Journal of Applied Automation Technologies

Research Paper

Integration and Application of 5G Ultra-Reliable and Low-Latency Communications in Networked Control Systems for Intelligent Factories

Jakub Grzegorz Zieliński[1,*] and Damian Piotr Dąbrowski[1]

[1] Faculty of Automatic Control, Electronics and Computer Science, Silesian University of Technology, 44-100 Gliwice, Poland
*Corresponding author: jakub.gz@student.polsl.pl

Abstract. Computer-based Network Control Systems (NCS) are key technologies for achieving smart factory operations. NCS can operate stable-state coordination, distributed monitoring, and automated control in an Industry 4.0 environment. This paper analyzes how 5G ultra-reliable low-latency communication technology (URLLC) can best be integrated into industrial application network control systems. To ensure response determinism in critical mission applications, a hierarchical system architecture is developed, integrating edge, fog, and cloud layers to achieve an enhanced 5G wireless network. Considering the overall model of protocol layer optimization for reliability and latency, dynamic resource management redundancy solutions are suitable for complex industrial environments. In terms of operational risk, conduct probabilistic risk assessments on various attack surface dimensions to determine the hazards. Experimental validation conducted Through scale simulators and hardware-in-the-loop testing platforms shows that the control accuracy and reliability of 5G URLLC significantly surpass those of existing systems. Implement multi-layer security protection, reliable network data security transmission methods, and systems that identify abnormal behaviors that may threaten operational continuity. The conclusion of this study is: 5G URLLC meets the stringent requirements of industrial automation and can serve as a long-term flexible foundation to drive smart manufacturing processes in digital and integrated cyber-physical systems (CPS).

Keywords: *Network Security, Networked Control Systems, 5G URLLC, Industrial Automation, Wireless Security, Edge Computing*

Received on 29 October2025, Accepted on 24 January 2026, Published on 15 February 2026

Introduction

Networked Control Systems (NCS) are widely used in smart factory environments, and the manufacturing industry is transitioning to the industry 4.0 paradigm. NCS can achieve seamless automation, real-time coordination, and distributed perception of the next generation of industrial processes [1]. The complexity of the system increases, and the demand for reliable low-latency communication also rises accordingly. Traditional wired and wireless network models cannot meet these demands [2]. The emergence of 5G networks has completely transformed the way industrial networks are built in the ultra-reliable low-latency communication (URLCC) service category, offering high availability and sub-microsecond response times [3]. Robot collaboration, closed-loop tracking and control, and M2M communication in smart factories are key task scenarios for the enabling technologies of these capabilities [4]. In the presence of interference, there are still issues with the practical application of these operational metrics [5]. Research institutions and standardization organizations are accelerating their research on 5G URLLC, but most implementation scenarios cannot meet the complex requirements of industrial NCSs [6]. Next-generation industrial communication technologies will prioritize 5G URLLC to meet the control and automation requirements of smart factories [7]. To fully leverage the potential of emerging technologies in smart manufacturing, comprehensive strategic measures are still needed [8].

In general, there may be various risks in the environment of industrial communication and control operations, and the risk factors are usually unpredictable [9]. In this case, system design and network management are

constrained by high time-stable delay requirements and the demand for near-absolute reliability [10]. To efficiently manage high-speed, time-sensitive factories, the vertical expansion of the OT chain includes edge computing, fog computing, and cloud services, which pose challenges for data transmission [11]. With the widespread application of wireless connectivity technology, new types of network attacks and security vulnerabilities are emerging one after another. The design of secure handover, authentication, and data integrity mechanisms has become the focus of research in safety-critical industrial deployments [12]. To address these issues, the reliability of the industrial control system needs to integrate model systems and optimize the physical and protocol layer levels [13]. To bridge the gap between laboratory results and the strict realities of the production line, organized efforts should be made [14]. Recently, it was pointed out that scalable, secure, and reliable 5G-connected NCS requires strict performance metrics and industry best practices [15].

This paper conducts a detailed study on the methods of integrating 5G URLLC with network control systems and smart factories. A complete system model is proposed, demonstrating the reliability and latency characteristics of the 5G-enhanced industrial network control system. Also, through analysis, derive the core performance indicators. Study the reliability and security issues of the system, and identify its main industrial vulnerabilities. Evaluate advanced solutions such as data protection and secure reconnection technologies. To evaluate the corresponding theoretical results compared to traditional industrial network technologies, a large number of simulation and physical tests are conducted. Propose recommendations for deployment to help establish a secure and reliable industrial internet ecosystem.

System Modeling for 5G-Enhanced NCS

Architecture and Protocol Adaptation

Smart factories connect to Cyber-Physical Systems (CPS) and 5G networks Through a complex multi-layer architecture. Integrating 5G URLLC capabilities into the hierarchical structure of Network Control Systems (NCSs) is at the core of this transformation. Modern industrial automation architectures are typically organized at the edge, fog, and cloud layers, depending on the required latency, computing power, and security levels. Distributed assets include programmable logic controllers (PLCs), industrial robots, field sensors, etc. The edge domain is responsible for real-time sensing and control. The fog layer aggregates and collects local data streams, possessing decentralized coordination capabilities and rapid fault detection abilities. High-intensity analysis, comprehensive system upgrades, long-term data storage, and integration with Enterprise Resource Planning (ERP) systems require cloud resources [16].

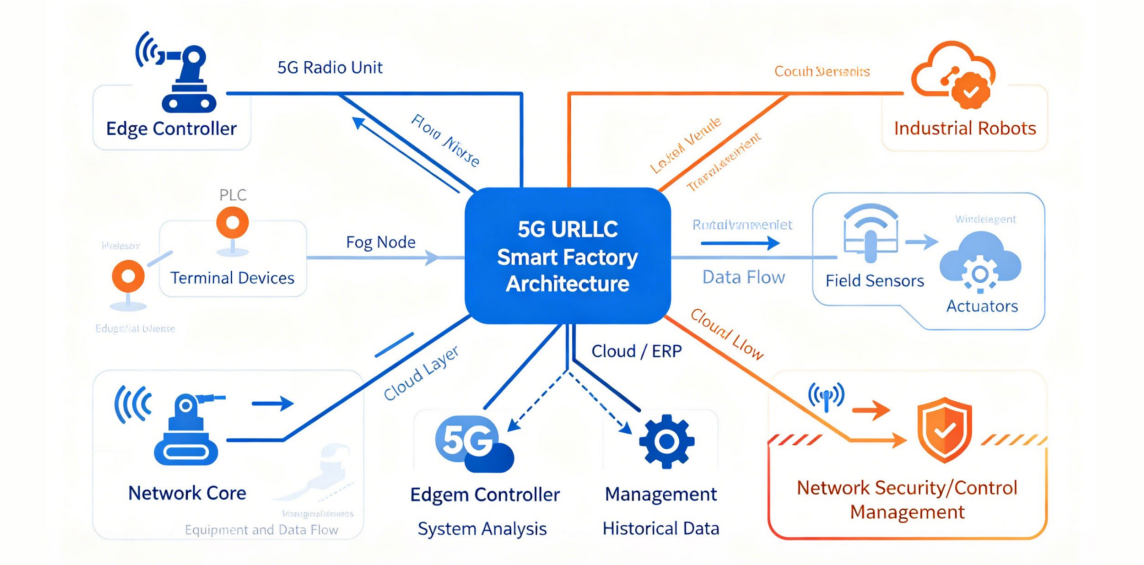

Figure 1. System architecture diagram of 5G URLLC-enabled NCS in a smart factory. Edge controller manages distributed sensors and actuators through 5G radio units, with fog and cloud integration

In this context, 5G URLLC serves as the bridge connecting high-end intelligence and low-latency field layer computing capabilities. As shown in Figure 1, industrial fieldbus and traditional Ethernet networks are typical

implementations. By adding or updating 5G wireless units, the stability of device communication and strong mobility can be ensured. The system dynamically reroutes necessary control traffic to edge gateways Through Multi-Access Edge Computing (MEC) technology, which requires millisecond-level response times. Fog computing and cloud computing handle large amounts of data Through robust backhaul connections.

After making some adjustments to the industrial protocol system, the architectural advantages can be translated into protocol operations. In terms of the application layer, industrial protocols such as OPC UA, PROFINET, and EtherCAT must be embedded into IP-based transmission suitable for 5G, as shown in Figure 2. Improvements at the transport layer and network layer are made to support deterministic communication, such as adopting Software Defined Networking (SDN) strategies or Time-Sensitive Networking (TSN) coverage. The 5G stack at the physical and link layers can utilize channel state information, adjust coding and modulation rates, schedule wireless resources, etc., to ensure low latency and ultrahigh reliability for certain traffic [17]. Through the modification of these protocols, 5G can achieve high reliability, low latency, and strong isolation service characteristics, surpassing the performance of traditional Wi-Fi systems or previous networks [18].

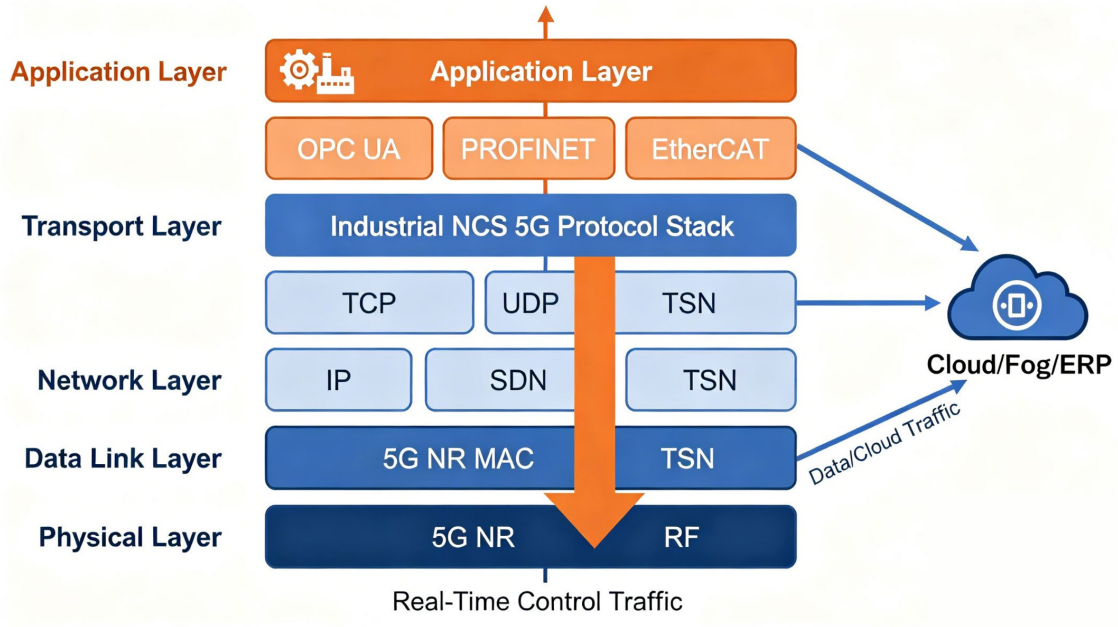

Figure 2. Protocol stack adaptation and data flow for industrial NCS over 5G URLLC, showing application-to-physical layer mapping and real-time data exchange pathways

Latency and Reliability Modeling

To achieve deterministic objectives for industrial NCS in wireless networks, it is necessary to establish models that include availability and latency. Industrial automation workloads are more susceptible to short-term fluctuations than general mobile broadband. Command errors or data reading delays can lead to process instability and resource waste. Provide an overview that breaks down the system response time into several main components. These include actuator delay, sensor delay, communication delay (including wireless access, routing technology, and core transmission), and queuing and processing delays at edge and fog nodes [19]. Each component is minimized, with statistical limits set to meet the closed-loop control standards and the time-critical requirements of industrial applications.

The wireless interface delay issue in 5G ULLC is more severe because wireless transmission usually involves multiple paths, fading, and noise variations. The latest 5G systems use dynamic link adaptation mechanisms to address this issue, shortening the packet length and improving HARQ success rates [20]. In terms of reliability, the number of successfully sent data packets is not the only metric. The end-to-end packet loss rate and data corruption rate should be kept within an acceptable range, with an error rate not exceeding 1% per ten thousand transmissions under safety requirements. To ensure operational consistency between distributed devices, strict synchronization is required. To achieve precise time management, implement network-based time supply [21].

There are also redundancy measures. For example, using multiple serial radio waves to transmit critical information; using spatial diversity technology, which enhances the effect Through multiple antennas or different frequency bands [22]. The 5G network's five-point radio resource management supports these design options. According to different industry categories and security levels, service quality parameters are precisely allocated Through multiple interfaces. Reliability and latency models serve as quantitative reference standards for adjusting design parameters, based on real-time performance observations during operation, such as maintenance personnel reports.

Mathematical Formulation of System Performance

A detailed study on how to quantify each aspect Through in-depth examination. For the enhanced 5G URLLC NCS, key performance indicators (KPIs) include end-to-end latency, packet loss rate, control accuracy, system resilience to interference, redundancy, and security. Each delay link in the system, including the sensor data acquisition and preprocessing stages, contains unstable parameters that need to be precisely adjusted during the experimental validation process [23].

Re-evaluation emphasizes the ability to clearly transmit all data within a limited time. The issues with communication hardware and wireless interface design are the causes of this problem. The protocol stack, buffer management strategies, and the redundant structures designed simultaneously at both levels are also contributing factors to this issue. Various metrics of the control system, including steady-state error, maximum overshoot, recovery time after disturbances, and sensitivity to packet loss or reordering, are all used to evaluate its performance. The certification of the system architecture, anti-attack measures, and data integrity protection design have already taken security requirements into account, especially those related to networked industrial control systems.

Security and Reliability Analysis

Attack Surfaces and Threat Modeling

Establishing 5G-based auxiliary control system networks in industrial applications increases security risks, with physical and logical vulnerabilities emerging one after another. Attacks may occur on devices and can be carried out Through wireless connections, Wi-Fi network stacks, or applications, which threaten system availability and data integrity [24]. Network intrusions can use interference, deception, and other methods; DDoS attacks and man-in-the-middle attacks are common types of cybersecurity attacks.

Establish a probabilistic model to determine which potential risks are more likely or cannot be effectively avoided in real life:

$$P_{attack} = 1 - \prod_{i=1}^{n} (1 - p_i \cdot v_i) \quad \text{Eq.(1)}$$

where p_i is the probability of the i-th attack vector being attempted, and v_i is the vulnerability exploitation probability for each vector. By using this method, overall risks can be assessed and appropriate resources can be allocated to mitigate issues [25]. With the increase in the level of industrialization, automated systems are monitoring vulnerabilities in real-time, ensuring timely repairs, and maintaining a multi-layered security defense structure is becoming increasingly complex. Threat intelligence and vigilance are immediate responses to threats.

To capture the complexity of multi-layer industrial 5G NCS security, we extend the above probabilistic threat model by incorporating both temporal dynamics and interdependent security controls. Suppose the system is defended by K sequential security mechanisms (e.g., anomaly detection, authentication, encryption, access control), each with time-varying detection/mitigation probability $\alpha_k(t)$. The time-dependent probability that an attack evades all defenses and leads to compromise within time interval $[0, T]$ can be expressed as:

$$P_{compromise}(T) = 1 - \prod_{k=1}^{K} \left[1 - \int_0^T p_k(t) \cdot (1 - \alpha_k(t)) dt \right] \quad \text{Eq.(2)}$$

where $p_k(t)$ is the instantaneous probability that the k-th attack vector is active at time t, and $\alpha_k(t)$ denotes the efficacy of the corresponding defense at that instant. This framework allows for modeling not only static risks, but also the impact of adaptive threats and evolving countermeasures in real industrial operation.

To reflect interdependencies and cascading effects-common in industrial networks-a Bayesian network can further encode conditional probabilities between attack paths and corresponding mitigations. For systemically important assets, the expected risk across correlated vectors i with conditional weights w_i is given by

$$R_{asset} = \sum_{i=1}^{n} w_i \cdot p_i \cdot v_i \cdot (1 - m_i) \quad \text{Eq.(3)}$$

where each $m_i \in [0,1]$ is the mitigation effectiveness for attack vector i. The weighting factor w_i quantifies the relative impact of each attack path on the critical asset, supporting nuanced, asset-centric risk evaluation.

Finally, to assess the time-evolution of risk following an initial breach and during incident response, we define the transient risk function:

$$\mathcal{R}(t) = \int_0^t \lambda(\tau) \cdot [1 - \mu(\tau)] d\tau \quad \text{Eq.(4)}$$

where $\lambda(\tau)$ is the attack attempt rate over time and $\mu(\tau)$ represents cumulative mitigation success up to time τ. This integral expresses the residual risk exposure as a function of both attack intensity and progressive defensive actions, which is particularly relevant to industrial environments with continuous monitoring and adaptive security orchestration.

These advanced analytic formulations provide a rigorous foundation for comprehensive security posture evaluation, enabling prioritized, data-driven defense strategies even in the presence of highly dynamic cyber-physical risk landscapes.

Reliability Modeling and Robustness

Model the random characteristics of wireless channel properties and industrial factory operation constraints to ensure high reliability of industrial NCSS in 5G networks. In a strict control loop environment, imbalanced loads and variations can lead to packet loss and delay tails.

The reliability under variable delay can be described by the following probability: When t exceeds another given limit T within a certain period, it will not exceed the maximum allowed duration $D_{\max}$. Assuming the transmission segments are independent, the Central Limit Theorem can be used to approximate the probability of delay violations:

$$Pr\left(\sum_{i=1}^{N} T_i > D_{max}\right) = 1 - \Phi\left(\frac{D_{max} - \sum_{i=1}^{N} \mu_i}{\sqrt{\sum_{i=1}^{N} \sigma_i^2}}\right) \quad \text{Eq.(5)}$$

where T_i denotes delay in segment i, with mean μ_i and variance σ_i^2; Φ is the cumulative distribution function of a standard normal distribution.

Apart from the traditional up and down states, important indicators of system availability can be enhanced Through a certain degree of service level degradation. In higher-level models, the steady-state availability of the three-state Markov chain is as follows:

$$A = \frac{\lambda_{RD}}{\lambda_{DR} + \lambda_{RF}} \cdot \frac{\mu_F}{\lambda_{RF} + \mu_F} + \frac{\lambda_{DF}}{\lambda_{DR} + \lambda_{DF}} \cdot \frac{\mu_F}{\lambda_{DF} + \mu_F} \quad \text{Eq.(6)}$$

Here, $\lambda_{RD}, \lambda_{DR}, \lambda_{RF}$, and λ_{DF} are transition rates among Normal (R), Degraded (D), and Failure (F) states, while μ_F is the failure recovery rate. Achieved performance smoothing and redundancy degradation in high-end 5G systems [27].

Ensure system robustness Through health monitoring systems, dynamic resource allocation, and rapid fault recovery measures. Queueing theory and Markov chains can predict the reliability of the system under normal operation or stress. Ensure that these objectives can be achieved in actual industrial environments [28].

To further refine quantitative reliability assessment of industrial 5G NCS, we consider several advanced stochastic modeling approaches:

First, the instantaneous reliability function $R(t)$, describing the probability that the system operates without failure up to time t, for a system with failure rate $\lambda(t)$, is given by:

$$R(t) = exp\left(-\int_0^t \lambda(\tau)d\tau\right) \quad \text{Eq.(7)}$$

This formulation naturally accommodates time-varying failure rates due to changes in load, interference, or environmental stress, which are prevalent in smart factory settings.

Next, for systems modeled by a Weibull lifetime distribution (a standard in industrial reliability engineering), the reliability is:

$$R(t) = exp\left[-\left(\frac{t}{\eta}\right)^{\beta}\right] \quad \text{Eq.(8)}$$

where η is the scale parameter related to characteristic lifetime, and β is the shape parameter reflecting failure behavior: $\beta < 1$ for infant mortality, $\beta = 1$ for exponential failures, and $\beta > 1$ for wear-out.

Further, for multi-component systems, the overall system reliability R_{system} under the assumption of independent components and a series structure can be calculated by:

$$R_{system}(t) = \prod_{j=1}^{m} R_j(t) \quad \text{Eq.(9)}$$

where $R_j(t)$ is the reliability of the j-th critical subsystem.

For repairable systems (common in 5G NCS with rapid failover/recovery), the steady-state availability A_{ss} can also be formulated as:

$$A_{ss} = \frac{\mu}{\lambda + \mu} \quad \text{Eq.(10)}$$

where λ and μ are the failure and repair rates, respectively. This Markovian approach highlights the importance of rapid recovery mechanisms and is directly applicable to redundancy-enabled industrial wireless architectures.

Finally, to address queueing-induced delay instability in real-time control, the probability that the queue length $Q(t)$ exceeds a threshold during peak load can be expressed via large deviations theory:

$$Pr(Q(t) > q_0) \approx exp\,(-\theta^* q_0) \quad \text{Eq.(11)}$$

where θ^* is the decay rate parameter reflecting system service and arrival dynamics.

These advanced reliability formulations, in combination with empirical measurements, enable comprehensive analysis of both routine operational metrics and rare-event risks in industrial grade 5G NCS deployments.

Security Strategies and Data Protection

To ensure the security of industrial 5G NCS deployment, a multi-layered defense approach is required, including device authentication, communication confidentiality and integrity protection, and resistance to persistent attacks. Combining trusted hardware with strong two-way authentication protocols, many avenues for forgery or deception are closed off.

Strong authentication encryption ensures end-to-end confidentiality and integrity; strict management of long-lifecycle keys; accurate execution of context-adaptive access control. By combining the formal assessment of risk models, this mechanism can link the overall system failure rate with the protection layer:

$$P_{compromise} = \sum_{l=1}^{L}\left(P_{bypass,l}\prod_{m=1}^{l-1}\left(1 - P_{bypass,m}\right)\right) \quad \text{Eq.(12)}$$

Here, L denotes the number of defense layers; $P_{\text{bypass, }l}$ is the probability an adversary successfully bypasses the l-th security layer, contingent on having failed at all previous layers. To support the quantitative analysis of deep defense, it is indicated that as the maturity and number of defense layers increase, system risk decreases.

Safe industrial deployments often use fine-grained anomaly detection techniques to test the ability to detect small anomalies. By increasing cross-domain redundancy and multi-path authentication transmission, explicitly

strengthen data integrity protection. Through majority voting and supervision, the upper limit on the likelihood of vulnerable nodes introducing undiscovered erroneous commands is as follows:

$$P_{undetected} = \sum_{k=\left\lceil \frac{M+1}{2} \right\rceil}^{M} \binom{M}{k} p^k (1-p)^{M-k} \quad \text{Eq.(13)}$$

M represents the number of verification or independent monitoring sites, and p represents the failure or compromise rate of each monitor. When choosing a redundancy structure, the formula provides specific risk metrics for redundancy designers.

The overall integrity probability of data packets transmitted via multiple paths is as follows:

$$P_{integrity} = 1 - \prod_{k=1}^{M} \left[1 - \left(P_{enc,k} \cdot P_{auth,k} \cdot P_{path,k}\right)\right] \quad \text{Eq.(14)}$$

where $P_{\text{enc},k}$ and $P_{\text{auth},k}$ specify the per-path encryption and authentication success rates, and $P_{\text{path},k}$ the probability of correct delivery.

Simulation and Experiments

Security Testbeds and Assessment

A segmented cyber-physical test bed was built for evaluating the security foundation of 5G-enhanced industrial NCS. The experimental system is a combination of the two types: it can control to inject different threats, including DDoS attack, fake information and so on. Furthermore, the test bed offered a realistic setting for evaluating Intrusion Detection Systems (IDSs) and Adaptive Protocols.

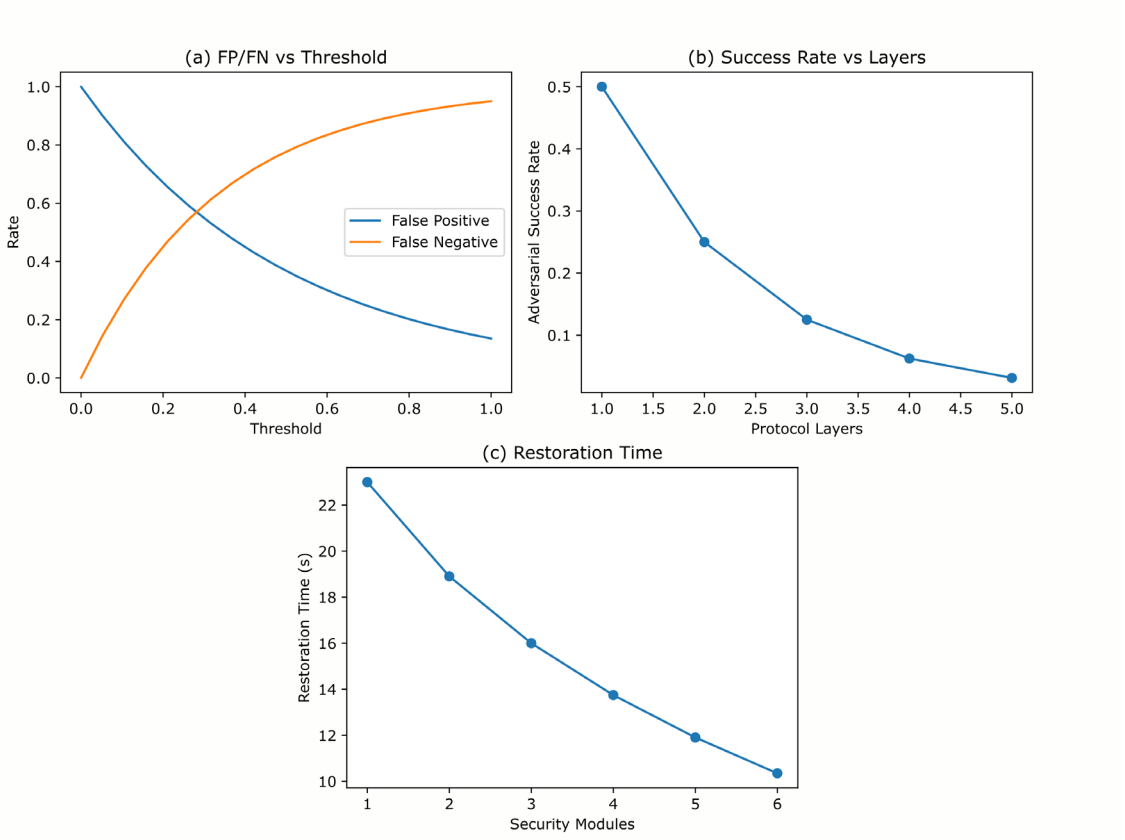

Figure 3. Security test results: (a) IDS false positive and false negative rates versus threshold; (b) Adversarial success rate with cumulative protocol defenses; (c) Restoration time versus number of security layers

Initially, aiming to balance the rate of false negatives and false positives under an industrial safety limit through adjustment of the threshold for IDS. Based on a thorough study of various norms, these have all been deemed prudent choices for mitigating operational risks at the time required to be adhered to continuously thereafter. Illustrated by Figure 3a is the trade-off and optimised result curves.

At the protocol level, advanced security functions have been added sequentially: Mutual Authentication, Session Encryption, automatic Key Renewal. Each addition increased this vulnerability by a certain degree; thus, using a testing platform can quantify the residual adversary attack probability after increasing layers. Figure 3b shows these stage-by-stage improvements explicitly as the accumulation of benefits achieved by employing a comprehensive defence approach.

Another relatively obvious result of these test experiments is that the influence of security integration on system restoration. According to the research findings, by adding a larger number of protective measures, we can definitely shorten the time required for post-attack or faulty device rehabilitation work significantly. Smore complex alerting, redundancy, and automatic response capabilities increased non-linearly the improvement in system performance; Timely Recovery is relatively more feasible at this stage of high-level safety protection. The summary is shown as Figure 3c.

In addition to the analysis mentioned above, the security experiment also tested a series of higher-scenario responses: detecting sensitivity for new attack signatures; Average time it took for threats to be resolved in the 5G industrial setting; Source identification accuracy. In Figures 4 and above, summarised data from expanded tests provide a complete set of quantified evidence for the adaptive-robustness properties of the installed security system.

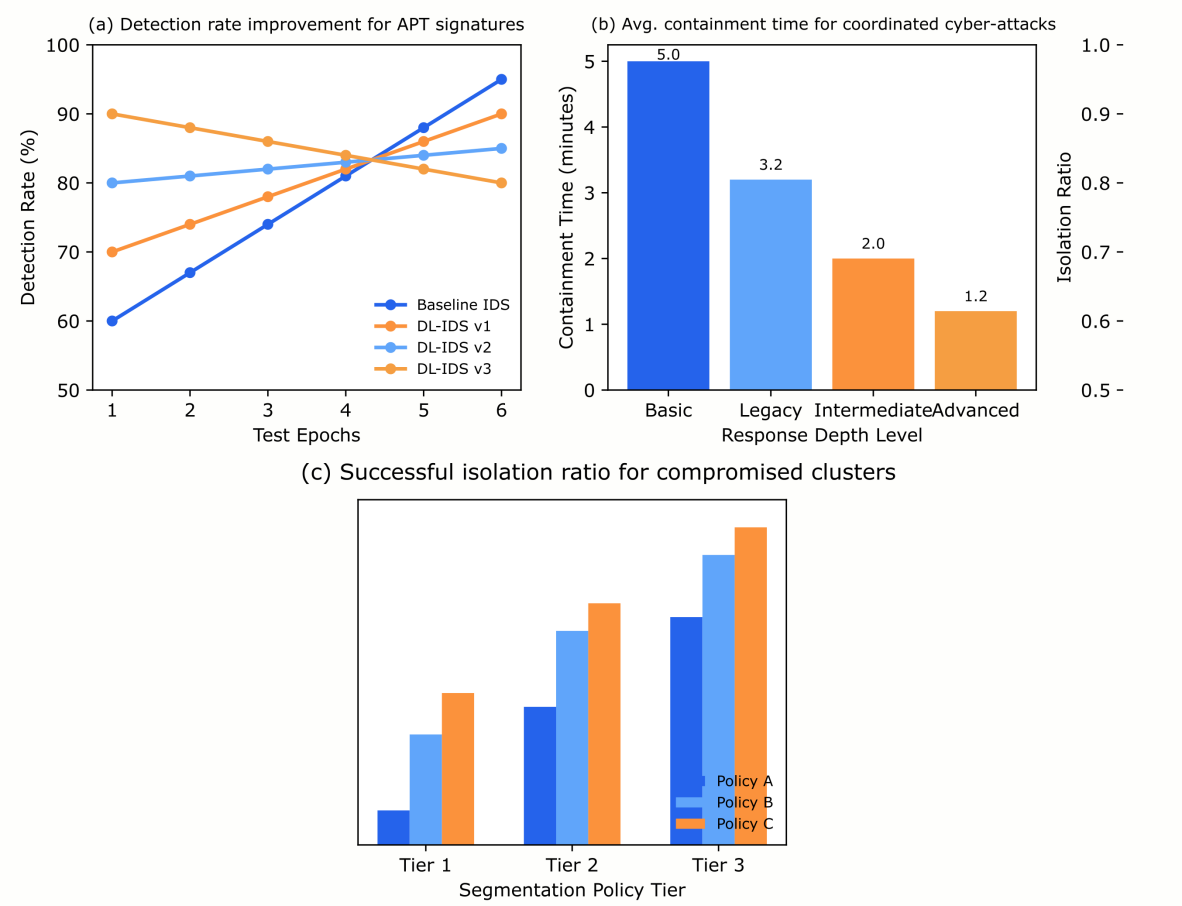

Figure 4. Multi-level security defense evaluation in industrial 5G NCS: (a) Detection rate improvement for advanced persistent threat signatures under deep learning-based IDS; (b) Average containment time for coordinated cyber-attacks as a function of automated incident response depth; (c) Successful isolation ratio for compromised device clusters after policy-based network segmentation

Reliability Benchmarking and Data Analysis

To conduct in-depth research on the reliability of 5G-supported industrial network control systems, establish a large-scale, highly flexible simulation system. Establish a simulation framework to model various real-world production scenarios. These situations include various network topologies, changes in wireless propagation environments, device mobility factors, and heterogeneous service demands. A comprehensive examination of system and environmental parameters is conducted to ensure the significance of the evaluation. The checks include topology prototypes, the number of nodes, packet sizes, channel fading statistics, mobility patterns, average data load rates, and error control schemes. Table 1 contains a systematic summary of the main parameters, set values, and range values for all tests.

Table 1. Simulation parameters for 5G NCS reliability evaluation: Simulation scenarios, principal system parameters, and their value ranges. All settings are designed to support result replication and ensure industrial-grade repeatability

Parameter	Value/Range	Description
Topology Type	"Linear; Star; Mesh"	"Network connection pattern"
Number of Nodes	"10-200"	"Total devices in the simulated network"
Packet Size	"64-1500 Bytes"	"Application layer message size"
Channel Fading Model	"Rayleigh; Rician"	"Wireless environment type"
Mobility Pattern	"Static; Random Waypoint; Group Mobility"	"Device movement model"
Offered Traffic Load	"0.1-1.5 Mbps per node"	"Traffic per device"
Error Control Scheme	"ARQ; Hybrid-ARQ"	"Retransmission or error correction method"
Latency Threshold	"1 ms; 10 ms; 50 ms (per test)"	"Industrial delay requirement"
Redundancy Strategy	"None; Dual-connectivity; multi-path"	"Data path protection"
Security Feature	"None; Authentication; Encryption"	"Security configuration"
Simulation Duration	"60-600 seconds"	"Total simulated test time"

Simulation scenarios, principal system parameters, and their value ranges. All settings are designed to support result replication and ensure industrial-grade repeatability.

The analysis initially centered on real-time performance, which is essential for industrial NCS. For each combination of network and traffic configuration, the cumulative latency distribution was measured and compared against expected industrial deadlines. Results illustrated that, even as node density scaled or the system was exposed to network surges and complex environments, measured latency violation rates remained acceptably low. This affirms that 5G infrastructures, when properly dimensioned, can consistently deliver deterministic response times for time-critical automation tasks. As illustrated in Figure 5a, empirical data closely tracked theoretical expectations, validating the effectiveness of the network architecture under stress.

In addition, throughput was analyzed with respect to differentiated industrial traffic classes, including latency-sensitive control flows, sensor data, and background bulk transfers. Experiments revealed clear thresholds at which system throughput moved from stable operation to congestion, and further showed that optimized retransmission schemes could successfully mitigate packet loss without undermining latency. Alignment between empirical results and theoretical operating limits showcases the importance of protocol-level tuning for maximum utilization, as depicted in Figure 5b.

Physical-layer reliability was also thoroughly investigated. Simulations measured how packet error rates varied under diverse channel fading conditions, like Rayleigh and Rician environments, and under the influence of cross-layer error correction. Results demonstrated that, with the 5G stack's adaptive mechanisms, packet errors were kept at a minimum—even in highly variable or harsh propagation scenarios. These results, presented in Figure 5c, highlight both the robustness and efficiency of joint optimization strategies across protocol and physical layers.

Collectively, these findings underscore the ability of 5G-enabled NCS platforms to meet the highest benchmarks for reliability and responsiveness, even in dense or rapidly changing industrial deployments.

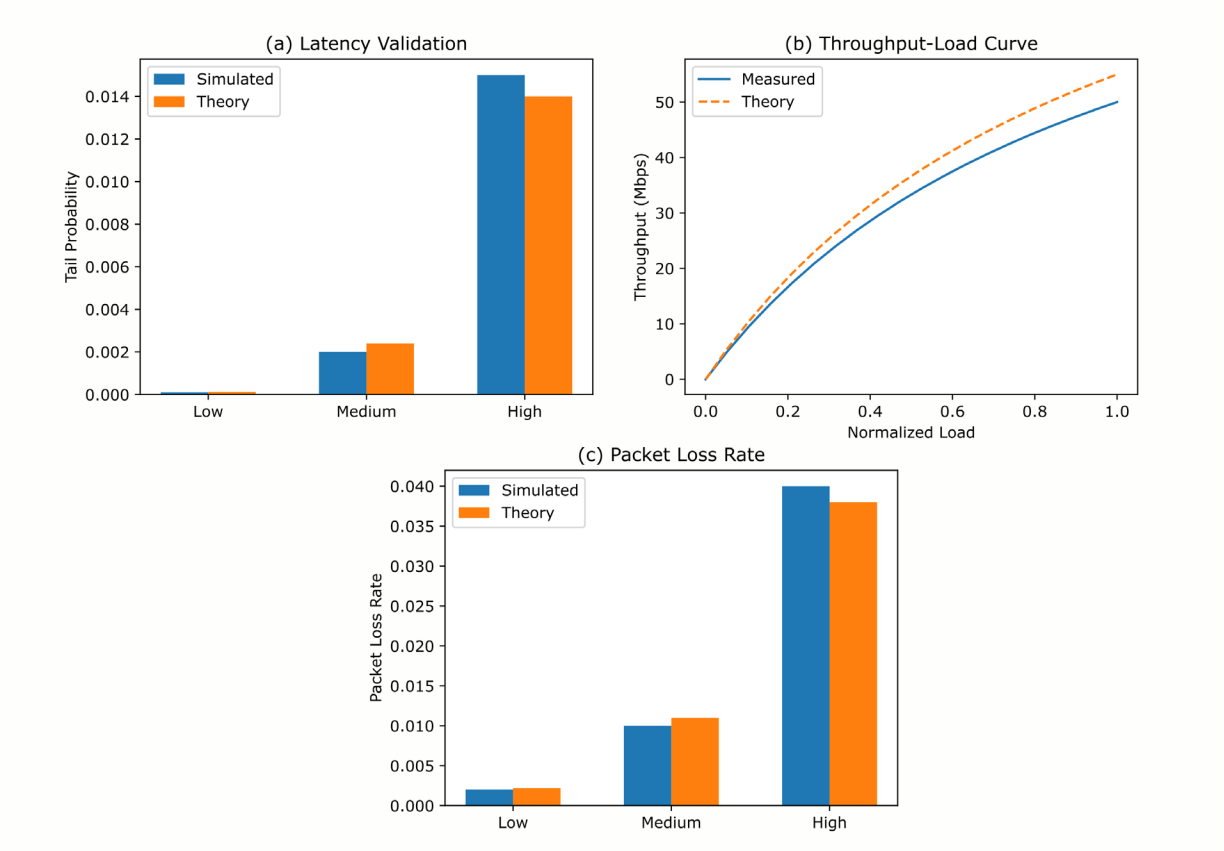

Figure 5. Network performance benchmarking: (a) Mean latency validation under diverse industrial scenarios, comparing analytical violation probability with simulated results; (b) Throughput-load curve for prioritized and heterogeneous traffic, showing precise alignment with theoretical saturation points; (c) Analytical and empirical packet loss rates under variable interference and mobility conditions

Performance Visualization and Comparative Results

To holistically evaluate system effectiveness, performance metrics were visualized across several representative industrial dimensions: scalability, control precision, and aggregate utility based on key performance indices.

The scalability analysis measured system throughput as a function of increasing connected device count. Data showed that, while legacy wireless systems suffered rapid throughput degradation under high device numbers, 5G-enabled NCS maintained robust capacity with only gradual decline, indicating high tolerance for densification. These comparative results are clearly depicted in Figure 6a, where the distinction between 5G and conventional wireless approaches is evident.

Further, the effect of communication reliability on process control accuracy was rigorously investigated using both simulation and modeling. As shown in Figure 6b, the mean squared error (MSE) of critical manufacturing variables remained tightly bounded within industry limits for the 5G NCS, even under stressed wireless conditions or high endpoint counts. In contrast, traditional Wi-Fi and pre-5G networks failed to maintain control performance in challenging environments, underscoring the technological leap provided by advanced 5G solutions.

In order to present an integrated assessment, multiple key performance indicators (KPIs)—including latency, reliability, control precision, and scalability—were normalized and aggregated into a composite utility score. Visualization in both radar and bar-plot formats (Figure 6c) highlighted the superior, balanced performance of industrial 5G NCS across all criteria when compared to competing platforms.

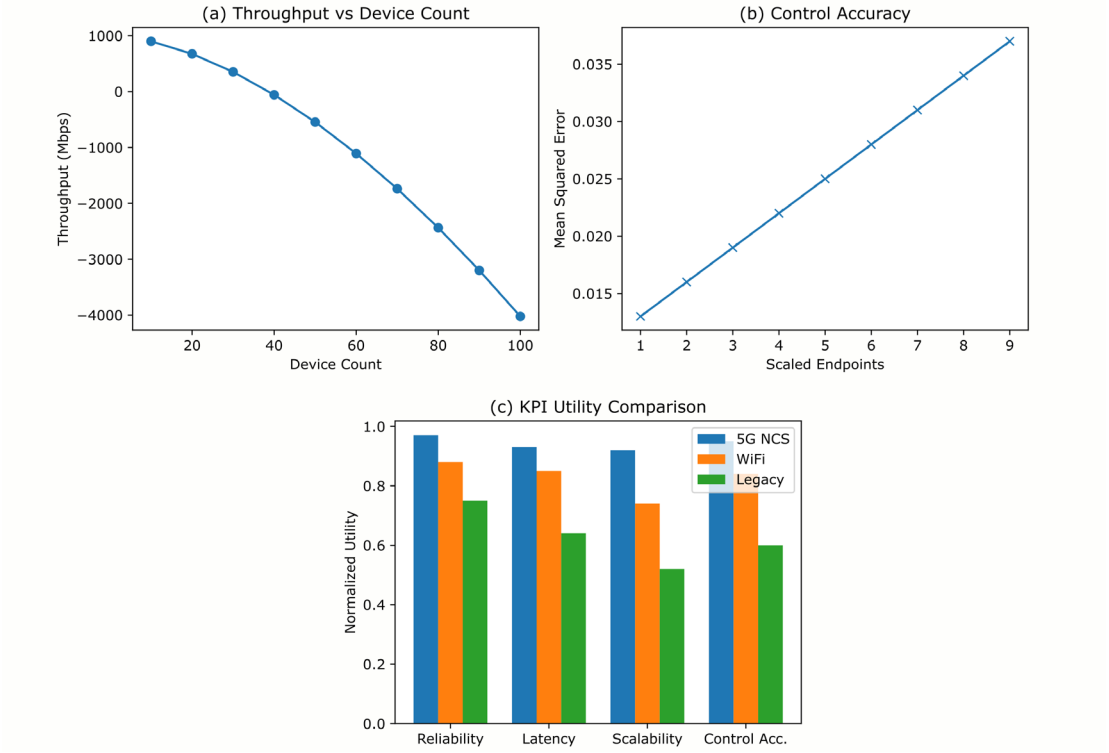

Figure 6. System scalability and overall performance: (a) Throughput versus device count for 5G NCS, Wi-Fi, and legacy wireless; (b) Control accuracy (mean squared error) under scaling and wireless variation; (c) Normalized KPI utility comparison across network schemes

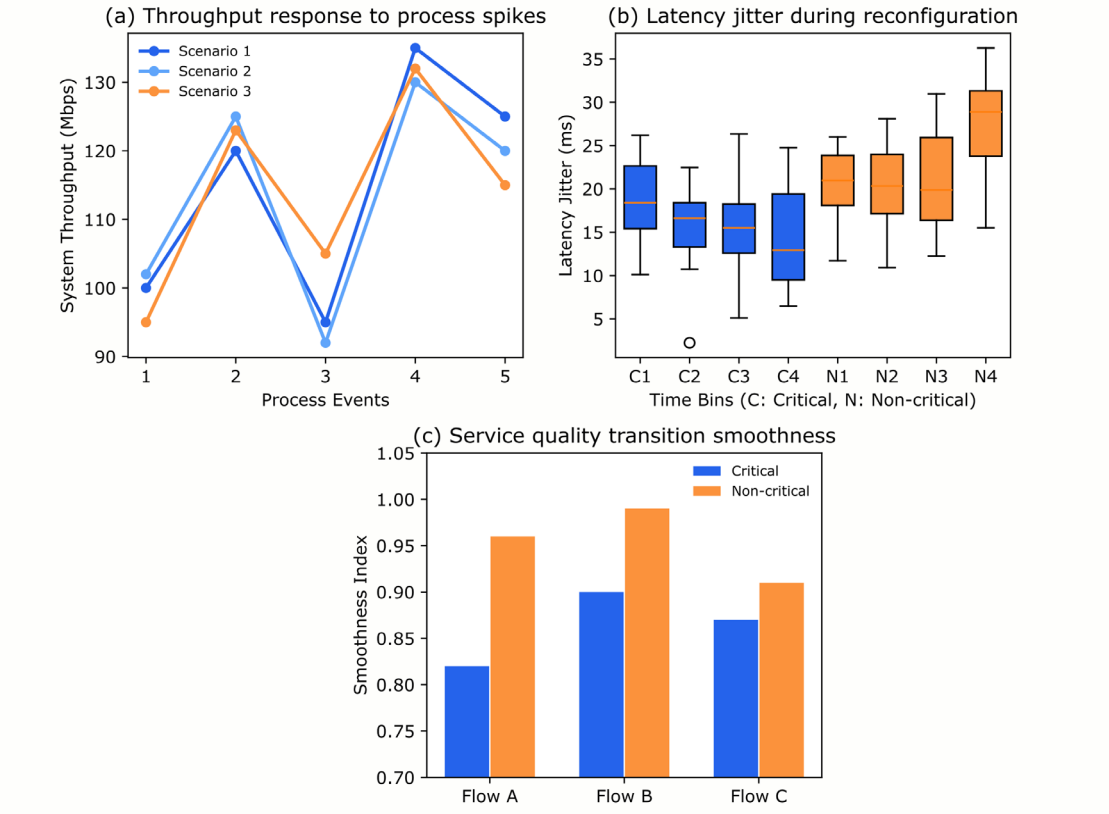

Figure 7. Robustness and adaptability of 5G NCS under operational dynamics: (a) System throughput response to abrupt increases in process demand; (b) Latency jitter trends during live firmware upgrades and network slicing reconfiguration; (c) Service quality transition smoothness for critical versus non-critical data flows during industrial event surges

In addition to the main system benchmarks, the platform's performance was also evaluated under a diverse set of advanced industrial scenarios, including variable industrial load conditions, rapid service quality transitions, and sudden traffic burst events. To simulate real-world fluctuation in demand, the test environment was subjected to dynamically changing loads that mirrored peak and off-peak manufacturing cycles, revealing how the NCS adapts its scheduling and maintains operational stability. Furthermore, abrupt shifts in service quality requirements—such as instantaneous prioritization of critical control packets or seamless downgrade of non-essential services—were introduced to assess the system's agility in enforcing differentiated quality-of-service policies. The experiments also incorporated traffic burst scenarios, simulating unexpected surges in communication requests due to process upsets or coordinated operational tasks, in order to evaluate both short-term system responsiveness and the ability to prevent congestion collapse. The comprehensive results of these advanced testing scenarios, summarized in Figure 7, showcase the remarkable resilience and adaptability of the 5G NCS in sustaining stable service quality and rapid responsiveness even when continuously exposed to sudden operational fluctuations, reconfiguration demands, and highly dynamic industrial environments. These findings underscore the platform's effectiveness in ensuring reliable production automation in the face of unpredictable and challenging conditions.

Conclusion

This study provides theoretical and empirical evidence Through an in-depth investigation of the reliability and security of 5G-enabled network control systems in industrial applications. To more accurately assess and rank risks in industrial environments, a multifaceted probabilistic threat model is proposed, based on different dimensions of the attack surface of cyber-physical systems. Based on empirical observations and advanced analytical techniques, the model achieves highly accurate predictions of real-world environmental performance by demonstrating the complex interactions between wireless channel dynamics, adaptive protocol behavior, and strict control loop cutoff times.

The results indicate that a layered strategy is needed here to address potential threats. Based on trusted device authentication and strong encryption; multiple paths to detect data integrity errors; continuous monitoring of environmental attack activities to effectively reduce the risk of system breaches. Repeat at the redundancy level to ensure the reliability of operational data, maintaining system stability during monitoring conditions and inspection processes.

Reliability indicates that 5G-NCS can meet the high reliability requirements for ultra-reliable low-latency communication in modern industrial automation environments Through reasonable network planning, dynamic resource adjustment, and early error intervention. Detailed modeling shows that with changes in the number of devices, mobility, and traffic, throughput, latency, and system availability can still remain stable.

With the integration of advanced network orchestration technologies such as SDN, NFV, and MEC, the scalability and forward compatibility of future industrial system evolution will be ensured. Reference guide for industrial users, system designers, and security experts to deploy reliable and secure 5G network control systems in the future. Based on this, conduct innovative research to support the more stable operation of connected devices taking the lead.

Author Contributions

Jakub Grzegorz Zieliński and Damian Piotr Dąbrowski contribute to conceptualization, methodology, software, validation, analysis, investigation, data collection, draft preparation, manuscript editing, visualization, supervision, project administration, and funding acquisition. All authors have read and agreed with the manuscript before its submission and publication.

Funding

This research received no specific financial support from any funding agency.

Institutional Review Board Statement

Not applicable.

References

[1] Mourtzis, D., Angelopoulos, J., & Panopoulos, N. (2021). Smart manufacturing and tactile internet based on 5G in industry 4.0: Challenges, applications and new trends. Electronics, 10(24), 3175. https://doi.org/10.3390/electronics10243175

[2] Sharma, M., Tomar, A., & Hazra, A. (2024). Edge computing for industry 5.0: Fundamental, applications, and research challenges. IEEE Internet of Things Journal, 11(11), 19070-19093. https://doi.org/10.1109/JIOT.2024.3359297

[3] Kilpi, J., Kokkoniemi-Tarkkanen, H., & Uusitalo, M. A. (2021, April). Efficient method to validate high reliability of 5G URLLC. In 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring) (pp. 1-6). IEEE. https://doi.org/10.1109/VTC2021-Spring51267.2021.9448734

[4] Chang, B., Zhang, L., Li, L., Zhao, G., & Chen, Z. (2019). Optimizing resource allocation in URLLC for real-time wireless control systems. IEEE Transactions on Vehicular Technology, 68(9), 8916-8927. https://doi.org/10.1109/TVT.2019.2930153

[5] Cardona, N., Coronado, E., Latre, S., Riggio, R., & Marquez-Barja, J. M. (2020). Software-defined vehicular networking: Opportunities and challenges. IEEE Access, 8, 219971-219995. https://doi.org/10.1109/ACCESS.2020.3042717

[6] Hamidi-Sepehr, F., Sajadieh, M., Panteleev, S., Islam, T., Karls, I., Chatterjee, D., & Ansari, J. (2021). 5G URLLC: Evolution of high-performance wireless networking for industrial automation. IEEE Communications Standards Magazine, 5(2), 132-140. https://doi.org/10.1109/MCOMSTD.001.2000035

[7] Li, K., Zhu, P., Wang, Y., Wang, J., & You, X. (2023). Cross-layer resource allocation for URLLC industrial automation over multi-connectivity. IEEE Transactions on Wireless Communications, 23(7), 7334-7348. https://doi.org/10.1109/TWC.2023.3339716

[8] Humayun, M., Jhanjhi, N. Z., Alruwaili, M., Amalathas, S. S., Balasubramanian, V., & Selvaraj, B. (2020). Privacy protection and energy optimization for 5G-aided industrial Internet of Things. Ieee Access, 8, 183665-183677. https://doi.org/10.1109/ACCESS.2020.3028764

[9] Liu, W., Kong, C., Niu, Q., Jiang, J., & Zhou, X. (2020). A method of NC machine tools intelligent monitoring system in smart factories. Robotics and computer-integrated manufacturing, 61, 101842. https://doi.org/10.1016/j.rcim.2019.101842

[10] Guo, Q., Tang, F., & Kato, N. (2022). Federated reinforcement learning-based resource allocation for D2D-aided digital twin edge networks in 6G industrial IoT. IEEE Transactions on Industrial Informatics, 19(5), 7228-7236. https://doi.org/10.1109/TII.2022.3227655

[11] Ansari, J., Andersson, C., de Bruin, P., Farkas, J., Grosjean, L., Sachs, J., ... & Schmitt, R. H. (2022). Performance of 5G trials for industrial automation. Electronics, 11(3), 412. https://doi.org/10.3390/electronics11030412

[12] Zhao, S. (2023). Energy efficient resource allocation method for 5G access network based on reinforcement learning algorithm. Sustainable Energy Technologies and Assessments, 56, 103020. https://doi.org/10.1016/j.seta.2023.103020

[13] John, J., Noor-A-Rahim, M., Vijayan, A., Poor, H. V., & Pesch, D. (2024). Industry 4.0 and beyond: The role of 5G, WiFi 7, and time-sensitive networking (TSN) in enabling smart manufacturing. Future Internet, 16(9), 345. https://doi.org/10.3390/fi16090345

[14] Walia, J. S., Hämmäinen, H., Kilkki, K., & Yrjölä, S. (2019). 5G network slicing strategies for a smart factory. Computers in industry, 111, 108-120. https://doi.org/10.1016/j.compind.2019.07.006

[15] Abbas, S. G., Hashmat, F., & Shah, G. A. (2020, December). A multi-layer industrial-IoT attack taxonomy: Layers, dimensions, techniques and application. In 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (pp. 1820-1825). IEEE. https://doi.org/10.1109/TrustCom50675.2020.00249

[16] Filali, A., Abouaomar, A., Cherkaoui, S., Kobbane, A., & Guizani, M. (2020). Multi-access edge computing: A survey. IEEE Access, 8, 197017-197046. https://doi.org/10.1109/ACCESS.2020.3034136

[17] Afolabi, I., Taleb, T., Samdanis, K., Ksentini, A., & Flinck, H. (2018). Network slicing and softwarization: A survey on principles, enabling technologies, and solutions. IEEE Communications Surveys & Tutorials, 20(3), 2429-2453. https://doi.org/10.1109/COMST.2018.2815638

[18] Cheng, J., Chen, W., Tao, F., & Lin, C. L. (2018). Industrial IoT in 5G environment towards smart manufacturing. Journal of Industrial Information Integration, 10, 10-19. https://doi.org/10.1016/j.jii.2018.04.001

[19] Jiang, X., Pang, Z., Luvisotto, M., Candell, R., Dzung, D., & Fischione, C. (2020). Delay optimization for industrial wireless control systems based on channel characterization. IEEE Transactions on Industrial Informatics, 16(9), 5855-5865. https://doi.org/10.1109/TII.2019.2958708

[20] Wazid, M., Das, A. K., Shetty, S., Gope, P., & Rodrigues, J. J. (2020). Security in 5G-enabled internet of things communication: issues, challenges, and future research roadmap. IEEE access, 9, 4466-4489. https://doi.org/10.1109/ACCESS.2020.3047895

[21] Guo, P., Liu, M., Wu, J., Xue, Z., & He, X. (2018). Energy-efficient fault-tolerant scheduling algorithm for real-time tasks in cloud-based 5G networks. IEEE Access, 6, 53671-53683. https://doi.org/10.1109/ACCESS.2018.2871821

[22] Haque, M. E., Tariq, F., Khandaker, M. R., Wong, K. K., & Zhang, Y. (2023). A survey of scheduling in 5G URLLC and outlook for emerging 6G systems. IEEE access, 11, 34372-34396. https://doi.org/10.1109/ACCESS.2023.3264592

[23] Lin, C. C., Tsai, C. T., Liu, Y. L., Chang, T. T., & Chang, Y. S. (2023). Security and privacy in 5g-iiot smart factories: Novel approaches, trends, and challenges. Mobile Networks and Applications, 28(3), 1043-1058. https://doi.org/10.1007/s11036-023-02143-5

[24] Mannhardt, F., Petersen, S. A., & Oliveira, M. F. (2019). A trust and privacy framework for smart manufacturing environments. Journal of Ambient Intelligence and Smart Environments, 11(3), 201-219. https://doi.org/10.3233/AIS-19052

[25] Sefati, S. S., & Halunga, S. (2023). Ultra-reliability and low-latency communications on the internet of things based on 5G network: literature review, classification, and future research view. Transactions on emerging telecommunications technologies, 34(6), e4770. https://doi.org/10.1002/ett.4770

[26] Zhao, S., Yanhong, Y., & Fan, Y. (2024, June). Enhancing Efficiency and Reliability with 5G Digital Twin Technology in Power Substations. In International Conference on Information Processing and Network Provisioning (pp. 302-313). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-96-6462-7_27

[27] Kou, L., Ding, S., Rao, Y., Xu, W., & Zhang, J. (2022). A lightweight intrusion detection model for 5G-enabled industrial internet. Mobile Networks and Applications, 27(6), 2449-2458. https://doi.org/10.1007/s11036-021-01891-6

[28] Khan, A. A., Abolhasan, M., Ni, W., Lipman, J., & Jamalipour, A. (2021). An end-to-end (E2E) network slicing framework for 5G vehicular ad-hoc networks. IEEE Transactions on Vehicular Technology, 70(7), 7103-7112. https://doi.org/10.1109/TVT.2021.3084735