TU Delft

Delft University of Technology

Document Version
Final published version

Licence
Dutch Copyright Act (Article 25fa)

Citation (APA)
Presekal, A., Rajkumar, V., Goyel, H., Cibin, N., Palensky, P., Godefrooi, J., & Ștefanov, A. (2026). Enhancing Brownfield Digital Substation Cyber Security with HMAC Authentication. In *Procedings of the 2026 IEEE PES International Meeting (PES IM)* IEEE. https://doi.org/10.1109/PESIM67009.2026.11438382

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
In case the licence states “Dutch Copyright Act (Article 25fa)”, this publication was made available Green Open Access via the TU Delft Institutional Repository pursuant to Dutch Copyright Act (Article 25fa, the Taverne amendment). This provision does not affect copyright ownership.
Unless copyright is transferred by contract or statute, it remains with the copyright holder.

Sharing and reuse
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.

Enhancing Brownfield Digital Substation Cyber Security with HMAC Authentication

Alfan Presekal*, Vetrivel Rajkumar*+, Himanshu Goyel*, Nicola Cibin*,
Peter Palensky*, Joey Godefrooi^, Alexandru Ştefanov*
*Delft University of Technology, +TenneT TSO B.V, ^STEDIN

2026 IEEE PES International Meeting (PES IM) | 979-8-3315-6645-6/26/$31.00 ©2026 IEEE | DOI: 10.1109/PESIM67009.2026.11438382

Abstract — **The increasing digitalization of power grids has introduced cyber security vulnerabilities. One of the vulnerabilities is related to the IEC 61850 Generic Object Oriented Substation Event (GOOSE) protocol for time-critical communication between Intelligent Electronic Devices (IEDs). This protocol lacks built-in message integrity and authentication mechanisms, making it susceptible to cyber attacks, e.g., spoofing. To address these vulnerabilities, IEC 62351-6:2020 recommends the usage of a Hash-based Message Authentication Code (HMAC). However, implementing this security measure in existing brownfield digital substations is challenging due to the lack of compatible commercial devices and is economically expensive. Therefore, this research proposes and evaluates a cost-effective cyber security enhancement using commodity hardware, e.g., Raspberry Pi, to implement HMAC-based message authentication for ensuring GOOSE message integrity and authentication in brownfield digital substations with respect to stringent time requirements for the operation of protective relays. The proposed solution ensures message integrity and authentication while maintaining compliance with standard requirements. Validation is performed using real commercial IEDs in a real-time Hardware-in-the-Loop (HIL) architecture, demonstrating that the solution meets substation time requirements. This approach provides a feasible and immediate cyber security enhancement for brownfield digital substations without requiring significant infrastructure changes.**

Keywords— cyber security, digital substation, GOOSE, HMAC, IEC 61850, message authentication, message integrity, operational technology

I. Introduction

Power system automation and communication are driving the transformation toward smart grids. However, increased digitalization introduces significant vulnerabilities, particularly in smart grid cybersecurity [1]. A prominent example is the cyberattack on Ukraine's power grid on December 17, 2016, which disrupted 200 MW of load by exploiting weaknesses in Operational Technology (OT) communication protocols through malicious payloads that opened substation circuit breakers [2],[3]. Additionally, experiments have shown that spoofing attacks can exploit vulnerabilities in the IEC 61850 Generic Object Oriented Substation Event (GOOSE) protocol [4],[5], enabling malicious control of breakers by injecting spoofed GOOSE messages. These incidents highlight the inadequate security of existing OT communication protocols.

IEC 61850 is central to communication in digital substations, replacing analog wiring with Ethernet-based messaging. It enables high-accuracy measurements, simplified device configuration, and real-time performance. Within IEC 61850, the GOOSE protocol transmits time-critical information, such as protection signals among Intelligent Electronic Devices (IEDs) using Ethernet multicast. This allows rapid, low-latency communication essential for isolating faults. However, the original GOOSE protocol lacks built-in message integrity and authentication check mechanisms, making it vulnerable to spoofing attacks.

To address this challenge, the IEC 62351-6:2020 standard has been introduced [6]. IEC 62351-6 addresses cyber security for IEC 61850 GOOSE and Sampled Values (SV) communication protocols used in substation automation, including protocols for communication between devices like circuit breakers, relays, and controllers. It ensures that communications between devices are validated to avoid unauthorized access and spoofing. Moreover, it proposes the adoption of message authentication codes to guarantee the integrity and authenticity of GOOSE and SV messages. For this purpose, the standard recommends the usage of Hash-Based Message Authentication Codes (HMAC) based on SHA-256 or Advanced Encryption Standard Galois Message Authentication Code (AES-GMAC). In this work, we select HMAC for digital substation IED message integrity and authentication checks because AES-GMAC requires an AES custom environment for its application [7]. Therefore, HMAC has more flexibility than AES-GMAC in terms of digital substation implementation.

Despite the growing need for cyber security compliance in digital substations, the IEC 62351-6 security standard has yet to be implemented in the existing infrastructure. A major obstacle is the requirement for system operators to integrate new devices that comply with the standard. To the best of our knowledge, such devices are not yet readily available on the market. This lack of commercially viable solutions makes immediate implementation infeasible. Even when such devices become available, interoperability and financial constraints of replacing or upgrading existing infrastructure pose a significant challenge. For many system operators, the high cost of new equipment and the associated integration efforts make compliance with IEC 62351-6 economically unfavorable. Therefore, in this research, we aim to enhance the cyber security of existing brownfield digital substations by using Raspberry Pi, a relatively low-cost commodity hardware. Our proposed solution can become an immediate alternative solution for enhancing cyber security using legacy devices in brownfield digital substations.

Several prior works have attempted to secure IEC 61850 communications. The authors in [8] implemented encryption and integrity checks for GOOSE and SV messages using AES 128 and HMAC SHA256. However, this implementation is based on an earlier version of IEC 62351-6, which is no longer recommended. In [16], the authors evaluate the performance of various GOOSE integrity checking mechanism in lab set up including HMAC SHA256, AES GMAC 64 and AES GMAC 128. In [9] and [15], a low-latency architecture using FPGAs achieved lower processing time for integrity check. However, the experiments in [9], [15-16], were not validated with actual protection devices. Instead they relied on open source libraries or custom relay implementations. While this could be an effective way for designing new protection devices, it does not provide a direct solution for existing infrastructure, which is

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE
979-8-3315-6645-6/26/$31.00 ©2026 IEEE
Authorized licensed use limited to: TU Delft Library. Downloaded on March 24,2026 at 06:54:34 UTC from IEEE Xplore. Restrictions apply.

typically proprietary and does not support such custom operations. More recently, [11] proposed a geometric algorithm for GOOSE message security using coordinate transformations, but it remains early-stage and is not aligned with IEC 62351-6:2020. A virtual bump-in-the-wire solution was introduced in [10], focusing on SDN-based traffic inspection. This approach does not require major modifications to existing infrastructure, as it introduces an intermediary device to perform the necessary custom operations.

The aforementioned literature review summarized the state-of-the-art add-on implementation of GOOSE message integrity and authentication mechanisms. However, those implementations lack validation using actual commercial relays / IEDs to secure GOOSE communications. Therefore, in this research, we propose and evaluate HMAC-based GOOSE message integrity and authentication using Raspberry Pi commodity hardware to improve cyber security on legacy devices in brownfield digital substations.

To summarize, the key contributions of this work are as follows:

1) We propose an application of HMAC using SHA 256 for GOOSE message integrity and authentication checking in a digital substation with real industrial hardware validation.
2) We demonstrate the implementation of commodity hardware applications, e.g., Raspberry Pi, for improving cyber security on legacy brownfield digital substations. The device modifies the legacy GOOSE packet to implement message integrity and authentication checking and successfully achieves the standard latency requirement below three milliseconds.
3) We present the validation and successful mitigation of GOOSE spoofing attacks using real commercial relays / IEDs in a real-time Hardware in the Loop (HIL) architecture. The HIL testbed represents a realistic environment of the digital substation operation with high fidelity.

The rest of this paper is organized as follows. Section II introduces the IEC 61850 and IEC 62351-6 standards. Section III describes the HIL and experimental setup, and Section IV presents the experimental results and discussion. Finally, section V presents the conclusions and future work.

II. IEC 61850 AND IEC 62351-6 STANDARDS

IEC 61850 is a comprehensive international standard for substation automation systems, facilitating interoperability between devices from different manufacturers. GOOSE, SV, and Manufacturing Message Specification (MMS) are key communication protocols included in IEC 61850 standard. In this work, we focus on the GOOSE protocol, i.e., IEC 61850-8-1. In addition, we also discuss the cyber security enhancement of the GOOSE protocol based on IEC 62351-6. A more detailed discussion is provided in the following subsections.

A. IEC 61850 GOOSE

IEC 61850 GOOSE is a communication protocol employed in digital substations for the transmission of real-time, high-priority messages. The structure of a typical GOOSE message/frame is shown in Fig. 1. It includes the physical destination and source addresses, i.e., Media access Control addresses, Virtual Local Area Network (VLAN) tag, type header, length of the data frame, and data payload. Under the data payload, the status and sequence number fields, i.e., stNum and sqNum, in the GOOSE message are often considered as basic security mechanisms. In the processing algorithm for GOOSE, each time a GOOSE message is sent, the sequence number is incremented by 1, with a maximum value of 2^{32} (an unsigned 32-bit integer) before it resets to 1. When an event occurs in the substation, such as a trip signal, the update frequency of GOOSE messages increases to ensure successful delivery. In this event mode, the transmission period falls between 0.5 and 5 milliseconds. Additionally, the status number is incremented by one, and the sequence number is reset to zero. Therefore, incoming GOOSE messages with a lower status number than the current one are not processed, and the frame is discarded.

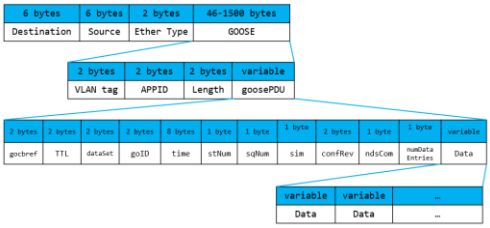


Fig. 1. Structure of GOOSE protocol message.

B. IEC 62351-6 GOOSE with HMAC

The IEC 62351-6:2020 standard recommends the usage of HMAC to ensure the integrity and authenticity of GOOSE and SV messages. In this research, the scope of implementation is limited to GOOSE messages. The standard recommends an extension to be appended at the end of the GOOSE payload with the following fields for integrity and authentication:

- version *(1 byte)*: current version of the extension protocol.
- timeofCurrentKey *(4 bytes)*: UNIX timestamp of when the secret key that is currently in use was generated.
- timeToNextKey *(4 bytes)*: expected UNIX timestamp of next key to be generated. It is to be set to -1 if the key is not planned to be changed.
- InitializationVector *(2 bytes, optional)*: value to initialize the hash algorithm.
- keyID *(4 bytes)*: unique ID of the current key in use.
- Massage Authentication Code value *(8-32 bytes)*: the actual message-authentication tag value.

The updated GOOSE message structure is visualized in Fig. 2. As can be seen, the extension field is appended at the end of the goosePdu, i.e., the GOOSE payload. This extension has a maximum length of 45 bytes, depending on the hashing algorithm used. For example, using SHA-256, the extension would be 45 bytes, with the Massage Authentication Code (MAC) tag being 32 bytes.

C. HMAC Calculation

This subsection presents the implementation of hash-based message authentication code calculation to secure GOOSE messages. The HMAC calculation, based on the reference in [12] is given by the Eq. 1 and Eq. 2. H is the cryptographic hash function; m is the message to be authenticated; K is the secret shared key; K' is a block-sized key derived from the secret key, K; either by padding to the right with zeros up to the block size, or by hashing down to less than or equal to the block size first and then padding to the right with zeros.; $\oplus$

979-8-3315-6645-6/26/$31.00 ©2026 IEEE
Authorized licensed use limited to: TU Delft Library. Downloaded on March 24,2026 at 06:54:34 UTC from IEEE Xplore. Restrictions apply.

represents a bitwise exclusive OR operation; o is the outer padding; and i is the inner padding. In this experiment we use static secret key K predefined in the device.

$$HMAC(K,m) = H\left(\left(K' \oplus o\right) \| H\left(K' \oplus i \| m\right)\right) \quad (1)$$

$$K' = \begin{cases} H(K) \Leftarrow K > blocksize \\ K \Leftarrow K \le blocksize \end{cases} \quad (2)$$

In our specific case, H refers to the SHA-256 algorithm, and m refers to the GOOSE payload, i.e., goosePdu. Since the payload contains stNum and sqNum, the resultant MAC tag of every outgoing GOOSE message is different. Furthermore, due to the inherent nature of secure cryptographic hash algorithms being a one-way process, it is computationally impossible to recover the original message, based on the MAC value alone [12]. Also, since the sqNum updates incrementally during normal operation, due to the avalanche effect of hashing, the HMAC output differs significantly.

III. Hardware in the Loop Experimental Setup

The HMAC HIL implementation follows a structured

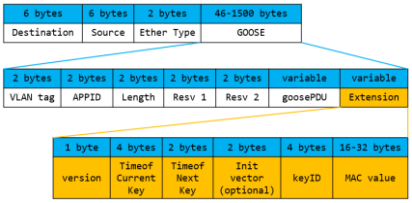


Fig. 2. Structure of GOOSE message with HMAC extension.

architecture, as illustrated in Fig. 3. This architecture is referred to as bump-in-the-wire. This setup involves a dedicated intermediary device, such as a Raspberry Pi, which is responsible for computing the MAC. Once the MAC value is generated, it is appended to the GOOSE message before being transmitted to the subscriber. Upon receiving the message, the subscriber recalculates and verifies the MAC value using the received GOOSE message and a pre-shared secret key. This newly computed value is then compared with the appended MAC in the received message. If the two values match, it confirms that the message is authentic and originates from a legitimate IED. Conversely, a mismatch indicates potential tampering or unauthorized message injection. By incorporating this verification process, the system ensures the authenticity of GOOSE messages, thereby mitigating cyber security threats such as spoofing and replay attacks.

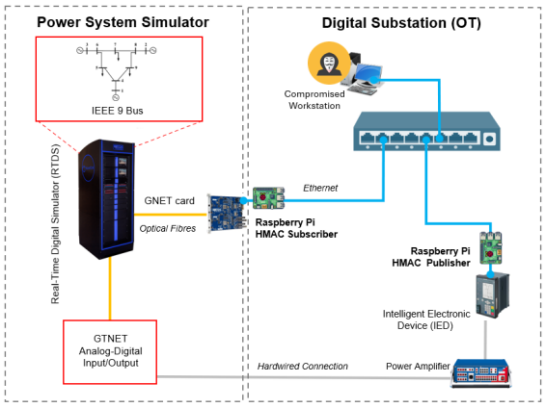


Fig. 3. Architecture of HIL setup of digital substation.

Fig. 4 shows the data flow diagram of the GOOSE message from the publisher IED to the subscriber Real-Time Digital Simulator (RTDS) GTNET card. Between IED to the switch and GTNET card to the switch, there are two Raspberry Pi devices that are implemented as bump-in-the-wire for the HMAC application. The HMAC generation and validation processes are implemented in Raspberry Pi 3B + with CPU ARM Cortex-A53 @ 1.4GHz and 1GB LPDDR2 SDRAM. The software application is implemented using C++ for packet processing and HMAC calculation. This implementation facilitates seamless integration into the communication framework while enhancing cyber security in substation automation networks. The entire operational flow of the HMAC-based authentication system is explained in Algorithm 1.

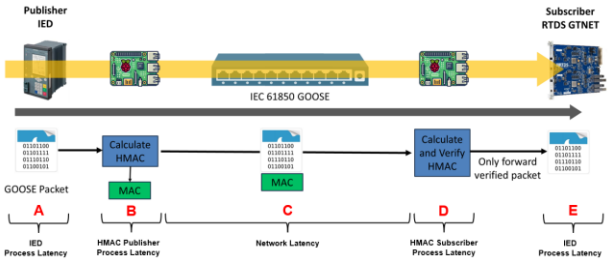


Fig. 4. HMAC bump-in-the-wire implementation flow diagram.

Algorithm 1: GOOSE message integrity and authentication with HMAC

Input : GOOSE message, secret key

Output : Modified GOOSE frame with HMAC tag

While receiving a GOOSE frame **do:**

Extract GOOSE data from a frame;

Identify the end of an APDU field;

Calculate HMAC using a shared secret key;

Append HMAC to GOOSE data;

Send modified frame;

End

In Fig. 3, the digital substation includes a compromised workstation, which allows adversaries to intercept broadcasted traffic from the switches. By collecting GOOSE traffic, the adversary can modify GOOSE packets and inject spoofed packets into the communication network. These malicious packets can mimic legitimate ones, triggering an unauthorized opening of the circuit breaker. This type of attack has been demonstrated in our previous research in [4],[13]. However, in this work, rather than conducting simulated cyber attacks, we focus on mitigation by implementing HMAC authentication. The compromised workstation is used to validate the effectiveness of the proposed HMAC authentication in preventing such attacks.

IV. Experimental Results and Discussion

A. GOOSE HMAC Time Latency

This subsection provides an evaluation of the time latency associated with the HMAC bump-in-the-wire application. The total latency is determined by assessing the delays in five key parts, A to E, as illustrated in Fig. 4. These components include the packet processing time for the HMAC publisher and subscriber, IEDs processing times, and the communication network latency due to message propagation, transmission, and queueing delays. By analyzing these factors, the evaluation shows the overall time latency incurred in the proposed application.

Fig. 5 shows the probability distribution of time latency on the publisher side in part B. Based on multiple experiments,

979-8-3315-6645-6/26/$31.00 ©2026 IEEE
Authorized licensed use limited to: TU Delft Library. Downloaded on March 24,2026 at 06:54:34 UTC from IEEE Xplore. Restrictions apply.

the results indicate that the average latency for the publisher is 0.30 milliseconds, with a standard deviation of 0.03. Similarly, Fig. 6 presents the probability distribution of time latency on the subscriber side in part D, where the average latency is measured at 0.45 milliseconds, also with a standard deviation of 0.03. Additionally, we consider the network latency between the publisher and subscriber in part C. As shown in Fig. 7, the probability distribution of network latency has an average value of 0.35 milliseconds with a standard deviation of 0.02.

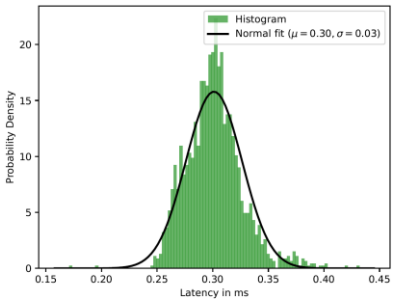


Fig. 5. Probability distribution of packet processing latency in the publisher (Part B).

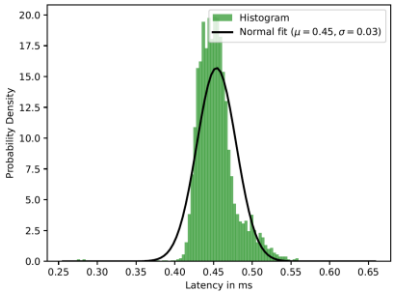


Fig. 6. Probability distribution of packet processing latency in the subscriber (Part D).

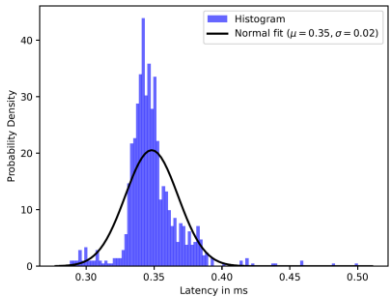


Fig. 7. Probability distribution of network latency (Part C).

Furthermore, the experiment also considers the latency in Part A and E depicted in Fig. 8 and Fig. 9. In Part A, the processing latency of the IED is 0.72 milliseconds, with a standard deviation of 0.09. Meanwhile, in Part E, the processing latency of the RTDS GTNET card is 0.10 milliseconds, with a standard deviation of 0.01. Based on the overall latency from all five parts depicted in Fig. 4, the total average latency from A to E is 1.92 ms. Therefore, this average value successfully meets the standard requirement of Transfer Time class 6 (TT6) with a maximum latency of 3 milliseconds, as specified in the IEC61850-5{ed}: 2013 standard [14]. In the experiment, we also consider the worst-case scenario latency based on the maximum latency from all parts. The largest possible latency based on the total largest latency from all parts is 2.663 milliseconds.

Furthermore, we obtained an IED processing latency validated by STEDIN, one of the distribution system operators in The Netherlands. In this scenario, the latency was measured based on a wired connection between the IED and Omicron, as depicted in Fig. 10. From the measurements, the IED processing latency is between 1.1–1.2 milliseconds. The measured latency aligns well with the maximum latency of 1.2 milliseconds specified in IEC61850-5{ed}:2013. Although this IED processing validation is not integrated into our HIL setup, it provides valuable insight into the potential latency introduced by the HMAC application in actual digital substations. Therefore, the IED processing time significantly contributes to meeting the minimum latency requirements. By incorporating an IED processing time of 1.2 milliseconds, the proposed implementation achieves a total latency of 2.928 milliseconds, which satisfies the TT6 maximum latency requirement. Based on experimental results and actual IED validation data, the proposed solution is effective to enhances the cyber security of GOOSE messages in protection and control applications within digital substations.

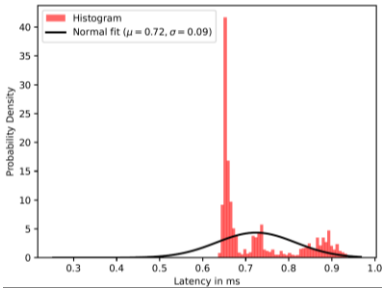


Fig. 8. Probability distribution of IED latency (Part A).

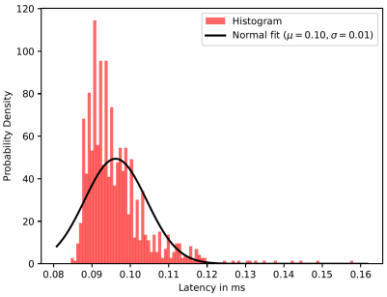


Fig. 9. Probability distribution of GTNET latency (Part E).

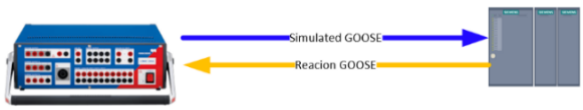


Fig. 10. IED GOOSE time processing validation.

B. Evaluation Against Spoofing Attacks

To evaluate the HMAC bump-in-the-wire application against spoofing attacks, we conduct simulated cyber attacks from a compromised workstation, as depicted in Fig. 3. The spoofing attack is implemented using Python with the Scapy library, a packet manipulation tool that enables the crafting of spoofed data packets and frames. In this simulation, malicious GOOSE traffic is generated to forcibly open the circuit breaker of a power system modeled in the RTDS. With access to the network switch, the attack script executes a spoofing cyber attack by injecting spoofed GOOSE data streams directly into the substation communication network. As a result, without the HMAC bump-in-the-wire application, the spoofed packet successfully opens the circuit breaker, leading to a disruption of the power system operation.

979-8-3315-6645-6/26/$31.00 ©2026 IEEE
Authorized licensed use limited to: TU Delft Library. Downloaded on March 24,2026 at 06:54:34 UTC from IEEE Xplore. Restrictions apply.

In another scenario, the experiments implement the HMAC bump-in-the-wire application, as illustrated in Fig. 4. Deploying the HMAC bump-in-the-wire application on the subscriber side ensures the integrity and authenticity of GOOSE messages. In this setup, adversaries cannot spoof a GOOSE packet without the correct HMAC tag. As a result, any GOOSE message from an attacker is dropped by the Raspberry Pi on the subscriber side, allowing only valid GOOSE messages with the correct HMAC tag to be forwarded to the RTDS GTNET card. This experiment demonstrates that the HMAC bump-in-the-wire application effectively prevents malicious GOOSE command injection attacks in digital substations.

V. Conclusion and Future Work

This research presents a cost-effective and practical approach to enhancing the cyber security of brownfield digital substations by implementing HMAC-based authentication using commodity hardware. Given the cyber security vulnerabilities of the IEC 61850 GOOSE protocol, our solution addresses the lack of built-in message integrity and authentication mechanisms by adopting the IEC 62351-6:2020 standard. Through a real-time HIL experimental setup with real commercial IEDs, we validated the proposed bump-in-the-wire architecture, demonstrating its effectiveness in preventing spoofing attacks and ensuring message integrity and authentication. Our evaluation shows that the system meets the latency requirements for protection signals, maintaining an overall average latency of 1.92 milliseconds, below the TT6 class requirement with a maximum latency of 3 milliseconds, as specified in the IEC61850-5{ed}:2013 standard. In the worst-case scenario, the overall latency reaches 2.63 milliseconds, which is below the TT6 class requirement. Based on the experiment, the proposed solution is effective in enhancing the cyber security of GOOSE messages in protection and control applications within digital substations.

Cyber security validation against simulated cyber attacks confirms that the HMAC bump-in-the-wire application successfully blocks spoofed GOOSE messages, preventing unauthorized control actions such as circuit breaker manipulation. This approach provides an immediate and deployable cyber security enhancement without requiring significant infrastructure upgrades, making it a viable solution for operators of brownfield digital substations. For future work, further optimization of processing efficiency and integration with other substation communication protocols could enhance the robustness of cyber security measures. Extending the bump-in-the-wire concept to support key management and cryptographic agility could further improve security resilience in digital substations.

Another challenge with secure GOOSE protocol implementations is the increased message size resulting from added security measures such as HMAC. This increase can potentially exceed the Ethernet frame size limitation of 1500 bytes, leading to fragmentation and complicating real-time performance. Future research should therefore investigate strategies to balance security features with payload efficiency, ensuring timely message delivery. Additionally, given the higher latency introduced by Routable GOOSE (R-GOOSE) over Wide Area Networks (WANs), inter-substation layer-2 GOOSE communication, such as Multiprotocol Label Switching (MPLS) or direct Ethernet connections, is being increasingly considered. Future studies can focus on secure implementations of these layer-2 connections using HMAC, aiming to achieve both low latency and enhanced cyber security for inter-substation communications.

Acknowledgment

This work was supported in part by the EU Horizon Europe COCOON Project with Grant Agreement No 101120221, in part by the EU Horizon Europe ESTELAR Project with Grant Agreement No 101192574, and in part by the EU Horizon 2020 Marie Sklodowska Curie InnoCyPES Project with Grant Agreement No 956433.

References

[1] G. N. Ericsson, "Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure," in IEEE Transactions on Power Delivery, vol. 25, no. 3, pp. 1501-1507, Jul. 2010.

[2] M. J. Assante, R. M. Lee, and T. Conway, "ICS defense use case no. 6: modular ICS malware," *Electricity Information Sharing Center (E-ISAC) Tech. Report*, pp. 1-27, vol. 2, Aug. 2017.

[3] A. Presekal, A. Ştefanov, V. S. Rajkumar, I. Semertzis and P. Palensky, "Advanced Persistent Threat Kill Chain for Cyber-Physical Power Systems," in IEEE Access, vol. 12, pp. 177746-177771, 2024.

[4] V. S. Rajkumar, M. Tealane, A. Ştefanov, A. Presekal and P. Palensky, "Cyber Attacks on Power System Automation and Protection and Impact Analysis," in Proc. ISGT-Europe, The Hague, Netherlands, 2020, pp. 247-254.

[5] J. Hoyos, M. Dehus and T. X. Brown, "Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure," 2012 IEEE Globecom Workshops, Anaheim, CA, USA, 2012, pp. 1508-1513

[6] International Electrotechnical Commission, IEC 62351-6:2020 - Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850, https://webstore.iec.ch/en/publication/63742, 2020, Accessed: 2025-1-20.

[7] H. Bühler, A. Walz, and A. Sikora, 'Benchmarking of symmetric cryptographic algorithms on a deeply embedded system', IFAC-PapersOnLine, vol. 55, no. 4, pp. 266–271, 2022.

[8] S. M. S. Hussain, S. M. Farooq and T. S. Ustun, "A Method for Achieving Confidentiality and Integrity in IEC 61850 GOOSE Messages," in IEEE Transactions on Power Delivery, vol. 35, no. 5, pp. 2565-2567, Oct. 2020.

[9] M. Rodríguez, J. Lázaro, U. Bidarte, J. Jiménez and A. Astarloa, "A Fixed-Latency Architecture to Secure GOOSE and Sampled Value Messages in Substation Systems," in IEEE Access, vol. 9, pp. 51646-51658, 2021.

[10] O. Tippenhauer, B. Chen, D. Mashima, and D. M. Nicol, 'Vbump: Securing ethernet-based industrial control system networks with vlan-based traffic aggregation', in Proceedings of the 2th Workshop on CPS&IoT Security and Privacy, 2021, pp. 3–14.

[11] M. F. Elrawy, C. Fioravanti, G. Oliva, M. K. Michael and R. Setola, "A Geometrical Approach to Enhance Security Against Cyber Attacks in Digital Substations," in IEEE Access, vol. 12, pp. 18724-18738, 2024

[12] M. Bellare, R. Canetti, and H. Krawczyk, 'Keying hash functions for message authentication', in Advances in Cryptology—CRYPTO'96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18--22, 1996 Proceedings 16, 1996, pp. 1–15.

[13] A. Presekal, A. Ştefanov, V. S. Rajkumar and P. Palensky, "Cyber Forensic Analysis for Operational Technology Using Graph-Based Deep Learning," 2023 IEEE SmartGridComm, Glasgow, United Kingdom, 2023, pp. 1-7.

[14] International Electrotechnical Commission, IEC61850-5{ed}:2013 - Communication networks and systems for power utility automation - Part 5: Communication requirements for functions and device models, https://webstore.iec.ch/en/publication/6012, 2013, Accessed: 2025-1-20.

[15] G. Elbez, H. B. Keller, and V. Hagenmeyer, 'Authentication of GOOSE messages under timing constraints in IEC 61850 substations', in 6th International Symposium for ICS & SCADA Cyber Security Research, 2019.

[16] S. M. S. Hussain, S. M. Farooq and T. S. Ustun, "Analysis and Implementation of Message Authentication Code (MAC) Algorithms for GOOSE Message Security," in IEEE Access, vol. 7, pp. 80980-80984, 2019.

979-8-3315-6645-6/26/$31.00 ©2026 IEEE
Authorized licensed use limited to: TU Delft Library. Downloaded on March 24,2026 at 06:54:34 UTC from IEEE Xplore. Restrictions apply.