# Designing a high-fidelity Testbed for 5G-based Industrial IoT

**Diogo Cruz, Tiago Cruz, Vasco Pereira and Paulo Simões**
University of Coimbra, CISUC, DEI, Portugal

diogocruz@student.dei.uc.pt
tjcruz@dei.uc.pt
vasco@dei.uc.pt
psimoes@dei.uc.pt

**Abstract:** With the rise of the Industrial IoT (Internet of Things) and Industry 4.0 paradigms, many control and sensor systems used for IACS (Industrial Automation and Control Systems) have become more complex, due to the increasing number of interconnected field devices, sensors and actuators often being geographically spread across large areas. Supporting these increasingly sophisticated networked scenarios calls for the involvement of telecommunications and utility providers to better support Machine-to-Machine (M2M) communications and infrastructure orchestration, for which 5G technology is considered a perfect match.

Nowadays, such 5G networks empower solutions both for consumer and for industrial IoT scenarios, providing the capacity and the means to seamlessly connect a massive number of gadgets and sensors, with diverse data rate requirements, low latency, and low power consumption. Part of this flexibility is also due to the nature of the 5G Service Architecture (SA), which is based on a microservice concept, dividing its core through multiple functions, allowing it to horizontally scale in a flexible way. Furthermore, the 3GPP specifications encompass specific support for verticals by means of slicing and 5G LANs, paving the way for a paradigm shift in terms of the relationship between service, telecom, and operational infrastructure tenants. However, such benefits come at the cost of extra complexity and, consequently, an increased vulnerability surface. This calls for further research focused on improving 5G infrastructure management, service integration and security, which cannot be safely undertaken in production environments, thus motivating the development of suitable 5G testbeds.

This research work, which was developed in the scope of the POWER and Smart5Grid P2020 projects, addresses the creation of a high-fidelity environment for 5G-related research, which encompasses a gNodeB and 5G core, together with emulated User Elements (terminal devices) and IoT nodes (in this specific case, Programmable Logic Controllers), constituting a 5G Industrial IoT scenario designed for development and validation of new solutions, security research, or even advanced training purposes. The entire infrastructure is supported via container orchestration technology, providing enhanced scalability and resilience characteristics.

**Keywords:** 5G, Industrial IoT, Testbeds, Cyber-ranges

## 1. Introduction

The fifth-generation standard for broadband cellular networks, often designated as 5G, was devised to provide faster internet speeds, lower latency, and more capacity than previous generations. It has the potential to be used in various applications, such as self-driving cars, remote surgery, virtual reality and more. 5G is also considered an enabler for evolved Internet of Things (IoT) use cases, allowing to create and support networks of intelligent devices and appliances, that are embedded with sensors, software, and other technologies that enable them to collect and exchange data with each other and with other systems. The IoT paradigm has the potential to revolutionize a wide range of industries, including healthcare, transportation, and manufacturing, by enabling the development of new products and services that can improve efficiency, productivity, and safety. Unsurprisingly, the integration of 5G technology with IoT is widely regarded as an opportunity to create new and innovative products and services, taking advantage of the faster, more responsive, and reliable connections provided by 5G networks, which can also scale to support a large number of devices and data-intensive applications.

This paper describes the design of a testbed for research of 5G-driven Industrial IoT, developed within the scope of the POWER (POWER, 2020) and Smart5Grid (Smart5Grid, 2021) research projects. This testbed includes a 5G Core (5GC), Programmable Logic Controller (PLC) instances, User Equipment (UE) instances, and Next Generation Radio Access Network (NG-RAN) emulation components, supported by means of a container orchestration framework infrastructure. This testbed is used to implement a 5G-enabled Supervisory Control And Data Acquisition (SCADA) Industrial IoT scenario using several PLCs, designed with two objectives in mind: to add a practical element to the research, and to help validate the testbed itself. Overall, this testbed aims to explore the potential of these technologies and their ability to drive progress in various fields.

The rest of this paper is organized as follows. Section 2 presents a quick primer on 5G technology. Section 3 introduces the key technologies that enable/support the testbed. Section 4 delves into the testbed from a user perspective, examining its structure and network topology. Section 5 describes how the testbed is used to implement a simple but representative Use Case, and Section 6 concludes the paper.

## 2. A quick primer on 5G technology

In the following subsections, we will explore the system overview of 5G, including its architecture based on the Service-Based Architecture (SBA) framework. We will also delve into the topic of 5G verticals and 5G Local Area Networks with support for the Industrial Internet of Things (IIoT).

### 2.1 System Overview

The current 5G specification is the culmination of the work started by the International Telecommunication Union in 2015, with the publication of the International Mobile Telecommunications – 2020 (IMT-2020) standard (ITU, 2015), which listed the requirements for future 5G networks. Following the availability of these requirements, the 3rd Generation Partnership Project (3GPP) (3GPP, 2022) started developing the technical specifications to implement the IMT-2020 standards in mobile communication networks. In 2018, 3GPP released its first package of technical specifications for standalone 5G networks, known as Release 15 (3GPP TSG, 2019). This release included the full batch of 3GPP specifications for 5G, introducing a New Radio (NR) access technology and other important concepts, geared towards improved reliability, increased modularity, and faster response times.

Release 16 (3GPP TSG, 2020), which was functionally frozen in December 2020, specified the second phase of 5G deployment. Release 16 built upon the foundations established in Release 15 to introduce new features and capabilities to further improve the performance of 5G networks. Some of the key features of Release 16 included:

- Enhanced Mobile Broadband: aimed at improving the quality of mobile broadband services by increasing the data rates and capacity of 5G networks.
- Ultra-Reliable Low Latency Communications: providing low latency and high reliability for applications that require real-time communication, such as remote surgery or autonomous driving.
  Massive Machine-Type Communications: allowing to support a large number of devices with low data rate requirements, such as sensors and other IoT devices.

Release 16 presented enhancements to the 5G Core network designed to increase its flexibility and ease of maintenance and provisioning, including support for network slicing, which allows for the simultaneous deployment and use of multiple Core Networks, each one specialized in providing a specific set of services and/or subscribers. It also introduced Network Function Virtualization (NFV) and support to edge computing, the latter targeted at bringing computational power closer to the end-user to reduce the response time of the network for applications that require low latency, such as virtual reality, autonomous driving, or evolved IoT.

Release 17 (3GPP TSG, 2022), functionally frozen in March 2022, brings a range of enhancements that focus on increasing capacity and coverage, improving latency, reducing power consumption, and expanding support for a wide range of devices and applications. Some of the key areas of improvement include further development of massive MIMO, coverage enhancements for diverse deployments, power savings for mobile devices, spectrum expansion to higher frequency bands, and enhanced support for ultra-reliable low-latency communication and private networks. Additionally, it includes new capabilities such as support for reduced capability devices (important in the scope of IoT), support for non-terrestrial networks, expansion of sidelink capabilities, and improved precise positioning. These enhancements push the technology boundaries on many fronts, making 5G more versatile and efficient.

Next, we will examine the architecture of 5G and explain the various components that make up this complex system. We will also discuss the functions and capabilities of these components, and how they contribute to the overall performance of 5G networks.

### 2.2 Architecture

As previously referred, the 5G architecture is an SBA. An SBA is a design approach for building systems in which the architecture elements are defined in terms of Network Functions (NFs) rather than by traditional network entities. In an SBA, any given NF offers its services to all other authorized NFs and/or to any "consumers" that are permitted to use these provided services. This approach offers modularity and reusability, as it allows for the creation of flexible and scalable systems that can be easily modified or expanded as needed to support new features and services. (3GPP, 2022).

In the context of 5G, the 3GPP has adopted an SBA framework for the 5GC. The 5GC is the part of the 5G network that controls the communication between the User Equipment (UE), itself composed of a Mobile Station and a Universal Subscriber Identity Module (USIM), and the data network. It is formed of several NFs that work together to provide various services to the UE. These NFs can be grouped into two main categories: the User Plane, which handles user data transport, and the Control Plane, which handles network signalling and control.

In 5G, there are two modes of operation: StandAlone (SA) and Non-SandAlone (NSA). The SA mode leverages the 5GC together with a Next Generation Radio Access Network (NG-RAN) to provide end-to-end connectivity to users, while the NSA mode relies on the Evolved Packet Core (EPC) or 4G/LTE infrastructure to provide connectivity and uses the 5GC and RAN for additional functionality and improved performance. Both modes offer various features and benefits, and the choice of which mode to use depends on the specific requirements and goals of the deployment.

In SA mode, the other major 5G component besides the 5GC is the NG-RAN. The NG-RAN is the network subsystem that provides wireless connection between the UE and the 5GC. The NG-RAN is responsible for transmitting and receiving radio signals to and from the UE and to perform radio resource management tasks such as allocation of radio resources and interference management. The main entity of the NG-RAN is the gNodeB (gNB), which is the radio transmitter responsible for transmitting and receiving radio signals to and from the UE. The gNB may be further divided into a gNB-Central Unit (gNB-CU) and one or more gNB-Distributed Units (gNB-DUs) linked by the F1 interface. The F1 interface supports signalling exchange and data transmission between the endpoints, separates Radio Network Layer and Transport Network Layer, and enables the exchange of UE-associated and non-UE-associated signalling.

The NG-RAN is connected to the 5GC via the NG interface, and it uses the 5GC to control the communication between the UE and the data network. The NG-RAN and the 5GC work together to provide various services to the UE, including voice and data communication, location services, and access to the internet and other data networks. Finally, the Xn control plane (Xn-C) interface is defined between two NG-RAN nodes. The transport network layer built on this interface is based on the Stream Control Transmission Protocol (SCTP) running on top of IP. **Figure 1** illustrates the connection between the NG-RAN and the 5GC.

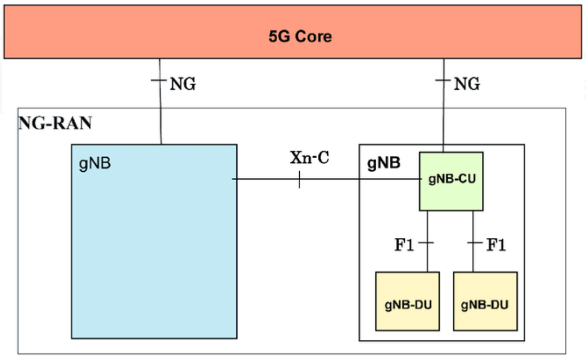


**Figure 1: Architecture 5G base station gNB. Source: (Tikhvinskiy et al., 2020)**

## 2.3 5G Verticals

A 5G vertical refers to a particular industry or market segment that a 5G network is designed to serve. Different industries may have specific requirements for connectivity or capabilities, and telecommunications companies may offer specialized solutions for each vertical to meet those needs. By segmenting the market into different verticals, companies can tailor their products and services to the specific needs of each industry. The main 5G verticals (5G-PPP JI, 2023) are:

- Automotive: Promoting self-driving vehicles and other transportation innovations, improving safety and reducing congestion.
- Manufacturing: Boosting the use of robotics and automation in manufacturing, improving efficiency and reducing costs.

- Media: Allowing higher-quality streaming of video and other media, as well as the use of virtual and augmented reality in the media industry.
- Energy: Facilitating the use of the Internet of Things (IoT) in the energy industry, allowing for the remote monitoring and control of power grids and other energy infrastructure.
- eHealth: Allowing remote surgery, telemedicine, and other healthcare services, permitting doctors to treat patients remotely and providing access to healthcare in underserved areas.
- Public Safety: Using faster response times for emergency services, as well as the use of drones and other technologies for search and rescue operations.
- Smart Cities: Enabling the use of IoT in city infrastructures, such as smart traffic systems and smart lighting, as well as the use of sensors and other technologies to improve services and living standards.

Overall, it is expected that 5G technology may enable the development of new and improved services across a wide range of vertical industries, with the potential to increase efficiency, improve safety, and enhance the quality of life for citizens.

### 2.4 5G Local Area Networks

A 5G Local Area Network (LAN) is a type of private cellular network that is designed specifically for use by enterprises. It integrates with an organization’s existing Information Technology (IT) infrastructure to provide high-speed, predictable wireless connectivity with deterministic performance and latency for mission-critical digital initiatives across the enterprise. 5G LANs differ from commercial 5G services and Managed Service Providers (MSPs) in that they offer more control and flexibility to the enterprise, as well as the ability to integrate seamlessly with the organization’s existing IT infrastructure and policies. 5G LANs use private spectrum and plug-and-play hardware and can be easily scaled and budgeted for without the need for specialized cellular network expertise. They are suitable for use in a variety of environments, including hospitals, factories, warehouses, and retail stores (Team Celona, 2020). Here are a few examples of how they might be used:

- Manufacturing: enabling IoT devices for instantaneous performance, output, and maintenance updates, and providing customized coverage and controls for applications, sensors, and devices.
- IIoT: supporting thousands of devices and sensors throughout industrial systems and offering wired-like reliability in complex environments with customized hardware, increased power levels, and multiple frequency bands.
- Healthcare: providing secure and reliable connections for patient room technologies and staff, and to configure service level objectives to serve patient health sensors, ventilators, clinical applications, and medical inventory levels.

Overall, 5G LANs offer a range of benefits for businesses and organizations that need high-speed, reliable wireless connectivity within a specific location. These networks can be deployed as standalone systems or as part of a larger 5G network, depending on the specific needs and requirements of the user.

### 2.5 5G Testbeds for IIoT integration and security research

There are recently developed testbeds for 5G research, as it is the case for the 5Greplay testbed (Salazar et al., 2021, which was designed for 5G security research and development of fuzzing platform for attack injection. BlueArch (Ghosh et al., 2019) uses several open-source components to provide a 5G customizable platform for experimentation of several scenarios, including IoT-based ones. (Amponis et al., 2022) also describes a testbed that shares some similarities with the one presented in this paper, designed as a cyber-range to test attacks against the 5G Core and RAN.

The testbed hereby presented distinguishes itself from previous efforts due to the fact that it’s based on a cloud native deployment, also being designed to incorporate a mix of real and emulated equipment, supporting an IIoT scenario that can be used for research purposes in a protected environment. It provides a realistic reproduction of the characteristic 5G service footprint, also including user equipment and an underlying infrastructure very similar the one found on commercial hosting platforms.

## 3. Enabling Technologies

This section introduces the key technologies that enable/support the testbed. These technologies have been carefully selected based on their common integration capabilities, as well as their popularity and proven track record in the industry. Additionally, other important factors were taken into consideration, such as their stability, security, scalability, ease of use, cost-effectiveness, and community support. Furthermore, the open-source nature of many of these technologies gives the advantage of being able to customize the technology to our specific needs, which can lead to cost savings and reduction of vendor lock-in. They also have a robust ecosystem of third-party tools and services, making them a suitable choice for organizations that want to integrate with their existing infrastructure.

## 3.1 Rancher's RKE and Server

Rancher Kubernetes Engine 2 (RKE2) (SUSE Rancher, 2023) is an open-source distribution for deploying and managing Kubernetes (K8s) (CNCF, 2022) clusters. It was chosen due to its ease of use, as well as for its opensource nature allowing for freedom in terms of usage and modification, providing flexibility in customization. Additionally, its reliability and robustness have been widely assessed in the scope of production environments and real-world scenarios.

The RKE2 deployment is complemented by a Rancher Server (SUSE Rancher, 2022) that provides a graphical user interface for managing a Kubernetes cluster, its containers, and applications. It is designed to make it easier for users to interact with their clusters and deploy and manage their applications. Some of the key benefits of using the Rancher server include its ease of use, which provides a user-friendly interface that makes it simple to manage and monitor a Kubernetes cluster, even for users who are not familiar with Kubernetes. Additionally, the Rancher server includes several functionalities that allow users to monitor and manage the resources within their cluster, such as the ability to view metrics, logs, and events for individual pods, as well as the ability to manage and scale deployments.

## 3.2 Open5GS and UERANSIM

Open5GS (Lee, 2022) is an open-source implementation of the 5GC and EPC written in the C programming language. It can act as a core network for New Radio (NR)/Long Term Evolution (LTE) setups and can operate in both StandAlone (SA) and Non-Standalone (NSA) modes. UERANSIM (Güngör, 2022) is the next generation of open-source 5G User Equipment (UE) and Next Generation Radio Access Network (NG-RAN) (gNodeB) implementation. It can be considered as a 5G mobile phone and a base station in basic terms, both running as virtualized instances. The UERANSIM project can be used to test the 5G main components and study the 5G system.

## 3.3 OpenEBS

OpenEBS is a technology that allows dynamic storage of persistent volumes (OpenEBS, 2021), making it a good fit for organizations with varying storage needs. It creates persistent volumes which are important for applications that need to retain data across restarts or failures. The automatic linking of a created volume with a specified application, such as a Database (DB), simplifies the process of setting up and configuring storage.

## 3.4 Kube-vip

Kube-Vip (Linux Foundation, 2022) provides Kubernetes clusters with a virtual IP and load balance for the control plane (to build a highly available cluster) and *LoadBalancer* type Kubernetes Services without relying on any external hardware or software. Regarding the cluster servers, there is a leader, and if the leader goes down, Kube-VIP quickly assigns another leader (about 10s) to always guarantee high availability.

## 3.5 OpenPLC

OpenPLC (OpenPLC Project, 2022) is the first fully functional standardized open-source PLC ("PLC", 2023), both in software and hardware. It is mainly used in industrial and home automation, IoT and SCADA research, as it carries built-in security features. It also does not require any additional licensing fees and allows for frequent updates and patches. The OpenPLC Project consists of two parts: Runtime and Editor. A Runtime is a portable software designed to run from the smallest of all microcontrollers (Arduino-compatible) to powerful servers in the cloud. The OpenPLC Editor is the software that runs on your computer and is used to create PLC programs. It is very simple to use and supports all languages that are compatible with PLC.

OpenPLC instances communicate with other PLCs primarily using Modbus (Modbus Organization, 2023) that runs over port 502 using Transmission Control Protocol (TCP)/Internet Protocol (IP), albeit other protocols, such as DNP3 (DNP ORG, 2023), are also supported. Modbus adopts a master-server communication pattern based on polled operations, where the slave synchronizes with the master by reading and writing specific registers that are configured by the user, such as output registers, input registers, and other types of registers. This allows the PLCs to exchange data and coordinate their actions to control and monitor industrial processes.

## 4. Design and Implementation of the Testbed

In this section, we will delve into the testbed from a user perspective, examining its structure and network topology. Additionally, we will cover how to check connectivity between PLCs and present a use case to illustrate and validate the testbed's capabilities.

### 4.1 User Viewpoint and Structure

The foundations of this testbed are based on a Kubernetes cluster, which enables the automatic management of resources according to predefined rules. The Rancher Kubernetes Engine 2 (RKE2) is the technology used for the production grade Kubernetes cluster distribution. A Rancher Server, complete with a graphical interface, was deployed within the cluster to control it. Kube-VIP was also deployed within the cluster to provide high availability using a floating virtual IP. To provide dynamic persistent volumes for the MongoDB database used in the 5GC, OpenEBS was deployed, which automates this process.

For the 5GC, the Open5GS implementation was used, which is composed of a set of functions deployed within the cluster. For users to connect to the 5G network, the radio simulator and user equipment are provided by UERANSIM, which is also deployed within the cluster. This implementation was used to provide access to the 5G network because it is inserted within the same namespace as the cluster, as otherwise it would not function properly. The implementation of the use case will be carried out by utilizing both OpenPLC and UERANSIM. In **Figure 2**, we can see a visual representation of the building blocks and tools used in the proposed testbed.

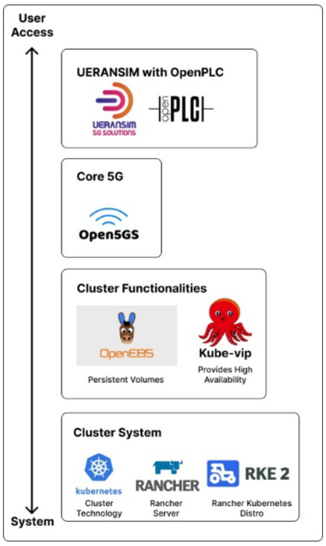


**Figure 2: Diagram of every technology used from a user perspective access to the testbed.**

The testbed specific structure is depicted in **Figure 3**. There are two ways to access the cluster: through a Virtual Machine (VM) that has a master node, or by connecting to an endpoint on the rancher server. Both methods require a Virtual Private Network (VPN) to the data center, managed by a hypervisor that oversees the allocation of resources, VMs, and networks, where this testbed is deployed. Additionally, it is possible to access one of the pods if they have an exposed web interface. The master nodes provide high availability using a floating Internet Protocol (IP) address. The Kube-VIP service allows for the creation of multi-node or multi-pod clusters, which can be used to provide even greater availability. In particular, the cluster can be configured to use an Address Resolution Protocol (ARP) mode, in which a leader is elected and inherits the virtual IP. This leader is responsible for load balancing within the cluster, allowing for the seamless integration of new worker nodes without interrupting the overall functionality of the cluster, even if the leader goes down.

The cluster operates by sharing resources between worker nodes, which Kubernetes uses to manage pods containing various technologies, including UERANSIM, OpenPLC, Open5GS functions, OpenEBS, Rancher Server, and Kube-VIP. These technologies are typically deployed in individual pods except for UERANSIM and OpenPLC, which are deployed together. These pods can be easily replicated to meet changing needs.

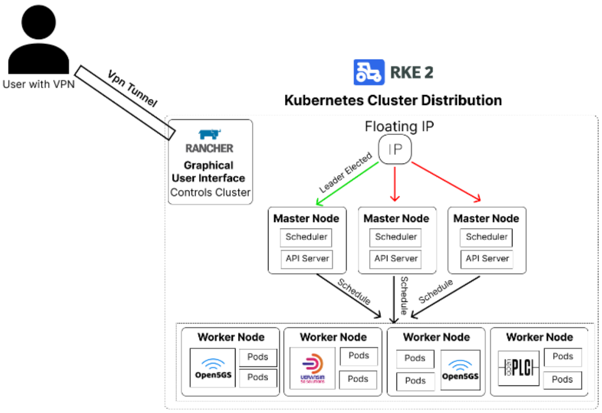


**Figure 3: Structure diagram of the testbed.**

Next, we will look at how the endpoints work in the Kubernetes cluster (**Figure 4**). In a K8s cluster, services typically have a fixed IP address that can be accessed over the internet without the need for an ingress. These services are configured with the "Load Balancing" type, which is provided by Kube-VIP and distributes the load evenly across all pods. Pods are one or multiple containers in runtime. The **Figure 4** shows 3 services with 3 pods each. For each service, there are 3 replicas of a pod. This example can be scaled as needed.

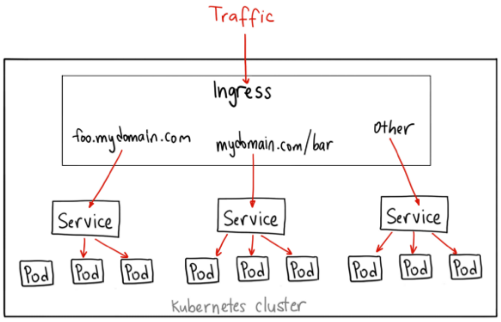


**Figure 4: Diagram of services in detail. Source: (Abualrob, 2022)**

## 4.2 Network Topology

For the network, we use port **group 223**, because it's configured with a DHCP Server and a VPN server facilitating the setup of the cluster and accessing it from a VPN client. **Figure 5** illustrates the testbed network topology.

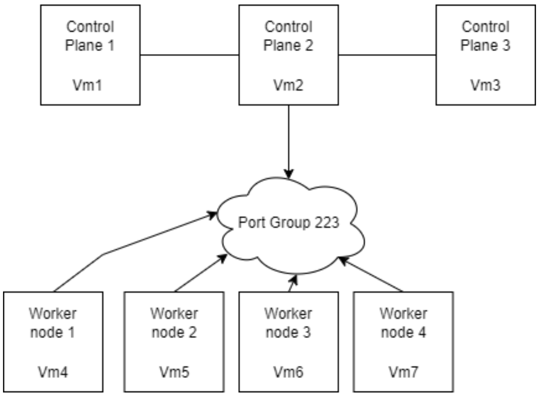
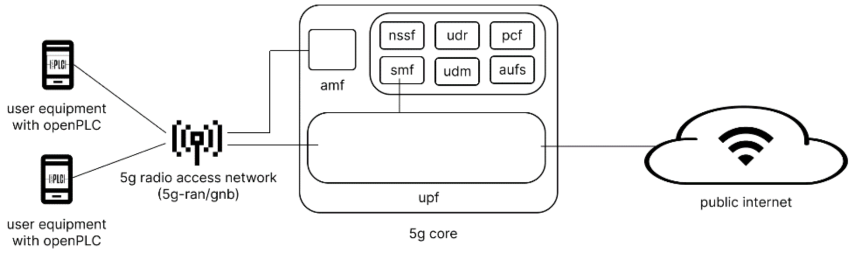


**Figure 5: Network topology of our testbed.**

The testbed implemented includes 7 VMs, three of them corresponding to the master nodes and having fixed IP addresses. These are responsible for managing the cluster, and resources and assigning tasks to the agent nodes (workers). Agent nodes(workers) have dynamic IP because they don't need to have static IPs, as they can be dynamically scaled up or down. These connect to the cluster from the virtual IP that makes the master nodes in high availability. There is a fixed IP range where the services are hosted automatically.

## 5. Use Case – OpenPLC communications using a 5G Core

This section describes a simple but representative Use Case: OpenPLC communications using a 5G Core. This use case demonstrates the capabilities of the testbed in the field of IIoT by creating a practical scenario where OpenPLC software is utilized within virtual containers and user equipment is used for network interfaces. The scenario involves connecting a master device to a slave device and verifying successful communication via the 5G network using the Modbus protocol. To test synchronization between OpenPLC registers through the 5GC, tools such as *tcpdump* (Tcpdump Group , 2023) and *Modbus poll (*Witte Software, 2023) can be used. *tcpdump* provides information on traffic between IP addresses and can verify the use of IPs belonging to the 5GC. *Modbus poll* can be used to read and write to registers belonging to the master and slave devices. **Figure 6** illustrates the communication between the OpenPLC instances.



user equipment with openPLC
user equipment with openPLC
5g radio access network (5g-ran/gnb)
amf
nssf
udr
pcf
smf
udm
aufs
upf
5g core
public internet

**Figure 6: OpenPLC use case. The master device connects to the User Plane Function (UPF) in the 5GC, then reaches the slave device.**

This IIoT scenario (see Figure 7) reproduces a hub-and-spoke topology similar to the one used in (Sousa et al., 2021), reproducing a topology with several geographically distributed elements. PLC master nodes query other PLC nodes to gather information from sensors, which are stored in specific Modbus holding registers – this scenario involves both horizontal (PLC-PLC) and vertical (PLC-HMI) communication patterns with polling cycles scheduled at 100ms intervals. Each Master has several configured PLC slaves, which are regularly pooled – the latter implement the control loops for locally attached sensors, also performing actuation. The underlying logic considers a process for controlling the water level control in a pumping station, using a level sensor and a water pump which is activated when a certain threshold is reached.

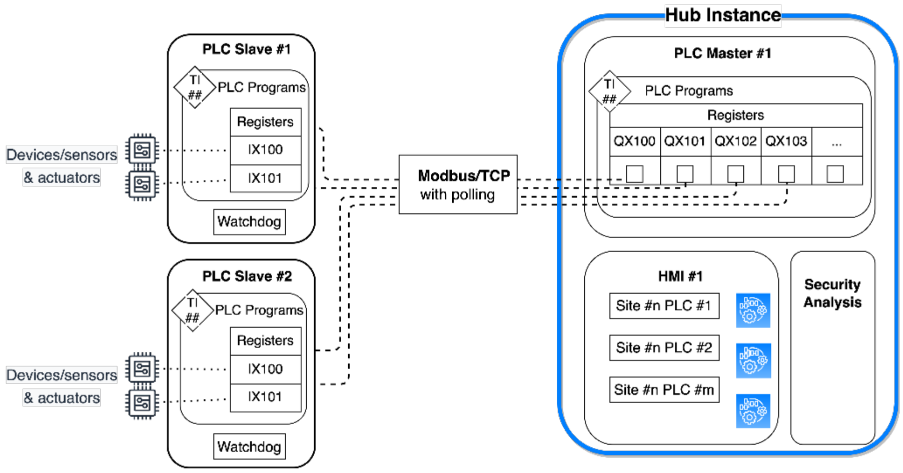


**Figure 7: Hub-and-spoke architecture for the IIoT scenario**

PLCs are programmed using Ladder Logic language, with the device and actuator information being mapped into PLC registers whose type is chosen accordingly with the nature of the involved data (Modbus is a very simple protocol with rudimentary data models) – for instance, discrete input coils (%IX addresses) can represent binary states (connected - 1/true, and disconnected - 0/false), while analog registers (%IW for input or %QW for outputs) can store values varying along a scale or range, being mapped in 16 bit registers. This architecture also enables the aggregation of data in Human-Machine Interface (HMI) consoles, providing informational dashboards can be designed to convey real-time information and also be used to trigger actions.

This architecture can accommodate a mix of real and emulated equipment, also being able to be fed by real data coming from a cyber-physical process used in production. In this latter case, it means that the proposed IIoT scenario can evolve into a Digital Twin, taking advantage of the specific 5G service assurance characteristics to offer an off-premises safety and security-enhancing service.

## 6. Conclusions

This paper has presented the development and implementation of a testbed for the evaluation of 5G and IIoT technologies. The testbed is based on open-source technologies such as UERANSIM as the Next Generation Radio Access Network (NG-RAN), Open5GS as the 5GC, OpenPLC to simulate PLCs, and RKE2 as the K8s distribution, which were chosen for their integration, popularity, and reliability. The testbed has been designed to provide a flexible and cost-effective solution for researchers and developers to simulate and benchmark their solutions in an easy-to-use framework.

To confirm the effectiveness of the testbed, a IIoT use case for OpenPLC communications using a 5G Core was implemented and the results showed successful communication between OpenPLC instances utilizing the 5GC. This use case not only validated the capabilities of the testbed in the field of IIoT but also demonstrated the potential for future advancements in industrial communication using 5G technology.

## Acknowledgments

This work was supported in part by the Fundo Europeu de Desenvolvimento Regional (FEDER)-Competitiveness and Internationalization Operational Program (COMPETE 2020), Portugal 2020 Framework, in the scope of the Smart5Grid Project, under Grant POCI-01-0247- FEDER-047226; and in part by the FCT–Foundation for Science and Technology, Instituto Público (I.P.)/MCTES through National Funds, within the scope of Centre for Informatics and Systems of the University of Coimbra (CISUC) Research and Development Unit, under Grant UIDB/00326/2020 and Project UIDP/00326/2020.

## References

3GPP TSG Group. (2019). 3GPP, Release 15. Available at: https://www.3gpp.org/specifications-technologies/releases/release-15

3GPP TSG Group. (2020). 3GPP, Release 16. Available at: https://www.3gpp.org/specifications-technologies/releases/release-16

3GPP TSG Group. (2022). 3GPP, Release 17. Available at: https://www.3gpp.org/specifications-technologies/releases/release-17

3GPP. (2022). 3GPP, a 5G analysis. Available at: https://www.3gpp.org/technologies/5g-system-overview

3GPP. (2022). 3GPP, about us. Available at: https://www.3gpp.org/about-us

5G-Infrastructure-PPP Joint Initiative. (2023). 5G And Verticals. Available at: https://5g-ppp.eu/verticals/

Abualrob, S. (2022). Kubernetes: Expose pod externally bypass service load balancing. Medium. Available at: https://medium.com/@suleimanabualrob/kubernetes-expose-pod-externally-bypass-service-load-balancing-bf89038afee2

Amponis, G. and Radoglou, P. and Thomas, G. and Ouzounidis, S. and Zevgara, M. and Moscholios, I. and Goudos, S. and Sarigiannidis, P. (2022) "Towards Securing Next-Generation Networks: Attacking 5G Core/RAN Testbed" in Proceedings of PACET 2022: PAnhellenic Conference on Electronics and Telecommunications, December 2-3, 2022, Tripolis, Greece.

CNCF (2022). Kubernetes Documentation. Available at: https://kubernetes.io/docs/home/

DAEnotes (2023). PLC Diagram. Available at: https://www.daenotes.com/electronics/industrial-electronics/PLC-programable-logic-control

DNP ORG. (2023). Overview Of DNP3 Protocol. Available at: https://www.dnp.org/About/Overview-of-DNP3-Protocol

Güngör, A. (2022). GitHub UERANSIM. Available at: https://github.com/aligungr/UERANSIM

In Wikipedia. (2023). PLC. Available at: https://en.wikipedia.org/wiki/Programmable_logic_controller

ITU. (2015). IMT-2020. Available at: https://www.itu.int/en/ITU-T/focusgroups/imt-2020/Pages/default.aspx

Lee, S. (2022). Open5gs - documentation. Available at: https://open5gs.org/open5gs/docs/

Linux Foundation. (2022). Kube-vip. Available at: https://kube-vip.io/docs/

Modbus Organization. (2023). The Modbus Official Site. Available at: https://modbus.org/

OpenEBS Project. (2021). OpenEBS. OpenEBS documentation: Openebs docs. Available at: https://openebs.io/docs/

OpenPLC Project. (2022). Open-source PLC software. Available at: https://openplcproject.com/

Pathak, R. (2022). Deploying 5g core network with open5gs and ueransim. Rahasak Labs. Available at: https://medium.com/rahasak/5g-core-network-setup-with-open5gs-and-ueransim-cd0e77025fd7

POWER Project. (2020). POWER - Empowering a digital future. Available at: https://www.cisuc.uc.pt/en/projects/power

Smart5Grid Project. (2021). Smart5Grid - Automated 5G Networks and Services for Smart Grids. Available at: https://www.cisuc.uc.pt/en/projects/smart5grid-automated-5g-networks-and-services-for-smart-grids

Ghosh, S. and Ugwuanyi, E. and Dagiuklas, T. and Iqbal, M. (2019) “BlueArch–An Implementation of 5G Testbed,” Journal of Communications vol. 14, no. 12, pp. 1110-1118, 2019. DOI.: 10.12720/jcm.14.12.1110-1118

Salazar, Z. and Nghia, H. and Mallouli, W. and  Cavalli, A. and Montes de Oca, E. (2021) 5Greplay: a 5G Network Traffic Fuzzer - Application to Attack Injection. In Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 21). Association for Computing Machinery, New York, NY, USA, Article 106, 1–8. https://doi.org/10.1145/3465481.3470079

Sousa, B. and Arieiro, M. and Pereira, V. and Correia, J. and Lourenço, N. and Cruz, T. (2021) ELEGANT: Security of Critical Infrastructures With Digital Twins, in IEEE Access, vol. 9, pp. 107574-107588, 2021, doi: 10.1109/ACCESS.2021.3100708

SUSE Rancher. (2022). Rancher Server v2.6.  Available at: https://rancher.com/docs/rancher/v2.6/en/

SUSE Rancher. (2023). Rancher’s next-generation kubernetes distribution. Available at: https://docs.rke2.io/

Tcpdump Group. (2023). TCPDUMP Official Website. Available at: https://www.tcpdump.org/

Team Celona. (2020). 5G LAN: What Is It & Why Will It Matter?  Available at: https://www.celona.io/5g-lan/5g-lan

Tikhvinskiy, V. and Koval, V. (2020). Architecture 5G base station gNB. Available at: https://www.researchgate.net/figure/Architecture-5G-base-station-gNB_fig5_339059845

Witte Software. (2023). Modbus Poll Official Website. Available at: https://www.modbustools.com/modbus_poll.html