



HAL
open science

A Prototype 5G/IoT Implementation for Transforming a Legacy Facility to a Smart Factory

Panagiotis Papaioannou, Nikolaos Tzani, Christos Tranoris, Spyros Denazis,
Alexios Birbas

► **To cite this version:**

Panagiotis Papaioannou, Nikolaos Tzani, Christos Tranoris, Spyros Denazis, Alexios Birbas. A Prototype 5G/IoT Implementation for Transforming a Legacy Facility to a Smart Factory. 17th IFIP International Conference on Artificial Intelligence Applications and Innovations (AIAI), Jun 2021, Hersonissos, Crete, Greece. pp.52-61, 10.1007/978-3-030-79157-5_5. hal-03789002

HAL Id: hal-03789002

<https://inria.hal.science/hal-03789002v1>

Submitted on 27 Sep 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License



This document is the original author manuscript of a paper submitted to an IFIP conference proceedings or other IFIP publication by Springer Nature. As such, there may be some differences in the official published version of the paper. Such differences, if any, are usually due to reformatting during preparation for publication or minor corrections made by the author(s) during final proofreading of the publication manuscript.

A prototype 5G/IoT implementation for transforming a legacy facility to a Smart Factory^{*}

Panagiotis Papaioannou¹, Nikolaos Tzanis², Christos Tranoris¹, Spyros Denazis¹, and Alexios Birbas¹

¹ Dept. of Electrical and Computer Engineering University of Patras Patras, Greece

² Dept of Research, Technology and Development Independent Power Transmission Operator (IPTO) Athens, Greece

{papa.john,sdena,birbas}@upatras.gr,n.tzanis@admie.gr,tranoris@ece.upatras.gr

Abstract. A typical factory consists of several low functionality sensors. This work presents an architecture that can enhance the day-to-day operation of the site by combining modern IoT and legacy equipment and transforming the site for the 5G era. Operation and security of the site will benefit from the low latency the proposed Mobile Edge Computing architecture offers. Constant and uninterrupted monitoring makes preventive maintenance decisions even more accurate. Multitier architecture allows monitoring of each site to be performed locally without delays, while overall monitoring and control of remote sites is feasible as well.

Keywords: Smart Factory · 5G · IoT.

1 Introduction

A Smart Factory is defined as a smart and reconfigurable network of interconnected sensors, machines, and production systems, which collect, exchange and analyze data in a unified and automated way [1]. It is characterized by the ability to collect, store, and handle large amounts of data, originating from different types of sensors, and support different applications with diverse requirements. Actions in a Smart Factory can be divided into three broad categories: operation, security, and maintenance. Maintenance activities require support of low cost, energy efficient sensors, planted in a distributed and heterogeneous infrastructure. Security and operation services ask for low latency and high reliability communication and high bandwidth for CCTV. Modern trends in network architectures and virtualization technologies such as Multi-access Edge Computing (MEC) and Network Function Virtualization (NFV), inherently supported by 5G, will be major enablers for the development of such Factories. MEC is used

^{*} Supported by the H2020 European Projects 5G-VINNI (grant agreement No. 815279) and 5G-VICTORI (grant agreement No. 857201)

to get processing power and storage capabilities as close to the edge of the mobile network as possible. No longer is there a simple base station or a cell tower but enough computing power to run services and applications near their source. These services can benefit greatly from the local processing by minimizing the transport delay to the core network.

NFV architecture separates network functions from the underlying infrastructure, providing optimized reconfiguration, easy integration of new services, and guaranteed isolation, through the concept of network slicing. Application and network functionalities are defined as Virtual Network Functions (VNFs) and orchestrated by an NFV Orchestrator (NFVO), responsible for the management of virtual resources across multiple data centers.

Through ICT-17 projects [2], 5G testbeds become available to verticals to test their applications and their benefit from the services provided by 5G. To this end, the 5G-VICTORI [3] project conducts large-scale trials for advanced vertical use case verification for Transportation, Energy, Media, and Factories of the Future related use cases.

For the Factories of the Future use case, the project's objective is to demonstrate how the concept of Smart Factory can be substantially improved by the services provided by an underlying 5G ICT infrastructure. Considering that traditional factories already use legacy infrastructure (sensors, networks, industrial protocols) for their operation, the smooth transition to a new, modern factory model must assure backward compatibility with the legacy equipment.

This paper describes the work related to the Factories of the Future use case, towards the transformation and modernization of the monitoring system of a traditional facility for the 5G era, by introducing the NFV and MEC architectures and incorporating the legacy equipment to the solution. The rest of the paper is organized as follows: In section II the details of the use case trials are presented. Section III describes the proposed architecture while section IV details the infrastructure of the used testbed. In sections V two specific use scenarios for our architecture are presented. Finally, we conclude this work by presenting the results of our approach and our future directions.

2 Specific Use Case

The trial takes place at the Independent Power Transmission Operator (IPTO) facility located near the University of Patras, Greece. The facility consists of two different sites divided by sea and electrically interconnected via a High Voltage (HV) submarine cable and is ideal for demonstrating how applications of the three different classes (operation, maintenance, security) can be supported by a 5G enabled infrastructure.

Operation: The two sites serve as terminal points of the submarine cable and are equipped with several hard-wired sensors, measuring various quantities such as oil pressure level, battery level, etc. The sensors produce thousands of measurements every minute, but only at local level, and provide limited information

through indication lights. A unified monitoring system, able to process data from both sites in real-time and generate alerts or auto trip signals in case of major problems, will lead to great improvement in power quality, and support fault prediction algorithms, minimizing the power network down-time. Since the legacy sensors are not network enabled, the first step is to enhance them with a network interface. In this sense, legacy sensors will be first connected to a Modbus TCP interface and then connected via ethernet to the rest of the network.

Preventive Maintenance: The overall infrastructure at both sites needs continuous monitoring, to schedule timely maintenance activities and prevent equipment degradation and failure. Currently, inspection of equipment, buildings, etc., is performed by personnel, and since the facilities are spread to remote and hard to reach locations, this is a demanding and costly task. Preventive maintenance applications collect measurements from sensors planted in key locations of the facilities, compare them with historical data and produce useful reports regarding the health of the infrastructure. For this reason, several wireless sensors will be planted to the facilities. Due to the enormous number of sensors that need to be used to cover every inch of the facilities and the difficulty to access many remote locations, low-cost and low-power devices must be used. This concept is directly related to the massive IoT (mMTC) concept, where small and infrequent data packets are transmitted from numerous standalone devices. The network technology providing connectivity to such devices must satisfy these requirements and support high capacity and low latency for some use cases.

Security: The two sites also serve as local warehouses for IPTO, where pieces of equipment such as copper cables and transformers are stored and maintained. ADMIE facilities have been the victim of copper cable theft and vandalism for several years. An advanced security system consisting of a set of FHD cameras and motion control sensors will be deployed in the facilities. The deployed equipment should be able to stream high quality data to be used complementary to the sensors generated data. An application will process the generated data, recognize unauthorized access to facilities and trigger corresponding alarms.

This particular use case can greatly benefit by using a MEC architecture. Operation and Security applications can meet their strict latency requirements, by leveraging the local processing capabilities of MEC architecture. Preventive maintenance activities also act on local level, so local storage and processing of the data produced by the various sensors, can lead to substantial reduction in cloud storage and communication bandwidth at the core network. Moreover, since a Smart Factory is a continuously evolving system, new services may be deployed in the future, especially in the areas of Industry 4.0 and 5G. In this sense, the proposed architecture, shown in Figure 1, is easily reconfigurable and expandable with the minimum cost and effort.

3 High Level Architecture

In order to fulfill the requirement for local processing and storage at each site, while also being able to connect and remotely configure the two sites as a unified monitoring system, the end-to-end architecture depicted in Figure 1 is considered. A multi-tier architecture will be implemented, where each site is able to perform local processing and storage activities, and information is forwarded to the core cloud only when necessary. At each site, except from the already installed sensors, new types of sensors based on a diverse set of different technologies (5G, NB-IoT etc.) will be deployed, as well as the required network elements that provide coverage to them.

Each site will have an Edge Cloud, consisting of a server with adequate computational capabilities to support the use case applications requirements. The server will host an Edge IoT Platform, responsible for the collection and storage of the measurements originating from the different sensors. Furthermore, the server will also host a set of Virtual Network Functions to facilitate our Use Case specifics.

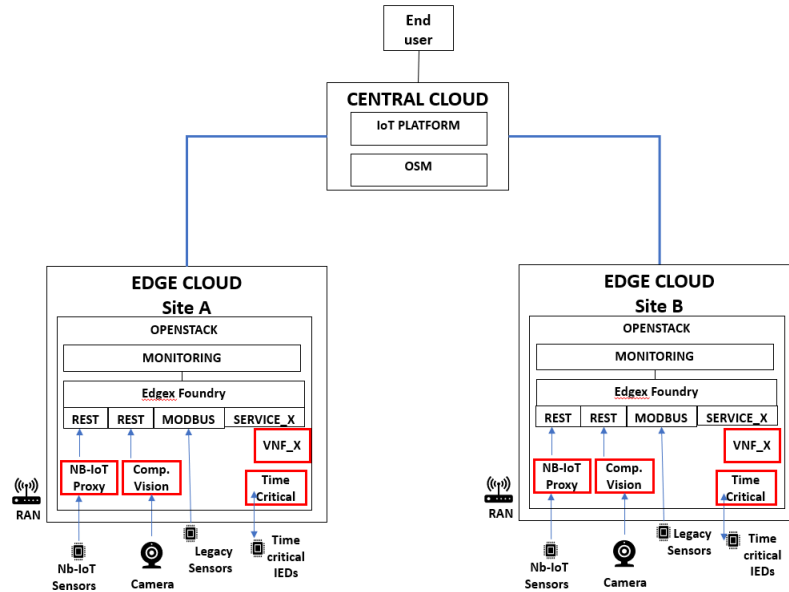


Fig. 1. Basic Architecture

NB-IoT Proxy: To support the NB-IoT connectivity, a VNF is deployed to act as a gateway for the NB-IoT devices. Besides being responsible for the reception and initial handling of the data received by the NB-IoT devices it also forwards

these to the Edge IoT Platform. Further functionality, like decision making or issuing commands to the NB-IoT devices can be added.

Optical Recognition: For other aspects of the use case, VNFs like optical recognition for the cameras is also planned to be deployed on the Edge cloud.

Time critical services: For the real-time operation case, a VNF checking the data received from specific Intelligent Electronic Devices (IEDs) and emitting control signals to them, in case of emergency, will be deployed.

Edge IoT platform: The deployed IoT platform is EdgeX Foundry [4], an open-source, vendor-neutral, Edge IoT platform, developed under the Linux Foundation Edge umbrella. EdgeX Foundry acts as a middleware between the various sensors and devices, and the vertical applications that use the information provided by these devices. The platform's architecture is depicted in Figure 2 and is organized as a set of different containerized microservices, each one belonging to one service family.

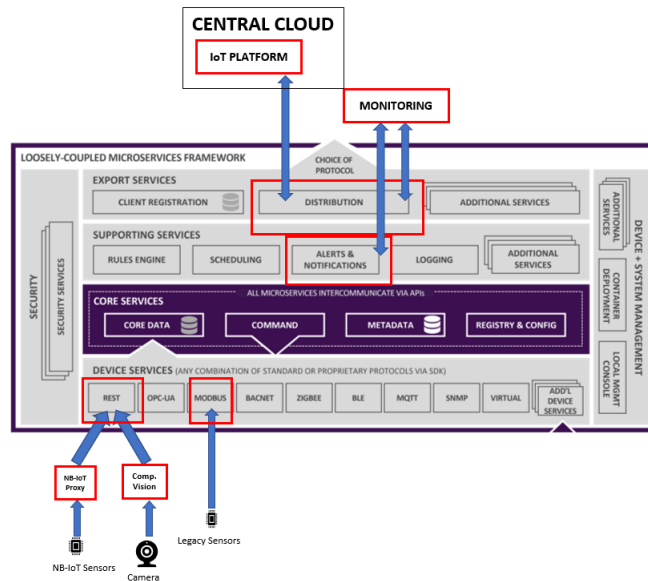


Fig. 2. EdgeX Architecture with added functionality

The Device Services family provide a southbound API with the different devices, sensors, and actuators. It is a set of connectors, encapsulating the specific

requirements of different open source or proprietary protocols, and providing a unified way for the interaction with the edge devices. These connectors are used to collect measurements from the edge devices and translate them into meaningful information or take commands from the vertical applications and transform them into protocol-specific messages understood by the edge devices. As implied by the name, the Core Services family performs the core functionality of the platform. Core data is a centralized database for data readings collected by devices and sensors, whereas core command enables the different microservices, applications, or external systems to interact with the end devices. The configuration and registry services are used to configure the specific deployment (e.g. add or remove a new sensor).

In our implementation, Modbus TCP and REST device services of EdgeX Foundry are used. Modbus device service is used for data collection and issuing of commands to the legacy Modbus sensors. The REST device service receives measurements from sensors using protocols not currently supported by an EdgeX device service. In this case, the NB-IoT-Proxy will be deployed as VNF, which receives the NB-IoT capable sensors' measurements, packets them in appropriate REST requests, and transmits them to the EdgeX REST device service.

Central Cloud: The two sites are interconnected through a core cloud infrastructure. The central cloud also hosts a set of Use case specific VNFs such as the IoT platform responsible for the collection, processing, and storage of the aggregated data from the two sites. It also gives remote access to the end user, and the ability to configure centrally the overall ICT infrastructure.

4 Infrastructure / Testbed

The infrastructure used for our experimentation is the Patras5G testbed infrastructure [5] [6], which currently deploys one of the main 5G experimental facilities in 5G-VINNI [7], a European HORIZON 2020 project. This 5G facility is used to host verticals and applications (in the areas of Media, Gaming, Transportation and Energy) from two ICT 19 European HORIZON 2020 projects (5G-SOLUTIONS [8] and 5G-VICTORI [3]).

The main cloud platform is located inside Patras University, and can host among others, 5G core network components and any NFV required for services oriented to the supported verticals. The cloud platform offers a total computing power of 212 CPUs and 768 Gigabytes of RAM and 30 TB of storage.

Furthermore, the facility can also deploy outdoor MEC units capable of supporting both cloud computing and 5G or other wireless connections. The main MEC unit of the facility is the "5G Autonomous Edge" [9], a mobile box, built for on-demand 5G deployments depending on the verticals' use case requirements. The Autonomous Edge (Figure 3) is based on 3 INTEL Xeon based servers giving in total 16 cores, 128 Gigabytes of RAM and 1 TB of storage. Additionally, it is connected with a 5G Software Defined Radio interface. (Ettus USRP N310 [10])



Fig. 3. Autonomous Edge and NB-IoT setup

Software wise, both core platform and MEC platform support the ETSI NFV architecture. A basic element of this architecture is the Management and orchestration (MANO), which is the framework that coordinates the network resources and the management of VNFs. Open Source MANO (OSM) [11] is the MANO used, while the virtualized environment is based on Openstack [12].

ETSI OSM is an ETSI initiative to create an Open Source NFV-MANO framework aligned with its reference architecture and standards. ETSI OSM provides an end-to-end network service orchestration functionality through the interaction of the core components of its architecture. The module Resource Orchestrator (RO) of OSM, plays a fundamental role since it is the block in charge of managing the allocation of computational resources (i.e., the compute, network, and storage). This accommodates the execution over an NFVI of various virtual network functionalities included in a network service. For this purpose, the RO supports the interactivity with a large variety of VIM solutions such as Openstack.

On top of the core platform and any number of deployed MEC devices, the Patras5G testbed infrastructure hosts an Operations Support System (OSS), called Openslice [13]. It supports VNFD/NSD onboarding to OSM and Network Service (NS) deployment management, which allows control of what applications and services can be run and deployed on our experimentation infrastructure.

Regarding 5G connectivity, the facility can support 4G/5G core services along with the required radio using SDR based solutions. Both open source and commercial implementations can be used and deployed as required. 5G capable UEs include mobile phones and CPEs acting as gateways to legacy devices. Furthermore, NB-IoT is also supported by the facility both in deploying such a network and providing NB-IoT enabled devices such as the Sara R410 NB-IoT developer boards [14]. These devices connect through a deployed NB-IoT network and can transmit information such as location, humidity, temperature etc.

For further support of the services provided by the Patras5G also provides monitoring solutions if required that allow the gathering of various metrics (sys-

tem or network related) from the deployed services and deliver them to the interested parties. The solution used is Netdata [15] an open-source, performance and health monitoring system for systems and applications which can be configured to gather metrics from various sources.

For more persistent storage and centric oriented monitoring, an IoT platform is deployed to gather data from each of the IPTO sites. Furthermore, VPN services are also available for secure and isolated services among the users of the infrastructure.

5 Scenarios

Towards a realization of the proposed architecture, in this section, two different operational scenarios are presented. In scenario 1, the services collect, store, and visualize a set of measurements from an NB-IoT gateway, whereas in scenario 2, the NB-IoT gateway and the EDGEX foundry are reconfigured by issuing specific commands to them.

Scenario 1: Figure 4 illustrates the complete flow for a set of measurements, originating from a Sodaq Sara R410 NB-IoT [14] gateway, to the end user.

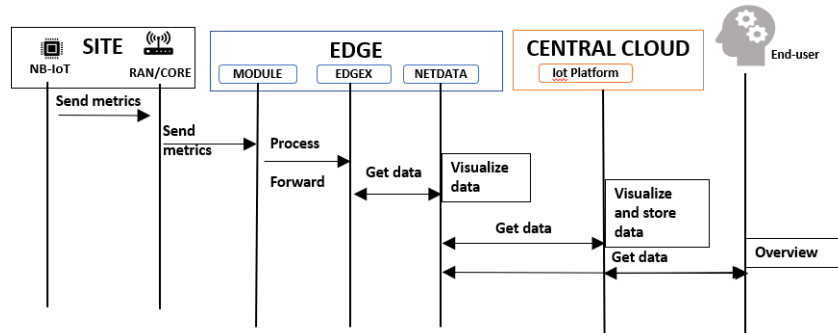


Fig. 4. Sequence diagram of NB-IoT data path

The NB-IoT device is connected to the NB-IoT cellular network, deployed by the Limenet Mini [16], and periodically sends the sensor's readings (temperature, humidity and location), via a custom-made UDP client. The gateway is configured to send a new set of measurements every 1 sec. The other end of the connection is the NB-IoT proxy deployed as VNF.

At the NB-IoT proxy, a UDP server receives the UDP packet and extracts the needed information. For each reading, a different HTTP request is constructed and sent to the corresponding REST device of the EdgeX Foundry REST device

service. In this scenario, three REST devices named `Sara_temp1`, `Sara_hum1` and `Sara_loc1` are added in the configuration service of EdgeX.

When the HTTP request for a reading is received by the assigned REST device, the device service translates the request and stores the reading at the EdgeX database via the Core Service functionality. From there, every vertical application can access the data via HTTP GET requests. MEC approach allows for the readings to be locally stored and further processed on site.

For real-time monitoring of the facility at a local level, a Netdata instance can also be deployed at the MEC whenever requested. This is achieved by instantiating a NS which deploys a VNF that automatically installs and configures Netdata. This VNF can communicate with EdgeX Foundry through periodic HTTP GET requests to collect and visualize the stored measurements. By accessing Netdata the site health status can be monitored locally. For a holistic monitoring of the IPTO sites, and for applications that require synchronized measurements from both sites, each MEC can also connect to an IoT platform on the core network allowing the monitoring of all sites on central IPTO site.

Scenario 2: Besides getting measurements from the deployed devices, the architecture also allows for on-the-fly configuration changes on the deployed services. This can be performed by using the day-2 configuration capabilities of the OSM, which allows us to send appropriate commands to the Network Functions to implement our services. This scenario can be seen in Figure 5.

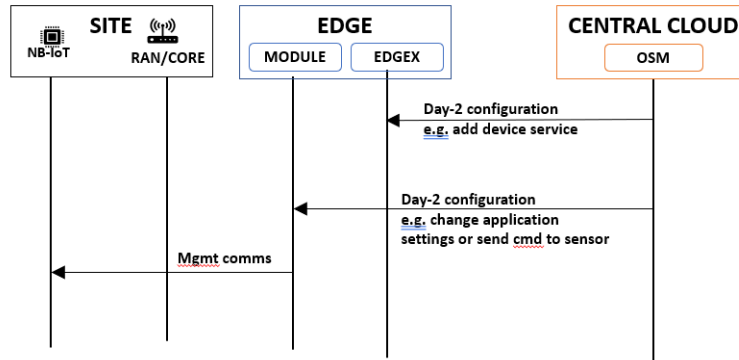


Fig. 5. Sequence diagram of control path

In this scenario two changes are performed to the previous setup. First, OSM's day-2 configuration capabilities can be used to add a new device entry at the EdgeX foundry Core service. As a second change, a modification of the reporting period of the UDP client in the NB-IoT gateway is required. This

time OSM issues a command to the NB-IoT endpoint with the new reporting period value. The NB-IoT endpoint then translates the command and forwards it to the respected NB-IoT gateway through their communication path. Instead of altering the reporting period, the command could refer to other configuration allowed by the software running on those devices, providing a rudimentary over-the-air update of those devices.

6 Conclusions and Future Work

This work presents current prototype results of the transformation process of a legacy facility to a Smart Factory, adopting a cloud-edge architecture and modern 5G/IoT solutions able to support sufficiently the different services deployed in a Smart Factory (operation, security, maintenance). By leveraging the concepts of NFV and MEC, and a set of open-source applications (EdgeX, Net Data, OSM), the IoT platform and related monitoring solution is centrally reconfigured in a flexible and cost effective manner, in order to support new services, especially in the areas of Industry 4.0 and 5G. Towards this realization, two different services are presented, for data collection and for on-the-fly reconfiguration.

Our next steps will be to enhance the solution with new functionality for the support of different industrial communication protocols, and new types of sensors. We will contribute to the open source community by extending the capabilities of the EdgeX platform. Furthermore, we will take advantage of the local processing capabilities provided by the architecture to achieve improved real-time equipment awareness and develop smarter control techniques.

References

1. Smart Factory of Industry 4.0: Key Technologies, Application Case, and Challenges, <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8207346>.
2. Information and Communication Technologies (H2020-ICT-2018-20) Call <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/ict-17-2018>.
3. 5G VICTORI Homepage, <https://www.5g-victori-project.eu/>.
4. EdgeX Foundry Homepage, <https://www.edgexfoundry.org/>.
5. Christos Tranoris, Spyros G. Denazis: Patras 5G: An open Source based End-to-End facility for 5G trial. In: ERCIM News 2019(117) (2019)
6. Patras 5G homepage, <https://wiki.patras5g.eu/>.
7. Horizon 2020 homepage, <https://www.5g-vinni.eu/>.
8. 5G Solutions project homepage, <https://www.5gsolutionsproject.eu/>.
9. Autonomous edge Homepage, <https://wiki.patras5g.eu/5g-autonomous-edge>.
10. Ettus Homepage, <https://www.ettus.com/all-products/usrp-n310/>.
11. OSM Homepage, <https://osm.etsi.org>.
12. Openstack Homepage, <http://www.openstack.org/>.
13. Openslice Homepage, <https://openslice.readthedocs.io/en/stable/>.
14. Sodaq Homepage, https://support.sodaq.com/Boards/Sara_AFF/.
15. NetData Homepage, <https://www.netdata.cloud/>.
16. LimeNetMini Homepage, <https://limemicro.com/products/systems/limenet-mini/>.