

Safety and Security: IO-Link Wireless and OPC UA over 5G under prEN 50742

Henry Beuster, Thomas Doeber, Gerd Scholl

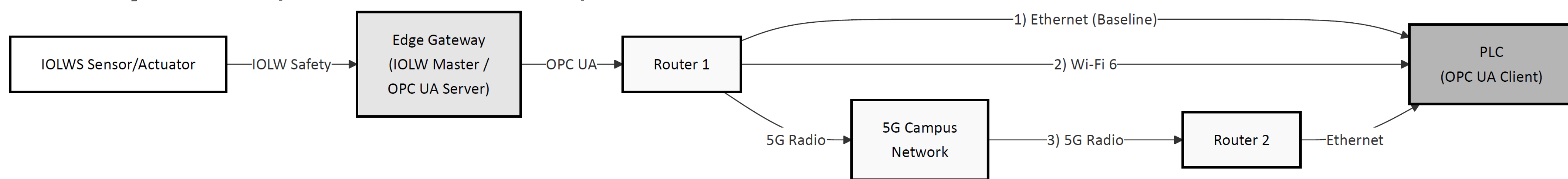


Fig. 1: System architecture and communication chain

Motivation

Challenge: Emerging regulations like prEN 50742 mandate the integration of cryptographic security mechanisms directly into safety-critical data streams.

Problem: While cryptography enhances security, its timing and packet size overheads might violate safety watchdogs and reduce system availability.

Objective: Empirical evaluation of safety-security convergence across a complete control chain, from an IO-Link Wireless Safety (IOLWS) device to a PLC via an OPC UA backbone.

Evaluated Security Configurations

To evaluate the timing impact, the conceptual Safety-Related Security Levels (SRLs) are mapped to concrete configurations at the field and backbone level:

- Plain (Baseline): No safety, no cryptography.
- SRL 0: Safety enabled, no cryptography.
- SRL 1: IOLW: Safety + 4-byte truncated MAC. OPC UA: Safety + HMAC-SHA256 signature (Sign).
- SRL 2: IOLW: Safety + 4-byte truncated MAC. OPC UA: Safety + Aes128Sha256RsaOaep (SignAndEncrypt).
- SRL 3: IOLW: Safety + AES-CCM (128 bit) encryption + 4-byte MAC. OPC UA: Safety + Aes128Sha256RsaOaep (SignAndEncrypt).

Results

Field-Level Bottleneck: Cryptographic execution time is negligible, but payload expansion (from 1 B in Plain to 11 B in SRL 3) severely restricts wireless fieldbus capacity. The maximum number of devices per IOLW track (5 ms cycle) drops from 8 to 2 (Fig. 2).

Backbone Latency: The transition from Plain to SRL 0 (bidirectional safety transaction) dominates the latency increase, while the addition of backbone transport security (SRL 0 to SRL 3) has less impact (+3.86 ms on 5G).

Determinism vs. Average Latency: Wi-Fi 6 achieves lower mean latency under SRL 3 (5.45 ms), but its stochastic channel-access leads to critical latency outliers. Private 5G exhibits higher mean latency (30.88 ms) but provides a deterministic distribution, preventing safety watchdog violations (> 50 ms) more effectively (Fig. 3).

Conclusion

Payload inflation caused by security regulations physically limits the achievable sensor density in high-speed wireless fieldbuses. For backbone networks, Private 5G is preferable to Wi-Fi 6 for safety functions, as it provides the physical-layer determinism necessary to avoid unnecessary system shutdowns in noisy industrial environments.

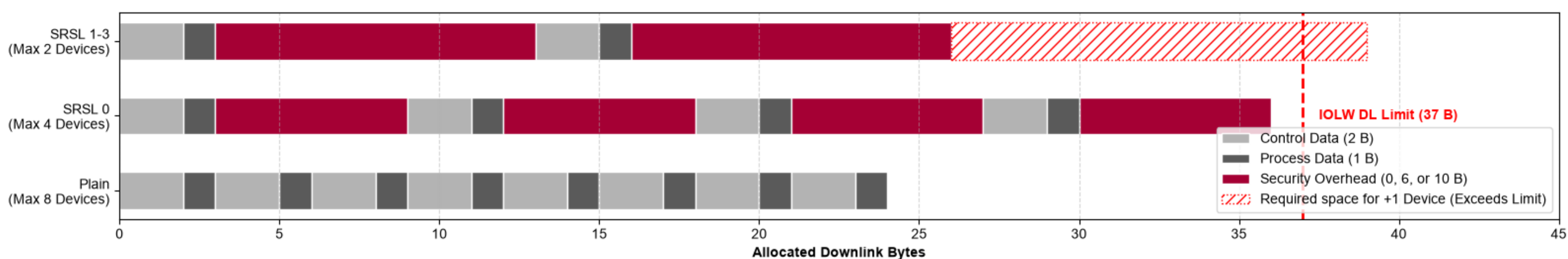


Fig. 2: IO-Link Wireless Capacity Bottleneck (Downlink Shared Budget)

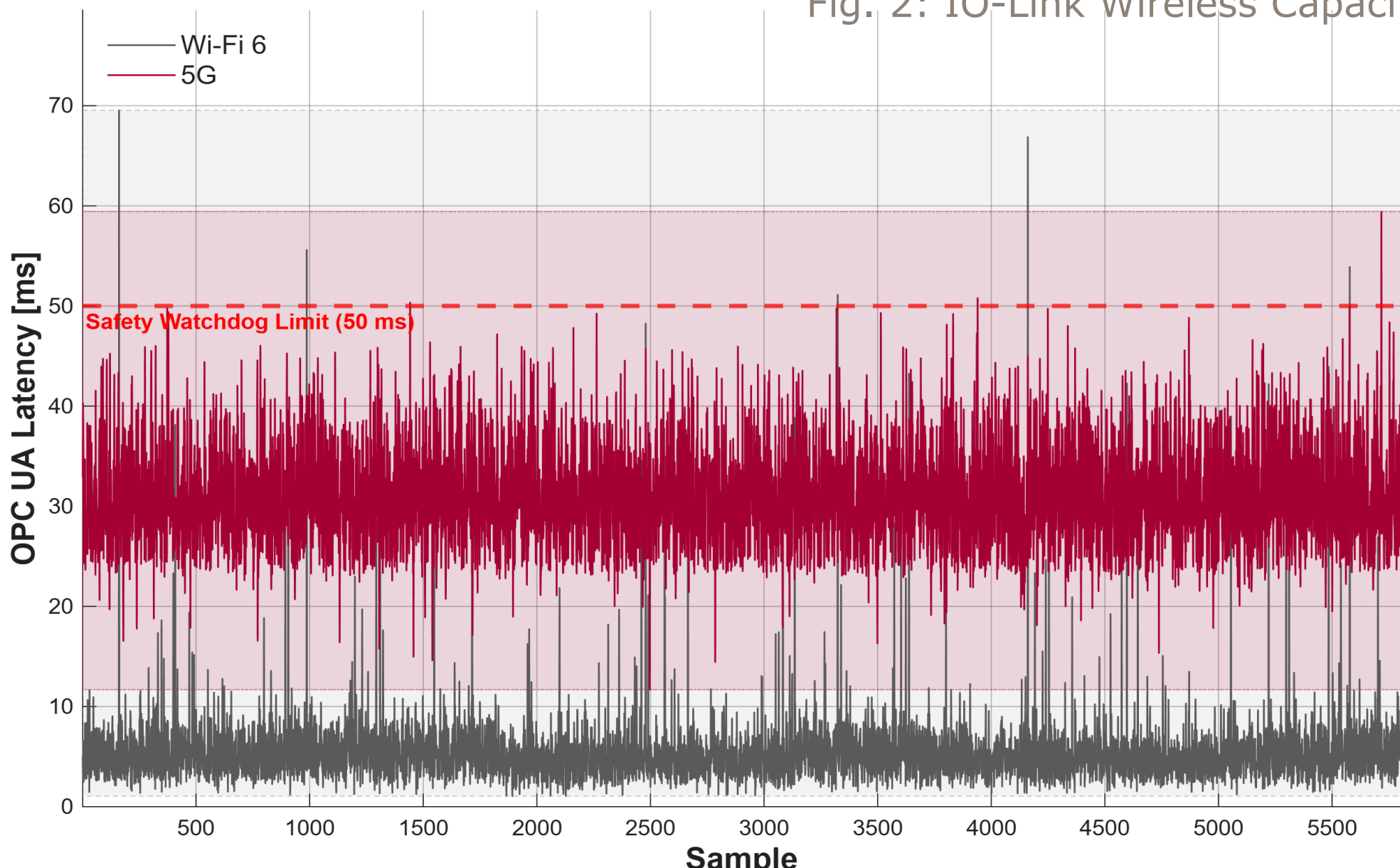


Fig. 3: Latency of Wi-Fi 6 and 5G setup

Outlook

Granular Determinism Modeling: Isolating fundamental latency components (e.g., compute delays vs. cycle-time issues) to establish a detailed determinism model.

Scalability & Resilience Testing: Evaluating the architecture's timing resilience under high network loads, heavy background traffic, and with a significantly scaled-up number of devices.

Protocol & Network Enhancements: Investigating the behavior of OPC UA PubSub implementations over wireless links and analyzing the impact of different 5G network slice configurations on safety critical traffic.



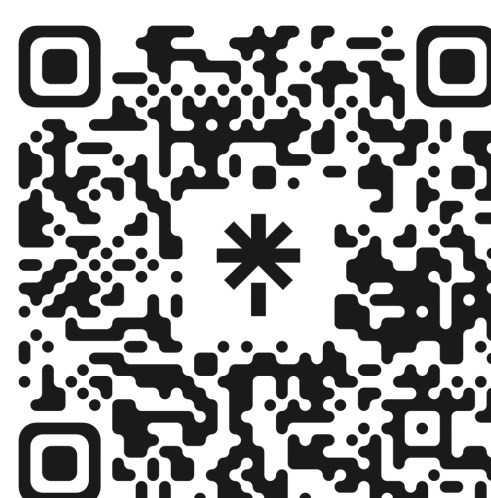
unibw.de



hsu-hh.de



dtec.bw.de



gefördert durch



Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr



Finanziert von der Europäischen Union
NextGenerationEU