Security Implications of 5G Communication in Industrial Systems

Stefan Lenz*
lenz@spice.rwth-aachen.de
RWTH Aachen University
Aachen, Germany

Sotiris Michaelides*
michaelides@spice.rwth-aachen.de
RWTH Aachen University
Aachen, Germany

Moritz Rickert
moritz.rickert@rwth-aachen.de
RWTH Aachen University
Aachen, Germany

Jonas Holtwick
jonas.holtwick@rwth-aachen.de
RWTH Aachen University
Aachen, Germany

Martin Henze†
henze@spice.rwth-aachen.de
RWTH Aachen University
Aachen, Germany

Abstract

Traditionally, industrial control systems (ICS) were designed without security in mind, prioritizing availability and real-time communication. As these systems increasingly become targets of powerful adversaries, security can no longer be neglected. Driven by flexibility and automation needs, ICS are transitioning from wired to 5G communication, introducing new attack surfaces and a less reliable communication medium, thereby exacerbating existing security challenges. Given their critical role in society, a comprehensive evaluation of their security is imperative. To this end, we introduce SWICS, a fully virtual testbed simulating an ICS in a realistic 5G environment, and study how this transition affects security under varying channel conditions. Our results show three key findings: under optimal channel conditions, industrial 5G networks can achieve resilience comparable to wired systems, while degraded channel conditions can amplify traditional attacks, threaten system stability, and undermine detection mechanisms based on predictable traffic patterns. We further demonstrate the inherent limits of securing 5G channels for ICS through eavesdropping and jamming on the open-air interface. Our work highlights the interplay between security and 5G channel conditions, showing that traditional security controls may no longer be sufficient and motivating further research.

CCS Concepts

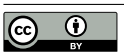
• **Security and privacy → Mobile and wireless security**; • **Networks → Cyber-physical networks**; **Mobile networks**.

Keywords

Security, industrial control systems, wireless communication, 5G

ACM Reference Format:
Stefan Lenz, Sotiris Michaelides, Moritz Rickert, Jonas Holtwick, and Martin Henze. 2026. Security Implications of 5G Communication in Industrial Systems . In *The 11th ACM Cyber-Physical System Security Workshop (CPSS '26), June 01–05, 2026, Bangalore, India.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3775042.3807886

*Both authors contributed equally to this research.
†Also with Fraunhofer FKIE.



CPSS '26, Bangalore, India

ACM ISBN 979-8-4007-2313-1/2026/06
https://doi.org/10.1145/3775042.3807886

1 Introduction

Industry 4.0 and the advent of the Industrial Internet of Things have revolutionized Industrial Control Systems (ICSs), which manage physical processes in manufacturing facilities and critical infrastructure [35]. Traditionally isolated, these control systems have evolved into highly interconnected networks [38]. In addition, security has historically been deprioritized in favor of high availability and reliable real-time communication [38]. However, recent cyberattacks against such systems—e.g., Stuxnet and the attacks on the Ukrainian power grid [34]—have shown that security can no longer be neglected to prevent harm of humans and infrastructure [22, 25, 70].

At the same time, ICSs are undergoing a second major transformation, as rising demands for flexibility and automation drive a shift from wired to wireless communication [11]. While industrial companies have long explored wireless approaches, earlier technologies could not meet stringent operational requirements [48]. Recent advances—most notably 5G with sub-1 ms latencies—make wireless solutions viable for even the most demanding ICSs [4, 6]. As a result, this transition is increasingly materializing in practice [11, 48]. However, despite these advantages, 5G networks complicate ICS security. Communication is now subject to physical-layer effects such as interference and propagation loss, which can impact process stability, weaken existing security controls including isolation strategies and introduce new attack vectors. Consequently, securing such systems has become more challenging than ever, especially as they are increasingly targeted by sophisticated adversaries [34, 48, 65].

To stay ahead of these threats, security must be considered from the outset when designing the next generation of industrial 5G-enabled ICSs, requiring a holistic understanding of how 5G communication affects security, including the effectiveness of existing security controls and the emergence of new attack vectors. To lay the foundation for these efforts, in this paper we provide the first comprehensive study of the security implications of transitioning to 5G in ICSs by (i) evaluating the process stability under attacks, (ii) assessing the effectiveness of existing security measures, and (iii) investigating additional attack vectors on the physical process. This work aims to raise awareness of the security implications of 5G-enabled ICS and stimulate further research toward proactive security design. More specifically, our contributions are:

(1) We develop and open-source SWICS [41], the first virtual and modular security testbed which interconnects industrial components over a realistically simulated 5G network, enabling reproducible research and facilitating future studies.

(2) By replicating well-known network-level attacks, we compare the resilience of 5G-enabled and wired ICSs, showing that the robustness of 5G depends on channel conditions (§5).
(3) By deploying and evaluating two communication-based intrusion detection systems, well-established security controls often used in ICSs, we show that traditional security approaches previously considered sufficient may no longer be effective (§6).
(4) We explore the wireless interface to study passive reconnaissance and jamming attacks, highlighting that disruptions mainly threaten availability—the most critical security aspect of ICSs—to reveal the limitations of 5G in ICS (§7).

Availability: Source code and artifacts are available at github.com/RWTH-SPICe/SWICS and doi.org/10.5281/zenodo.19550997

2 Security of (Wireless) ICSs

To lay the foundation for our work, we introduce the core concepts of ICSs (§2.1) and explain how 5G, with its ability to operate in the mmWave spectrum, enables sub-1 ms latencies (§2.2). We then review prior research on the security implications of 5G in ICSs and show that existing testbeds do not support comprehensive studies of integrating 5G into ICSs, highlighting our contributions (§2.3).

2.1 Industrial Control Systems

Industrial Control Systems (ICSs) form the backbone of modern production and critical infrastructure by linking physical components with digital control and monitoring systems [38]. They are structured into three levels: *fieldbus*, *control*, and *supervisory*. At the fieldbus level, sensors monitor the physical environment and relay process values to the control level, while actuators such as motors or valves receive low-level control signals to directly influence the physical process. Controllers, e.g., Programmable Logic Controllers (PLCs), interpret sensor data and compute the commands that drive these actuators, forming together a continuous sensing–actuation loop known as the process cycle. Controllers also report the current process state to the supervisory level, e.g., a Human-Machine Interface (HMI), enabling humans to oversee and steer operations.

Because of their tight coupling with the physical world, ICSs must meet stringent safety and availability requirements [48], demanding strict network performance guarantees, especially low latency, minimal jitter, and low packet loss [48]. Due to the increasing connectivity of ICSs to the Internet [38], it is more important than ever to develop security measures that do not interfere with these requirements. Thus, to study ICS security, research relies on *testbeds*, i.e., physical or virtual replicas of real systems, to avoid harming actual infrastructure [22]. Unlike physical testbeds, virtual testbeds eliminate the need for expensive hardware, enhance reproducibility, and allow for controlled experiments.

2.2 Wireless Communication in ICSs

Driven by demands for increased automation, flexibility, and efficiency in production and critical infrastructure, ICSs are currently shifting from traditional wired to wireless communication [48]. While several wireless technologies are suitable for industrial use cases, the fifth generation of cellular networks (5G) offers submillisecond latencies, making it particularly promising for industrial applications with strict latency requirements [4, 48].

In contrast to most wireless technologies, 5G comprises three main components: user equipment (UEs), gNodeBs (gNBs), and the Core Network (CN). UEs, such as sensors, PLCs, or HMIs, act as endpoints that generate and consume data, while gNBs provide the radio access interface and connect UEs to the CN, which handles data routing and connection management. Notably, 5G distinguishes between control and user plane traffic: control plane messages, which manage signaling and system operation, are mandatorily integrity protected, whereas user plane traffic (i.e., the industrial data) is not [48]. This distinction has important security implications, as enabling integrity protection for user plane traffic introduces additional overhead that may conflict with stringent sub-millisecond latency requirements [47]. For our analysis of the *wireless* channel in ICSs, we abstract from this architectural complexity and focus on *UEs*, *gNBs*, and the *wireless physical channel* between them, where these trade-offs become most relevant.

A key advancement of 5G is its support for mmWaves (>24 GHz), which enable significantly shorter transmission intervals, as low as 15.625 µs, compared to sub-6 GHz bands with slot durations around 0.25 ms [45]. This finer scheduling granularity enables end-to-end latencies below 1 ms, making 5G well-suited for latency-critical ICSs, particularly for applications requiring tight timing and high reliability, in contrast to alternatives such as Wi-Fi [48].

Challenges in mmWave Environments. While mmWave is essential for achieving sub-ms latency, it introduces challenges such as high propagation loss, limited coverage, strong sensitivity to blockage, and susceptibility to environmental factors such as the weather [8]. Due to these limitations, line-of-sight (LoS) conditions between UEs and gNBs are often necessary. These issues are mitigated through dense cell deployments that reduce transmission distances, as well as techniques such as MIMO and beamforming, which improve reliability and capacity by using multiple antennas and directing signals efficiently [19]. Although less reliable, non-line-of-sight (NLoS) communication remains possible via signal reflections [33]. In industrial settings, these challenges are more manageable due to controlled environments, particularly in stationary ICSs that enable stable LoS links and precise beamforming.

2.3 Related Work

Although the security of ICS has received significant research attention in recent years (e.g., [7, 12, 13, 50, 51, 57]), the implications of transitioning from wired to 5G communication remain underexplored. Previous work [5, 48] discusses the integration of 5G into ICSs and the associated security challenges, but only on a theoretical level. We attribute this gap to the lack of testbeds that integrate 5G (mmWave) communication in ICSs. In the following, we review existing wireless ICS testbeds to highlight this deficiency, then analyze studies on ICS security in traditional wired settings, and finally discuss research on 5G security in general-purpose applications.

Testbeds for ICS Security. Testbeds are crucial for safely evaluating cyber-physical attacks within ICS environments (cf. §2.1). Although numerous ICS security testbeds exist, they predominantly rely on wired communication or focus on wireless protocols, which are less promising than 5G mmWave. For example, Conti et al. [22] surveyed 61 ICS security testbeds, all of which use only wired communication. While Kampourakis et al. [37] examined 46 wireless

testbeds in cyber-physical systems, only four specifically target industrial processes, and none employs cellular communication (4G/5G). Similarly, in the IoT context, De Santana et al. [24] identified only three industrial testbeds involving 4G/5G technology.

Table 1 summarizes these existing wireless testbeds relevant to ICS security. As shown, no existing testbed relies on 5G mmWave for communication [9, 31, 40, 52, 55, 64, 73]. Thus, experiments investigating the wireless channel may not be transferable to 5G mmWave due to its sub-1 ms latency capabilities. Lastly, none of the existing testbeds allow reproducible research, e.g., evaluating the impact of different attacks under identical wireless channel conditions and physical process state. To bridge this gap, we introduce SWICS, the first virtual testbed that integrates 5G mmWave into an ICS and fully relies on simulation to enable replicable research.

Security Experiments on ICS. Traditional ICS research has extensively studied the impact of cyberattacks on physical processes. Rodofile et al. [57] conducted injection and flooding attacks on a mining refinery. Munteanu et al. [51] analyzed attacks on sensors and actuators in a water tank system, using statistical model checking to evaluate their impact and intrusion detection performance. Mohammed et al. [50] examined Denial of Service (DoS) attacks on oil and gas infrastructure, assessing impact and detection methods. These are among many other works such as [7, 12, 13], exploring attacks on ICSs. These studies further highlight the lack of focus on the security implications of transitioning to 5G-enabled ICSs.

Studies on 5G Security. While related work does not specifically assess the practical security implications of transitioning to 5G for ICSs, different research streams have studied 5G security in general-purpose settings. For example, Ludant et al. [43] demonstrated low-power DoS attacks on 5G's physical layer under a strong attacker model, and Birutis et al. [18] investigated jamming in commercial 5G, measuring bandwidth degradation but not latency, which is critical in industrial settings. Previous generations, such as LTE [17, 72], have also been studied without considering ICS impact. Nevertheless, these works highlight the need to consider wireless-medium vulnerabilities when analyzing ICSs security and support the transition to 5G for evolving industrial demands [48]. Lastly, studies exploring attack vectors introduced by other wireless technologies in ICS, e.g., Wi-Fi [9, 55, 64, 73] may not be transferable to mmWave.

Take Away: Despite the transition to wireless ICSs, research on the security implications remains limited, largely due to the lack of publicly available testbeds, ultimately highlighting the need for a virtual 5G-ICS testbed, that enables reproducible research.

3 SWICS – Simulating Wireless Communication in Industrial Control Systems

To address the lack of testbeds that combine industrial physical processes with 5G, and to enable reproducible research, we introduce SWICS, a fully virtual, simulation-based ICS testbed. In this section, we motivate the use of simulation and discuss its benefits (§3.1). We then present the design of the simulated ICS, an enhanced version of a state-of-the-art industrial testbed, and describe its integration into the ns-3 simulator (§3.2). Finally, we detail our realistic configuration of the 5G network reflecting real-world deployments (§3.3).

Table 1: The current landscape of security testbeds for wireless ICS lacks a platform that supports 5G mmWave.

Study	ICS Focus	Tech.	Real Process	Reproducibility
Prakash et al. [55]	Yes	Wi-Fi$^{\delta}$	Yes	No
Adepu et al. [9]	Yes	Wi-Fi$^{\delta}$	Yes	No
Tomić et al. [64]	Yes	Wi-Fi$^{\delta}$	Yes	No
Yasaei et al. [73]	Yes	Wi-Fi$^{\delta}$	Yes$^{\alpha}$	No
Gardiner et al. [31]	Yes	4G$^{\delta}$	Yes$^{\beta}$	No
Oliver et al. [52]	No	5G$^{\delta}$	Yes	No
Lee et al. [40]	Yes	5G$^{\delta}$	No$^{\gamma}$	No
SWICS (this work)	Yes	5G	Yes$^{\alpha}$	Yes

$^{\alpha}$Simulated $^{\beta}$Subprocess $^{\gamma}$Replay traffic $^{\delta}$sub-6 GHz

3.1 The Benefits of Simulation-based Testbeds

Comprehensively analyzing the security of wireless industrial systems presents several major challenges. First, deploying attacks or testing defense mechanisms on real industrial systems is inherently risky, as such actions may disrupt production, critical processes, or even endanger human safety. Second, introducing a wireless communication channel further complicates experimentation: Wireless conditions fluctuate due to seemingly insignificant and uncontrollable factors such as dust particles (cf. §2.2). These fluctuations make it nearly impossible to recreate identical radio environments across experiments. More importantly, the inherent non-determinism of the physical wireless medium prevents observed effects from being reliably attributed to specific system changes, attacks, or defenses. This lack of traceability and consistency undermines fair evaluation, reproducibility, and confidence in experimental results. While constructing small-scale physical testbeds is possible, it is extremely costly and still offers limited control over environmental conditions.

On the other hand, a fully virtual testbed enables safe and replicable experimentation with precise control over industrial networks. Consequently, as the foundation for our research on the security implications of wireless communication in industrial systems, we develop SWICS [41], the first virtual testbed to interconnect ICS components over 5G. SWICS follows the discrete-event simulation (DES) paradigm to accurately model an ICS, where industrial devices control a responsive physical process communicating via 5G. Leveraging DES enables fine-grained, deterministic control over both physical and wireless dynamics, allowing us to isolate factors such as communication type or attack presence and reliably attribute any differing outcomes to isolated system parameters.

3.2 Simulation of the Industrial Control System

At the core of SWICS sits the physical process of the simulated ICS. To enable the rapid execution of multiple attacks, we require a physical process that is inherently robust and can quickly recover from attacks. Consequently, we adapt the existing design of a simulated water bottle-filling plant [27] relying on a conveyor belt for automated bottle transport [25]. We further advance this design by increasing both the physical realism and operational complexity of the system. Fig. 1 visualizes our resulting 5G-enabled ICS.

ICS Operation and Enhancements. The ICS controls two central functions of the bottle-filling process: positioning bottles beneath the water tank using a conveyor belt and regulating water inflow to

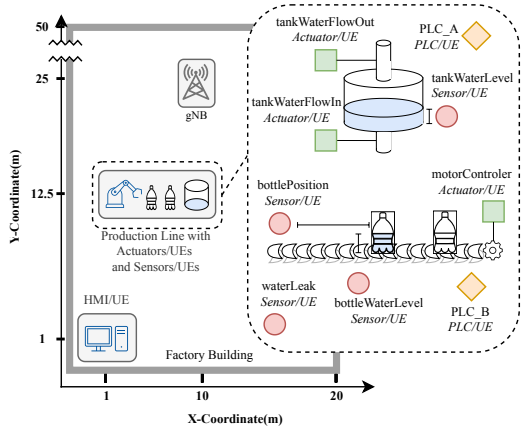


Figure 1: SWICS simulates a bottle-filling plant [25], comprising a water tank, valve-actuators, fill-level and spill sensors, a conveyor belt, an HMI, two PLCs, and 5G communication.

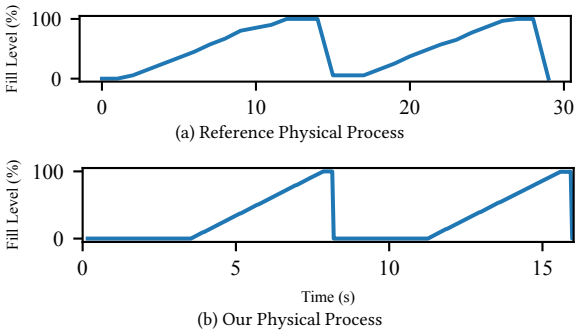


Figure 2: SWICS's behavior (b) closely matches the original reference simulated process [27] (a). To improve realism, we smooth bottle filling by increasing the polling rate and model liquid flow using Torricelli's law, yielding more realistic filling times and reflecting the natural acceleration of liquid.

the tank and outflow into bottles (cf. Fig. 1). Two PLCs and one HMI coordinate these tasks. PLC_A regulates water flow by opening the output valve when a bottle is detected and closing it once the desired fill level is reached. It also monitors the tank level sensor to refill the tank as needed by opening the input valve. PLC_B manages conveyor movement based on the sensors for bottle position and fill level, stopping the belt when an empty bottle arrives beneath the tank and restarting it once filling is complete. The HMI collects an overview of the process state from PLC_A and PLC_B.

To improve realism beyond prior work, we extend the simulated process in four ways. First, we add a water-leak sensor that allows PLC_A to detect abnormal outflow conditions. Second, we introduce measurement noise by applying up to 0.5% random error to all sensor readings, reflecting imperfections common in industrial environments. Third, we replace fixed liquid flow-rate approximations with a physically accurate model based on Torricelli's law [63], making fill times dependent on the current tank level. Finally, we integrate an HMI that periodically polls the system state and logs timeouts, enabling operator visibility. Lastly, to ensure safe operation, we additionally implement an emergency mechanism: if sensor readings cease for a predefined interval, the PLCs halt the process by closing all valves and stopping the conveyor belt. Together, these enhancements yield a more realistic, fault-aware, and operationally complete representation of an industrial bottle-filling system.

Implementation. We implement our ICS in the *ns-3* simulator, with all components realized as *ns-3 Applications*. This approach allows seamless integration with existing ns-3 classes, including those for TCP/IP communication and the deployment of applications on any *ns-3 Node*. It also enables flexible and rapid addition of new components, making SWICS an extendable testbed for future experiments across adifferent scenarios. We also extend *ns-3* to fully support the Modbus protocol, which is widely used in ICSs [22].

Accuracy. To ensure accuracy of our physical process, we analyze its behavior over time. Fig. 2 (b) exhibits the expected behavior: as bottles fill with liquid, the fill level sensor detects an increasing level, and the corresponding measurement level rise. Once a bottle is filled, it moves forward to accommodate a new empty bottle, causing the sensor to report an empty state. The time interval between consecutive bottles is reflected in the flat portions of the graph. We validate our implementation by comparing it to the original process (cf. Fig. 2 (a)), observing comparable overall behavior, while SWICS shows smoother sensor readings due to a higher polling rate.

3.3 Integration of 5G Communication

By simulating a physical process and leveraging the deterministic nature of DES, SWICS provides a solid foundation for studying the security implications of 5G in ICSs. To simulate 5G, we use a state-of-the-art ns-3 module and configure it in accordance with relevant studies to ensure high accuracy.

mmWave Module. We add 5G communication between the ICS components by utilizing the *mmWave* ns-3 3GPPP-compliant extension [46], which is widely used in academia (e.g., [39, 53, 56]). This extension implements 5G-specific behavior at the PHY and MAC layers on top of the LTE module to enable end-to-end simulation of 5G mmWave networks. As such, it enhances LTE eNBs and UEs with mmWave capabilities by supporting, e.g., 5G frame structure, transmission/reception, and beamforming, allowing realistic simulation of communication in mmWave spectrum. While ns-3 currently lacks a full-stack 5G implementation, the mmWave module fully meets our research needs, as we focus solely on studying the impact of the 5G channel in ICSs.

Topology. Our network consists of 10 UEs, one for each industrial device (sensors, actuators, PLCs, HMI), positioned in a factory-sized building measuring 50 m × 20 m × 10 m (cf. Fig. 1). Further, we place one gNB within the facility that is connected to the core network, facilitating communication between the devices. All UEs are stationary at ground level, while the gNB has a height of 9.5 m, enabling LoS between them. The gNB utilizes an 8×8 MIMO configuration and the UEs a 2×2 MIMO configuration, both employing beamforming to overcome challenges w.r.t. mmWaves (cf.§2.2).

Realism. To ensure accurate and realistic network behavior, we configure our network based on 3GPP specification and prior works. First, we set our network to operate on band n257 (28 GHz), which is well suited for industrial applications due to its low latency [32].

We configure the gNB transmission power to 34 dBm, in line with 3GPP specifications, which define transmission power for medium-range base stations up to 38 dBm [3, §6.2]. For UEs, band n257 encompasses all power categories (1-7) defined by 3GPP [1, §6.2.1]. We select power category 3 (23 dBm), designed for applications requiring lower power output, such as industrial devices. To account for effects such as signal attenuation in industrial environments, we use the 3GPP indoor factory channel model [2, 54, §7].

Take Away: To investigate the impact of 5G on ICS security, we introduce SWICS which accurately simulates both the physical process and wireless 5G channel. Thus, we ensure that our experiments closely reflect real-world results.

4 Analysis Methodology

To analyze the implications of transitioning from wired to 5G communication in ICS, we deploy SWICS in both a 5G mmWave configuration and a traditional Ethernet setup. (cf. §3). Then, we compare the functionality of the ICS utilizing both media under benign and attack conditions. By maintaining consistent parameterization across all deployments, we ensure that any observed differences are solely attributable to the communication medium.

In addition to the physical medium, we evaluate changing channel conditions, which are a critical factor influencing network performance, especially considering that 5G mmWave deployments operate at very high frequencies rendering them particularly sensitive to environmental impact (cf. §2.2). Consequently, in our experiments, we consider three deployment scenarios:

Wired. A wired version of the deployment described in §3 where all 5G connections are replaced with 100 Mbit/s Ethernet, serving as baseline for comparison.

5G-GC. The 5G setup as described in §3 operating under optimal channel conditions.

5G-DC. The same 5G setup as before with intentionally degraded channel conditions, achieved by increasing noise to emulate interference from a device operating on the same area and frequency.

Using these scenarios, we evaluate how the communication medium influences the impact of network-level attacks. To this end, we first define a threat model based on realistic assumptions and prior work (§4.1), ensuring it is robust and applicable to real-world 5G ICSs. We then create a baseline scenario in which SWICS's physical process operates without interference (§4.2). Building on this benign scenario, we execute well-known attacks—common in publicly available studies and datasets—against the ICSs (§4.3). To assess the security implications of each deployment, we compare differences in each attack regarding their direct effect on the physical process (§5), the performance of existing security measures (§6), and novel attack vectors of the wireless channel (§7).

4.1 Threat Model and Scope

Before assessing 5G's impact on ICS security, we define our threat model consideing two different attacks with distinct capabilities:

Insider. To highlight the potential impact of insufficient security in ICSs, we consider an attacker capable of injecting, blocking, and modifying packets in both deployments. Achieving these capabilities requires access to the ICS network, depending on the underlying communication medium (Fig. 3). As ICSs prioritize operational goals, security controls are often omitted with recent studies showing that only 6.5% of industrial devices use TLS with 42% being misconfigured [23]. Therefore, we assume the absence of *end-to-end security* in wired industrial deployments. Thus, in such settings (Fig. 3 (a)), physical or logical access to a network interface—e.g., via a compromised port, a completed ICS cyber kill chain [16], or a misconfigured TLS client—is sufficient to obtain these capabilities. We further assume that such capabilities remain achievable in 5G-enabled ICS, as it remains unclear if adoption of end-to-end security will increase when switching to 5G. Moreover, 5G user plane security controls may be disabled in favor of sub-1 ms communication requirements [47]. Even when user plane security is enabled, attackers may exploit vulnerable ICS endpoints [66] or unsecured wired segments in hybrid deployments routed through the 5G network. In addition, the 5G infrastructure introduces further attack vectors: an adversary may exploit the open wireless interface—e.g., via signal overshadowing [72]—to deploy a rogue base station (Fig. 3(b)), which can then be used to relay, intercept, and modify traffic, effectively acting as a machine-in-the-middle [58].

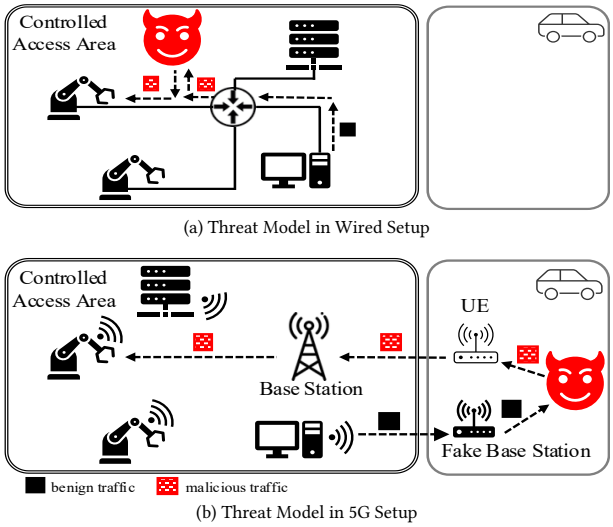


Figure 3: We assume that the attacker can modify ICS traffic the *wired* (a) and *5G* (b) deployments, although the means to achieve these capabilities depend on the physical medium.

Outsider. To further illustrate the security implications of 5G for ICSs, we consider a threat model for wireless deployments under the assumption of a *perfectly secured ICS*. In this setting, the attacker is limited to interacting with the (encrypted) radio channel over the open air interface, with no access to internal system components or interfaces. We use this model to highlight security complications introduced by wireless communication in §7.

Ultimately, this threat model emphasizes the need for security-by-design in future 5G-enabled ICS, as also highlighted by the European Union Agency for Cybersecurity [29]. We further elaborate on the implications of our assumptions in §8.

4.2 Benign Scenario

To serve as a reference for our experiments, we establish an attack-free scenario which solely contains benign process behavior with a total duration of 20 minutes. In this scenario, bottles are being filled normally for 10 minutes. After that point, to introduce variability, the HMI halts the physical process, causing the conveyor belt to stop. After 1 minute, the HMI issues a command to restart the process. Upon restarting, the physical process resumes in two stages, initially operating at half speed before gradually returning to normal speed after another 2 minutes. These fluctuations introduce complexity by disrupting the otherwise deterministic traffic patterns, thereby creating a more realistic reference scenario and also aligning with the diversity requirement of datasets for security evaluation [22].

4.3 Attack Scenarios

Following Conti et al. [22], we implement four representative cyber-attack scenarios an *insider* can perform: DoS, Machine-in-the-Middle, Suppression, and Injection . While well studied in wired ICSs (cf. §2.3), their impact on the physical process in 5G remains largely unexplored, particularly how the communication medium affects attack behavior and consequences. To investigate this, we use SWICS to compare process stability under both wired and 5G attack scenarios. For each attack, we schedule multiple variants with increasing durations on the baseline scenario. Leveraging the deterministic nature of discrete event simulation, attacks are precisely scheduled at 200 s, 400 s, 600 s, 800 s, and 1000 s. This ensures identical process states and enables a clear comparison across scenarios.

Denial of Service (DoS). Flooding attacks are among the most common types of DoS attacks. They typically involve sending a large volume of data to a target, exhausting the network's capacity or overwhelming its computational resources, rendering it unable to process legitimate traffic. This attack type is easy to set up and poses a significant threat to industrial processes, indiscriminately disrupting normal operations without requiring extensive knowledge of the process, leading to unpredictable behavior. We implement the DoS attack by simulating an attacker retransmitting numerous Modbus read requests from the HMI to PLC_A during the given attack schedules. We intentionally set the number of injected packets so that the attack affects the physical process without causing a water spill to remain as subtle as possible.

Machine in the Middle (MitM). In this attack, the attacker exploits the absence of integrity protection—common in ICSs [35]—to modify legitimate packets. By positioning themselves on the communication path, the attacker can intercept and alter packets such as sensor readings or PLC commands. While such attacks are straightforward in wired networks (e.g., via a physical MiTM or ARP spoofing), they have also been shown to be feasible in cellular communication if integrity protection is absent [58]. To implement this attack, we send altered commands to the *motionController* regulating the conveyor belt by replacing *stop commands* with a *keep moving* command. Thus, we prevent the conveyor belt from stopping and potentially cause liquid spillage as bottles do not stop beneath the filling station.

Injection. To conduct an injection attack, an attacker only requires access to the communication network. Exploiting the lack of authentication, the attacker can then inject messages into the network, pretending to be one of the two communicating parties, potentially sending unexpected commands or false sensor readings. If the channel provides origin authentication, the attacker can still intercept legitimate packets and re-inject them to the destination at a later time (a.k.a. a replay attack). In our scenarios, we implement the replay variant by re-transmitting *open* commands to the tank's liquid output valve from PLC_A. Depending on the physical process state—i.e., whether a bottle is positioned under the valve—the attack may cause liquid spills.

Suppression. In contrast to previous attacks, where an attacker manipulates legitimate communication to compromise the system, a suppression attack disrupts the physical process by selectively dropping packets, such as PLC commands. This can be achieved by compromising either the sender/receiver, infiltrating the network somewhere along the path between them, or in 5G through methods such as smart reactive jamming [15]. We simulate this attack by blocking the PLC's network interface during specified time frames, preventing it from transmitting any messages. As a result, commands such as opening/closing valves are not issued during these intervals, potentially causing spills.

Take Away: Using SWICS we study the impact of 5G on ICS security by comparing the effects of well-established attacks. By using consistent parameterization, we ensure that any diverging behavior can be attributed solely to the physical medium.

5 Impact on the Physical Process

The primary goal of ICS security is to prevent and minimize damage to the physical process. After outlining our methodology, we evaluate the impact of 5G on this process by deploying each attack described previously across all scenarios. We then evaluate differences in the behavior of the physical process (i.e., conveyor belt speed or water spills) compared to its expected behavior. By monitoring these attributes, we can quantify the effects of attacks, utilizing the number of liquid spills as a measure of critical failure. In this section, we review all attacks and report differences in their effects across the three scenarios. Due to SWICS's determinism and consistent parameterization, we can attribute any observed differences solely to the communication medium.

Results. To show the impact on the physical process, Fig.4 visualizes the conveyor belt speed over time for each scenario. The red-shaded regions in the plots denote active attack periods, allowing for a clear comparison of the process response during and after disruptions. Further, Tab. 2 complements this by summarizing the amount of liquid spilled as detected by the corresponding sensor.

Benign. In this configuration, the physical process runs smoothly and identically across all scenarios. Even for 5G-DC, the system's robustness and high sensor polling rate ensure that packet losses and increased jitter caused by noise do not affect process operation.

DoS. Similarly to the benign scenario, during the DoS attack, we observe no substantial differences between 5G-GC and Wired. All short attack variants appear to have no impact on the physical process, likely due to its inherent robustness. However, when considering the 5G-DC, particularly from the third attack variant onward (yellow in Fig. 4), the attack clearly impacts the physical process. The third attack variant coincides with the moment the PLC issues

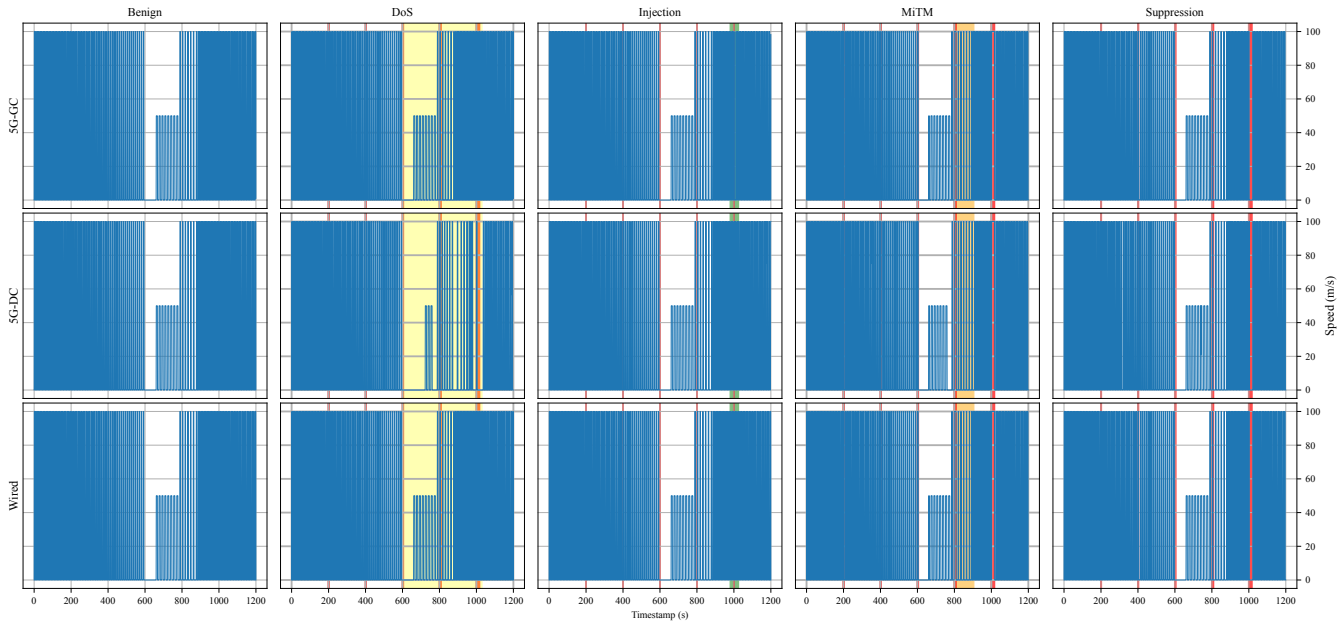


Figure 4: The conveyor belt speed in the *Wired*, *5G-GC*, and *5G-DC* deployments is stable under benign conditions. Under attack, *Wired* and *5G-GC* show similar resilience with only minor jitter-induced deviations, whereas the noisy *5G-DC* deployment significantly amplifies the effects of DoS and MiTM attacks due to increased jitter, packet loss, and latency.

Table 2: Liquid spills as a measure of critical failure show the increased effect of attacks against the 5G-DC scenario.

	Benign	DoS	Injection	MitM	Suppr.
Wired	0	0	0	4	2
5G-GC	0	0	1	4	2
5G-DC	0	1 (long)	0	5	2

a command to stop the conveyor belt, which continues to move briefly afterward at half speed. Although the stop command from the PLC reaches the conveyor belt and it eventually stops, the flooding attack causes queues to overflow, resulting in excessive packet drops and triggering retransmissions. This effect, combined with the noisy 5G channel that introduces additional packet losses, leads to delays in the delivery of subsequent PLC commands, e.g., to restart the conveyor. The increased latency in PLC start/stop commands becomes more evident in the fourth attack variant, where the conveyor belt experiences extended and inconsistent periods of motion and halting. Finally, for the fifth, most intense attack variant, communication is completely disrupted, resulting in a total loss of availability. In the 5G-DC, this variant also leads to a long liquid spill, as delayed control signals prevent timely process control.

Injection. The injection attack is designed to open the liquid valve at random time points, potentially causing spills. Our results reveal an unexpected outcome. In the Wired setup, the attack has no effect because the injected packet arrives immediately before a legitimate update, which nullifies the attack's effect before it is registered by the system. In the 5G-GC scenario, however, the legitimate packet arrives later due to increased delays, causing a water spill. In the 5G-DC deployment, an earlier burst of packet loss causes a shift in the update cycle, which coincidentally results in the legitimate update packet to arrive just before system reading; effectively nullifying the attack similar to the Wired deployment by pure chance.

MitM. The MiTM attack targets the conveyor belt PLC, aiming at disrupting timing-critical operations such as placing bottles under the valve. As shown in Tab. 2, both Wired and 5G-GC setups experience four spills, while 5G-DC sees one additional spill—all occurring during attacks. The difference lies in how each network handles the third attack variant. In Wired and 5G-GC, the attack command arrives just before a legitimate stop command, which quickly overrides it due to the controller's polling rate—limiting the impact. In 5G-DC, however, higher jitter and MiTM processing delays cause the altered packet to arrive too late, making the spill unavoidable. The noisy channel also delays benign PLC instructions causing the conveyor belt to remain at a lower speed for extra process cycles compared to the other scenarios (orange in Fig. 4).

Suppression. During the suppression attack, we observe identical effects across all scenarios. Because the attacker drops all packets, additional latency and occasional packet loss caused by network conditions have no substantial impact. As a result, each scenario experiences two liquid spills. In the final variant, the attack escalates to a DoS, triggering the SWICS's safety mechanism ultimately halting the production process (cf. §3.2).

Take Away: While reliable 5G channels can match the resilience of wired networks under optimal conditions, a degraded channel can amplify the effects of traditional attacks.

6 Impact on Security Measures

As the introduction of the 5G can amplify the effects of network attacks and degrade the security of the system, the question arises whether traditionally deployed countermeasures remain effective. A vital part of any defense-in-depth strategy in industrial systems are anomaly-based intrusion detection systems, which aim to detect attacks before they cause damage to the physical process [70]. These systems work under the assumptions that the behavior of the physical process and communication patterns are predictable, while attacks change this behavior noticeably.

However, due to the fluctuating and unreliable nature of the wireless medium, these assumptions may no longer hold. Therefore, we assess the performance of current, state-of-the-art detection approaches in 5G industrial settings, especially under varying channel conditions. We base our analysis on two widely researched communication-based detection approaches, which build their models based on network timings and packet sequences (e.g., [20, 30, 42, 59]). We exclude approaches that solely monitor the process state (e.g., [14, 68]) or host-behavior (e.g., [28]) as these systems are unaffected by the fluctuating physical channel, and their effectiveness presents challenges orthogonal to our work. However, we note that an effective intrusion detection strategy should monitor multiple characteristics simultaneously [67], rendering the methods we evaluate a vital part of modern cyber-defense.

To assess the performance of network-based intrusion detection mechanisms in 5G-enabled ICS, we evaluate the impact of 5G on model quality (§6.1) and alert behavior (§6.2) across all deployment scenarios (cf. §4) and under dynamic channel conditions.

6.1 Impact on Timing-based Intrusion Detection

A widely used strategy of network-based intrusion detection in industrial systems relies on the inter-arrival timing of network packets, i.e., the time that passes between two network packets of the same communication flow or type [42, 59]. The underlying assumption of this approach is that attacks observably impact packet timings compared to benign conditions. In the following, we assess whether this assumption still holds when using 5G in ICSs.

Experimental Setup. To assess the impact of 5G on timing-based intrusion detection, we utilize the IPAL framework [70] which provides an open-source implementation of Lin et al.'s [42] detection approach. This approach extracts the inter-arrival times for the individual flows in the network and models them using bounds based on average timings within a given window. Consequently, to assess the suitability of a timing-based detection approach for ICS using 5G, we compare the model quality using the distributions of inter-arrival times for each deployment scenario. To this end, we extract attack-free network traffic from SWICS for each deployment as training data and compute the three corresponding models.

Results. Fig. 5 shows the distribution of inter-arrival times for all flows for the *Wired*, *5G-GC*, and *5G-DC* model. We observe two peaks in all three distributions around 0.04 s and 0.10 s. These peaks arise because the flows within the network tend to average these specific inter-arrival times. Traditionally, the timing-based detector relies on tight bounds, derived from low network jitter, to identify deviations caused by attacks. The *Wired* model (red in Fig. 5) exhibits such tight bounds as indicated by the narrower peaks around 0.04 s and 0.10 s. Although the model trained on *5G-GC* data (blue in Fig. 5) exhibits similarly narrow peaks with a similarly small standard deviation for individual flows, we observe additional peaks around 0.03 s, 0.06 s, and 0.09 s in the model's distribution resulting from additional retransmissions caused by the less reliable wireless channel. Finally, the model for the degraded wireless channel (5G-DC) (green in Fig. 5) exhibits broader peaks in the distribution, showing higher deviation in the observed timings, potentially marking more behavior as benign.

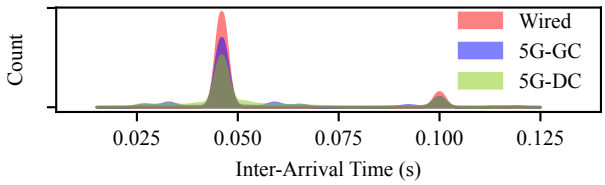


Figure 5: The distributions of inter-arrival times in the Wired, 5G-GC, and 5G-DC scenarios showcase that increased jitter widens the bounds of the inter-arrival time detector [42], potentially allowing malicious behavior.

These results show that degraded channel conditions negatively impact the training data quality of a timing-based detection system, leading to a more relaxed model that allows broader behavior and may detect less malicious activity, thus decreasing its effectiveness.

6.2 Impact on Alert Behavior

In addition to monitoring timings, communication-based intrusion detection systems utilizing packet sequences present another established method for attack detection in industrial settings (e.g., [20, 30]). Similar to the timing-based approach, these systems rely on deterministic traffic to produce consistent packet sequences under benign conditions assuming that attacks alter this sequence. In the following, we assess the suitability of both timing-based and sequence-based mechanisms—on the example of Ferling et al.'s [30] detection approach based on Discrete Time Markov Chains (DTMCs)—for ICS using 5G. Furthermore, we also test how these approaches adapt to a fluctuating wireless medium.

Experimental Setup. We generate a dataset from the network traffic of each deployment and attack scenario (cf. §4.3) realized with SWICS [41]. Then, we train and deploy each intrusion detection model on each respective dataset to assess detected attacks and false alerts. Additionally, we evaluate the robustness of the inter-arrival time based and sequence-based detectors under fluctuating channel conditions and thus their suitability for usage in 5G-enabled ICSs. To this end, we study alert behavior when models are trained on data from one 5G scenario and deployed in the other (e.g., trained in 5G-GC and deployed in 5G-DC, and vice versa). Furthermore, we conduct these experiments using the IPAL framework [70], to allow for a direct comparison between the detectors.

Results. Fig. 6 compares the ground truth of attacks (top row; red boxes) and the alerts of the intrusion detection systems for each channel configuration (i.e., *Wired*, *5G-GC*, *5G-DC*) as well as dynamic noise levels simulated by switching training and test data

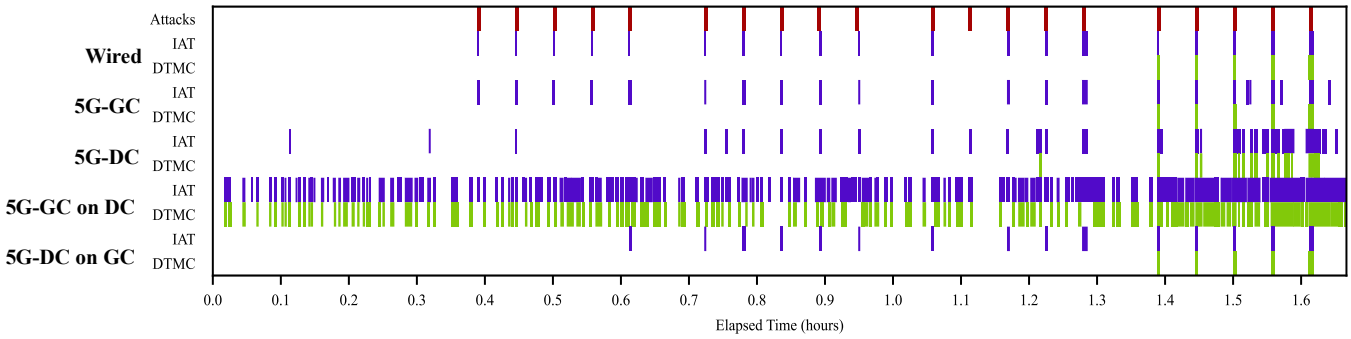


Figure 6: The alert behavior of communication-based detectors deployed in the *Wired* and *5G-GC* deployments show the accuracy of the inter-arrival timing-based detector [42] (IaT - blue) and sequence-based intrusion detection [30] (DTMC - green). The models derived from the *5G-DC* produce additional false alerts and detects fewer attacks due to increased jitter and delays. Deploying the 5G models in different channel conditions (5G-GC on DC and 5G-DC on GC) impacts their alert behavior significantly, even rendering benign behavior indistinguishable from attack periods (5G-GC on DC).

(*5G-GC on DC* and *5G-DC on GC*). Setting a baseline for comparison, the timing-based detector performs nearly perfectly in the *Wired* scenario, detecting 19 out of 20 attacks without raising false alerts. This performance showcases how the models tight bounds result in high detection capabilities. Similarly, the *5G-GC* model detects 19 out of 20 attacks in the 5G-GC dataset (Fig. 6 5G-GC). Furthermore, the timing-based detector produces 4 false alerts towards the end of the dataset, which result from jitter in the wireless medium. DTMC accurately detects 5 out of 20 attacks in the *Wired* and *5G-GC* deployments, but misses the remaining 15, likely caused by DTMC's permissiveness toward minor packet sequence changes.

The results for the *5G-DC* deployments show a degradation in detection performance for both detection approaches. The timing-based model trained and evaluated on the degraded channel (Fig. 6 5G-DC) still detects 15 out of the 20 attacks, but produces 17 false alerts. Because most of these false alerts cluster near the end of the dataset, they make the last four true alerts unrecognizable. Moreover, both approaches produce additional false alerts in the *5G-DC* scenario, caused by high jitter in the noisy channel.

To test the effectiveness of these traditionally well-working detection approaches under the novel challenges presented by the dynamic 5G channel, we evaluate *5G-GC* models on noisy-channel datasets and vice versa. We observe that the noisy channel alters the inter-arrival times and the packet sequences to such a degree that both *5G-GC* models flag the behavior as alerts. These constant false alerts render attack-free periods indistinguishable from attacks. Conversely, deploying the *5G-DC* model in the noiseless channel (Fig. 6 5G-DC on GC) reduces alerts. In this case, improved channel conditions reduce false alerts for both detectors, enhancing DTMC's performance to correctly detect 5 out of 20 attacks, similar to the *Wired* and *5G-GC* baselines. Similarly, the timing-based approach detects 15 out of 20 attack scenarios—still, 4 less than the model trained under these channel conditions.

These results show that communication-based intrusion detection is sensitive to channel variation, hindering the collection of high-quality training data [10, 69]. Moreover, in 5G communication-based detection becomes unreliable, as static models struggle to distinguish poor channel quality from actual attacks.

Take Away: As current assumption of predictable communication behavior no longer hold under dynamic channel conditions, existing intrusion detection systems become unreliable presenting novel concerns including the collection of training data.

7 Attacks on the Wireless Interface

So far, our analysis has focused on the impact of 5G on traditional ICS attacks and security mechanisms. However, transitioning to a wireless link introduces new vulnerabilities and increases exposure to external threats, which we examine in this section. Specifically, we show how an *outsider* attacker can extract critical information about the ICS (§7.1), which can be leveraged to perform jamming attacks that disrupt system operation (§7.2). While such attacks have been studied in other wireless ICSs (cf. §2.3), our results indicate that in 5G, MIMO enables significantly more effective and stealthier jamming, potentially even at low transmission power.

7.1 Passive Reconnaissance

Extracting communication patterns from a wired ICS is usually challenging, as it requires physical or logical network access. With a wireless medium, however, eavesdropping becomes effortless. Anyone with commercial-grade radio equipment, such as an SDR, and open-source software can analyze the wireless spectrum. Spectrum analyzers are tools that provide a visual representation of signal frequencies, allowing detailed observation of transmission presence, strength, and patterns over time. This enables an attacker to passively monitor communication, identify active frequency bands, and infer key operational characteristics of the system.

To assess susceptibility to passive reconnaissance attacks, we deploy a customized spectrum analyzer module *outside the facility perimeter*. Fig. 7 shows the monitored 5G channel, where transmission intervals appear as regions of high signal power. These observations allow an attacker to infer the ICS process cycle and mount targeted reactive jamming attacks [60], selectively disrupting critical signals—even if traffic is encrypted.

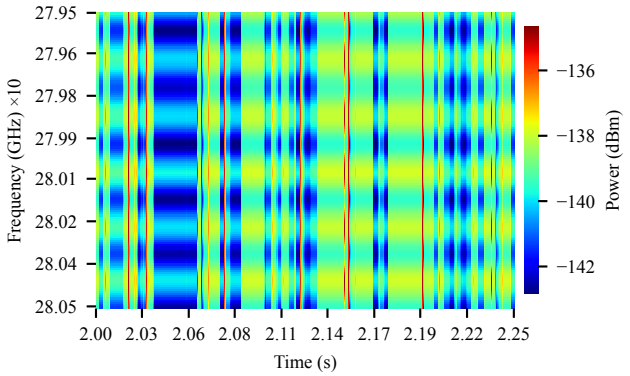


Figure 7: By passively monitoring the 5G channel even from outside the industrial premises, an attacker can infer critical details about an ICS such as the process cycle.

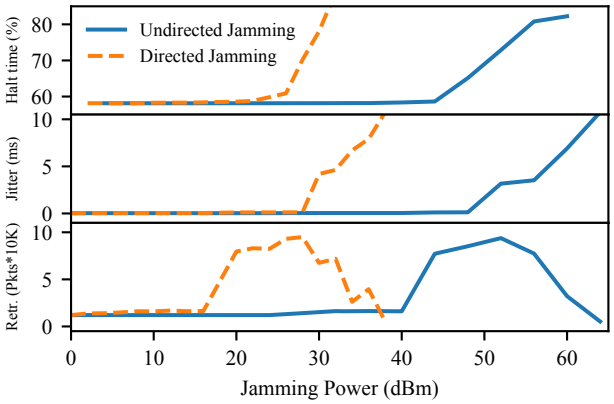


Figure 8: Impact of jamming from outside the factory on the ICS: jitter (Top), retransmissions (Mid), and halting time (Bottom). Directed jamming causes similar disruption to undirected jamming with half the transmission power.

7.2 Jamming to Disrupt the Physical Process

In 5G networks, DoS attacks can be launched by any adversary within communication range, without requiring network access. A jammer interferes with legitimate transmissions by emitting radio signals, potentially degrading or blocking communication. In 5G-enabled ICSs, this is particularly critical as jamming directly targets system availability [48]. We distinguish between constant jamming, which continuously emits noise, and reactive jamming, which transmits only upon detecting legitimate signals (e.g., via spectrum analysis as in §7.1), making it more stealthy.

Experimental Setup. To simulate jamming, we implement a custom physical-layer device in ns-3. When activated, it signals the channel model to inject a high-power signal for a fixed duration, increasing background noise, leading to malformed or dropped packets. We also add MIMO support to reflect real-world mmWave 5G devices (cf. 2.2), enabling disruption via lower-power directional transmissions. We apply jamming intermittently across the process for short intervals, covering about 50% of the simulation time. This approach lies between reactive and constant jamming. Our aim is to observe its effects at different process stages.

Impact on Network Performance. To assess the impact on network performance, we consider two key metrics: jitter (variance in latency) and number of retransmissions. In our experiments, we jam until jitter reaches 10 ms, a commonly accepted upper bound for time-critical industrial applications [48]. Even if average latency remains below 1 ms, exceeding this jitter threshold violates latency guarantees. As shown in Fig. 8 (Top), a directed jammer outside the facility using 4×4 antennas can significantly increase jitter with transmission power only slightly above that of a legitimate UE, making detection difficult. In contrast, undirected jamming requires roughly twice the gNB's transmission power and is therefore easier to detect. Retransmissions (Fig. 8 (Mid)) show a similar trend: directed jamming disrupts communication with less than half the power required for undirected jamming. Retransmissions initially increase as packet corruption triggers recovery mechanisms, but eventually decrease once noise prevents successful transmission altogether, effectively collapsing communication. This packet loss can be catastrophic—e.g., if safety-critical commands fail to arrive. Overall, directed jamming below 20 dBm can induce severe packet loss, highlighting that an attacker with a compromised UE/gNB and a small antenna array can launch effective, low-power jamming attacks that are difficult to detect and significantly increase risk.

Impact on the Physical Process. To evaluate the impact of jamming on the physical process, we consider the fraction of time the conveyor belt is stationary. Under normal conditions, the conveyor belt is stationary roughly 55% of the time, as it only operates to position a new bottle under the valve. As shown in Fig. 8 (Bottom), with increased jamming power, the halting time rises because more packets are lost, triggering the safety mechanism (cf. §3.2) that causes a full shutdown when no messages are received within a specified time frame. Consistent with the impact on network performance, directed jamming causes the same disruption as undirected jamming but requires only about half the transmission power. Specifically, directed jamming achieves an 80% halting time at around 30 dBm transmission power, while undirected jamming requires approximately 55 dBm to produce the same effect.

Take Away: Introducing a wireless medium to ICSs broadens the attack surface, enabling stealthy reconnaissance and jamming. In 5G mmWave MIMO environments, an attacker with a compromised device and spectrum analyzer can perform directional jamming to disrupt the ICS without triggering alarms.

8 Discussion and Future Work

Our analysis shows that 5G communication can amplify traditional ICS attacks, challenge existing security measures, and introduce new attack vectors. To contextualize these findings, we discuss key methodological choices and limitations, and identify promising countermeasures. For each aspect, we also outline directions for future research.

Choice of Attack Vectors. Our work focuses on assessing the security challenges arising from introducing 5G communication

into ICSs. However, we do not simulate a full 5G protocol stack in SWICS, but instead focus on the impact of the wireless medium—specifically the mmWave spectrum—on the security of the physical process. Although, we consider vulnerabilities in the 5G infrastructure in our threat model (§4), the security and weaknesses of 5G protocols and components are generalizable across use-cases and have been extensively studied [21, 36, 43, 44, 71]. However, it is important to note that these vulnerabilities expand the traditional attack surface of ICSs, especially w.r.t. to availability(c.f. §5). Future work should therefore focus on integrating a full 5G protocol stack in ns-3 and conducting a 5G-focused security analysis in ICSs.

Selection of Intrusion Detection Systems. Intrusion detection systems have long been a popular security control for ICS due to their ability to retrofit security into legacy systems [70]. For our analysis, we focus on two relatively simple intrusion detection strategies that rely on predictable communication patterns, such as packet sequences and inter-arrival times—techniques traditionally effective in ICS [70]. Our results show that these approaches struggle under the inherently dynamic conditions of 5G networks, particularly when channel conditions degrade compared to the training phase. These findings highlight that traditional ICS security controls cannot be assumed to remain effective in wireless environments and must be re-evaluated and updated. Operators must either include varying channel conditions in the training data—complicating the already challenging task of collecting representative data [10, 22, 69]—or find alternative protection mechanisms, which can be developed, studied, and evaluated using SWICS.

Transferability to real ICS. We emphasize that behavior of real-world ICSs depends on many factors such as, the specific topology (network or other devices), network setup, device types, and more. Therefore, transferring the results presented in this paper might not transferable to other systems "1-to-1". Instead, this study aims to provide general insight on the effects of 5G on ICS security, where we took multiple steps to ensure a close representation of real-life systems. Thus, to recreate a realistic 5G channel, we utilized network and channel models that are standardized by the 3GPP and that are calibrated against real-world 5G networks. Furthermore, we conduct our experiments using 5G mmWave and thus ensure that any observed effects are likely to be amplified in other wireless technologies commonly used in industry that do not offer such high performance guarantees. At last, we intentionally select a simple and robust bottle-filling process with the rationale that if attacks can cause substantial disruptions even in such a simple and robust scenario, their effects are likely to be even larger in more complex systems as they would occur in the real-world. In total, these decisions aim to provide a realistic understanding of ICS security under 5G. Nevertheless, SWICS allows replacing the underlying ICS or the wireless technology with minimal effort to conduct research on more involved deployments in the future.

Countermeasures. The choice of countermeasures in industrial 5G networks is strongly influenced by the requirements of the underlying physical process. A key advantage of 5G is its support for optional user plane security mechanisms, which provide encryption and integrity protection across the 5G infrastructure [48]. These controls can be used in networks with latency requirements between 1-10 ms. However, for sub-ms latency requirements, such mechanisms may become impractical due to their overhead. In such cases security protocols such as TLS or IPsec can be employed [26, 49], as they provide end-to-end protection avoiding additional per-hop processing delays. Further, latency-free alternative controls—such as intrusion detection systems that account for varying channel conditions or approaches based on payload inspection—can be employed to further enhance system security.

To mitigate attacks on the wireless interface, techniques such as beamforming, frequency hopping, and MIMO-based spatial filtering have been proposed [62]. Nevertheless, complete protection is unattainable without enclosing the factory in a Faraday cage, making physical security measures—e.g., extending the controlled physical perimeter to increase the cost and detectability of jamming—an essential complement to cybersecurity.

Ethical Considerations. Analyzing attacks on ICSs raises ethical considerations. To minimize harm, we rely on a fully virtual testbed, eliminating risks to deployed systems and human operators. All attacks are implemented in an abstracted simulation, do not produce executable malicious code, and are based solely on publicly available information. This enables us to study the security implications of 5G in ICSs while reducing the risk of misuse.

9 Conclusion

To address the increasing demand for flexibility in modern ICSs, a transition from wired to 5G communication is underway [11, 48, 61]. However, the security implications of switching to 5G in ICSs remain underexplored. To fill this gap, we present SWICS [41], the first virtual ICS-security testbed utilizing 5G and capturing a thoroughly modeled physical process. To enable reproducibility and facilitate further research, we make SWICS freely accessible [41].

Using SWICS, we assess the impact of 5G on the security of ICS, including the stability of the physical process under various attack scenarios (§5), the consequences for existing security measures (§6), and the increased risk from novel wireless-only attack vectors (§7). To this end, we directly compare traditional wired communication with 5G under varying channel conditions. Our findings show that under optimal conditions 5G provides comparable stability and security as the wired medium. However, a degraded channel poses substantial challenges for the security of ICSs, especially w.r.t. the susceptibility to cyber-attacks as well as communication-pattern based attack detection. Lastly, the wireless interface of 5G opens novel attack vectors for reconnaissance and jamming attacks, which may compromise availability.

Our results highlight the need to adapt existing ICS security measures when transitioning to 5G to account for fluctuations in channel quality and to consider resilience strategies against wireless-attacks such as jamming. Ultimately, we emphasize the need for comprehensive countermeasures fit for ultra-low latency applications that explicitly account for the effects of a 5G channel.

Acknowledgments

We sincerely thank the shepherd and the reviewers for their feedback on improving this work. Funded by the Foundation for Innovation in Higher Education (Freiraum Project RealistICS) and the German Federal Ministry of Research, Technology and Space (BMFTR) under funding reference number 16KIS2409K (6GEM+). The authors are responsible for the content of this publication.

References

[1] 3rd Generation Partnership Project (3GPP). 2023. *TS 38.521-2 V16.4.0; User Equipment (UE) conformance specification; Radio transmission and reception; Part 2: Range 2 standalone.* Technical Report.

[2] 3rd Generation Partnership Project (3GPP). 2024. *TR 38.901 V18.0.0; Study on channel model for frequencies from 0.5 to 100 GHz.* Technical Report.

[3] 3rd Generation Partnership Project (3GPP). 2024. *TS 38.104 V18.9.0; Base Station (BS) radio transmission and reception.* Technical Report.

[4] 5G-ACIA. 2019. 5G for Automation in Industry. https://5g-acia.org/wp-content/uploads/2021/04/5G-ACIA_5G-for-Automation-in-Industry-.pdf

[5] 5G-ACIA. 2021. *Security Aspects of 5G for Industrial Networks.* Technical Report. https://5g-acia.org/whitepapers/security-aspects-of-5g-for-industrial-networks/ Last accessed: June 18, 2024.

[6] 5G-ACIA. 2025. Industrial 5G Edge Computing - Use Cases, Architecture and Deployment. https://5g-acia.org/whitepapers/industrial-5g-edge-computing-use-cases-architecture-and-deployment/. Accessed: 2025-05-21.

[7] Syed Ghazanfar Abbas et al. 2024. SAIN: Improving ICS Attack Detection Sensitivity via State-Aware Invariants. In *USENIX '24.*

[8] Esmail M M Abuhdima et al. 2021. Impact of Weather Conditions on 5G Communication Channel under Connected Vehicles Framework.

[9] Sridhar Adepu et al. 2017. WaterJam: An Experimental Case Study of Jamming Attacks on a Water Treatment System. In *QRS-C '17.*

[10] Chuadhry M. Ahmed et al. 2020. Challenges in Machine Learning based approaches for Real-Time Anomaly Detection in Industrial Control Systems. In *CPSS '20.*

[11] Adnan Aijaz. 2020. Private 5G: The Future of Industrial Wireless. *IEEE Industrial Electronics Magazine* 14.

[12] Wael Alsabbagh et al. 2024. A Payload of Lies: False Data Injection Attacks on MQTT-based IIoT Systems. In *IECON '24.*

[13] Daniele Antonioli et al. 2017. Gamifying ICS Security Training and Research: Design, Implementation, and Results of S3. In *CPS '17.*

[14] Wissam Aoudi et al. 2018. Truth Will Out: Departure-Based Process-Level Detection of Stealthy Attacks on Control Systems. In *CCS '18.*

[15] Youness Arjoune and Saleh Faruque. 2020. Smart Jamming Attacks in 5G New Radio: A Review. In *CCWC '20.*

[16] Michael J Assante and Robert M Lee. 2015. The Industrial Control System Cyber Kill Chain. *SANS Institute InfoSec Reading Room.*

[17] Sulabh Bhattarai et al. 2015. On Simulation Studies of Jamming Threats against LTE Networks. In *ICNC '15.*

[18] Agnius Birutis and Anders Mykkeltveit. 2022. Practical Jamming of a Commercial 5G Radio System at 3.6 GHz. *ICMCIS* 205.

[19] Agnius Birutis et al. 2022. *A Study of 5G New Radio and Its Vulnerability to Jamming.* Technical Report. Norwegian Defense Research Establishment.

[20] Marco Caselli et al. 2015. Modeling message sequences for intrusion detection in industrial control systems. In *ICCIP '15.*

[21] Merlin Chlosta et al. 2021. 5G SUCI-catchers: still catching them all?. In *WiSec '21.*

[22] Mauro Conti et al. 2021. A Survey on Industrial Control System Testbeds and Datasets for Security Research. *IEEE Communications Surveys & Tutorials* 23, 4.

[23] Markus Dahlmanns et al. 2022. Missed Opportunities: Measuring the Untapped TLS Support in the Industrial Internet of Things. In *ASIA CCS '22.*

[24] Khalil G Queiroz de Santana et al. 2024. Cybersecurity Testbeds for IoT: A Systematic Literature Review and Taxonomy. *Journal of Internet Services and Applications* 15.

[25] Alireza Dehlaghi-Ghadim et al. 2023. ICSSIM — A Framework for Building Industrial Control Systems Security Testbeds. *Computers in Industry* 148.

[26] Erik Dekker and Patrick Spaans. 2020. Performance comparison of VPN implementations WireGuard, strongSwan, and OpenVPN in a 1 Gbit/s environment.

[27] Marietheres Dietz et al. 2020. Integrating Digital Twin Security Simulations in the Security Operations Center. In *ARES '20.*

[28] Constantine Doumanidis et al. 2023. ICSML: Industrial Control Systems ML Framework for native inference using IEC 61131-3 code. In *CPSS '23.*

[29] ENISA. 2019. *INDUSTRY 4.0 CYBERSECURITY:CHALLENGES & RECOMMENDATIONS.* Technical Report.

[30] Benedikt Ferling et al. 2018. Intrusion detection for sequence-based attacks with reduced traffic models. In *MMB '18.*

[31] Joseph Gardiner et al. 2019. Oops I Did it Again: Further Adventures in the Land of ICS Security Testbeds. In *CPS-SPC '19.*

[32] GSMA. 2022. 5G mmWave Deployment Best Practices: Design White Paper. https://www.gsma.com/solutions-and-impact/technologies/networks/wp-content/uploads/2022/10/FINAL-5G-mmWave-Deployment-Best-Practices-Design-White-Paper-November-2022.pdf

[33] Karsten Heimann et al. 2020. Reflecting Surfaces for Beyond Line-Of-Sight Coverage in Millimeter Wave Vehicular Networks. In *2020 IEEE VNC.*

[34] Kevin E. Hemsley and Dr. Ronald E. Fisher. 2018. *History of Industrial Control System Cyber Incidents.* Technical Report. Idaho National Laboratory, USA.

[35] Martin Henze et al. 2017. Network Security and Privacy for Cyber-Physical Systems. *Sec. and Priv. in CPS: Foundations, Principles and Applications.*

[36] Syed Rafiul Hussain et al. 2019. Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information. In *NDSS '19.*

[37] Vyron Kampourakis et al. 2023. A Systematic Literature Review on Wireless Security Testbeds in the Cyber-Physical Realm. *Computers & Security* 133.

[38] Eric D. Knapp. 2024. Industrial Cybersecurity History and Trends. In *Industrial Network Security.*

[39] Andrea Lacava et al. 2024. Programmable and Customized Intelligence for Traffic Steering in 5G Networks Using Open RAN Architectures. *ITMC '24* 23.

[40] Gyeoul Lee et al. 2021. Network Flow Data Re-collecting Approach Using 5G Testbed for Labeled Dataset. In *ICACT '23.*

[41] Stefan Lenz et al. 2026. SWICS. https://github.com/RWTH-SPICe/SWICS.

[42] Chih-Yuan Lin et al. 2018. Timing-Based Anomaly Detection in SCADA Networks. In *CRITIS '21.*

[43] Norbert Ludant and Guevara Noubir. 2021. SigUnder: a stealthy 5G low power attack and defenses. In *WiSec '21.*

[44] Norbert Ludant et al. 2025. Low-Layer Attacks Against 4G/5G Networks. In *WiSec '25.*

[45] Arman Maghsoudnia et al. 2024. Ultra-Reliable Low-Latency in 5G: A Close Reality or a Distant Goal?. In *HotNets '24.*

[46] Marco Mezzavilla et al. 2018. End-to-End Simulation of 5G mmWave Networks. *IEEE Communications Surveys & Tutorials* 20.

[47] Sotiris Michaelides et al. 2026. Evaluation of Security-Induced Latency on 5G RAN Interfaces and User Plane Communication. In *Proceedings of the 19th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec).*

[48] Sotiris Michaelides et al. 2025. Secure Integration of 5G in Industrial Networks: State of the Art, Challenges and Opportunities. *Fut. Gen. Com. Sys.* 166.

[49] Sotiris Michaelides et al. 2025. Assessing the Latency of Network Layer Security in 5G Networks. In *WiSec '25.*

[50] Abubakar S. Mohammed et al. 2023. Detection and Mitigation of Field Flooding Attacks on Oil and Gas Critical Infrastructure Communication. *Com. & Sec.* 124.

[51] Andrei Munteanu et al. 2020. Impact Analysis of Cyber-Physical Attacks on a Water Tank System via Statistical Model Checking. In *FormaliSE '20.*

[52] Ian Oliver et al. 2018. A Testbed for Trusted Telecommunications Systems in a Safety Critical Environment. In *SAFECOMP '18.*

[53] Natale Patriciello et al. 2019. An E2E simulator for 5G NR networks. *Simulation Modelling Practice and Theory* 96.

[54] Hitesh Poddar et al. 2023. ns-3 Implementation of Sub-Terahertz and Millimeter Wave Drop-based NYU Channel Model (NYUSIM). In *WNS3 '23.*

[55] Jay Prakash and Chuadhry Mujeeb Ahmed. 2017. Can You See Me: On Performance of Wireless Fingerprinting in a Cyber Physical System. In *HASE '17.*

[56] Darijo Raca et al. 2020. Beyond Throughput, The Next Generation: A 5G Dataset with Channel and Context Metrics. In *MMSys '20.*

[57] Nicholas R. Rodofile et al. 2017. Process Control Cyber-Attacks and Labelled Datasets on S7Comm Critical Infrastructure. In *Information Security and Privacy.*

[58] David Rupprecht et al. 2019. Breaking LTE on Layer Two. In *S&P '19.*

[59] Mahmoud Salem et al. 2016. Anomaly Detection Using Inter-Arrival Curves for Real-Time Systems. In *ECRTS '16.*

[60] Shreya Savadatti et al. 2024. An Extensive Classification of 5G Network Jamming Attacks. *Sec. and Commun. Netw.*

[61] Amina Seferagić et al. 2020. Survey on Wireless Technology Trade-Offs for the Industrial Internet of Things. *Sensors* 20.

[62] Paweł Skokowski et al. 2022. Jamming and jamming mitigation for selected 5G military scenarios. *ICMCIS '22* 205.

[63] tec-science. 2019. Discharge of Liquids (Torricelli's law). online. https://www.tec-science.com/mechanics/gases-and-liquids/discharge-outflow-liquid-speed-torricellis-law/, last accessed: 2024-10-21.

[64] Ivana Tomić et al. 2018. Design and Evaluation of Jamming Resilient Cyber-Physical Systems. In *SmartData '18.*

[65] Pavan G V et al. 2022. Survey on Security Risks in 5G Private Industrial Networks. In *I4C '22.*

[66] Zibo Wang et al. 2023. A Survey on Programmable Logic Controller Vulnerabilities, Attacks, Detections, and Forensics. *Processes* 11, 3.

[67] Konrad Wolsing et al. 2023. One IDS is not enough! Exploring Ensemble Learning for Industrial Intrusion Detection. In *ESORICS '23.*

[68] Konrad Wolsing et al. 2022. Can Industrial Intrusion Detection Be SIMPLE?. In *ESORICS '22.*

[69] Konrad Wolsing et al. 2024. Deployment Challenges of Industrial Intrusion Detection Systems. In *ESORICS '24.*

[70] Konrad Wolsing et al. 2022. IPAL: Breaking up Silos of Protocol-dependent and Domain-specific Industrial Intrusion Detection Systems. In *RAID '22.*

[71] Jiarong Xing et al. 2024. On the Criticality of Integrity Protection in 5G Fronthaul Networks. In *USENIX '24.*

[72] Hojoon Yang et al. 2019. Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE. In *USENIX '19.*

[73] Rozhin Yasaei et al. 2020. IoT-CAD: context-aware adaptive anomaly detection in IoT systems through sensor association. In *ICCAD '20.*