C. Alcaraz, "Secure Interconnection of IT-OT Networks in Industry 4.0", *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies*, pp. 201-217, 2019.
http://doi.org/https//doi.org/10.1007/978-3-030-00024-0_11
NICS Lab. Publications: https://www.nics.uma.es/publications

Secure Interconnection of IT-OT networks in Industry 4.0

Cristina Alcaraz
Computer Science Department, University of Málaga, Spain,
Campus de Teatinos s/n, 29071, Malaga, Spain
{alcaraz}@lcc.uma.es

Abstract

Increasingly, the society is witnessing how today's industry is adapting the new technologies and communication protocols to offer more optimal and reliable services to end-users, with support for inter-domain communication belonging to diverse critical infrastructures. As a consequence of this technological revolution, interconnection mechanisms are required to offer transparency in the connections and protection in the different application domains, without this implying a significant degradation of the control requirements. Therefore, this book chapter presents a reference architecture for the new Industry 4.0 where the interconnection core is mainly concentrated in the Policy Decision Points (PDP), which can be deployed in high volume data processing and storage technologies such as cloud and fog servers. Each PDP authorizes actions in the field/plant according to a set of factors (entities, context and risks) computed through the existing access control measures, such as RBAC+ABAC+Risk-BAC (Role/Attribute/Risk-Based Access Control, respectively), to establish coordinated and constrained accesses in extreme situations. Part of these actions also includes proactive risk assessment measures to respond to anomalies or intrusive threats in time.

1 Introduction

Industry, in general, is accepting the incorporation of the new technologies, networks and communication protocols to modernize its systems and allow a wider connection from anywhere, at any time and in anyhow. There are already several related works reflecting this progress [66, 30, 19, 65, 16], in which multiple cyber-physical devices interact with control processes and manufacturing chains for greater production, distribution and quality of service. This technological confluence is mainly based on the new paradigms of the Internet of Things (IoT), such as the Industrial IoT (IIoT), and the new edge computing infrastructures, such as cloud and fog computing [34]; all of them working as part of a heterogeneous network where Information Technologies (IT) merge with the Operational Technologies (OT), in order to maximize, optimize and customize the production tasks, and offer a greater range of functional possibilities and services for a better industrial sector, economy and society [21].

But when different IT-OT domains have to coexist to collaborate each other, interconnection mechanisms have to be extensively considered as mentioned in our previous works [11, 10]. In both works, different entities and application domains of the smart grid interconnect to provide a rapid and effective action in the field. Now, we expand the concept to include the Policy Decision Points (PDP) in the edge computing (i.e. in the cloud as a centralized component and in the fogs as part of each application domain) to not only simplify computational costs involved in the interconnection processes, but also take advantage and benefits of the new technologies of Industry 4.0. In this sense, we provide a reference architecture for any "smart" scenario (e.g. smart factories [54, 16], smart cities [39], smart healthcare, etc.) of the new Industry 4.0 together with its influence sectors, ensuring at all time operational and control performance, dependability, survivability, sustainability and safety-critical [7].

Through the PDP nodes, different stakeholders and industrial domains can converge in the connections and cooperate in a same common environment, offering a federated network composed of multi-domains. However, this type of collaboration and the need to modernize control and operational processes may also bring about numerous classes of anomalies that may, in turn, lead to subsequent and drastic threats [50]. For this reason, the access to our domains is strictly restricted to: The type of roles assigned to each entity (either IT-OT devices, software processes or physical entities) that wishes to take access to the different resources of the system, the real state of the context (e.g. severity level of a threat, criticality level of the context, number of isolated controllers, segmented and uncontrolled areas, etc.) and the risks associated with that context. To orchestrate all these actions, our approach contemplates the traditional authorization mechanisms [41] based on RBAC+ABAC+Risk-BAC (Role/Attribute/Risk-Based Access Control, respectively), as well as the IEC-62351-8 standard [35].

The standard IEC-62351 [33] comprises specific eleven parts to manage critical environments, such as power grids and their substations. Concretely, these parts include the specification of security profiles for IEC 60870-5 objects [32], XML files and communication channels, as well as the definition of security architectures and roles. But from these eleven parts, we especially focus on the IEC-62351-8 [35] by encompassing a useful set of particular entities, such as human operators, security administrators and engineers, together with their roles and rights. Apart from considering this standard as part of our approach, the architecture proposed also addresses aspects related to risk management from a proactive perspective, so as to offer an imminent response before major and serious disruptions arise within the system or between systems.

In either case, all these functional aspects are widely described in this chapter, which is organized as follows: Section 2 presents the interconnection architecture taking into account the restrictions of the context and the characteristics of the new industry. In this section, a set of assumptions are establihed to simplify the design and the scope of the approach. Each component of the architecture is widely described in Section 3.1 and Section 3.2, in which we consider the inclusion of the new edge computing infrastructures to address the policy decision points. The feasibility of the approach is, to the contrary, analyzed in Section 3.3 so as to show the effectiveness of the components and guarantee protection to each of the industrial areas and their final services. Lastly, Section 4 concludes the book chapter and presents future work.

2 Interconnection architecture for Industry 4.0 scenarios

When different application domains need to be interconnected each other, it is commonly applied interconnection frameworks based on Policy Enforcement Points (PEP) and PDP [60]. Through PEP, entities (i.e. physical members, IT-OT devices or software processes) can request access to the different resources of the system. In this case, the PEP intercepts and forwards the request to the PDP so that this latter can manage the authorization policies and determine the access level to the different sections of the system according to a set of factors: The type of entity, the resources and the context. Once the decision is taken by the PDP, the PEP processes it to permit or deny access to the interested entity, thereby protecting the critical resources of the system.

This way of connecting systems can also allow today's industry to interconnect industrial multi-domains, at which the creation of a cooperative environments is generally required to transparently connect providers, customers and other industrial networks [66]. In this sense, our architecture should follow a collaborative interconnection model where interconnection components (i.e. PDP) should maintain certain information of the own federated network. The architectures presented in [25], [11] and [10] are clear federation examples. The former is a patent where users and domains are able to transparently connect each other. The patent characterizes the inter-domain communication through an additional Meta Policy Decision Point (MPDP) to manage authentication and authorization processes between domains. The works [11] and [10], to the contrary, assign all the authentication process in the respective domains and concentrate all the authorization process in intermediaries PDP working like proxies.

If we unify both ideas and adapt them to our architecture, we can find a way to connect different industrial domains together with their application sub-domains, at which different protocols and technologies can coexist. To do this, we assume the following structural conditions, technologies and stakeholders:

Structural conditions: Today the new industrial revolution accepts the inclusion of the new IT to manage, manipulate and store operational data and processes. This also means that industrial networks have to protect IT-OT connections through perimeter protection elements such as industrial firewalls and/or Virtual LAN (VLAN) for segmentation, Intrusion Detection/Prevention Systems (IDS/IPS) and Virtual Private Networks (VPN) for a secure tunneling through IPSec.

Technologies: Apart from the technological diversity in control terms (e.g. sensors, actuators, controllers − remote terminal units or programmable logic controllers −, robot units, etc.) and the proliferation of industrial communication protocols (e.g. OPC-UA, 6LowPAN, IO-Link, EtherNet/IP and EtherCAT, WirelessHART, ISA100.11a or ZigBee PRO) [6, 16], there is an important need to integrate IT services to render large industrial data streams and processes. Among these IT services, we stress the cloud and the fog computing [34], which can compute contextual information for future administrative or operational actions, and benefit the control (per domain) and the processes related to context management,

predictive maintenance, detection of anomalies and equipment failures, performance monitoring, governance, auditing or forensic.

As for security, it is widely assumed that all sections of the interconnection system, including the Machine-to-Machine (M2M) communication between devices, are protected through the existing security mechanisms and standards [33]. Beyond the perimeter protection, cryptography, key management systems, identity management, access control and traditional security protocols such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS) are also essential for processing, storing and transferring critical data from a secure perspective [24]; without ruling out high-level security services such as privacy, trust or quality of service [12].

Stakeholders: As stated in [16], customers and providers may also be part of the operational procedures to accelerate, customize and optimize the manufacturing and logistic processes, maximizing operational performance and costs in the plant/field. This also means that the model proposed should allow the influence of external connections with access to IT networks, such as the cloud or the fog. From the set of entities specified in [35], we also identify, among others, the participation of engineers, auditors and security administrators since they can interact with the system to offer essential actions for the production and distribution of minimal services to end-users, such as energy, water or food.

All these assumptions are also illustrated in Figure 1. This figure clearly represents the technological confluence of the new Industry 4.0 composed of diverse operational and control areas, and multiple types of stakeholders. As can be observed, each domain comprises a set of OT devices working with different communication protocols and interacting with IT networks, such as industrial wireless sensor networks, RFID (Radio-Frequency Identification) or fog-computing. The role of the fog-computing is to locally provide a mean of processing and storage of large volumes of data, the information of which can also be compiled by a federated cloud infrastructure, common for all the application domains. The cloud technology, to the contrary, serves as a holistic environment capable of managing data related to users, control and context belonging to the different "smart world" scenarios (e.g. smart factories, smart grid, smart cities, smart health-care, etc.), the services of which are fundamental for social and economic well-being.

To articulate all these connections, the architecture accommodates two classes of PDP: One global to the entire system and another local to each application domain. The global PDP is shaped in the cloud to (i) receive information of the context from each local PDP deployed in the fog and (ii) offer an overview of the state of the entire system and its correct performance. The PDP in the cloud is denoted here as PDP-cloud and the PDP in the fog is called MPDP-fog in relation to the MPDP described in [25]. The access to each one of these two kinds of policy decision points relies on the type of entity (human operators, providers, customers, administrators, auditors, engineers, processes or IT-OT devices). Local entities linked to local operational actions

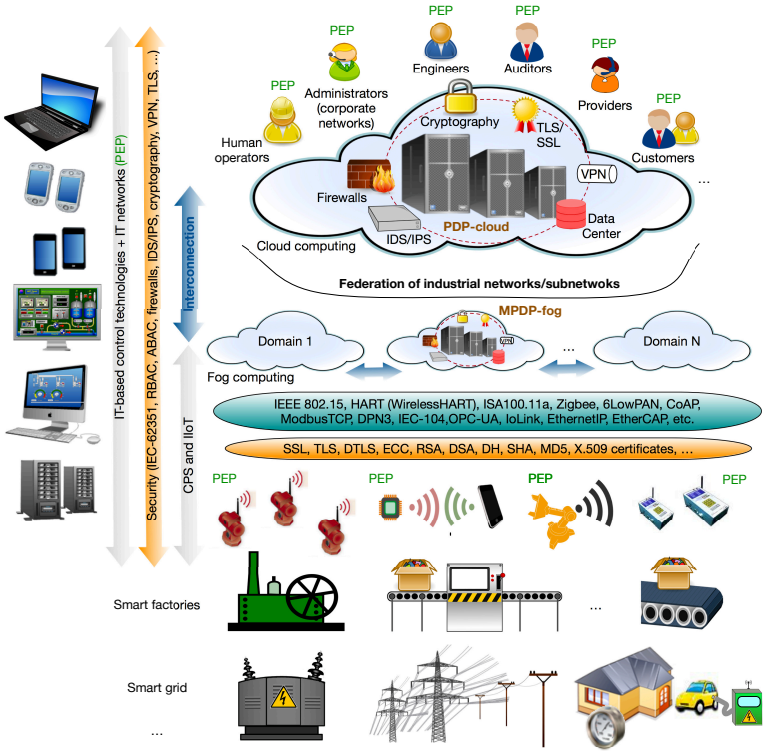

Figure 1: Secure interconnection architecture for Industry 4.0 scenarios

in the field or in the process plant should consider the access through its corresponding MPDP-fog; whilst remote entities (administrators, engineers, operators located at SCADA (Supervisory Control And Data Acquisition) centers, providers, auditors, etc.) to the different local domains should access through the PDP-cloud. This functional characteristic is also illustrated in Figure 2.

Figure 2 is an example of how remote stakeholders are able to gain access through PEP instances to the PDP-cloud. However, the secure interoperability between IT-OT networks, the devices of which generally present performance limitations [10, 7], adds the need to locally delegate all the authorization process and translation actions of security policies and communication protocols to the MPDP-fog nodes. This condition endorses that the PDP-cloud is only able to authenticate external entities and validate the access according to the context, leaving all access responsibility to the meta PDP. In this way, the architecture simplifies the centralized actions in the cloud and any bottleneck occurrence. Note that this restriction is also subject to M2M communications of each domain. In this case, the authentication procedure is concentrated in each MPDP to locally handle PEP calls between domains and unburden the cloud of these operations.

3 Interconnection components for Industry 4.0 connections

Both the architecture of the PDP-cloud and the MPDP-fog are described in detail in this section together with those components that these include. More specifically, the actions taken by the PDP-cloud are firstly addressed to show how external connections are managed from an independent infrastructure to each domain, and later the specific components of the meta PDP are analyzed.

3.1 PDP-cloud: modules and functionality

Figure 3 represents the architectonic design of the modules that integrate the PDP operations required between entities and domains. Particularly, the architecture adds two chief components: The *PDP manager* and the *context awareness manager*. The former is in charge of validating the authentication tokens provided by each entity. This means that each entity must authenticate by itself from its own organization, delegating all the authorization process in the policy decision points.

Authentication is a procedure required to validate the identity of an entity and favor legitimate access to resources of the system. If the authentication is made from the entity premise and the access through the cloud, then it is required to consider the solutions described in [13]. This survey classifies the methods according to the location of the authentication modules, where the methods implemented in the "entity side" are mainly based on identity and context schemes. Chow et al., for example, define in [52] an identity-based authentication scheme, the core of wich is focused on the zero-knowledge authentication, the digital signature, and the fuzzy method. In contrast, Schwab and Yang specify in [18] a federated authentication framework, known as TrustCube with similar features to the OpenID technology, managing multiples types

of policies related to the platform, devices and users. This way of authenticating in the entity side would not only reduce maintenance costs of databases in the cloud side, but it would also benefit the user's mobility. Human operators, engineers or even customers using mobile devices within a specific application scenario, such as manufacturing plants in smart factories or smart grid substations, can request PEP instances from any where, at any time and in any how, thereby promoting the new paradigms of the IoT; i.e. the IIoT.

But despite this local procedure, any validated identity in its premise also has to show its authenticity and legitimacy in the PDP-cloud through the use of authentication tokens. These tokens should add certain information about the previous authentication process and specific information about the PEP request, such as: The identity of the resource and the domain, and the type of action to be performed on the resource. All this information is compiled by the PDP manager together with additional information related to the roles and permissions assigned to the entity, the criticality level of the context in which the resource is being deployed and the risks associated to that context. The context information is obtained through the context awareness manager, responsible of computing the level of observation and controllability received from the application domain itself. This information is generally associated with attribute values that explain among other things: Which sensors, actuators or controllers are isolated, how many sub-areas are segregated, which nodes are working and which are not, status of communication links, operating systems or network parameters, etc.

Apart from the *authentication module* of tokens, the PDP manager is also composed of two further components: The *access token manager* and the *access prioritization manager*. These two components are based on the Role-Based Access Control (RBAC) strategy as recommended by the standard IEC-62351-part 8 [35]. Concretely, the standard defines seven specific roles for engineering and control scenarios managing different types of rights, such as the human operator with the capacity for viewing, reading, reporting and controlling operational objects and processes, or the engineer with the ability for viewing, reading, reporting, configuring and managing objects, databases and file systems. In addition to these roles, the standard reserves until 32.767 roles for private use, allowing to allocate new Industry 4.0 stakeholders as identified in Section 2. In our case, we could define capacities for viewing, reading and reporting operational objects assigned to auditors and customers, adding configuration support to providers.

This way of orchestrating permissions together with the dynamic capacity of RBAC for separation of duties, commonly known as Dynamic Separation of Duties (DSD), permits the system to redistribute security controls according to the security policies of each organization and the contextual conditions, adding versatility in the approach and dynamism in the protection process. To do this, the *risk assessment manager*, included as part the context awareness manager, has to compile all the information from the domains and contrast the existence or the persistence of possible risks [49] in the domains demanded where the control should prevail in extreme situations. This means that each entity should support at least two roles, one working as primary and other as secondary; and in this way, when control areas lack of enough connectivity, only authorized entities with determined roles could gain access to the affected area and take the control of this one. This propriety of DSD is widely described and implemented in

[11, 10].

The context can also be managed by the *early warning manager* to estimate in optimal times and from a local or global perspective, the real state of the system for the next stage; and in the worst case, to prepare and activate the protection mechanisms related to location and alerting of human operators, as well as establish the prioritization levels taking into account the DSD properties. Any estimation must be loaded to the database for future risk assessments, in which a set of parameters should be evaluated, such as: The frequency, the relevance and the severity of the threat in the different domain/s, the criticality of the scenarios and their resources, the degree of devastation and the consequences (e.g. in social or economic terms), etc. The computation of all of these inputs will allow to compute and estimate any cascading effect between subsystems or systems, track and visualize in real time the threat in order to tackle the problem, and improve the regulatory procedures related to governance, auditing and forensic.

All this context information is part of the Policy Information Point (PIP) as specified in the RFC-2904 [60] for the interconnection of systems. A PIP refers to the management point where a set of attribute values related to resources, subjects and environment is compiled and normalized, to later determine the severity degree of the area and permit or not access to the area. This features also allows us to adapt the methods Attribute-Based Access Control (ABAC) and Risk-Based Access Control (Risk-BAC), and combine them with RBAC, in order to further restrict access conditions. Through ABAC+Risk-BAC, it is possible to take more stringent decisions established by the real attributes of the context and the risks associated with that context [57], further delimiting the access conditions by dynamically managing roles. In the literature, there several related works for IoT and IIoT environments [38, 29, 14], which can be considered for future implementations.

Finally, the *access manager*, integrated in the PDP manager, computes not only the information received from the respective modules but also verifies the legitimacy of the permissions to be executed in the field. For this action, it is necessary to contrast the information with the security policies stored in the databases, which are managed by technical administrators, installers or engineers through Policy Administration Points (PAP). Once the information is processed, the manager generates an access token to later validate the entity and the access itself in the destination domain. To accelerate the management of future related PEP instances or detect possible abuses in the requests (i.e. replay attacks), the access manager also needs to keep a temporal copy of each instance managed through a cache memory.

3.2 MPDP-fog: modules and functionality

This section presents the architectonic model of the meta policy decision points configured in the respective fog infrastructures installed in each of the application domains (see Figure 4). Similar to the PDP-cloud architecture, each MPDP-fog includes two chief modules: The *access manager* and the *domain awareness manager*. The first module contains an *authentication component* capable of addressing two types of actions depending on the origin and the class of token: (i) Verify the authenticity of the access tokens received from the cloud and (ii) validate the identity of those PEP instances established from other domains.

In this state, the technical capacities of the technologies are also keys to determine the authentication mode. For example, M2M communication based on IIoT devices and manufacturing machines (e.g. sensors, actuators, controllers or robots) are not generally tamper-resistant to attacks and they are based on constrained hardware components [4], working by themselves at remote locations such as substations or operational plants [40]. To reduce computational and communication overheads, the use of lightweight authentication schemes at the application layer and security protocols at the transport layer (TLS or Datagram TLS (DTLS)) are extensively considered in the literature [28, 1]. However, the design of lightweight solutions (at the application layer) for certain paradigms like IIoT, is still a great challenge for the scientific community [67]. In this case, we stress some works related to cyber-physical systems and IIoT such as [26], [53] and [17]. Esfahani *et al.* propose in [26] a mutual authentication mechanism for M2M communication using simple primitives and mathematical operations (hashes and XOR), thereby simplifying the authentication processes. In [53], the authors, to the contrary, offer an authentication framework to validate the identity of each object in the IIoT according to the device-specific information; and in [17], Chin *et al.* similarly propose M2M two-layer-based authentication framework for smart grid scenarios where smart meters are authenticated by a public key infrastructure and digital signature.

At the transport layer, there are already available several communication protocols for IoT, such as [58, 64]: 6LowPAN (IPV6 over Low power wireless Personal Area Network) [47], MQTT (Message Queue Telemetry Transport) [44, 58], AMQP (Advanced Message Queuing Protocol) [58], XMPP (Extensible Messaging and Presence Protocol) [61], DDS (Data Distribution Service) [45], and CoAP (Constrained Application Protocol) [48]; all of them supporting authentication measures through SSL and DTLS sessions. Namely, all the protocols except CoAP are based on TLS, whilst CoAP is focused on DTLS [26, 1]. Moreover, XMPP and AMQP can also use the Simple Authentication and Security Layer (SASL) protocol to authenticate devices [42, 43]. However, for all these protocols and the existing works related to the IoT field [37, 31, 63, 62] is recommendable to verify the suitability of the approach taking into account the technical restrictions of the IIoT devices together with control requirements as specified in [7].

Continuing with the actions of the access manager, the system has to validate all the previous states before computing any new access request. The goal is to reduce any computational cost involved in the context evaluation and translation of security policies and communication protocols. As stated in Section 2, the operational performance is critical at this interconnection point since multiple and concurrent access requests are generally demanded in this stage; either from the cloud or from any application area (through a new PEP request). To ensure this performance level, the system needs to temporarily cache all the actions performed by the access manager to avoid passing through the translators of communication protocols and security policies. Normally, both modules demand computation and time to address translation tasks considering the management and updating of specific tables for the matching of protocols (including ports and IP addresses) and policies. Nonetheless, this computational consumption is heavily dependent on the type of implementation designed for the translation engine. For example, the work [23] proposes a protocol translator for industrial communication

based on a service-oriented architecture, translating on-demand and at a low-latency cost; whilst [36] traduces the communication according to algebraic specifications and [11, 10] are based on a rule-based expert translation system.

In either case, these translations benefit interoperability tasks in such a way that IIoT entities in general, can connect with each other transparently as stated in [11, 10]. Both works reflect similar goals to the proposed approach, in which different interfaces can establish connectivity without need to follow an equivalent security policy criterion for all parties and taking into account the natural conditions of the context to activate the DSD mechanisms if they are necessary. To go beyond these two works, our meta PDP nodes are not only able to handle the access according to the RBAC+ABAC properties, but they are also able to proactively determine the accessibility level according to the risks of the context. At this point, the risk management is critical to locally determine the severity degree of a threat and assess the consequences to establish much more restrictive conditions per area instead of only processing it in a centralized node as outlined in [11, 10].

Therefore, all our policy decision points, pertinent to the PDP-cloud and MPDP-fog, manage the access taking into account the capacities provided by RBAC+ABAC +Risk-BAC [41]. In particular, the access prioritization is under the restrictions given by the RBAC-based *access prioritization manager* as specified in Section 3.1. This manager activates the DSD mechanism according to the risk evaluation given by the *domain awareness manager*, which includes four similar components to the context manager of the PDP-cloud. The main difference that keeps the awareness manager of the MPDP-fog regarding the PDP-cloud is that the domain awareness manager is mainly focused on locally computing the context at which the application scenario is being developed. The information processed by this module can be very versatile, the data of which can belong to the physical world (e.g. humidity, temperature, pressure, etc.) and/or the virtual world through software processes, software agents (e.g. through opinion dynamics [49, 51]) or logs.

3.3 Suitability of the architecture for Industry 4.0 scenarios

Considering the control requirements specified in [7], this section analyses the suitability of the architecture proposed in Section 2 and its functions for future Industry 4.0 scenarios. In [7] five requirements for industrial control systems are identified: Real-time performance, dependability, sustainability, survivability and safety-critical; and for each of these requirements, the impact on the different elements and services of the system (information, resources, control, minimal services) is assessed. To adapt these five control requirements to our architecture, the analysis will primarily be focused on evaluating the five control requirements taking into account the primary needs of the new Industry 4.0 and the interconnection requirements defined in [9], such as rapid access, transparency in the connections, communication in real time, availability and reliability, also adding protection of devices and security in the multi-domain connections.

Real-time performance: One of the main goals of including policy decision points in edge computing infrastructures is precisely to decrease the number of connections to the different application domains. Entities connecting from the cloud,

first need to validate their access. If the access is not proper, then the system denies the entry in the field/plant, thereby reducing the number of connections in the domains and unnecessary overloads. This feature is also contemplated in each domain individually where entities first has to locally authenticate in their premise, so as to later gain access to the resources of other domain, thereby protecting the access to constrained resources. On the other hand, the use of cache memories and different authorization mechanisms, in which access privileges are restricted according to roles, contextual conditions of each domain and risks associated with these domains, also avoid serious overheads that may hamper the operational and control processes and cause significant delays.

Dependability and survivability: The possibility of managing risks from a proactive and reactive perspective, allows the system to detect anomalies and response accordingly, ensuring availability of resources at all time and reliability of their services. Many of the anomalies come from the malfunctions or unsuitable configurations of systems or networks, or deficiencies in the coexistence of multiple systems [8], which may consequently bring about numerous security problems [15, 50]. Moreover, this manner of offering automatic fault detection also adds a significant reduction of maintenance costs and benefits the future Industry 4.0 services allocated in the cloud, such as predictive maintenance and the optimization of operational services and equipment. In this case, our risk assessment and early warning managers should connect with external services to feed up any suspicious of threat, risk or anomaly, or could even connect with specialized cyber-security centers (e.g. computer emergency response teams such as the CNN-CERT [20] or the ICS-CERT [22]) to alert of extreme situations. Also related to cyber-defense, the use of cache memories aids to detect replay attacks by simply tracking the last PEP requests, IP addresses and timestamps as specified in [5]. And though the advanced security services are not extensively considered in this chapter, such as privacy and trust, they are also essential as part the M2M communications and particularly between cloud/fog-IIoT devices [55, 46].

Sustainability: The abilities of the system to manage risks and supply accountability capacities (see Figures 3 and 4) allow the system to provide a more reliable governance, auditing and forensic services. The records in each one of the incoming points of the system can determine the type of access in the field/plant, the actions carried out in the resources, the entities or organizations responsible for these actions, the access periods and abuses in the connections. These inputs can even feed up the risk assessment and early warning managers to estimate inappropriate actions, anomalies or threats, and this can also help the system to review its security policies and any regulation framework required to respond accordingly. Evidently, if this process is rigorously considered, the system can comply with the interconnection requirements at all time and be sustainable for the control; i.e. maintain control services at all times and for a long period, at an acceptable level for the protection of resources and critical infrastructures [7]. This sustainability feature is also supported by the abilities of each MPDP to translate protocols and security policies, and if, in addition, the corresponding

modules are regularly updated, the system also ensures a tenable interconnection.

Safety-critical: In this aspect, we highlight the capacity of the system to protect the critical resources from external accesses, and especially when the domain hosting the resources present extreme crisis situations. Under these critical circunstances, it is always recommendable to recover and return the control [3, 2] to the affected area, and to avoid, as much as possible, expanding the effect of the threat to the rest of interconnected domains, known as cascading effect. In addition to this, the management of proactive responses also aims to reduce possible secondary effects in the system or between systems, reducing the risk levels in advance [56] and any threatening effect that may entail a drastic cascading effect.

Taking into account all these control and interconnection principles, we consider that our architecture is suitable for the new control industry, in which a set of (IT-OT) technologies, protocols and networks have to coexist for a long period of time. From these technologies, we particularly focus on the cloud and fog infrastructures to accommodate the approach and reduce computational and communication costs, as well as enhance their resources to add additional capacities related to interconnection and protection in different terms and levels; all of them necessary for the new Industry 4.0 scenarios.

4 Conclusions and future work

A multi-domain interconnection architecture is proposed in this book chapter to connect multiple federated areas belonging to critical infrastructures (e.g. manufacturing industry and supply chains, food production plants, power grids and smart cities [39], and water treatment plants) without breaking the control requirements that generally these infrastructures demand. Typical domains are, for example, the generation, transmission and distribution substations configured as part of smart grid, or the different manufacturing sections corresponding to smart factories or supply chains. To do this, the architecture is based on a two layer interconnection system composed of two kinds of policy decision points; one located at a centralized system and another distributed throughout the different application domains. The centralized node corresponds to a cloud server capable of managing any entry belonging to external entities of the system or subsystems, such as customers, providers, auditors, etc.; whilst the distributed PDP are in charge of controlling any access coming from other domains or from the cloud.

This architecture based on two-layers incorporates in each PDP a set of functional modules with the ability to handle the access according to the characteristics and intentions of each entity together with their roles, the real state of the context and its resources, as well as the risks associated to this context. Therefore, the approach includes components capable of orchestrating aspects related to RBAC+ABAC+Risk-BAC with support for proactive solutions before serious interruptions may arise within the entire system. For the future, we intend to implement all these components in our laboratory [59] to later include them as part of the goals of the European SealGRID project [27]. And with this, show all the functionalities of the architecture for the new control industry, further considering the incorporation of specific services related to protection of communication channels (entities-cloud/fog, cloud-fog, M2M), privacy and trust.

Acknowledgments

This work has been mainly supported by the EU H2020 project SealGRID (8.06.UE/47.8035), with partial support of the project DISS-IIoT financed by the University of Malaga (UMA) by means of the "I Plan Propio de Investigación y Transferencia" of UMA where specific knowledge about assembly and configuration of IIoT and control components has been widely received.

References

[1] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys Tutorials **17**(4), 2347–2376 (2015)

[2] Alcaraz, C.: Resilient industrial control systems based on multiple redundancy. International Journal of Critical Infrastructures (IJCIS) **13**(2/3), 278 – 295 (2017)

[3] Alcaraz, C.: Cloud-assisted dynamic resilience for cyber-physical control systems. IEEE Wireless Communications **25**(1), 76–82 (2018)

[4] Alcaraz, C., Cazorla, L., Fernandez, G.: Context-awareness using anomaly-based detectors for smart grid domains. In: 9th International Conference on Risks and Security of Internet and Systems, vol. 8924, pp. 17–34. Springer, Trento (2015)

[5] Alcaraz, C., Fernandez-Gago, C., Lopez, J.: An early warning system based on reputation for energy control systems. IEEE Transactions on Smart Grid **2**(4), 827–834 (2011)

[6] Alcaraz, C., Lopez, J.: A security analysis for wireless sensor mesh networks in highly critical systems. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews **40**(4), 419–428 (2010)

[7] Alcaraz, C., Lopez, J.: Analysis of requirements for critical control systems. International Journal of Critical Infrastructure Protection (IJCIP) **5**, 137–145 (2012)

[8] Alcaraz, C., Lopez, J.: Wide-area situational awareness for critical infrastructure protection. IEEE Computer **46**(4), 30–37 (2013)

[9] Alcaraz, C., Lopez, J.: Secure interoperability in cyber-physical systems. In: Security Solutions and Applied Cryptography in Smart Grid Communications, chap. 8, pp. 137–158. IGI Global, USA (2017)

[10] Alcaraz, C., Lopez, J., Choo, K.K.R.: Resilient interconnection in cyber-physical control systems. Computers & Security **71**, 2–14 (2017)

[11] Alcaraz, C., Lopez, J., Wolthusen, S.: Policy enforcement system for secure interoperable control in distributed smart grid systems. Journal of Network and Computer Applications **59**, 301–314 (2016)

[12] Alcaraz, C., Zeadally, S.: Critical control system protection in the 21st century: Threats and solutions. IEEE Computer **46**(10), 74 – 83 (2013). DOI 10.1109/MC.2013.69

[13] Alizadeh, M., Abolfazli, S., Zamani, M., Baharun, S., Sakurai, K.: Authentication in mobile cloud computing: A survey. Journal of Network and Computer Applications **61**, 59 – 80 (2016)

[14] Atlam, H.F., Alenezi, A., Walters, R.J., Wills, G.B., Daniel, J.: Developing an adaptive risk-based access control model for the internet of things. In: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 655–661 (2017)

[15] Cazorla, L., Alcaraz, C., Lopez, J.: Cyber stealth attacks in critical information infrastructures. IEEE Systems Journal **12**, 1778–1792 (2018)

[16] Chen, B., Wan, J., Shu, L., Li, P., Mukherjee, M., Yin, B.: Smart factory of industry 4.0: Key technologies, application case, and challenges. IEEE Access **6**, 6505–6519 (2018)

[17] Chin, W.L., Lin, Y.H., Chen, H.H.: A framework of machine-to-machine authentication in smart grid: A two-layer approach. IEEE Communications Magazine **54**(12), 102–107 (2016)

[18] Chow, R., Jakobsson, M., Masuoka, R., Molina, J., Niu, Y., Shi, E., Song, Z.: Authentication in the clouds: A framework and its application to mobile users. In: Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop, CCSW '10, pp. 1–6. ACM, New York, NY, USA (2010)

[19] Cisneros-Cabrera, S., Ramzan, A., Sampaio, P., Mehandjiev, N.: Digital marketplaces for industry 4.0: A survey and gap analysis. In: L.M. Camarinha-Matos, H. Afsarmanesh, R. Fornasiero (eds.) Collaboration in a Data-Rich World, pp. 18–27. Springer International Publishing, Cham (2017)

[20] CNN-CERT: Centro Cripotológico Nacional. https://www.ccn-cert.cni.es, last retrieved in June 2018 (2006)

[21] Dar, K.S., Taherkordi, A., Eliassen, F.: Enhancing dependability of cloud-based IoT services through virtualization. In: Internet-of-Things Design and Implementation (IoTDI), 2016 IEEE First International Conference on, pp. 106–116. IEEE (2016)

[22] Department of Homeland Security: Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). https://ics-cert.us-cert.gov, last retrieved June 2018 (2004)

[23] Derhamy, H., Eliasson, J., Delsing, J.: Iot interoperability on-demand and low latency transparent multiprotocol translator. IEEE Internet of Things Journal **4**(5), 1754–1763 (2017). DOI 10.1109/JIOT.2017.2697718

[24] Dzung, D., Naedele, M., Von Hoff, T.P., Crevatin, M.: Security for industrial communication systems. Proceedings of the IEEE **93**(6), 1152–1177 (2005)

[25] Edwards, N.J., Rouault, J.: Multi-domain authorization and authentication (2008). US 7.444,666B2

[26] Esfahani, A., Mantas, G., Matischek, R., Saghezchi, F.B., Rodriguez, J., Bicaku, A., Maksuti, S., Tauber, M., Schmittner, C., Bastos, J.: A lightweight authentication mechanism for m2m communications in industrial iot environment. IEEE Internet of Things Journal pp. 1–1 (2017)

[27] European Commision: SealGRID: Scalable, trustEd, and interoperAble pLatform for sEcureD smart GRID. http://www.sgrid.eu/, last retrieved in June 2018 (2018)

[28] Ferrag, M.A., Maglaras, L.A., Janicke, H., Jiang, J.: Authentication protocols for internet of things: A comprehensive survey. CoRR **abs/1612.07206** (2016)

[29] Fraile, F., Tagawa, T., Poler, R., Ortiz, A.: Trustworthy industrial iot gateways for interoperability platforms and ecosystems. IEEE Internet of Things Journal pp. 1–1 (2018)

[30] Grangel-González, I., Baptista, P., Halilaj, L., Lohmann, S., Vidal, M.E., Mader, C., Auer, S.: The industry 4.0 standards landscape from a semantic integration perspective. In: 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1–8 (2017)

[31] Hernández-Ramos, J.L., Pawlowski, M.P., Jara, A.J., Skarmeta, A.F., Ladid, L.: Toward a lightweight authentication and authorization framework for smart objects. IEEE Journal on Selected Areas in Communications **33**(4), 690–702 (2015)

[32] IEC-61850: Power utility automation - communication networks and systems in substations - parts 1-10. TC 57 - Power systems management and associated information exchange (2003)

[33] IEC-62351: IEC-62351 parts 1-8: Information security for power system control operations, international electrotechnical commission. http://www.iec.ch/smartgrid/standards/, last retrieved in June 2018 (2007-2011)

[34] Industrial Internet Consortium, Edge Computing Task Group: Introduction to edge computing in IIoT. An Industrial Internet Consortium White Paper, IIC:WHT:IN24:V1.0:PB:20180618, https://www.iiconsortium.org,last retrieved June 2018 (2018)

[35] International Electrotechnical Commission: IEC-62351-8, Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control. http://www.iec.ch/smartgrid/standards/, last retrieved in June 2018. (2011)

[36] Ishihara, Y., Seki, H., Kasami, T.: A translation method from natural language specifications into formal specifications using contextual dependencies. In: Proceedings of the IEEE International Symposium on Requirements Engineering, pp. 232–239 (1993)

[37] Lee, J.Y., Lin, W.C., Huang, Y.H.: A lightweight authentication protocol for internet of things. In: International Symposium on Next-Generation Electronics (ISNE), pp. 1–2 (2014)

[38] Liu, Q., Zhang, H., Wan, J., Chen, X.: An access control model for resource sharing based on the role-based access control intended for multi-domain manufacturing internet of things. IEEE Access **5**, 7001–7011 (2017)

[39] Lom, M., Pribyl, O., Svitek, M.: Industry 4.0 as a part of smart cities. In: 2016 Smart Cities Symposium Prague (SCSP), pp. 1–6 (2016)

[40] Lopez, J., Alcaraz, C., Roman, R.: Smart control of operational threats in control substations. Computers & Security **38**, 14–27 (2013)

[41] Lopez, J., Rubio, J.E.: Access control for cyber-physical systems interconnected to the cloud. Computer Networks **134**, 46 – 54 (2018)

[42] Norris, R., Miller, J., Saint-Andre, P.: XEP-0034: SASL integration. https://xmpp.org/extensions/xep-0034.html, last retrieved in June 2018 (2017)

[43] OASIS: OASIS Advanced Message Queuing Protocol (AMQP) version 1.0 Part 5: Security. http://docs.oasis-open.org/amqp/core/v1.0/amqp-core-security-v1.0.html, last retrieved in June 2018 (2012)

[44] OASIS: MQTT and the NIST cybersecurity framework version 1.0. http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/mqtt-nist-cybersecurity-v1.0.html,last retrieved in June 2018 (2014)

[45] OMG: Data ditribution service specification v1.4. https://www.omg.org/spec/DDS/About-DDS/, last retrieved in June 2018 (2015)

[46] Pearson, S., Benameur, A.: Privacy, security and trust issues arising from cloud computing. In: Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on, pp. 693–702. IEEE (2010)

[47] Qiu, Y., Ma, M.: A mutual authentication and key establishment scheme for M2M communication in 6LoWPAN networks. IEEE Transactions on Industrial Informatics **12**(6), 2074–2085 (2016)

[48] Raza, S., Shafagh, H., Hewage, K., Hummen, R., Voigt, T.: Lithe: Lightweight secure CoAP for the Internet of Things. IEEE Sensors Journal **13**(10), 3711–3720 (2013)

[49] Rubio, J.E., Alcaraz, C., Lopez, J.: Preventing advanced persistent threats in complex control networks. In: European Symposium on Research in Computer Security, vol. 10493, pp. 402–418. 22nd European Symposium on Research in Computer Security (ESORICS 2017), 22nd European Symposium on Research in Computer Security (ESORICS 2017) (2017)

[50] Rubio, J.E., Alcaraz, C., Roman, R., López, J.: Analysis of intrusion detection systems in industrial ecosystems. In: Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017), vol. 4, pp. 116–128 (2017)

[51] Rubio, J.E., Roman, R., Alcaraz, C., Zhang, Y.: Tracking advanced persistent threats in critical infrastructures through opinion dynamics. In: European Symposium on Research in Computer Security. Springer, Springer, Barcelona, Spain (In Press)

[52] Schwab, D., Yang, L.: Entity authentication in a mobile-cloud environment. In: Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, CSIIRW '13, pp. 42:1–42:4. ACM, New York, NY, USA (2013)

[53] Sharaf-Dabbagh, Y., Saad, W.: Cyber-physical fingerprinting for Internet of Things authentication: Demo abstract. In: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, IoTDI '17, pp. 301–302. ACM, New York, NY, USA (2017)

[54] Shrouf, F., Ordieres, J., Miragliotta, G.: Smart factories in industry 4.0: A review of the concept and of energy management approached in production based on the internet of things paradigm. In: Industrial Engineering and Engineering Management (IEEM), 2014 IEEE International Conference on, pp. 697–701. IEEE (2014)

[55] Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A.: Security, privacy and trust in Internet of Things: The road ahead. Computer networks **76**, 146–164 (2015)

[56] Thamhain, H.: Managing risks in complex projects. Project management journal **44**(2), 20–35 (2013)

[57] Thomas, M.V., Chandrasekaran, K.: Identity and Access Management in the Cloud Computing Environments, chap. 3, pp. 61–89. ISI Global (2016)

[58] Thota, P., Kim, Y.: Implementation and comparison of M2M protocols for Internet of Things. In: 2016 4th Intl Conf on Applied Computing and Information Technology/3rd Intl Conf on Computational Science/Intelligence and Applied Informatics/1st Intl Conf on Big Data, Cloud Computing, Data Science Engineering (ACIT-CSII-BCD), pp. 43–48 (2016)

[59] University of Malaga: DISS-IIoT: Design and Implementation of Security Services for the Industrial Internet of Things. https://www.nics.uma.es/projects/diss-iiot, last retrieved in June 2018 (2018)

[60] Vollbrecht, J., Calhoun, P., Farrell, S., Gommans, L., Gross, G., de Bruijn, B., de Laat, C., Holdrege, M., Spence, D.: AAA authorization framework. RFC 2904 (2000)

[61] Wang, H., Xiong, D., Wang, P., Liu, Y.: A lightweight XMPP publish/subscribe scheme for resource-constrained IoT devices. IEEE Access **5**, 16,393–16,405 (2017)

[62] Wang, K.H., Chen, C.M., Fang, W., Wu, T.Y.: On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags. J. Supercomput. **74**(1), 65–70 (2018)

[63] Wu, X.W., Yang, E.H., Wang, J.: Lightweight security protocols for the Internet of Things. In: 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1–7 (2017)

[64] Yassein, M.B., Shatnawi, M.Q., Al-zoubi, D.: Application layer protocols for the Internet of Things: A survey. In: 2016 International Conference on Engineering MIS (ICEMIS), pp. 1–4 (2016)

[65] Zheng, P., wang, H., Sang, Z., Zhong, R.Y., Liu, Y., Liu, C., Mubarok, K., Yu, S., Xu, X.: Smart manufacturing systems for industry 4.0: Conceptual framework, scenarios, and future perspectives. Frontiers of Mechanical Engineering **13**(2), 137–150 (2018)

[66] Zhong, R.Y., Xu, X., Klotz, E., Newman, S.T.: Intelligent manufacturing in the context of Industry 4.0: A review. Engineering **3**(5), 616 – 630 (2017)

[67] Zhou, W., Zhang, Y., Liu, P.: The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. CoRR **abs/1802.03110** (2018)

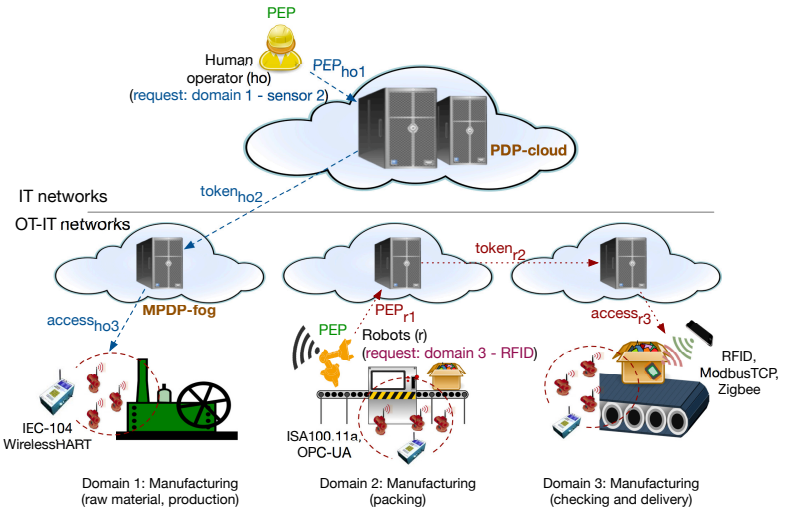

Figure 2: Connection between: Entities, cloud server and fog servers

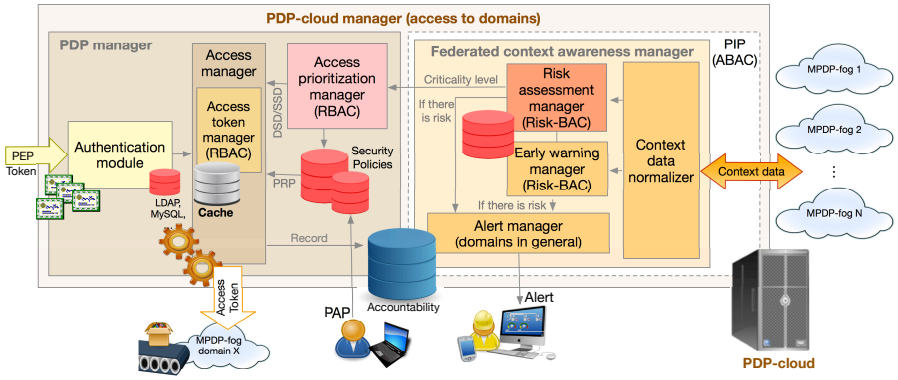

Figure 3: PDP-cloud: Architecture and functional components

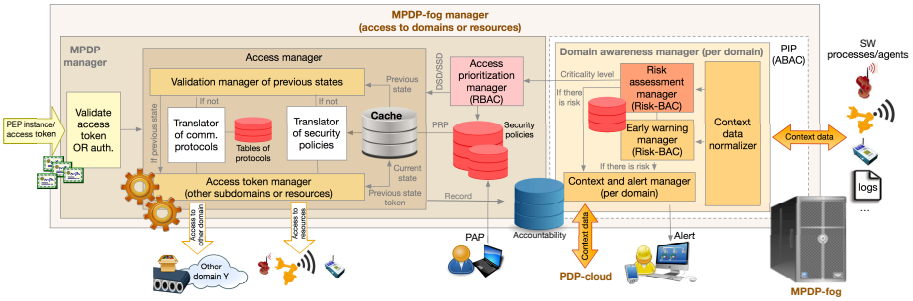

Figure 4: MPDP-fog: Architecture and functional components