

# Network Slicing in the IIoT Era: Architectures, Blueprints, and Tooling Ecosystem

Engin Zeydan<sup>‡</sup>, Yekta Turk<sup>†</sup>, Tharaka Hewa<sup>¶</sup>, Madhusanka Liyanage<sup>\*</sup>, Abdullah Aydeger<sup>§</sup>,  
Francisc Wilhelmi Roca<sup>||</sup> Luis Blanco<sup>‡</sup>

<sup>‡</sup>Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Spain,

<sup>†</sup>Aselsan Corp. Istanbul, Turkiye, 34396,

<sup>¶</sup>CWC, University of Oulu, Finland

<sup>\*</sup>Network Softwarization and Security Labs (NetsLab), School of Computer Science, University College Dublin, Ireland,

<sup>§</sup>Dept. of Electrical Engineering and Computer Science, Florida Institute of Technology, Melbourne, USA,

<sup>||</sup> Universitat Pompeu Fabra (UPF), Spain

Email: <sup>‡</sup>engin.zeydan@cttc.cat, <sup>†</sup>yekta.turk@gmail.com, <sup>¶</sup>tharaka.Hewa@oulu.fi, <sup>\*</sup>madhusanka@ucd.ie,

<sup>§</sup>aaydeger@fit.edu, <sup>||</sup>francisco.wilhelmi@upf.edu <sup>‡</sup>luis.blanco@cttc.cat

**Abstract**—Industrial Internet of Things (IIoT) applications demand deterministic communication with high reliability, low latency, and adaptability to dynamic workloads. Network slicing, a key enabler in 5G and beyond, offers the potential to meet these stringent requirements by creating logically isolated and customized network partitions. This paper presents a comprehensive study on the design and realization of network slicing tailored for IIoT systems. Our aim is to bridge the gap between standards-driven network slicing concepts and their practical application in industrial automation networks. First, we analyze both core and radio access network (RAN) perspectives, emphasizing slice-specific architectural considerations and mapping them to 3GPP standards. Then, we propose a blueprint-based design approach for edge-centric slice deployment and present a catalogue of lightweight, standardised slice profiles derived from 3GPP specifications and testbed experiences in the literature. In addition, we survey an array of open-source and commercial tools used for slice provisioning, orchestration, and monitoring.

**Index Terms**—IIoT, slice blueprint, tooling, network slicing.

## I. INTRODUCTION

The emergence of the Industrial Internet of Things (IIoT) has redefined communication requirements in industrial environments, pushing networks to support ultra-reliable, low-latency, and scalable connectivity for a broad range of applications [1]. From robotic control and automated guided vehicles (AGVs) to sensor telemetry and visual inspection, IIoT workloads demand deterministic service quality, strict isolation, and dynamic reconfigurability, characteristics not easily supported by traditional monolithic network architectures [2], [3]. Network slicing, a core feature introduced in 5G and further enhanced in 5G-Advanced and prospective 6G systems, offers a means to partition physical infrastructure into multiple logically isolated and service-tailored virtual networks [4]. Each slice can be designed and optimized according to a specific application class, such as ultra-Reliable Low-Latency Communication (uRLLC), enhanced Mobile Broadband (eMBB), or massive Machine-Type Communications (mMTC), as formalized in 3GPP TS 23.501 [5]. By enabling dedicated control and user planes for each service category,

network slicing facilitates fine-grained orchestration of network resources and Quality of Service (QoS) guarantees, capabilities that are particularly relevant for mission-critical IIoT applications.

Established industrial communication protocols such as Ethernet Time Sensitive Network (TSN), ProfiNET and EtherCAT offer deterministic latency and reliability, but are often restricted to rigid topologies, have limited scalability and are not flexible enough to dynamically adapt to heterogeneous workloads. In addition, these technologies typically require specialised hardware and a high level of reconfiguration effort to accommodate changes to production lines or operational requirements. In contrast, B5G network slicing introduces a software-defined paradigm that enables the dynamic, on-demand provisioning of logically isolated virtual networks, each tailored to specific application requirements. This enables scalable, flexible and secure connectivity across different IIoT devices and factory zones, reducing operational complexity while meeting stringent performance guarantees [6].

This paper explores the design and deployment of network slicing architectures tailored to IIoT scenarios, covering both core network and Radio Access Network (RAN) domains [7]. It presents a catalog of lightweight slice blueprint configurations, aligned with 3GPP guidelines, and adapted to specific industrial tasks with diverse latency, bandwidth, and reliability requirements. In addition, the paper surveys a comprehensive set of tools and platforms, ranging from open-source orchestrators to commercial SDN/NFV solutions, used for slice lifecycle management, automation, and monitoring [8].

While the existing literature has addressed network slicing in general, few papers have focused on specific blueprint realizations for the IIoT or analysed the gaps in deploying these solutions in environments constrained by legacy systems, safety certifications (e.g. IEC 61508, IEC 62443) and deterministic control cycles. For this reason, the study also critically examines deployment challenges, including protocol heterogeneity, latency limits and integration overhead, and proposes standards-based mitigation strategies. Ultimately, this study

aims to provide a reference framework for IIoT stakeholders to enable systematic blueprint selection, slice orchestration and deployment in edge-centric industrial environments. The analysis are particularly relevant for network architects and industrial system integrators looking to harmonise 5G capabilities with Operational Technology (OT) requirements.

## II. NETWORK SLICING FOR IIoT

We introduce the integration of network slicing concept into IIoT devices. Network slicing is an approach that is commonly utilized to facilitate IIoT network solutions [9]. It allows for the creation of distinct and isolated logical networks on a shared infrastructure [10]. Network slicing is critical to the IIoT because it enables the creation of multiple virtual networks within a single physical infrastructure, each optimized for the specific bandwidth, latency, security and reliability requirements of applications. This technology increases operational flexibility and security and supports various IIoT applications with tailored network resources, improving system efficiency and reducing costs. Network slicing serves various purposes: (i) Segregating different security zones within a factory environment [11], [12]. (ii) Separating different service categories, such as isolating critical communication from non-critical communication [13]. (iii) Establishing a non-public IIoT network on a public network infrastructure that is concurrently employed for public mobile communication [14].

### A. Dynamic Network Slicing: A Core Network Perspective

At the heart of dynamic network slicing are the Core Slice Management Function (CSMF), the Network Slice Subnet Management Function (NSSMF) and the Network Slice Selection Function (NSMF). These components play a critical role in orchestrating and managing the slices, ensuring efficient resource allocation and delivering exceptional QoS. The CSMF plays a crucial role in coordinating the entire lifecycle of network slices. It configures them to meet the specific operational requirements of the industry, manages resource allocation efficiently and provides continuous monitoring to ensure that each slice performs optimally under different conditions. This is crucial for processes where timing and data integrity are critical, such as automated production lines or robotic control systems. The NSMF is responsible for selecting the most appropriate network slice for a particular industrial application or device, optimizing network performance to increase throughput and reliability, and improving overall operational efficiency. This function is critical in environments where multiple types of industrial applications run concurrently and require different network capabilities.

The NSSMF manages the individual subnets within each network slice, ensuring efficient resource allocation that can be quickly adapted to the requirements of individual applications. This flexibility is critical in industrial environments where production requirements can change rapidly and network resources need to be reallocated instantly without affecting other operations within the network [15]. Together, these features enable dynamic network slicing to effectively support

a wide range of industrial applications, from IoT device management to complex machine-to-machine communication and cloud robotics. By dynamically allocating and managing network resources, dynamic network slicing helps to minimize operational disruptions and improve the adaptability of network infrastructures to changing industrial requirements. Furthermore, dynamic network slicing underpins the shift towards Slice as a Service (SaaS) models in industry [16], revolutionizing the way network resources are customized and used to drive innovation and efficiency in industrial operations. This capability allows industry to scale its network functions up or down as needed in real time and provides a more flexible and cost-effective approach to managing networked operations.

### B. Networking Slicing for RAN Domain

Network slicing in the RAN area plays a crucial role in supporting the diverse and demanding communication requirements of industrial automation. From an industrial RAN management perspective, network slicing enables the segregation of communications for critical machine operations from less critical IoT monitoring traffic, improving both reliability and efficiency. This segregation is critical in environments where precision and uptime are paramount, such as automated manufacturing and process control systems. For example, without separation, bulk video streams or MQTT sensor floods could delay or drop mission-critical messages. Factors such as real-time production requirements, machine-to-machine communication requirements and data prioritization for critical control signals are taken into account to ensure network resources are optimized for maximum industrial performance. In addition, network slicing in the RAN area requires careful orchestration and automation of network components such as routers, switches and base stations. This orchestration is not just about managing traffic, but also about configuring the network for the high reliability and low latency required for operations such as robotic automation and real-time defect detection in manufacturing processes. Legacy wired technologies (like 4–20 mA, Profibus, etc.) have benefits such as ultra-stable, low-noise signaling, intrinsic safety in hazardous areas and mature technologies. However, they cannot support mobility, fast reconfiguration, or rich data (e.g., video, XR), all essential for modern dynamic manufacturing needs in Industry 4.0/5.0.

According to the GSMA definition, a network slice is an independent end-to-end logical network that runs on a shared physical infrastructure and is capable of providing a negotiated QoS [17]. In an industrial environment, this means that each network slice can be tailored to support specific facets of industrial operations, from telemetry data collection to high-speed automation control, each with its own performance characteristics and security protocols. In addition to this general definition, there are various implementations that are often meant when network slicing is mentioned. The best-known definition for the 5G core specification in [18], is a logical network that provides specific network capabilities and network characteristics and comprises the core network

ID	Use Case	Slice Type	SST/SD (3GPP)	5QI	Rel.	Latency	Scheduler	Deployment	Edge Resources	Notes
BP-URLLC-01	Robotic arm control	URLLC	SST=2 (URLLC), SD=01	85	99.999%	≤1ms	Short DRX, PDCCH boost	On-prem 5G SA	≤2 vCores, 512MB RAM, RAN slice	Latency-critical, periodic task control. Derived from Table 5.7.4-1, TS 23.501.
BP-mMTC-01	Temp. sensor grid	mMTC	SST=3 (mMTC), SD=03	72	95.0%	≤500ms	RRC idle opt.	Edge NPN	10K UEs, low CPU, shared RAN	Sparse, energy-efficient uplink bursts. Uses standard mMTC profile.
BP-eMBB-01	UHD inspection video	eMBB	SST=1 (eMBB), SD=02	9	99.0%	≤20ms	Long DRX, uplink-opt.	MEC-assisted NPN	≥200 Mbps, 1GB RAM	Bandwidth-heavy, jitter-tolerant video. Matches eMBB 5QI mapping.
BP-URLLC-02	AGV coordination	URLLC	SST=2 (URLLC), SD=04	84	99.999%	≤5ms	Tight HARQ, QoS-aware	Dual-slice on-prem	4 vCores, det. resource map	Fast mobility sync, critical ops. Refers to URLLC AGV profile.
BP-mMTC-02	Maint. sensors	mMTC	SST=3 (mMTC), SD=05	74	97.0%	≤300ms	DRX cycling, long IDLE	Standalone NPN	1K+ UEs, small cache	Event-based, delay-tolerant signals. Matches 5QI 74 spec.
BP-HYBRID-01	XR + control loop	Hybrid	SST=1+2 (Hybrid), SD=07	90	99.99%	≤10ms	ML-guided composite	Federated edge/core	Dynamic CPU, hybrid DRX+URLLC	Interactive, human-in-loop workload. Custom scheduler profile.
BP-eMBB-02	Factory floor stream	eMBB	SST=1 (eMBB), SD=06	7	98.0%	≤30ms	Uplink-priority PDU	5GC + Edge CDN	50 Mbps uplink / UE	Multi-camera real-time broadcast. Uses 5QI 7 for video UL.

TABLE I: Lightweight Slice Blueprint Catalog for Edge-Centric Industrial Deployments

- **SST**: Slice/Service Type, 1: eMBB, 2: URLLC, 3: mMTC (3GPP TS 23.501 §5.15.2.2).
- **SD**: Slice Differentiator, Distinguishes slices under the same SST category.
- **5QI**: 5G QoS Identifier, Maps to latency, reliability, and packet loss KPIs.
- **DRX**: Discontinuous Reception, UE power-saving mechanism.
- **HARQ**: Hybrid Automatic Repeat reQuest, Combines FEC and retransmissions for reliability.
- **PDCCH**: Physical Downlink Control Channel, Carries scheduling and control messages.
- **RRC**: Radio Resource Control, Controls signaling and connection states in RAN.
- **NPN**: Non-Public Network, Private 5G deployment for enterprise/industrial use.
- **MEC**: Multi-access Edge Computing, Brings computation closer to the edge to reduce latency.

and the network functions of the user plane. Methods that at least partially implement the above definition are not limited to next-generation mobile networks, but are also available in previous-generation mobile networks.

### III. NETWORK SLICE BLUEPRINT AND COMPARISONS

#### A. Slice Blueprint Examples

Table I contains a catalogue of blueprint configurations for different classes of 5G network slices aimed at industrial edge deployments, e.g. in smart factories, warehouses and automation plants. The table contains various considerations.

- **Blueprint Use Case Mapping**: Use cases (e.g., robotic control, AGV, video uplink) have categorized IIoT applications by their latency/reliability/data needs.
- **5G Slice Design Parameters**: Each slice blueprint includes a 5QI value, reliability level, and latency budget based on 3GPP TS 23.501 (Table 5.7.4-1) and TS 28.531. For example: 5QI 85 for URLLC (robotic control), 5QI 7 for uplink-heavy eMBB, and 5QI 72/74 for mMTC use cases. Slice/Service Type (SST) and Slice Differentiator (SD) values are standardized according to 3GPP TS 23.501 §5.15.2.2, where SST = 1 (eMBB), SST = 2 (URLLC), and SST = 3 (mMTC). The Slice Differentiator (SD) provides additional distinction between multiple slices of the same service type.

- **Management and Lifecycle Considerations**: Scheduling behaviors such as DRX tuning, HARQ strictness, and QoS-aware prioritization aligns with [19] and the slice-level parameters defined in 3GPP TS 28.531 and TR 28.824.
- **Deployment Topologies**: Deployment patterns (e.g., on-prem 5G SA, federated MEC, standalone NPN) are deployment modes for private 5G and industrial testbeds (see [19] and Section II.D). Examples such as “Edge CDN + 5GC” or “Dual-slice on-prem” are common IIoT architectures used in 5G-VINNI and Imagine-B5G testbeds.
- **Resource Envelopes**: Minimal resource allocations (e.g., CPU ≤ 2 vCores, uplink throughput, number of UEs) were estimated using (i) capacity assumptions from testbeds (Section 6.1 and Table 4 in [19]), (ii) 5G-ACIA and 5G-ERA slice resource patterns.

In conclusion, instead of dynamic per-slice optimization, predefined blueprints support fast instantiation, risk isolation, and deterministic performance in edge-limited industrial deployments. URLLC slices require more CPU and deterministic scheduling, but can operate on limited bandwidth, mMTC slices tolerate latency and jitter but must support high UE density and energy-efficiency. Hybrid slices (e.g., XR + control), on the other hand, must bridge both tight latency and high data rates. These blueprints can be implemented with slice managers such as (i) The custom slice manager PoCs such as

in [19]. (ii) Commercial slice orchestrators (e.g., Nokia NaC [20], 5Growth-VS [21]).

Note that the hybrid slice entry (SST = 1+2) in Table I represents a conceptual extension rather than a formally defined combination in current 3GPP specifications. Emerging IIoT and XR+control scenarios often require simultaneous support for low-latency control traffic and high-throughput media streams. These are currently managed either by provisioning multiple concurrent slices or through composite application-layer logic. The blueprint entry labeled SST=1+2 reflects such a hybrid application demand, not a native 3GPP-defined slice type. Future slicing frameworks may formalize such hybrid classes through slice orchestration or nested slice composition.

### B. Comparison with Deterministic Industrial Protocols

While 5G network slicing introduces unprecedented flexibility in creating isolated, performance-tailored virtual networks, it must be contextualized alongside existing deterministic communication solutions in industrial settings. Technologies such as TSN, OPC-UA with TSN extensions, and DDS provide bounded latency, jitter control, and real-time guarantees, crucial for closed-loop control and safety-critical operations. However, these protocols are often restricted to wired environments, lack dynamic reconfigurability, and require strict topological planning. In contrast, network slicing allows dynamic lifecycle management, mobility support, and end-to-end resource abstraction across both the core and RAN. Furthermore, slicing supports multi-tenancy and service multiplexing on shared infrastructure, enabling integration of critical and non-critical services with diverse QoS needs. Therefore, slicing does not aim to replace TSN or DDS but can serve as a complementary layer, especially in brownfield environments where backward compatibility and wireless flexibility are needed.

### C. Roadmap Considerations

Beyond the implementation of blueprints in open-source testbeds such as OpenAirInterface and ETSI OpenSlice, a broader roadmap is needed to facilitate the widespread adoption of IIoT slicing. This includes: (i) integration with industrial-grade platforms that support real-time operational requirements, such as Siemens Industrial Edge or Rockwell FactoryTalk; (ii) establishing reference certification frameworks that align slicing behavior with standards like IEC 62443 (security) and IEC 61508 (functional safety); (iii) developing vendor-neutral APIs and interoperability test suites to allow seamless coordination between public networks and private 5G non-public networks (NPNs); and (iv) initiating collaborative pilots with industrial partners to trial blueprint instantiations in real factory floors with measurable KPIs. These steps will help transition slicing from proof-of-concept toward operational-grade deployment in production environments.

### D. Cost-Benefit Considerations

From a deployment perspective, network slicing introduces overhead in terms of orchestration complexity, compute resource requirements, and slice lifecycle management.

Compared to traditional isolation approaches like VLAN-based segmentation or dedicated Access Point Names (APNs), slicing requires a more sophisticated control plane (e.g., NSMF/NSSMF) and a runtime capable of managing dynamic QoS guarantees across virtualized infrastructure. However, the benefits often outweigh the costs in industrial settings. Unlike VLANs or APNs, which provide coarse-grained separation without QoS enforcement, slices can be customized per service class (e.g., URLLC vs. mMTC), support mobility, and offer programmable APIs for dynamic instantiation. Moreover, slicing enables better resource consolidation and multitenancy on shared 5G infrastructure, reducing the need for dedicated hardware and simplifying upgrades.

## IV. TOOLS FOR NETWORK SLICING

Some advanced software and hardware tools that enable the creation and management of logical networks are:

- 1) Network management software such as Cisco Prime Infrastructure, SolarWinds Network Performance Monitor and PRTG Network Monitor, which enable centralized control and monitoring of network devices and performance. In industrial settings, these tools help maintain critical network performance and efficiently manage large numbers of IoT devices.
- 2) Network virtualization software such as VMware NSX and Microsoft Hyper-V that enables the creation of virtual networks that can be easily deployed, configured and managed. These are essential to create isolated network slices that can be used without physical changes to the network for various industrial applications, from assembly lines to robotic automation.
- 3) Network automation tools such as Ansible and Puppet, Chef, SaltStack, Cisco ACI, Juniper Networks Junos and Arista Networks EO that automate network configuration, orchestration and management, reducing the time and effort required to deploy and maintain networks for handling various production processes.
- 4) Software Defined Networking (SDN) controllers such as OpenDayLight and VMware NSX, which enable centralized control of network traffic and the implementation of advanced network security policies [33], [34]. Sophisticated network security policies and traffic segmentation are crucial for protecting sensitive industrial data and ensuring the reliable operation of critical industrial controls.
- 5) Hardware switches and routers with advanced features, such as high-performance processing, advanced security features, and support for SDN. They can cope with the high data throughput and connectivity requirements of modern industrial operations and ensure that the network slices perform optimally under different load conditions.
- 6) Network monitoring tools such as Wireshark and Packet Capture that provide real-time insight into network traffic and help identify and resolve network performance issues. They are an important capability for industrial networks to preemptively identify and resolve problems that could lead to downtime or inefficiencies in automated processes.

TABLE II: Slicing-Relevant Tools

Usage Area	Tool	Description	Open Source	Key Features
SDN Controller	OpenDaylight [22]	Modular SDN controller enabling programmable flow-based slicing.	Yes	Multi-vendor, extensible architecture
SDN Controller	VMware NSX [23]	Micro-segmentation and slice-aware virtual networks.	No	Policy-driven automation, VMware integration
Network Automation	Cisco ACI [24]	Centralized automation for slice lifecycle in data center fabric.	No	Policy abstraction, fabric control
Network Automation	Juniper Junos [25]	Automation via commit-rollback and telemetry-based workflows.	No	Single OS, programmable CLI
Network Automation	Arista EOS [26]	Slice-aligned container isolation with extensible APIs.	No	Fault isolation, cloud-native APIs

TABLE III: General Network and Monitoring Tools

Usage Area	Tool	Description	Open Source	Key Features
Monitoring	Wireshark [27]	Protocol analyzer for verifying slice QoS/QCI performance.	Yes	Packet-level inspection, filtering
Monitoring	PRTG [28]	Health monitoring and alerting across slice network nodes.	No	Custom dashboards, SNMP support
Automation	Ansible [29]	Agentless orchestration for NSMF/NSSF configuration.	Yes	YAML templates, REST support
Automation	Puppet [30]	Declarative infra provisioning for slice VNFs.	Yes	Configuration consistency, scalability
Cloud Mgmt	AWS CloudFormation [31]	Template-driven IaC for 5G slicing in AWS.	No	Drift detection, YAML/JSON stacks
Cloud Mgmt	Azure Resource Manager [32]	Group-based cloud slice deployments.	No	Resource templates, API-based provisioning

7) Cloud management platforms, such as AWS CloudFormation, Azure Resource Manager, Google Cloud Deployment Manager, and Oracle Cloud Resource Manager which provide a centralized platform for managing and provisioning virtual networks in the cloud. This flexibility supports the deployment of network slices in cloud environments and optimizes operations such as data analytics, storage solutions and more across multiple industry sites.

Tables II and III offer a categorized overview of toolsets relevant to the deployment, orchestration, and monitoring of network slicing in industrial 5G environments. These tools are broadly divided into slicing-relevant platforms and general-purpose network support tools, with attention to both proprietary and open-source solutions. Table II lists core slicing-enabling solutions that offer direct support for slice abstraction, automation, and control. In contrast, Table III highlights tools used for broader support in monitoring, automation, and resource management, which although not exclusive to slicing, are frequently integrated into slice lifecycle management. An application-driven evaluation is critical for aligning tool capabilities with the stringent needs of IIoT slice types. For instance, URLLC slices, with sub-millisecond latency and ultra-high reliability requirements, benefit from tools that offer low-latency orchestration (e.g., Cisco ACI for deterministic policy enforcement) and tight resource isolation (e.g., VMware NSX for micro-segmentation). Tools like OpenDaylight can support slice-level flow steering and limited DRX configuration via programmable SDN controllers, although they require integration with RAN-specific orchestrators to enable fine-tuning. Slice differentiation across the RAN domain is best supported by commercial platforms like Nokia NaC and Juniper Junos, which can provision differentiated scheduling profiles at the

radio level via vendor-specific extensions. However, these tools vary significantly in openness, scalability, and compliance with 3GPP-defined slice attributes (e.g., SST/SD, 5QI). Future benchmarking efforts should systematically evaluate these tools against IIoT-specific KPIs such as jitter, control loop stability, and deployment overhead across URLLC, mMTC, and hybrid slice scenarios.

## V. CONCLUSIONS AND FUTURE WORK

This paper has examined the applicability of 5G network slicing for Industrial Internet of Things (IIoT) environments by analyzing slicing requirements across the core and RAN domains, and proposing a detailed set of blueprint configurations tailored to typical industrial scenarios. The proposed blueprints, grounded in 3GPP specifications such as TS 23.501 and TS 28.531, demonstrate how differentiated service types (e.g., URLLC, mMTC, eMBB) can be mapped to real-time industrial tasks such as robotic control, automated video inspection, and sensor grid telemetry. We further reviewed a range of orchestration and monitoring tools, identifying their relevance, interoperability, and limitations for IIoT slicing deployments. While comprehensive, these tools often lack deterministic guarantees or certified integration paths for industrial-grade operations, especially in settings that must comply with safety and security standards such as IEC 61508 or IEC 62443 [35].

The proposed slice blueprints have not yet been validated through testbed deployments or simulation studies. Future work will focus on instantiating selected blueprints in real-world edge testbeds using open-source platforms such as OpenAirInterface, Open5GS [36], and ETSI OpenSlice. This will enable empirical evaluation of key metrics such as latency compliance, reliability under load, and resource elasticity.

Additionally, integration with industrial control standards (e.g., IEC 61508 for functional safety [37], OPC-UA with TSN for real-time communication) will be explored in collaboration with automation vendors to assess interoperability and certification. These steps are critical to transitioning blueprint-based network slicing from conceptual design to trusted industrial deployment.

#### ACKNOWLEDGEMENT

This work is partly supported by the CONFIDENTIAL-6G project (Grant ID. 101096435) funded by the European Commission, the Ensure-6G project (Grant ID. 101182933) funded by the European Commission, the CONNECT phase 2 (Grant no. 13/RC/2077\_P2) project funded by the Research Ireland, UNITY-6G project, funded from European Union's Horizon Europe Smart Networks and Services Joint Undertaking (SNS JU) research and innovation programme under the Grant Agreement No 101192650.

#### REFERENCES

- [1] T. Zhang, C. Xue, J. Wang, Z. Yun, N. Lin, and S. Han, "A survey on industrial internet of things (iiot) testbeds for connectivity research," *arXiv preprint arXiv:2404.17485*, 2024.
- [2] T. Wang, D. Li, B. Zhang, X. Liu, and W. Shang, "Resilient topology re-configuration for industrial internet of things: A feature-driven approach against heterogeneous attacks," *Entropy*, vol. 27, no. 5, p. 503, 2025.
- [3] A. Aydeger, E. Zeydan, L. Blanco, J. Mangues, T. Hewa, and M. Liyanage, "Identity management for enhanced security in industrial automation and control systems," in *2025 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. IEEE, 2025, pp. 217–222.
- [4] J. Ordóñez-Lucena, P. Ameigeiras, L. M. Contreras, J. Folgueira, and D. R. López, "On the rollout of network slicing in carrier networks: A technology radar," *Sensors*, vol. 21, no. 23, p. 8094, 2021.
- [5] 3rd Generation Partnership Project (3GPP), "System architecture for the 5g system (5gs); stage 2," 3GPP, Technical Specification TS 23.501 V19.4.0, Jun. 2025, release 19, Accessed: 28 June 2025. [Online]. Available: [https://www.3gpp.org/ftp/Specs/archive/23\\_series/23.501/23501-1940.zip](https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/23501-1940.zip)
- [6] A. Aydeger, N. Saputro, and K. Akkaya, "Cloud-based deception against network reconnaissance attacks using sdn and nfv," in *2020 IEEE 45th Conference on Local Computer Networks (LCN)*. IEEE, 2020, pp. 279–285.
- [7] A. Aydeger, E. Zeydan, and J. Mangues, "Post-quantum cryptography integration to o-ran," in *2025 IEEE 22nd Consumer Communications & Networking Conference (CCNC)*. IEEE, 2025, pp. 1–2.
- [8] A. Aydeger, N. Saputro, and K. Akkaya, "Utilizing nfv for effective moving target defense against link flooding reconnaissance attacks," in *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*. IEEE, 2018, pp. 946–951.
- [9] T. Umagiliya, S. Wijethilaka, C. De Alwis, P. Poramage, and M. Liyanage, "Network Slicing Strategies for Smart Industry Applications," in *2021 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 2021, pp. 30–35.
- [10] S. Zhang, "An overview of network slicing for 5G," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 111–117, 2019.
- [11] C. De Alwis *et al.*, "A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions," *IEEE Communications Surveys & Tutorials*, 2023.
- [12] Y. Wu *et al.*, "A survey of intelligent network slicing management for industrial IoT: Integrated approaches for smart transportation, smart energy, and smart factory," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1175–1211, 2022.
- [13] C. Bektas *et al.*, "Reliable Software-defined RAN Network Slicing for Mission-Critical 5G Communication Networks," in *2019 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2019, pp. 1–6.
- [14] S. Wijethilaka and M. Liyanage, "Survey on network slicing for internet of things realization in 5G networks," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 957–994, 2021.
- [15] X. Li, D. Li, J. Wan, A. V. Vasilakos, C.-F. Lai, and S. Wang, "A review of industrial wireless networks in the context of industry 4.0," *Wireless networks*, vol. 23, no. 1, pp. 23–41, 2017.
- [16] T. O. Atalay, D. Stojadinovic, A. Famili, A. Stavrou, and H. Wang, "Network-slice-as-a-service deployment cost assessment in an end-to-end 5g testbed," in *GLOBECOM 2022-2022 IEEE Global Communications Conference*. IEEE, 2022, pp. 2056–2061.
- [17] GSMA, "An Introduction to Network Slicing, (White Paper)," <https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf>, 2017, [Online; accessed January-2023].
- [18] 3GPP, "System Architecture for the 5G System; Stage 2 (Release 15)," TS 23.501, 2018.
- [19] A. Perdigão, J. Quevedo, and R. L. Aguiar, "Automating 5g network slice management for industrial applications," *Computer Communications*, vol. 229, p. 107991, 2025.
- [20] Nokia Corporation, "Network as Code Partner Program," <https://www.nokia.com/programmable-networks/network-as-code/partner-program/>, 2025, accessed: 2025-06-01.
- [21] 5GROWTH Project, "5GROWTH Vertical Slicer (5Gr-VS)," <https://github.com/5growth/5gr-vs>, 2025, accessed: 2025-06-01.
- [22] The Linux Foundation, "OpenDaylight: Open Source SDN Controller," <https://www.opendaylight.org/>, 2025, accessed: 2025-06-01.
- [23] VMware, Inc., "VMware NSX – Networking and Security Virtualization," <https://www.vmware.com/products/cloud-infrastructure/nsx>, 2025, accessed: 2025-06-01.
- [24] Cisco Systems, Inc., "Cisco Application Centric Infrastructure (ACI)," <https://www.cisco.com/site/us/en/products/networking/cloud-networking/application-centric-infrastructure/index.html>, 2025, accessed: 2025-06-01.
- [25] Juniper Networks, "Junos OS – Network Operating System," <https://www.juniper.net/us/en/products/network-operating-system/junos-os.html>, 2025, accessed: 2025-06-01.
- [26] Arista Networks, "Arista EOS® – Cloud Network Operating System," <https://www.arista.com/en/products/eos>, 2025, accessed: 2025-06-01.
- [27] Wireshark Foundation, "Wireshark: The World's Leading Network Protocol Analyzer," <https://www.wireshark.org/>, 2025, accessed: 2025-06-01.
- [28] Paessler AG, "PRTG Network Monitor," <https://www.paessler.com/prtg>, 2025, accessed: 2025-06-01.
- [29] Ansible Community, "Ansible: Radically Simple IT Automation," <https://github.com/ansible/ansible>, 2025, accessed: 2025-06-01.
- [30] Performer Software, "Puppet: Infrastructure Automation & Operations at Scale," <https://www.puppet.com/>, 2025, accessed: 2025-06-01.
- [31] Amazon Web Services, "AWS CloudFormation – Infrastructure as Code," <https://aws.amazon.com/cloudformation/>, 2025, accessed: 2025-06-01.
- [32] Microsoft Azure, "Azure Resource Manager – Manage and Visualize Resources," <https://azure.microsoft.com/en-us/get-started/azure-portal/resource-manager>, 2025, accessed: 2025-06-01.
- [33] A. Aydeger, N. Saputro, K. Akkaya, and S. Uluagac, "Assessing the overhead of authentication during sdn-enabled restoration of smart grid inter-substation communications," in *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2018, pp. 1–6.
- [34] A. Aydeger, K. Akkaya, and A. S. Uluagac, "Sdn-based resilience for smart grid communications," in *2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN)*. IEEE, 2015, pp. 31–33.
- [35] A. Aydeger, N. Saputro, K. Akkaya, and S. Uluagac, "Sdn-enabled recovery for smart grid teleprotection applications in post-disaster scenarios," *Journal of Network and Computer Applications*, vol. 138, pp. 39–50, 2019.
- [36] S. Hoque, A. Aydeger, and E. Zeydan, "Post-quantum secure ue-to-ue communications," in *2024 15th International Conference on Network of the Future (NoF)*. IEEE, 2024, pp. 28–30.
- [37] A. Aydeger, K. Akkaya, M. H. Cintuglu, A. S. Uluagac, and O. Mohammed, "Software defined networking for resilient communications in smart grid active distribution networks," in *2016 IEEE International Conference on Communications (ICC)*. IEEE, 2016, pp. 1–6.