2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) | 978-1-6654-5556-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/SmartGridComm57358.2023.10333884

Integrating 5G Technology for Improved Process Monitoring and Network Slicing in ICS

Jared M. Aguayo[‡], Abel O. Gomez Rivera[†], Deepak K. Tosh[‡]
[‡]Department of Computer Science, University of Texas at El Paso, TX, USA
[†] Sandia National Laboratories, Albuquerque, NM, USA
jmaguayo@miners.utep.edu, aogomez@sandia.gov, dktosh@utep.edu

***Abstract*—Industrial Control Systems (ICS) are crucial for monitoring physical processes that support essential cyber-enabled services like power generation. The use of proprietary communication and lack of effective intrusion detection mechanisms pose constraints for efficient operation. Therefore, there is a need to modernize these systems with decentralized technologies like Edge Computing and 5G. However, integrating 5G and Edge Computing into large-scale ICS networks presents implementation and performance challenges. To address these challenges, this paper proposes an integrated ICS architecture that combines 5G and Edge Computing technologies with traditional ICS protocols. The objective is to minimize implementation and operational difficulties while improving the monitoring of physical processes and enabling robust intrusion detection. The proposed architecture outlines the necessary components, services, and communication protocols required for the integration of 5G and Edge Computing.**

***Index Terms*—Cyber-Physical Systems, 5G, Software Define Network, Operational Technology, Edge Computing**

I. Introduction

Industrial Control Systems (ICS) play a crucial role in operating the cyber-enabled critical infrastructures, such as power plants and manufacturing. These systems often consist of legacy Operational Technology (OT) devices which communicate over proprietary industrial communication protocols that often lack robust security mechanisms. Thus, there is no guarantee of device authenticity and integrity of physical processes [1]. Sensing information represents the operational data gathered by physical processes from the environment, while non-process-related sensing information provides insights into the state-of-health of OT. Thus, it would be useful to segregate the network traffic based on the type of data, its priority, availability of network resources, and applications' needs. The current OT network infrastructure does not offer the flexibility to manage such advanced needs. Furthermore, the increasing cyber attacks in recent years has also augmented the urgency to modernize the OT networks by adopting more flexible and resilient communication technology and protocols.

Software Defined Networking (SDN) [2] is a next-generation network management architecture that revolutionizes the management of traditional network systems by simplifying their complexity and enabling reconfigurable communication. In the context of industrial communication protocols, state-of-the-art SDN mechanisms can greatly enhance the management of sensing data transactions. By decoupling process sensing data from non-process sensing information, SDN can enable efficient and secure data communication in ICS, while leveraging traditional industrial communication protocols. Furthermore, SDN technology seamlessly integrates with next-generation communication protocols like 5G, which could offer low latency and high availability services to meet various operational needs of ICS. By adopting 5G technology, operators of ICS can swiftly enable resilient component monitoring services that are flexible and fault tolerant. Although such functionalities exist in current ICS environments, the decisions are typically made at the supervisory nodes, thus incurring additional overheads such as network resources and latency. Thus, facilitating a 5G-integrated edge computing service for component health monitoring and anomaly detection could be a game changer for critical infrastructure networks.

The modular virtualization and containerization tools of 5G, enable the deployment of flexible services that extend the capabilities of traditional systems. 5G provides a reliable infrastructure that meets the demands of modern network management, while also supporting the integration of traditional industrial communication protocols. In parallel, Edge Computing complements 5G by delivering modular network services that facilitate low latency and real-time access to sensing information. Thus, the convergence of SDN, 5G, and Edge Computing technologies offers tremendous potential for revolutionizing network management in ICS. By embracing these next-generation communication technologies, ICS operators can establish resilient and flexible monitoring services, enhance fault tolerance, and enable real-time access to critical sensing information, thereby driving efficiency and reliability.

This work focuses on the development of a novel 5G-edge integrated architecture for ICS to seamlessly manage the OT network to facilitate efficient non-process-related sensing information. The integration of next-generation communication technologies into legacy ICS is a complex task due to the inherent design and operational constraints of ICS. This paper addresses the challenges by tightly integrating the 5G communication technology and Edge Computing. Specifically, it presents a comprehensive analysis of the novel architecture derived from integration of 5G-Core to better understand its benefits. Furthermore, we discuss the advantages to facilitate the integration of an operational layer based on edge computing principles. This Edge Computing based operational layer incorporates Industrial Communication Protocol Translators (IPTs), which are responsible for translating legacy industrial

communication protocols [3] into more resilient and flexible communication protocols, such as standardized 5G links. By leveraging IPTs, the architecture aims to bridge the gap between legacy protocols and modern communication standards, thereby enhancing the overall performance, capabilities, and security of ICS. The contributions of this paper are as follows:

- Present a comprehensive analysis of the challenges and benefits of integrating 5G and Edge Computing.
- Introduce a novel pathway to modernize legacy ICS, by enhancing legacy industrial communication protocols.
- Evaluate the operational overheads and overall impact of next-gen communication technology in ICS.

The structure of the paper is as follows. Section II highlights related work. Section III discusses an overview of the challenges of implementing 5G technology and Edge Computing. Section IV describes the results and experiment setup. Section V finally concludes and provides future directions.

II. Related Work

One important area of research in ICS security is the implementation of dynamic communication protocols that are more flexible and robust such as 5G and edge computing technologies. These technologies have the potential to greatly enhance the performance and efficiency of ICS systems, as well as enable new applications that were not previously possible such as intelligent performance monitoring. Next-gen communication technologies can be more efficient, reliable, and easier to maintain than legacy technology, which can help to improve overall operational efficiency and reduce costs associated with maintenance and downtime. The implementation of 5G and edge computing in traditional ICS is an active area of research, with many challenges and opportunities. Authors in [4] introduce the concept of next-generation broadband wireless access networks, such as 5G and beyond in the context of private networks through detailed exploration and analysis of challenges posed by the dynamic and heterogeneous nature of wireless networks.

Authors in [5] provided a comprehensive review of edge computing for the Industrial Internet-of-Things (IIoT). The authors discussed the challenges and opportunities of edge computing, as well as its potential applications in ICS. The paper also presented a detailed overview of the various edge computing architectures and technologies that are currently available. In [6] authors examined the challenges and future directions of edge computing in the context of the IoT. The paper provides an overview of the key concepts and technologies of edge computing, and discusses some of the key challenges and open research issues that need to be addressed in order to fully realize the potential of this technology. Authors in [7] explored the potential of network slicing for 5G and future mobile networks. The paper presents a detailed overview of the key concepts and technologies of network slicing. The authors also present a number of use cases for network slicing in industrial settings, such as factory automation and smart cities. A survey presented in [8] provided a survey of 5G networks for IIoT, with a focus on architecture, use cases, and implementation. In [9] authors proposed a number of countermeasures to address security and privacy threats that are associated with edge computing in ICS systems. The authors also present a set of use cases for secure and private edge computing in ICS. In [10] authors demonstrated the feasibility and evaluated the performance of an industrial closed-loop control application operating over 5G links.

While previous approaches have provided an overview of the benefits and challenges of 5G and edge computing in ICS, there is a lack of empirical research that evaluates the performance of 5G and edge computing in realistic and large-scale ICS scenarios. Therefore, this work introduces a purpose-driven network virtualization framework that aims to enable next-gen communication systems in realistic ICS architectures. In particular, the purpose-driven network virtualization framework provides fault tolerance and introduces data duplication through the implementation of edge computing and dedicate 5G communication channels which control non-process related sensing information without reducing the operational capabilities of traditional process-based ICS networks or without becoming overly specific to a set of OT devices and industrial communication protocols.

III. 5G and Edge Computing Integrated ICS

The implementation of 5G networks in traditional ICS provides numerous technical benefits, including more flexible networks and architectures [11]. 5G networks enable greater connectivity, allowing for more devices to be connected to the network and communicate with each other. Additionally, 5G networks [12] offer greater bandwidth, enabling faster and more reliable communication between devices. These technical benefits enable more flexible network architectures, as 5G networks can adapt to changing network demands and allow for greater scalability. Furthermore, 5G networks can support a wider range of applications, from low-latency industrial control applications to high-bandwidth multimedia applications, which further increases their flexibility. Overall, the technical benefits of 5G networks can help modernize legacy ICS improving their performance and reliability.

Edge computing offers numerous technical benefits in terms of more flexible networks and architectures for ICS. By pushing computation and processing capabilities closer to the edge of the network, edge computing reduces the latency associated with transferring data to and from centralized servers. This enables faster decision-making and reduces the impact of network latency on critical applications. Additionally, edge computing allows for distributed data processing and storage, which can improve the scalability and resiliency of ICS. Overall, edge computing provides a more flexible and scalable architecture, enabling more efficient and effective monitoring and management of industrial processes and services.

Legacy communication protocols such as *Modbus* [13] provide high-performance efficiency without considering sensing information's operational security or integrity. Traditional ICS are designed to operate in closed environments in which the authenticity and integrity of process and non-process sensing

information is taken for granted. ICS lack the capacity to support operational and security upgrades, thus enabling standard cyber threats that can disrupt the operational hours of critical cyber-enabled services such as power generation. The 5G-edge integrated architecture described in this work leverages dynamic edge layers devices and flexible 5G communication channels that introduce novel industrial communication protocol translators to enable more robust security and better monitoring of industrial services. In the following sections, we describe the challenges and requirements to enable 5G technology and edge computing in traditional ICS.

A. Resilient OT Through 5G Technology and Edge Computing

OT devices use proprietary communication protocols that do not prioritize data trustworthiness or identity verification. This creates a challenge for ICS ecosystems that require real-time monitoring of physical processes, which necessitates the use of legacy industrial communication protocols with performance trade-offs to meet critical operational requirements like low latency and real-time data transmission. However, these legacy protocols do not have the capacity to integrate new technologies like 5G mechanisms, and the lack of resources for integrating complex operations like authentication, integrity verification, and decoupling of sensing information prevents the adoption of 5G technology. ICS ecosystems require two types of sensing information to make critical operational decisions: (1) process OT data that represents information gathered from the environment and (2) non-process OT data that represents the state-of-health of physical devices and processes. While Supervisory Control and Data Acquisition (SCADA) systems [14] are commonly used to gather and monitor sensing information, they integrate legacy industrial communication protocols that lack robust security mechanisms to ensure the integrity and provenance of the sensing information.

In this study, we present a novel 5G-edge integrated architecture for ICS that leverages Industrial Communication Protocol Translators (IPT) to enable the integration of 5G and edge computing technologies. Our IPTs facilitate the collection and monitoring of non-process sensing information with a high degree of granularity. We define non-process sensing information as physical process data that reveals the state-of-health of processes and devices. We propose a virtual network management interface that decouples OT data sensing from non-process OT information. By separating sensing information, our 5G-edge integrated architecture provides robust and resilient network management of legacy industrial communication protocols and improves intrusion detection in constrained environments. Typically, industrial communication protocols transmit all sensing information through a single serial connection, which can result in noise and inefficiencies. To address this issue, we designed the 5G-edge integrated architecture to capture non-process sensing information without disrupting the traditional data flow of industrial communication protocols. Our IPTs enable the decoupling of sensing information through dedicated 5G channels that support flexible sensing transaction rates. We integrated scalable modular services that can support dynamic networks, allowing OT operators to monitor non-process sensing information in detail while reducing the amount of noise in traditional industrial communication protocols. Overall, our 5G-edge integrated architecture improves the efficiency of intrusion detection and monitoring performance of physical processes, making it a promising solution for future ICS systems.

B. Infrastructure Requirements

Overall, the integration of 5G technology and edge computing into existing systems, such as ICS, requires additional next-generation components that consist of more robust and heterogeneous devices that can integrate more complex technology. One important consideration is that 5G-enabled components will need to be fully IP-enabled [15]. Another challenge is determining how to deploy 5G network intelligence at the edge, in the fog, in a private/public, or on-premises, which represents an area of research that needs to be addressed before adopting 5G technology. Precisely locating 5G devices and services can introduce network latency challenges, which require reliable low latency and high data transfer rates to meet the crucial operational requirements of critical CPS ecosystems. Edge computing is well-suited for low latency networks that rely on real-time access to process and non-process sensing information.

The security of ICS ecosystems is crucial as they often transmit sensitive information related to national security. This necessitates reliable access control policies. To ensure confidentiality and control access policies, Mobile Private Networks (MPN) through private 4G LTE networks are commonly used. However, as 5G networks are becoming more prevalent, it is expected that 5G private networks will also be used for this purpose. One major challenge in deploying 5G MPNs is the significant cost associated with obtaining a licensed spectrum. Nevertheless, MPNs have an advantage over public networks as they can be configured to meet specific requirements based on the type of work and environment. This flexibility is particularly important in heterogeneous CPS ecosystems that monitor a diverse set of physical processes.

In general, the proposed next-generation ICS architecture consists of three layers: (1) the Enterprise Layer, which includes state-of-the-art enterprise services for monitoring OT devices, (2) a Control Layer that provides intelligent network management through Open 5G core technology and dedicated communication channels, and (3) a data layer that enables 5G-compatible field sensors to communicate with enterprise servers to track process data and device health. Figure 1 provides an overview of a 5G-edge integrated ICS architecture designed to enable robust intrusion detection and improve monitoring performance of physical processes. The architecture utilizes flexible industrial communication protocols translators that implement next-gen communication technology such as 5G and network management

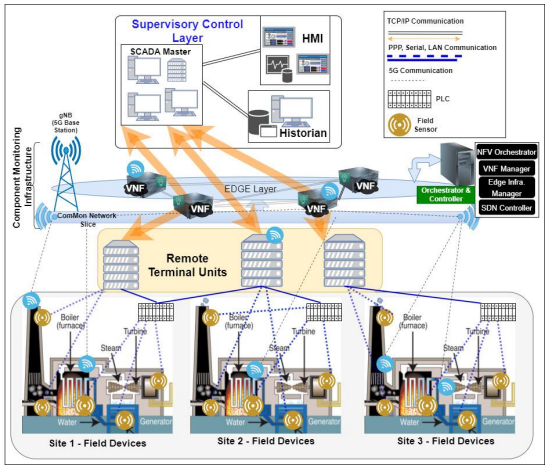

Fig. 1. 5G-edge Integrated ICS Architecture

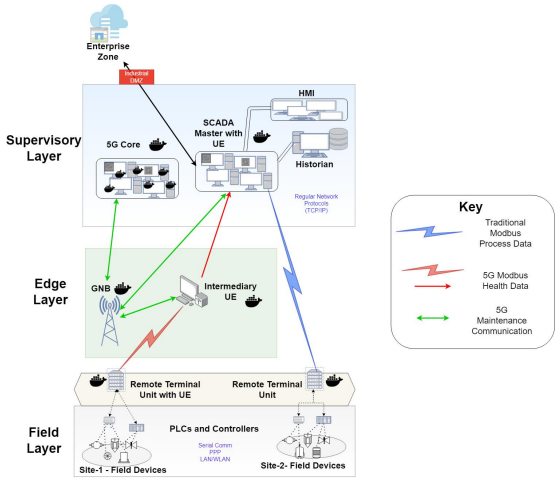

Fig. 2. Experiment Environment

C. Cybersecurity Threats

The integration of 5G and Edge Computing in traditional ICS ecosystems has the potential to revolutionize the way these systems operate, offering increased efficiency, flexibility, and real-time data processing capabilities. However, this integration also poses several challenges and risks that must be carefully managed to ensure the security and reliability of ICS. One of the main challenges associated with the integration of 5G and Edge Computing in ICS is the need to modernize legacy industrial communication protocols. In general, traditional ICS were designed without the consideration of modern cybersecurity threats, making them vulnerable to attacks that can cause significant damage to critical infrastructure [16]. Another challenge associated with the integration of 5G and Edge Computing in ICS is the potential for increased cybersecurity threats. The integration of 5G and Edge Computing can introduce new attack vectors and increase the risk of cyber-physical attacks on ICS. To mitigate these threats, advanced security measures such as real-time threat detection and incident response systems are necessary. Edge Computing can prevent standard cyber attacks by implementing robust authentication and mobile technology that enables flexible architectures.

D. Industrial Protocol Translators

In this research, we assume a traditional ICS architecture that incorporates standard industrial communication protocols like Modbus [13] and TCP/IP. The main objective of our novel 5G-edge integrated ICS architecture is to seamlessly integrate 5G technology and Edge Computing without disrupting the existing process sensing communication and services in deployed ICS ecosystems. To achieve this, we introduce Industrial Protocol Translators (IPTs). These IPTs are strategically positioned between the traditional OT devices and the controllers, minimizing any disruptions to the established operations. We design the 5G-edge integrated ICS architecture with modular services that can be enabled or disabled through Application Programming Interfaces (APIs). This allows for the adaptation of services to different requirements and protocols.

E. Opportunities

The integration of 5G and edge computing in traditional ICS offers several opportunities. One of the primary opportunities is the potential to improve the performance of industrial processes. 5G's ultra-high bandwidth and low latency capabilities can enable real-time communication between machines and systems, allowing for faster decision-making and response times. Edge computing can also improve performance by enabling data processing and analytics closer to the source of the data, reducing the amount of data that needs to be transmitted to centralized servers for processing. Another opportunity is the potential to enhance the flexibility and scalability of ICS. By leveraging 5G and edge computing, ICS can become more dynamic and adaptable to changing operational demands. This can help organizations achieve greater efficiency and responsiveness in their operations. Moreover, the integration of 5G and edge computing can also improve the security of ICS. By enabling more secure and efficient communication and data management, organizations can better protect their critical infrastructure and sensitive information from cyber threats.

IV. Evaluation Setup and Results

A. Experiment Environment

This portion details the experimental environment established for the overlaying of 5G in industrial control systems testbed for advanced monitoring. The system infrastructure was developed using an open-source software platform, Open5GS, which enabled the simulation of 5G communication, in tandem with UERANSIM software, which facilitated the emulation of user equipment (UE) and 5G base stations. These applications were hosted in Docker containers to to increase flexibility and scalability for the testbed.

The experimental testbed's network architecture, comprising three distinct layers: the field layer, the edge layer, and the supervisory layer, is illustrated in Figure 2. Each layer, endowed

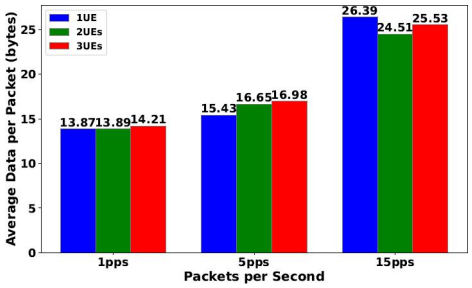

Fig. 3. Average data per packet

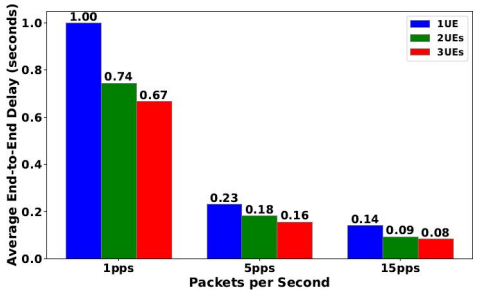

Fig. 4. Average end-to-end delay

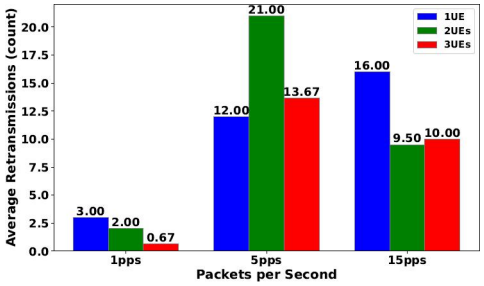

Fig. 5. Comparison of number of re-transmissions

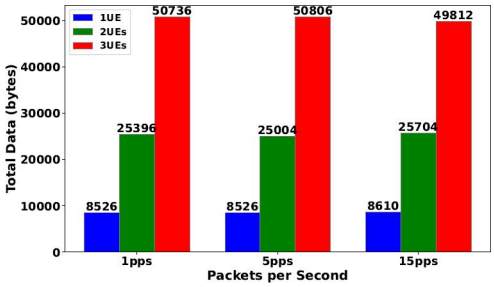

Fig. 6. Total amount of data transmitted

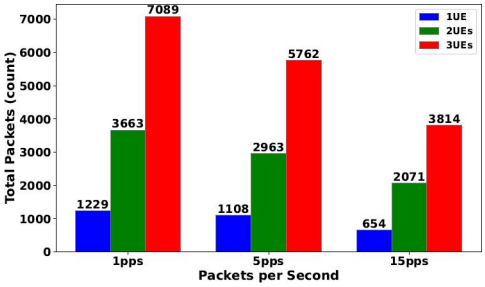

Fig. 7. Comparison of packets transferred and packets/s

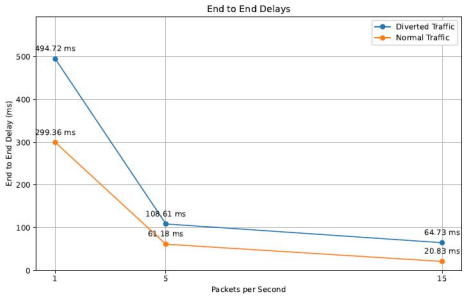

Fig. 8. End-to-end Delay: Normal vs Diverted Traffic

with unique components, is designed to facilitate seamless data transfer and communication. Highlighting the diversity in data flow, the schematic uses color-coded data communication: red for health data being transferred as Modbus over 5G, providing essential insights for advanced monitoring; green for 5G status communication, encompassing vital messages ensuring the stability and reliability of the network; and blue for process data being transferred over traditional Modbus, representing the constant stream of information generated by the industrial control system's processes from field devices. This color-coordinated representation offers a clear and engaging visual guide to understanding the dynamics of our 5G-integrated ICS.

Field Layer: This foundational layer comprised two Docker containers configured to act as Remote Terminal Units (RTUs). One of these containers was equipped with a UE, whereas the other was not. The UE-equipped container was designated for transmitting health data across the network, leveraging the capabilities of Open5GS while the other was tasked with transmitting process data over traditional Modbus communication.

Edge Layer: The second layer of the network comprised of a few Docker containers, which host the 5G Base station and a another intermediary UE. The UE in this layer received the health data from the UE in the field layer, processed it, and then forwarded it onward to the supervisory layer. This layer has the capability to do in depth analysis on the packets traveling through it before getting to the supervisory layer,

Supervisory Layer: This layer, considered the uppermost layer in the architecture, was home to several Docker containers functioning as a Supervisory Control and Data Acquisition (SCADA) Master and the 5G core. The SCADA master container received both process data and health data, health from the edge layer and process from the field layer. The 5G core is comprised of multiple containers for the many network functions it provides and manages connections with all the 5G related nodes to ensure smooth communication.

Through this network topology and the application of network slicing techniques, we were able to simulate an environment for transmitting health data from the field layer

to the enterprise layer, underlining the potential of 5G for improved monitoring within industrial control systems. The following sections will discuss the specific procedures and results obtained during the experimentation phase.

B. Experiment Setup

To evaluate the performance of the proposed 5G-based industrial control system, we conducted a series of experiments focusing on various network performance metrics.

- Number of packets transmitted
- Number of re-transmissions
- Average end-to-end delay
- Average amount of data per packet

The experiments involved Modbus 5G communication through multiple layers, exchanging a total of 300 packets at varying rates: one packet per second (pps), five pps, and 15 pps. The UE within the RTU on the field layer would start sending Health data to the edge layer, then some small-scale processing would be done such as checking the data in the Modbus packets, and lastly it would be forwarded to the supervisory layer's SCADA master. These experiments were designed to test the viability of introducing an edge layer to an ICS environment that the overlay 5G network would be able communicate and process health data through.

In addition to these measures, we consider the potential use of this superimposed network as a contingency solution in instances of regular communication disruption. Metrics are also considered that encompass the potential increase in latency as a result of transmission through additional network layers. To simulate a realistic network environment, we introduced a 20 percent chance of packet loss on the interface. This allowed us to examine the system's resilience and ability to handle packet loss, which is a common issue in wireless communication.

C. Findings

In this section, we clarify the findings obtained from the analytical assessment of the Open5GS testbed, with a specific focus on packet transmissions from the field layer to the supervisory layer. We scrutinized four metrics: total packets sent, average re transmissions, average bytes per packet, and end-to-end delay, at different transmission intervals, specifically 1, 5, and 15 packets per second and different numbers of UEs transferring from 1, 2, and 3 UEs. Following that, we look at the overlaid 5G network as a possible fail safe option for process data to be transferred.

The overlay 5G network provides the opportunity for extensive processing within an edge layer before getting to the supervisory layer since the health and process data are separated. This allows for the availability that an ICS environment demands while being able to analyze crucial data simultaneously. We explore the key metrics obtained from packet captures, analyzed based on varying packet-per-second rates and an increment of User Equipment (UEs) evaluated at one, two, and three UEs.

Retransmissions: With a single UE, retransmissions peak at a rate of 1 packet per second, potentially indicating inefficiencies in handling rapid, singular packet exchanges. When the UEs increase to two, the highest retransmissions occur at the 5 packets-per-second rate, perhaps due to network congestion. Notably, with three UEs, the most retransmissions happen at the 1 packet-per-second rate, suggesting challenges in managing simultaneous active UEs at lower packet sending rates as shown in Figure 5. Artificial packet loss of 20 percent was applied on the interfaces and the with the margin of retransmissions being minor, the randomness of the packet loss had an effect on the retransmission results as well. Specifically, their is marginal difference between 5 and 15 packets-per-second rates, leading to increase congestion since the packet rates are increasing as a commonality of increasing the rate at which packets are sent.

End-to-End Delay: When analyzing the end-to-end delay show in Figure 4, significant delay is observed with 1 UE at 1 packet per second, which decreases as we move to higher packet-per-second rates. This trend persists with two and three UEs, indicating the network's proficiency in managing higher data throughput, and its potential for optimization for smaller packet-per-second rates. With the packet rates being higher, even though they experienced higher retransmissions, the retranmissions are handled quicker than at the slower 1 packet-per-second rate since multiple ACKs can be received in a shorter time frame to trigger the retransmission versus the slower alternative. Continued analysis remains a top priority in order to identify key network parameters that will contribute to the overall optimization of the baseline network data.

Total Data Per Packet and Total Packets Sent: These metrics show a proportional increase with the number of UEs, indicating the network's effective use of capacity. Importantly, the totals remain relatively similar across all packet rates for the same number of UEs depicted in Figure 6

Average Data Per Packet: The consistency of the average data per packet across different UEs suggests that the network can manage multiple UEs without impacting the average packet data. However, as the packet sending rate increases, so does the average data per packet, as shown in Figure 3. The rate increases lead to larger amounts of data being buffered before being sent, which attributes to the larger the packet sizes, as the application side maintains uniform packets.

By examining the data in this way, we provide a deep, metric-based analysis of the network's behavior under various conditions. This provides invaluable insights for potential network optimization and capacity planning strategies which are necessary when considering the overlay network in an ICS environment. These metrics establish a foundational benchmark that delineates the performance capabilities of the testbed. Understanding these capabilities help guide scalability and availability of the overlaid network within an ICS network slice. Our research also involved examining a Remote Terminal Unit (RTU) within the field layer, which diverts traffic to the User Equipment (UE) to transmit process data alongside health data over a 5G network in scenarios where regular

communication is disrupted, serving as a failsafe. This strategy is particularly crucial in mitigating network failures or warding off denial of service attacks.

We broadened our analysis to compare the end-to-end delay of transmitting process data concurrently with health data over 5G, against the delay inherent in regular communication in Figure 8 . The assessment was conducted for packet-per-second transmission intervals of 1, 5, and 15 aggregating the end-to-end delays of multiple UEs into a value. The findings, as depicted in the chart, demonstrate a discernible increase in overhead when transmitting over 5G, attributed to the simultaneous transmission of health data. This data is a step in analyzing the effects of different applications of an overlayed 5G network that would aid in improving the resilience of an Industrial Control System environment using this architecture.

This insight is essential for exploring strategies to manage health data communication during a failsafe event, to ensure the seamless, real-time transmission of process data. For instance, possibilities include reducing the transmission rate of health data to avert congestion, locally storing health data until the failsafe condition is rectified, or even rerouting the health data to other UEs, allowing the process data exclusive use of the current communication line.

In the subsequent analysis, we explored the concept of traffic diversion to alternative UEs. We timed how long it took for a UE to re-establish connection following a failure, aiming to gauge the reliability and resilience that can be expected during such events. This evaluation, resulting in about a one second delay from failure to up time, also helped estimate the time it could potentially take to redirect traffic to other UEs if necessary, serving as additional failsafe measures and thus enhancing network robustness. This will help provide a baseline to determine valid strategies to further improve failsafe within future iterations of the testbed.

Ensuring the network's resilience against failures and denial of service attacks is of paramount importance in an environment where high standards of availability are expected. These measures and analyses help construct a framework for a more reliable and robust communication system.

V. Conclusion and Future Directions

In this paper, we have addressed the challenges and operational constraints associated with enhancing monitoring services and achieving a resilient architecture in traditional ICS by leveraging next-generation communication technologies such as 5G and Edge Computing. We have examined the physical limitations of implementing dynamic and flexible protocols that require specific network operations, including low latency and high availability. To overcome these challenges, we have proposed a novel 5G-edge integrated ICS architecture that integrates traditional OT devices with modern communication protocols. This architecture seamlessly integrates 5G technology and Edge Computing without disrupting existing process sensing communication and services. SDN facilitates the separation of network layers, allowing OT operators to monitor process sensing data and non-process data with a high degree of granularity. This enhances the efficiency of monitoring and provides better insights into the system's operation. Overall, the integration of 5G technology, Edge Computing, and intelligent network management technologies offers significant opportunities for improving the monitoring services and resilience of traditional ICS. The proposed architecture provides a foundation for further advancements in the field and paves the way for more secure and efficient critical infrastructure management. In future iterations of the 5G-edge integrated ICS architecture, we envision the development of a high-fidelity experimental testbed.

References

[1] N. Kshetri and J. Voas, "Hacking power grids: A current problem," *Computer*, vol. 50, no. 12, pp. 91–95, 2017.

[2] M. Alsaeedi, M. M. Mohamad, and A. A. Al-Roubaiey, "Toward adaptive and scalable openflow-sdn flow control: A survey," *IEEE Access*, vol. 7, pp. 107 346–107 379, 2019.

[3] S. Jaloudi, "Communication protocols of an industrial internet of things environment: A comparative study," *Future Internet*, vol. 11, no. 3, p. 66, 2019.

[4] C. Singhal and S. De, *Resource allocation in next-generation broadband wireless access networks*. IGI Global, 2017.

[5] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A systematic survey of industrial internet of things security: Requirements and fog computing opportunities," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2489–2520, 2020.

[6] T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, and D. O. Wu, "Edge computing in industrial internet of things: Architecture, advances and challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2462–2488, 2020.

[7] H. Zhang, N. Liu, X. Chu, K. Long, A.-H. Aghvami, and V. C. M. Leung, "Network slicing based 5g and future mobile networks: Mobility, resource management, and challenges," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 138–145, 2017.

[8] A. Mahmood, L. Beltramelli, S. Fakhrul Abedin, S. Zeb, N. I. Mowla, S. A. Hassan, E. Sisinni, and M. Gidlund, "Industrial iot in 5g-and-beyond networks: Vision, architecture, and design trends," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4122–4137, 2022.

[9] Y. Zheng, A. Pal, S. Abuadbba, S. R. Pokhrel, S. Nepal, and H. Janicke, "Towards iot security automation and orchestration," in *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 2020, pp. 55–63.

[10] K. Nikhileswar, K. Prabhu, D. Cavalcanti, and A. Regev, "Time-sensitive networking over 5g for industrial control systems," in *2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2022, pp. 1–8.

[11] L. Chettri and R. Bera, "A comprehensive survey on internet of things (iot) toward 5g wireless systems," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16–32, 2020.

[12] J. H. Park, S. Rathore, S. K. Singh, M. M. Salim, A. Azzaoui, T. W. Kim, Y. Pan, and J. H. Park, "A comprehensive survey on core technologies and services for 5g security: taxonomies, issues, and solutions," *Hum.-Centric Comput. Inf. Sci*, vol. 11, no. 3, 2021.

[13] C. Parian, T. Guldimann, and S. Bhatia, "Fooling the master: Exploiting weaknesses in the modbus protocol," *Procedia Computer Science*, vol. 171, pp. 2453–2458, 2020.

[14] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on scada systems: secure protocols, incidents, threats and tactics," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1942–1976, 2020.

[15] E. O'Connell, D. Moore, and T. Newe, "Challenges associated with implementing 5g in manufacturing," in *Telecom*, vol. 1, no. 1. MDPI, 2020, p. 5.

[16] B. Liu, Z. Luo, H. Chen, and C. Li, "A survey of state-of-the-art on edge computing: Theoretical models, technologies, directions, and development paths," *IEEE Access*, vol. 10, pp. 54 038–54 063, 2022.