

Network Slicing for Industrial Automated Services

Engin Zeydan[‡], Yekta Turk[†], Tharaka Hewa[¶], Madhusanka Liyanage^{*}, Abdullah Aydeger[§],

Francesc Wilhelmi Roca^{||} Luis Blanco[‡]

[‡]Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Spain,

[†]Aselsan Corp. Istanbul, Turkiye, 34396,

[¶]CWC, University of Oulu, Finland

^{*}Network Softwarization and Security Labs (NetsLab), School of Computer Science, University College Dublin, Ireland,

[§]Dept. of Electrical Engineering and Computer Science, Florida Institute of Technology, Melbourne, USA,

^{||} Universitat Pompeu Fabra (UPF), Spain

Email: [‡]engin.zeydan@cttc.cat, [†]yekta.turk@gmail.com, [¶]tharaka.Hewa@oulu.fi, ^{*}madhusanka@ucd.ie,

[§]aaydeger@fit.edu, ^{||}francisco.wilhelmi@upf.edu [‡]luis.blanco@cttc.cat

Abstract—With the advent of Industry 4.0, the need for advanced network architectures capable of supporting diverse, latency-sensitive, and safety-critical applications has intensified. Network slicing, a central enabler in 5G and beyond, offers the ability to create multiple logically isolated network instances tailored to specific industrial use cases. In this paper, we analyse the suitability and limitations of network slicing in the context of Industrial Internet of Things (IIoT) environments, especially in the area of smart manufacturing and process automation. In addition to design considerations, we critically analyse deployment challenges such as legacy system integration, safety certification (IEC 61508/62443), orchestration overhead and latency determinism. Real-world insights from EU testbeds (5G-VINNI, 5G-ERA) and industry pilots (5G-ACIA) are integrated to show practical gaps between theory and practise. We also consider when slicing is justified over simpler alternatives such as static QoS provisioning or time sensitive network overlays.

Index Terms—Network Slicing, Industry Automation, Network Services.

I. INTRODUCTION

Network slicing is a novel conceptual approach to the design and implementation of service provider networks in the context of Industry 4.0 and Industry 5.0. Instead of the traditional view of a single, all-encompassing network that performs different functions, advanced technologies such as virtualization and Software Defined Networking (SDN) enable the creation of logical networks built on a common infrastructure. This enables greater flexibility, scalability and customizability in the provision of network services tailored to specific requirements [1], [2]. In industrial settings, network slicing is particularly advantageous for segmenting network architecture to support varied operational technologies and communication demands, ranging from real-time machine control systems to large-scale data aggregation and analytics. Each network slice is designed to serve specific business functions or operational requirements within industrial environments, facilitating optimized performance and resource allocation [3]. These slices are fully functional networks that can independently manage, maintain, and secure their operations from end to end [4]. For instance, one slice might be dedicated to handling sensitive control signals for machinery with stringent latency and reliability requirements, while another might manage routine data collection tasks that demand higher bandwidth but are

less sensitive to delays. This separation ensures that critical control functions remain unaffected by fluctuations in the less critical data traffic. Moreover, the integration of network management and operational support systems within each slice allows for autonomous, yet harmonized operations across the industrial spectrum. The flexibility of network slicing enables not only the inclusion of both stationary and mobile network components but also supports the adaptation of network functions, resource assignments, and integrations with third-party services [5], [6].

Federated network slicing extends these capabilities by enabling slices to span across multiple physical network infrastructures, thus offering a robust solution for industries that operate on a global scale. This can be particularly useful for multinational industrial operations that require consistent service levels across different geographic regions [7]. In practical terms, network slices can be designed to include specific components like a dedicated core network control plane and user plane network functions, which are essential for maintaining high-performance standards required in automated and smart manufacturing processes. Network slices support negotiated Quality of Service (QoS) or specific service capabilities that form Service Level Agreements (SLAs). These are critical to meeting the exact requirements of industrial applications [8]. Resources, whether physical or logical, can be assigned to a specific slice as separate instances, or they can be shared by multiple slices [9]. Note also that these resources do not necessarily come only from the provider's network. Some resources can also be used by other providers (e.g. using federation capabilities [10]), to enable functions such as aggregation and roaming. Authors in [11] focus on automation, slice lifecycle, standards-based design (CSMF, NSMF, NSSMF), Proof-of-Concept (PoC), and a digital twin architecture for slice management. Ultimately, in an industrial automation context, network slicing not only enhances the efficiency and flexibility of network resource utilization but also boosts security and reliability by isolating critical operations [12]. This isolation helps mitigate risks associated with network failures and cyber threats, ensuring continuous and secure operations across the factory floor.

II. NETWORK SLICING DESIGN FOR IIOT

The development of Industrial Internet of Things (IIoT) systems requires careful consideration to ensure that they are robust, efficient and secure for industrial use. Key criteria to consider are high reliability, scalability, stringent security, real-time data processing, energy efficiency, interoperability and durability, while maintaining cost efficiency to optimize industrial processes and improve productivity. Network slices are composed of different types of resources [13]. These resources can include physical industry assets that can be allocated or profiled for a particular slice, and in some cases, dedicated physical industry resources can be assigned as needed. The slices also consist of logical units such as configured network functions, management functions, Virtual Private Networks (VPNs) and more. Resources, whether physical or logical, can be dedicated to a specific slice as separate instances, or they can be shared among multiple slices depending on the requirements of industrial applications. For example, a network slice handling real-time monitoring of manufacturing equipment might require fast data processing and ultra-reliable connectivity, while another slice managing routine environmental monitoring might not require such stringent performance parameters. It is important to note that not all of these resources are necessarily generated in the provider's network. Some resources can be obtained from other service providers and enable functions such as aggregation and roaming [14].

Network slices that can be customised for specific business requirements or industrial applications require a set of lifecycle management functions [15]. These functions are responsible for creating, modifying (e.g. upgrading) or removing slices for specific services in the factory as required. These functions must also be highly responsive to changes in factory operational requirements, adapting slices in real time to accommodate shifts in production or seamlessly integrating new IoT devices into the network. On the other hand, the intent-based network approach can simplify the complexity of managing network slices by allowing operators to formulate their high-level intentions, while the underlying system autonomously translates, deploys, monitors and adapts the network slices to fulfill these intentions throughout their lifecycle [16], [17]. This capability is particularly beneficial in complex industrial environments where operating conditions and requirements can change rapidly.

After defining the industrial applications and the associated network slices, the data traffic need to be assigned to or routed through the corresponding network slice. In most scenarios, a single device uses only one slice, so it is easy to assign each user equipment (UE) to a specific slice. However, there are cases where a device in the factory floor area can process traffic for multiple slices simultaneously [18]. In complex industrial environments, devices may therefore need to interact with multiple network slices simultaneously, a common scenario in smart factories where machines communicate across different operational processes [19]. A fundamental aspect of mobile networks to guarantee a certain service performance

and QoS is the implementation of dedicated bearers. These bearers are often used to meet the requirements of specific use cases or services. Within the Radio Access Network (RAN), these bearers correspond to the radio bearers that the scheduler can use to deliver the QoS specific to each bearer. In some cases, dedicated resources can be assigned exclusively to specific bearers. At the network edges, bearers can be identified and treated individually by applying filters to packet headers. To manage traffic effectively, advanced filtering techniques are used to ensure that each data packet is correctly identified and routed according to its priority and security requirements.

III. DEPLOYMENT SCENARIOS FOR NETWORK SLICING IN IIOT

In Fig. 1, three different methods for network slicing in mobile networks are presented [20]. *(i) PLMN IDs and RAN Sharing:* With the first approach, eNodeBs can publish announce Public Land Mobile Network (PLMN) IDs by using RAN sharing. For example, one PLMN could handle critical machine-to-machine communications that require ultra-reliable, low-latency connections, while another could manage routine monitoring data. To guarantee that traffic is correctly routed to and from the appropriate core network and that the PLMN IDs are advertised, both the RAN and the core network must support this functionality. The UE chooses a network by following the normal methods, wherein some networks (like the home network) might be favored. It is important to note that a UE can only be served by a single PLMN, except in cases with multi-SIM UEs where multiple PLMNs can be used. *(ii) APN-Based Traffic Forwarding:* The second solution in Fig. 1 is to use the Access Point Names (APNs) configured in the UE. In this scenario, the RAN announces a single PLMN ID, but the user plane traffic is forwarded to the corresponding core network based on the APN. A UE can have multiple APNs configured, which can lead to multiple IP addresses when establishing packet data network (PDN) sessions (multi-homing). However, ensuring that the correct source IP address is used for transmission in the uplink can be complex. It should be noted that setting multiple APNs in the same UE for Internet applications may not be supported by all devices. This setup allows industrial systems to direct different types of operational data to specific parts of the core network. This ensures that traffic from critical operations does not interfere with less critical data streams, preserving the integrity and responsiveness of mission-critical communications. This solution does not require any changes in the RAN, but support in the core networks is necessary. *(iii) Advanced Slicing with NSSAI:* For the 5G slicing in Fig. 1, Network Slicing Selection Assistance Information (NSSAI) is introduced to support the slice selection, which consists of a list of Single (S-NSSAI). Each S-NNSAI contains a Slice Service Type (SST). SST refers to the expected behaviour of network slicing in terms of functions and services. This feature is critical for industrial environments where different operations—from automated production lines to sensitive quality

control processes—require uniquely configured network slices to ensure their performance requirements are accurately met.

There are several sub-options for implementing slicing in 5G, such as service-based slicing (creating virtual slices within a single application or service, with each slice providing a specific level of performance or QoS) [21], function-based slicing (creation of virtual slices within a specific function or process, where each slice provides a certain level of performance or functionality) [22], resource-based slicing (creating virtual slices within a specific resource or component, with each slice providing a specific level of performance or capacity) [23], hybrid slicing (combining multiple slicing approaches to create a customized solution tailored to specific requirements) [24]. In Release 15 and later versions of 3rd Generation Partnership Project (3GPP), 5G slicing extends this capability and theoretically enables an *unlimited number of slices*. However, practical implementation and resource constraints in the UE, RAN and Core may impose limitations. Once traffic has been allocated to its respective slice, the next consideration is how to ensure service performance. In many IIoT scenarios, guaranteed service performance for prioritized traffic is crucial [25], especially in IIoT environments where delayed data can lead to operational disruptions or safety issues. In a regular 5G network or within a single network slice, traffic flows can be segregated using traffic flow separation techniques, as shown in Fig 2. In this way, dedicated resources can be allocated to the critical traffic of the IIoT device. In 5G, admission control mechanisms are used to ensure that the number of admitted prioritized traffic flows with guaranteed transmission resources, such as a guaranteed bit rate, does not exceed the available resources [26].

Note that the targets of latency ≤ 1 ms and reliability $>99.999\%$ originate from ITU-R M.2410 and 3GPP TR 22.261 as theoretical URLLC performance objectives at the radio interface. However, these values are not equivalent to system-level dependability guarantees required in process automation. Standards such as IEC 61508 quantify reliability using Failure In Time (FIT) metrics and probabilistic Safety Integrity Levels (SIL), where, for example, SIL 3 demands a dangerous failure probability between 10^{-7} and 10^{-8} per hour. In contrast, a 5G link-level reliability of 99.999% implies a packet error rate (PER) of 10^{-5} , which is insufficient for SIL 2/3 safety applications without further architectural redundancy. Therefore, any attempt to use 5G slices in safety-critical process control must involve formal reliability modeling (e.g., fault tree or Markov analysis) and may require functional safety islands, redundant slices, or certified safety relays as enforcement points. Emerging work in 5G-ACIA, OPC Foundation, and vendors like Siemens and Bosch Rexroth explores this reliability translation, but robust certification pathways are still in progress.

When it comes to resource allocation between slices, the reservation of resources in the physical infrastructure is based on the cumulative demand of critical traffic flows within each slice and not on individual traffic flows. This total resource requirement for industrial applications is specified

in the network slice SLA. It is important to note that the allocation of resources is not fixed and static. Optimal efficiency can be achieved by allowing unused resources from one slice to be used by another slice [27]. This setup is crucial for industrial applications where demand can fluctuate significantly. It ensures that resources are not only available when they are needed, but also conserved when they are not required, supporting sustainable operating practices. Another important requirement is that each network slice has access to the guaranteed service flows when required and fulfills the availability levels defined in the SLA. At the same time, Artificial Intelligence (AI)-assisted network slicing approaches in next-generation wireless networks are proposed in [28]–[31], as promising and innovative approach that utilises AI technologies to improve the efficiency, flexibility, and performance of network slicing.

IV. DEPLOYMENT CHALLENGES AND MITIGATION

The use of network slicing in the IIoT presents distinct challenges due to the deterministic performance, heterogeneity, and security-critical nature of industrial environments. These challenges are amplified in edge deployments with limited compute capacity and constrained orchestration. This section outlines key deployment challenges and proposes mitigation strategies grounded in 3GPP standards and recent research advances.

- 1) *Heterogeneous Device Ecosystems*: IIoT environments include legacy fieldbuses (e.g. Modbus, PROFIBUS), modern IP-based sensors and high-bandwidth XR/Vision devices. The integration of these endpoints into a unified 5G slice is hindered by incompatible protocols and inconsistent timing semantics. To mitigate this, protocol adaptation layers such as Open Platform Communications Unified Architecture (OPC UA) can abstract device heterogeneity via TSN in combination with slice-aware gateways or semantic edge proxies. Device abstraction layers and software-defined translation mechanisms can also enable seamless communication between different device types. These gateways can provide uniform slice descriptors that map to S-NSSAI parameters and enable backward-compatible integration with 5G management planes (as recommended in 3GPP TR 28.824).
- 2) *Extreme Low Latency for Real-Time Control*: Use cases such as robot arms, AGVs, and closed-loop control require latencies of ≤ 1 ms and $> 99.999\%$ reliability. Wireless link volatility and electromagnetic interference complicate this requirement. As mitigation, edge-based User Plane Functions (UPFs), configured via pre-instantiated URLLC blueprints (e.g., SST=2, 5QI=85), can localize traffic and eliminate core delays. RAN slicing with short DRX cycles and HARQ prioritization should be used for deterministic behavior. These behaviors align with slice profile parameters in 3GPP TS 28.531 Table 6.1.1.2-1.
- 3) *Scalable Resource Allocation for Fluctuating Workloads*: Production workloads in factories fluctuate due to batch changes, maintenance cycles, or event-triggered uplink

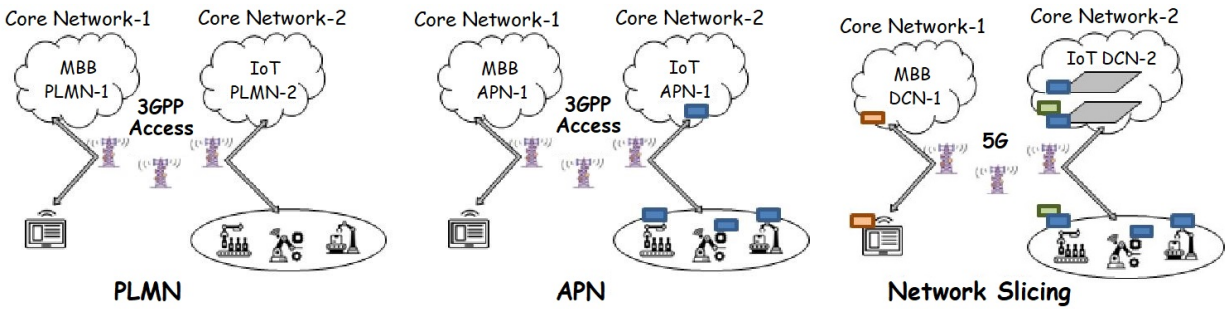


Fig. 1: Three different mechanisms for slicing the mobile network: PLMN, APN, and NS [20].

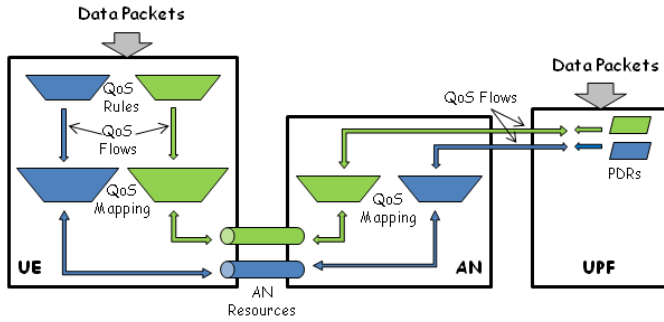


Fig. 2: QoS mechanism in the 5G system interacting with different entities.

bursts. Static slice configurations risk either resource starvation or under-utilization. To address this, intent-aware slice orchestration and traffic-aware auto-scaling mechanisms (as explored in [11]) should be used. Additionally, predefined slice templates with elastic resource ranges (CPU, bandwidth) can be provisioned using TS 28.531's slice lifecycle operations, enabling slice resizing without full redeployment. AI-driven predictive analytics can anticipate resource needs and enable dynamic allocation. Implementing hierarchical resource pooling across factories and regional networks can also provide scalability while optimizing resource utilization.

- 4) *Physical Security and Data Privacy in Harsh Environments*: Industrial networks in remote or hazardous areas are susceptible to tampering, device hijacking, or side-channel attacks. Furthermore, operational data often includes proprietary manufacturing processes. Physical security can be enhanced using tamper-resistant Trusted Platform Module (TPM)-equipped devices and secure boot chains. For privacy, privacy-preserving mechanisms such as Secure Multi-Party Computation (SMPC) or federated learning can isolate sensitive data from shared slice infrastructure. TS 28.531 Section 6.3.2 supports this via slice-level confidentiality and integrity policies.
- 5) *Ensuring QoS Across Multi-Domain Operations*: Many IIoT workflows span production (low latency), quality assurance (high throughput), and logistics (high mobility), each with different QoS requirements. This leads to conflicts when these domains share slice infrastructure. To mitigate this, federated slice orchestration using domain-specific slice instances (each with its own SST/SD + QoS

profile) should be coordinated via the cross-domain management model in TR 28.824 Section 6.4.1. Per-domain SLA enforcement should be done using telemetry-aware policy control functions (PCFs).

- 6) *Energy Efficiency for Large-Scale Deployments*: Thousands of IIoT endpoints with 24/7 operation lead to high power demand, especially when slices use persistent bearers or high DRX duty cycles. To improve efficiency, energy-aware slice scheduling algorithms can dynamically reduce UE activity cycles based on application semantics (e.g., using DRX cycling for mMTC). Low-power protocols such as NB-IoT or NR RedCap can be included in the slice profile. These optimizations are supported by energy management descriptors in the slice template extensions proposed in TR 28.824.
- 7) *Real-Time Adaptability to Industrial Failures*: Unplanned link or device failures (e.g., robot controller crashes, link loss) can disrupt time-critical processes if the slice does not adapt. Mitigation involves deploying self-healing slice managers that monitor telemetry and invoke template-based reconfiguration workflows (e.g., through the NSMF/NSMF-SMF interfaces defined in TS 28.531). Backup paths and multipath UPF routing can ensure continuity, while AI-based anomaly detection can trigger preconfigured fallback slice instantiations with degraded QoS modes.
- 8) *Regulatory and Integration Challenges in Process Automation*: Beyond technical feasibility, deploying 5G network slicing in process industries is subject to regulatory and certification constraints. Systems that affect safety, such as emergency stop mechanisms, must comply with functional safety standards like IEC 61508 or domain-specific variants (e.g., ISO 13849 for machinery). Any communication slice responsible for transporting safety-relevant signals must demonstrate deterministic performance under fault conditions, and such behavior must be auditable. In parallel, cybersecurity requirements such as IEC 62443 mandate asset identification, secure remote access, and network segmentation — which must be preserved even in virtualized and multi-tenant slice environments. Integration into existing industrial control systems (DCS, SCADA, PLCs) also presents non-trivial challenges. These legacy systems are often built for wired, cyclic protocols (e.g., 4–20 mA, PROFIBUS DP) with vendor-specific interfaces. Seamless integration requires slice-aware gateways that not

only support protocol translation but are also compatible with safety PLCs certified under SIL 2 or SIL 3 levels. Projects such as 5G-ACIA testbeds and the Fraunhofer 5G Industry Campus Europe have begun to explore this area, but broad industry-wide validation is still in the early stages.

V. NETWORK SLICING SUITABILITY FOR INDUSTRIAL AUTOMATION

While 5G network slicing has become a prominent architectural feature, its suitability for Industrial Automation Services (IAS) is not widely recognised. The underlying assumptions of slicing — such as isolation, dynamic scalability and service differentiation — need to be carefully considered in the context of industrial requirements and operational practises. Network slicing promises tailored QoS, logical isolation, and lifecycle management per application class — aligning well with the heterogeneity of industrial systems (e.g., AGV control vs. condition monitoring). In factory scenarios, slices allow separate optimization for latency-sensitive control loops (URLLC) and bandwidth-hungry applications (e.g., HD inspection via eMBB). Slicing also provides a means to enforce deterministic behaviors in wireless domains, which historically lacked predictable performance. Furthermore, slicing enables co-existence of public and private traffic in shared infrastructure, supports multi-tenancy for integrators and OEMs, and simplifies governance over multi-vendor deployments. With 3GPP-compliant slice descriptors and orchestration interfaces (e.g., NSMF, NSSMF), lifecycle operations can be automated — a critical feature in dynamic production environments.

Despite these advantages, the assumption that slicing is “the right tool” needs to be nuanced due to following reasons: (i) Slice management introduces orchestration overhead, control-plane traffic, and integration complexity. In static or small-scale environments (e.g., brownfield process automation), this complexity may outweigh the benefits. (ii) Safety-critical functions in process automation (e.g., per IEC 61508/IEC 62443) demand proven reliability over years. Slicing, being dynamic and software-defined, lacks formal verification paths for Safety Integrity Levels (SIL), making it unsuitable for the highest safety-critical loops without redundant architectural overlays. (iii) Industrial control prefers predictability over elasticity. While slicing enables flexibility, the dynamic behavior of shared RAN or virtualized UPFs may undermine the deterministic guarantees required in closed-loop control. (iv) Alternatives such as Time Sensitive Network (TSN) over Ethernet, or dedicated private 5G networks with static QoS classes, may offer simpler and more certifiable paths for many industrial setups. For example, wireless 4–20 mA emulation over fixed URLLC bearers could satisfy specific use cases without full slice lifecycle orchestration.

Slicing can be most effective when (i) Multiple industrial applications with diverse requirements share the same 5G infrastructure. (ii) Resources are constrained (e.g., at the edge), requiring prioritized handling or isolation. (iii) Dynamic reconfiguration is necessary, such as during shift changes,

predictive maintenance, or when serving mobile production units. In contrast, for ultra-critical deterministic control loops requiring long-term safety certification, slicing may serve as a supporting layer — not the primary control path.

VI. LESSONS FROM REAL-WORLD INDUSTRIAL SLICING DEPLOYMENTS

Real-world testbeds and pilot deployments reveal crucial insights that extend beyond theoretical models for a structured view of slice instantiation for industrial automation. Several European Union research initiatives such as *5G-VINNI*, *5G-INDUCE*, and *5G-ERA* have deployed 5G slices in industrial environments ranging from manufacturing plants to energy systems. These projects validate architectural blueprints but also highlight the need for adaptive lifecycle management and brownfield integration.

- *5G-VINNI*: This large-scale facility validated end-to-end network slicing for verticals including smart manufacturing. Their trials revealed that blueprint reuse (e.g., predefined URLLC or eMBB slices) reduced provisioning time, but failed to capture real-time workload variance without dynamic scaling extensions. Slice adaptation to robot arm control required coupling with industrial controllers to respect PLC-level timing.
- *5G-INDUCE and 5G-ERA*: These projects focused on dynamic slice instantiation across factories. For example, in the *dynamic predictive maintenance* use case of 5G-ERA, slices had to be reconfigured during maintenance anomalies, which challenged static blueprint assumptions. AI-assisted orchestration showed promise in adapting CPU and bandwidth envelopes based on machine telemetry. However, limited support for real-time reallocation at the edge remains a bottleneck.
- *5G-ACIA Pilots (Bosch, ABB)*: Industrial slicing pilots coordinated by 5G-ACIA (e.g., Bosch’s Stuttgart plant) exposed regulatory and safety gaps. Even with compliant radio KPIs, URLLC slices could not be certified for SIL 2/3 usage due to lack of deterministic end-to-end modeling and insufficient support for system-level failure probabilities (as required by IEC 61508). Operators had to resort to isolated non-critical applications such as video inspection or non-blocking AGV routing.

Based on these deployments, we also observe the following limitations that challenge the direct application of abstract slice templates: (i) Real factories operate with legacy fieldbus systems (e.g., 4–20 mA, PROFIBUS), which are not natively IP-based. Adapters or gateways introduce timing uncertainties that may violate the assumptions of the blueprint latency models. (ii) No current slice management solution satisfies functional safety standards such as IEC 61508 or IEC 62443. This means that safety-critical loops must remain physically isolated or monitored through certified relays. (iii) While slice managers exist, most require cloud connectivity for decision-making. In disconnected or air-gapped factory networks, orchestrators must run on-site with hardened reliability — a feature still under development in commercial platforms. (iv)

Resource prediction and slice scaling remain research prototypes. While ML-based estimators exist (e.g., in 5G-ERA), they require long training periods and significant instrumentation of the plant floor, limiting immediate applicability.

VII. CONCLUSIONS

Network slicing has become a transformative technology to meet the demands of Industry 4.0 and automated industrial services. By leveraging the flexibility and scalability of 5G networks, network slicing meets the diverse requirements of IIoT, including ultra-low latency, high reliability and robust security. This paper examined the critical aspects of network slicing, covering design, implementation in core and RAN domains, and deployment scenarios. This paper has emphasized that dynamic and adaptive network slicing is essential to accommodate the variability of industrial workloads and ensure efficient resource utilization. In addition, the integration of advanced tools such as AI/ML for orchestration and real-time optimization further enhances the potential of network slicing in IIoT environments. Despite the promising possibilities, challenges such as interoperability, standardization and cost-efficient use remain. Addressing these issues requires collaboration between industry stakeholders, academia and policy makers. As the technology matures, network slicing will continue to play a central role in shaping the future of industrial networking, driving efficiency and innovation across all industries.

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] 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.
- [2] 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.
- [3] I. Afolabi, T. Taleb, P. A. Frangoudis, M. Bagaa, and A. Ksentini, "Network Slicing-based Customization of 5G Mobile Services," *IEEE Network*, vol. 33, no. 5, pp. 134–141, 2019.
- [4] R. Su *et al.*, "Resource allocation for network slicing in 5G telecommunication networks: A survey of principles and models," *IEEE Network*, vol. 33, no. 6, pp. 172–179, 2019.
- [5] H. Wu, G. T. Nguyen, A. K. Chorppath, and F. Fitzek, "Network slicing for conditional monitoring in the industrial internet of things," *Transport*, vol. 2018, 2017.
- [6] X. Li *et al.*, "Network slicing for 5G: Challenges and Opportunities," *IEEE Internet Computing*, vol. 21, no. 5, pp. 20–27, 2017.
- [7] T. Taleb, I. Afolabi, K. Samdanis, and F. Z. Yousef, "On Multi-domain Network Slicing Orchestration Architecture and Federated Resource Control," *IEEE Network*, vol. 33, no. 5, pp. 242–252, 2019.
- [8] 3GPP, "System Architecture for the 5G System; Stage 2 (Release 15)," TS 23.501, 2018.
- [9] L. Ji *et al.*, "Dynamic network slicing orchestration for remote adaptation and configuration in industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4297–4307, 2021.
- [10] K. Antevski and C. J. Bernardos, "Federation in dynamic environments: Can blockchain be the solution?" *IEEE Communications Magazine*, vol. 60, no. 2, pp. 32–38, 2022.
- [11] A. Perdigão, J. Quevedo, and R. L. Aguiar, "Automating 5g network slice management for industrial applications," *Computer Communications*, vol. 229, p. 107991, 2025.
- [12] A. Aydeger, E. Zeydan, J. Mangues-Bafalluy, S. Arslan, and Y. Turk, "Enhancing electric vehicle security and privacy through decentralized identity management," *Digital Threats: Research and Practice*, 2025.
- [13] R. Su *et al.*, "Resource allocation for network slicing in 5G telecommunication networks: A survey of principles and models," *IEEE Network*, vol. 33, no. 6, pp. 172–179, 2019.
- [14] S. Zhang, "An overview of network slicing for 5G," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 111–117, 2019.
- [15] L. U. Khan, I. Yaqoob, N. H. Tran, Z. Han, and C. S. Hong, "Network slicing: Recent advances, taxonomy, requirements, and open research challenges," *IEEE Access*, vol. 8, pp. 36 009–36 028, 2020.
- [16] K. Abbas, T. A. Khan, M. Afaq, and W.-C. Song, "Network slice lifecycle management for 5G mobile networks: An intent-based networking approach," *IEEE Access*, vol. 9, pp. 80 128–80 146, 2021.
- [17] K. Abbas, M. Afaq, T. Ahmed Khan, A. Rafiq, and W.-C. Song, "Slicing the core network and radio access network domains through intent-based networking for 5G networks," *Electronics*, vol. 9, no. 10, p. 1710, 2020.
- [18] C. Chang *et al.*, "Performance isolation for network slices in industry 4.0: The 5Growth approach," *IEEE Access*, vol. 9, pp. 166 990–167 003, 2021.
- [19] 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.
- [20] Ericsson, "Network Sharing and Slicing for Railway," <https://bit.ly/3UqfBH>, 2018, [Online; accessed December-2023].
- [21] M. Arif *et al.*, "On the demonstration and evaluation of service-based slices in 5G test network using NFV," in *2019 IEEE Wireless Communications and Networking Conference Workshop (WCNCW)*. IEEE, 2019, pp. 1–6.
- [22] K. Trantzas, C. Tranoris, and S. Denazis, "Defining a management function based architecture for 5G network slicing," in *2021 IEEE 7th International Conference on Network Softwarization (NetSoft)*. IEEE, 2021, pp. 63–69.
- [23] D. Marabissi and R. Fantacci, "Highly flexible RAN slicing approach to manage isolation, priority, efficiency," *IEEE Access*, vol. 7, pp. 97 130–97 142, 2019.
- [24] S. Khan *et al.*, "Highly accurate and reliable wireless network slicing in 5th generation networks: a hybrid deep learning approach," *Journal of Network and Systems Management*, vol. 30, no. 2, p. 29, 2022.
- [25] T. P. Raptis, A. Passarella, and M. Conti, "Performance analysis of latency-aware data management in industrial IoT networks," *Sensors*, vol. 18, no. 8, p. 2611, 2018.
- [26] A. Aydeger and E. Zeydan, "Blockchain-based self-sovereign identity in 6g non-public networks: Enhanced security in industrial cyber-physical systems," in *2024 20th International Conference on Network and Service Management (CNSM)*. IEEE, 2024, pp. 1–7.
- [27] S. Li, Y. Zhang, S. Yuan, and T. Ma, "User scheduling and slicing resource allocation in industrial internet of things," *China Communications*, vol. 20, no. 6, pp. 368–381, 2023.
- [28] X. Shen *et al.*, "AI-assisted network-slicing based next-generation wireless networks," *IEEE Open Journal of Vehicular Technology*, vol. 1, pp. 45–66, 2020.
- [29] W. Wu, C. Zhou, M. Li, H. Wu, H. Zhou, N. Zhang, X. S. Shen, and W. Zhuang, "Ai-native network slicing for 6g networks," *IEEE Wireless Communications*, vol. 29, no. 1, pp. 96–103, 2022.
- [30] J. Mei, X. Wang, K. Zheng, G. Boudreau, A. B. Sediq, and H. Abou-Zeid, "Intelligent radio access network slicing for service provisioning in 6G: A hierarchical deep reinforcement learning approach," *IEEE Transactions on Communications*, vol. 69, no. 9, pp. 6063–6078, 2021.
- [31] W. Guan, H. Zhang, and V. C. Leung, "Customized slicing for 6G: Enforcing artificial intelligence on resource management," *IEEE Network*, vol. 35, no. 5, pp. 264–271, 2021.