End-to-End Security of Smart Meter Infrastructure–Based Control Chains: A STRIDE Analysis of Residual Risks Beyond the Smart Meter Gateway

Julian Britz, Sascha Kaven, Felix Scholl, Kolja Eger and Volker Skwarek
Competence Center for Renewable Energies and Energy Efficiency | CyberSec Research and Transfer Centre
University of Applied Sciences Hamburg
Hamburg, Germany
e-mail: {julian.britz|sascha.kaven|felix.scholl|kolja.eger|volker.skwarek}@haw-hamburg.de
Julian Maximilian Behrensen and Milena Zachow
Electrical Engineering and Computer Science
Technical University of Applied Sciences Lübeck
Lübeck, Germany
e-mail: {julian.maximilian.behrensen|milena.zachow}@th-luebeck.de

***Abstract*—In the future, due to the increasing load and generation in energy systems, distribution system operators will have to intervene manually in a network-effective manner. In Germany, the implementation takes place via the legally mandated Smart Meter Gateway architecture, including a large number of process steps and different roles. This results in a multitude of potential cybersecurity risks, some of which have a significant impact on grid stability. This paper therefore examines the risks associated with ad-hoc control in the event of a grid congestion situation. The results can be applied to interventions pursuant to §14a of the German Energy Industry Act in the event of excessive loads and to §9 of the German Renewable Energy Sources Act in the event of excessive generation, as the data flow is identical in both cases. To the best of our knowledge, we therefore provide the first comprehensive threat analysis with a focus on these two legal provisions. We show that various risks prevail, particularly at the endpoints. However, despite the multitude of specifications, the Smart Meter Gateway is not without risks. Across all steps, the use of TLS 1.2 and missing acknowledgments poses a significant security risk. To counteract these, we identified mitigations that need to be taken into account for further legal requirement development. We provide an overview of the German implementation of the Renewable Energy Directive and the measures taken to maintain grid stability. We also highlight the resulting cybersecurity risks and how they can be addressed.**

Keywords-Smart Meter Gateway; §14a EnWG; §9 EEG; Load Control; STRIDE Threat Modeling.

I. Introduction

The German implementation of the Renewable Energy Directive (RED) represents a unique approach. While most countries primarily rely on incentives, Germany enables direct intervention by Distribution System Operators (DSO) [1]. With the accelerating transition to renewable energy sources, power grids face increasing challenges from variable generation and demand patterns. The most prominent is grid congestion, where the available distribution capacity is insufficient to accommodate the current power flows. Therefore, in order to protect grid stability, German DSO have the ability of intervening in home owners systems in an effective manner. Due to the high security requirements, a large number of specifications had to be defined for the implementation of the Smart Meter Gateway (SMGW) architecture. Here, the SMGW serves as the central security anchor and communication hub. End consumers with an annual consumption between 6 000 and 100 000 kWh, as well as systems in accordance with §14a (3) of the German Energy Industry Act (EnWG), are eligible for the installation of SMGW. The mandatory installation quota corresponds to the legal requirements at 20.2% on 30 September 2025, whereas the overall proportion is only 3.8% [2]. In contrast, the proportion of smart meters installed in France reached 90% in 2021 and in the UK more than 60% at the end of 2023 [3][4]. However, it should be noted that their functionality differs fundamentally. While in France and the UK, smart meters are largely responsible for transmitting measured values, in Germany they also act as a central link in the transmission of control signals. This necessitates significantly higher security requirements.

The German energy industry is currently implementing §14a EnWG on the control of flexible loads. According to the legally mandated §14a (3) EnWG flexible loads are defined as electric vehicle charging infrastructure, heat pumps, air conditioning and stationary energy storage systems, which can be summarized as Controllable Local Systems (CLS) [5]. If transmitted measured values indicate a grid congestion situation, §14a EnWG enables DSOs to request temporary load reductions from CLS with an installed power above 4.2 kW. In the interest of fairness, the targeted plants must be selected without discrimination [6].

Furthermore, the transmission of the control signal relies on a complex and highly distributed communication chain spanning across regulated infrastructure, backend systems and customer-owned environments. The backbone of this chain is formed by the SMGW, which is comprehensively secured by the German Federal Office of Information Security (BSI) technical guidelines [7][8]. These guidelines define cryptographic mechanisms, certificate-based authentication and operational processes for secure Wide-Area-Network (WAN), Local-Metrological-Network (LMN), Home-Area-Network (HAN) and Local-Area-Network (LAN) communication. Whereas, the HAN is a subnet of the

LAN containing only the CLS-adapter [9]. Components and responsibilities for these are shown in Figure 1. It should be noted that the role of the External Market Participant (EMT) can also be fulfilled by the supplier or direct marketer. However, an ad-hoc control signal can only be sent by the DSO, as it affects grid stability. Due to the guidelines given, the SMGW and its directly connected communication partners constitute a tightly regulated security domain with a high degree of standardization.

In the WAN, the Gateway Administrator (GWA) is the only role authorized to contact the SMGW without an existing connection. The DSO acts in the role of the EMT. When exclusively receiving data, the passive EMT (pEMT) role applies and when generating and transmitting control signals, the role of the active EMT (aEMT) is used. The specific control commands are transmitted via a proxy mechanisms and executed by customer-side CLS-adapter before it is forwarded either via phase-free relay contacts or digitally to downstream CLS.

The extension of the SMGW centered architecture shifts the effective system boundary into environments that are only partially standardized, heterogeneously implemented and mainly outside the direct control of regulated actors. Customer routers, (cloud-based) Energy Management Systems (EMS) and locally connected devices introduce additional trust boundaries and dependencies not fully addressed by existing technical guidelines. Consequently, there is a recognizable structural asymmetry in the system's security posture. On the one hand, communication segments adjacent to the SMGW are strongly protected through mutual TLS, certificate pinning and strict profile-based authorization, on the other hand, residual risks arise at architectural endpoints. We identified the following predominant risks:

- missing semantic binding of control commands to assets [10],
- availability dependencies on customer-provided infrastructure [11],
- weak security of local device ecosystems behind the CLS-adapter [12],
- information disclosure in backend systems [13],
- Denial of Service (DoS) during SMGW wake up [14],
- the use of TLS version 1.2 [15][16],
- repudiation due to lack of explicit acknowledgments along the §14a EnWG control chain [17]

These weaknesses can undermine both the effectiveness and trustworthiness of §14a EnWG control measures, even in fully compliant implementations.

This paper applies a systematic STRIDE threat modeling approach to an end-to-end ad-hoc control signal transmission process, explicitly including backend systems and the customer domain in scope. Ad-hoc control refers to proxy communication channels that are dynamically established by the SMGW on request, whereas scheduled variants rely on predefined activation times or recurring communication windows [18]. The aim of this paper is not to challenge the robustness of the SMGW security architecture, but to identify and characterize open risks beyond its immediate protection domain.

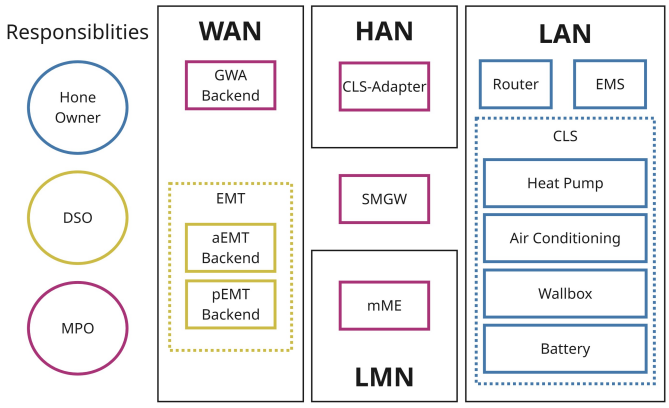

Figure 1. Overview of the SMGW components across the WAN, HAN, LAN and LMN.

In Section II, we present the methodological approach, including definitions, assumptions and limitations. Section III describes the process of transmission of control signals in detail. Based on this, Section IV presents the remaining cybersecurity risks before describing the potential threat scenarios is Section V. Afterwards, necessary mitigations are shown in Section VI. Finally, the results are summarized in Section VII and future work is discussed in Section VIII.

II. Methodology

This paper uses a structured threat modeling approach based on the STRIDE methodology to identify and analyze cybersecurity risks in the §14a EnWG and §9 of the German Renewable Energy Sources Act (EEG) control chain using OWASP Threat Dragon [19]. STRIDE was proposed by Microsoft and represents a bridge for six different types of security threats [20]:

- *Spoofing*: authentication weaknesses,
- *Tampering*: integrity violations,
- *Repudiation*: missing non-repudiation mechanisms,
- *Information Disclosure*: confidentiality violations,
- *Denial of Service*: availability constraints,
- *Elevation of Privilege*: privilege escalation.

It was selected due to its systematic and attacker-oriented classification of threats, making it well suited for complex and distributed systems with multiple trust boundaries and heterogeneous actors [21].

A. Scope Definition

The modeled architecture extends across the control signal transmission chain in accordance with §14a, starting from the backend systems of an aEMT, traversing the gateway administration and communication infrastructure and extending into the customer domain where control actions are executed. In the WAN, the SMGW typically communicates via LTE, CDMA 450 MHz or Broadband Powerline communication (BPL)

[22]. Customer-side components and cloud-based services are deliberately included within the scope.
The model incorporates:

- Backend systems of actors in the WAN
  - GWA, commonly fulfilled by the Metering Point Operator (MPO)
  - EMT, in case of ad-hoc control fulfilled by the DSO
- SMGW with its WAN, LMN and HAN interfaces,
- Metering infrastructure in the LMN with its SMGW interface,
- CLS-adapter with its SMGW and LAN interfaces,
- Proxy-based communication channel between WAN and HAN participants,
- Customer routers, (cloud-based) EMS and CLS.

Supply chain attacks are not within the scope of this analysis. This exclusion applies to vulnerabilities through compromised firmware, third-party software or manufacturer-operated backend platforms. It is nevertheless important to mention that recent findings underline the relevance of such risks, e.g., critical security weaknesses in inverter systems and associated monitoring platforms found by Bitdefender in 2024 [23].

B. Trust Assumptions and Communication Modes

It is assumed that the specifications defined in the BSI TR-03109 series are implemented, meaning that communication segments directly connected to the SMGW rely on mutual TLS using X.509 certificates issued by the Smart Meter Public Key Infrastructure (SM-PKI), certificate pinning and profile-based peer authentication. This includes the WAN-side roles of the GWA and the EMT. For the CLS-adapter and the modern Metering Equipment (mME), a direct trust model is applied, as defined for CLS communication in the BSI TR-03109-5 series [9]. In this, trust anchors are installed prior to first use through organizational processes with self-signed certificates for subsequent TCP/TLS communication.

C. Threat Identification Using STRIDE

Threats were identified and classified according to the six STRIDE categories. Next, they were divided into those that are effectively mitigated by existing technical guidelines and those that remain open due to missing or incomplete safeguards. Threat severity was assessed using the Common Vulnerability Scoring System (CVSS) score to support prioritization. Nevertheless, reliance on numerical risk scores is avoided. The emphasis is on identifying structurally open attack vectors and assessing their potential impact on overall system operation.

D. Analysis Focus and Limitations

The analysis focuses on risks that affect the correctness, availability and accountability of §14a EnWG and §9 EEG control actions. Although our findings do not imply that existing standards are insufficient, they highlight that strong transport-layer and identity security at standardized interfaces do not automatically translate into end-to-end operational security. Given the critical role of grid stability in maintaining reliable power supply and the potential consequences of compromised control action, which range from localized blackouts to cascading failures across regional networks, understanding these residual risks is essential for DSOs and regulators. Therefore, our findings need to be interpreted as complementary to compliance-focused security assessments and as a basis for targeted improvements at system endpoints and organizational boundaries.

III. Ad-Hoc Control Signal Transmission Process

In this section, we describe the data flow in the ad-hoc control signal transmission process step by step. The individual steps are enumerated below and illustrated in Figure 2. The process is based on the metering concept defined by the Association for Electrical, Electronic & Information Technologies (VDE) Forum Network Technology/Network Operation (FNN) and does not provide separate measurement of the CLS [24].

1. First, electrical measurement values are captured at the mME and transmitted to the SMGW via the LMN interface [8]. Communication is based on a communication profile configured and implemented by the GWA. Tariff Use Cases (TAF) determine which data are transmitted and at what times. In case of §14a EnWG, the tariff use case 10 (TAF10) is decisive, involving grid relevant data, such as active and reactive power [25]. The SMGW acts as the primary communication station, actively querying or receiving measurement data. Communication between mME and SMGW is secured using mechanisms defined in BSI TR-03109-1, including authenticated and integrity-protected transport protocols, whereby the SMGW acts as the central trust anchor and only accepts measurement data from administratively configured devices.
2. After collection by the SMGW, the prepared measurement data are transmitted to authorized external systems, either directly to the EMT or via a GWA acting as an intermediary when regulatory requirements mandate encryption. In both cases, transport security is ensured through mutually authenticated TLS connections, with the SMGW acting as the initiating client.
3. Data are received and evaluated by the pEMT to assess the current grid state. Based on this and/or further measurements, the EMT derives control decisions.
4. If the request of a load reduction is necessary, the aEMT sends a request via the web API of the GWA to initiate a CLS communication channel at the SMGW between the aEMT and the CLS-adapter. This channel is established specifically for control communication and is distinct from the measurement data paths.
5. Afterwards, the GWA sends an unencrypted UDP wake-up message to the SMGW requesting the establishment of a TLS connection between them.
6. If certain conditions are met, such as the absence of a current connection, the SMGW establishes a management connection to the GWA. By means of this connection, the GWA requests the establishment of a TLS proxy communication channel between the CLS-adapter and the aEMT. Proxy communication profiles, configured by the GWA beforehand,

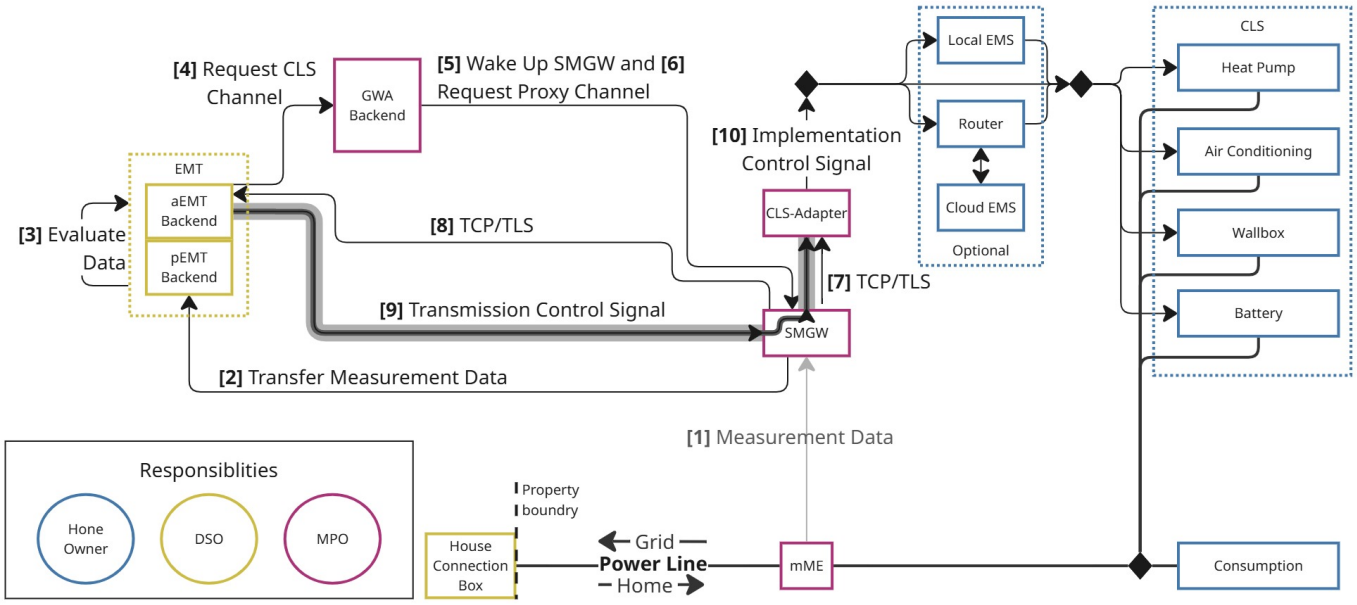

Figure 2. Ad-hoc control process according to §14a EnWG.

define which aEMT is permitted to communicate with which CLS-adapter.

7. Based on the provided conditions, the SMGW opens a TCP/TLS connection to a CLS-adapter in the HAN. This connection forms the HAN-side leg of the end-to-end TLS proxy channel between the CLS and the aEMT. It minimizes coupling between standardized metering functions and application-specific control protocols, but also shifts responsibility for semantic correctness to the communicating endpoints.
8. Subsequently, this is also done on the WAN with the aEMT as the endpoint. Together with HAN-side connection the SMGW forms a transparent, end-to-end proxy channel, without imposing interoperability or security requirements on the application protocol carried inside the tunnel.
9. After this, the SMGW relays application data between the aEMT and the CLS-adapter and acts solely as a transport proxy [18][26]. The application protocol inside the tunnel can conform to IEC 61850, EEBUS (CLS.EEDI) or OpenADR [9].
10. Control signals received by the CLS-adapter are forwarded via ethernet to a EMS or directly to the controllable device [27]. If an EMS is used, it can either be processed locally within a customer-side EMS device or in a cloud-based EMS backend [28]. In the latter case, the signal traverses the customers router and the public Internet to the EMS backend, where it is processed and subsequently sent to the CLS. This communication resides outside the regulated SMGW security domain and marks the responsibility boundary between the MPO and the CLS operator [28][29].

IV. Open Cybersecurity Risks

The SMGW and its standardized communication interfaces are effectively protected by regulatory requirements. Still, a significant number of relevant cybersecurity risks remain open at the architectural endpoints. These open risks concentrate primarily at two locations:

- Backend systems operating in the role of an aEMT and
- Customer domain downstream of the CLS-adapter

Our threat analysis leaks a variety of risks in the ad-hoc control signal transmission process. In total, 108 threats were found, whereby 24 remain without sufficient mitigation. The overall results of the STRIDE analysis are shown in Figure 3 and the threat model and threat report are publicly available at [30].

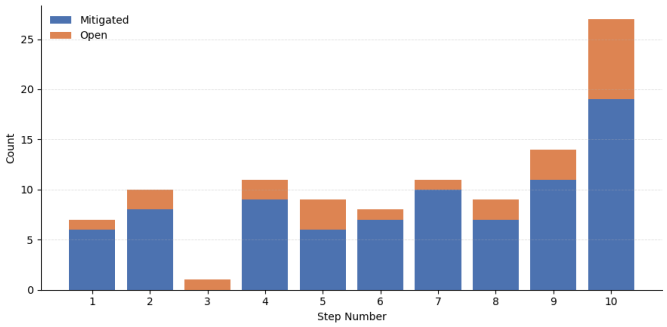

Figure 3. Open and mitigated threats along the process chain.

The identified risks can be grouped into general Cyber-Physical System (CPS) risks that inherently arise whenever control functionality depends on customer-operated infrastructure and structurally novel risks that specifically result from the SMGW architecture.

A. General CPS Risks

1) Availability Dependencies on Customer-Provided Infrastructure: While communication between the SMGW and

backend systems is, with the exception of signal strength and the resulting accessibility issues, designed to be robust, the execution of control commands depends on the availability of local networks, customer routers and in some deployment models (cloud-based) EMS. Through potential disruptions of these components, a systematic availability risk arises, as it would impede signals from reaching the CLS. This is particularly interesting in light of the fact that it cannot be mitigated through cryptographic or protocol-level security measures.

2) Security Gaps Behind the CLS-Adapter: Hardware and Software residing in front of the meter (directly connected to the SMGW) adhere strictly to requirements. For example, the GWA needs to be ISO27001 certified and in case of an external cloud, a risk-analysis is mandatory [31]. The situation is different for EMS and behind-the-meter CLS (connected to the CLS-adapter without direct connection to the SMGW). There are no requirements regarding the use of cloud providers or standardized protocols, whereby the VDE FNN recommends the use of the KNX- and EEBUS communication standards for the transmission of control signals [32]. Still, compromised local devices or insufficiently isolated network segments allow attackers to inject unauthorized control commands, escalate privileges or interfere with legitimate control actions [33].

B. SMGW Architecture Specific Risks

1) Endpoint Identity and Channel Binding Ambiguities: First, risk arises from the semantic binding between control commands, communication channels and controlled assets. Although the proxy-based TCP/TLS connections between the SMGW, the aEMT and the CLS-adapter are strongly authenticated at the transport layer, the association at the aEMT side of an incoming proxy connection with a specific CLS is not enforced by standardized mechanisms. If channel differentiation relies solely on loosely coupled identifiers, control messages may be misattributed or routed to unintended recipients. As a result, correct channel-to-asset binding becomes a shared responsibility between the aEMT and the CLS operator.

2) Information Disclosure at Backend and Endpoint Systems: In addition to attacks with direct effect on the control signals, sensitive operational data, such as grid states and measurement data may be exposed through logging, monitoring interfaces or insufficient access controls at backend systems and customer-side components.

3) SMGW waking-up risks: As the wake-up message, send by the GWA and received by the SMGW, uses UDP, attackers may observe, record and replay structurally valid messages. An attacker may be able to reconstruct valid-looking messages and repeatedly transmit them to the SMGW. Although the consequences of transmitting a valid message are minor and the number of valid messages per minute is bound to 10, there are no requirements limiting the number of invalid messages. While replayed messages can result in a denial of service by triggering the rate limit, invalid messages can lead to a denial of service through resource exhaustion.

4) Mandatory TLS 1.2 Usage: A notable concern arises from the mandated use of TLS version 1.2 for securing communications within all steps [8]. While TLS 1.2 provides robust authentication and encryption, recent research, including algorithm substitution attacks on cryptographic protocols (ASAP) [15] has demonstrated that it remains susceptible to sophisticated subversion attacks. In such algorithm substitution attacks (ASA), adversaries can covertly replace cryptographic implementations with subverted versions that leak secret information embedded within protocol messages. The ASAP paper described how TLS 1.2, unlike TLS 1.3, does not mandate mechanisms to cryptographically bind or attest to the algorithms in use throughout the handshake and data exchange phases. As a result, one can embed maliciously altered random number generators, signature schemes or encryption primitives, which allow the attacker to decrypt the communication, inject false data or otherwise undermine the confidentiality and integrity without raising traditional alarms or detection mechanisms. In addition, TLS 1.3 streamlines the handshake process, which reduces latency and enhances connection setup speed by reducing round trips. It also removed support for vulnerable and outdated cryptographic algorithms, such as AES-CBC, in favor of elliptic curve Diffie-Hellman (ECDHE) and authenticated encryption with associated data (AEAD). The handshake message message is also encrypted and forward secrecy is enhanced, ensuring long-term key compromises do not expose past communication sessions [34].

5) Repudiation Risks Due to Missing End-to-End Acknowledgments: Furthermore, repudiation is likely to happen due to missing acknowledgments at any stage. While certain process steps provide indirect confirmation (e.g., the establishment of a management or proxy connection, TCP), we found that no component explicitly acknowledges successful processing or execution of the requested action. In particular:

- GWA does not explicitly acknowledge aEMT requests to initiate CLS communication
- SMGW does not confirm the receipt of wake-up messages
- Neither EMS nor CLS confirm the successful execution of control commands

The absence of explicit acknowledgments prevents reliable verification of whether a requested load reduction was actually implemented. As CLS are not required to have a separate mME, it is also not possible to determine from the counter values whether the control signal has been carried out or not. This offers the possibility for home owners to actively prevent the realization of control signals.

The VDE FNN is already aware of this problem, which is why it has published a paper entitled "Control with verification in the SMGW" that describes implementation with confirmations [35]. However, this publication is not binding. In general, the control section is completely remodeled. The control signal, including the value to which it has to be reduced, is sent directly from the aEMT to the GWA. The proxy channel is not used in this case. However, sending the power value in the first message accelerates the execution of the control action, reducing opportunities for intermediate verification steps or

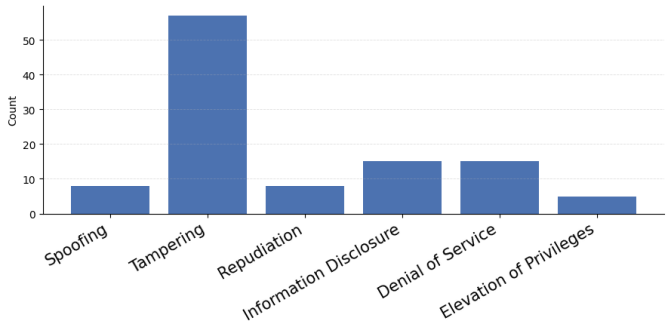

Figure 4. Distribution of identified threat types.

anomaly detection mechanisms that occur during the multi-step communication sequence. Furthermore, this approach does not provide a solution for ensuring the final implementation of the CLS.

C. Representative Threat Scenarios

The following examples illustrate what these risks can look like in practice.

TABLE I. REPRESENTATIVE ATTACKER PROFILES AND OPERATIONAL IMPACT

Scenario	Attacker Profile	Impact
Customer-domain disruption	External network adversary	Command not executed
CLS downstream compromise	Compromised local device or EMS	Unauthorized control injection
Channel misbinding (aEMT)	Compromised backend actor	Unintended load reduction
Backend information leakage	Insider or external backend attacker	Exposure of grid or measurement data
wake-up replay / flooding	External network attacker	Failure to execute control signals
TLS 1.2 subversion	Advanced cryptographic adversary	Confidentiality/integrity compromise
Missing acknowledgments	Home owner	Unverifiable control execution

Table I shows that attacker profiles and motives vary. To minimize risks, appropriate mitigations are presented in the following.

D. Summary of Risk Distribution

While major threats appear on the WAN- and LAN-side endpoints, the BSI decided to require UDP for waking up the SMGW and therefore reduce connection overhead, without rate limiting for valid and invalid messages resulting in a DoS risk. The EMT is responsible for preventing TCP/TLS connection misrouting, while homeowners must ensure secure IT operations within their LAN. The usage of TLS version 1.2 offers attackers additional vectors. Lastly, the repudiation due to missing acknowledgments in all steps remains an unresolved problem with potentially high risks. Although the majority of identified threats, as shown in Figure 4 are tampering cases, most of these risks are already mitigated, reducing their overall impact on the systems security posture.

V. RELEVANT MITIGATIONS

In this section, we summarize the main technical and organizational measures that can reduce the identified residual risks along the ad-hoc control signal transmission chain.

A. Baseline Protections at Standardized Interfaces

Throughout the set of mandatory security mechanisms defined by the BSI TR-03109 series, segments that are directly connected to the SMGW benefit from a high level of security guarantees. These include:

- Mutual TLS authentication with certificate pinning,
- Profile-based authorization of communication partners,
- Cryptographic integrity protection of measurement data,
- Enforced termination of connections if certificate validation fails

The threat model confirms that these measures are effective in mitigating classical network-level attacks in close proximity to the SMGW. However, this does not imply complete end-to-end security. To gain a higher level of safety, further measures need to be implemented, such as acknowledgment messages and rate limiting for valid and invalid messages.

B. Resilience Measures for Customer Domain Availability Dependencies

To avoid risks arising from customer-owned infrastructure, further specifications regarding power and network-related assets are needed. These include an explicit definition of degraded-mode behaviors for loss of connectivity. Concrete fallback scenarios shall therefore be specified and implemented in the assets. In this context, [35] presented a proposal on how to use predefined power envelopes in the event of a communication failure. Furthermore, basic cybersecurity protective measures, such as rate limiting, should be mandatory to avoid cascading retry storms. Since it is infeasible to make household networks inaccessible to attackers, grid-connected devices with a high impact on the stability, like CLS, must implement measures to counter attacks. Regarding the EMT, it is essential to detect suspicious behavior of the systems at an early stage, to have sufficient time to take action. Thus, indisputable confirmation of the realization of the required measure is recommended.

C. Hardening and Segmentation Behind the CLS-Adapter

While the role of the GWA must be ISO27001 certified and a risk analysis must be carried out for the use of external cloud providers, there are no requirements for the use of EMS systems. As previously demonstrated, this area of application in particular poses significant safety risks. At the very least, every EMS cloud provider must have a cloud security concept in place.

D. Strong Channel-to-Asset Binding at aEMT Endpoints

As it is absolutely important for control signals to reach the intended CLS-adapter, errors are not permitted at this point. Therefore, it is crucial that the EMT binds incoming proxy communication channels to a unique combination of

SMGW and CLS-adapter identifier to know exactly which asset will be addressed. This binding needs to be stored safely and out of reach of unauthorized people. In case of ambiguity, the message should be discarded. By enforcing semantic consistency between transport-level connections and application-level control targets, the risk of misdirected or unintended control actions is reduced. It is advisable to publish an implementation guideline on how the data can be stored and processed at EMT side in order to avoid mix-ups.

E. Endpoint Data Protection and Secure Logging Practices

Endpoints, WAN- as well as LAN-side, should complement secure transport mechanisms with disciplined data handling practices to reduce information disclosure risks. This is about minimizing sensitive data in logs and protecting logs through appropriate access controls and integrity mechanisms. It is crucial to note that confidentiality guarantees extend beyond the communication channel and are maintained throughout the data lifecycle.

F. Mitigation of Risks Related to the SMGW Wake-Up Mechanism

The requirements for contacting the SMGW are strict and well defined. Nevertheless, the scope of checks that need to be done by the SMGW to recognize a message as valid or not is comprehensive. To avoid resource exhaustion, we recommend applying early and lightweight filtering of incoming wake-up messages before initiating costly cryptographic validation steps. While TCP/TLS would prevent passive observation and replay of wake-up messages, it would introduce stateful connection handling, which is undesirable for a lightweight wake-up mechanism. Therefore, we rather recommend complementing rate limiting for valid wake-up requests by prioritization mechanisms that ensure legitimate wake-up messages from authorized sources are not starved by excessive invalid or replayed traffic. One simple solution would be extending the rate limit to invalid messages and reducing valid time windows.

G. Mitigation of Risks Related to TLS Version Support

As seen in previous sections, the use of TLS version 1.2 does have security vulnerabilities. This highlights the need to migrate to TLS 1.3, which structurally mitigates the attacks, as shown by [15]. The use of TLS 1.2 should therefore be prohibited in the SMGW environment and at least all parties involved in the SM-PKI should be required to use TLS 1.3. A protocol version fallback to older TLS versions should never be accepted, even if version negotiation fails during the handshake. Therefore, security testing should explicitly verify that downgrade attempts are rejected and that fallback to older TLS versions is technically impossible.

H. Mitigation of Repudiation Risks Through Explicit Acknowledgments

A key problem that extends across all process steps is the missing of explicit acknowledgments. For those involved, it is easy to deny receiving messages and their incorrect implementation. To mitigate these repudiation risks, the §14a EnWG and §9 EEG control process should incorporate explicit acknowledgments to confirm receipt and execution of requested actions.

- Channel establishment requests initiated by the aEMT should be acknowledged by the GWA
- Receipt of wake-up messages by the SMGW should be acknowledged, independent of subsequent management or proxy connection establishment
- Control commands forwarded to the CLS should include a mechanism for the CLS to acknowledge successful receipt and execution, optionally distinguishing between acceptance and actual implementation
- CLS-adapter should provide execution feedback, enabling correlation between issued commands and observed asset behavior

I. Summary

To increase the safety of the §14a EnWG ad-hoc control signal transmission chain, especially endpoint responsibility strengthening is required. While the SMGW centered security architecture provides a robust foundation, end-to-end security can only be achieved if backend systems and customer domain components implement complementary safeguards. While there are some risks that arise at certain points, the security vulnerabilities in the use of TLS 1.2 and the existing deniability also pose risks that extend across the entire process chain. To this end, existing specifications must be revised and expanded to include specifications regarding endpoints.

VI. Conclusion and Future Work

In this paper, we provide to the best of our knowledge the first threat analysis with a focus on §14a EnWG and §9 EEG that is made openly available for DSOs, regulators and researchers. Whereas the ad-hoc control signal transmission chain demonstrates a high level of security within the SMGW domain, it does not achieve end-to-end security when the endpoints are included. The STRIDE analysis shows that risks predominantly arise at architectural endpoints, where no general specifications prevail.

The absence of explicit end-to-end acknowledgments creates significant repudiation risks, limiting the enforcement of grid-serving control actions. To solve this problem, the entire process chain, including the assets, must be able to prove tamper-proof that the control signals have been implemented. The mandatory use of TLS 1.2 represents a systemic weakness, as it remains susceptible to algorithm substitution attacks. It underscores the necessity of a migration to TLS 1.3. Customer-side infrastructures and (cloud-based) EMS introduce additional availability and security dependencies. Here, clearly defined fallback scenarios must be implemented.

Beyond these, the control signal transmission chain is exposed to general supply chain attacks, including compromised firmware, manipulated software updates and subverted third-party components at both backend and device levels.

It should also be noted that encryption algorithms currently in use (elliptic curve and RSA) are not secure in the post-quantum era. Due to the long service life of critical infrastructure, it is therefore important to take early action.

In summary, strengthening endpoint responsibilities, introducing verifiable control execution with proof-of-action mechanisms and extending regulatory requirements beyond the SMGW are necessary to achieve end-to-end security.

The next step would be to validate the identified risks through empirical testing and operational experience. Therefore, a testbed that maps the entire control chain would have to be implemented in order to realistically simulate the cases. A hardware-in-the-loop test environment is ideal for demonstrating the effects on the grid. Co-simulation is required to link the grid simulation with the network simulation. In addition, with the appropriate test environment, risks could be discovered that remain undetected in theory and it could also be used as an exploit demonstrator to show weaknesses and its impact.

This setup can also be used to investigate the handling and risks of the VDE FNN implementation note on the subject of control with verification [35]. In this context, it would be interesting to compare these approaches with the one presented in this paper in order to identify any advantages and disadvantages of the respective models and possibly implement an even better approach.

Future research could address the question of how the process of drafting legislation could be optimized. In the case of the SMGW architecture, it has become apparent that the back-and-forth between legislators and industry leads to delays. Approaches, such as central testing stations, where effects can be tested early in a practical setting, could be helpful in quickly finding suitable solutions.

In addition, there are still considerable uncertainties regarding the controllability of supply chain attacks and the handling of post-quantum cryptography in the current process chain and must be investigated by future research.

Acknowledgment

This work was carried out in the context of the research project SimCyberGrid, which is funded by the German Federal Ministry for Research, Technology and Space (code: 13FH637KA2) and the research project FARFALLE, which is funded by the German Federal Ministry for Economic Affairs and Climate Action (code: 03EI6136C).

References

[1] J. Hawran and P. Suchomski, "International comparison of smart meter solutions and functionalities in Europe", 2026, Accessed: Mar. 13, 2026. [Online]. Available: https://www.ffe.de/veroeffentlichungen/internationaler-vergleich-von-smart-meter-loesungen-und-funktionali-taeten-in-europa/.

[2] Bundesnetzagentur, "Rollout of smart metering systems: Quarterly surveys", 2025, Accessed: Mar. 13, 2026. [Online]. Available: https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/NetzzugangMesswesen/Mess-undZaehlwesen/iMSys/artikel.html.

[3] Forschungsstelle für Energiewirtschaft e.V., "Technical framework conditions for demand-side flexibility", 2025, Accessed: Mar. 13, 2026. [Online]. Available: openaccess.ffe.de/wp-content/uploads/2025/05/Final_Technical-Framework-Conditions-for-Demand-Side-Flexibility.pdf.

[4] UK Department for Energy Security and Net Zero, "Smart Meters Consultation: Government Response to the Mid-Point Review – Analytical Annex", 2023, Accessed: Mar. 13, 2026. [Online]. Available: https://assets.publishing.service.gov.uk/media/64a66ec1c531eb001364ff02/smart-meters-consultation-government-response-mid-point-review-analytical-annex.pdf.

[5] *Energy Industry Act*, Federal Republic of Germany, last amended 2025, 2005.

[6] Bundesnetzagentur, "BK6-22-300", 2023, Accessed: Mar. 13, 2026. [Online]. Available: https://www.bundesnetzagentur.de/DE/Beschlusskammern/1_GZ/BK6-GZ/2022/BK6-22-300/Beschluss/BK6-22-300_Beschluss_20231127.pdf.

[7] Bundesamt für Sicherheit in der Informationstechnik, "Protection Profile for a Smart Meter Gateway (SMGW-PP), Version 2.0", Tech. Rep. BSI-CC-PP-0073-V2, 2024.

[8] Bundesamt für Sicherheit in der Informationstechnik, "Requirements for the Interoperability of the Smart Meter PKI, Version 2.0", Tech. Rep. TR-03109-1, 2024.

[9] Bundesamt für Sicherheit in der Informationstechnik, "Communication adapter", Tech. Rep. TR-03109-5, 2023.

[10] C. Freudenmann et al., "Open and Secure: Amending the Security of the BSI Smart Metering Infrastructure to Smart Home Applications via the Smart Meter Gateway", in *Smart Energy Research. At the Crossroads of Engineering, Economics and Computer Science*, C. Derksen and C. Weber, Eds., Cham: Springer International Publishing, 2017, pp. 136–146, ISBN: 978-3-319-66553-5. DOI: 10.1007/978-3-319-66553-5_10.

[11] S. Tanimoto et al., "Risk Assessment of Home Gateway/Smart Meter in Smart Grid Service", in *2016 5th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*, 2016, pp. 1126–1131. DOI: 10.1109/IIAI-AAI.2016.25.

[12] M. Orlando et al., "A Smart Meter Infrastructure for Smart Grid IoT Applications", *IEEE Internet of Things Journal*, vol. 9, no. 14, pp. 12 529–12 541, 2022, ISSN: 2327-4662, 2372-2541. DOI: 10.1109/JIOT.2021.3137596.

[13] Z. Zhang et al., "Achieving Privacy-Friendly Storage and Secure Statistics for Smart Meter Data on Outsourced Clouds", *IEEE Transactions on Cloud Computing*, vol. 7, no. 3, pp. 638–649, 2019, ISSN: 2168-7161. DOI: 10.1109/TCC.2017.2685583.

[14] H. Kumar, P. Nnaji, and S. Kumar, "Smart Meter Performance Under Wired and Wireless Cyber Security Attack", in *2024 IEEE World AI IoT Congress (AIIoT)*, 2024, pp. 0061–0067. DOI: 10.1109/AIIoT61789.2024.10578962.

[15] S. Berndt et al., "ASAP: Algorithm Substitution Attacks on Cryptographic Protocols", in *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, Accessed: Feb. 07, 2025, Association for Computing Machinery (ACM), 2022, pp. 712–726. DOI: 10.1145/3488932.3517387.

[16] S. B. Alemu, "The transformation of TLSfrom version 1.2 to 1.3Efficiency vs Security vs Interoperability", 2020, Accessed: Mar. 13, 2026. [Online]. Available: https://ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/appliedcrypto/education/theses/Bachelor's-Thesis-SamuelBedassaAlemu.pdf.

[17] K. Förderer, M. Lösch, R. Növer, M. Ronczka, and H. Schmeck, "Smart Meter Gateways: Options for a BSI-Compliant Integration of Energy Management Systems", *Applied Sciences*, vol. 9, no. 8, p. 1634, 2019, ISSN: 2076-3417. DOI: 10.3390/app9081634.

[18] Bundesamt für Sicherheit in der Informationstechnik, "Appendix 6 Operational processes involving the SMGW, Version 2.0", 2024, Accessed: Mar. 13, 2026. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/

Publikationen/TechnischeRichtlinien/TR03109/TR-03109-1_Anlage_Betriebsprozesse_v2_0.pdf.

[19] OWASP Foundation, "OWASP Threat Dragon Documentation", 2025, Accessed: Mar. 13, 2026. [Online]. Available: https://www.threatdragon.com/docs/.

[20] L. Kohnfelder and P. Garg, "The STRIDE Threat Model", 1999, Accessed: Mar. 13, 2026. [Online]. Available: learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20).

[21] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Stride-based threat modeling for cyber-physical systems", in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2017, pp. 1–6. DOI: 10.1109/ISGTEurope.2017.8260283.

[22] VDE Thüringen e.V., "Smart meter gateways in rollout", 2019, Accessed: Mar. 13, 2026. [Online]. Available: https://www.vde-thueringen.de/resource/blob/1929426/3746f3868f025db258e69b42e6540e0e/16-ppc-kohlsdorf-smart-meter-gateways-im-rollout-data.pdf.

[23] J. Siemer, "Bitdefender reports on the risk of hacker attacks on deye inverters and the solarman monitoring platform", pv magazine Deutschland, 2024, Accessed: Mar. 13, 2026. [Online]. Available: https://www.pv-magazine.de/2024/08/08/bitdefender-berichtet-ueber-gefahr-von-hacker-angriffen-auf-deye-wechselrichter-und-solarman-monitoring-plattform/.

[24] VDE Verband der Elektrotechnik, Elektronik und Informationstechnik e. V. – Forum Netztechnik/Netzbetrieb, "Connection and operation of generation plants, storage facilities and consumption devices on the low-voltage grid", 2025, Accessed: Mar. 10, 2026. [Online]. Available: https://www.vde.com/resource/blob/2434724/02833b45ff85c9b9beb3a37073755444/vde-fnn-hinweis-anschluss-betrieb-niederspannung-data.pdf.

[25] Bundesamt für Sicherheit in der Informationstechnik, "Errata for BSI TR-03109-1 V1.0.1 – TAF9 and TAF10", Tech. Rep. Errata für die BSI TR 03109-1 V1.0.1 – TAF 9 und 10, 2019.

[26] T. Riedel and M. Berg, "Guide to regulatory requirements for external market participants (emt)", 2024, Accessed: Mar. 13, 2026. [Online]. Available: https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2024/Leitfaden_Regulatorische_Vorgaben_fuer_externe_Marktteilnehmer.pdf.

[27] VDE Verband der Elektrotechnik, Elektronik und Informationstechnik e. V. – Forum Netztechnik/Netzbetrieb, "Characteristics of the digital interface on controllable devices or on an energy management system", 2024, Accessed: Mar. 13, 2026. [Online]. Available: https://www.vde.com/resource/blob/2292786/5d38accc5ab02ad04df7cab8a64f1f63/impuls--digitale-schnittstelle-data.pdf.

[28] VDE Verband der Elektrotechnik, Elektronik und Informationstechnik e. V. – Forum Netztechnik/Netzbetrieb, "Cybersecurity in the use of cloud-based energy management systems", 2025, Accessed: Mar. 13, 2026. [Online]. Available: https://www.vde.com/resource/blob/2381556/7acb1ddff231b8d83432cf76c920a92e/vde-fnn-hinweis-schnittstellen-steuerungseinrichtung-data.pdf.

[29] Bundesverband der Energie- und Wasserwirtschaft, "Recommendations for connecting and operating controllable consumer devices until technical standards are available", 2025, Accessed: Mar. 13, 2026. [Online]. Available: https://www.bdew.de/media/documents/20250808_BDEW_AWH_Empfehlungen_Anschluss_steuerbare_Verbrauchseinrichtungen.pdf.

[30] J. Britz, J. M. Behrensen, and S. Kaven, "OWASP Threat Model", 2026, Accessed: Mar. 13, 2026. [Online]. Available: https://github.com/SimCyberGrid/STRIDE_14a_EnWG_Control_Chain.

[31] Bundesamt für Sicherheit in der Informationstechnik, "Smart Meter Gateway administration", Tech. Rep. TR-03109-6, 2025.

[32] VDE Verband der Elektrotechnik, Elektronik und Informationstechnik e. V. – Forum Netztechnik/Netzbetrieb, Ed., *Control box specifications: Functional and design features*, 1.5. Berlin, Germany, 2025, p. 223, E-Book/PDF; Bestellnummer 636511.

[33] S. Lakshminarayana et al., *Cybersecurity threats to power grid operations from the demand-side response ecosystem*, Feb. 2, 2025. DOI: 10.48550/arXiv.2310.18820. arXiv: 2310.18820[cs].

[34] A. Ali and V. P. Singh, "Comparative Analysis of Transport Layer Security (TLS) Versions", *International Journal for Research in Applied Science and Engineering Technology*, vol. 11, no. 12, pp. 680–684, 2023, ISSN: 23219653. DOI: 10.22214/ijraset.2023.57430.

[35] Bundesamt für Sicherheit in der Informationstechnik, "Control with verification in the smart meter gateway", Tech. Rep. TR-03109-1 - implementation note, 2025.