C. Alcaraz, and J. Lopez, "Secure Interoperability in Cyber-Physical Systems", *Security Solutions and Applied Cryptography in Smart Grid Communications, IGI Global, USA*, pp. 137-158, 2017.
http://doi.org/10.4018/978-1-5225-1829-7.ch008
NICS Lab. Publications: https://www.nics.uma.es/publications

Secure Interoperability in Cyber-Physical Systems

Cristina Alcaraz
Computer Science Department,
University of Malaga, Spain
alcaraz@lcc.uma.es

Javier Lopez
Computer Science Department,
University of Malaga, Spain
jlm@lcc.uma.es

ABSTRACT

Transparency in control transactions under a secure network architecture is a key topic that must be discussed when aspects related to interconnection between heterogeneous cyber-physical systems (CPSs) arise. The interconnection of these systems can be addressed through an enforcement policy system responsible for managing access control according to the contextual conditions. However, this architecture is not always adequate to ensure a rapid interoperability in extreme crisis situations, and can require an interconnection strategy that permits the timely authorized access from anywhere at any time. To do this, a set of interconnection strategies through the Internet must be studied to explore the ability of control entities to connect to the remote CPSs and expedite their operations, taking into account the context conditions. This research constitutes the contribution of this chapter, where a set of control requirements and interoperability properties are identified to discern the most suitable interconnection strategies.

Keywords: Cyber-Physical Systems, Interoperability, Secure Interconnection, Control Systems, Authentication, Authorization, Control Access, Internet of Things.

INTRODUCTION

In the last few years, we have witnessed how the advent of new technologies, such as the Internet and wireless communication infrastructures, has radicalized the current control systems, the infrastructures of which are becoming smarter with a strong dependence on heterogeneous cyber-physical systems (CPSs). CPSs are collaborative systems comprising autonomous and intelligent control devices (e.g., smart meters, gateways, servers working as front-ends, remote terminal units (RTUs), sensors, smart industrial engineering devices, mobile robots, smart-phones, and many other cyber-physical control elements) capable of managing data flows and operations, and monitoring physical entities integrated as part of critical infrastructures (CIs). A Smart Grid system is a clear example of the composition of these systems based on complex communication infrastructures (Yan et al., 2012). Their technologies, from diverse vendors or manufactures, manage a set of fundamental services according to the real demand, facilitating

effective energy production, the management and notification of electricity pricing, as well as the provision of customizable services to end-users.

However, the composition of diverse types of networks requires addressing aspects related to the interoperability, so as to ensure control from anywhere and at any time. Cyber-physical devices located at different locations should be managed irrespective of the types of devices and protocols, and they must allow control entities to assist in a situation when needed. To address this heterogeneity, it is necessary to include a set of fundamental requirements linked to the underlying interconnection system, among them: authentication, authorization and policy management because (i) any unauthorized access to restricted devices may become a threat, and (ii) authorized access under different policies may hamper the monitoring tasks. Intermediary policy enforcement systems with support for dynamic access could be an easy way of ensuring interoperable communication between different CPSs. If, in addition, the context has to consider dynamic access, the resulting system is a decision-making system with the capability to adapt the access to the type of context. These fundamental conditions are primarily related to the connectivity phase in which control entities may require the absolute connection with the desired destination node; and this connection is strongly linked to the privileges assigned to the control entities (human operators, processes), the intentions of these entities in the field and the contextual conditions.

However, the construction of specific interoperability architectures may lead to certain questions related to: (i) whether these architectures may directly connect with the end cyber-physical devices instead of going through the main interfaces (gateways or front-ends) that generally comprise the current control systems; or (ii) to directly connect with the control devices (e.g., RTUs, sensors, actuators). To do this, it is necessary to analyze the existing interconnection strategies of CPSs to the Internet to determine which approach is the most suitable for maintaining the interoperability in restricted control contexts, assessing the connection level and timely access in extreme situations. The result of all this research constitutes the main contribution of this chapter, which is organized as follows. First, we contribute with a generic interconnection architecture based on decision points, so as to provide the architectonic basis required for subsequent research. In the third section, we identify the control requirements that all CPSs and their devices have to comply with, and present the different interconnection strategies to substations (where the CPSs are deployed). Lastly, we evaluate and discuss the properties of the CPSs in the fourth section according to the present constraints of the control systems, and provide the conclusions and future work.

SECURE INTEROPERABILITY: DIVERSITY, INTERACTION AND COLLABORATION

As mentioned, in the majority of CIs and their physical systems all activity must be supervised, either locally or remotely, by complex and decentralized monitoring systems comprising large and small communication infrastructures. All these infrastructures base their communications on wired and wireless infrastructures, and are responsible for transferring evidence from one point of the CI to another. The back-haul and the Internet constitute, in this case, the main communication infrastructures that connect the different network distributions, while wireless technologies favor the monitoring and control transactions at local. The result is a road-map of interconnections comprising two heavily interconnected systems based on both cyber and physical elements.

Cyber-physical devices: Technologies and Communication Systems

The new smart CPSs adapted to the new Industry bring about fresh research challenges: *to provide connectivity without compromising the operating performance, security and safety-critical of the underlying systems* (Alcaraz & Lopez, 2012). For example, data streams have to be transmitted between

different types of networks and computed on different types of devices with very different computational capacities (Alcaraz et al., 2015). Specifically, cyber-physical devices can be categorized according to their software (SW) and hardware (HW) capacities:

- *Weak*: it corresponds to those devices that are extremely constrained computationally but have sufficient capacity to run simple (arithmetic and logical) operations or predefined instructions.
- *Heavy-duty:* includes those devices that are relatively expensive from a computational point of view whose components are able to execute simple or complex operations or processes. Within this category, the industrial WSNs (IWSNs) are considered as an alternative, fundamental to the control. Their communications, mostly dependent on gateways, can support diverse communication standards, such as ZigBee PRO/Smart Energy (Zigbee, 2010), WirelessHART (HART, 2010) and ISA100.11a (ISA, 2010), and all of them rely on the IEEE 802.15.4 technology (IEEE, 2006). These CPS-specific protocols share certain functions and topologies, such as secure connectivity through symmetric and asymmetric cryptography, capacity to gain local access in substations and compatibility with 6LowPAN (Montenegro et al., 2007), energy saving, coexistence with other systems, data reliability and mesh communication (Alcaraz & Lopez, 2010).
- *Powerful-duty*: contains all those devices with significant and sufficient capacity to address any complex operation with a significant computational cost.

Table 1 Typical cyber-physical devices and protocols

Weak	**Heavy-duty**	**Power-duty**
~ 4MHz, 1KB RAM and 4KB-16KB ROM (home-appliances, sensors)	~ 13MHz-180MHz, 256KB-512KB RAM and 4MB-32MB ROM (RTUs, smart meters, concentrators), or ~ 4MHz- 32MHz, 8KB-128KB RAM, 128KB-192KB ROM (industrial wireless sensor networks (WSNs))	Working at GHz with more than 2 processors per system and with at least a cache per processor, 16-32 GB RAM (servers, proxies or gateways)
6LowPAN	Zigbee PRO/Smart Energy Wireless HART ISA100.11a 6LowPAN Modbus-TCP/IP, DNP3, IEC-104 TCP/IP	TCP/IP Modbus-TCP/IP, DNP3, IEC-104 Zigbee PRO/ Smart Energy Wireless HART ISA100.11a

Table 1 summarizes the computational differences of existing CPSs and the diversity in their communications; where connection to the real world is generally reached through specific interfaces. These interfaces can range from gateways to traditional servers working as front-ends (e.g., data concentrators or RTUs). In this context, any adversarial influence may impact on the availability of resources given that the main interfaces are generally considered as single failure points. Any congestion could isolate the network, and interrupt control activities such as the typical 'store-and-forward' between RTUs. This also means that the availability of the different control points is critical to ensure controllability from anywhere at any time, meaning that security is a key requirement for interconnection. One easy way to ensure this requirement in a complex interoperability architecture would be through the following components (Alcaraz et al., 2016a):

- **Authentication and access control** across the different distributions, considering the existing network topologies and the different roles of the control entities, which may also be mobile.

- **Authorization** is a security concept that allows interconnected systems to check and prove the identity of an entity, either a process or a human operator, and its rights to manage critical data associated with measurements, alarms, events or instructions.
- **Interoperability** is, contrarily, a property related to compatibility, where interfaces can interact and work with each other, not only in the present but also in the future without any type of access or implementation restrictions, in addition to permitting useful information to be exchanged between interfaces.

The composition of these three requirements comprises the functional stages of any policy enforcement point (PEP) together with its distributed policy decision points (PDPs). A PEP corresponds to a network device in which policy decisions are established according to the kind of access and its permissions. However this policy enforcement also depends on the decision taken by the PDPs in charge of evaluating and issuing authorization decisions.

Policy Enforcement Point: Architecture and Connectivity

The architecture that we consider here is decentralized, where the interconnection of CPSs is basically focused on a few proxies (see Figure 1). These proxies, linked to the functionality of the PDPs, are responsible for connecting different types of networks, offering peer- to-peer communication and relaying via the Internet. However, the connectivity to the different individual elements that comprise the CPSs is not always established through a direct connection from PDPs. Rather these connections are carried out through intermediary nodes serving as front-ends or gateways (as was stated in the previous section), which are in charge of controlling all the incoming and outgoing connections from their networks towards their closest PDPs. However, these connections must be restricted under specific authentication and authorization procedures, following access control schemes like those recommended by the IEC-6235-8 (IEC-62351, 2007).

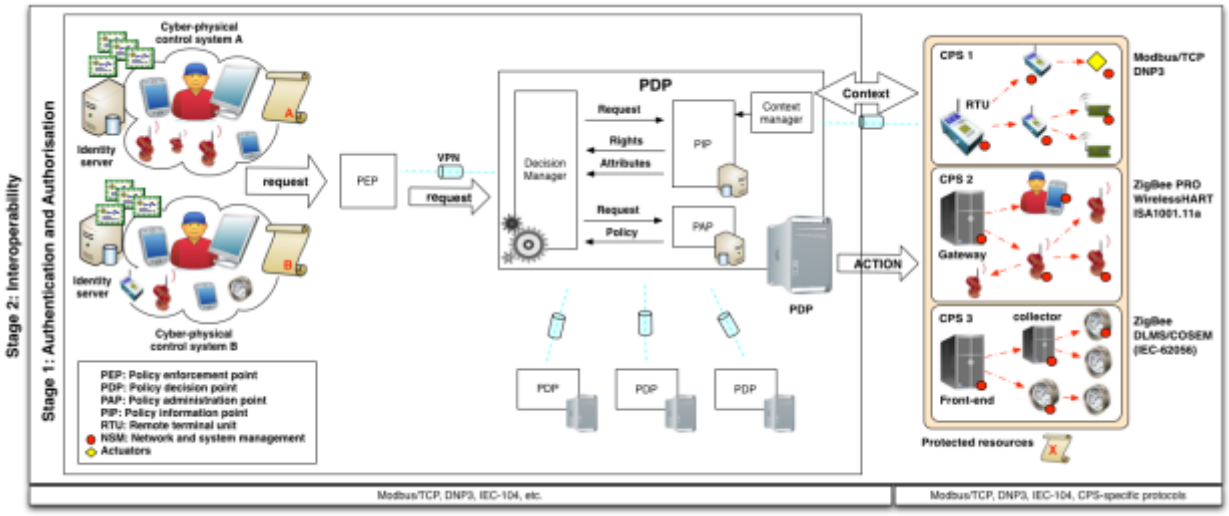

Figure 1. General architecture for distributed cyber-physical control systems

The IEC-62351-8 is part of the IEC-62351 series (IEC-62351, 2007) that establishes end-to-end security in control systems and the protection of the communication channels. Concretely, the IEC-62351-8 recognizes the RBAC model as a potentially efficient mechanism for wide use in control systems and distributed services. Only authorized users and automated agents can gain access to restrictive data objects, which may be located at distant geographical points and close to the observation scenario.

Moreover, through RBAC it is possible to reallocate system controls and their security as defined by the organization policy, where the purpose is: (i) to introduce authorization aspects under the condition of subjects-roles-rights where a limited number of roles can represent many entities, and roles can be assigned to entities by non-expert personnel (Coyne & Weil, 2013); (ii) boost role-based access control in the power system management; and (iii) enable heterogeneity and audited interoperability between the different elements of a CPS (sensors, meters, etc.).

Table 2. Roles and permissions established by the IEC-62351-8 standard

Roles	**View**	**Read**	**Dataset**	**Reporting**	**Fileread**	**Filewrite**	**Filemgnt**	**Control**	**Config**	**Settinggroup**	**Security**
Viewer	✓			✓							
Operator	✓	✓		✓				✓			
Engineer	✓	✓	✓	✓		✓	✓		✓		
Installer	✓	✓		✓		✓			✓		
SECADM	✓	✓	✓			✓	✓	✓	✓	✓	✓
SECAUD	✓	✓		✓	✓						
RBACMNT	✓	✓					✓		✓	✓	

Viewer	Capacity to view data objects.
Operator	Capacity to view data objects and values, and perform control.
Engineer	Capacity to view data objects and values, access datasets and files, and configure servers.
Installer	Capacity to view data objects and values, write files and configure servers.
SECADM	Capacity to manage users-roles-rights, and change security setting.
SECAUD	Capacity to audit the system by viewing audit logs.
RBACMNT	Hereditary role from the SECADM with only the ability to manage roles and rights.

However, RBAC can be problematic when the application context is dynamic, where the access is limited to contextual states such as the saturation or isolation degree in substations, or the availability of nodes or objects. In this case, ABAC could solve these weaknesses by simplifying the model and applying labelled objects and dynamic attributes instead of permissions, and complement the tasks of RBAC by considering roles as attributes. Notwithstanding, ABAC has certain limitations in accountability terms where it is not possible to audit which entities have access and what permissions have been granted to an entity (Coyne & Weil, 2013). So the implementation of both approaches together could be a good approach to promote their potential features. To combine them, it is necessary to define specific rules to control the different access modes, which, in turn, have to be instanced according to the characteristics of the context. In this case, the decision managers of both approaches must be integrated inside the policy information points (PIPs), where the PIP modules have to determine the type of permission for a specific entity and the associated attributes, which are primordially related to the characteristics of the context.

This is also represented in Figure 1, where each entity belonging to an infrastructure or CPS has to authenticate itself to its own identity server corresponding to its own infrastructure. At this point, IEC-

62351-8 recommends depending on a third entity (e.g., the security administrator) responsible for assigning roles to subjects and managing access tokens; generating and maintaining the basic security credentials (e.g., the typical tuple, username and password) in conjunction with X.509 certificates. If this first stage for the interconnection is overcome, the identity server provides an authentication token holding the information related to the requester and the protected object/device in the destination.

Once the authentication token has been obtained, the requester needs to have the tools necessary for access in the field. For that, a PEP service associated with the infrastructure has to be connected with the closest PDP with connectivity to the remote substation. When the PEP service establishes such a connection, the decision manager of the PDP has to first validate the authentication token (e.g., verify the entity and check the correctness of the token such as its type, size, content and format) and obtain information from the PIP module to proceed with the authorized connection. This authorization contains the final access decision managed by the decision manager in charge of computing: (i) the heterogeneity of the system, (ii) the information provided by the PIP module, and (iii) the security policies (e.g., IEC-62351-(4-6)) and the actions (see Table 2) given by the policy administration point (PAP). The information provided by the PIP module is related to the type of permission associated with the role of the requester and the attributes related to the natural state of the context requested. Observing Figure 1 it is possible to see that a great deal of this information can come from the context manager, also restrained inside the PIP modules. These managers are responsible for periodically examining the state of the application context, as well as the degree of criticality and/or accessibility of the resources, such as nodes and links. Although this information is crucial to determine the level of access to an entity, it also requires that the gateways periodically validate their contexts where the states may be subject to NSM (network and system management) objects, also defined as part of the IEC-62351-7 standard.

NSM objects are dynamic processes running through the different cyber-physical systems to monitor the health of the critical systems and their subsystems. The information from these objects should be managed for each CPS so as to detect possible anomalies that should be notified to the closest context managers. Depending on the context, the interconnection system can, in addition, activate one of the special functional features of RBAC, known as dynamic separation of duties (DSD). DSD allows multiple mutually exclusive roles (e.g., either Engineer or Operator) working independently but not at the same time or simultaneously. In this way, in crisis contexts only authorized personnel with capacity for the ‘control’ (see Table 2) is able to gain access, thereby avoiding bottlenecks and delays in the operational tasks. However, there may be the extreme case in which the rate of congestion may become quite notable, and the main interfaces (gateways, front-ends) may not be able to connect to the primary PDPs. In this case, one possible solution would be to let the cyber-physical devices with TCP/IP or 6LowPAN compatibility to promptly connect with the context managers integrated as part of the PDPs. To determine this possibility and its validity for holistic protection of the entire system, the remainder of this chapter focuses on analyzing the different connection measures and the current constraints of the context.

REQUIREMENTS AND INTEGRATION STRATEGIES FOR INTEROPERABILITY

There are currently several ways to connect cyber-physical elements to the Internet and, therefore, several interconnection strategies that enable the connection to different control entities (Christin et al., 2009). However, the process of determining which strategy is more effective for an architecture deployed within a CI can also require assessing the effectiveness of the existing approaches according to specific requirements of the application context and the interoperability requirements.

Control and Automation Requirements

Five control requirements are defined in (Alcaraz & Lopez, 2012) and considered in this study: two of them related to operating performance, i.e., real-time performance and sustainability, and three associated with security, i.e., dependability, survivability and safety-critical. The nature of these requirements, however, also obliges us to consider a subset of attributes associated with the control and the characteristics of the CPSs, since they can all have a direct influence on the properties of interoperability and automation. For example, any new upgrade of the system not only involves important changes to the network architecture, but also significant overheads in the end-devices, where any intermediary connection process (e.g., agreement algorithm, access control, authorization, and policy management) and the TCP/IP-based routing may result in important delays in the control. Given this, this section introduces the basic requirements that both control systems and CPSs must consider:

- **Real-time performance** subject to certain operational deadlines and delays, and linked to the effectiveness of the maintainability, upgrading of the system and the interoperability of its components. At this point, we consider the overhead as a main attribute where (i) it is essential to comply with a suitable trade-off between the number of devices and their overall cost within the system, and (ii) the devices should not have an excess of workloads and unnecessary resources. Within this requirement, we identify three properties:

    - *Computational overhead* to comprise those technological capacities (e.g., memory, CPU cf. Table 1) that are needed within an end-device to implement specific control algorithms, applications and protocols, such as NSM, ZigBee, DNP3 or ISA100.11a. Note that in the PDPs, the computational cost invested in the negotiation algorithms and policy management also has a direct effect on the time needed for the access.
    - *Communication overhead* includes all those characteristics associated with a wireless communication channel, such as bandwidth, delays and complexities related to the header size of the protocols. For example, most of the devices shown in Table 1 follow the IEEE 802.15.4 standard with a transfer rate of 250 Kbit/s, and others can manage various protocols (e.g., Modbus-TCP/IP) complicating the header space, thus reducing the bytes available for the transmission of data. Moreover, the abuse of the channel and the authorized access through specific roles may also increase the rate of communication overhead between the PDPs and the main interfaces, thereby producing significant congestions in the substations.
    - Efficient *responsiveness* by optimizing resources and protocols. Concretely, this property is related to the functional features of the existing CPS-specific protocols (e.g., WirelessHART), which deal with the specific characteristics of the application context and its networks to promote their best services (Alcaraz & Lopez, 2010), such as: redundancy, link robustness through frequency hopping and blacklisting methods, control of packet collisions through a specific TDMA (time division multiple access) with a fixed time-slot, routing discovery, low-duty cycle, maintenance tasks through hand-held devices, prioritization and alert management, as well as diagnostic mechanisms with support in NSM objects. This optimization in PDPs is related to the optimization of PIP and PAP modules, and the decision managers.

- **Sustainability** defined as "*that development that is able to meet the needs of the present without compromising the ability of future generations to meet their own needs*" in (UNGA, 2007); i.e., the system has to continue to function like the day it was deployed irrespective of any extension of components or systems, updates, upgrades or modifications. Its main properties are:

    - *Maintenance* corresponds to the ability of the system to update resources, prevent the occurrence of faults and errors caused by vulnerabilities, or upgrade services through patches. To do so, the system must locally and/or remotely validate the functionality of

resources and periodically test functions. The properties associated with maintainability are:

- *Addressing* through unique identifiers to locate and reach up processes and cyber-physical devices. Therefore, this property is linked to how the different nodes are accessed and who is responsible for storing and managing these identities.
- *Access* to (locally or remotely) address validation tasks of resources. This also means that this property is concerned with the current complexity of accessing the cyber-physical devices through IP connections or specific protocols.
- *Maintainability*, to the contrary, focuses on all those upgrading, updating, modification and optimization processes of HW/SW components. So this property aims to consider the number of changes or improvements made to a CPS.

- *Scalability* and *extensibility* with regard to the capacities of the system to add new HW and SW components, respectively. Substations composed of complex CPSs tend to last for a long time, and this entails adapting new devices, applications, services and objects.
  - As part of the scalability, *mobility* is an elemental property to be considered here. It is related to the system's capacity to permit the dynamic access in wireless networks. Any new joining or leaving from the network should not impact on the overall performance of the network. This property is in turn linked to rapid *addressing* in the field and the *access* at local or remote.

- **Dependability** defined as "*the ability of the system to properly offer its services on time, avoiding frequent and severe internal faults*" in (Al-Kuwaiti, 2009), includes reliability, maintainability, safety and security as main attributes. The first attribute is detailed below, and the rest, except maintainability, are described later.

  - *Reliability* is a concept that refers to the capacity of the system to offer its services within desired quality thresholds, irrespective of the criticality of the context. Concretely, this property holds two fundamental properties:
    - *Availability* of data, resources and links, but focused on terms of fault-tolerance through redundancy strategies, and on terms of security through defense and self-healing mechanisms. If a resource does not offer the correct service at a given moment, then the resource will be unavailable and therefore unreliable. Moreover, if this situation is not controlled properly, it may take on a corrosive nature, since control components are closely interconnected, exponentially increasing the costs of maintainability.
    - *Robustness* through preventive and corrective measures, where the repair of states and parameters must be achieved in an acceptable time average and at an acceptable quality. This property is closely related to resilience and self-healing because it allows the system to continue its services, despite security breaches caused within the system.

- **Survivability** comprises "*the capability of a system to fulfil its mission and thus to face malicious, deliberate or accidental faults in a timely manner*" in (Knight & Strunk 2004). Note that this feature is what distinguishes it from dependability. Survivability is part of the dependability, but in this case, dependability is intended to provide services in the presence of internal faults, which may be later exploited by malicious actions. Under this concept, a survivable system also assumes as attributes, resilience, availability - both described above -, safety and security, but here we primarily focus on security. In this sense, if the security is not fully addressed, any threat may potentially impact on the control and its performance, harming

not only the safety of the CI itself, but also social and economic welfare. As this may also affect the integrity of the system itself, only authorized entities with restrictive permissions (IEC-62351-8, see Table 1) should have access to execute, modify or read sensitive data, and any action in the field should be subject to accountability. Therefore, its properties are as follows:

  - *Secure channel* includes all those security mechanisms and services (e.g., cryptography, key management systems, virtual private networks (VPNs) or firewalls) that favor the confidentiality and integrity of communication channels. And this compromise involves not only the security of communication channels of the CPSs but also the channels between PDPs and CPSs.
  - *Authentication* and *authorization*. Both properties deal with the types of mechanisms (e.g., decentralized in PDPs), credentials (e.g., certificates, keys) and tools (e.g., RBAC, ABAC) that can be used to validate identities and verify whether a given entity is able to perform a determined operation in a cyber-physical device, in a process or in an object (e.g., IEC 61850).
  - *Detection* and *response* refer to the main traceability structures and inspection of packets, as well as all those mechanisms that permit the automatic response to incidents with support for alert management (Alcaraz & Lopez, 2016b). At this point, NSM objects may have a significant influence on the detection processes.
  - *Accountability* to log any activity in the system, and includes the use of specific accountability protocols and external systems to offer support for massive critical data streams. These systems can range from simple systems (local servers, external hard devices) to complex infrastructures such as cloud-computing or fog-computing.
  - *Trust* and *privacy* due to the need to collaborate between cyber-physical devices. Both properties are related to the nature of the mechanisms, where trust management systems help measure the degree of collaboration; whereas privacy schemes prevent or reduce the exposure of sensitive data (e.g., energy usage) or the location of nodes.

- **Safety-critical** contemplates "*those systems that can potentially lead to serious consequences due to the existence of unplanned events, which could result in human deaths or injuries, or even significant physical damage*" (Bowen & Stavridou, 1993). This requirement embraces all those basic protection requirements described above, in order to manage the preparedness and mitigation of a critical system against advanced threats.

Once the control requirements have been addressed according to the properties of the CPSs, four interoperability requirements can be identified: (i) *ease and speed* of access; (ii) *transparency* in and during the connection; (iii) *availability* of resources (links and nodes) and data; and (iii) *reliability* of the communication. The access is related to the capacity of the system to gain virtual access to specific devices and operate through them in the field. Any overhead in the computation and/or communication in the destination nodes may affect the access, so there is an intrinsic dependence between the properties of cyber-physical networks and the interoperability properties. Precisely, Table 3 shows this characteristic, in which it is possible to see how the network properties, corresponding to the performance, sustainability and dependability of control systems, have a certain repercussion on the access.

As for communication, it concerns the capacity of the system to offer communication resources and robustness in case of an emergency, where there exists the probability of activating the DSD mechanisms to permit the access to restricted entities (e.g., Operators or SECADM), devices or objects. If the communications are feasible, it is also necessary to consider the capacity of the end-nodes to properly manage and process actions on time. A great deal of this communication can be related to the context, where context managers (linked to or integrated inside PIPs) can request general conditions about the nature of the network and their devices, and in this way establish the access or activate the DSD in

extreme cases (e.g., congestion or isolation of areas, inoperative devices, manipulation of variables, etc.). So the management of NSM objects throughout the network is crucial to maintain a correct functionality in PDPs y CPSs, and therefore, the access in the field.

Table 3 Dependence on control requirements and interconnection properties

	Performance			**Sustainability**					**Depend**		**Survivability**						
Interoperab.	Comp. overhead	Com. overhead	Responsiveness	Scalab. & extensib.	Mobility	Addressing	Access	Maintainability	Availability	Robustness	Secure channel	Authentication	Authorization	Detection & response	Accountability	Trust	Privacy
Rapid access	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Transparency				✓	✓	✓	✓	✓				✓	✓				
Availability	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓				
Reliability	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Interconnection Strategies between PDPs and CPSs

To address the interoperability, it is necessary to analyze the existing interconnection strategies that help Internet entities connect to the different elements of a CPS. Currently, there are five connectivity models, classified as *stack-based* and *topology-based* (see Figure 2) (Christin et al., 2009). In the stack-based class, the remote interconnection depends on the topological characteristics, the protocols and the capacities of the nodes; whereas the topology-based connectivity depends on the location of those nodes that provide access to the Internet.

Concretely, the stack-based class holds three approaches: *front-end* (**SbC-1**), *gateway* (**SbC-2**) and *TCP/IP* (**SbC-3**). The front-end solution, still in force in substations, permits control entities (e.g., SCADA centres) to reach CPSs without communicating directly with each other. In this scenario, the CPSs are completely independent from the Internet and can implement their own stack of protocols (e.g., ZigBee, ISA100.11a, or WirelessHART). This allows the front-ends to act as intermediary nodes with the capacity to interpret communication protocols and serve as data concentrators. The gateway solution, to the contrary, translates the lower layer protocols (e.g., TCP/IP and CPS-specific protocols, or legacy protocols and CPS-specific protocols) and routes the information from one point to another, separating the control network from the Internet. In this sense, PDPs and cyber-physical devices or processes can exchange information without establishing a direct connection, where any operational transaction needs to traverse the gateway to convert the input request in a packet that can be understood by the destination node.

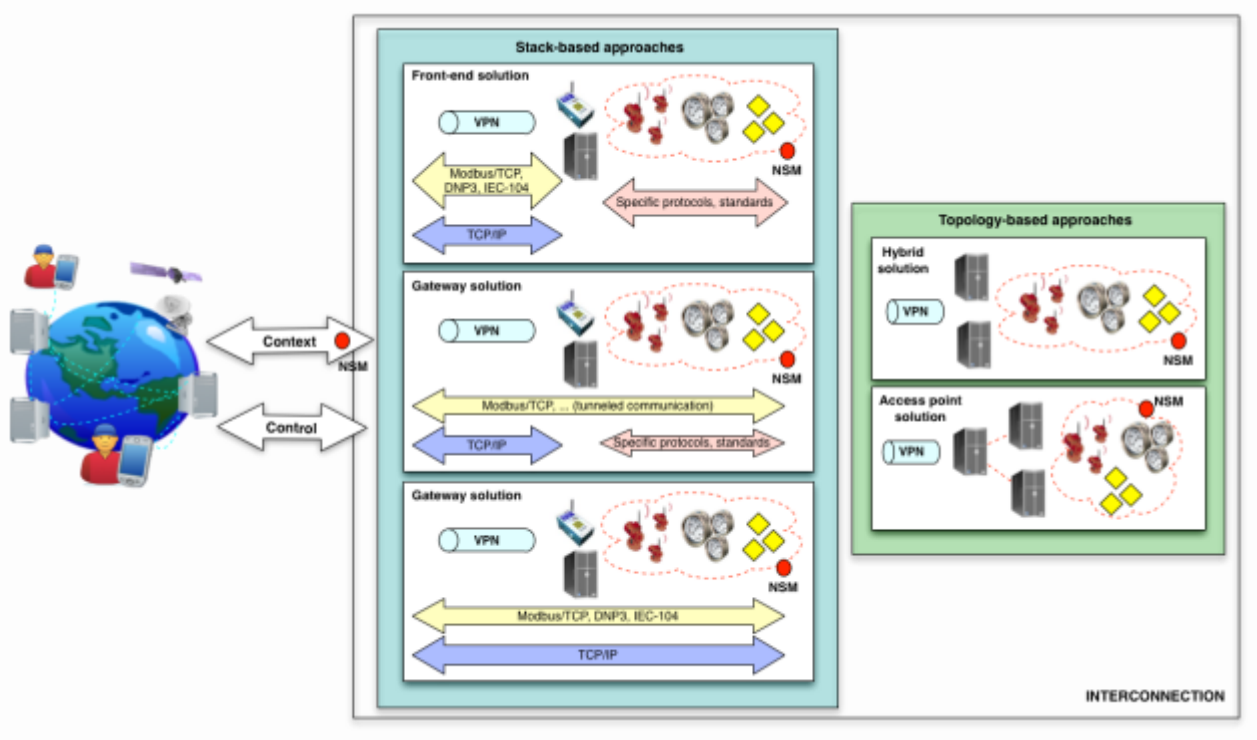

Figure 2. Interconnection strategies

As for the third approach, the TCP/IP solution, it assumes that cyber-physical devices are able to implement the TCP/IP stack or have a certain compatibility with 6LoWPAN, promoting the paradigm of the *Internet of Things* (IoT) (Ovidiu, 2009). In this way, the application context remains fully integrated in the Internet via IPv6 or 6LowPAN, where PDPs, Internet entities (e.g., human operators, the central system or processes) and cyber-physical elements (e.g., smart sensors) can establish a direct connection with each other. However, this characteristic unfortunately does not always work. The approach still relies on the computational capacities of CPSs to support the TCP/IP stack and its payloads, in which devices classified as weak or heavy-duty may have certain difficulties to adapt the stack.

Regarding the topology-based classification, it comprises two kinds of approaches: *hybrid solutions* (**TbC-1**) and *access point* (**TbC-2**) solutions. The hybrid solution assumes the existence of a few nodes within the network with the ability to directly access the Internet. Generally, these nodes are associated with front-ends, where the devices have to traverse them to connect with the control entities, and vice-versa. The specific features of this type of approach are related to its capacity to offer redundancy (more than one front-end or gateway) and autonomy by allowing each substation to implement its own intelligence. On the other hand, when hierarchical CPSs can be built, it is advisable to consider the access point solution, where the top of the tree is composed of Internet-enabled nodes (backbones) and the connection to the Internet is done through them. The backbones permit the adaptation or addition of complex resources, in addition to implementing faster and more complex networks (e.g., WiFi, Bluetooth), through which human operators can connect using hand-held interfaces. Note that hybrid configurations are also possible, except for TCP/IP solutions, where a backbone-type distribution with the Internet-enabled nodes can act as front-ends, isolating the CPS from the Internet, or as gateways, allowing direct data exchange between control entities and cyber-physical devices.

INTERCONNECTION BETWEEN SYSTEMS: ANALYSIS AND DISCUSSION

Assuming the functional features of the PDPs to manage access requests according to privileges and the contextual conditions of the destination network, this section analyzes the benefits and drawbacks of the interconnection strategies, taking into account the control and interoperability requirements introduced in previous sections.

- **Real-time performance** supported by the properties related to computational and communication overhead, the optimization degree of the underlying protocols and the algorithms implemented. However, the effectiveness of these properties heavily depends on the architecture defined for the interoperability and the computational capacities of the devices. For example, although the authentication in the PDPs can be done using (i) a PULL model (first gains access to the cyber-physical control object so that it can authenticate the identity of the requester using the authentication servers) or (ii) a PUSH model (first fetches the access token from the identity servers before accessing the objects), the on-demand PULL model requires additional communication for the authentication, resulting in quite a costly procedure (Hong et al., 2009). And if, in addition, PDPs connect with areas based on heavy-duty devices (e.g., RTUs), these may have certain capacities to support solutions that demand enough intelligence to: (i) execute control applications, security services (cryptography primitives, link-layer security, end-to-end security, authentication and authorization (both in local), accountability, detection mechanisms, etc.) and diagnostic mechanisms; and (ii) implement the TCP/IP stack and/or legacy protocols (e.g., Modbus-TCP, DNP3). These computational features vary significantly in weak devices, where large and complex operations may not be processed properly. Moreover, these HW/SW differences also affect the connectivity model, and concretely *stack-based* ones (**SbC-1/-2/-3**) or *topology-based* ones (**TbC-1/-2)**.

  Communication overhead also heavily depends on the design of the network. The interoperability architectures should be built following the cache philosophy in which front-ends or gateways (**SbC-1/-2**) not only serve as mere interconnection interfaces but also as data storage interfaces for the rapid provision of data or actions in the field. Nonetheless, the processing of packets in such interfaces (i.e., in **SbC-1/-2/-3**) may add an extra penalty to the overall performance of the CPSs. Concretely, this penalty in TCP/IP solutions (**SbC-3**) is limited to the size of the 6LowPAN headers − of the current industrial protocols are compatible to 6LowPAN (e.g., ISA100.11a) −, and **SbC-1/-2** solutions depend on the optimization of the local headers of the CPS-specific protocols and on header compressors (optional). On the other hand, the functional features of the communication infrastructures also help the correct functioning of the automation and monitoring tasks. For example, high-speed communication technologies (e.g., the use of back-hauls for large distances, and the use of 802.15.4-based networks working at 250 Kbit/s and 802.11b-based networks at 11 Mbit/s for local control) allow rapid data management.

  Optimization of services is also essential to reduce overheads. Many of the current communication protocols (e.g., WSN-specific protocols) are designed to optimize resources, the use of which can improve the behavior of all the interconnection solutions (**SbC-1/-2**, **TbC-1/-2**), except for those based on **SbC-3** where the routing is associated with IP addresses. In addition, WSN-specific protocols generally define their own MAC layer services. For example, WirelessHART and ISA100.11a implement a specific TDMA with a fixed time slot to improve the quality of service of the data-link layer, a hopping/blacklisting method to avoid disturbances in the channel, and a redundant mesh routing (Alcaraz & Lopez, 2010). Likewise, the optimization of interoperability services incorporated inside PDPs is also key to reducing the access time in the field. For example, the implementation of rule-based expert systems to manage authorization aspects according to the security policies could be a good approach. Intelligent

engines could manage different security policies associated with different CPSs and manage the access according to their security policies.

- **Sustainability** led by the properties related to scalability, extensibility and maintenance. It is clear that any rise in terms of resources and services, certainly adds functional complexities to the access. Fortunately, this increase does not necessarily hamper the inclusion of new interconnection services to the Internet. Namely, for the inclusion of new members or the leaving of existing nodes, **SbC-1/-2** only require updating the routing table and the mechanisms of the CPS-specific protocols in the main interfaces of the network (front-ends, servers or gateways); whereas **SbC-3** requires updating the routing table of each Internet-enabled device. **TCb-1/-2** is similar to **SbC-3**, but if the communication infrastructure is totally distributed, the changes made within the table have to be addressed in all the end-devices or depend on centralized interfaces. Regarding extensibility, this property largely depends on the capacity of the nodes to add or adapt new SW services.

  The properties associated with maintenance are addressing, (local or remote) access and maintainability. For the management of addressing, both **SbC-1** and **SbC-2** require translating the identities (e.g., ID in DNP3 Address to ID in WirelessHART EUI-64 Address) from substations; whereas in **SbC-3** the translation is managed from the central system to open a direct connection with the devices in the field. The complexity increases in decentralized networks, i.e., in the **TbC-1/-2** approaches, as it is necessary to replicate the translation tables in the Internet-enabled nodes or to create a centralized service that provides a translation interface.

  Regarding the access, if human operators, with the roles of Engineer, Installer or SECADM (or RBACMNT) have to have access in the field to manage maintenance tasks (e.g., with permissions of configuration − cf. Table 2) via PDPs or locally, they can use the device to execute data retrieval services. In distant controls, these entities particularly have to request the access through intermediary interfaces (gateways/front-ends) and establish TCP/IP direct connection with the network devices. If the communication is, to the contrary, done locally, operators can take advantage of the local services of the CPS-specific protocols. They can, for example, use the services offered by the internal protocols through external connections offered by other networks, such as mobile ad hoc networks, to gain access to the front-end or the gateway (**SbC-1/-2**). In contrast, in **SbC-3**, the access has to be carried out through specific addresses, the IP of which has to be known beforehand; and in **TbC-2** there exists the need to know the location of the interface that manages the services/data of the node that human operators want to connect to.

  As for SW upgrading, this can be executed from the central system to all the interconnection architecture, including PDPs and the CPSs. And in this case, the effectiveness of the updates depends on the interconnection strategies. For example, **SbC-1** and **TbC-2** are the simplest solutions, as the updating is only carried out in one device (the front-end or backbone node, respectively), but this process unfortunately disables the access. This drawback does not appear in **SbC-2**/**-3** and **TbC-1** since the updating is gradually addressed in each network device.

- **Dependability** is a fundamental property for context managers, which receive network status directly from gateways and front-ends (**SbC-1**/**-2**), or directly from Internet-enabled cyber-physical devices. To ensure this, dependability has to be supported by the properties related to availability and robustness, but the notion of availability is a weak property in **SbC-1** and **SbC-2**. Both front-ends and the gateways are single failure points where attackers may consciously launch denial of services (DoS) attacks, leaving the network uncontrolled from the remote point of view. But even so, the smart nature of many of the nodes belonging to the **SbC-2** solution may allow the underlying system to temporarily work in a standalone fashion, as happens with

IWSNs. So, an easy way to overcome the problem in **SCb-1**-based networks would be through the replication of the main interfaces, as provided by the **TbC-1** solution.

Other replication-based strategies for resilience are, for example, (i) checkpoint-based rollback with dependency on storage points (e.g., concentrators of **SbC-1/-2** or external infrastructures such as cloud-computing), or (ii) log-based rollback (also known as message logging protocols) composed of checkpoints and a record of non-deterministic events (Bansal et al., 2012) (Treaster, 2005). However, the checkpoints are, in general terms, expensive and experts like Ruchika in (Ruchika, 2013) and Veronese et al. in (Bessani et al., 2009) recommend applying heterogeneous replication-based checkpoints to enhance performance and guarantee tamper-resistance to faults.

This also means that the implementation of robust solutions can also bring about significant complexities in determined solutions, especially in **SbC-2**/**-3** y **TbC-1**/**-2**. Namely, **SbC-1** may be able to implement self-healing mechanisms (e.g., store-and-forward) that ensure transparency in the connection and restoration in the case of incidences. However the self-healing mechanisms in solution **SbC-2** may generally be less transparent since data messages are transferred as are, to the destination node. Likewise, TCP/IP solutions (i.e., **SbC-3** and **TbC-2**) depend on the HW/SW resources, and for this reason they tend to be quite susceptible to threats to availability (e.g., DoS attacks). Similarly, PDPs are also single failure points where primary PDPs may be disabled or remain inoperative, thereby affecting the access. In this case, the corresponding PEP services should connect to other PDPs following a specific delegation scheme.

- **Survivability** led by a set of security properties such as authentication, authorization, detection, response, accountability, trust and privacy. Here, the adversarial scope is relevant because depending on the network configuration, the attacker may target a particular node. In **SbC-1**, **TbC-1**/**-2**, the most attractive nodes are precisely those that are located in the main interfaces that divide the CPS from the rest of the network, where attackers can modify measurement values, produce false injection, manipulate data (measurements, commands or alarms), impersonate identities, and so on. Although this problem is apparently controlled by **SbC-3** and partially so by **SbC-2**, because the services are provided directly by the nodes, they are more likely to draw attention and be used to lead advanced attacks (Cárdenas et al., 2011).

  Many advanced attacks target the integrity or availability of resources, sensitive data and identity. So one way of protecting the communication channels would be through the TCP/IP security services (relevant in **SbC-3**) and taking into account the security standards for industrial communication networks such as the IES-62351-(3-6). Series 3-6 of the standard specify the use of TLS/SSL together with key exchange algorithms (Diffie–Hellman, RSA), digital signature (Digital Signature Standard, RSA), encryption algorithms (RCA-128, 3DES or AES-128/256 bits) and secure hash algorithm. As a complement, VPNs in specific sections of the network, i.e., between PDPs and the main interfaces (**SbC1**/**-2**, see Figures 1 and 2) can also help in the network designs.

  In substations, the **SbC-1** and **SbC-2** solutions can protect the communication channels by applying the primitive security measures offered by the CPS-specific protocols; e.g., Zigbee PRO/Smart Energy and ISA100.11a, which support key management through symmetric/asymmetric cryptography and certification. Similarly, intrusion detection mechanisms with support for automated response could also be considered as possible additional measures for the protection of the different system assets. However, this protection in distributed environments (**SbC-2**/**-3**) may become quite costly since each device needs to inspect each input data and the actions carried out in the surroundings. If these actions are based on simple techniques (e.g.,

based on statistical data) or are managed by powerful (de)centralized systems (e.g., front-ends and gateways in **SbC-1**/**-2**, respectively), the computational cost may be less.

Authentication and authorization in CPSs are two other security measures, in which it is important to determine the location of the authentication services. Although, the approach proposed in this chapter is based on an architecture in which the access request from external entities is validated by PDPs, the IEC-62351-8 standard recommends verifying the access in each end-point. This means that the authentication in **SbC-1** should center on the front-ends and the rest of the solutions should fall on the end-points. To reduce costs in the latter case, the authentication could, for example, depend on additional (de)centralized services (e.g., lightweight directory access protocol, remote authentication dial-in user service or Kerberos) to avoid replication in distributed environments. On the other hand, the management of authentication and authorization databases can become expensive, as their maintenance depends on the size of the network and on the security policies specified for each area. Furthermore, this problem may even be higher in the authorization databases where roles and permissions (e.g., IEC-62351-8 reserves 32.767 roles for private use) may change more frequently than the identities.

With respect to accountability, it is advisable to specify centralized approaches in which the evidence can be stored in a single entity. However, this condition only works in **SbC-1**/**2** solutions, but with the exception that the gateway can only extract statistical data from the packets. As for **SbC-3**, where the interactions are stored in all sensor nodes, the amount of information that can be stored is limited by the storage capacity of the network nodes. To solve these limitations, it is possible to download the information to external infrastructures (e.g., in a fog/cloud system (Alcaraz et al., 2011)) or powerful dedicated devices (e.g., **TbC-1**/**-2**), thereby favoring auditing and forensic tasks.

Trust and privacy are two other security measures needed to increase trust in the collaborations between nodes (e.g., PDPs-to-front-end, gateway-to-end-devices, etc.), and protect the data beyond the confidentiality and the location of these nodes. In this respect, the cyber-physical devices developed in **SbC-2/-3** solutions could require reserving (i) the communication space to manage the interconnection to the Internet and (ii) the computational space to ensure secure end-to-end communication. In addition, **SbC-3** also requires each connection to verify the trust values before making a decision; a condition that is not required in **SbC-1**. Concentrators, i.e., the front-ends, have a more holistic vision of the network as a whole, so they can, a priori determine the most suitable nodes for the execution of actions.

Privacy in CPS contexts can be achieved in two ways: through data privacy and location-based privacy. Data privacy involves protecting the communication channels (either via the Internet or wireless networks) and any activity associated with users' lifestyle routines. This principally affects the hierarchical interconnection solutions (**SbC-1**/**-2**, **TbC-2**). At this point, privacy becomes an important issue when (i) the activity pattern may be deduced by analyzing the signals received from home-appliances, known as load signatures or power fingerprints (Zeadally et al., 2012); and (ii) lightweight mechanisms have to be supported to process and coordinate specific strategies as proposed in (Kalogridis, 2010). In contrast, location privacy consists in preventing external entities from inferring the location of devices by, for example, analyzing the network traffic (Pai, 2008). However, current techniques still require complex synchronization methods, and HW and SW resources that may be excessive for some devices classified as weak and heavy-duty. This also means that the integration of privacy techniques might be too costly for some interconnection strategies because the computation of the approaches is normally implemented in the end-nodes (such as **SbC-2/-3**).

Further Discussion and Future Work

Once the interoperability and control requirements together with the interconnection strategies have been presented, it is now necessary to discuss which interconnection strategy or strategies are the most suitable for critical scenarios. We first discuss the strategy **SbC-3,** as nowadays, many CPSs are part of the IoT (e.g., smart industrial sensors), and leave the rest of the solutions to be discussed later; i.e.:

- **TCP/IP solution**: **SbC-3** could certainly provide rapid access and availability of resources when sensitive parts of the system are seriously compromised (e.g., isolated areas of a CPS). In this case, Internet-enabled devices could take decisions by themselves to alert human operators to a situation in time, without traversing the front-ends or gateways; and operators could act accordingly while these devices still conduct monitoring tasks. Unfortunately, depending on the capacities of these elements and their susceptibility to specific attacks on the availability (e.g., DoS), the alert in these critical situations may not reach the control entity in time, affecting, in this case, the access. On the other hand, the availability of the resources largely depends on (i) the capacity of the nodes to support different types of services and complex applications, and on (ii) the functional features of the interconnection approaches. For example, **SbC-3** is able to provide gradual updates for the entire network and to ensure resilience in the advent of severe faults, significantly favoring partial access to end-devices. However, this interconnection approach is not able to provide redundancy-based/roll-back-based restoration mechanisms as they demand replication of resources or keeping evidence to ensure the roll-back process. In contrast, **SbC-1** or **SbC-2** with **TbC-1** are able to provide the service by relying on possible additional powerful devices for redundancy or roll-back.

  Regarding communication within **SbC-3**, it does not benefit from the optimized services that some CPS-specific protocols offer, such as WirelessHART or ISA100.11a. They, for example, provide a selective range of network topologies (e.g., mesh, many-to-one, star) with the capacity to offer routing mechanisms that allow the path redundancy and the specification of the special services of the link layer like those for the coexistence, collision and congestion. In addition, the network architecture is fully distributed, which makes it difficult to adapt store and forward mechanisms and capacities for support interfaces working as cache. This deficiency further complicates the monitoring tasks of the context managers in charge of continuously requesting the network status, which, together with the overhead implicit in the channels (due to complex IP headers), can, sooner or later, impact on the access.

- **Front-end solution**: solves some of the problems of **SbC-3**, but even so it still has certain drawbacks that affect the access. For example, control entities have to traverse the concentrator, which has to proceed with the translation of identities and the conversion of packets (e.g., Modbus/TCP to ISA100.11a), thereby increasing the time periods for the access and/or assistance in the field. Additionally, the front-end is a concentrator that permits implementing diverse security mechanisms (authentication, authorization, detection, response and accountability) and complex resilience mechanisms, which probably require computational capacities and the adaptation of other approaches, like **TbC-1**, for redundancy. This redundancy helps protect the entire CPS from adversarial influences, and at least, in the main input points.

  Unlike **SbC-3**, **SbC-1** can take advantage of the optimized services of the CPS-specific protocols, such as redundant paths to reach a determined node in the network. This feature benefits, in parallel, the work of the NSM objects, which have to go through the system to determine the saturation levels, quality of service and activity of each resource included within a CPS. If there is isolation or congestion in certain parts of the system, these NSM objects can reach the concentrator using the mesh properties and the redundant services that many of the internal

protocols offer. This way of concentrating the data at a single point favors the context management, and therefore the access management in the field.

- **Gateway solution**: adds certain functional features of the **SbC-1** solution and the **SbC-3** solution. Namely, **SbC-2** is able to (i) configure communication environments based on CPS-specific protocols with support for store and forward mechanisms; and (ii) provide a direct connection to the nodes. However, these functionalities increase the complexity in the end-nodes, and therefore the execution of a critical action in the field. In addition, control entities have to traverse the gateway to analyze the incoming connections, detect threats (in the application layer) and log actions and events, further complicating the access. As for the management of the context, **SbC-2** has similar capacities to **SbC-1**.

- **Hybrid and Access Point solutions**: are two approaches that benefit the control architectures for maintenance and redundancy purposes. For example, **TbC-1** solutions favor the access even when the primary interfaces (the front-ends or gateways) are subverted. In this case, redundant mechanisms are activated together with the DSD mechanisms to leave the access free to only authorized personnel with the specific roles and privileges (e.g., Operators or SECADM with specific control actions). However, the replication of resources (e.g., routing tables) is a handicap that may hamper the access and the management of the context. A way to lessen these complications would be through the implementation of suitable communication infrastructures composed of technologies potentially capable of processing and maintaining large databases with the capacity to ensure a high rate of replications.

Table 4 Association of interconnection strategies and control requirements in CPSs

	Performance			**Sustainability**						**Depend.**		**Survivability**						
	Comp. overhead	Com. overhead	Responsiveness	Scalability	Mobility	Extensibility	Addressing	Access	Maintainability	Availability	Robustness/resilience	Secure channel	Authentication	Authorization	Detection & response	Accountability	Trust	Privacy
SbC-1	⋆	○	⋆,○	+	+	⋆	◇	◇,○	–	–	◇	◇	◇	◇	◇	+	◇	◇
SbC-2	⋆	○	⋆,○	+	+	⋆	+	○	–	–	◇	◇	◇	◇	◇	+	◇	◇
SbC-3	⋆	–	⋆	+	+	⋆	–	+	+	+	+	●	●	●	◇	⋆,●	◇	◇
TbC-1	⋆	●	⋆,○	◇,●	+	⋆	–	+	+	+	+	◇	●	●	◇	+	◇	◇
TbC-2	⋆	●	⋆,○	◇,●	+	⋆	–	–	–	–	●	◇	●	●	◇	●	◇	◇

+	property provisioned ('–' is the opposite). Note that '+' is integrated as part of the rest of the symbols described below.
⋆	depends on the type of devices: weak, heavy-duty or powerful-duty.
●	depends on architecture (e.g., centralized or distributed) and technologies (e.g., TCP/IP).
○	depends on the optimization of the CPS-specific protocols.
◇	depends on the overhead implied in the services integrated (security, translation).

Table 5 Characteristics of the integration and their strategies in interoperability

	Interoperability			
	Rapid access	Transparency	Availability	Reliability
SbC-1	◇,○	+	–	⋆,◇,○
SbC-2	○	+	–	⋆,◇,○
SbC-3	+	+	+	⋆,◇
TbC-1	–	+	+	+
TbC-2	–	+	⋆	●

Table 4 and Table 5 summarize all of these features and conclude this chapter. Specifically, we conclude that the full integration of the Internet-enabled devices to the Internet may produce high computational and communication costs where each device must process and maintain a routing table. This characteristic, certainly undesirable for the operational performance, is, to the contrary, beneficial in certain critical situations where the access to network interfaces is not always possible. Given this, we also believe that the hybrid configuration based on **SbC-1/2** and **TbC-1** in '*normal situations*' may still be effective to gain a desired interoperability, where the reliability of the communication can be subject to the redundancy given by **TbC-1**. Only in emergency situations, can the solution **SbC-3** be of special relevance where PDPs can transparently access the cyber-physical devices to manage '*critical situations*'.

To incorporate these combinations (i.e., **SbC-1** or **SbC-2** and **TbC-1**; and **SbC-3**) in complex systems, the interoperability architecture defined in Figure 1 must, therefore, be configured so that: *all the PDPs are able to access the front-ends or gateways in normal situations, and in turn, be able to directly access Internet-enabled devices in extreme situations.* But while these solutions can be effective for today's industry, it is still necessary to find a way to create self-sufficient systems where end-devices should form part of the IoT despite their current HW/SW constraints. So as future work, it would useful to study how to bring all the functionality of the Internet to specific cyber-physical devices and vice versa, and not in exceptional cases only.

ACKNOWLEDGMENT

The first author receives funding from the *Ramón y Cajal* research programme financed by the Ministerio de Economía y Competitividad. In addition, the work presented her has also been partially supported by PERSIST (TIN2013-41739-R) financed by the same ministry.

REFERENCES

Al-Kuwaiti, M., Kyriakopoulos, N., & Hussein. S. (2009). A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability. *IEEE Communications Surveys and Tutorials*, 11(2):106–124.

Alcaraz, C., & Lopez, J. (2010). 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.

Alcaraz, C., & Lopez, J. (2012). Analysis of requirements for critical control systems.

International Journal of Critical Infrastructure Protection, 5:137–145.

Alcaraz, C., Agudo, I., Nuñez, D., & Lopez, J. (2011). Managing incidents in smart grids á la cloud. *In the IEEE CloudCom 2011* (pp. 527–531), Athens, Nov-Dec. IEEE Computer Society.

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

Alcaraz, C., Lopez, J., & Wolthunsen, S. (2016a). Policy enforcement system for secure interoperable control in distributed Smart Grid systems. *Network and Computer Applications*, Elsevier, 59: 301–314.

Alcaraz, C., Lopez, J., and Choo, & K-K. (2016b). Dynamic restoration in interconnected RBAC-based cyber-physical control systems. In the *14th International Conference on Security and Cryptography (SECRYPT 2016)* (vol. 4, pp. 19-27), Lisbon, July. SCITEPRESS.

Bansal, S., Sharma, S., & Trivedi, I. (2012). A detailed review of fault tolerance techniques in distributed systems. *International Journal on Internet and Distributed Computing Systems*, 1(1):33–39.

Bessani, A., Veronese, G., Correia M., & Lung, L. (2009). Highly-resilient services for critical infrastructures. *In Proceedings of the Embedded Systems and Communications Security Workshop*.

Bowen J., & Stavridou, V. (1993). Safety-critical systems. Formal Methods and Standards, *Software Engineering Journal*, 8:189209.

Cárdenas, A., Amin, S., Lin, Z., Huang, Y., Huang, C., & Sastry, S. (2011). Attacks against process control systems: Risk assessment, detection, and response. *In the 6th ACM Symposium on Information, Computer and Communications Security* (pp. 355–366), Hong Kong, March. ACM.

Coyne, E., & Weil. T. (2013). ABAC and RBAC: Scalable, flexible, and auditable access management. *IT Professional*, 15(3):14–16.

Christin, D., Reinhardt, A., Mogre, P., & Steinmetz, R. (2009). Wireless sensor networks and the internet of things: Selected challenges. *In 8th GI/ITG KuVS Fachgespr¨ach Drahtlose Sensornetze*.

HART Communication Foundation - IEC 62591. (2010). Industrial communication networks Wireless communication network and communication profiles WirelessHART. Retrieved on May, 2016, from http://www.hartcomm.org/

Hong, J., Suh, E., & Kim. S. (2009). Context-aware systems. *Expert Syst. Appl.*, 36(4):8509–8522.

IEC-62351 (2007). IEC-62351 (1-8): Information security for power system control operations, international electrotechnical commission. Retrieved in May 2016, from http://www.iec.ch/smartgrid/standards/

IEEE Standard, 802.15.4-2006. (2006). Wireless medium access control and physical layer specifications for low-rate wireless personal area networks.

ISA100.11a - IEC 62734. (2009). Wireless systems for industrial automation: Process control and related applications. Retrieved on May 2016, from http://www.isa.org/

Kalogridis, G., Efthymiou, C., Denic, S., Lewis, T., & Cepeda, R. (2010). Privacy for smart meters: Towards undetectable appliance load signatures. *In IEEE SmartGridComm* (pp. 232–237).

Knight, J., & Strunk, E. (2004). Achieving critical system survivability through software architectures. *In Architecting Dependable Systems II* (vol. 3069, pp. 51–78). Springer.

Kuzlu, M., & Pipattanasomporn, M. (2013). Assessment of communication technologies and network requirements for different smart grid applications. *In Innovative Smart Grid Technologies* (pp. 1–6).

Montenegro, G., Kushalnagar, N., Hui, J., & Culler, D. (2007). RFC 4944: Transmission of IPv6 packets over IEEE 802.15.4 networks.

Ovidiu, V., Harrison, M., Vogt, H., Kalaboukas, K., Tomasella, M., Wouters, K., Gusmeroli, S., & Haller, S. (2009). Internet of things strategic research roadmap. *European Commission - Information Society and Media DG.*

Pai, S. (2009). Transactional confidentiality in sensor networks. *IEEE Security & Privacy*, 6:28–35.

Ruchika, M. (2013). Schemes for surviving advanced persistent threats. Diss. Faculty of the Graduate School of the University at Buffalo, State University of New York.

Treaster, M. (2005). A survey of fault-tolerance and fault-recovery techniques in parallel systems. CoRR, abs/cs/0501002.

United Nations General Assembly. Development and international co-operation (1987). Chapter 2: Towards Sustainable Development, Commission on Environment and Development: Our Common Future, Document, A/42/427.

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE Communications Surveys & Tutorials*, PP(99):1–16.

Zeadally, S., Pathan, A., Alcaraz, C., & Badra, M. (2012). Towards privacy protection in smart grid. *Wireless Personal Communications*, 73:23–50.

ZigBee Alliance. (2010). Zigbee specifications. Retrieved in May 2016, from http://www.zigbee.org/