Poster: Towards an Automated Security Testing Framework for Industrial UEs

Sotiris Michaelides*, Daniel Eguiguren Chavez*, and Martin Henze*§
*Security and Privacy in Industrial Cooperation, RWTH Aachen University, Germany
§Cyber Analysis & Defense, Fraunhofer FKIE, Germany
michaelides@spice.rwth-aachen.de · daniel.eguiguren@rwth-aachen.de · henze@spice.rwth-aachen.de

***Abstract*—With the ongoing adoption of 5G for communication in industrial systems and critical infrastructure, the security of industrial UEs such as 5G-enabled industrial robots becomes an increasingly important topic. Most notably, to meet the stringent security requirements of industrial deployments, industrial UEs not only have to fully comply with the 5G specifications but also implement and use correctly secure communication protocols such as TLS. To ensure the security of industrial UEs, operators of industrial 5G networks rely on security testing before deploying new devices to their production networks. However, currently only isolated tests for individual security aspects of industrial UEs exist, severely hindering comprehensive testing. In this paper, we report on our ongoing efforts to alleviate this situation by creating an automated security testing framework for industrial UEs to comprehensively evaluate their security posture before deployment. With this framework, we aim to provide stakeholders with a fully automated-method to verify that higher-layer security protocols are correctly implemented, while simultaneously ensuring that the UE's protocol stack adheres to 3GPP specifications.**

***Index Terms*—5G, User Equipment, Industrial Contol Systems, Security Testing**

1. Introduction

5G not only represents the latest generation of mobile networks, serving billions of users globally [1], but also is the first mobile technology to provide low latency and high reliability guarantees required for its utilization in industrial systems and critical infrastructure [2].

However, the integration of 5G into industrial environments substantially expands the attack surface of security-critical environments [3], [4], as new components and communication interfaces are introduced into the system architecture [5]. Although 5G introduces enhanced security mechanisms compared to previous generations, many of these improvements are optional features, leaving network operators with the discretion to implement them or not [2]. Experience from real-world deployments shows that security features are either not being implemented [6] or not configured/implemented correctly [7].

Likewise, the increasing interconnection of industrial systems and resulting broadened attack vectors [8] require the use of secure communication protocols, e.g., TLS [9]. When integrating 5G into industrial networks, their use becomes imperative as (i) user plane (UP) protection in 5G does not provide end-to-end security and (ii) optional UP protection is often disabled due to its substantial impact on network latency [10]–[12], which threatens real-time data transmission as required by industrial use cases. However, large-scale measurements of industrial deployments show that security protocols are often either not used at all or configured insecurely [9], [13].

Consequently, before deploying industrial user equipments (UEs) such as 5G-enabled industrial robots, operators of industrial networks should first check whether both the 5G functionality and security protocols used for industrial communication are implemented and configured securely. While both scientific approaches and practical tools exist to perform such tests *for individual aspects* [14]–[18], a comprehensive framework that allows to automate the execution and evaluation of security tests for both the 5G part and the secure implementation of industrial communication on top of 5G are missing.

Our vision. To support the *secure* integration of 5G-enabled industrial devices, we envision an *automated* security testing framework that assists operators to *comprehensively* test industrial UEs for the correct implementation and configuration of all relevant security features. Such a framework should not only cover 5G specific aspects such as a device complying to unauthenticated commands [17], but also ensure that upper layer security protocols such as TLS are used and correctly configured, e.g., not using outdated ciphers. In the end, such a framework should empower operators to verify the security posture of safety-critical industrial components *before* they get deployed to a production 5G environment.

Our contributions. In this paper, we report on our ongoing work in developing the first automated security framework specifically tailored for examining the security posture of industrial UEs. To this end, we build upon previous research to integrate existing and novel security tests into a unified framework that automatically tests the compliance of the industrial UE's 5G protocol stack with the 3GPP specifications as well as the correct implementation and configuration of secure industrial protocols, especially those relying on TLS.

2. Technical Background & Related Work

To lay the foundation for our work, we introduce the most important aspects of 5G and discuss related work.

5G Components. As depicted in Fig. 1, an industrial 5G network consists of three primary components that together manage both *Control Plane (CP)* and *User Plane(UP)* traffic: the *industrial User Equipment (UE)*, the *Radio Access Network (RAN)*, and the *5G Core*

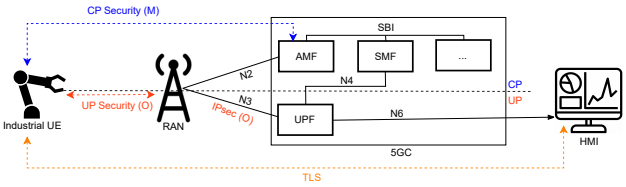


Figure 1: High-level architecture of an industrial 5G network showing the industrial UE, RAN, and 5GC with associated planes and security controls.

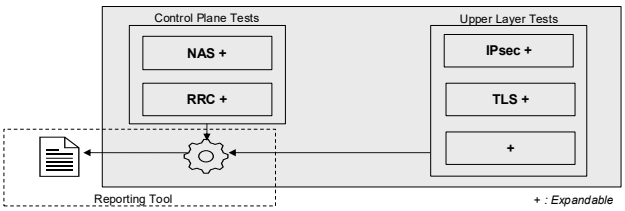


Figure 2: Overview of our framework concept. Its modular design enables the integration of additional test cases and new upper layer protocols.

(5GC). The UE is the end-user device (such as industrial sensors or robots) paired with authentication credentials. UEs initiate connections and generate both UP data (e.g., application traffic) and CP signaling (e.g., session setup, mobility management). To facilitate this, UEs employ the *Radio Resource Control (RRC)* protocol [19] to communicate with the RAN and the *Non-Access Stratum (NAS)* protocol [20] to interact with the 5GC. The RAN serves as the intermediary between the UE and the 5GC, handling all wireless communication. Its responsibilities include among others, managing radio resources and enforcing Quality of Service. The RAN also plays a dual role by relaying both CP signaling (i.e., NAS) and UP data between the UE and the 5GC. At the core of the network, the 5GC consists of modular network functions responsible for processing and routing both types of traffic. CP functions include the Access and Mobility Management Function (AMF), which handles tasks such as authentication and mobility management. On the UP, the User Plane Function (UPF) is responsible for packet forwarding and routing user data to external data networks.

5G Planes & Security. *CP* data, exchanged between network components, is mandated by the 5G specification to be end-to-end integrity protected between the UE and the 5GC (specifically, the AMF). These signaling messages are critical for reliable network operation and support key functions such as session management and mobility handling. In contrast, *UP* data—the actual application (e.g., industrial) data transmitted by the end device—is only optionally protected. Even when optional security mechanisms are enabled (cf. Fig. 1), they do not ensure true end-to-end protection. Interfaces such as N6, which connects the UPF to external data networks, lack standardized security and are left to operator discretion. These gaps highlight the necessity of higher-layer security protocols (e.g., TLS) to ensure end-to-end protection of user data—especially in latency-sensitive deployments.

Related Work. Prior works focus on testing either TLS or 5G CP protocols. Our work bridges these approaches by proposing the first unified framework integrating tests from both fields and automating testing.

Several tools test the security of implementations of security protocols such as TLS and IPsec (e.g., [14], [15]), mostly offering similar functionality. In this work, we use *testssl* [16], a lightweight yet comprehensive command-line tool for automated testing of TLS security features on server endpoints. It provides detailed reports on supported versions and cipher suites, analyzes preconfigured settings for vulnerabilities or misconfigurations, and detects known TLS exploits such as Heartbleed and LOGJAM.

To assess the correctness of individual aspects of the 5G control plane, several academic testing frameworks have been developed. Bitsikas et al. [17] introduced a tool to evaluate UE compliance with 3GPP NAS and RRC specifications, using modified Open5GS and srsRAN instances along with JSON-defined test cases. Upon receiving specific uplink messages, the framework hijacks the 5GC or RAN to inject custom downlink commands, logging interactions via PCAPs and system logs. Building on this, Khandker et al. [18] proposed an automated framework for NAS-layer testing. It generates test cases from user input, executes them via modified network components, and evaluates UE responses using rule-based or LLM-based analysis against 3GPP specifications.

3. Automated Security Testing Framework

While prior work tests individual security aspects of industrial UEs, we strive to integrate a comprehensive set of tests into a unified and automated framework.

Concept. Our framework assesses the security posture of industrial UEs by testing the specification compliance of their 5G protocol stack implementation as well as the correct implementation and configuration of upper layer security protocols. We focus on widely adopted protocols that are secure when properly configured. Our tests aim to identify known vulnerabilities (e.g., TLS Heartbleed) or insecure configurations that could weaken security. For instance, using deprecated algorithms such as RC4 in TLS can expose communications to known attacks.

As depicted in Fig. 2, our automated security test framework integrates tests for the correct implementation of the control plane primary signaling protocols: *RRC* and *NAS* as well as for the correct implementation and configuration of upper layer security protocols such as *TLS* and *IPsec*. Our framework not only automates the execution of such tests but further more unifies the representation of reported test results.

Implementation. The novelty of our approach lies in the full automation of multiple security tests, which is crucial for industrial UEs that rely on secure communication protocols. To showcase the feasibility of our approach, we combine and extend three existing testing tools.

The first component is the tool developed by Bitsikas et al. [17], which conducts a series of static, predefined test cases on the CP of 5G, covering both the NAS and RRC layers. The second component is *testssl* [16], which performs a series of tests on the TLS protocol. The third component is based on the evaluation tool by Khandker et al. [18]. We have expanded its evaluation capabilities for a defined subset of RRC-layer test cases,

#	Testcase	Test Content	Status	Remark
1	NAS_testcase_21	Hooking point: security mode complete Downlink command: identity request 5G-AKA: Completed Message send as: Plain Requested identity: SUCI	Pass	After key establishment, plain message should be discarded
2	RRC_testcase_3	Hooking point: security mode complete Downlink command: security mode command AS security activation: Completed Message send as: Plain integrity_prot_algorithm: nia0	Pass	UE did not process plain Security Mode Command message
3	TLS_testcase_1	Hooking point: client_hello Arguments: --null-ciphers	Pass	Server does not offer NULL ciphers
	ALL	-	Pass	All testcases successfully completed

Figure 3: Our framework consolidates all security testing results in one unified, reader-friendly report.

enabling the framework to examine the UE's behavior against the 3GPP specification [19], [20] on both the NAS and RRC layers. Additionally, we added support for the automatic verification of TLS test case results against the BSI recommendations. Our framework consolidates the results of these different tests to generate a unified, reader-friendly report as exemplarily depicted in Fig. 3.

4. Preliminary Results

As a proof of concept, we deploy our framework in a realistic setup as shown in Fig. 4 to perform preliminary testing. We utilize ROS2, which provides a robotic arm simulation, with all traffic sent by the robot secured using TLS. We further employ a UE with a MediaTek Dimensity 700 baseband as a gateway for the robot, handling all 5G communication. The 5G network is realized using Open5GS, srsRAN, and a URSP B210. We run our automated testing framework on a machine equipped with 128 GB of RAM and an Intel Core i9-14900 processor.

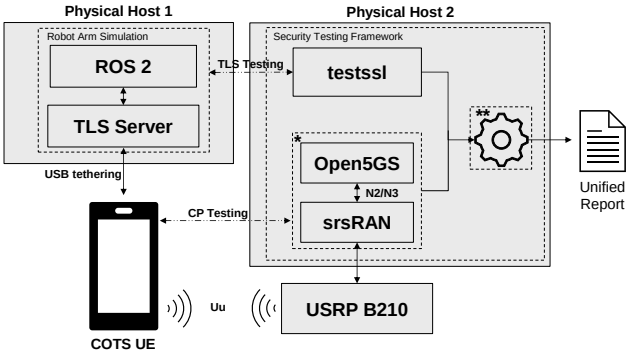
Testing Performance. In its current state, our framework implements security testing for TLS using the *testssl* tool, supporting all of its available features. It also includes 53 test cases for the NAS layer and 16 for the RRC layer. In terms of performance, all tests are executed in approximately 30 minutes. Of this, ∼99% is dedicated to the CP tests, as each test requires a full network restart.

Initial Findings. While our current focus is on expanding test case coverage for 5G signaling protocols and enhancing unified reporting, preliminary testing using our real-world setup and the expanded RRC evaluation has already uncovered a vulnerability in the RRC layer of a tested UE which may lead of the extraction of UE capabilities before security activation. We are in the process of disclosing this vulnerability to the manufacturer.

5. Conclusion & Future Work

With our automated security testing framework, we aim to provide industrial companies with a fully automated tool to efficiently test industrial UEs before deploying them into the production network. Our prototype implementation, which has already been deployed and tested, uncovered a vulnerability in the MediaTek Dimensity 700.

Future work will focus on expanding the CP tests as well as adding more upper layer security protocols, e.g., IPsec, and secure industrial protocols, e.g., OPC UA. Subsequently, we will leverage our framework to comprehensively test commercial industrial UEs.



** [17], ** [18] expanded with RRC evaluation*

Figure 4: Our setup used to gather preliminary results.

Acknowledgments. Funded by the German Federal Office for Information Security (BSI) under project funding reference number 01MO24003B (CSII). The authors are responsible for the content of this publication.

References

[1] A. Koutsos, "The 5G-AKA authentication protocol privacy," in *IEEE EuroS&P*, 2019.

[2] S. Michaelides *et al.*, "Secure Integration of 5G in Industrial Networks: State of the Art, Challenges and Opportunities," *Future Generation Computer Systems*, 2025.

[3] J. M. Vidal *et al.*, "Poster: Mitigation of DDoS attacks in 5G networks: A bio-inspired approach," in *IEEE EuroS&P*, 2017.

[4] J. Bodenhausen *et al.*, "Securing Wireless Communication in Critical Infrastructure: Challenges and Opportunities," in *MobiQuitous*, 2023.

[5] M. Henze *et al.*, "Towards Secure 5G Infrastructures for Production Systems," in *ACNS*, 2024.

[6] O. Lasierra *et al.*, "European 5G security in the wild: Reality versus expectations," in *ACM WiSec*, 2023.

[7] D. Rupprecht *et al.*, "Call me maybe: Eavesdropping encrypted LTE calls with ReVoLTE," in *USENIX Security*, 2020.

[8] L. Bader *et al.*, "Comprehensively Analyzing the Impact of Cyberattacks on Power Grids," in *IEEE EuroS&P*, 2023.

[9] M. Dahlmanns *et al.*, "Missed Opportunities: Measuring the Untapped TLS Support in the Industrial Internet of Things," in *ACM ASIA CCS*, 2022.

[10] T. Heijligenberg *et al.*, "BigMac: Performance Overhead of User Plane Integrity Protection in 5G Networks," in *ACM WiSec*, 2023.

[11] O. Zeidler *et al.*, "Performance Evaluation of Transport Layer Security in the 5G Core Control Plane," in *ACM WiSec*, 2024.

[12] S. Michaelides *et al.*, "Assessing the Latency of Network Layer Security in 5G Networks," in *ACM WiSec*, 2025.

[13] M. Dahlmanns *et al.*, "Easing the Conscience with OPC UA: An Internet-Wide Study on Insecure Deployments," in *ACM IMC*, 2020.

[14] Borja *et al.*, "Iker," https://github.com/libcrack/iker, 2015.

[15] A. Kario, "Tlsfuzzer: Ssl and tls protocol test suite and fuzzer," https://github.com/tlsfuzzer/tlsfuzzer, 2025.

[16] D. Wetter and contributors, "testssl.sh: A free command line tool for testing tls/ssl encryption," https://testssl.sh/, 2025.

[17] E. Bitsikas *et al.*, "UE Security Reloaded: Developing a 5G Standalone User-Side Security Testing Framework," in *ACM WiSec*, 2023.

[18] S. Khandker *et al.*, "ASTRA-5G: Automated Over-the-Air Security Testing and Research Architecture for 5G SA Devices," in *ACM WiSec*, 2024.

[19] 3GPP, "Ts 38.331, v18.5.0," 2024.

[20] 3GPP, "Ts 24.501, v18.10.0," 2025.