applied sciences

MDPI

Article

Towards Flexible Integration of 5G and IIoT Technologies in Industry 4.0: A Practical Use Case

Jorge Sasiain, Ane Sanz, Jasone Astorga and Eduardo Jacob *

Department of Communications Engineering, Faculty of Engineering in Bilbao, University of the Basque Country UPV/EHU, Plaza Ingeniero Torres Quevedo, 1, 48013 Bilbao, Spain; jorge.sasiain@ehu.eus (J.S.); ane.sanz@ehu.eus (A.S.); jasone.astorga@ehu.es (J.A.)

* Correspondence: eduardo.jacob@ehu.eus; Tel.: +34-946-014-214

Received: 27 September 2020; Accepted: 26 October 2020; Published: 29 October 2020

Abstract: The Industry 4.0 revolution envisions fully interconnected scenarios in the manufacturing industry to improve the efficiency, quality, and performance of the manufacturing processes. In parallel, the consolidation of 5G technology is providing substantial advances in the world of communication and information technologies. Furthermore, 5G also presents itself as a key enabler to fulfill Industry 4.0 requirements. In this article, the authors first propose a 5G-enabled architecture for Industry 4.0. Smart Networks for Industry (SN4I) is introduced, an experimental facility based on two 5G key-enabling technologies—Network Functions Virtualization (NFV) and Software-Defined Networking (SDN)—which connects the University of the Basque Country's Aeronautics Advanced Manufacturing Center and Faculty of Engineering in Bilbao. Then, the authors present the deployment of a Wireless Sensor Network (WSN) with strong access control mechanisms into such architecture, enabling secure and flexible Industrial Internet of Things (IIoT) applications. Additionally, the authors demonstrate the implementation of a use case consisting in the monitoring of a broaching process that makes use of machine tools located in the manufacturing center, and of services from the proposed architecture. The authors finally highlight the benefits achieved regarding flexibility, efficiency, and security within the presented scenario and to the manufacturing industry overall.

Keywords: industry 4.0; 5G; NFV; SDN; IIoT; access control; manufacturing process; aeronautics advanced manufacturing center

1. Introduction

Currently, a revolution is taking place in the way manufacturing processes are being designed. This revolution, generally labeled Industry 4.0 [1], envisions fully interconnected scenarios in the manufacturing industry to improve the efficiency, quality, and performance of the manufacturing processes. Industry 4.0 embraces the use of information and communication technologies in industrial scenarios to achieve a greater smartization and autonomy of the manufacturing processes through the integration of cyber-physical systems and the interconnection of machines, devices, sensors, and people.

On 1 June 2017, the European Parliament adopted a resolution on developing an integrated industrial digitalization strategy for the EU [2], highlighting "a cutting-edge digital infrastructure", as one of its four pillars. This pillar targets not only applications but also infrastructure improvements. It is precisely in the delivery of this flexible, agile, and resilient infrastructure and in the evolution towards fully interconnected scenarios where communication technologies can play a decisive role.

Two of these technologies that are additionally concerned with this article are Network Functions Virtualization (NFV) and Software-Defined Networking (SDN), both of which are considered key

enablers of the fifth generation of mobile networks (5G) to achieve a flexible and agile network platform over which to deploy heterogeneous services [3,4]. These technologies represent an evolution towards the softwarization and virtualization of the network infrastructure and the network functions. The integration of NFV and SDN in the manufacturing industry (Figure 1) can greatly simplify the design and deployment cycle of new and innovative manufacturing services while achieving better utilization of computing and networking physical resources.

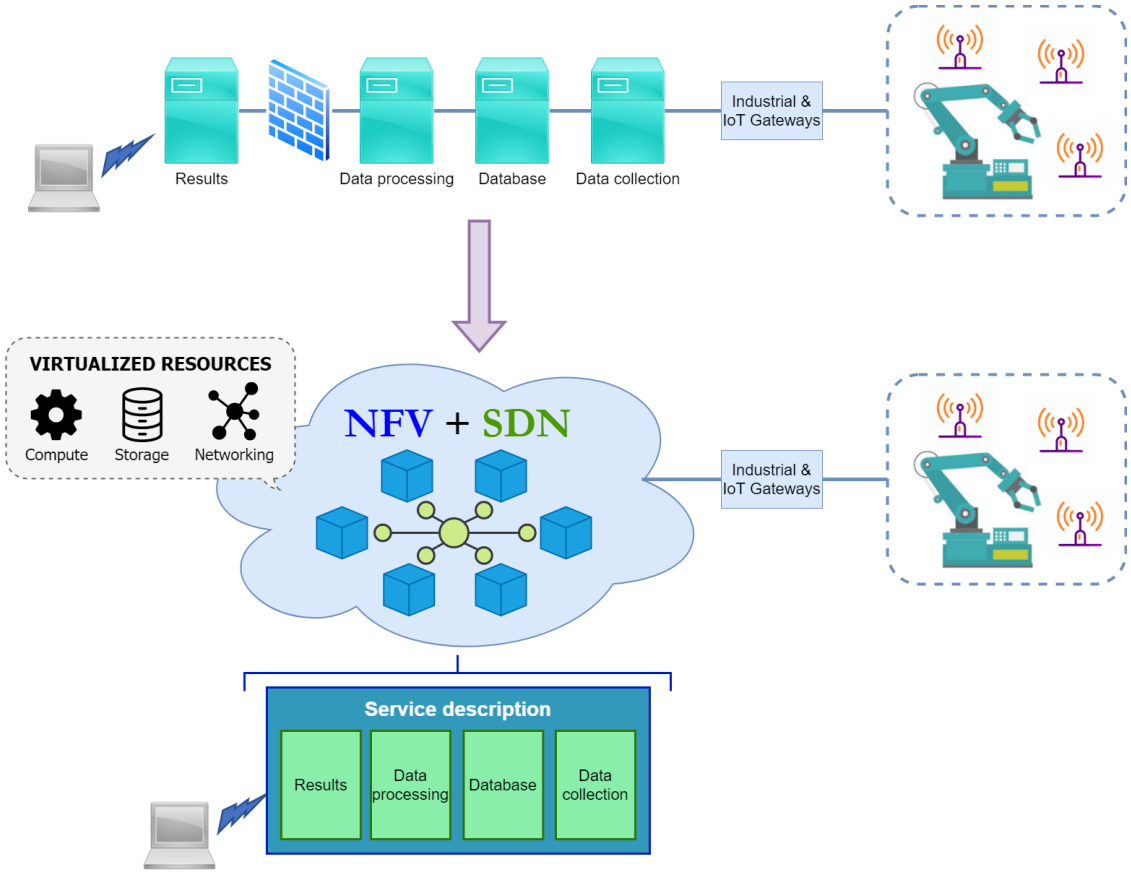

Figure 1. Integration of Industry 4.0 with Network Functions Virtualization (NFV) and Software-Defined Networking (SDN).

In contrast, traditional network architectures present several shortcomings in regards to flexibility, accessibility, and dynamicity that can be further aggravated in industrial scenarios where the coexistence with heterogeneous devices, machine tools, and industry-specific protocols is a reality. These problems and limitations can be summarized as follows:

- Deployment times of new services are slow and often involve the acquisition of dedicated hardware components to support specific functionalities. This is also tied to an inefficient use of hardware resources. Not only does this have an impact on the deployment costs, but also on the overall quality of the manufacturing processes. It can also negatively impact innovation in the manufacturing industry.
- Services are difficult to re-utilize. A solution specifically deployed for a given manufacturing process or machine tool may be directly applicable to satisfy the requirements of other ones. However, there are no convenient mechanisms to ease the re-utilization of services in such cases, often leading to duplication of efforts and resources in setting them up.

- Configurability of services is limited. Solutions are deployed rather statically and the lifecycle management or reconfiguration of a service often requires significant manual intervention and hardware manipulation, and sometimes even the acquisition of additional hardware components.
- The isolation between different business processes is difficult to enforce and manage. The concerns in relation to the privacy and security of critical data mean that some processes are not connected to a shared network infrastructure or to the Internet, limiting their capabilities.

The Industry 4.0 paradigm also envisions the integration of Industrial Internet of Things (IIoT) technologies [5]. These technologies consist of a massive deployment of interconnected devices which are responsible for gathering, analyzing, sending, and monitoring data on a large scale. Most of these IIoT applications comprise small sensors with limited capabilities and resources, named Constrained Device Sensor (CDS). These interconnected sensors form a Wireless Sensor Network (WSN), in which the CDSs are able to communicate with each other making use of suitable communication protocols. IIoT technologies enable the achievement of most of the Industry 4.0 main objectives, such as the increase of the manufacturing process efficiency, the reduction of production times, and the improvement of the user experience.

However, the integration of WSNs into industrial environments comes with security issues that must be overcome. The wireless nature of the sensors comprising the WSN and their limited processing capacity leads to a higher vulnerability to attacks. This implies the need of introducing robust security mechanisms that avoid unauthorized attacks such as data tampering or data filtration. Moreover, as these devices do not support traditional security mechanisms due to their heavy constraints, protecting these devices is not straightforward, becoming a hindrance to achieving secure IIoT applications.

The objectives of the present article are threefold. The first objective is to develop an NFV- and SDN-enabled architecture capable of overcoming the aforementioned limitations. In this regard, the pursued goals are to move away from static solutions over dedicated hardware and evolve towards the more cost- and resource-efficient virtualization and softwarization mechanisms; improve the accessibility, reusability, and lifecycle management of services; and provide highly granular service isolation at data and performance levels. To realize this first objective, the introduction of Smart Networks for Industry (SN4I) is proposed, an NFV- and SDN-enabled experimental facility deployed across the Faculty of Engineering in Bilbao (EIB) and the Aeronautics Advanced Manufacturing Center (CFAA). SN4I has been envisioned to study the integration of NFV and SDN technologies in coexistence with industrial networks and protocols whilst enabling the deployment of innovative manufacturing services leveraging the benefits of these technologies.

The second objective is to integrate several CDSs in a WSN supported by the NFV- and SDN-enabled infrastructure to make possible the integration of IIoT applications. These IIoT applications will be strengthened by the use of a lightweight access control protocol that prevents them from receiving unauthorized accesses to the sensors and improves the security vulnerabilities that wireless scenarios entail. Moreover, this protocol will also provide a dynamic and fine-grained access control between the users and the sensors, enabling a flexible behavior of the IIoT applications. The WSN will also leverage the benefits of SDN and NFV in regards to network slicing and overall flexibility, providing added dynamicity to the integration of sensor services into different processes.

The third objective is to demonstrate a use case deployed over such infrastructure in a manufacturing center that also permits to validate the architecture. It consists of the monitoring of a broaching process in the CFAA through the integration of virtualized Machine Learning (ML) services to enhance the process, as well as services from the WSN for additional data gathering. To feed the ML algorithms, data from the broaching process will be collected from several broaching tool components, and, additionally, information related to environmental conditions will be gathered from the CDSs in the WSN. The description of the use case in the present article focuses on discussing how the services and components involved in this use case have been integrated into the proposed infrastructure.

The article is structured as follows. Section 2 addresses the related work in the field of NFV and SDN technologies in industrial scenarios and the securization of IIoT applications. Section 3 describes the main technologies concerned with the article, and Section 4 gives a detailed explanation of the aforementioned SN4I experimental facility. Then, in Section 5, the use case of a 5G-enabled smart broaching process is presented. Following that, Section 6 illustrates the main benefits provided by this work. Finally, Section 7 gathers the main conclusions.

2. Related Work

This section gathers related works both in terms of the application of NFV and SDN 5G technologies to industrial scenarios so as to the securization of such scenarios.

2.1. 5G, NFV and SDN in Industrial Environments

The 5GPPP association, a European initiative concerned with the delivery of solutions, architectures, technologies, and standards for the ubiquitous next-generation communication infrastructures [6], identified seven different verticals to the targets of the next wave of 5G applications: Automotive, Manufacturing, Media, Energy, Public Safety and SmartCities. A series of R&D projects under the 5GPPP programme such as 5GTANGO [7], 5G SMART [8], 5G CONNI [9], and 5G-Transformer [10] has worked on developing 5G pilots for several of these vertical use cases, with some of them focusing on smart manufacturing and Industry 4.0 use cases. There are also initiatives such as the 5G Alliance for Connected Industries and Automation (5G-ACIA) [11] pushing for the integration of 5G technologies in the manufacturing vertical. Fraunhofer's International Center for Networked, Adaptive Production (ICNAP) [12], was founded in late 2016 to find out which new approaches in information technology can lead the way towards Industry 4.0.

NFV and SDN are consolidated technologies that have provided substantial benefits to the world of communications and computing for the past decade. However, as vertical industries evolve towards an adoption of the emerging 5G technologies [13], the range of application of 5G technologies such as NFV and SDN is expanding. Wollschlaeger et al. [14] presented a review of technological trends in the world of industrial communication, highlighting the role of 5G technologies in industrial automation. The article calls for the adoption of 5G technologies such as NFV and SDN to achieve harmonized service provisioning on top of the heterogeneity and complexity of industrial networks, in which Ethernet and 5G communication and legacy industrial communication systems will likely coexist. Similarly, Rao and Prasad [15] highlighted the critical role that 5G technologies will play in enabling the ultra-low latency and reliability and high data rate requirements of Industry 4.0, and in driving several of its use cases.

Precisely, several efforts to bring NFV and SDN technologies into industrial environments have already been carried in the context of the Industry 4.0 revolution. These contributions align with the fundamental intentions of the present article, as they demonstrate that the intelligence and overall quality of industrial processes can be enhanced thanks to more flexible and fine-grained communications while addressing limitations of traditional network architectures such as lack of automation and adaptivity to varying and requirements imposed by heterogeneous use cases. Ma et al. [16] proposed the deployment of an SDN-based infrastructure in an industrial environment, which, also leveraging network virtualization and NFV for the implementation of network services, optimizes service quality and improves industrial production efficiency. Peuster et al. [17] demonstrated how NFV technology can greatly simplify the realization of a smart manufacturing application, in which several network services are deployed to interconnect machines and to collect and aggregate sensor data. Mekikis et al. [18] showcased the implementation of a 5G experimental platform for Tactile Internet in industrial environments leveraging NFV and SDN technologies. Other work (e.g., [19,20]) focus on the applicability of NFV and SDN to deploy security services and enhance security in industrial networks. Although this is not specifically a direct objective of the integration of NFV and SDN in our work, they illustrate how the adoption of these technologies can lay the

foundations for the implementation of more robust and flexible security mechanisms and applications in comparison to traditional industrial networks.

In regards to solutions aimed at providing additional flexibility and dynamicity to IIoT networks through the adoption of NFV and SDN technologies, the authors of [21,22] proposed the introduction of network slicing mechanisms in IIoT scenarios with a large amount of sensors deployed for different monitoring purposes. They focused on applying network slicing to address varying Quality of Service requirements of different IIoT applications. This differs from our intentions of leveraging network slicing to rather enable a dynamic assignment of these IIoT applications to different business processes.

2.2. Security for IIoT Applications

The development of IIoT applications involves the deployment of a large number of resource-deprived sensors to gather data on a massive scale, in order to feed ML algorithms that will improve decision-making and smartize manufacturing processes. The use of such limited devices has meant that, when designing IIoT applications, the development of lightweight and feasible communication protocols has been prioritized, leaving security issues in the background. In fact, most IIoT industrial communication protocols used today, such as MQTT, AMQP, and XMPP, rely on implementing Transport Layer Security (TLS) [23] or Datagram Transport Layer Security (DTLS) [24] at the transport layer for building their secure version.

The realization of the Industry 4.0 concept, based on massive data gathering and artificial intelligence techniques, will result in improved manufacturing processes and decision making. However, it will also open the door to new security vulnerabilities coming from the Internet and not known to the traditionally isolated industrial environments. The authors of [25–27] presented the features and challenges of security and privacy for IoT. Although the implementation of secure transport layer channels is essential to build secure communications, it is not enough, and application layer security mechanisms for IoT must also be developed. Such security mechanisms have already been researched and developed for Internet-connected resource-rich devices and communications for years, and are widely used nowadays. However, traditional security mechanisms designed and evaluated for the resource-rich devices are not directly applicable to IoT environments, due to the high resource constraints of the IoT devices. In fact, security mechanisms widely used in the traditional Internet require high computational capabilities and storage capacity, features not available in current IoT devices. For this reason, in addition to using lightweight and feasible application layer industrial protocols, IoT networks require also the development of specific security mechanisms that will take the special characteristics of the targeted environments into account.

Regarding the protection of data confidentiality and integrity at the application layer, Object Security for Constrained RESTful Environments [28] (OSCORE) has been proposed. However, this protocol is specifically tailored to the operation of the CoAP [29] protocol and is not easily extensible to other protocols such as MQTT, XMPP, etc. This protocol makes it possible to protect the integrity and confidentiality of CoAP messages even when the communication includes a proxy, which is usual in industrial communication, and, therefore, the DTLS session is terminated at the proxy.

Nevertheless, implementing security mechanisms that protect the confidentiality and integrity of the communications is not enough to have a secure IoT application. In fact, while traditional IoT scenarios comprise sensors that gather data and send it to a centralized server, the next-generation IoT, designed for Industry 4.0, envisions the use of smart sensors behaving as small servers. In such scenarios, the clients establish a direct end-to-end (E2E) connection with the sensors in order to get the data. Moreover, these scenarios also allow some kind of configuration of the sensor parameter by the end users. Therefore, in these new applications, it is very important to implement a strong access control process, in order to guarantee that only authorized users establish a connection with the sensors. Besides, due to the dynamic nature of IoT applications, the access control solutions should be as expressive as possible, in order to evaluate not only the permissions of the users but also the local context conditions.

Different approaches have been carried out to develop access control mechanisms for the IoT. On the one hand, some traditional solutions have been adapted for the IoT. For example, Seitz et al. [30] proposed the Authorization Framework for the IoT, which adapts eXtensible Access Control Markup Language (XACML) for IoT applications. This proposal defines very expressive security policies, but they are too heavy to be implemented in the most constrained devices. Similarly, Zhang and Gong [31] proposed the Usage-based access control (UCON) adapted to IoT. However, these two approaches are based on a centralized architecture, where a central server performs all the access control processes, so they do not offer any expressiveness as they do not take into account any local condition of the devices.

Among the solutions based on a distributed architecture, Hernández-Ramos et al. [32] proposed Distributed Capability-Based Access Control (DCapBAC) for IoT, which offers capability-based access control, exchanging tokens that contain information about the users and their permissions. However, this mechanism has been developed using Java, and, as its framework is rather heavy, it is not suitable for most constrained devices.

Another possible solution is the Delegated CoAP Authentication and authorization Framework (DCAF), proposed in [33], which uses security policies that consider local conditions of the sensors. However, the implementation of this mechanism requires the establishment of DTLS channels, and this increases the overhead of the messages exchanged, wasting the resources of the devices. Moreover, this solution uses Concise Binary Object Representation [34] (CBOR) to encode and compress the policies, and as it is a generic compressor, it does not offer a high enough compression rate.

To deal with some of the aforementioned problems, the Ladon [35] protocol was developed, an access control solution feasible even in the most constrained devices. This protocol performs the authentication and E2E authorization of the users wanting to access a resource in the sensors. However, the security policies it uses are rather static, reducing the expressiveness of the process. As an evolution of Ladon, Hidra [36] allows for the enforcement of highly expressive policy-based security policies which also include local context conditions, such as battery level. For this reason, this work proposes to extend the applicability scenarios of Hidra by integrating it in a 5G-enabled industrial environment as an orchestrated NFV network service. In this way, the IIoT applications can implement robust access control mechanisms in a fast and flexible way.

3. Building Technologies

This section provides an overall overview of the main technologies upon which the proposed 5G-enabled industrial network is built.

3.1. NFV and SDN

As previously stated, the core technologies that realize the proposed infrastructure are NFV and SDN. Each of them plays a critical role in enabling a more agile, flexible, and cost-efficient provisioning of network services.

NFV technology is concerned with the abstraction, or decoupling, of network functions from physical hardware. Thanks to virtualization, a plethora of application services (such as data processing services) and network services (such as firewalls and NAT) that have traditionally run on dedicated servers and appliances can be relocated into commodity hardware as virtual services. Each of the hardware servers comprising an NFV infrastructure exposes their available physical resources (such as CPU, memory disk, and network interfaces) as virtual resources, and each virtual service or virtual service component is assigned a specific portion of these virtual resources on demand. Virtual services can be deployed in an isolated fashion regardless of the hardware server that they have been allocated into.

The NFV architectural framework standardized by the European Telecommunications Standards Institute (ETSI) is depicted in Figure 2 below. The NFV Infrastructure (NFVI) comprises the totality of the physical resources, possibly including resources from different locations or domains. These physical resources may include computing, storage, and networking resources, and together build

the environment that is capable of supporting the creation of Virtual Network Functions (VNFs). A virtualization layer in the NFVI abstracts these hardware resources into a pool of virtual resources that can be conveniently sliced and allocated to multiple VNFs.

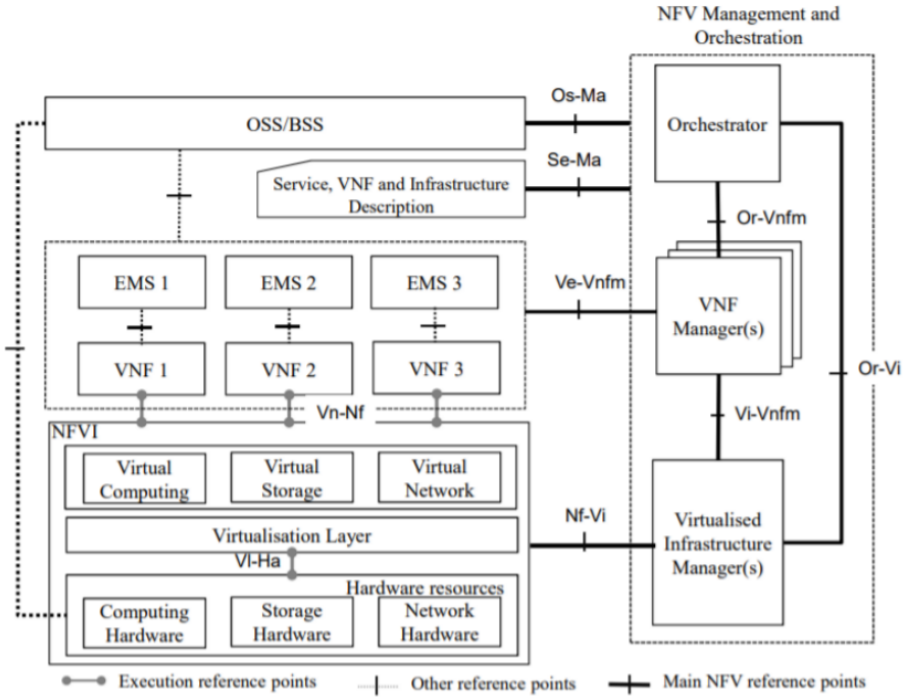

Figure 2. ETSI NFV reference architectural framework.

In NFV, the intelligence is provided by the NFV Management and Orchestration (MANO) block. MANO performs all the actions that involve the life cycle management (e.g., creation, configuration, and termination) of the aforementioned VNFs. Furthermore, a Network Service (NS) can encompass multiple VNFs providing a broader service on the whole. MANO can be subdivided into the Virtualized Infrastructure Manager (VIM), and a higher level NFV Orchestrator (NFVO). The VIM is responsible for the interaction with the NFVI resources across one domain during VNF allocation and deallocation tasks, whereas the NFVO works at the level of NSs and VNFs, managing their life cycle.

In an NFV/SDN scenario, if NFV technology realizes the deployment of services leveraging virtualization mechanisms, SDN is the technology that realizes the interconnection of those services and their components. Traditional networking has been implemented in such a way that the functionality to forward the network packets and the functionality to decide how they are forwarded are contained in the same device. These functionalities are known as data plane and control plane, respectively.

As represented in Figure 3, SDN thrives on the separation of these two planes to enable the implementation of a more centralized control plane in which each forwarding device is no longer responsible for making their own forwarding decisions. Instead, control plane tasks are relegated to one or more centralized controllers possessing a broader view of the whole network topology and conditions. These controllers enforce the forwarding logic into each device, which now only has to execute data plane tasks (packet forwarding). Thus, network devices do not need to use specific protocols and exchange information between them in order to make coherent forwarding decisions. SDN also results in greater programmability and reconfigurability of the network thanks to the centralization of the forwarding intelligence and the high granularity provided in the classification of network traffic.

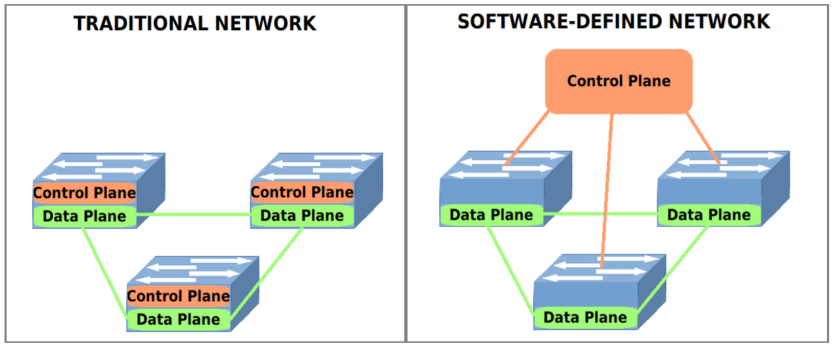

Figure 3. Traditional network versus software defined network.

3.2. OpenStack, Open Source MANO, and ONOS

SN4I makes use of various software products that orchestrate and manage the physical components (physical servers and interconnected switches) that make up the infrastructure, according to the previously explained NFV and SDN technologies. These software components are OpenStack, Open Source MANO (OSM), and Open Network Operating System (ONOS).

OpenStack implements the Virtualized Infrastructure Manager (VIM) of the NFV architectural framework previously shown in Figure 2. It also provides a common virtualization layer to the hardware servers in the NFVI it manages in order to abstract their physical resources into virtual resources. OpenStack is ultimately capable of controlling a pool of virtual resources and allocate different kinds of resources from it in order to instantiate Virtual Machines (VMs). OpenStack can also manage the life cycle of these VMs, as well as set up their internal means of interconnection. A VM holds a component of a VNF (a VNF can contain one or more VMs) and can be exposed and perceived by an end user just as a real dedicated computer system.

Open Source Mano (OSM) is, as its name implies, the MANO of SN4I. OSM is an ETSI NFV-aligned Management and Orchestration software that provides an upper layer to the OpenStack services. OSM provides the SN4I infrastructure managers with a tool to design and build NSs and VNFs composed of eventual VMs, as well as Virtual Links and Connection Points between their components. OSM is then responsible for interacting with OpenStack in order to realize the components and interconnections of the designed NSs into the NFVI. OSM exposes interfaces to manage the life cycle of these NSs and VNFs and includes rich features for their monitorization, as well as for the configuration and automation of their functionality.

Finally, Open Network Operating System (ONOS) performs as the controller of the SDN network infrastructure, which comprises both inter-VIM and intra-VIM connections. In SN4I, ONOS, through a protocol named OpenFlow, populates into the data plane devices the forwarding rules that make possible the interconnection of all the components of a given process (i.e., a given NS), while simultaneously ensuring that they are isolated from other processes' traffic. Furthermore, ONOS can be integrated with OSM in order to automatically install these forwarding rules that correspond to the NSs' Virtual Links.

3.3. Hidra

As previously mentioned, in the IoT scenarios designed for Industry 4.0, the sensors behave as small servers, and the users establish a secure E2E connection with them to either receive data or configure some parameters. In this context, strong access control mechanisms must be implemented, in order to guarantee that only authorized users can establish a connection with the devices. Moreover, due to the dynamic nature of the IIoT applications, these access control mechanisms should be flexible and expressive, so that they permit or deny the access to the users based not only on the permissions but also on the local context conditions.

Hidra [36] is a security protocol that guarantees both authentication and authorization of a remote subject wanting to establish an E2E connection with a CDS. The aim of Hidra is to offer a strong and dynamic access control solution that can be implemented even in the most constrained devices.

To provide expressiveness to the access control procedure, this protocol combines the centralized and distributed architectures, performing the authorization in two steps. On the one hand, the centralized server named Access Control Server (ACS) performs the authentication and preliminary authorization of the requesting subjects, discarding most unauthorized requests and hence avoiding unnecessary messages with the CDSs. On the other hand, to enable expressive context-based access control, each CDS is a distributed control point that performs the local authorization. This authorization is performed based on local context conditions such as the battery level of the sensor or the environmental parameters. The access decision is made after applying a very expressive security policy.

Figure 4 shows the detailed operation of Hidra. First, in Phase 1, the Delegated Authentication of the user is performed, where the user authenticates to the ACS and requests a Ticket Granting Ticket (TGT). In the case of successful authentication, the ticket is sent to the user.

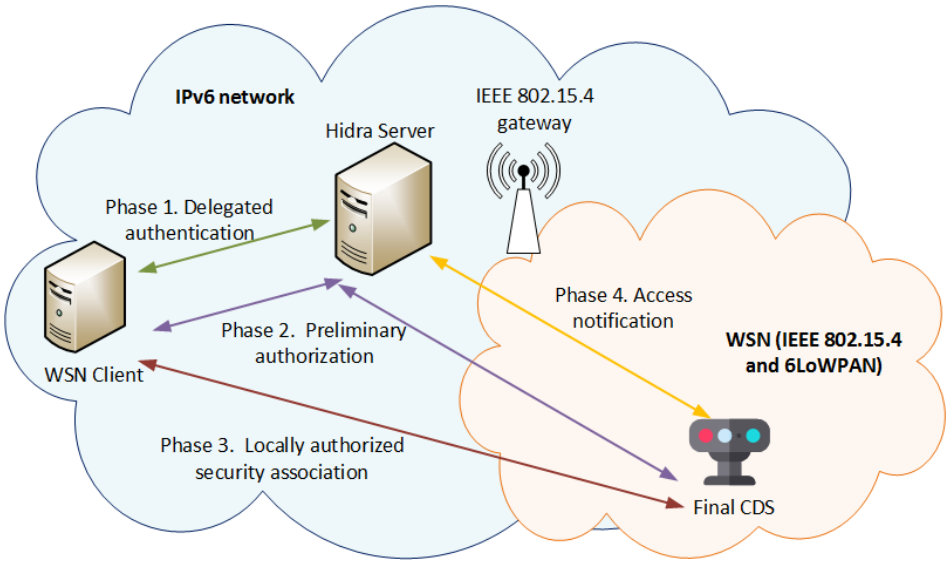

Figure 4. Hidra operation.

In Phase 2, the Preliminary Authorization is performed in the ACS, based on the attributes of the user, on the resource, and on the expected actions. The subject uses the TGT to demonstrate that it is an already authenticated entity and obtain the resource tickets required to access any resource on the CDSs. The Credential Manager (CM) of the ACS checks if the user has the proper permissions, and if so, it sends a message to the CDS containing the security policy to be applied. Besides, this message also contains a session key to be checked by the CDS in order to guarantee the freshness of the message.

If Phase 2 has proved successful, as the user has already the ticket to access the CDS, in Phase 3, the Locally Authorized Security Association is performed in the CDS. When the user sends a message containing the ticket, the CDS applies the security policy previously received in order to make an access decision. The application of this expressive policy means that the access decision is made based on current local context conditions for every access attempt. If the CDS decides to permit the access, an E2E security connection is established between the subject and the CDS.

Finally, in Phase 4, the Access Notification is performed, where the sensor sends to the ACS the details of the access attempt, both permitted and denied, for logging and accounting procedures.

The use of the aforementioned expressive security policies requires the definition of a proper policy language. The policy language defined for Hidra consists of different structs, some optional and some mandatory, enabling the reduction of the policy length when simple policies are needed. These structs go nested one inside another starting from a basic "Policy" struct, as shown in Figure 5, and the

order is crucial so that the meaning of the policy does not change. Each defined policy will have at least an identification number and a granting effect for the access request, which can be "permit" or "deny". This effect prevails in case the policy has no other construct or in case there is any contradiction on them. Apart from that, it is possible to add one or some rules in order to define the different situations that must be evaluated and the related effects.

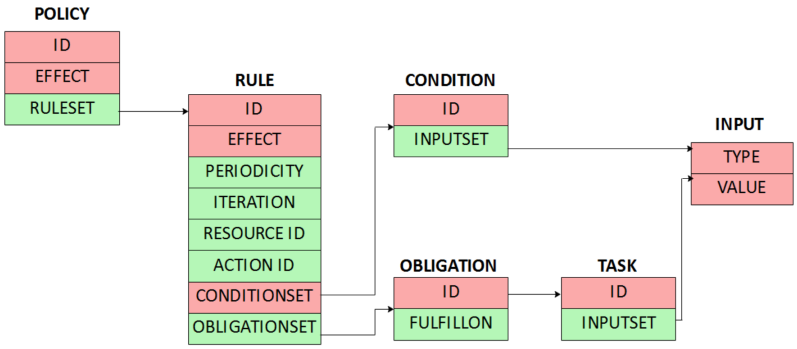

Figure 5. Hidra policy language structure.

Once the policy is defined, and before conveying it to the CDS so that it can be applied, it is necessary to encode it to a proper binary codification. The Authorization Policy Binary Representation (APBR) codification has been developed specifically for Hidra, as it encodes the security policies based on the policy language. Since it is a specific codification, it offers very high compression rates compared to other generic codifications. Moreover, due to the high compression rates, it optimizes the resources of the CDSs when decoding and applying the policy.

4. Proposed Architecture

This section focuses on the description of the proposed architecture that is intended to meet the first two objectives of this work: the deployment of the NFV- and SDN-enabled architecture for Industry 4.0, and the inclusion of a WSN for IIoT applications. For this purpose, the components and operation of the SN4I experimental facility are described, in addition to how the WSN has been implemented.

As introduced before, SN4I is an NFV- and SDN-enabled experimental facility deployed across the Faculty of Engineering in Bilbao (EIB) and the Aeronautics Advanced Manufacturing Center (CFAA). These two locations are interconnected through a layer-2 SDN network at a rate of 10 Gbps. Both datacenters are equipped with the hardware and software components that enable the deployment of virtual services in the infrastructure, leveraging NFV technology. The complete infrastructure comprises several SDN switches and servers, amounting to a total computing and storage capacity of around 250 dual-threaded cores, 1 TB of RAM, and 25 TB of storage. Two OpenStack nodes deployed in EIB and the CFAA manage the resources of their respective locations, and three ONOS controllers manage, respectively, the data plane connectivity in the EIB domain, the CFAA domain, and the Wide Area Network between both locations. Finally, an Open Source MANO on top orchestrates the whole NFV and SDN infrastructure. A high-level view of the SN4I infrastructure is shown in Figure 6.

In addition, a WSN has been integrated into this architecture, enabling the deployment of several constrained sensors in the CFAA in order to monitor different environmental parameters such as temperature, humidity, or lightness. The aim of this network is to implement different IIoT applications in the CFAA using Hidra as the access control protocol. Different protocols are used within the WSN, which are suitable for IIoT applications and devices. These protocols are IEEE 802.15.4 [37], 6LoWPAN [38] and RPL [39]. The interconnection between the WSN and the wired SN4I is performed through a 6LoWPAN Border Router, which is implemented by means of a Raspberry Pi running the necessary protocol translation and packet routing functions and a CDS connected to the Raspberry

Pi in order to allow for the wireless transmission using the IEEE 802.15.4 protocol. The integration between the sensor network and the CFAA plant network is depicted in Figure 7.

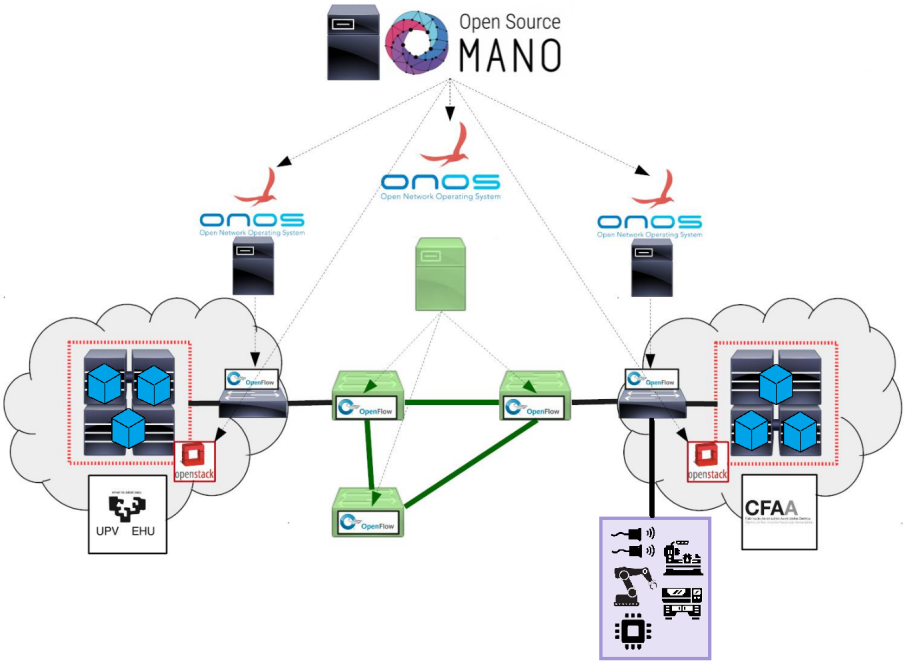

Figure 6. Proposed Architecture.

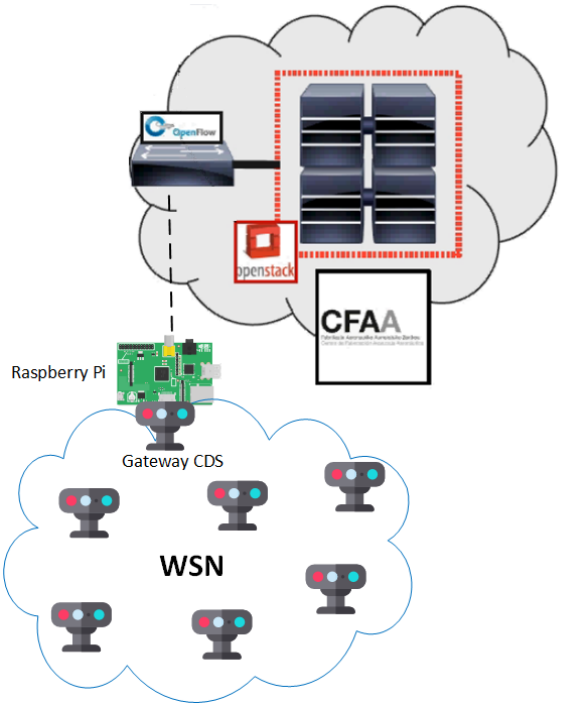

Figure 7. Integration of the Wireless Sensor Network (WSN) in the CFAA.

The SN4I infrastructure is designed in a way to ensure that different services are isolated from each other at both the computing level and the networking level, despite making use of a shared pool of physical resources. Not only does this address performance issues due to the contention of resources between different services, but also confidentiality and privacy issues with the data of

different services. With this aim, the SN4I network is segmented at the layer-2 level into multiple isolated VLANs, with each of these resulting slices being allocated to a different NS. This kind of VLAN encapsulation also translates smoothly to OpenStack, as it can support the use of underlying VLAN networks by appropriately tagging the traffic of VMs. OpenStack also provides a separate IPv4/IPv6 layer-3 network for the VMs located in each of these VLAN-segmented slices.

Each NS maps logically to a given manufacturing process and provides it, on demand, with the necessary resources and virtual services. This isolation between NSs ensures the avoidance of data filtration between different processes. Furthermore, by configuring the corresponding rules and policies in the associated ONOS controller, it can be ensured that machine tools that are physically connected to one of these slices are similarly isolated from other slices and from the rest of the network.

The process to create a new NS can be summarized as follows. Firstly, the NS is designed and described in a way that OSM understands it. The description of the NS reflects its composition in terms of VNFs and Virtual Links between them. In addition, each VNF also requires its own descriptor in order to indicate the requirements of each of its contained VMs, in terms of resources (disk, memory, and CPU), interfaces and internal links, configuration scripts, and other features. This process is known as onboarding in NFV terminology. NSs and VNFs that have been onboarded become available in the OSM catalog for instantiation. The NS being instantiated results in OSM negotiating with OpenStack how and where to deploy the VMs with the provided requirements. Once the resulting VMs have been created, OSM can also interact with the ONOS controller in order to install their connectivity requirements into the data plane. A unique VLAN is automatically selected for the NS in order to isolate it from other NSs. Besides, the addition of the WSN introduces an additional dimension to the design of NSs, as services provided by the CDSs can be dynamically allocated to some of these NSs together with the services provided by the VNFs that they are composed of.

5. Use Case

This section gathers the use case presented in this paper consisting of a 5G-enabled smart broaching process. First, the overall aim and scenario of the use case are presented, and then the two isolated network slices used to support the process are described: the first network slice contains the broaching tool and the virtual functions that implement the ML algorithms, while the second slice is devoted to the IIoT network and its corresponding security mechanisms.

5.1. Scenario

As previously introduced, the use case presented here consists in the monitoring of a broaching process. This broaching process is performed by a broaching bench installed in the CFAA.

Broaching is the process of removing material from a surface (usually metal) in order to shape it, which enables the manufacturing of complex profiles. Broaching has a wide range of application in the aeronautic and automotive industries. For example, it is the standard process for producing fir-tree slots in turbine discs due to the complex and delicate cuts that need to be applied to the pieces. For the broaching process, a broaching tool is employed.

A broaching tool is equipped with a series of cutting teeth placed throughout a row. There is a progressive rise in height per tooth, which indicates the amount of material that each tooth can remove on every pass. Broaching is a very expensive process for various reasons. The complex geometry of a broach results in a high tooling cost, and the large number of teeth that needs to be constantly grounded into the work piece leads to high tool wear, negatively impacting their lifetime.

To overcome these shortcomings, ML techniques will be introduced in the broaching process in order to monitor it and improve performance. The ML method will imply the analysis of real-time contextualized data obtained from the broaching machine and its environment, combined with historical records, in order to obtain a model that can accurately represent the process and predict the results. This ML approach is intended to achieve early detection of tool wear and disturbances,

leading to an increased lifetime of the tool and helping to achieve the quality requirements for the aeronautical industry in the resulting pieces.

5.2. Broaching Process Slice

The broaching process use case makes use of a slice of the infrastructure by deploying an NS with two VNFs. Each of these VNFs contains a VM based on a Windows 10 Operating System and together have been allocated a total of around 500 GB of disk space, 48 GB of RAM, and 9 virtual CPUs. This NS has been deployed entirely in the infrastructure within the CFAA data center to guarantee minimum latency with the broaching tool. The broaching process slice is isolated from the rest of the network through the use of VLAN segmentation, as explained above. In addition, a management interface is provided to the VMs for Internet access and so that authorized users can access them remotely.

As for the purposes of each VM, one of them is used to support an Open Platform Communications United Architecture (OPC UA) client. Using the OPC UA protocol, it collects parameters of the broaching process exposed by the OPC UA server in the Computer Numerical Control (CNC) of the broaching tool to aid with the monitorization of the process. Meanwhile, the second VM contains Promind software. Promind is fed large amounts of data collected by a data logger installed in the broaching tool, and by the IIoT devices deployed in a separate network slice, in order to predict the behavior of the broaching process and detect possible faults in real-time using ML algorithms.

In addition, a second NS containing a single VNF, contains the client responsible for collecting environmental data from the IIoT devices. For this data collection to be carried out securely, the client first authenticates to the Hidra server and obtains the necessary service tickets in order to be entitled to obtain the corresponding data from the deployed CDSs. As already mentioned, the Hidra server and the WSN belong to a different slice, which is covered later in Section 5.3.

The topology of this slice encompassing the two NSs and the involved broaching tool components is shown in Figure 8.

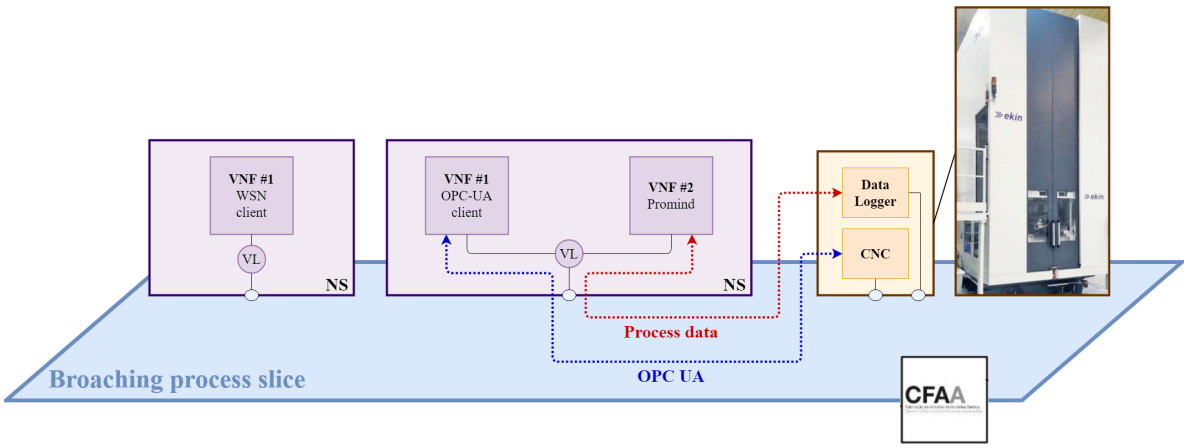

Figure 8. Broaching process slice.

5.3. IIoT Network Slice

Similar to the NS deployed for the broaching process, the sensor network uses its own VLAN-segmented slice of the infrastructure. The NS deployed in the IIoT network slice is meant to provide the WSN network in the CFAA with access control mechanisms. The NS is composed of one VNF with one VM. It makes use of a total of 100 GB of disk, 8 GB of RAM, and 2 virtual CPUs from the resources available in the EIB data center. Therefore, this slice spans both the EIB and CFAA datacenters and is connected through the WAN infrastructure of SN4I. The reason for physically locating the access control services in the EIB data center is that it is also used to support other WSN deployments, which shows the flexibility provided by NSs and the isolation between them.

The VM used is based on an Ubuntu 18.04 operating system. It contains the Hidra server, responsible for implementing all the Access Control Server functions. This machine receives every request from subjects wanting to access any CDS deployed in the WSN of the CFAA. In this context, the subject requesting access to the sensors is the client of the broaching process slice aforementioned, but there could also be clients from other processes. Therefore, the Hidra server implements all the functions involved in the authentication and preliminary authorization phases, including the conveyance of the corresponding security policy to the final CDSs. Moreover, it also implements a LOG server to receive from the sensors the details of all the access attempts in order to perform a real-time monitorization of different parameters. This monitorization allows an efficient management of users' activity, detailing which user did what, when, and in which CDS.

The topology of this slice is shown in Figure 9.

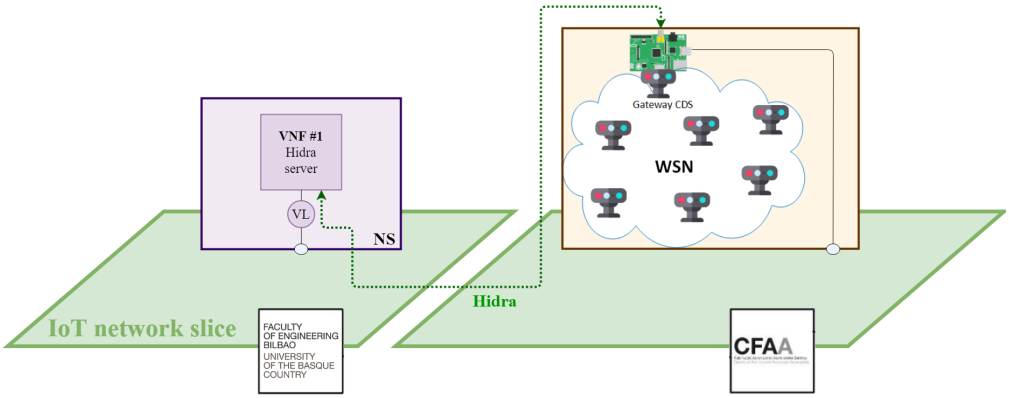

Figure 9. Industrial Internet of Things (IIoT) network slice.

5.4. Global Operation

As the broaching process slice and the IIoT network slice reside in different VLANs, layer-3 routing is necessary to enable the connectivity between them. OpenStack supports the creation of virtual routers to make this possible without additional VMs being necessary for their implementation. Furthermore, a virtual firewall defines the security policies that make sure each component of the broaching process slice can only access the components of the IIoT network slice that it is authorized to (such as the Hidra client establishing a connection with the Hidra server and the sensors of the WSN). The virtual firewall can also be created in OpenStack on top of the virtual router.

Thanks to the expressiveness provided by the Hidra access control mechanism, IIoT applications, such as the client gathering data from the broaching process slice, can be granted or revoked access to any of the resources provided by the CDSs in a very granular, dynamic, and flexible manner. In this way, requesting clients within the different slices of SN4I will be granted or revoked access to the data and management services provided by the different CDSs deployed in the WSN according to a very expressive access control policy that allows also the evaluation of local context conditions. As an example, a client preliminary authorized by the ACS to perform a certain operation on a specific CDS could then be denied the requested operation by the CDS itself according to the evaluation of the "battery level" local variable, if, for instance, performing the requested operation would imply draining the battery of the CDS before its finalization.

The overall topology combining both slices is shown in Figure 10.

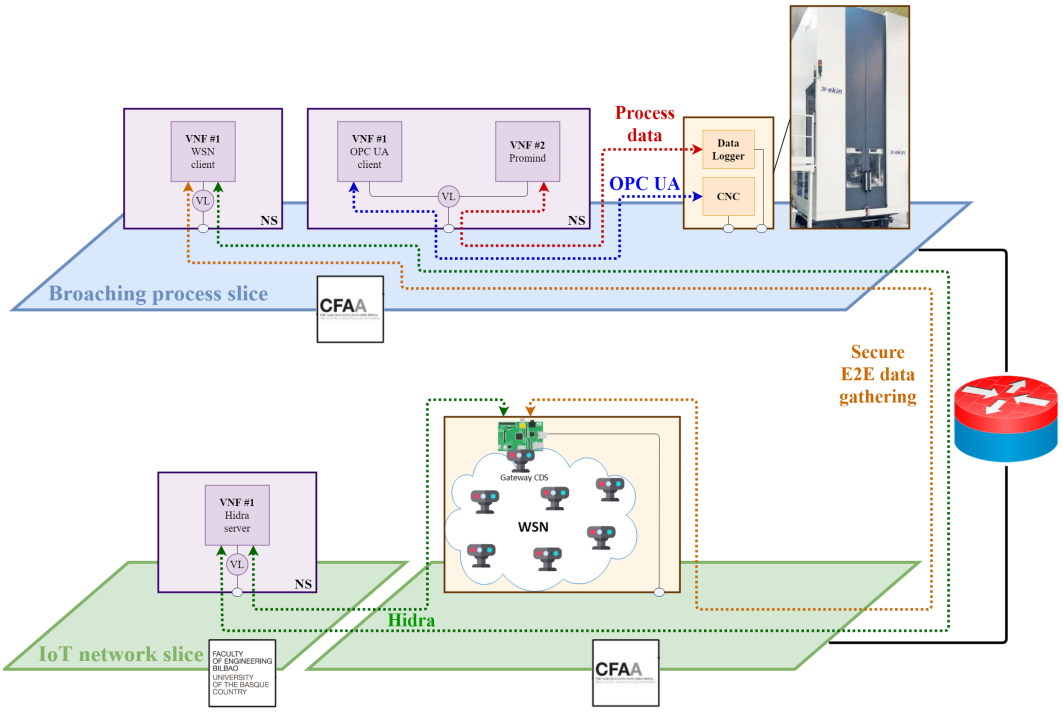

Figure 10. Global operation.

6. Benefits

This section describes the main benefits provided by this work, focusing on the enhancements and new opportunities provided by the proposed architecture, which integrates state-of-the-art technologies such as NFV to the industrial environment where it has been deployed.

This work proposes a new approach to managing the life cycle of services, evolving from the traditional monolithic approach to acquiring and deploying network services based on hardware-specific and vendor-specific solutions, to a much more flexible one leveraging virtualization and softwarization. Overall, this leads to a substantial simplification and agilitization in the deployment cycle of new services, also resulting in a reduction in service downtime and in flexible mechanisms to continuously enhance and configure the services as needed. As such, a flexible platform is provided in which it is possible to deploy a wide variety of services (i.e., VNFs), ranging from ML applications and databases to security functions such as firewalls, Intrusion Detection Systems (IDSs), or, as a more specific example, the Hidra server covered in the article. These services can then become part of the service catalog so that an authorized user can deploy any of them in the corresponding slice in just minutes. VNFs from the catalog can be combined in different ways and with different connectivity patterns in order to create rich NSs specifically tuned to satisfy the requirements of a given use case.

The ability to deploy services in separate slices provides isolation at both the data and performance levels for different manufacturing processes. This is particularly important in industrial scenarios in order to avoid data leaks between different business processes, in addition to ensuring a lack of resource contention that could impact the performance of the applications. This is further enabled thanks to the high granularity provided by SDN to classify network traffic, which makes it possible to define traffic flows as specific or granular as necessary, taking into account all the security, privacy, and performance (e.g., bandwidth) considerations involved. Furthermore, this isolation is achieved despite all services sharing the same underlying networking and computing infrastructure, which significantly reduces the deployment costs.

However, this flexibility is not just restrained to services specifically designed for the CFAA. The open nature of the NFV standards enables interoperability between different NFV solutions. This means that VNFs designed within SN4I can also be offered by third parties and directly used in

other infrastructures. The opposite is also true, and VNFs from external vendors or designers can be added to the SN4I catalog and integrated into NSs provided by SN4I and into its specific computing and networking infrastructure.

Meanwhile, the heavily automatized and agile service deployment and life cycle management open up the possibility to introduce new ways in which services can transition from a development version to production deployment. A service can be first tested and validated in a local datacenter with minimum resources, and then deployed and integrated into the production datacenter in-plant, adjusting the resource and connectivity requirements as appropriate. This effectively aligns with the Continuous Integration/Continuous Delivery (CI/CD) paradigm frequently used in software development, which is driven by introducing ongoing automation and monitoring in the development process through incremental changes and continuous feedback in the integration and delivery of the product.

Even though SN4I currently comprises two datacenters in two separate locations (EIB and CFAA), the integration of additional datacenters is possible. Under the orchestration of the same centralized NFV MANO, it is possible to attach additional remote datacenters, or even public clouds, which could provide additional hardware resources and capabilities in order to adapt to the requirements of future applications. While the two currently integrated datacenters are OpenStack-based, other datacenter or cloud technologies such as Amazon Web Services (AWS), VMware vCloud, Kubernetes public and private clusters, and OpenNebula can also be supported under the same management and orchestration plane.

Regarding the IIoT slice and the deployed WSN, one of the main benefits of this architecture is that sensors can serve multiple applications, meaning that they do not need to be statically assigned to a single process. Although in the use case presented in this work the whole WSN is shown to be associated with the broaching process, it is possible to set up additional processes that also make use of the services offered by the WSN in different ways. This effectively enables a scenario where sensors, and, more specifically, the services they provide, can dynamically float across one or more processes on demand, adjusting their assignments based on the needs of each process at any given moment. Each of these processes can leverage the authentication and authorization mechanisms provided by Hidra and can either make use of the previously discussed IIoT slice or set up their own local Hidra service thanks to the Hidra VNF available in the service catalog.

Moreover, with such an expressive access control mechanism and with the use of the security policies, it is possible to grant or revoke access to any resource in the CDSs according to the evaluation of some local context conditions. As previously described, this access control decision is made based on a security policy, being the use of highly expressive security policies essential in order to obtain a fine-grained access control procedure. For example, the request of a preliminarily authorized user can then be denied if the battery level is not enough to perform the requested operation. In this context, sensors can be considered easily reconfigurable, since, through the access control, the values can be set and accessed depending on the result of the security policy evaluation. Therefore, the flexible IIoT integration is made possible as the behavior of the sensors can be personalized or configured by means of conveying the proper security policy to be applied in every particular case.

A summary of the benefits provided by this work, including their impact on industrial environments, as well as their impact on the specific use case presented in Section 5, is presented in Table 1.

Table 1. Summary of benefits.

Benefit	Overall Impact	Impact on Use Case
More agile and automatized deployment cycle of services.	Reduction in deployment time and costs. Faster transition between local deployment to in-plant deployment.	Faster deployment and production start-up of data recollection and ML services.
More flexible lifecycle management of services.	Easier upgrade, adaptation, and configuration of services, and service downtime reduction.	Ability to automate specific service tasks. Ability to quickly scale resources on demand and integrate new service components if required by the process.
Service isolation at data and performance level.	Data leak avoidance between business processes and avoidance of performance issues due to resource contention.	Guarantees offered in the isolation of the broaching process traffic as well as in the performance and bandwidth of the ML services.
Intelligent service placement, efficient resource allocation, and highly granular network traffic classification.	Lower costs and better performance due to the optimization of computing and networking resources and intelligent matching of hardware capabilities.	Computing resources efficiently assignable based on ML processing requirements. Bandwidth adaptable for different traffic flows of the broaching tool and between the service VMs.
Service catalog availability.	Faster service delivery and faster introduction of new services. Ability to export and import designed services.	Ability to export services or components designed for this process to other processes for immediate deployment. Ability to quickly import and deploy already designed external services to this process.
Interoperability between NFV solutions.	Ability to integrate with other data centers or other NFV technologies, including public clouds and containerized environments.	Ability to introduce additional hardware capabilities if beneficial to the process.
Dynamically assignable and shareable sensors and sensor services.	Lower costs due to usage optimization and fast service provisioning due to dynamicity.	Obtainable environmental data from sensors dynamically adaptable to varying process requirements.
Strong but lightweight and expressive support of security policies.	Customizable and fine-grained security policies and high reconfigurability with a minimal performance impact.	Usage of sensor services customizable to process requirements.

7. Conclusions

In this work, a 5G-enabled architecture is presented based on Smart Networks for Industry (SN4I), an experimental facility for Industry 4.0 based on NFV and SDN that spans between the Aeronautics Advanced Manufacturing Center (CFAA) and the Faculty of Engineering in Bilbao (EIB) at the University of the Basque Country. To complete the proposed architecture, the integration of a WSN is shown, in order to enable the deployment of IIoT applications with the implementation of appropriate security mechanisms.

The substrate provided by the proposed IT infrastructure, in which isolated slices composed of machine tools, sensors, and interconnected Virtual Network Functions can be flexibly deployed and configured, has enabled the development of the use case presented in this work, consisting in a 5G-enabled smart broaching process. In this use case, the monitoring of the broaching process is enabled through ML VNFs and through the measurement of environmental parameters from the WSN.

Furthermore, to guarantee secure access and use of the information that these sensors gather, the WSN has been protected with a strong and expressive access control mechanism named Hidra.

Additionally, this work presents several benefits that the adoption of a 5G-enabled architecture can provide to industrial environments in terms of flexibility, agility, efficiency, and automation in the deployment and life cycle management of services capable of empowering manufacturing processes. It is also shown how these benefits align with the characteristics of the presented use case. Overall, the authors believe that the architecture presented fosters innovation in the manufacturing processes by providing an IT-based playground that can contribute to an improvement of their overall quality and performance.

The work presented here paves the way for the future: SN4I and CFAA have recently been integrated into the 5G Euskadi Pilot, which will allow the use of Ultra-Reliable Low-Latency Communications (URLLC) and massive Machine Type Communications (mMTC) communication services and Multi-access Edge Computing (MEC) technologies in the CFAA. All technologies presented here—the use of NFV and SDN through a standardized, 5G compliant and technology agnostic MANO; the use of a flexible and secure IIoT WSN; and the integration with industrial protocols—will integrate seamlessly with the coming technologies.

Author Contributions: J.S. and E.J. contributed to the design and implementation of the NFV/SDN platform. A.S. and J.A. contributed to the design and implementation of the IIoT access control mechanisms. All authors contributed to the conceptualization of the use case. J.S. and A.S. contributed to the writing. J.A. and E.J. contributed to the final review. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Spanish Ministry of Economy, Industry and Competitiveness through the State Secretariat for Research, Development and Innovation under the "Adaptive Management of 5G Services to Support Critical Events in Cities (5G-City)" TEC2016-76795-C6-5-R and "Towards zero touch network and services for beyond 5G (TRUE5G)" PID2019-108713RB-C54 projects and in part by the Department of Economic Development and Competitiveness of the Basque Government through the 5G4BRIS KK-2020/00031 research project.

Acknowledgments: We acknowledge the Aeronautics Advanced Manufacturing Center for offering us the possibility to integrate our SN4I infrastructure with the machine tools in the center.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lasi, H.; Fettke, P.; Kemper, H.G.; Feld, T.; Hoffmann, M. Industry 4.0. *Bus. Inf. Syst. Eng.* **2014**, *6*, 239–242. [CrossRef]
2. European Parliament. Legislative Train 08.2020. Digitising European Industry. Available online: https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-digitising-european-industry (accessed on 28 October 2020).
3. Yousaf, F.Z.; Bredel, M.; Schaller, S.; Schneider, F. NFV and SDN—Key technology enablers for 5G networks. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 2468–2478. [CrossRef]
4. Bouras, C.; Kollia, A.; Papazois, A. SDN & NFV in 5G: Advancements and challenges. In Proceedings of the 2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), Paris, France, 7–9 March 2017; pp. 107–111.
5. Wan, J.; Tang, S.; Shu, Z.; Li, D.; Wang, S.; Imran, M.; Vasilakos, A.V. Software-defined industrial internet of things in the context of industry 4.0. *IEEE Sens. J.* **2016**, *16*, 7373–7380. [CrossRef]
6. 5G Infrastructure Public Private Partnership (5G PPP). 5G and Verticals. Available online: https://5g-ppp.eu/verticals/ (accessed on 28 October 2020).
7. 5GTANGO. 5G Development and Validation Platform for Global Industry. Available online: https://5gtango.eu/ (accessed on 28 October 2020).
8. 5G SMART. 5G for Smart Manufacturing. Available online: https://5gsmart.eu/ (accessed on 28 October 2020).
9. 5G CONNI. Private 5G Networks for Connected Industries. Available online: https://5g-conni.eu/ (accessed on 28 October 2020).

10. 5G-Transformer. 5G Mobile Transport Platform for Verticals. Available online: http://5g-transformer.eu/ (accessed on 28 October 2020).
11. 5G-ACIA. 5G Alliance for Connected Industries and Automation. Available online: https://www.5g-acia.org/ (accessed on 28 October 2020).
12. ICNAP. International Center for Networked, Adaptive Production. Available online: https://www.vernetzte-adaptive-produktion.de/en.html (accessed on 28 October 2020).
13. Zafeiropoulos, A.; Gouvas, P.; Fotopoulou, E.; Tsiolis, G.; Xirofotos, T.; Bonnet, J.; Carrozzo, G.; Rizou, S.; Gavras, A.; Barros, M.J.; et al. Enabling Vertical Industries Adoption of 5G Technologies: A Cartography of evolving solutions. In Proceedings of the 2018 European Conference on Networks and Communications (EuCNC), Ljubljana, Slovenia, 18–21 June 2018; pp. 1–9.
14. Wollschlaeger, M.; Sauter, T.; Jasperneite, J. The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0. *IEEE Ind. Electron. Mag.* **2017**, *11*, 17–27. [CrossRef]
15. Rao, S.K.; Prasad, R. Impact of 5G technologies on industry 4.0. *Wirel. Pers. Commun.* **2018**, *100*, 145–159. [CrossRef]
16. Ma, Y.W.; Chen, Y.C.; Chen, J.L. SDN-enabled network virtualization for industry 4.0 based on IoTs and cloud computing. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, Korea, 19–22 February 2017; pp. 199–202.
17. Peuster, M.; Schneider, S.; Behnke, D.; Müller, M.; Bök, P.B.; Karl, H. Prototyping and demonstrating 5G verticals: the smart manufacturing case. In Proceedings of the 2019 IEEE Conference on Network Softwarization (NetSoft), Paris, France, 24–28 June 2019; pp. 236–238.
18. Mekikis, P.V.; Ramantas, K.; Antonopoulos, A.; Kartsakli, E.; Sanabria-Russo, L.; Serra, J.; Pubill, D.; Verikoukis, C. NFV-enabled experimental platform for 5G Tactile Internet support in industrial environments. *IEEE Trans. Ind. Inform.* **2019**, *16*, 1895–1903. [CrossRef]
19. Behnke, D.; Müller, M.; Bök, P.B.; Schneider, S.; Peuster, M.; Karl, H.; Rocha, A.; Mesquita, M.; Bonnet, J. NFV-driven intrusion detection for smart manufacturing. In Proceedings of the 2019 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Dallas, TX, USA, 12–14 November 2019; pp. 1–6.
20. Petroulakis, N.E.; Fysarakis, K.; Askoxylakis, I.; Spanoudakis, G. Reactive security for SDN/NFV-enabled industrial networks leveraging service function chaining. *Trans. Emerg. Telecommun. Technol.* **2018**, *29*, e3269. [CrossRef]
21. Wu, H.; Nguyen, G.T.; Chorppath, A.K.; Fitzek, F. Network Slicing for Conditional Monitoring in the Industrial Internet of Things. Available online: https://sdn.ieee.org/newsletter/january-2018/network-slicing-for-conditional-monitoring-in-the-industrial-internet-of-things (accessed on 28 October 2020).
22. Wu, H.; Tsokalo, I.A.; Kuss, D.; Salah, H.; Pingel, L.; Fitzek, F.H. Demonstration of network slicing for flexible conditional monitoring in industrial IoT networks. In Proceedings of the 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 11–14 January 2019; pp. 1–2.
23. Rescorla, E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. 2018. Available online: https://dx.doi.org/10.17487/RFC8446 (accessed on 28 October 2020).
24. Rescorla, E.; Modadugu, N. Datagram Transport Layer Security Version 1.2. RFC 6347. 2012. Available online: https://dx.doi.org/10.17487/RFC6347 (accessed on 28 October 2020).
25. Riahi Sfar, A.; Natalizio, E.; Challal, Y.; Chtourou, Z. A roadmap for security challenges in the Internet of Things. *Digit. Commun. Netw.* **2018**, *4*, 118–137. [CrossRef]
26. Wei, W.; Yang, A.T.; Shi, W.; Sha, K. Security in Internet of Things: Opportunities and Challenges. In Proceedings of the 2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI), Beijing, China, 20–21 October 2016; pp. 512–518.
27. Roman, R.; Zhou, J.; Lopez, J. On the features and challenges of security and privacy in distributed internet of things. *Comput. Netw.* **2013**, *57*, 2266–2279. [CrossRef]
28. Selander, G.; Mattsson, J.; Palombini, F.L.S. Object Security for Constrained RESTful Environments (OSCORE). RFC 8613. 2019. Available online: https://dx.doi.org/10.17487/RFC8613 (accessed on 28 October 2020).
29. Shelby, Z.; Hartke, K.; Bormann, C. The Constrained Application Protocol (CoAP); RFC 7252. 2019. Available online: https://dx.doi.org/10.17487/RFC7252 (accessed on 28 October 2020).

30. Seitz, L.; Selander, G.; Gehrmann, C. Authorization framework for the Internet-of-Things. In Proceedings of the 2013 IEEE 14th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Madrid, Spain, 4–7 June 2013; pp. 1–6. [CrossRef]
31. Zhang, G.; Gong, W. The Research of Access Control Based on UCON in the Internet of Things. *J. Softw.* **2011**, *6*, 724–731. [CrossRef]
32. Hernández-Ramos, J.; Jara, A.J.; Marín, L.; Skarmeta, A. DCapBAC: Embedding Authorization logic into Smart Things through ECC optimizations. *Int. J. Comput. Math.* **2014**, *93*, 345–366. [CrossRef]
33. Beltran, V.; Skarmeta, A.F. An overview on delegated authorization for CoAP: Authentication and authorization for Constrained Environments (ACE). In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016; pp. 706–710.
34. Bormann, C.; Hoffman, P. Concise Binary Object Representation (CBOR). RFC 7049. 2019. Available online: https://dx.doi.org/10.17487/RFC7049 (accessed on 28 October 2020).
35. Astorga, J.; Jacob, E.; Huarte, M.; Higuero, M. Ladon: End-to-end authorisation support for resource-deprived environments. *IET Inf. Secur.* **2012**, *6*, 93–101. [CrossRef]
36. Uriarte, M.; Astorga, J.; Jacob, E.; Huarte, M.; Carnerero, M. Expressive Policy-Based Access Control for Resource-Constrained Devices. *IEEE Access* **2018**, *6*, 15–46. [CrossRef]
37. IEEE Standards Association. *IEEE Standard for Low-Rate Wireless Networks*; IEEE Standards Association: Piscataway, NJ, USA, 2016; Volume 802.
38. Montenegro, G.; Kushalnagar, N.; Hui, J.; Culler, D. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944. 2007. Available online: https://dx.doi.org/10.17487/RFC4944 (accessed on 28 October 2020).
39. Winter, T.; Thubert, P.; Brandt, A.; Hui, J.; Kelsey, R.; Levis, P.; Pister, K.; Struik, R.; Vasseur, J.; Alexander, R. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550. 2012. Available online: https://dx.doi.org/10.17487/RFC6550 (accessed on 28 October 2020).