Computers and Electrical Engineering 66 (2018) 407–419

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Software-defined networking in cyber-physical systems: A survey[☆]

Elias Molina[*], Eduardo Jacob

Department of Communications Engineering, University of the Basque Country UPV/EHU, Alameda de Urquijo s/n, 48013 Bilbao, Spain

ARTICLE INFO

Article history:
Received 9 January 2017
Accepted 12 May 2017
Available online 26 May 2017

Keywords:
Cyber-Physical Systems
Industrial Control Systems
OpenFlow
Smart Grid
SDN

ABSTRACT

Cyber-Physical Systems (CPSs) rely on networks that interconnect sensors and actuators to perform measurement, supervision and protection functions in different domains, such as transportation and industrial automation control systems. These networks must be able to support mobile wireless CPSs that are demanding new requirements related to flexibility and heterogeneity without compromising the Quality of Service (QoS). However, it is hard to determine, for example, the optimal resource allocation or the most reliable paths without global network information. In this way, the Software-Defined Networking paradigm is being considered as key to overcome such emerging needs. In particular, an SDN controller is able to establish paths between sensors and actuators according to bandwidth, latency, redundancy, and safety considerations. Thus, the goal of this paper is to review the state of the art of SDN approaches applied to mission-critical applications by identifying trends, challenges and opportunities for the potential development of software-defined cyber-physical networks.

1. Introduction

Recently-coined terms, such as for example, Industry 4.0, the Fourth Industrial Revolution or Industrial Internet, revolve around the use of Cyber-Physical System (CPSs); that is to say, complex architectures where physical entities or processes are remotely controlled by cyber-components. These components are in charge of performing the configuration of communication capabilities and the data-processing functions, as sketched in Fig. 1. The purpose of this figure is to illustrate the communication between the physical domain, formed by networked nodes, and the cyber domain, where the control plane should ensure satisfactory performance in meeting different requirements related to system manageability, security, reliability, and so on. Fig. 1 also shows a wide range of mission-critical applications, such as transportation, industrial automation systems or electrical power grids, and some illustrative scenarios that have received considerable attention in recent years.

CPSs have emerged on the basis of Industrial Control System, where data acquisition and processing elements of a Networked Control System (NCS) are traditionally arranged in hierarchical levels and applications (ANSI/ISA-95 model). Until now, the design of industrial automation networks has been based on an isolation model, where the control of the Operational Technology (OT) is separate from the Information Technology (IT) perspective. However, despite the previously mentioned levels representing a hierarchical architecture, a CPS tends to be designed as a network connecting all physical

[☆] Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. Joy I-Z Chen.

[*] Corresponding author.
E-mail addresses: elias.molina@ehu.es, eliasmoli@outlook.com (E. Molina).

http://dx.doi.org/10.1016/j.compeleceng.2017.05.013
0045-7906/© 2017 Elsevier Ltd. All rights reserved.

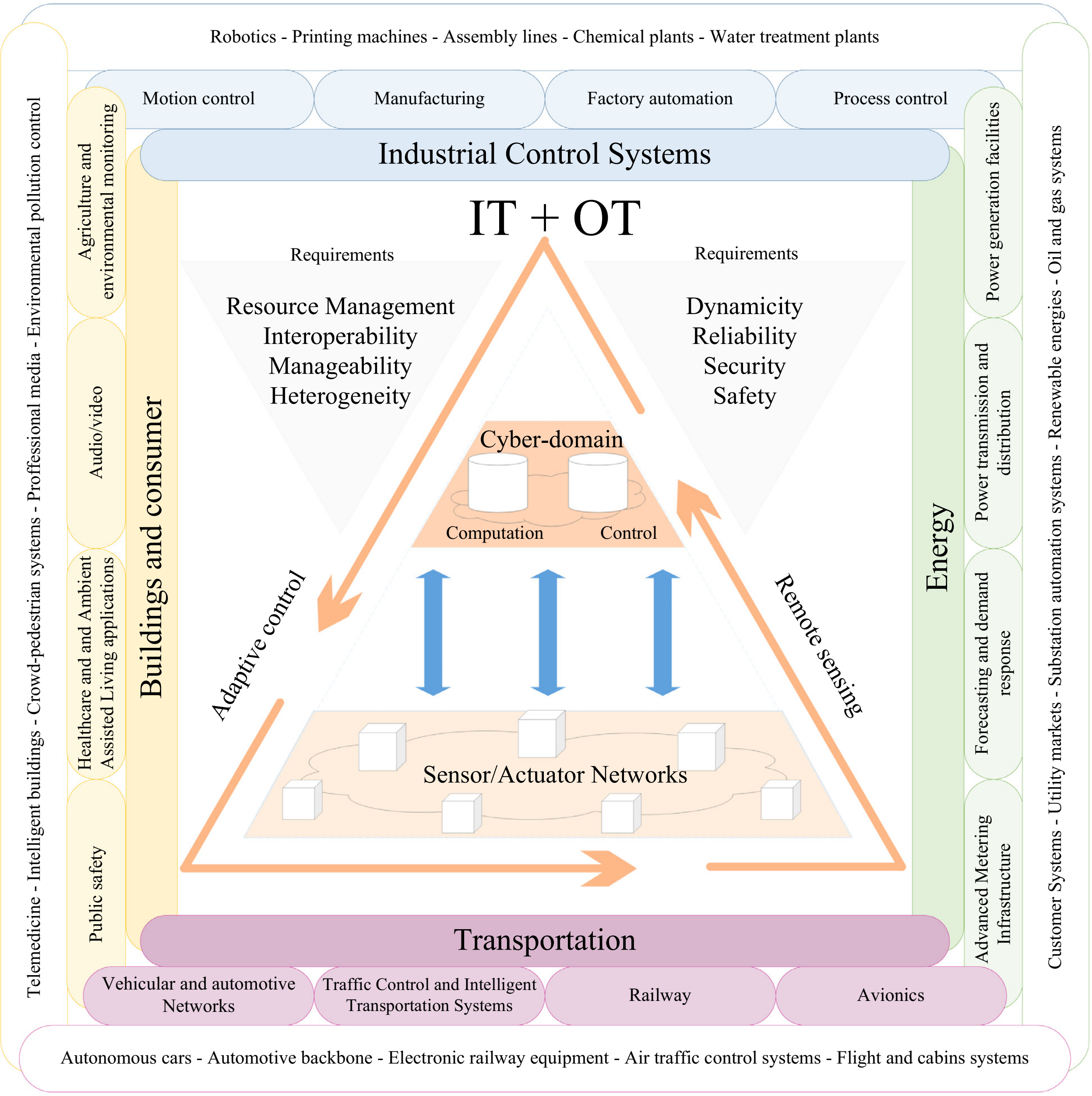
Robotics - Printing machines - Assembly lines - Chemical plants - Water treatment plants
Motion control
Manufacturing
Factory automation
Process control
Industrial Control Systems
IT + OT
Requirements
Resource Management
Interoperability
Manageability
Heterogeneity
Requirements
Dynamicity
Reliability
Security
Safety
Cyber-domain
Computation
Control
Sensor/Actuator Networks
Adaptive control
Remote sensing
Buildings and consumer
Agriculture and environmental monitoring
Audio/video
Healthcare and and Ambient Assisted Living applications
Public safety
Telemedicine - Intelligent buildings - Crowd-pedestrian systems - Proffessional media - Environmental pollution control
Energy
Power generation facilities
Power transmission and distribution
Forecasting and demand response
Advanced Metering Infrastructure
Customer Systems - Utility markets - Substation automation systems - Renewable energies - Oil and gas systems
Transportation
Vehicular and automotive Networks
Traffic Control and Intelligent Transportation Systems
Railway
Avionics
Autonomous cars - Automotive backbone - Electronic railway equipment - Air traffic control systems - Flight and cabins systems

Fig. 1. CPS feedback operation, applications and requirements.

and computational elements in a production infrastructure. Thus, the significance of the CPSs lies on a fully integration between production processes and communications. This paper presents a thorough analysis of the requirements of emerging CPSs, which pose new challenges to the current network architectures. Particularly, it is necessary to design communication systems that enable dynamic performance, where changes in physical device settings involve responses from the network configuration. The cooperative interaction between network protocols and advanced control systems will provide a new ecosystem for future CPS applications. This gives the Software-Defined Networking (SDN) paradigm the opportunity to play a leading-edge role in building CPSs.

Software-defined networks are those in which control and data plane are decoupled. Standardized protocols, such as OpenFlow, Forwarding and Control Element Separation (ForCES, RFC 5810) or the combination of the Path Computation Element Protocol (PCEP, RFC 5440) and BGP Link State Distribution (BGP-LS, RFC 7752) schemes allow external entities to have a global view of the network. Although the SDN technologies are now well-known in data center and telecom environments, the provided programmability is becoming attractive for smart industrial applications. In this way, there are new approaches to extend existing SDN architectures to enable enabling industrial-grade QoS capabilities within CPS domains.

In order to contribute to the development of future software-defined cyber-physical networks, the aim of this work is to review relevant literature on the integration of SDN in critical CPS communications.

The remainder of the paper is organized as follows. The major requirements of cyber-physical networks are given in Section 2. Sections 3 and 4 present an overview of the opportunities offered by SDN in terms of Quality of Service (QoS), security and reliability. Finally, the paper is concluded in Section 5.

2. Cyber-Physical Networks

Industrial networks have special characteristics related to the impact of service failure severity and the latency requirements, which are significantly higher than conventional networks. Sauter et al. [1] detailed specific industrial Ethernet stack implementations, and highlight industrial wireless communication as an important current research area. In addition, this review paper reflected an evolution from heterogeneity of isolated networks towards heterogeneous systems that share the same network infrastructure, using the TCP/IP stack. A common integration strategy in these network environments had been to introduce middleware schemes for translating protocols and dynamically adjusting (QoS) parameters. However, these adaptation layers are usually complex and resource consuming. The same authors envisioned that a combination of IEEE 802-based networking solutions in both wired and wireless domains tends to facilitate seamless network integration. Thus, converging technologies reduce the number of gateways and simplify the overall management.

In general, CPSs rely on multiple networks, whether wired or wireless, to which impose industrial-grade requirements, where dependability, safety and performance characteristics of critical and non-critical services coexist. Moreover, although wireless links suffer from unreliable data transmission due to non-deterministic factors, these networks have to ensure continuity of operations, so that availability and performance are not affected. Specifically, wireless automation requirements are specified in IEC 62657-1, differentiating them according to the critically of applications. Mature wireless technologies, including IEEE 802.11, 802.15.1 or 802.15.4 standards, can be applied in industrial applications through robust network designs in error-prone channels. More specifically, Gungor et al. [2] assessed the opportunities offered by Wireless Sensor Network (WSN) to smart grid applications, as well as their technical challenges, such as ensuring a certain latency or (QoS). These challenges are associated with changes in the topology and connectivity due to the conditions of the physical layer.

Furthermore, there are emerging wireless technologies for automation and control applications, such as WirelessHART (IEC 62591), ISA100.11a (IEC 62734) or WIA-PA (IEC 62601). They are all based on the IEEE 802.15.4e Media Access Control (MAC) layer, which uses Time Slotted Channel Hopping (TSCH) to provide reliable communication and deterministic latency. TSCH combines frequency hopping and multi-channel Time Division Multiple Access (TDMA) with a very low cycle time. In terms of network management, ISA100.11a and WIA-PA are designed to support centralized and distributed architectures, whereas WirelessHART uses a centralized control plane. In this case, the “Network Manager” is responsible for configuring the network resources and managing routes between devices, so that field nodes need not be concerned with these tasks. Despite the fact that WirelessHART technology may be suitable for implementing many CPSs, current research directions are towards hierarchical network architectures that enhance scalability. Thus, large WSN can be divided into multiple subnetworks and local network managers, which have to be coordinated with a global manager. Moreover, it would be appropriate to establish a unified codesign where the network resource allocation should be dependent on the control design.

2.1. Network requirements

Typical industrial network configurations are mostly built on managed devices, which support priority queuing and access control protocols, being also necessary to implement physical redundancy. In the case of the smart grid, standardization bodies have published network engineering recommendations (eg, IEC 61850-90-4/12 and IEEE 1615) for inter- and intra-substation communications, including traditional protocols that meet general network requirements. Regarding management tools, the standard IEEE 1615 indicates that being able to access all of these devices from a central location would facilitate faster troubleshooting and reconfiguration. Diverse (QoS) requirements imposed by CPSs are detailed below.

2.1.1. Priority and bandwidth constraints

In addition to the criticality-driven nature, different types of flows are expected. Concerning the size and volume of data traffic, digital measurements are usually carried in small packets. With regard to traffic patterns, CPS applications generally generate periodic Constant Bit Rate (CBR) traffic, and aperiodic messages, both Variable-Bit Rate (VBR) and Available-Bit Rate (ABR) traffic. As a representative example, the IEC 61850 standard, which is focused on communication networks in power automation systems, defines different services:

- CBR: the Sampled Value (SV) are used to continuously send measures.
- VBR: the Generic Object Oriented Substation Event (GOOSE) protocol is used to periodically transmit heartbeat messages and send data bursts upon the occurrence of a trigger.
- ABR: the Manufacturing Message Specification (MMS) to asynchronously transmit general purpose and supervisory control data.

The two former are time-sensitive services in a publisher/subscriber model, while (MMS) is used for non-time-critical client/server applications.

To achieve adequate performance in industrial networks, common layer 2 control protocols perform traffic filtering and prioritization. Hence, Virtual LAN (VLAN, IEEE 802.1Q) tags provide network segmentation and identify the priority of frames. Also, the Priority-based Flow Control (PFC, IEEE 802.1Qbb) intends to avoid frame loss caused congestion, since it allows a receiver to send a PAUSE request for different classes of traffic.

2.1.2. Predictability and timeliness

Delay requirements depend on the specific industrial application; for example, the maximum transfer times for teleprotection systems can be less than 5 ms. Best-effort services may not be adequate in those scenarios where the worst-case delay is a targeted metric. In fact, hard real-time services require time-sensitive networks, whose control and management planes guarantee a low deterministic latency and jitter.

According to the framework for CPSs published by the NIST [3], “time correctness by design” enables many safety-critical systems that are based on timing analysis techniques. In order to provide a network-wide clock reference and create a correct scheduling in distributed CPS domains, it is necessary to achieve accurate synchronization for coordinating processes, timestamping of events or latency measurement. Different techniques allow network devices to synchronize themselves; for example, Synchronous Ethernet (SyncE, ITU-T Std. G.8261/2/4) provides frequency transfer using the carrier data link (physical layer), whereas the packet layer-based Precision Time Protocol (PTP, IEEE 1588) enables phase and time synchronization. Also, the White Rabbit project[1] is based on both SyncE and PTP protocols and accomplishes sub-nanosecond clock synchronization.

In addition, as stated in [4], to achieve a deterministic network, it must have a “formal verification of maximum end-to-end latencies”. In order to achieve this, the Network Calculus (NC) provides a theoretical framework that can be used to analytically evaluate real-time constrained applications. Thus, using network simulation tools, such as widely used OPNET Modeler and NS2, allows network designers to identify bounded delays for different types of traffic on the basis of NC. In the case of avionics industry, the Avionics Full DupleX Switched Ethernet (AFDX, ARINC 664 Part 7) is a suitable protocol for offering predictable timing behavior through the pre-establishment of the so-called Virtual Links (VLs). VLs are static paths previously computed by NC that guarantee a certain bandwidth, and limited latency and jitter. One of the main advantages of AFDX networks is to be based on commercial off-the-shelf (COTS) Ethernet components with support for (QoS).

Moreover, aircraft data and other mission-critical networks will evolve to unified systems that mix AFDX traffic and TCP/IP best effort services without using gateway functions. As an example, the SAE AS6802 Time-Triggered Ethernet (TTEthernet) standard is another relevant technology used in aerospace and automotive industries. It is based on static time-triggered schedules and allows AFDX and synchronous time-triggered traffic to share the same network. It should be noted that although wireless extensions to the time-triggered paradigm, at present, no TDMA data link layer compatible with, for example, existing IEEE 802.11 WiFi networks has been standardized.

However, in any case, SAE AS6802 and AFDX standards impose static resource allocations. Hence, providing reconfiguration capability in the event of failures is a need for avionics networks, and still applicable to other CPSs.

2.1.3. Robustness and survivability

According to [4], “the main task of safety-critical networks is to provide guaranteed delivery of all packets”. Thus, underlying networks have to meet certain levels of reliability to ensure no interruption in mission-critical CPSs. Quantitative metrics for resilient control systems include recovery time and performance degradation. In this way, redundancy is the most accepted method for maintaining continuous network operation, since a very low, or even zero, recovery time and packet loss rate can be achieved by using spatial and temporal redundancies. The IEC 62439 standard defines different layer 2 mechanisms to build high-availability industrial networks, being applicable to specific topologies. For example, ring topologies can be protected with the Media Redundancy Protocol (MRP), achieving lower convergence time with respect to Rapid-Spanning Tree Protocol (RSTP). Under this umbrella, it is interesting to note the High-availability Seamless Redundancy (HSR, IEC 62439-3 Clause 5) and the Parallel Redundancy Protocol (PRP, IEC 62439-3 Clause 4), which provide zero recovery time by duplicating data and network resources. It is worth to remark that the aforementioned AFDX protocol follows the same principles.

Moreover, link-state routing has been recently proposed for layer 2 frame forwarding. Thus, unlike spanning tree techniques, Shortest Path Bridging (SPB, IEEE 802.1aq) and Transparent Interconnection of Lots of Links (TRILL, RFC 7176) enable shortest path forwarding in mesh topologies. Both technologies have been proposed for industrial automation systems by the INTEGRIS project[2].

2.1.4. Network cyber-security

Securing CPS is essential to ensure integrity and confidentiality for critical applications. A thorough overview of standards and guidelines for overcoming cyber-security issues in CPS operations is given by the NIST Special Publication 800-82[3], where protection mechanisms against common threats and vulnerabilities are identified, suggesting countermeasures to reduce their risks. Besides mechanisms for ensuring authentication and integrity of critical services [3], network security

[1] White Rabbit project, Open Hardware Repository.

[2] INTEGRIS (INTelligent Electrical Grid Sensor communications) FP7-ICT project.

[3] NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security.

deeply depends on restricting physical and logical access to cyber-physical components, as recommended in most security standards (eg, ISA-99/IEC 62443-1-3). For example, boundary protection can be obtained through a De-Militarized Zone (DMZ), whereas Access Control List (ACL) and stateful packet inspection or application-gateway firewalls provide traffic filtering.

2.1.5. Network management and monitoring

Besides mentioned requirements, it is also necessary to support performance and fault monitoring, which could be carried out with the Simple Network Management Protocol (SNMP, RFC 3411). For example, like most traditional Network Management System (NMS), the PROFINET standard uses SNMP to retrieve Link Layer Discovery Protocol (LLLDP) data and thereby extracting the network topology of industrial networks. In addition, lightweight adaptations of monitoring protocols are being developed for CPSs applications, such as, for example, the TinyIPFIX version[4] of the IP Flow Information Export (IPFIX, RFC 7011) protocol, that serves for transmitting smart metering data in WSN.

Furthermore, management functions can be implemented with the NETCONF (RFC 6241) protocol, which poses numerous advantages over proprietary Command Line Interfaces (CLI). The authors of [5] studied how SNMP and NETCONF protocols can be used on resource-constrained Internet of Things (IoT) environments. On the other hand, the commercial product “Cisco Connected Grid (NMS)” can be considered as combination of hardware and software to unify the monitoring and management functionalities. However, being a proprietary solution does not facilitate the interoperability, which is a major goal of the smart grid.

2.2. Shortcomings of traditional control protocols

To satisfy the previous requirements, it is necessary a global control of network resources. In general, industrial networks are designed, configured and tested according to a pre-defined policy enforcement in order to meet high levels of performance and reliability. In the majority of cases, this is carried out in a static way, requiring a great deal of manual configuration. Yet, despite the fact that fixed and dedicated infrastructures make easier to provide QoS guarantees for critical services, they do not support the adaptability demanded by reconfigurable CPSs [6]. Moreover, in agreement with [7], conventional fixed network protocols fail to address the dynamic aspects of CPS applications. To overcome this ossification, the SDN technologies can play an important role in the future cyber-physical networks.

3. Applying SDN to CPSs

In software-defined networks, the control plane is separated from the data plane, and implemented in external entities. Among different protocols that define southbound interfaces to communicate both network planes, OpenFlow is the most widely used SDN protocol, whereby a controller establishes the forwarding rules for flows arriving at a network device.

3.1. Controller-based CPSs

A logically centralized controller, in combination with network awareness, can offer QoS support for critical applications, and it “may reduce complexity and cost, and increase flexibility”, as extracted from [3]. With the aim of achieving self-reconfigurable CPSs, most researches have emphasized the use of closed-loop feedback SDN systems. Thus, a so-called MAPE (Monitor, Analyze, Plan and Execute) process [6] adapts the network resources to dynamic conditions. This is enhanced by the development of the SDN application tier, which embeds the CPS-specific properties. Fig. 2 shows a multi-layered programmable network whose control plane implements multiple network functions, such as monitoring, routing or traffic filtering, while exchanging CPS-specific information.

In order to be flexible, modular applications interact with the network control logic using a northbound interface. On the other hand, as shown in Fig. 2, the southbound interfaces hide the network complexity and translate the network policies to control instructions. Thus, the control plane can be seen as a gateway converting a general northbound API into data path changes.

Analogous to control theory, where stability, observability and controllability are key concepts, the monitoring system receive real-time per-flow meters and the platform allows network planners to define thresholds for triggering different control plane actions. Fig. 2 outlines a control diagram where an adaptive system dynamically operates according to the received feedback (measures, events or triggers). For example, changes in network topology, bandwidth saturation or failures must be taken into account by the controller and acts consequently. Consequently, similar to the feedback loop model of NCSs, the SDN controller has a holistic network view and enables (QoS)-aware routing optimizations. In this line, a CPS platform should be aware of the state of network devices with the aim of establishing a dynamic resource management, and flow scheduling. Liwewise, the Smartc2net project [8] has proposed a network (QoS) manager that implements adaptive routing by evaluating Key Performance Indicator (KPI) of smart grid applications. This feedback loop approach has also been modeled in [3]. It defines the “CPS Network Manager (CNM)”, which is in charge of allocating bandwidth for each time-sensitive application and determining the transmission scheduling on CPS nodes. Moreover, the CNM communicates with

[4] IETF TinyIPFIX for smart meters in constrained networks.

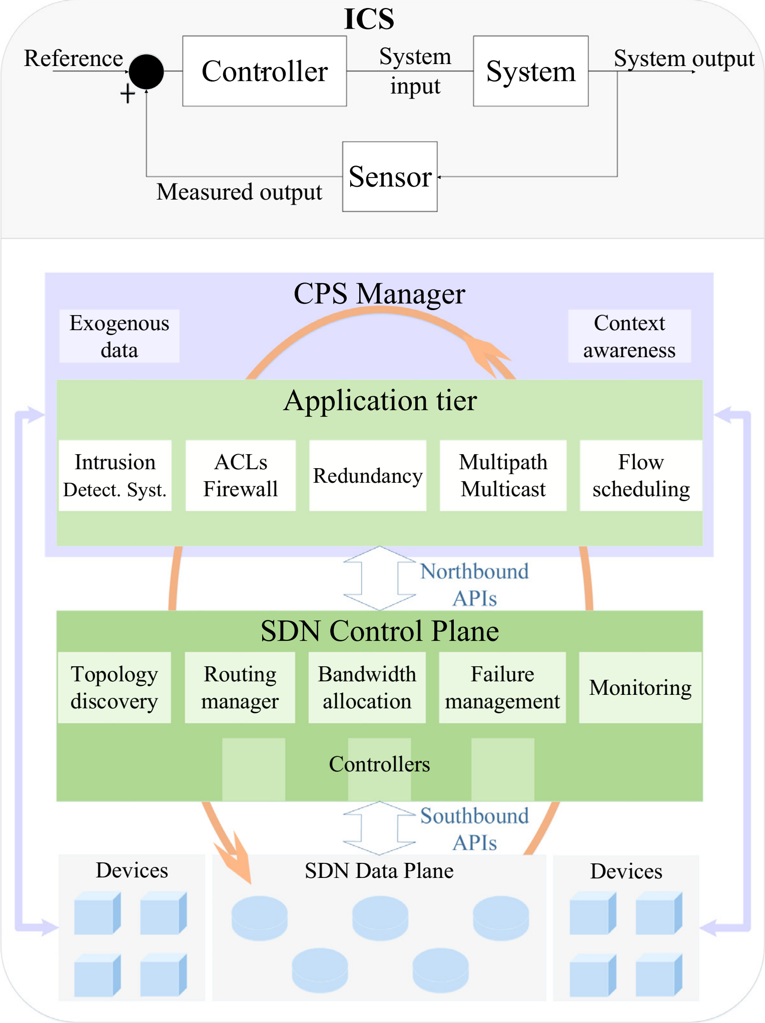

Fig. 2. SDN controller-based CPSs including a control-loop feedback mechanism commonly used in ICSs.

an SDN “Centralized Network Controller (CNC)”, which determines the topology and configures network devices of CPS domains.

3.2. Study cases and emerging trends

Wireless, broadband, global and reliable communication infrastructures are the basis for operation of CPSs in the factories of the future. Moreover, CPSs involving remote operation of machines and robots require low and bounded latencies, which is in line with the so called “Tactile Internet” applications. In these contexts, there are two major trends regarding CPSs: 5G networks and Industry 4.0, which involve massive connectivity of critical systems, and SDN is becoming a major building block for both concepts. One of the most prominent examples of the appropriateness of SDN technologies in the industrial context is that the CPS Public Working Group (PWG), formed by the NIST, has recently determined the adoption of SDN technologies to dynamically manage cyber-physical networks [3]. Regarding the scope, the SDN paradigm is being studied in a broad spectrum of applications, including, for example, inter- and intra-vehicular, healthcare, manufacturing, entertainment, smart grid and, in general, in networks where situational awareness and adaptability are key features that simplify and enable flexible services.

In this context, the NIST’s CPS program predicts “advanced cyber-physical systems that are reliable, resilient, effective, safe, sustainable, secure, and privacy enhancing, by 2020” [3]. Diverse approaches focused on such qualitative attributes will be detailed below.

Table 1
High-level summary of research topics.

Manageability	Resource allocation	Real-time
Orchestration and network reconfiguration	Traffic shaping and bandwidth allocation	Scheduling algorithms
Heterogeneous wireless and wired networks	Load balancing and multipathing	Formal analysis
Centralized and distributed schemes	Unicast and multicast traffic	Congestion control
In-band and out-of-band control	Traffic aggregation	Synchronization
Reliability	Security	Interoperability
Failure detection	Network access control	Legacy systems
Recovery time analysis	Stateless and stateful rules	Uniformity of interfaces
Wireless networks	Control plane protection	Standardization efforts
Protection and failover strategies	Prevention, detection and response	Level of commercial support

4. Challenges and benefits of software-defined cyber-physical networks

Potentials of SDN-enabled cyber-physical networks are discussed subsequently, along with their main limitations. In particular, Table 1 lists the topics covered in this chapter.

4.1. Manageability

With the growing number of networked devices, sophisticated management techniques are required. Different studies have compared traditional versus SDN management and identified requirements that are emerging with the advent of this new paradigm. Traditional methods generally require network operators to deal with low-level vendor-specific configurations to enforce complex high-level network policies. On the contrary, management of software-defined networks are highly simplified as elements are controlled with standard protocols. Thus, SDN provides network programmability, which has actually become a must for future networks.

With regard to software-defined wireless networks, route computation in WSN by a centralized SDN controller is similar to the “Network Manager” used in ISA100.11a, WirelessHART and 6TiSCH[5]. Indeed, routing states in the latter protocol, which enables IPv6 over IEEE802.15.4e TSCH, are provisioned by a Path Computation Element (PCE), although 6TiSCH also supports distributed and hybrid approaches. The authors of [9] envisioned software-defined WSN, where the network controller is in charge of traffic scheduling and end-to-end (QoS) to overcome specific problems, such as “unadaptable and inflexible change in application demands” or “inefficient resource utilization”. In the case that the sensors themselves perform flow-based packet forwarding, it will be important to consider the inherent Wireless Sensor Network (WSN) constraints by reducing the control overhead so that the underlying network is not overloaded by OpenFlow messages. With a similar goal, Kim et al. [10] implemented an SDN-based large-scale wireless network to support Advanced Metering Infrastructure (AMI) systems, as an important part of the smart grid. Instead of using OpenFlow, Kim et al. overcame the resource limitation of AMI devices by proposing a control message exchange based on the Constrained Application Protocol (CoAP, RFC 7252). As a result, the proposed SDN routing application is advantageously compared, in terms of delay and message reliability, with traditional routing protocols for Mobile Ad hoc Network (MANET).

Given the importance of heterogeneous and interoperable CPSs, an example of interconnected networks is found in [11]. In this study a robotic system is attached to a WirelessHART mesh, which, at the same time, is connected to an OpenFlow network providing (QoS) guarantees. However, these networks are not actually integrated, but they operate independently from each other. Otherwise, the authors of [12] applied the SDN technology to smart grid heterogeneous networks. They evaluated the data-plane performance of an experimental test-bed using Ethernet, IEEE 802.11 and Broadband Power Line (BPL), and they concluded that the obtained results were compatible with smart grid supervision services. Another remarkable example is UbiFlow [13], which addresses the IoT mobility management issue in wide-scale heterogeneous networks, including WiFi and WiMAX. UbiFlow is formed by coordinated controllers that provide efficient handover, load balancing and flow scheduling based on Network Calculus. Also, industrial heterogeneous wireless networks (IEEE 802.15.4, 802.11 and 802.16) can be centrally controlled with an SDN approach. The authors of [14] proposed a RESTful-based framework that supervised workers’ conditions. This framework manages QoS and reliability by monitoring the state of each communications link. It requires that local agents implemented at each node collects local measurements, which are accessible by a central application.

From a scalability point of view, the original centralized approach does not scale as a distributed one, at least in large-scale networks. However, SDN technologies already allow a network to be controlled by multiple coordinated external agents, which also alleviates bottleneck issues. In any case, the separated control plane should be integrated with discovery, provisioning and monitoring processes of a (NMS). For example, an SDN controller usually discovers all switches and links via LLDP. Once determined, information about the network’s graph topology feeds QoS and policy management modules. Therefore, NMS used in industrial networks could benefit from the SDN reconfigurability.

[5] IETF 6TiSCH Working Group, IPv6 over the TSCH mode of IEEE 802.15.4e.

4.2. Resource allocation

Hard-to-solve routing problems benefit from global view of the network performed by a separate control logic. Consequently, a controller is able to determine suitable provision of resources. After the discovery process, the SDN controller is responsible for performing traffic engineering in CPS networks, configuring the routing path between senders and receivers, whether unicast or multicast streams. This can also include traffic shaping, bandwidth reservation, as well as network virtualization. As a starting point, an architecture for industrial network virtualization is presented in [15], in which a slice manager provides logical isolation by assigning network resources to different automation applications. This slice manager is supposed to be compatible with control protocols such as OpenFlow, ForCES or other industrial Ethernet protocols.

Furthermore, the use of SDN has demonstrated to be effective in providing resources in Local Area Network (LAN) based on the IEC 61850 specification. Dorsch et al. [8] used OpenFlow to establish traffic shaping policies that differentiate high- and low-priority flows in IEC 61850 substations. Moreover, taking into account the importance of layer 2 multicast frames in IEC 61850-based substations, SMARTFlow [16] computes layer 2 multicast trees to forward critical frames and rearrange the paths in case of failure. SMARTFlow was compared to other multicast solutions, such as GARP Multicast Registration Protocol (GMRP).

Given the potential relevance of load balancing in CPSs, an OpenFlow network can overcome the limitations of spanning tree protocols in layer 2 networks by spreading traffic across multiple paths without blocking links. Also, taking the manufacturing systems as a case study, Nayak et al. [6] proposed two routing algorithms to calculate edge-disjoint routes for time-sensitive communication flows. Despite the fact that these algorithms work well with networks with high path diversity, the authors suggested that the time-sensitive traffic should operate in a time-multiplexed manner. Accordingly, the same authors underscored that a logically centralized control plane would simplify the algorithms for such multiplexed access to network resources.

4.3. Time-sensitive SDN

Some heuristic routing algorithms for time-sensitive software-defined networks are presented below. A time-aware network controller should collect relevant performance metrics provided by network devices, such as forwarding latency, to guarantee bounds on latency. This information can be used to compute data paths, and perform traffic scheduling and bandwidth reservation for time-sensitive streams. Nevertheless, the CPS Public Working Group (PWG) asserts that SDN technologies may degrade timing performance, and hence the effect of SDN on timing performance should be carefully studied [3].

It is necessary to mention those research activities that analytically have evaluated the time behavior of SDN systems. Specifically, the authors of [17] used the Network Calculus to model the behavior of SDN switches and controllers, as well as to evaluate admission control for end-to-end real-time (QoS) provisioning. In order to enhance the scalability of a centralized network controller, Huang et al. [17] investigated admission control with flow aggregation, where individual flows with same forwarding and performance requirements are combined. As a consequence, the amount of flows processed by the controller and network devices is reduced. On the other hand, an SDN model for deterministic real-time QoS is proposed in [18]. In this Reference, taking into account that a Mixed Integer Program (MIP) is too resource demanding for realistic-sized industrial networks, the authors proposed an algorithm that reduces the computational cost for solving the routing problem at runtime. From another point of view, routing and priority ordering should be addressed together to support end-to-end hard real-time guarantees.

Focusing now on avionics systems, they are relevant critical scenarios where SDN concept has been recently proposed to achieve deterministic latencies. Heise et al. [4] proved that the OpenFlow protocol performs a similar operation to AFDX. They used the OpenFlow meter tables and the “drop” action when a flow rate is exceeded, while partial matching for MAC addresses is applied to determine the Virtual Links. Then, the authors compared the performance of software and hardware OpenFlow switches versus AFDX, discussing the advantages and shortcomings of using OpenFlow in terms of performance and configuration. Yet, in any case, Heise et al. conceived a static use of OpenFlow, so that a controller installs rules in a bootstrap or maintenance stages, but no controller interaction is assumed during operation. On the other hand, Li et al. [19] understood a “software-defined AFDX” that adapts the QoS configuration depending on the network state and improve the resource utilization. For such purpose, Li et al. aimed to optimize the control channel by reducing the number of out-of-band messages between switches and multiple OpenFlow controllers.

Regarding the scheduling of real-time CPSs, the authors of [20] emphasized that most networking technologies used in safety-critical CPSs, such as SAE AS6802, only support a static pre-configuration. On the other hand, a logically centralized scheduler computing and allocating time slots facilitates the achievement of guarantee bounded delays. Thus, taking into account current trends in CPSs, in which sensors (ie, publishers) and actuators (ie, subscribers) are dynamically plugged, King et al. [20] proposed a publish-subscribe networking middleware where an OpenFlow-based control receives subscription service requests with the QoS specifications. Thus, the controller is responsible for performing the scheduling algorithm, admission control and orchestrating all the network reconfiguration. King et al. evaluated the enhancement in the timing performance compared to a conventional switch. However, as authors noted, it is a preliminary approach which must be extended to complex networks.

Furthermore, one of the main prerequisites to deploy time-sensitive networks is to study how SDN systems interacts with synchronization mechanisms. ReversePTP [21] implements a centralized version of the Precision Time Protocol (PTP), where the switches act as master nodes and the controller as slave, estimating its clock offset. According to the experimental tests, the precision of ReversePTP and PTP are similar. Also, Reference [22] proposed OpenFlow extensions to ensure that a controller interoperates with SyncE networks and it is able to calculate and configure synchronization trees.

Moreover, the explicit use of time measures allows scheduling schemes to be dynamically adapted according to network congestion and delay. In [23], an OpenFlow controller measures the propagation time to dynamically allocate bandwidth, having assumed that network devices are synchronized.

From a performance point of view, the adequacy of OpenFlow hardware and software switches in smart grid scenarios is studied in Reference [24], where multicast packets carried information about measuring electrical waves in the grid (also commonly known as phasor measurement units). The results indicate that OpenFlow is suitable even for demanding real-time applications.

4.4. Industrial-grade reliability

From the point of view of resilience, the previously-mentioned distributed control approach avoids single points of failures, mitigating robustness problems. But in any case, by decoupling control and data planes, two scenarios are distinguished: in-band and out-of-band control planes. On the one hand, an in-band configuration does not need additional physical resources, whereas an out-of-band control plane may result expensive for Wide Area Network (WAN) with multiple controllers. On the other hand, not separating control from data traffic may involve reliability issues as network failures affect both planes; in that event the control channel needs to repair before the controller can recover the data plane. Since both approaches have advantages and disadvantages depending on the specific use case, a hybrid model is suggested in which out-of-band control is used in a failure free scenario, reverting to in-band control when the out-of-band network goes down.

From another point of view, mobile environments serve to emphasize the importance of maintaining the connectivity of the control channel, since wireless links suffer from unreliable data transmission. As Huang et al. identified [25], mobile scenarios might affect the liveness of a controller-switch connection. Accordingly, Huang et al. strengthened the survivability of SDN-based vehicular networks by adding a packet-processing service in the data plane. Specifically, network devices employ connection state detection and self-learning mechanism, so that the amount of control packets is reduced. Unlike a pure SDN approach and facing the possibility of a control connection failure, robustness can be improved through hybrid networks.

Furthermore, in connection with Operations, Administration and Management (OAM) functions, it has been proved that the failure detection is more efficient and scalable when it is handled by distributed network components than when it is performed by a centralized controller (eg, through the topology discovery service using LLDP). As a consequence, the Open Networking Foundation, which is in charge of standardizing and promoting the OpenFlow protocol, stated that "rapid protection switching implies that the associated protocols and state machines" must reside on network elements themselves, "with the SDN controller responsible for pre-computing recovery resources, provisioning recovery behavior and subscribing to notifications".

With regard to SDN proposals for improving reliability of mission-critical CPSs, a controller can provide failover mechanisms by populating the forwarding tables either in advance, so that pre-installed instructions serve as backup rules, or on-demand by network devices. Thus, for example, an SDN controller could make reliable routing decisions based on the location and movement information of mobile nodes. Otherwise, the authors of [8] analyzed the failover performance of IEC 61850 traffic, by comparing an SDN solution with routing legacy algorithms (OSPF and MPLS with RSVP-TE) in terms of recovery time and QoS for different type of traffic. Despite pre-calculating alternative routes, which speeds up the recovery process, the solution proposed in [8] involved an interaction with an OpenFlow controller. Namely, switches notify link/ports failures to the controller, which has to re-route traffic by modifying the forwarding tables. On the contrary, starting on version 1.1, the OpenFlow protocol enables the self-healing of a switch through the "Fast failover" feature, which achieves an automated recovery upon a network failure. This avoids discovery and convergence delays, and reduces the recovery time as compared to (RSTP) because.

Given the relevance of multicast publisher/subscriber schemes in cyber-physical networks, different research approaches have focused on protecting these streams. Specifically, the authors of [26] proposed algorithms that proactively or reactively deploy multicast backup multicast trees. These authors not only presented the fault tolerance of their scheme, but also the required number of control messages. Furthermore, the approach adopted by Popovic et al. [27] guaranteed zero recovery time in case of single failures. This was achieved by constructing node-redundant multicast trees that are used in parallel. Popovic et al. based their solution on active redundancy, as indicated by the IEC 62439-3 standard. In this regard, Reference [7] exploited the SDN features to develop an analytical model that considers the timing constraints of traffic in heterogeneous Machine-to-Machine (M2M) communications. Thus, they consider the simultaneous transmission of real-time data via multiple paths, while non-real-time traffic is forwarded along distinct routes to the destination.

The use of previously-mentioned multipath solutions could be also leveraged to prevent eavesdropping or tampering of sensitive information. Other SDN-based security techniques are presented below.

4.5. Network security in Cyber-Physical Systems

From the security perspective, besides the previously identified traffic isolation, an external controller is able to enforce filtering rules that prevent cyber-physical networks from malicious attacks. In an SDN approach, dynamic security policies can restrict the communication paths to only those required by the control applications. Thus, the amount of potential attacks in CPSs will be reduced as the number of allowed connections decreases. Genge et al. [28] gathered an overview of mechanisms for protecting ICS and emphasized the opportunities of SDN. They described a possible SDN controller intervention to protect sensitive streams against Distributed Denial of Service (DDoS) attacks. Also, Genge et al. suggested the realization of complex intrusion and anomaly detection modules that alert the controller to block or re-route malicious traffic.

Furthermore, References [28,29] proposed emulation tools for CPSs and they studied how an OpenFlow-based control served in the detection and prevention of attacks. In [29], the Mininet network emulator is connected to a set of simulated and physical processes and industrial protocols. These tools are used to demonstrate the mitigation of DDoS attacks [28] and Man-in-the-Middle (MitM) ones [29]. In any case, these proposals rely on constant monitoring, which allows a central service to detect anomalous activity or exceeding a certain threshold, and hence to reconfigure the network accordingly.

It is interesting to note that a centralized controller could facilitate Denial of Service (DoS) attacks. Therefore, it is recommended to distribute the control plane, avoiding single points of configuration.

4.6. Interoperability and standardization of SDN

To connect collaborative CPS ecosystems, such as, for example, autonomous vehicles interacting with intelligent transportation systems, standard interfaces and protocols are clearly required. In fact, open standards reduce reliance on vendor-specific appliances and facilitate seamless integration of CPSs. For example, the NIST Framework and Roadmap for Smart Grid Interoperability[6] has identified relevant protocols and has grouped them according to the principal domain that they apply to.

In this way, the emerging SDN concept tends to homogenize the low-level interfaces. Unlike proprietary implementations, the control of vendor-neutral network devices is unified as the forwarding tables are configured by open protocols between controllers and network devices, which enables the manageability and interoperability of heterogeneous cyber-physical networks. However, an important challenge is the compatibility of SDN with proprietary or legacy systems. Thus, a preliminary proposal for the integration of the SDN concepts with the PROFINET standard is provided in [30]. Also, the SUNSEED project[7] studied the combination of Multiprotocol Label Switching (MPLS) and SDN technologies for Wide Area Measurement System (WAMS) in smart grid communications.

The use of SDN in CPSs is receiving interest from standardization bodies, such as the Institute of Electrical and Electronic Engineers (IEEE) or the Internet Engineering Task Force (IETF). Concerning the former, focused on layers 1 and 2, the IEEE 802.1 Time-Sensitive Networking (TSN) Task Group[8] promotes the interoperability between networked devices. It has proposed Ethernet extensions that include the Stream Reservation Protocol (SRP, 802.1Qcc) to implement admission control and resource reservation to guarantee QoS, as well as parallel redundancy schemes. TSN and SDN complement each other and fit together, since IEEE 802.1 TSN systems allow a central control element to compute and establish the demanded network resources. Moreover, according to the IEEE 802.1CF project, “modern heterogeneous networks, such as smart grid, home automation, and IoT suffer from limitations in service control, security and provisioning”. Hence, this project follows the SDN principles with the aim of unifying shared network control interfaces, and the reducing the barriers to new network technologies and network operators.

Regarding the IETF initiatives, whose interest lies in the upper layers, the newly-formed Deterministic Networking (DetNet) group aims to establish time-sensitive solutions in (WAN). After analyzing requirements and use cases, the DetNet group has adopted an SDN architecture to support the required traffic engineering capabilities. In the same way, the 6TiSCH protocol is another IETF initiative to centralize the flow scheduling and route computation tasks in time-sensitive wireless networks, and it considers that existing SDN protocols could be extended to address such needs.

Besides these ongoing activities, there are several research funded projects aimed at implementing SDN-based CPS architectures. In line with the Industry 4.0 principles, these projects advocate for software-defined industrial control architectures that simplify the network configuration. For instance, the VIRTUWIND project[9] has among its objectives to define programmable industrial networks in operational wind parks via SDN. Another example is the SAFURE project[10], which gives an SDN controller the responsibility for reconfiguring safety-critical real-time networks.

In any case, despite all these efforts towards interoperable systems, there is still a need for close coordination between standardization bodies, industry forums and open-source projects in order to support multi-vendor networks.

[6] NIST Smart Grid Framework.

[7] SUNSEED (Sustainable and robust networking for smart electricity distribution) FP7-ICT project.

[8] IEEE Time-Sensitive Networking Task Group.

[9] VIRTUWIND (Virtual and programmable industrial network prototype deployed in operational Wind park) 5G-PPP Project.

[10] SAFURE (SAFety and secURity by design for interconnected mixed-critical cyber-physical systems) H2020 Project.

Table 2
SDN characteristics relevant to CPSs and open research issues.

	CPS needs	SDN provides
Manageability and interoperability	Support heterogeneous traffic and topologies from different applications	Integration of management and monitoring functionalities into a logically centralized controller with a global view of the network
There is the need to support overlapping decentralized control schemes, but maintaining global meaningful information and consistency		
Resource allocation and real-time performance	Network management using context information and predictable timing behavior	Flow-based forwarding and dynamic adaptation of QoS and scheduling policies according to the network conditions Simplification of load balancing and multipath techniques
To improve predictability of SDN applications, it is necessary to use timing as a correctness criterion and to include detailed analyses of the temporal performance in the implementation of network functions		
Reliability and security	High availability and scalability	Computation and installation of protection paths using a distributed control plane
	Attack prevention, detection and mitigation	Anomalous event detection and situational awareness system Isolation by enforcing high-level security policies
To support reliable mission-critical services, safety and security-by-design methodologies should be developed for validation and verification of software systems		

4.7. Summary and future directions

After analyzing the potential of applying SDN to CPSs, Table 2 briefly summarizes some SDN characteristics that meet essential needs of CPSs, as well as challenges ahead for future research.

As gathered from the literature, SDN has drawn much research attention in the industrial networking arena. As an example of a commercial product, Fujitsu[11] has implemented an SDN-based packet optical networking platform in utilities and energy sectors. However, SDN is in an early developmental stage, and its adoption in mission-critical systems is a major challenge that still requires extensive experimental validation. Indeed, future research could be hindered by the lack of testing in realistic production scenarios. On the other hand, the long life cycles of industrial network equipment protect the investment already made [1]. Thus, it can be assumed that resistance to change in IT systems, as well as organizational characteristics, may affect the growing acceptance of SDN in existing CPSs.

5. Conclusion

The scope of CPSs is extremely broad, ranging from smart factories to energy and transportation domains. The control and management of cyber-physical networks should be tightly coupled to the underlying conditions. However, traditional network control strategies generally fail to support for heterogeneous and dynamic environments. This paper highlights the emerging trends in CPSs and reviews the benefits and challenges of adopting SDN technologies, achieving adaptive mission-critical infrastructures. As outlined, an SDN substrate forms a closed-loop feedback control that reconfigures QoS and routing policies according to changes in the CPS context, while guaranteeing security, reliability, and real-time requirements at the same time.

Acknowledgement

The work described in this paper was produced within the Training and Research Unit UFI11/16 funded by the University of the Basque Country (UPV/EHU). This research was partly funded by the Spanish Ministry of Economy and Competitiveness under the “Secure deployment of services over SDN and NFV based networks” project S&N-SEC TEC2013-47960-C4-3-P.

References

[1] Sauter T. The three generations of field-Level networks - evolution and compatibility issues. Ind Electr IEEE Trans 2010;57(11):3585–95. http://dx.doi.org/10.1109/TIE.2010.2062473.

[2] Gungor V, Lu B, Hancke G. Opportunities and challenges of wireless sensor networks in smart grid. Ind Electr IEEE Trans 2010;57(10):3557–64. http://dx.doi.org/10.1109/TIE.2009.2039455.

[3] National Institute of Standards and Technology (NIST). Framework for cyber-physical systems; 2016. Release 1.0.

[4] Heise P, Geyer F, Obermaisser R. Deterministic OpenFlow: performance evaluation of SDN hardware for avionic networks. In: network and service management (CNSM), international conference on; 2015. p. 372–7. http://dx.doi.org/10.1109/CNSM.2015.7367385.

[5] Sehgal A, Perelman V, Kuryla S, Schonwalder J. Management of resource constrained devices in the internet of things. Commun Mag IEEE 2012;50(12):144–9. http://dx.doi.org/10.1109/MCOM.2012.6384464.

[11] Fujitsu, Software-Defined Networking for the Utilities and Energy Sector.

[6] Nayak NG, Durr F, Rothermel K. Software-defined environment for reconfigurable manufacturing systems. In: Internet of Things (IOT), international conference on the; 2015. p. 122–9. http://dx.doi.org/10.1109/IOT.2015.7356556.

[7] Lien S-Y. Resource-optimal heterogeneous machine-to-Machine communications in software defined networking cyber-Physical systems. Wireless Person Commun 2015;84(3):2215–39. http://dx.doi.org/10.1007/s11277-015-2560-6.

[8] Dorsch N, Kurtz F, Georg H, Hagerling C, Wietfeld C. Software-defined networking for smart grid communications: applications, challenges and advantages. In: Smart grid communications (SmartGridComm), IEEE international conference on; 2014. p. 422–7. http://dx.doi.org/10.1109/SmartGridComm.2014.7007683.

[9] Hu L, Qiu M, Song J, Hossain M, Ghoneim A. Software defined healthcare networks. Wireless Commun IEEE 2015;22(6):67–75. http://dx.doi.org/10.1109/MWC.2015.7368826.

[10] Kim J, Ko Y-B, Filali F. A lightweight CoAP-based software defined networking for resource constrained AMI devices. In: smart grid communications (SmartGridComm), IEEE conference on; 2015. p. 1–6.

[11] Han S, Mok A, Meng J, Wei Y-H, Huang P-C, Leng Q, et al. Architecture of a cyberphysical avatar. In: Cyber-physical systems (ICCPS), ACM/IEEE conference on; 2013. p. 189–98. http://dx.doi.org/10.1145/2502524.2502550.

[12] Rinaldi S, Ferrari P, Brandao D, Sulis S. Software defined networking applied to the heterogeneous infrastructure of Smart Grid. In: factory communication systems (WFCS), IEEE conference on; 2015. p. 1–4. http://dx.doi.org/10.1109/WFCS.2015.7160573.

[13] Wu D, Arkhipov D, Asmare E, Qin Z, McCann J. UbiFlow: Mobility management in urban-scale software defined IoT. In: computer communications (INFOCOM), IEEE conference on; 2015. p. 208–16. http://dx.doi.org/10.1109/INFOCOM.2015.7218384.

[14] Gisbert JR, Palau C, Uriarte M, Prieto G, Palazón JA, Esteve M, et al. Integrated system for control and monitoring industrial wireless networks for labor risk prevention. J Netw Comput Appl 2014;39:233–52. http://www.sciencedirect.com/science/article/pii/S1084804513001744.

[15] Huth H-P, Houyou A. Resource-aware virtualization for industrial networks: a novel architecture combining resource management, policy control and network virtualization for networks in automation or supervisory control and data acquisition networks. In: data communication networking (DCNET), international conference on; 2013. p. 1–7. http://dx.doi.org/10.5220/0004508900440050.

[16] Lopes Y, Fernandes NC, Bastos CAM, Muchaluat-Saade DC. SMARTFlow: a solution for autonomic management and control of communication networks for smart grids. In: applied computing, ACM symposium on; 2015. p. 2212–17. ISBN 978-1-4503-3196-8. doi:10.1145/2695664.2695733.

[17] Huang J, He Y, Duan Q, Yang Q, Wang W. Admission control with flow aggregation for QoS provisioning in software-defined network. In: global communications conference (GLOBECOM), IEEE; 2014. p. 1182–6. http://dx.doi.org/10.1109/GLOCOM.2014.7036969.

[18] Guck J, Reisslein W, Kellerer W. Model-based control plane for fast routing in industrial QoS networking. In: Quality of service (IWQoS), IEEE/ACM 23nd international symposium of; 2015. p. 65–6. http://dx.doi.org/10.1109/IWQoS.2015.7404708.

[19] Li Z, Li Q, Zhao L, Xiong H. Openflow channel deployment algorithm for software-defined AFDX. digital avionics systems conference (DASC), IEEE/AIAA; 2014. 4A6–1–4A6–10 http://dx.doi.org/10.1109/DASC.2014.6979466.

[20] King A, Chen S, Lee I. The MIDdleware assurance substrate: enabling strong real-time guarantees in open systems with OpenFlow. In: Object/Component/Service-oriented real-time distributed computing (ISORC), IEEE symposium on; 2014. p. 133–40. http://dx.doi.org/10.1109/ISORC.2014.49.

[21] Mizrahi T, Moses Y. Using ReversePTP to distribute time in software defined networks. In: Precision clock synchronization for measurement, control, and communication (ISPCS), IEEE symposium on; 2014. p. 112–17. http://dx.doi.org/10.1109/ISPCS.2014.6948702.

[22] Suarez R, Rincon D, Sallent S. Extending OpenFlow for SDN-enabled synchronous ethernet networks. In: Network softwarization (NetSoft), IEEE conference on; 2015. p. 1–6. http://dx.doi.org/10.1109/NETSOFT.2015.7116183.

[23] Miyata H, Namiki M, Sato M. pmqFlow: design of propagation time measuring QoS system with OpenFlow for process automation. In: Industrial electronics society (IECON), conference of the IEEE; 2014. p. 3693–9. http://dx.doi.org/10.1109/IECON.2014.7049049.

[24] Goodney A, Kumar S, Ravi A, Cho Y. Efficient PMU networking with software defined networks. In: Smart grid communications (SmartGridComm), IEEE conference on; 2013. p. 378–83. http://dx.doi.org/10.1109/SmartGridComm.2013.6687987.

[25] Huang T, Yan S, Yang F, Pan T, Liu J. Building SDN-based agricultural vehicular sensor networks based on extended open vswitch. Sensors 2016;16(1):108. http://dx.doi.org/10.3390/s16010108. http://www.mdpi.com/1424-8220/16/1/108.

[26] Gyllstrom D, Braga N, Kurose J. Recovery from link failures in a Smart Grid communication network using OpenFlow. In: Smart grid communications (SmartGridComm), IEEE conference on; 2014. p. 254–9. http://dx.doi.org/10.1109/SmartGridComm.2014.7007655.

[27] Popovic M., Khalili R., Le Boudec J.-Y. Performance Comparison of Node-Redundant Multicast-Distribution Trees in SDN-Based Networks; 2015. Technical Report.

[28] Genge B, Graur F, Haller P. Experimental assessment of network design approaches for protecting industrial control systems. Int J Crit Infrastruct Prot 2015;11:24–38. http://dx.doi.org/10.1016/j.ijcip.2015.07.005. http://www.sciencedirect.com/science/article/pii/S1874548215000463.

[29] Antonioli D, Tippenhauer NO. MiniCPS: a toolkit for security research on CPS networks. In: Cyber-physical systems-security and/or PrivaCy, ACM workshop on; 2015. p. 91–100. ISBN 978-1-4503-3827-1. http://doi.acm.org/10.1145/2808705.2808715.

[30] Ahmed K, Blech J, Gregory M, Schmidt H. Software defined networking for communication and control of cyber-physical systems. In: Parallel and distributed systems (ICPADS), IEEE international conference on; 2015. p. 803–8. http://dx.doi.org/10.1109/ICPADS.2015.107.

Elias Molina is currently a PhD student at the University of Basque Country (UPV/EHU). He received a B. Sc. degree in Telecommunication Engineering from the University of Seville and an M. Sc degree in ICTs and Mobile Networks from the UPV/EHU, in 2010 and 2012, respectively. He worked from 2010 to 2012 as a trainee engineer in Tecnalia Research & Innovation.

Eduardo Jacob received his MSc in Industrial Communications and Electronics from the University of the Basque Country (UPV/EHU) in 1991. He received his PhD in ICT at the same university in 2001. He is an assistant professor at the Faculty of Engineering of Bilbao, where he is acting as the Head of the Communications Engineering Department and leads the I2T research lab.