirements that the CPS must address. This is the main objective of the orchestration layer. This layer also organizes how the requirements are connected to the other components of the architecture; since it is an SRA, we shall focus specifically on the safety and security requirements that the CPS must meet. It is important to explain the

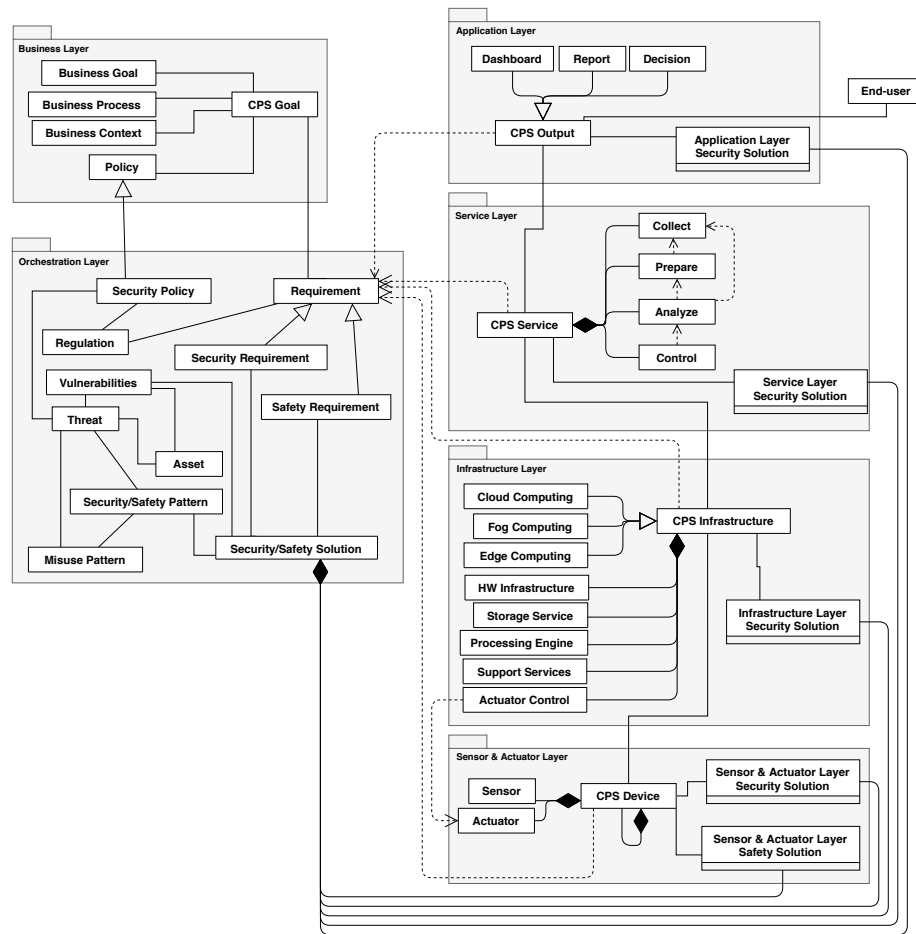


Figure 2: Elements of the Layers of our SRA

difference between safety and security requirements, since a CPS is not only concerned with the security of the data used in the system, but also has a physical part, and it is, therefore, necessary to take the physical safety of both the sensors and actuators, and the stakeholders related to the CPS into account. Figure 4 shows the different elements of the orchestration layer.

These requirements must be aligned with the CPS goals. One of the main elements to consider when defining requirements is the regulation that may affect the context in which the CPS is implemented. A CPS implemented in a medical monitoring system does not, for example, have the same limitations as one implemented in a robotic system for an industrial environment. The legislation will limit the use of the data depending on the sensitivity of the data. These laws, which are intrinsic to the context of the company, must be aligned with the organization's security policies, which must be taken into account when defining the CPS goal.

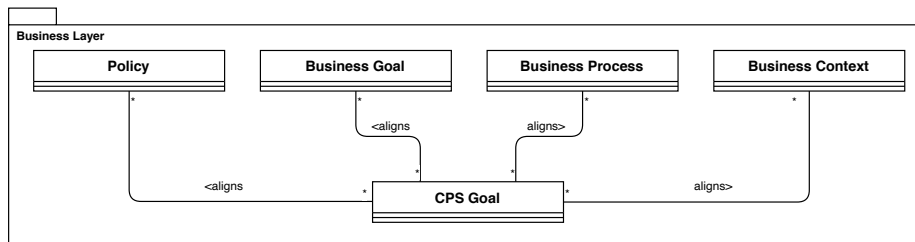


Figure 3: Elements of the Business Layer

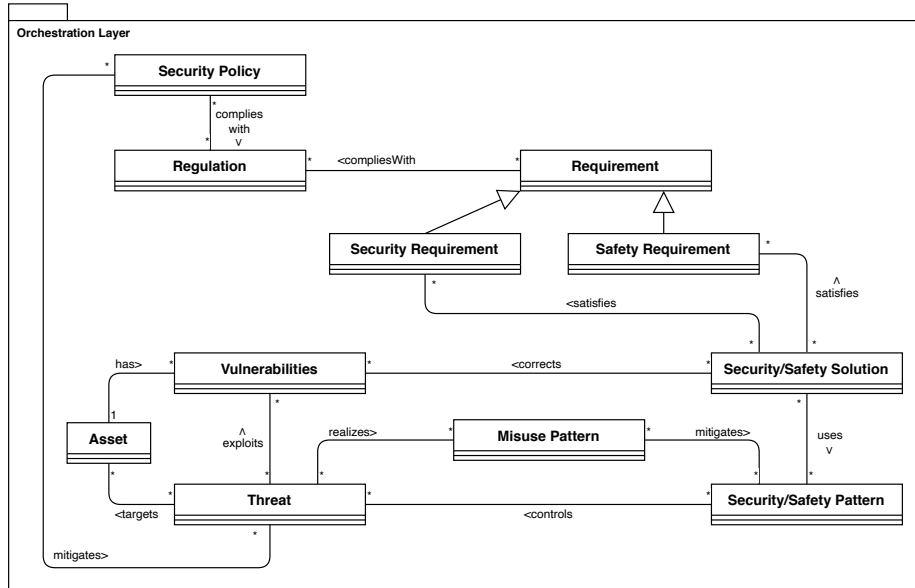


Figure 4: Elements of the Orchestration Layer

Security requirements are related to the ability of the CPS to ensure that all of its processes, mechanisms (both physical and cyber) and services are afforded internal or external protection from unintended and unauthorized access, change, damage, destruction or use. These could be the data anonymity, confidentiality and integrity that must be guaranteed, along with the authentication and authorization mechanisms required in order to prevent unauthorized users (i.e., humans and devices) from accessing the system. Safety requirements can, meanwhile, be interpreted as the ability of the CPS to ensure the absence of catastrophic consequences for the life, health, property or data of CPS stakeholders and their physical environment [Griffon et al., 2017].

These problems are usually addressed through the use of general mechanisms such as access control, risk control, external and internal audits, encryption or ensuring the origin and traceability of data from sensors or other data sources [Ashibani and Mahmoud, 2017, Alguliyev et al., 2018]. These are normally traditional security management techniques that are applicable to any IT system, but which are adapted to meet the inherent characteristics of a CPS.

These safety and security requirements are satisfied by different safety and security solutions, which, at this level, have a high level of abstraction since they will be implemented in a more specific manner in the rest of the layers of the architecture. Since it is defined as being the mechanism used to address a security or safety requirement, it can be concluded that these solutions have the main objective of correcting or addressing system vulnerabilities. At this point, the orchestration layer is constructed from a series of elements that comprise a typical security ontology like those in security methodologies such as ASE [Uzunov et al., 2015]. Vulnerabilities are, therefore, security holes that the different assets of the system have, and which suppose a threat to the system if they are exploited. One way in which to assist in the implementation of these security solutions is through the use of security patterns.

A pattern is a solution to a recurring problem that indicates how to defend against a threat, or set of threats, in a concise and reusable manner [Fernandez B, 2013]. Patterns are abstract solutions that must be tailored to where they are applied. Furthermore, our architecture includes the use of misuse patterns in order to understand how each attack works and to guide the application of the different security patterns that can be used to prevent a threat [Fernandez et al., 2009]. For example, a security requirement indicates the need to keep track of the actions performed on the sensitive data of the CPS; the implementation of this security solution can be guided by the use of the "Logger and Auditor" security pattern.

Finally, it should be noted that there are other types of requirements that are necessary when implementing a CPS, such as performance or quality requirements. However, our architecture has the objective of incorporating security into this type of environment, and we, therefore, focus only on those requirements and security solutions that help to achieve this objective. The following layers define the elements that can be used when implementing a CPS.

3.3 Application Layer

The application layer marks the beginning of the CPS elements, since it is at this particular level that the requirements specified in the previous layer are implemented. The application layer consists specifically of those elements related to the output generated by the CPS. This output can have different formats depending on the business needs (see Figure 5). It is, therefore, possible to display these results by employing dashboards, which allow users to perform interactions with the CPS, such as activating certain actuators. These dashboards can indicate, in real time, the status of the system. It is also possible to show the results in a more traditional manner through reports that explain the actions taken or average levels of certain system indicators. Likewise, it is conceivable that the results may not be displayed visually but may inform the decision as to which actuators should be either activated or deactivated under certain circumstances. The data used and displayed in this layer are the result of executing the different functions of the service layer.

It is important to highlight the fact that in many scenarios it is necessary to have a communication with an end-user that is considered an external agent to the system. This end-user does not have to be a human being but can be an auxiliary system that receives the output data from the CPS as input for its own processes. When accessing these results, it is necessary to have control over what and who accesses the data. Authorization and authentication mechanisms must, therefore, be implemented for this purpose in order to guarantee the security and privacy of the data generated by the CPS. These

mechanisms are the concrete implementation of the security solutions that were defined in the orchestration layer and act as a gateway to the system.

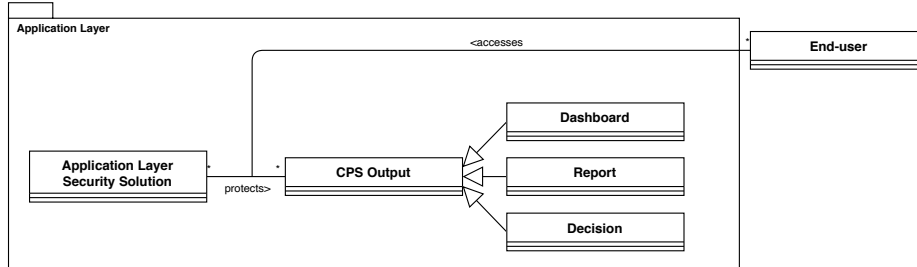


Figure 5: Elements of the Application Layer

3.4 Service Layer

The service layer has the objective of meeting the requirements established in the orchestration layer, including the security requirements. In order to achieve this goal, this layer is composed of different services or activities that can be considered as the SaaS (Software as a Service) layer of a CPS. Figure 6 shows the different services that of which this layer is composed, along with the security solution that must map the security solution from the orchestration layer; for example, the data collected may need to be properly secured by using encryption mechanisms, or an analysis of the data must preserve its privacy.

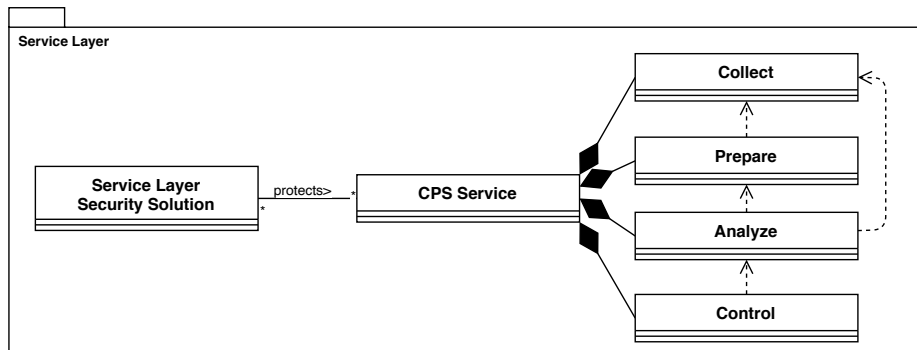


Figure 6: Elements of the Service Layer

These activities (shown in Figure 7) can be considered as the typical data lifecycle in this type of environment. As will be noted in Figure 6, not all the activities can communicate with each other, and there is a sequential order of execution. This implies that one of these activities is not mandatory in a CPS. There are consequently four main activities that can be performed in a typical CPS:

- The collect activity acts as an ETL (Extract, Transform, and Load) process and combines sets of data from different data sources (mostly sensors from the Sensor & Actuator layer) with the objective of unifying them. The data collected in this activity will be used in the following activities.
- The prepare activity has the purpose of validating and cleaning the data. This activity is not mandatory in these kinds of systems, since they usually have real-time needs. Several techniques can be used to prepare the data, such as data wrangling, which is the process of transforming raw data into another format of data that is more suitable.
- The analysis activity processes the data generated by the system in order to obtain valuable information that can help in the decision-making process. This activity is critical and includes the definition of different algorithms and methods with which to ensure the proper functioning of the CPS. In many cases, the insights generated by this activity automatically suppose an activation of different CPS actuators.
- The control activity is crucial in a CPS, since its main purpose is to manage the different sensors and actuators of the environment. The functioning of this activity is based on the insights generated by the analysis activity and on the decisions made by the end-user in the application layer. This activity also monitors the status of the different devices that comprise the CPS.

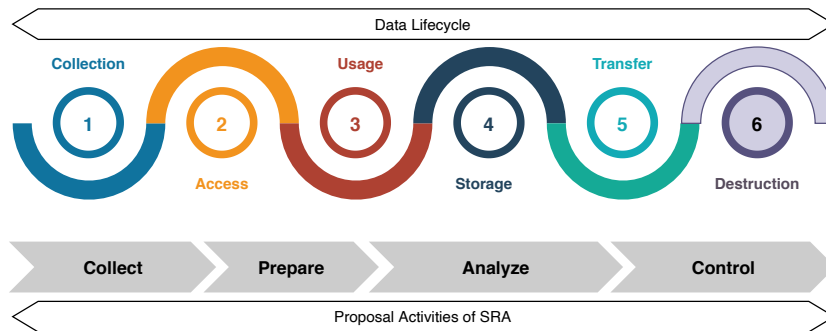


Figure 7: Data Lifecycle vs. proposal activities of our SRA

The data stored and managed in these activities form the basis for the generation of the various reports, dashboards, etc. used in the previous application layer. All of these activities must additionally be supported by the next layer of the architecture: the infrastructure layer.

3.5 Infrastructure Layer

The infrastructure layer has the objective of supporting all the different services and processes provided and executed in the CPS. Figure 8 depicts the main elements of this infrastructure layer. As it can be seen in the figure, there are three main possibilities when implementing a CPS infrastructure: the use of a Cloud Computing solution, a Fog Computing solution, or an Edge Computing solution. All these solutions are well-known

infrastructures, which are not defined in depth herein since it is not within the scope of the work [Casola et al., 2018, Fernandez et al., 2016b]. The decision made regarding the type of infrastructure to be supported by the CPS will depend on the requirements of the system. Security should also be taken into account when making this decision, since in the case of opting for a Cloud solution, security is delegated to the third-party provider of the infrastructure. However, in the case of deciding on a Fog computing solution, security must emphasize enhancing the security of access to stored data. Moreover, if the CPS is implemented through an Edge computing infrastructure, security must emphasize the CPS devices, since most of the actions will be performed on them, such as the security of the network communications between the devices.

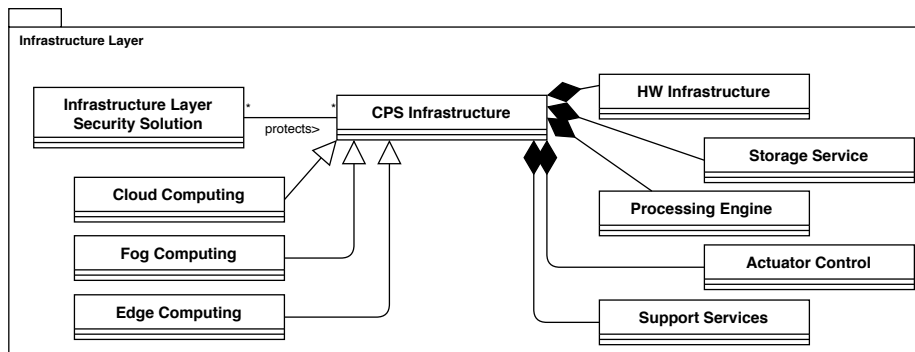


Figure 8: Elements of the Infrastructure Layer

As stated above, the choice of infrastructure will affect the implementation of the components that comprise the CPS architecture. However, this should not affect the elements of the SRA; for example, in the case of selecting an Edge Computing solution, the data analysis service will be performed on the devices of the CPS itself, but this service will continue to be offered to the end-users.

A set of components related to the different functions they provide is also integrated into the CPS infrastructure. First, the hardware infrastructure contains all the different physical resources, such as servers, needed to support the CPS. All the data generated by the CPS, along with data from external data sources that are needed to perform the analysis service, are located in the storage service. There are generally three different ways in which to store data: structured, semi-structured and non-structured. Depending on the data handled by the CPS, it will be necessary to choose the implementation of one or several databases of these types. The purpose of processing engine is to establish the way in which data is analyzed in the CPS. Data can be processed in three ways: i) the batch processing executes different jobs in a sequential mode by writing data on the disk in order for it to be stored between phases; ii) the streaming processing analyzes data in real time, thus making it suitable for applications in which requirements indicate a need for an analysis of the data generated at the present time; iii) and in between these technologies is interactive processing, which allows queries to be performed while the relevant data is still being collected. The actuator control manages the communications with the actuators of the CPS, signifying that when an actuator needs to be activated or deactivated owing to a decision made by the upper layers, this mechanism contacts the

appropriate actuator. Finally, a few support services may need to be implemented in the CPS, such as resource monitoring or orchestration services.

3.6 Sensor & Actuator Layer

The last layer of our architecture is related to the different devices that comprise the CPS. These devices are generally divided into two large groups: on the one hand, the sensors, which obtain real-time data that indicate the state of the CPS or a specific variable, such as temperature or position. The actuators are those devices that cause changes in the CPS owing to actions controlled by the upper layers, such as a sprinkler or a robotic arm. There are, on the other hand, CPS devices that consist of both a sensor and an actuator, such as water pumps with flow sensors. Moreover, some CPS devices may be more complex, and can, therefore, be considered as an aggregation of different devices. Figure 9 depicts the main components of this layer.

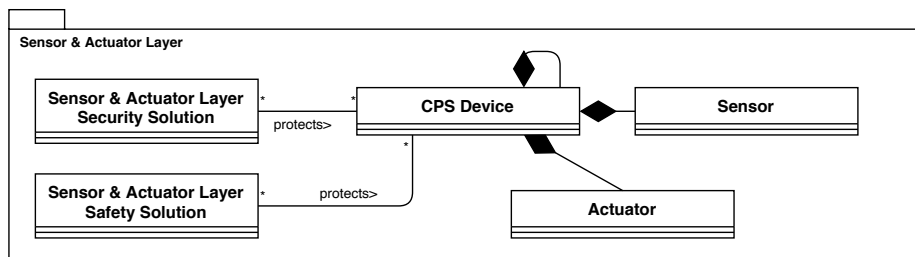


Figure 9: Elements of the Sensor & Actuator Layer

With regard to the security of this layer, it is necessary to point out that there are two levels of security. Firstly, the security of the sensors, which are usually related to the means employed in order to send and receive data; secondly, the data generated by the sensors and the data received by the actuators in order to perform an action. In contrast, the physical safety that was defined in the orchestration layer is implemented here, and this includes any incident that may occur in the physical world and that may affect the operation of both sensors and actuators. This can range from the sabotage of sensors, to the manipulation of the information they read, to possible infrastructure risks such as wildfire, or even the physical safety of the workers operating the CPS.

3.7 Network Fabric

According to the NIST proposal, the network fabric is directly involved in the communications among all the components of a CPS. Many communication protocols for the different levels that provide connectivity could be used in order to connect the different links between the different layers of our architecture. Communication requirements vary widely among the different types of CPS networks, depending on their purpose and resource constraints.

The communication protocols within CPS ecosystems can be either wireless or wireline-based. There is a plethora of wireless communication protocols, including

short-range radio protocols such as ZigBee, Bluetooth/Bluetooth Low Energy (BLE), Wi-Fi/Wi-Fi HaLow, Near Field Communication (NFC) or Radio Frequency Identification (RFID), or mobile networks and longer-range radio protocols, such as Lo-RaWAN, SigFox NarrowBand-IoT (NB-IoT), or LTE-M. Each of them is defined in its own standard. For example ZigBee and ZigBee 3.0 are based on the IEEE 802.15.4 standard. Wired communication protocols and links, such as Ethernet, USB, SPI, MIPI and I2C, among others, also provide access to the devices. Moreover, it is worth high-lighting that CPS communications also support non-IP based protocols, such as SMS, LiDar, Radar, etc.

The leading communication technologies used in the CPS world are IEEE 802.15.4, low power WiFi, 6LoWPAN, RFID, NFC, Sigfox, LoraWAN, and other proprietary protocols for wireless networks.

The Sensor and Actuator layer is composed of devices that are inherently re-source constrained, such as limited processing speed, storage capacity, and communication bandwidth, signifying that they can use protocols such as IEEE 802.15.4 (Zigbee), and 801.15.1 (Bluetooth). These protocols are generally characterized by lower bandwidth, low energy consumption, and a short range. These devices generate large amounts of information that flow to higher layers to be stored, processed and analyzed. They employ many technologies, such as databases, cloud computing, and big data processing modules.

The upper layers require communication protocols with longer ranges, which are in the local area network (LAN) class, such as IEEE 802.11 (WiFi). Robust and efficient routing protocols need to be designed for and adapted to CPS in order to provide efficient and robust communication in this highly variable and dynamic environment.

TCP is not a good option for communication in low power environments, as it has large overheads owing to the fact that it is a connection-oriented protocol [Zaidan et al., 2018]. UDP is, therefore, preferred because it is a connection less protocol and has low overheads.

The application layer is responsible for data formatting and presentation. The application layer on the Internet is typically based on HTTP. However, HTTP is not suitable in resource constrained environments. Many alternate protocols have been developed for these environments, such as CoAP (Constrained Application Protocol) and MQTT (Message Queue Telemetry Transport).

4 Case Study

In order to facilitate the understanding of our SRA proposal for CPS, we created a case study by following the components recommended by the architecture described above. This application of our architecture to a real scenario allowed us to both refine the SRA and test the usefulness of the proposal when building this type of systems. In this section, we explain the different elements of this case study and how they can be mapped onto the different components of our SRA.

As shown in Figure 10, our case study deals with a CPS system for a hydroponic crop, involving both hardware (sensors, actuators and controllers) and software components (system for storage, dashboard, monitoring and decision making with Big Data technology). This type of agriculture has become increasingly popular in recent times, especially in drier areas, owing to its lower water demand, the use of nutrients rather than soil to produce plant growth, and the smaller surface needed to provide a financial benefit. The problem that arises with this technique is, however, that it requires more

attention from the operator, i.e., the farmer. To overcome this problem, our research group created a prototype solution which is based on CPS.

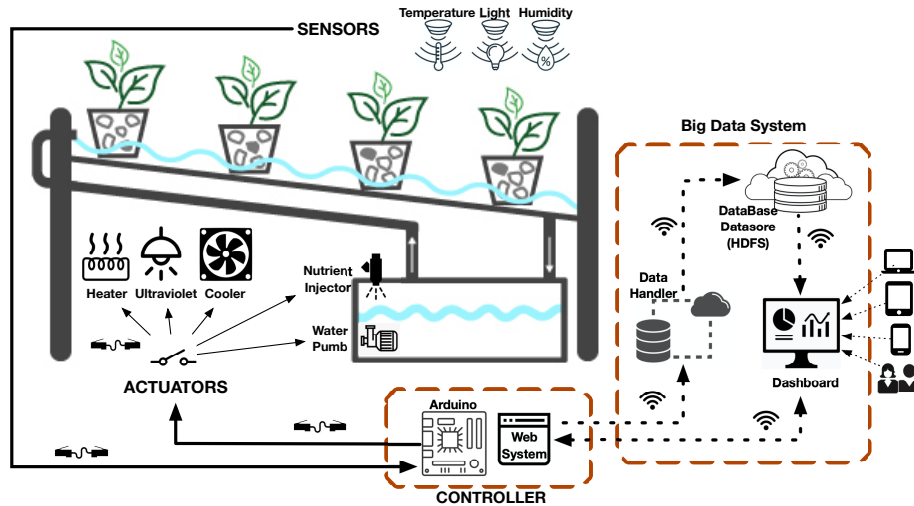


Figure 10: Hydroponic crop for the case study

The hydroponic crop is controlled via a set of sensors that measure the temperature, light and humidity of the environment. A set of actuators, such as a heater, a cooler, an ultraviolet injector and a water pump, are activated or deactivated by commands sent from the controller, which is an Arduino device linked to a web service. In addition to the physical part, the controller is also connected to a visualization and control system that makes use of Big Data technologies: we have deployed a dashboard in order to be able to control the hydroponic crop in real time and to consult statistics, and a data handler so as to process the sensor data, which is received from the controller and stored in the database or datastore (HDFS and HBASE, respectively). The data generated by the sensors is processed in near real time using Apache Spark algorithms, and the connection with the controller is wireless. In the following subsection, we compare the solution proposed for the hydroponic crop with the components of our own SRA for CPS.

4.1 Mapping between the SRA for CPS and the Case Study

This subsection presents a discussion of the similarities between our proposal and the case study. To this end, we carried out a comparison of the elements used to control the hydroponic crop with the architectural components of our own proposal. At this point, it is important to highlight that some of the components of our SRA are not mandatory, since one of the main objectives of the architecture is for it to be sufficiently abstract to cover any kind of CPS scenario.

The first two layers to be considered are, therefore, the business and orchestration layers. These are used to define how the system will be implemented. In this case, as it is a prototype created for purely scientific purposes, the business layer is somewhat diluted,

Security requirement	Security pattern
RQ1. Data must be encrypted	Symmetric encryption [Fernandez B, 2013]
RQ2. Manage access to the system	Authenticator [Fernandez B, 2013]
RQ3. Manage privileges over the system	Role-based access control [Fernandez B, 2013]
RQ4. Vulnerabilities management	Undeveloped pattern
RQ5. Log control	Security logger/Auditor [Fernandez B, 2013]
RQ6. Provide network security	Transport Layer Security [Fernandez B, 2013]
RQ7. Prevent sensors and actuators from being subject to sabotage	Hardware IoT [Schuß et al., 2018]

Table 2: Security requirements of the hydroponic crop and the security patterns used to address them

although it can be stated that the objective of the CPS is “the creation of a hydroponic crop from scratch in order to study the typical elements of CPS, along with its specific security needs”. With regard to the orchestration layer, it is mainly in charge of defining the requirements that must be satisfied by the CPS. In this case, as we are dealing with an SRA we shall, therefore, focus on those requirements that are related to the security of the system and the safety of the different devices. However, although they are not within the scope of this sub-section, it is clear that the system has a number of functional requirements that must be met, such as constantly controlling the optimal amount of light that the plants should receive. In addition to defining the requirements, this layer oversees the establishment of possible security solutions with which to satisfy these requirements, which attempt to control the different vulnerabilities of the system. If possible, security patterns are used to facilitate the definition and implementation of these security solutions. Table 2, therefore, lists the main security requirements of the system, along with the security patterns that can be used to address these issues.

The next layer of our architecture is the application layer, in which the data is consumed by the end-users (or by the CPS elements themselves) through different functionalities or applications. In the case of the hydroponic crop, there is, therefore, a dashboard with which to represent the CPS status in real-time. This dashboard, which uses Dash, makes it possible to control the different actuators of the system, including programming their behavior in accordance with sensor readings or other needs. In order to access the dashboard and to configure the actions of the actuators, the end user must first be authenticated and authorized. Note also that all the actions performed by each user must be stored in a log so as to guarantee the traceability of the system.

Next is the service layer, which, as its name suggests, provides the different services of the CPS. As explained above, the first service is data collection, which, in this case study, is the storage of the data generated by the sensors and the actuators in an HBASE database. This data may, on some occasions, be encrypted. The next service is the preparation of the data. This service is not necessary in our case study, since the data generated are consumed in real time and are, therefore, managed automatically without the need for any filtering. The data generated by the sensors, and the data stored from the execution of the actuators, are analyzed in real time by using the Pandas library supported by Apache Spark. This has the main purpose of showing the current state of the hydroponic crop and enabling the operator to make different decisions as regards modifying the state of the actuators. This control of the actuators is the last of the services performed in our case study: in this scenario, the control service is managed by means of the configurations defined in the dashboard of the application layer.

With regard to the infrastructure layer, in this case we opted for a cloud computing solution, in which the data is stored and processed in an AWS solution, thus allowing the hardware management to be outsourced and to be made it transparent to the user. When

determining the processing engine, we specifically opted for a solution based on Apache Spark that processes both real-time and stored data. Moreover, the data is stored in an HDFS. All these elements are managed by an Amazon EMR Platform from AWS, and the direct management of the sensors and actuators is carried out by an Arduino device.

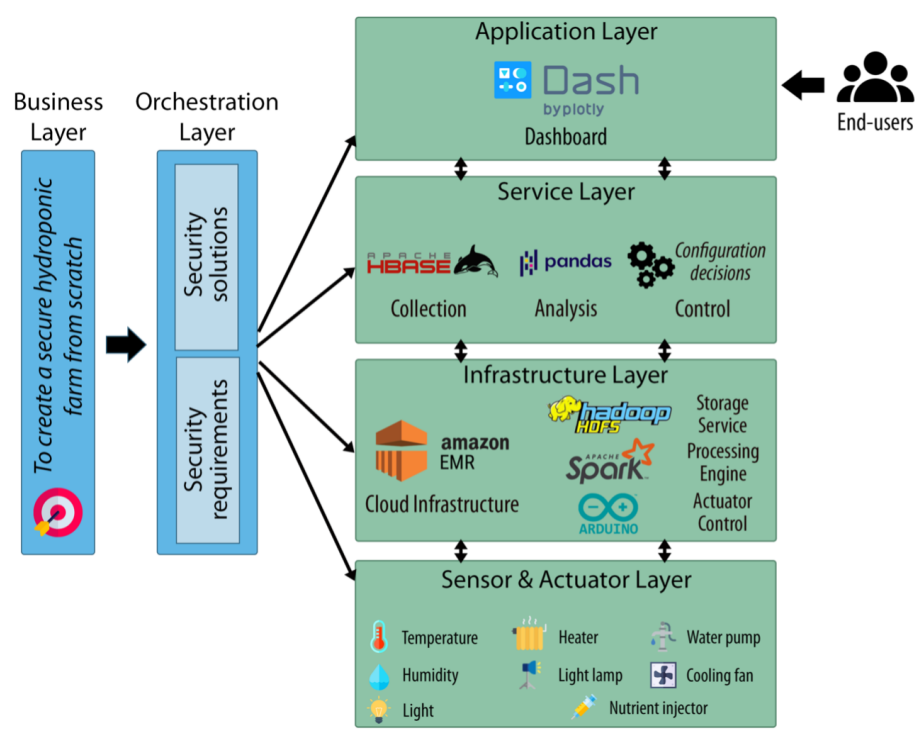


Figure 11: Summary of the main components of the SRA and the technologies used in the case study

These sensors and actuators make up the last layer of our architecture. In the case study, the hydroponic crop is monitored by humidity, light and temperature sensors, while the actuators are ultraviolet lamps, heaters, cooling fans, water pumps and nutrient injectors. As can be seen, there is a close relationship between some of the actuators and the sensors, as in the case of the light sensors and the ultraviolet lamps. However, other actuators are more independent and their operation is usually programmed as a routine or through an analysis based on past experience, as is the case of the nutrient injector. The last main component of our architecture is the network fabric, which is responsible for ensuring communication between the other components of the SRA. In the case study, this connectivity is achieved mainly via WiFi connections, since the sensors and actuators are connected directly to the Arduino device. This device oversees the sending and receiving of HTTP requests between the AWS servers, in which the analysis and consumption of the information generated by the hydroponic crop is performed.

Finally, Figure 11 shows a summary scheme of how the different components of

our SRA correspond to the different elements present in the hydroponic crop. As can be seen, our architecture is able to cover the complete scenario from its conception to the definition of its components. The SRA, therefore, provides developers with a framework in which to build secure CPS from scratch, and facilitates their work through the abstract definition of the different elements that should be part of this type of environment. It will then be the responsibility of the developer to instantiate and understand each of the components of the architecture and to determine how they can help them to meet the given requirements of their scenario.

5 Conclusions and Future Work

A Security Reference Architecture (SRA) is a key element that, together with the appropriate methods and techniques, helps developers by providing them with a guide that will allow them to consider and identify security requirements, mechanisms and solutions from a high level of abstraction. In this paper, we present our proposal for a specific SRA for CPS environments. This has been done by considering the most widely accepted proposals made by both the industry and the scientific community. These proposals usually lack detail as to the specific components of which each of the layers of the architecture is composed. An SRA can be a very useful tool, since it allows the identification and definition of the key elements needed to build a CPS. The SRA presented in this paper can be used as a guide for stakeholders when creating a CPS from scratch.

Our SRA is defined by means of UML class diagrams with the aim of improving the understanding of the different components that make up a CPS and how they relate to each other in a more precise way. Moreover, the use of UML diagrams enables the application of different security and safety patterns that can be used to facilitate the implementation of security mechanisms. Our SRA is, therefore, composed of six different layers plus a network fabric that represent the main elements of a CPS. These layers in turn represent different levels of abstraction, from the business goals of the company to the different actuators of the CPS.

In order to show the practical application of our proposal, we have applied our SRA to a laboratory case study for the construction of a secure CPS environment, specifically a hydroponic crop, which is introduced in this paper.

With regard to future work, we intend to apply our proposal to other CPS integrated into industrial exploitations. Moreover, we are working on the creation and adaptation of different security and safety patterns specific to this type of ecosystem. We are also interested in the process that defines the main steps needed to create a secure CPS from the phase of the analysis and definition of its security requirements to its secure operation; this process will be based upon the SRA presented in this paper, owing to the definition it provides for the different elements of this type of environment. In the next phases of our SRA, we are additionally defining a set of security requirements for CPS environments by creating a metamodel that will help define the requirements and associated patterns for the subsequent analysis and diagnosis of the security configurations and solutions resulting from these requirements.

Acknowledgements

This work was funded by the ECLIPSE project (RTI2018-094283-B-C31 funded by “Ministerio de Economía y Competitividad and the Fondo Europeo de Desarrollo Regional

FEDER”), the GENESIS project (SBPLY-17-180501-000202 funded by ”Consejería de Educación, Cultura y Deportes de la Dirección General de Universidades, Investigación e Innovación de la JCCM”), and the Programa Operativo Regional FEDER 2014/2020.

References

- [Addo et al., 2014] Addo, I. D., Ahamed, S. I., Yau, S. S., and Buduru, A. (2014). A reference architecture for improving security and privacy in internet of things applications. In *Proceedings - 2014 IEEE 3rd International Conference on Mobile Services, MS 2014*, pages 108–115.
- [Ahmadi et al., 2018] Ahmadi, A., Cherifi, C., Cheutet, V., and Ouzrout, Y. (2018). A review of CPS 5 components architecture for manufacturing based on standards. In *International Conference on Software, Knowledge Information, Industrial Management and Applications, SKIMA*, volume 2017-December, pages 1–6.
- [Alguliyev et al., 2018] Alguliyev, R., Imamverdiyev, Y., and Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry*, 100:212–223.
- [Alur, 2015] Alur, R. (2015). *Principles of cyber-physical systems*. MIT Press.
- [Ashibani and Mahmoud, 2017] Ashibani, Y. and Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, 68:81–97.
- [Avgeriou, 2003] Avgeriou, P. (2003). Describing, Instantiating and Evaluating a Reference Architecture: A Case Study. Technical report.
- [Bader et al., 2019] Bader, S. R., Maleshkova, M., and Lohmann, S. (2019). Structuring reference architectures for the industrial Internet of Things. *Future Internet*, 11(7):151.
- [Baloyi and Kotzé, 2018] Baloyi, N. and Kotzé, P. (2018). A data privacy model based on internet of things and cyber-physical systems reference architectures. In *ACM International Conference Proceeding Series*.
- [Banerjee et al., 2011] Banerjee, A., Venkatasubramanian, K. K., Mukherjee, T., and Gupta, S. K. S. (2011). Ensuring safety, security, and sustainability of mission-critical cyber-physical systems. *Proceedings of the IEEE*, 100(1):283–299.
- [Barat et al., 2017] Barat, S., Clark, T., Barn, B., and Kulkarni, V. (2017). A model-based approach to systematic review of research literature. In *ACM International Conference Proceeding Series*, pages 15–25.
- [Blouin and Borde, 2020] Blouin, D. and Borde, E. (2020). Aadl: A language to specify the architecture of cyber-physical systems. In *Foundations of Multi-Paradigm Modelling for Cyber-Physical Systems*, pages 209–258. Springer.
- [Brewer, 2013] Brewer, T. (2013). Introduction in Proceedings of the Cybersecurity in Cyber-Physical Systems Workshop, April 23-24, 2012. Gaithersburg, MD. National Institute of Standards and Technology.
- [Bunte et al., 2019] Bunte, A., Fischbach, A., Strohschein, J., Bartz-Beielstein, T., Faeskorn-Woyke, H., and Niggemann, O. (2019). Evaluation of Cognitive Architectures for Cyber-Physical Production Systems. In *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, volume 2019-September.
- [Butun, 2020] Butun, I. (2020). *Industrial IoT*. Springer.
- [Casola et al., 2018] Casola, V., De Benedictis, A., Rak, M., and Villano, U. (2018). Security-by-design in multi-cloud applications: An optimization approach. *Information Sciences*, 454:344–362.
- [Cheng et al., 2019] Cheng, L., Yu, T., Jiang, H., Shi, S., Tan, Z., and Zhang, Z. (2019). Energy internet access equipment integrating cyber-physical systems: Concepts, key technologies, system development, and application prospects. *IEEE Access*, 7:23127–23148.

- [Craggs et al., 2019] Craggs, B., Rashid, A., Hankin, C., Antrobus, R., Serban, O., and Thapen, N. (2019). A reference architecture for IIoT and industrial control systems testbeds.
- [Das et al., 2012] Das, S. K., Kant, K., and Zhang, N. (2012). *Handbook on Securing Cyber-Physical Critical Infrastructure*. Elsevier.
- [Dimitrakos, 2018] Dimitrakos, T. (2018). How to develop a security controls oriented reference architecture for cloud, IoT and SDN/NFV platforms. In Gal-Oz, N. and Lewis, P. R., editors, *IFIP Advances in Information and Communication Technology*, volume 528, pages 1–14, Cham. Springer International Publishing.
- [Dresch et al., 2015] Dresch, A., Lacerda, D. P., Antunes Jr, J. A. V., Dresch, A., Lacerda, D. P., and Antunes, J. A. V. (2015). Systematic Literature Review. In *Design Science Research*, chapter Chapter 7, pages 129–158. Springer International Publishing, Cham.
- [European Commission, 2013] European Commission (2013). Cyber-Physical Systems: Uplifting Europe's Innovation Capacity. Technical report, Brussels.
- [Fabian et al., 2010] Fabian, B., Gürses, S., Heisel, M., Santen, T., and Schmidt, H. (2010). A comparison of security requirements engineering methods. *Requirements engineering*, 15(1):7–40.
- [Fernandez et al., 2016a] Fernandez, E., Yoshioka, N., Washizaki, H., and Syed, M. (2016a). Modeling and Security in Cloud Ecosystems. *Future Internet*, 8(4):13.
- [Fernandez et al., 2016b] Fernandez, E. B., Monge, R., and Hashizume, K. (2016b). Building a security reference architecture for cloud systems. *Requirements Engineering*, 21(2):225–249.
- [Fernandez et al., 2009] Fernandez, E. B., Yoshioka, N., and Washizaki, H. (2009). Modeling misuse patterns. In *2009 International Conference on Availability, Reliability and Security*, pages 566–571. IEEE.
- [Fernandez B, 2013] Fernandez B, E. (2013). *Security patterns in practice: designing secure architectures using software patterns*. John Wiley & Sons.
- [Fortino et al., 2020] Fortino, G., Fotia, L., Messina, F., Rosaci, D., and Sarné, G. M. (2020). Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges. *IEEE Access*, 8:60117–60125.
- [Frazzon et al., 2013] Frazzon, E. M., Hartmann, J., Makuschewitz, T., and Scholz-Reiter, B. (2013). Towards socio-cyber-physical systems in production networks. *Procedia CIRP*, 7:49–54.
- [Griffor et al., 2017] Griffor, E., Wollman, D., and Greer, C. (2017). Framework for Cyber-Physical Systems: Volume 1, Overview. Technical Report June, National Institute of Standards and Technology, Gaithersburg, MD.
- [Guth et al., 2017] Guth, J., Breitenbucher, U., Falkenthal, M., Leymann, F., and Reinfurt, L. (2017). Comparison of IoT platform architectures: A field study based on a reference architecture. In *2016 Cloudification of the Internet of Things, CIIoT 2016*, pages 1–6.
- [Hansch et al., 2019a] Hansch, G., Schneider, P., and Brost, G. S. (2019a). Deriving impact-driven security requirements and monitoring measures for industrial IoT.
- [Hansch et al., 2019b] Hansch, G., Schneider, P., Fischer, K., and Böttinger, K. (2019b). A Unified Architecture for Industrial IoT Security Requirements in Open Platform Communications. In *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, volume 2019-September, pages 325–332.
- [Haque et al., 2014] Haque, S. A., Aziz, S. M., and Rahman, M. (2014). Review of cyber-physical system in healthcare. *International Journal of Distributed Sensor Networks*, 2014(4):217415.
- [Horowitz and Pierce, 2013] Horowitz, B. M. and Pierce, K. M. (2013). The integration of diversely redundant designs, dynamic system models, and state estimation technology to the cyber security of physical systems. In NIST, editor, *Systems Engineering*, volume 16, pages 401–412. NISTIR 7916.

- [Jara et al., 2014] Jara, A. J., Genoud, D., and Bocchi, Y. (2014). Big data for cyber physical systems an analysis of challenges, solutions and opportunities. In *Proceedings - 2014 8th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2014*, pages 376–380. IEEE.
- [Kim and Kumar, 2012] Kim, K. D. and Kumar, P. R. (2012). Cyber-physical systems: A perspective at the centennial. *Proceedings of the IEEE*, 100(SPL CONTENT):1287–1308.
- [Kitchenham, 2004] Kitchenham, B. (2004). Procedures for Performing Systematic Reviews, Version 1.0. *Empirical Software Engineering*, 33(2004):1–26.
- [Kitchenham and Charters, 2007] Kitchenham, B. and Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering.
- [Konstantinou et al., 2015] Konstantinou, C., Maniatakos, M., Saqib, F., Hu, S., Plusquellic, J., and Jin, Y. (2015). Cyber-physical systems: A security perspective. In *2015 20th IEEE European Test Symposium (ETS)*, pages 1–8. IEEE.
- [Koziolok et al., 2018] Koziolok, H., Burger, A., and Doppelhamer, J. (2018). Self-Commissioning Industrial IoT-Systems in Process Automation: A Reference Architecture. In *Proceedings - 2018 IEEE 15th International Conference on Software Architecture, ICSA 2018*, pages 196–205.
- [Koziolok et al., 2020] Koziolok, H., Burger, A., Platenius-Mohr, M., Rückert, J., Mendoza, F., and Braun, R. (2020). Automated industrial IoT-device integration using the OpenPnP reference architecture. *Software - Practice and Experience*, 50(3):246–274.
- [Krco et al., 2014] Krco, S., Pokric, B., and Carrez, F. (2014). Designing IoT architecture(s): A European perspective. In *2014 IEEE World Forum on Internet of Things, WF-IoT 2014*, pages 79–84. IEEE.
- [Lee, 2015] Lee, E. A. (2015). The past, present and future of cyber-physical systems: A focus on models.
- [Lee et al., 2015] Lee, J., Bagheri, B., and Kao, H. A. (2015). A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters*, 3:18–23.
- [Lee et al., 2013] Lee, J., Lapira, E., Bagheri, B., and an Kao, H. (2013). Recent advances and trends in predictive manufacturing systems in big data environment. *Manufacturing Letters*, 1(1):38–41.
- [Li et al., 2020] Li, N., Liu, K., Chen, Z., and Jiao, W. (2020). Environmental-perception modeling and reference architecture for cyber physical systems. *IEEE Access*, 8:200322–200337.
- [Liu et al., 2018] Liu, Z., Wang, Z., Ren, Y., Feng, Q., Fan, D., and Zuo, Z. (2018). A city medical resources distribution optimization platform based on cyber physical systems (cps). In *2018 International Conference on Sensing, Diagnostics, Prognostics, and Control (SDPC)*, pages 269–273.
- [Ma et al., 2017] Ma, Z., Hudic, A., Shaaban, A., and Plosz, S. (2017). Security viewpoint in a reference architecture model for cyber-physical production systems. In *Proceedings - 2nd IEEE European Symposium on Security and Privacy Workshops, EuroS and PW 2017*, pages 153–159.
- [Maleh, 2020] Maleh, Y. (2020). *Machine Learning Techniques for IoT Intrusions Detection in Aerospace Cyber-Physical Systems*, pages 205–232. Springer International Publishing, Cham.
- [Marques et al., 2012] Marques, A. B., Rodrigues, R., and Conte, T. (2012). Systematic literature reviews in distributed software development: A tertiary study. In *2012 IEEE Seventh International Conference on Global Software Engineering*, pages 134–143. IEEE.
- [Medvidovic and Taylor, 2010] Medvidovic, N. and Taylor, R. N. (2010). Software architecture. In *Proceedings of the 32nd ACM/IEEE International Conference on Software Engineering - ICSE '10*, volume 2, page 471, New York, New York, USA. ACM Press.

- [Mihalache et al., 2019] Mihalache, S. F., Pricop, E., and Fattahi, J. (2019). *Resilience Enhancement of Cyber-Physical Systems: A Review*, pages 269–287. Springer International Publishing, Cham.
- [Moghaddam et al., 2018] Moghaddam, M., Cadavid, M. N., Kenley, C. R., and Deshmukh, A. V. (2018). Reference architectures for smart manufacturing: A critical review. *Journal of Manufacturing Systems*, 49.
- [Moness and Moustafa, 2016] Moness, M. and Moustafa, A. M. (2016). A Survey of Cyber-Physical Advances and Challenges of Wind Energy Conversion Systems: Prospects for Internet of Energy. *IEEE Internet of Things Journal*, 3(2).
- [Monostori, 2014] Monostori, L. (2014). Cyber-physical production systems: Roots, expectations and R&D challenges. In *Procedia CIRP*, volume 17.
- [Monostori et al., 2016] Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., Sauer, O., Schuh, G., Sihn, W., and Ueda, K. (2016). Cyber-physical systems in manufacturing. *CIRP Annals*, 65(2).
- [Monteiro et al., 2018] Monteiro, P., Carvalho, M., Morais, F., Melo, M., Machado, R. J., and Pereira, F. (2018). Adoption of Architecture Reference Models for Industrial Information Management Systems. In *9th International Conference on Intelligent Systems 2018: Theory, Research and Innovation in Applications, IS 2018 - Proceedings*, pages 763–770.
- [NIST Group Big Data Public Working, 2018] NIST Group Big Data Public Working (2018). NIST Big Data Interoperability Framework: volume 6, reference architecture, version 2. Technical Report June, National Institute of Standards and Technology, Gaithersburg, MD.
- [Novak and Treytl, 2008] Novak, T. and Treytl, A. (2008). Functional safety and system security in automation systems-a life cycle model. In *2008 IEEE International Conference on Emerging Technologies and Factory Automation*, pages 311–318. IEEE.
- [Nowakowski et al., 2018] Nowakowski, E., Farwick, M., Trojer, T., Haeusler, M., Kessler, J., and Breu, R. (2018). Enterprise architecture planning in the context of industry 4.0 transformations. In *Proceedings - 2018 IEEE 22nd International Enterprise Distributed Object Computing Conference, EDOC 2018*, pages 35–43.
- [Piètre-Cambacédès and Chaudet, 2010] Piètre-Cambacédès, L. and Chaudet, C. (2010). The sema referential framework: Avoiding ambiguities in the terms “security” and “safety”. *International Journal of Critical Infrastructure Protection*, 3(2):55–66.
- [Qin et al., 2020] Qin, W., Chen, S., and Peng, M. (2020). Recent advances in Industrial Internet: insights and challenges. *Digital Communications and Networks*, 6(1):1–13.
- [Rajkumar et al., 2010] Rajkumar, R., Lee, I., Sha, L., and Stankovic, J. (2010). Cyber-physical systems: The next computing revolution. In *Proceedings - Design Automation Conference*, pages 731–736, New York, New York, USA. ACM Press.
- [Rawat et al., 2015] Rawat, D. B., Bajracharya, C., and Yan, G. (2015). Towards intelligent transportation Cyber-Physical Systems: Real-time computing and communications perspectives. In *Conference Proceedings - IEEE SOUTHEASTCON*, volume 2015-June, pages 1–6. IEEE.
- [Romero and Fernandez, 2017] Romero, V. M. and Fernandez, E. B. (2017). Towards a security reference architecture for cyber- physical systems. In *Proceedings of the LACCEI international Multi-conference for Engineering, Education and Technology*, volume 2017-July.
- [Sabrina, 2019a] Sabrina, F. (2019a). A Novel Entitlement-based Blockchain-enabled Security Architecture for IoT. In *2019 29th International Telecommunication Networks and Applications Conference, ITNAC 2019*, pages 1–7.
- [Sabrina, 2019b] Sabrina, F. (2019b). Blockchain and Structural Relationship Based Access Control for IoT: A Smart City Use Case. In *Proceedings - Conference on Local Computer Networks, LCN*, volume 2019-October, pages 137–140.

- [Schuß et al., 2018] Schuß, M., Iber, J., Dobaj, J., Kreiner, C., Boano, C. A., and Römer, K. (2018). Iot device security the hard(ware) way. In *Proceedings of the 23rd European Conference on Pattern Languages of Programs*, EuroPLoP '18, New York, NY, USA. Association for Computing Machinery.
- [Sharpe et al., 2019] Sharpe, R., van Lopik, K., Neal, A., Goodall, P., Conway, P. P., and West, A. A. (2019). An industrial evaluation of an Industry 4.0 reference architecture demonstrating the need for the inclusion of security and human components. *Computers in Industry*, 108:37–44.
- [Shi-Wan et al., 2017] Shi-Wan, L., Bradford, M., Jacques, D., Graham, B., Chigani, A., Martin, R., Murphy, B., and Crawford, M. (2017). The Industrial Internet of Things Volume G1 : Reference Architecture. *Industrial Internet Consortium White Paper*, Version 1.:58 Seiten.
- [Suh et al., 2014] Suh, S. C., Tanik, U. J., Carbone, J. N., and Eroglu, A. (2014). *Applied Cyber-Physical Systems*, volume 9781461473. Springer New York, New York, NY.
- [Syed and Fernandez, 2018] Syed, M. H. and Fernandez, E. B. (2018). A reference architecture for the container ecosystem.
- [Tantawy et al., 2020] Tantawy, A., Abdelwahed, S., Erradi, A., and Shaban, K. (2020). Model-based risk assessment for cyber physical systems security. *Computers Security*, 96:101864.
- [Torkaman and Seyyedi, 2016] Torkaman, A. and Seyyedi, M. A. (2016). Analyzing IoT Reference Architecture Models. *International Journal of Computer Science and Software Engineering ISSN*, 5(8):2409–4285.
- [ur Rehman et al., 2018] ur Rehman, S., Iannella, A., and Gruhn, V. (2018). A Security Based Reference Architecture for Cyber-Physical Systems. In *Communications in Computer and Information Science*, volume 942, pages 157–169.
- [Uzunov et al., 2015] Uzunov, A. V., Fernandez, E. B., and Falkner, K. (2015). Ase: A comprehensive pattern-driven security methodology for distributed systems. *Computer Standards & Interfaces*, 41:112–137.
- [VID/VDE, 2015] VID/VDE (2015). Reference Architecture Model Industrie 4.0 (RAMI4.0). *Igarss 2014*, 0(1).
- [Walter Colombo et al., 2020] Walter Colombo, A., Jan Veltink, G., Roa, J., and Laura Caliusco, M. (2020). Learning industrial cyber-physical systems and industry 4.0-compliant solutions. In *2020 IEEE Conference on Industrial Cyberphysical Systems (ICPS)*, volume 1, pages 384–390.
- [Wang et al., 2010] Wang, E. K., Ye, Y., Xu, X., Yiu, S. M., Hui, L. C., and Chow, K. P. (2010). Security issues and challenges for cyber physical system. In *Proceedings - 2010 IEEE/ACM International Conference on Green Computing and Communications, GreenCom 2010, 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing, CPSCom 2010*, pages 733–738. IEEE.
- [Wang et al., 2015] Wang, L., Törngren, M., and Onori, M. (2015). Current status and advancement of cyber-physical systems in manufacturing. *Journal of Manufacturing Systems*, 37:517–527.
- [Weber et al., 2017] Weber, C., Königsberger, J., Kassner, L., and Mitschang, B. (2017). M2DDM - A Maturity Model for Data-Driven Manufacturing. *Procedia CIRP*, 63:173–178.
- [Weyrich and Ebert, 2016] Weyrich, M. and Ebert, C. (2016). Reference architectures for the internet of things. *IEEE Software*, 33(1):112–116.
- [Xiong et al., 2015] Xiong, G., Zhu, F., Liu, X., Dong, X., Huang, W., Chen, S., and Zhao, K. (2015). Cyber-physical-social system in intelligent transportation. *IEEE/CAA Journal of Automatica Sinica*, 2(3):320–333.
- [Yli-Ojanperä et al., 2019] Yli-Ojanperä, M., Sierla, S., Papakonstantinou, N., and Vyatkin, V. (2019). Adapting an agile manufacturing concept to the reference architecture model industry 4.0: A survey and case study. *Journal of Industrial Information Integration*, 15:147–160.

[Yu and Xue, 2016] Yu, X. and Xue, Y. (2016). Smart Grids: A Cyber-Physical Systems Perspective.

[Zacchia Lun et al., 2019] Zacchia Lun, Y., D’Innocenzo, A., Smarra, F., Malavolta, I., and Di Benedetto, M. D. (2019). State of the art of cyber-physical systems security: An automatic control perspective. *Journal of Systems and Software*, 149.

[Zaidan et al., 2018] Zaidan, A. A., Zaidan, B. B., Qahtan, M., Albahri, O., Albahri, A., Alaa, M., Jumaah, F. M., Talal, M., Tan, K. L., Shir, W., et al. (2018). A survey on communication components for iot-based technologies in smart homes. *Telecommunication Systems*, 69(1):1–25.

[Zander et al., 2015] Zander, J., Mosterman, P. J., Padir, T., Wan, Y., and Fu, S. (2015). Cyber-physical Systems can Make Emergency Response Smart. *Procedia Engineering*, 107:312–318.

[Zibuschka et al., 2019] Zibuschka, J., Horsch, M., and Kubach, M. (2019). The Entourage privacy and security reference architecture for internet of things ecosystems. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft für Informatik (GI)*, P-293:119–130.