PERFORMANCE IMPACT ASSESSMENT OF OPC UA SECURITY FEATURES IN NUCLEAR CONTROL SYSTEMS

LUDGER PETERS
Fraunhofer SIT | ATHENE
Darmstadt, Germany
Email: ludger.peters@sit.fraunhofer.de

GEORGIOS GKOKTIS
Fraunhofer SIT | ATHENE
Heilbronn, Germany
Email: george.gkoktsis@sit.fraunhofer.de

MICHAEL ECKEL
Fraunhofer SIT | ATHENE
Darmstadt, Germany
Email: michael.eckel@sit.fraunhofer.de

Abstract

OPC Unified Architecture (OPC UA) has emerged as the standard communication protocol for industrial automation systems, including critical nuclear facility control networks. While OPC UA's comprehensive security features provide essential protection against cyber threats, their implementation introduces both computation and communication overhead that must be carefully evaluated in time-critical applications.

This paper presents a heuristic performance evaluation of OPC UA security functionalities across different security policy configurations. We analyze the performance impact of various security modes (None, Sign, Sign-And-Encrypt) and their possible configurations on the system performance in a representative control system scenario.

The findings provide practical guidance for nuclear facility operators in selecting appropriate OPC UA security configurations that maintain robust cybersecurity protection while meeting operational performance requirements. The research contributes to security-by-design principles for nuclear industrial control systems, providing empirical data to inform security policy decisions in critical infrastructure.

1. INTRODUCTION

The digitalization and tighter coupling of IT and OT systems fundamentally changed the security posture of industrial control systems (ICS), including nuclear facilities [1], [2]. Modern nuclear facilities increasingly rely on networked digital instrumentation and control (I&C) systems to improve availability and economic performance. But this connectivity also induces new attack surfaces that must be addressed [3], [4], [5]. To address the functionality of digital I&C Systems several communication protocols established over the last decades. One of these prominent protocols is OPC Unified Architecture (OPC UA) [6], [7]. The OPC UA specification incorporates a comprehensive security architecture with configurable security policies and message security modes [8], [9].

Nuclear I&C systems need to comply with rigorous functional and temporal requirements. These are defined at multiple levels. The overarching IAEA standard SSR-2/1 for defines the relevant response times in nuclear I&C control and safety systems [10]. However, all available requirements destinctively lack specific numerical control execution time requirements, as these are subject to the nature of the controlled system. In other words, I&C systems must be "fast enough" for the desired process or safety function. The required response times are derived from plant-specific safety and process analyses and are documented in the I&C requirements specification. The I&C design must then demonstrate compliance by analysis and measurement, as required for example by IEC 61513 [11]. In practice, protection and power-control functions (e.g. reactor power control or turbine control and protection) are often engineered in the order of roughly 10 ms or larger. However most other functions can be much slower, due to the relevant, process based, physical time constants. Microsecond-scale application-level response times do typically not arise nuclear I&C, even though underlying communication and hardware latencies may be in the microsecond range.

Despite extensive research on ICS security and communication-induced delays in networked control, there is limited empirical data on the latency overhead of communication security in I&C communication. This

includes, but is not limited to, nuclear process control systems. Existing work on I&C and Industrial Internet of Things (IIoT) security focuses primarily on architectural aspects and cryptographic hardening, for example via Trusted Platform Modules (TPMs) or Pub-Sub deployments [12], [13]. At the same time, cryptographic performance studies on embedded devices show that resource-constrained platforms can experience non-trivial overhead from symmetric and asymmetric primitives [14], [15], [16], underscoring the need for measurements in realistic control scenarios.

This paper addresses this gap through a heuristic performance evaluation of OPC UA security functionalities in a baseline control system. Targeted to be exploitable for I&C systems in at nuclear applications. We measure round-trip latency and timing variability for three OPC UA message security modes (None, Sign, SignAndEncrypt) under the Basic256Sha256 policy, using a client–server testbed deployed in both virtualized and real-time Linux environments. The measurements are interpreted against conservative delay and jitter envelopes derived from communication delay studies in power systems and transportation cyber-physical systems [17], [18], [19] and from nuclear I&C timing categories and qualification principles [10], [11]. The contributions of this paper are as follows: i) We present experimental evidence that better inform the Security-Performance trade space for OPC-UA implementations, ii) we provide an initial insight of the security performance of OPC UA Field Extension (FX), in performance critical environments.

The remainder of this paper is organized as follows. Section 2 reviews OPC UA security in industrial and nuclear control and summarizes key results on communication latency and control performance. The following section describes the experimental setup, measurement procedure, and evaluation criteria. In section 4 presents the measured results and their interpretation. Section 5 discusses implications for nuclear deployment, provides configuration guidance, and highlights limitations and additional relevant literature. Section 6 concludes the research and identifies directions for future work.

2. BACKGROUND AND RELATED WORK

2.1. FieldBus Security in Industrial and Nuclear Control

Peters et al. [7], analyse the different approaches to the threat assumptions in the three prominent Fieldbus protocols of the European Industrial space. In that paper the open availability of OPC UA stands out. This is furthermore underlined by the availability of the open62541 OPCUA stack [20]. The remainder of this section describes the implementation of OPC UA.

OPC UA is a service-oriented, platform-independent communication standard that unifies data modelling and messaging for industrial automation systems. The OPC UA security architecture provides defence-in-depth through application-layer security, user and application authentication, and integration with transport-layer protections [8]. Message security modes define how integrity and confidentiality are applied to individual messages:

- **None**: no application-layer cryptographic protection
- **Sign**: digital signature to ensure integrity and source authentication
- **Sign-and-Encrypt**: combined signature and encryption to provide integrity and confidentiality

Security policies (e.g., Basic256Sha256) instantiate these modes with specific cryptographic algorithms, typically combining RSA-based asymmetric cryptography with AES and HMAC-based symmetric primitives [8]. OPC UA FX extends these concepts to field-level, high-performance communication, emphasizing consistent security configuration in constrained environments [7], [9].

Industrial adoption of OPC UA has grown rapidly, particularly as part of Industry 4.0 initiatives and converged OT/IT architectures [6]. In IIoT scenarios, OPC UA security can be extended by hardware-based roots of trust such as TPMs [12]. Furthermore, remote attestation mechanisms enabled by TPMs can provide additional assurance by allowing devices to cryptographically prove their software configuration and integrity state to remote verifiers, which is particularly valuable in nuclear I&C environments where system integrity must be continuously verified. However, OPC UA is increasingly considered not only for general industrial applications but also for safety-relevant domains such as nuclear power, where cybersecurity requirements must be reconciled with strict safety and reliability constraints [2], [3].

ICS and nuclear cybersecurity surveys stress that cyber measures must be integrated with functional and timing requirements rather than treated as add-ons [4], [5], [21], [22]. For digitalized nuclear control systems, this implies that protocol-level protections, including OPC UA security modes, must be assessed not only for cryptographic strength but also for their impact on control-loop timing and determinism.

Cryptographic performance studies on embedded platforms show that algorithm choice, key length, and implementation strategy can significantly affect execution time and resource usage [14], [15], [16]. These results indicate that security configurations which are acceptable for supervisory SCADA traffic may not be trivially applicable to faster protection or control loops without careful performance assessment.

2.2. Timing Requirements and Communication Delay in Control Systems

As introduced before, the timing requirements for nuclear power plants are defined by the IAEA in SSR-2/1 [10]. More general requirements like IEC 61508 [23] define the general requirements fore the safety of control systems.

IEC 61513 specifies that performance requirements for systems important to safety, including timing and response characteristics, must be derived from plant safety and process analyses, documented in the I&C system requirements, and verified by analysis and testing [11]. No fixed generic response times are mandated; instead, the "fast enough" criterion is applied per function and plant design. In practice, fast protection and control functions in current reactor designs are often engineered around ≈10 ms response times, while many auxiliary or supervisory functions operate at much slower time scales (seconds to minutes). As these standards deliberately do not include specific timing requirements, the timing evaluation will be based on this 10 ms requirement boundary condition, using a conservative control system stability approach.

3. METHODOLOGY

3.1. Experimental Architecture

We evaluate OPC UA message security modes in a simplified client–server architecture representative of intra-plant sensor data transmission to process controllers.

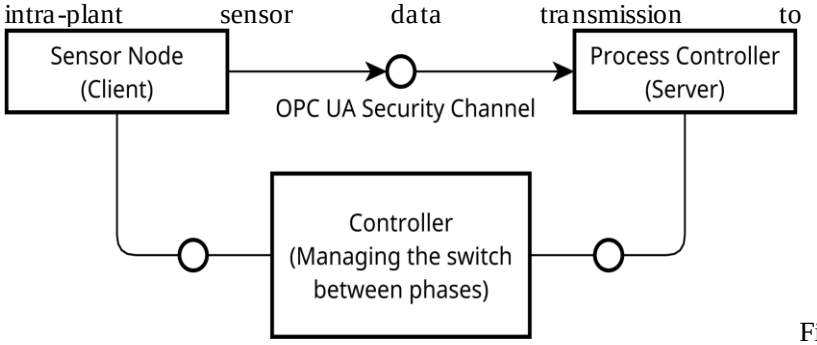

Figure 1 displays the simplified experimental setup. The setup has deliberately been chosen to maximize the overhead impact on data transmission to display a worst-case scenario.

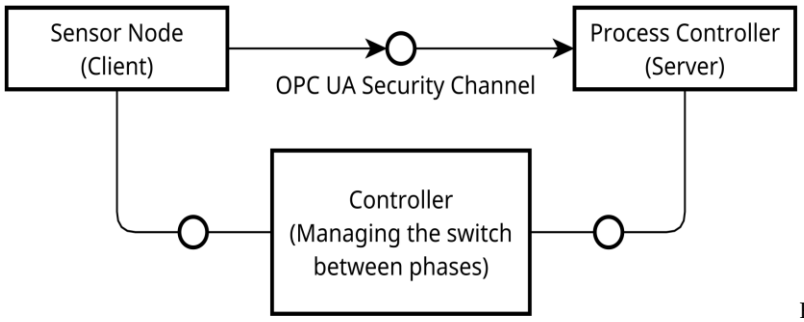

Figure 1: Experimental testbed architecture

- OPC UA Server: Emulates a nuclear process controller that receives sensor data from the sensor nodes. Returning minimal acknowledgments (256-byte) to confirm receipt.
- OPC UA Client: Represents a field sensor node that transmits raw sensor data to the server. Records precise send/receive timestamps to measure send operation latency under security modes.
- Phase Controller: Coordinates security mode transitions during all test phases.

Latency is measured as the client-observed round-trip time from sensor data transmission (Write request) to controller acknowledgment (Write response).

3.2. Execution Environments and OPC UA Configurations

To study the influence of operating-system behavior and execution environment on latency and jitter, we consider three configurations, shown in Table 1.

The virtualized configuration represents a typical non-real-time deployment in a constrained container environment, which was also used for testing and is included to show the impact of a real time vs non real time execution. The PREEMPT_RT configurations represent real-time-optimized deployments on embedded hardware, with real-time scheduling configured to reduce scheduling-induced jitter. Run 2 and run 3 were executed on the same hardware setup to validate the measured run times, as tests with only the sender being deployed on Real Time (RT) capable hardware did report similar delta result while reporting completely different execution times.

Table 1: Execution Environment Configuration

Configuration	Platform	Operating System
Run 1 (virtualized reference)	Docker Container	Ubuntu 22.04 LTS
Run 2 (Real Time)	Raspberry Pi 4 (client), Raspberry Pi 5 (server)	Raspberry Pi OS + PREEMPT_RT
Run 3 (Real Time Validation)	Raspberry Pi 4 (client), Raspberry Pi 5 (server)	Raspberry Pi OS + PREEMPT_RT

3.3. Measurement Procedure and Metrics

1. **Initialization:** Controlled reset, configuration of CPU affinity and real-time scheduling (for PREEMPT_RT runs).
2. **Session setup:** OPC UA secure channel and session establishment.
3. **Steady-state measurement:** The client sends data at a set rate of 1000 messages each second interval for a sustained period of 10 minutes for real-time runs and a short 20 second docker only reference run, under constant payload size and security mode.
4. **Data collection:** The client stores the high-resolution timestamps at request send and response receive using a monotonic clock with nanosecond resolution locally. Round-trip latency L is computed per message as

From the collected data of every run and security mode we compute the following:

- Sample size n
- Mean latency μ
- Standard deviation σ
- Coefficient of variation CV = as a normalized jitter metric
- Minimum and maximum latency (L_min, L_ max)

We interpret the measured latencies in relation to a representative control period T_c as defined in Section 2.2, using the dimensionless delay ratio and the worst-case ratio.

4. RESULTS

4.1. Measured Latency and Jitter

The complete set of latency measurements for all combinations of environment (Runs 1–3) and security mode (None, Sign, SignAndEncrypt) is summarized in Table 2.

In all configurations, mean round-trip latencies are in the 150–225 µs range. The main differences between environments and modes are:

- **Virtualized environment (Run 1):** Mean latencies vary between 167–225 µs, but jitter is high: CV ranges from 0.25 (SignAndEncrypt) to 0.48 (None). The None mode exhibits the largest variability and tail latency, indicating that scheduler effects dominate and can overshadow cryptographic overhead.
- **Real-time environments (Runs 2–3):** Mean latencies cluster around 153 µs (None), 188 µs (Sign), and 212 µs (SignAndEncrypt), with stable results in both runs. Jitter is low and consistent across modes, with CV approx 0.04 in all cases. Maximum observed latencies remain below 423 µs.

Table 2: Summary of OPC UA round-trip latency measurements across runs and security modes. (Run 1: Docker, Runs 2+3: Real-Time Linux)

Run	Profile	Samples	Min (µs)	Max (µs)	Mean (µs)	Median (µs)	Std Dev (µs)	CV
1	None	19523	26.27	462.85	224.74	226.67	107.61	0.48
1	Sign	17894	73.03	321.39	167.43	154.35	54.91	0.33
1	Sign+Encrypt	19168	96.04	360.59	187.92	178.68	46.89	0.25
2	None	599878	75.15	305.4	153.47	153.04	5.93	0.04
2	Sign	599503	110	374.77	188	187.39	7.63	0.04
2	Sign+Encrypt	599272	132.01	422.24	211.92	211.16	8.56	0.04
3	None	599839	75.48	305.75	153.69	153.07	6.91	0.04
3	Sign	599483	108.11	375.01	188.42	187.55	8	0.04
3	Sign+Encrypt	599288	131.31	422.45	211.96	211.25	8.56	0.04

4.2. Security Overhead

In the real-time runs, the impact of OPC UA security modes on latency is clearly visible and consistent across Runs 2–3:

- None → Sign: Mean latency increases from ≈153.5 µs to ≈188 µs, an overhead of about 35 µs (≈22%).
- Sign → SignAndEncrypt: Mean latency increases further to 212 µs, an additional 24 µs (≈13%).
- None → SignAndEncrypt: Total overhead is ≈59 µs, corresponding to a ≈38% increase over the unsecured mode.

Jitter remains low and nearly unchanged across modes (CV ≈ 0.04), indicating that the cryptographic processing cost manifests primarily as a uniform shift in mean latency, not as increased variability.

In the virtualized run, the ordering of mean latencies (None > SignAndEncrypt > Sign) is counterintuitive and reflects scheduler and contention effects dominating cryptographic overhead. This reinforces the conclusion that non-real-time containerized environments are inappropriate for deriving reliable timing guarantees for safety-critical applications.

For $T_c = 5$ ms, even the highest mean latency observed (SignAndEncrypt, ≈212 µs) yields $\delta \approx 0.042$, and the worst-case observed latency (≈422 µs) yields $\delta_{max} \approx 0.084$. Thus, in real-time environments, enabling full message security (SignAndEncrypt) has a negligible effect on delay margins relative to the admissible bounds as discussed in Section 2.2. While a percentile overhead calculation is meaningful, the quantitative overhead is also significant. With a total overhead of 59 µs, it is within the performance requirements of most Field-Bus applications. It is safe to assume that OPC UA FX, given that the same Security Specification also applies for the Field Bus extension, will be performing in similar performance tolerances.

5. DISCUSSION

5.1. Implications for Nuclear I&C Deployment

As shown previously the latency overhead induced by the deployment of security functionalities is clearly measurable in our experiment. Despite inducing nearly 40% overhead the overall latency in the communication network does not change in magnitude and is within the quantitative tolerance boundaries of most Field-Bus applications. Therefore, our conservative loop execution times variation does not significantly change that outcome. As such, these experiments support the application of security functionalities, since the overhead is not significant by margins. However, the remaining stability of control loop execution needs to be proven by the system designers.

It is also noteworthy that this overhead is systematic and not erratic. This suggests that, once the security configuration and platform are fixed, the additional delay introduced by OPC UA security is predictable and can be accounted for in timing analyses and safety demonstrations. This added delay can be considered as a deterministic overhead system behavioral budget and is not exhibiting behavior of unbounded jitter. This property makes our observation conducive to criticality based configurations of the protocol, under specific safety constraints.

5.2. Limitation of this research

To place this research into context, it has to be noted that the following limitations apply:

- **Testbed scope:** The evaluation focuses on point-to-point OPC UA communication between two nodes connected using a simple router. Additional latency and jitter from switches, routers, firewalls, and wireless links are not explicitly modeled and may be significant in some deployments.
- **Single security policy and cryptographic suite:** We evaluate Basic256Sha256 as a representative OPC UA security policy. Other policies, including future post-quantum–resistant options, may exhibit different performance characteristics. The relative ordering of security modes (None to Sign to SignAndEncrypt) is likely to persist, but absolute overheads may change significantly with future algorithm choices.
- **Platform selection:** Raspberry Pi hardware approximates embedded controllers but does not fully represent nuclear-grade PLCs or safety-related platforms.
- **Latency-only focus:** We emphasize delay and jitter. Reliability aspects such as packet loss, reordering, and information freshness (age-of-information) are only qualitatively considered, although they also affect control performance.

Within these limitations, the presented results provide a useful quantitative reference point, as they isolate the OPC UA security processing overhead in a controlled setting and demonstrate that, on representative embedded hardware with real-time scheduling. Future work should extend this analysis to OPC UA FX PubSub deployments, more complex network topologies, and post-quantum enabled security policies to fully characterize the security-performance trade space for next-generation nuclear control systems.

6. CONCLUSION AND FUTURE WORK

In this paper, we evaluated the performance overhead that is induced by switching between the security modes of the OPC UA protocol. We run three separate lines of experimentation, based on various degrees of virtualization and abstraction, measuring the latency between sending an OPC UA frame and the time it takes to write a response on the receiver of the frame (Write-Request to Write-Response interval). We additionally compute an additional latency on our measured times to compensate for any jitter that may inherently be present on the communication channel.

Our results show that the introduced overhead in terms of latency from increasing the security of the communication channel are only marginal in absolute terms, where our worst-case scenario indicates a 59 µs total overhead, from switching between SecurityMode:None to SecurityMode:Sign&Encrypt. This overhead, however,

is still within the tolerance levels of Industrial Communication Channels, and especially squarely under the 10 ms limit of I&C standardized tolerance limits.

Based on this finding, we hypothesize that the OPC UA FX protocol will perform within similar performance boundaries.

We aim to test this hypothesis in our Future Work, where we will be investigating a PubSub TNC implementation of the OPC UA FX protocol. Furthermore, we aim to investigate the performance of post-quantum signing and encryption methods, to have an initial benchmark of the performance of OPC UA and OPC UA FX with PQC methods. Additionally, we plan to evaluate the performance impact of integrating remote attestation protocols and trusted execution environments (TEEs) with OPC UA security, as remote attestation could provide runtime integrity verification of control system components.

ACKNOWLEDGEMENTS

This research work was supported by the National Research Center for Applied Cybersecurity ATHENE [24] and conducted as part of its project "Real-time Automated Attack Isolation for Smart Home Energy Systems" (HomePPSec). ATHENE is funded jointly by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research and the Arts.

REFERENCES

[1] G. Yadav and K. Paul, "Architecture and security of SCADA systems: A review," *Int. J. Crit. Infrastruct. Prot.*, vol. 34, p. 100433, Sep. 2021, doi: 10.1016/j.ijcip.2021.100433.

[2] A. Ayodeji, M. Mohamed, L. Li, A. Di Buono, I. Pierce, and H. Ahmed, "Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors," *Prog. Nucl. Energy*, vol. 161, p. 104738, Jul. 2023, doi: 10.1016/j.pnucene.2023.104738.

[3] J. Peterson, M. Haney, and R. A. Borrelli, "An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants," *Nucl. Eng. Des.*, vol. 346, pp. 75–84, May 2019, doi: 10.1016/j.nucengdes.2019.02.025.

[4] T. N. I. Alrumaih, M. J. F. Alenazi, N. A. AlSowaygh, A. A. Humayed, and I. A. Alablani, "Cyber resilience in industrial networks: A state of the art, challenges, and future directions," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 9, p. 101781, Oct. 2023, doi: 10.1016/j.jksuci.2023.101781.

[5] A. Saini, K. Krishan, and M. S. Gaur, "Analyzing ICS security: A survey of design principles, risks, threats, and mitigation methods," *Comput. Electr. Eng.*, vol. 132, p. 110967, Apr. 2026, doi: 10.1016/j.compeleceng.2026.110967.

[6] "Profinet most widespread, OPC UA on the rise." Accessed: Feb. 03, 2026. [Online]. Available: https://www.industrial-production.de/control-technology/market-study-on-plc-systems--profinet-most-widespread--opc-ua-on-the-rise.htm

[7] L. Peters, G. Gkoktsis, and M. Cäsar, "Comparative Analysis of Threat Assumptions in Field Level Protocol Security," Sep. 2025.

[8] "UA Part 2: Security - 4 OPC UA security architecture." Accessed: Feb. 16, 2026. [Online]. Available: https://reference.opcfoundation.org/Core/Part2/v104/docs/4

[9] "UAFX Part 80: Overview and Concepts - 5.4.4 Security configuration." Accessed: Feb. 16, 2026. [Online]. Available: https://reference.opcfoundation.org/UAFX/Part80/v100/docs/5.4.4

[10] IAEA, *Safety of nuclear power plants: design*. in IAEA Safety Standards Series No. SSR-2 / 1 (Rev. 1), no. v. SSR-2/1 (Rev. 1). Vienna, Austria: International Atomic Energy Agency, 2016.

[11] International Electrotechnical Commission, *IEC 61513 Nuclear power plants – instrumentation and control for systems important to safety – general requirements for systems*, IEC 61513, Geneva, Switzerland., 2011.

[12] O. Gilles, D. Gracia Pérez, P.-A. Brameret, and V. Lacroix, "Securing IIoT communications using OPC UA PubSub and Trusted Platform Modules," *J. Syst. Archit.*, vol. 134, p. 102797, Jan. 2023, doi: 10.1016/j.sysarc.2022.102797.

[13] M. Eckel *et al.*, "Implementing a Security Architecture for Safety-Critical Railway Infrastructure," in *2021 International Symposium on Secure and Private Execution Environment Design (SEED)*, Washington, DC, USA: IEEE, Sep. 2021, pp. 215–226. doi: 10.1109/SEED51797.2021.00033.

[14] D. Abbasinezhad-Mood and M. Nikooghadam, "Design of an enhanced message authentication scheme for smart grid and its performance analysis on an ARM Cortex-M3 microcontroller," *J. Inf. Secur. Appl.*, vol. 40, pp. 9–19, Jun. 2018, doi: 10.1016/j.jisa.2018.02.007.
[15] H. Bühler, A. Walz, and A. Sikora, "Benchmarking of Symmetric Cryptographic Algorithms on a Deeply Embedded System," *IFAC-Pap.*, vol. 55, no. 4, pp. 266–271, 2022, doi: 10.1016/j.ifacol.2022.06.044.
[16] N. B. F. Silva, D. F. Pigatto, P. S. Martins, and K. R. L. J. C. Branco, "Case studies of performance evaluation of cryptographic algorithms for an embedded system and a general purpose computer," *J. Netw. Comput. Appl.*, vol. 60, pp. 130–143, Jan. 2016, doi: 10.1016/j.jnca.2015.10.007.
[17] H. Ali and D. Dasgupta, "Effects of Time Delays in the Electric Power Grid," in *Critical Infrastructure Protection VI*, vol. 390, J. Butts and S. Shenoi, Eds., in IFIP Advances in Information and Communication Technology, vol. 390. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 139–154. doi: 10.1007/978-3-642-35764-0_11.
[18] S. Liu, P. X. Liu, and X. Wang, "Stability analysis and compensation of network-induced delays in communication-based power system control: A survey," *ISA Trans.*, vol. 66, pp. 143–153, Jan. 2017, doi: 10.1016/j.isatra.2016.09.022.
[19] D. Kumar, G. L. Raja, O. Al Zaabi, M. Alkhatib, and U. R. Muduli, "Resilient PID Controller for Communication Latency in Interconnected Power Systems," in *2024 IEEE Energy Conversion Congress and Exposition (ECCE)*, Oct. 2024, pp. 1653–1658. doi: 10.1109/ECCE55643.2024.10861882.
[20] F. Palm, S. Gruner, and J. Pfrommer, "open62541 – der offene OPC UA Stack".
[21] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 9, pp. 52–80, Jun. 2015, doi: 10.1016/j.ijcip.2015.02.002.
[22] Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1–27, Feb. 2016, doi: 10.1016/j.cose.2015.09.009.
[23] International Electrotechnical Commission, *IEC 61508: functional safety of control systems*, Standard IEC 61508, Geneva, Switzerland., 2010. [Online]. Available: https://webstore.iec.ch/en/publication/22273
[24] National Research Center for Applied Cybersecurity ATHENE c/o Fraunhofer Institute for Secure Information Technology SIT, "National research center for applied cybersecurity ATHENE." [Online]. Available: https://athene-center.de/