A Tutorial and Security Overview on the IEEE 2030.5-2018 Standard

Diego Passos, Cledson de Sousa, Rafael C. Gomes, Danilo F. Assis, Fernanda G. O. Passos, and Célio Albuquerque

***Abstract*—The rapid growth of grid-integrated solar plants and Distributed Energy Resources (DER) has introduced advanced electrical devices into both domestic and industrial environments. In this expanding landscape, standardization is essential to ensure compatibility, security, and seamless communication among devices from various manufacturers. This paper explores the IEEE 2030.5-2018 standard, which is designed to facilitate communication between the Smart Grid and its end-users. While providing a comprehensive overview of the standard, we particularly focus on its security features, with an emphasis on the challenges associated with managing digital certificates within the IEEE 2030.5 framework. Additionally, we conduct a systematic review of the existing literature related to this standard.**

***Index Terms*—IEEE 2030.5; Distributed Energy Resources; Smart Grids; Interoperability.**

I. Introduction

THE usage of renewable energy sources in residences and commercial establishments – solar energy sources, in particular – has been altering how energy is produced and distributed through the power grid. In this new paradigm, the so-called Distributed Energy Resources (DERs) [1] play an important role, as houses and other types of end users now also generate and inject energy into the power grid. Therefore, the traditional unidirectional energy flow – from the utility to the customers – is transformed into a multi-directional one: from the utility to the customers, from the customers to the utility, and even from customer to customer.

A concrete example of the rapid growth in distributed energy resources can be seen in Brazil, where the installed capacity of photovoltaic solar energy grew from 24 gigawatts (GW) in 2023 to over 39 GW as of August 2024 [2]. Similarly, as of December 2023, Australia's photovoltaic (PV) systems have surpassed a total installed capacity of 34.2 gigawatts [3].

For the most part, however, the current structure of the power grid is not designed to cope with distributed energy generation [1], [4]. Multi-directional energy flows require the existence of a data network between the utility and each DER, requiring a strong coordination between the various devices connected to the power grid in order to prevent failures and overloads. This network must be secure – as potentially sensitive information of the customers can be disclosed –, efficient (in response time, for example) and resilient – since the power grid is a critical infrastructure. However, this expansion of DER systems also introduces significant vulnerabilities. In August 2024, an ethical hack [5] exposed weaknesses in Virtual Power Plant (VPP) systems, particularly due to inadequate cryptographic practices, such as the use of an insecure proprietary Application Programming Interface (API) and small keys. This incident serves as a stark reminder of the 2015 cyberattack on Ukraine's power grid, where attackers compromised critical infrastructure, leading to widespread blackouts. These events highlight the ongoing need for vigilance and continuous improvement in securing DER communication systems to safeguard the integrity of the rapidly expanding smart grid.

California's Rule 21 is one of the many programs for the interconnection of distributed energy generation to the power grid in the state. It establishes a set of requirements for the interconnection, operation and metering of distributed energy sources to the main grid [6]. This interconnection requires the usage of energy inverters: devices that convert Direct Current (DC) to Alternating Current (AC). Some inverters, called *smart inverters*, offer other more advanced functionalities through specific communication interfaces. Those advanced functionalities allow a precise management of the production, consumption, and availability of the energetic surplus generated by distributed sources. The DERs possess the capability to adjust their operational parameters (such as power output, voltage and frequency regulation) in response to the local environmental conditions, thus enabling them to more effectively adapt to their surroundings [7].

The Smart Inverter Working Group (SIWG) [8] was established to develop and promote advanced functionalities for smart inverters as part of the smart grid initiative. Its purpose is to address the challenges posed by the increasing penetration of distributed energy resources (DERs) by enhancing the capabilities of inverters to actively participate in grid management. This includes improving reliability, resilience, and efficiency of the electric grid by enabling inverters to communicate with and respond to grid conditions in real-time. The workgroup organized its activities in three phases:

- **Phase 1 – Autonomous Functionalities**: defining the more fundamental functions that an inverter connected to a DER should perform, such as anti-islanding protection and voltage and frequency ride-through capabilities [9].

This work is supported in part by CAPES, CNPq and FAPERJ.

R. Gomes, D. Assis and C. Albuquerque are with the Computer Science Department, Universidade Federal Fluminense, Niterói/RJ, Brazil, e-mail: rafaelcaveari@id.uff.br, danilofernassis@gmail.com, celio@ic.uff.br

C. de Sousa is with the Telecommunications Engineering Department, Universidade Federal Fluminense, Niterói/RJ, Brazil, e-mail: cledsons@id.uff.br

D. Passos and F. G. O. Passos are with Instituto Superior de Engenharia de Lisboa (ISEL), Lisbon, Portugal, and also with Laboratório MídiaCom, Universidade Federal Fluminense, Niterói/RJ, Brazil, e-mail: dpassos@ic.uff.br, fernanda@midiacom.uff.br

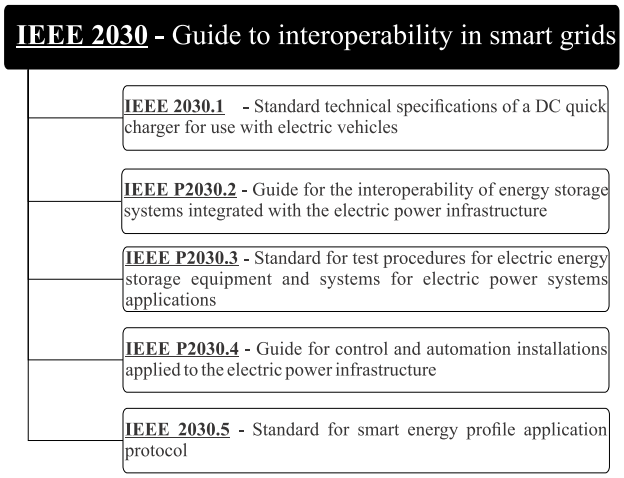


Fig. 1. Non exaustive suite of the IEEE 2030 standards for smart grid interoperability.

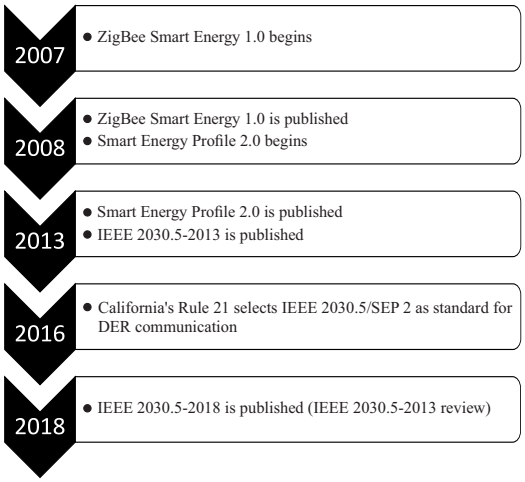


Fig. 2. The evolution of IEEE 2030.5.

- **Phase 2 – Communication Protocol**: defining the communication protocol to be used for the exchange of messages between the utilities and the DERs.
- **Phase 3 – Advanced Functionalities**: consider more advanced functionalities that could also be implemented by the inverters as different modes based on active power operation.

California's Rule 21 defined that the communication between the utilities and the DERs should use the Institute of Electrical and Electronics Engineers (IEEE) 2030.5 standard. The standard was explicitly designed to facilitate interoperable communication across a diverse spectrum of devices and services, such as smart thermostats, demand response programs, smart meters, the charging of electrical vehicles, and smart inverters. The particular usage of the standard by California's Rule 21 was consolidated at the Common Smart Inverter Profile (CSIP) IEEE 2030.5 Implementation Guide for Smart Inverters [10].

IEEE 2030.5 is part of IEEE 2030 – a guide that provides alternative approaches and good practices to achieve smart grid interoperability of the Electric Power System (EPS) [11]. The IEEE 2030 Smart Grid Interoperability Reference Model (SGIRM) is a reference instrument to provide stakeholders with a common understanding of the interoperability criteria from the perspectives of the power system, communications and information technology [11]. Fig. 1 provides an overview diagram of a set of the IEEE 2030 projects[1] and protocols for smart grid interoperability.

The IEEE 2030.5 standard is an evolution of the *ZigBee Smart Energy Profile 1.x* (SEP 1), as illustrated in Fig. 2. The Smart Energy Profile (SEP) was first developed by the ZigBee Alliance in 2007 to provide interoperability between ZigBee devices present in a residential smart grid – often called Home Area Network (HAN). Since then, it has undergone several revisions and updates. However, SEP 1 is limited to the use of the ZigBee technology and protocol stack (including IEEE 802.15.4). The development of Smart Energy Profile 2.0 (SEP 2), which evolved from SEP 1, started in 2008. It was designed to use widely disseminated communication technologies that support the Internet Protocol (IP), as illustrated in Fig. 3. In 2011, the HomePlug Alliance, Wi-Fi Alliance, HomeGrid Forum, and ZigBee Alliance formed the Consortium for *Smart Energy Profile 2* Interoperability (CSEP) aiming to create compliance tests to promote the certification of devices that make use of SEP 2. In 2013, SEP 2 was formally published by the ZigBee Alliance and the HomePlug Powerline Alliance. In the same year, the IEEE adopted SEP 2 as the IEEE 2030.5-2013 standard. In 2016, *California's Rule 21* defined IEEE 2030.5 (SEP 2) as the standard to be used in DERs communication. Recently IEEE 2030.5-2018 has been updated to incorporate IEEE 1547-2018 functionalities within the standard — the IEEE 1547-2018 is a related standard that focuses in establishing in number of requirements for the interconnection between DERs and power systems. This standard operates at the application layer and relies on web services to facilitate the communication between devices. It incorporates relevant security measures and makes use of the contemporary internet protocols to transmit its messages [12]. The revision, published in 2018, was meticulously designed to align with the requirements of California's Rule 21. Subsequently, the IEEE formally recognized and adopted this version as the IEEE 2030.5-2018 standard.

The use of IEEE 2030.5 for DER communications in California and its review in 2018 confirms its relevance concerning the communication of DERs and also the communication between so-called Internet of Things (IoT) [14] devices present in a HAN. Even so, studies of the IEEE 2030.5 standard in the scientific literature are scarce and most of them provide only a superficial approach or describe some implementation, without detailing its structure, architecture, and security issues. Instead, they address other related issues, *e.g.* communication performance or evaluation purposes [15], [16].

The objective of this paper is to provide a tutorial-style introduction to the IEEE 2030.5-2018 standard as well as an

[1] The letter "P" in IEEE standard acronyms, such as "IEEE P2030.2", denotes a "project" or "proposed" standard, indicating that the standard is in the development phase and has not been finalized yet.

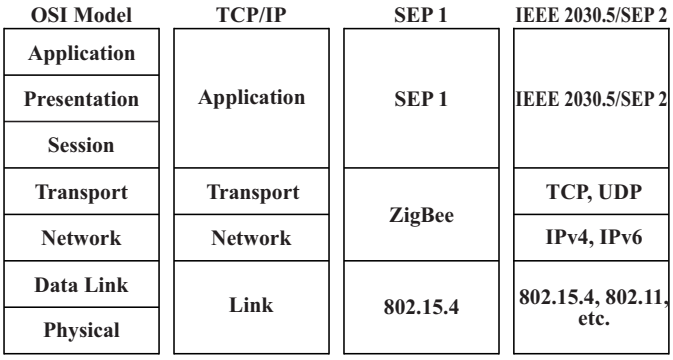


Fig. 3. Comparison between ISO/OSI, TCP/IP, SEP 1 and IEEE 2030.5/SEP 2 network stacks. Adapted from [13].

overview of its recent related literature, specifically focusing on the security aspects of device communications. This is done by means of both a systematic review of the related literature as well as description of the standard itself. In this description, we cover several aspects of the IEEE 2030.5, including its application scenarios, nomenclature, communication protocols, provided services, and security policies and mechanisms. Based on this description, we particularly highlight a significant gap in the standard, which is the absence of mechanisms for digital certificate revocation and its life cycle management. We also underscore works that propose advanced cybersecurity measures and strategies aimed at mitigating these and other vulnerabilities. To the best of our knowledge, there are no other similar works on the IEEE 2030.5 standard, specifically, available in the literature. Hence, we aim at filling this gap.

The rest of the paper is outlined as follows: Section II offers an overview of the existing literature related to the IEEE 2030.5 standard, highlighting the key areas that have been explored and identifying gaps in the current research. Section III explores potential applications and the communication topologies essential for linking devices between power utilities and consumers. Section IV details the architectural components of the standard. Section V examines the standard's security measures, focusing on authentication and the public-key infrastructure of IEEE 2030.5. Section VI presents a proof-of-concept, demonstrating practical attacks to exploit identified security weaknesses. In Section VII, we more thoroughly review the literature regarding solutions and best practices to mitigate these security vulnerabilities and other strategies to bolster Smart Grid security. This section also sheds light on various efforts to navigate challenges associated with diverse vendors and devices constrained by CPU and memory resources. The paper concludes with Section VIII, summarizing key findings and reflecting on future research directions.

II. Overview of the Related Literature

We undertook a systematic literature review centered on the IEEE 2030.5 standard by leveraging three primary scientific databases: *IEEE Explore*, *Scopus*, and *Google Scholar*. These databases are renowned for housing some of the most pertinent scientific publications in the realms of Computer Science and Engineering [17]. Our search across these platforms was guided by the keyword *"IEEE 2030.5"*, chosen due to its official recognition by the IEEE for this particular standard. This targeted approach yielded a corpus of more than 300 scholarly works, encompassing a variety of formats including technical reports, peer-reviewed journal articles, recognized industry standards, technical reports and magazines.

Once this initial set of studies was collected, the next steps were to screen the retrieved studies and select the relevant ones for a more in depth analysis. To that end, we proceeded to define a set of three exclusion criteria. The first exclusion criterion refers to the year of publication. The IEEE 2030.5 was formally adopted with this nomenclature by the IEEE in 2013, so a filter was applied to select works published starting that year. The second exclusion criterion is about patents. We would like to focus on scientific works which analyze the standard in some form. Therefore, patents were disregarded. The last exclusion criterion aims to eliminate duplicated documents and works that only mention IEEE 2030.5, without analyzing it, *i.e.*, which do not explain or define its structure, architecture, or operation. For example, we found several documents on smart grids that, when discussing communication, only mention IEEE 2030.5 along with other available standards and protocols, without presenting any details on how it operates. Fig. 4 shows the number of remaining documents after applying those filters in each step.

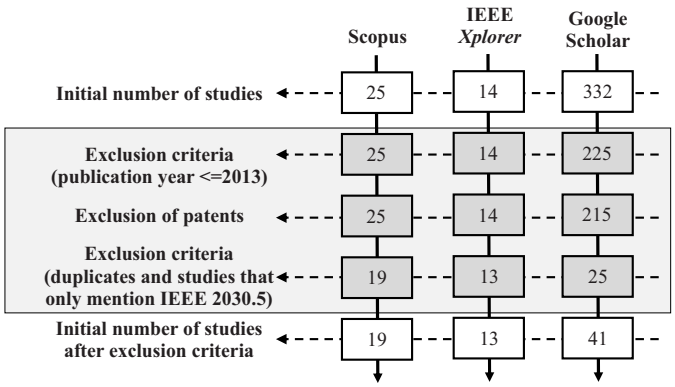


Fig. 4. Number of remaining documents per step.

After a further refinement of those 73 papers, the final selection of 46 works is presented in Table I. This table is organized by the year of publication, and it includes a classification for each type of work related to IEEE 2030.5. The classes used are:

- *Draft* – preliminary version of the standard.
- Standard – final version of the standard.
- Tech Report – Corporate or public reports and analyses from industry that are not specifically related to security.
- Secondary – superficially describes IEEE 2030.5.
- Implementation – describes an implementation of the IEEE 2030.5 – *e.g.*, performance evaluation.
- Security – document that addresses security aspects of IEEE 2030.5 and other standards/protocols.

As shown in Table I, from 2013 to 2019 there has been an increase in the number of published papers that address

TABLE I
SELECTED STUDIES SORTED BY YEAR OF PUBLICATION.

Title	Year	Classification
IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard (Draft) [18]	2013	Draft
IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard [19]	2013	Standard
Model-driven development of a standard-compliant Customer Energy Manager [20]	2015	Secondary
Standardization of Smart Grid Customer Interfaces [21]	2015	Secondary
Advanced inverter functions and communication protocols for distribution management [22]	2016	Secondary
Exploring emerging cybersecurity risks from network-connected DER devices [23]	2017	Secondary
Cyber security primer for DER vendors aggregators and grid operators [24]	2017	Security
IEEE Draft Standard for Smart Energy Profile Application Protocol [25]	2017	Draft
Upper-middleware development of smart energy profile 2.0 for demand-side communications in smart grid [26]	2018	Secondary
General Requirements for Designing and Implementing a Cryptography Module for Distributed Energy Resource (DER) Systems [27]	2018	Security
IEEE Approved Draft Standard for Smart Energy Profile Application Protocol [28]	2018	Draft
IEEE Standard for Smart Energy Profile Application Protocol [29]	2018	Standard
Implementation of a Smart Grid Communication System Compliant with IEEE 2030.5 [16]	2018	Implementation
Application Prospect of Edge Computing in Power Demand Response Business [30]	2018	Secondary
Recommendations for trust and encryption in DER interoperability standards [31]	2019	Security
Cybersecurity Risk Assessment for California's Smart Inverter Functions [32]	2019	Security
Simulation and analysis of OpenADR agents using VOLTTRON platform [33]	2019	Secondary
IPv6-Based Smart Grid Communication over 6LoWPAN [34]	2019	Secondary
DER-TEE: Secure Distributed Energy Resource Operations Through Trusted Execution Environments [35]	2019	Secondary
Evolution of Distributed Energy Resource Grid Interconnection Standards for Integrating Emerging Storage Technologies [36]	2019	Secondary
Cyber Attack and Defense for Smart Inverters in a Distribution System [37]	2019	Security
Recommended functionalities for improving cybersecurity of distributed energy resources [38]	2019	Secondary
PV Cybersecurity Final Report [39]	2019	Security
Communication protocols for the IoT-based smart grid [40]	2019	Secondary
IEC 61850 and IEEE 2030.5: A Comparison of 2 Key Standards for DER Integration: An Update [41]	2019	Tech Report
Considerations on Communication Infrastructures for Cooperative Operation of Smart Inverters [42]	2019	Secondary
Transactive Demand Response Operation at the Grid Edge using the IEEE 2030.5 Standard [43]	2020	Implementation
Cyber-Physical Security and Resiliency Analysis Testbed for Critical Microgrids with IEEE 2030.5 [7]	2020	Security
Assessing DER network cybersecurity defences in a power-communication co-simulation environment [44]	2020	Security
CReST-VCT System Integration Framework [45]	2020	Implementation
Distributed energy resource aggregation using customer-owned equipment: A review of literature and standards [46]	2020	Secondary
Testbed Demonstration for Distribution Grid Controls with High DER Integration [47]	2020	Implementation
Evaluation of interoperable distributed energy resources to ieee 1547.1 using sunspec modbus, ieee 1815, and ieee 2030.5 [48]	2020	Implementation
Distributed intrusion detection system for Modbus protocol [49]	2020	Security
Integrating System to Edge-of-Network Architecture and Management for SHINES (SEAMS) Technologies of High Penetration Grids [50]	2020	Tech Report
Real-Time Hardware-in-the-Loop Distributed Energy Resources System Testbed using IEEE 2030.5 Standard [51]	2021	Implementation
An Energy Service Interface for Distributed Energy Resources [52]	2021	Implementation
A practical three-layer energy management framework for future distribution systems [53]	2021	Implementation
Model-Based Interface Design for Smart Field-Device Integration [54]	2022	Implementation
A Privacy-Preserving Strategy for the Trust Layer of the Energy Grid of Things Distributed Energy Resource Management System [55]	2022	Implementation
Interoperability Profile for Electric Vehicle Fleet Managed Charging [56]	2022	Implementation
Incentivizing distributed energy resource participation in grid services [57]	2022	Implementation
Low-Cost Communication Interface between a Smart Meter and a Smart Inverter [58]	2022	Implementation
IEEE 2030.5 Test Tools [59]	2023	Implementation
VOLTTRON IEEE 2030.5 Agent [60]	2023	Implementation
Post-Quantum Cryptography (PQC)-Grade IEEE 2030.5 for Quantum Secure Distributed Energy Resources Networks [61]	2024	Security

IEEE 2030.5. Fig. 5 presents the evolution in the number of studies over the years[2]. Possibly, the adoption of the standard by *California's Rule 21* in 2016 and the growing need for control over smart devices in smart grids and HANs has been contributing to this increase in the number of scientific works for the past 5 years, with respect to the years before. In addition, the year 2019 noticed the highest number of published studies. This peak is possibly justified by releasing

[2]Data as of August 2024.

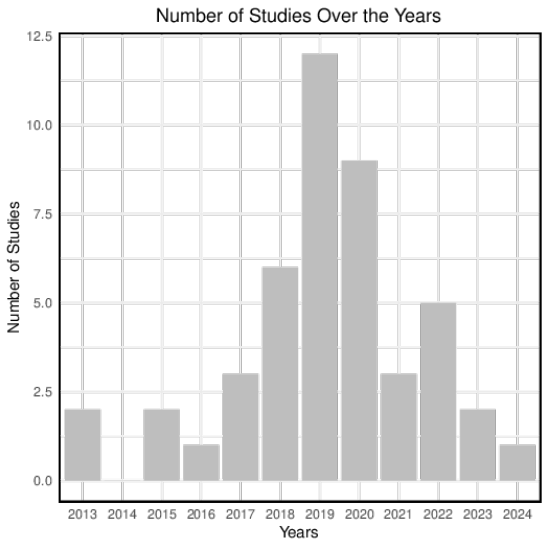


Fig. 5. Distribution of the selected studies per year.

the final version of the standard in 2018.

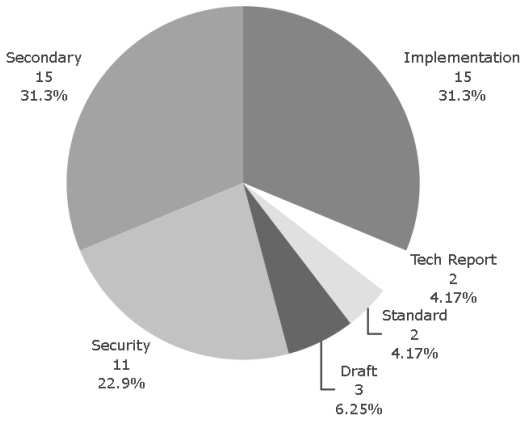


Fig. 6. Distribution of studies per classification.

When examining the spectrum of selected studies illustrated in Fig. 6, a noticeable observation is the dominance of secondary and implementation works. As a result, no studies in the scientific literature address the IEEE 2030.5 in full, comprising a complete review of its structure, development, implementation architecture, and communication security of the entities involved. Instead, those studies can be classified as follows:

a) Drafts and standards: documents [18], [25], [28] are drafts, *i.e.*, they are preliminary versions of the standard. Documents [19], [29] are the final ratified versions of the standard published in 2013 and 2018, respectively.

b) Security-related works: most papers classified as *Security* conduct security studies, analyses, and evaluations of the protocols and standards used in the communication of DERs. However, these approaches are secondary in nature, as they mention IEEE 2030.5 only superficially without delving deeply into its structure, architecture, or specificities. These works typically describe potential risks and vulnerabilities and propose alternatives to improve communication security, but they do not thoroughly explore IEEE 2030.5 itself.

For example, Sarker et al. [7] present a cyber-physical testbed that integrates OpenDSS and Mininet with IEEE 2030.5, enabling the analysis of microgrid resilience under cyberattack scenarios, such as Malicious DER Control and Coordinated Sequence Attack. This approach allows for the exploration of vulnerabilities and resilience in microgrids, particularly within military installations. The paper contributes to the field of microgrid cybersecurity and resilience by introducing a simulation platform that combines OpenDSS for physical layer simulation and Mininet for cyber layer simulation. This integration facilitates the examination of the IEEE 2030.5 standard in microgrid environments, providing a valuable tool for researchers and practitioners. Additionally, the study introduces a resilience metric that incorporates both cyber and physical aspects, offering a detailed resilience analysis by assessing both topological and physical factors, helping to explain the impact of cyber threats on microgrid operations and supports the development of effective mitigation strategies. However, the validation of the results is based on simulations, which, while valuable, may not fully reflect real-world conditions, potentially limiting the practical applicability of the findings. Moreover, the focus on specific attack scenarios within military microgrids may limit the generalization of the results to other types of microgrids or broader DER systems outside military contexts.

Baker *et al.* [27] offer a detailed examination of the essential requirements for designing and implementing cryptographic modules within DER systems. The paper presents an in-depth analysis of system requirements, cryptographic techniques, and practical implementation strategies, with a particular emphasis on the need for interoperability with existing standards such as IEEE 1547. It also provides practical guidance on hardware implementation options, including Trusted Platform Modules (TPMs) and Bump-in-the-Wire (BITW) solutions. The necessity of cryptography in DER systems, especially in the context of grid communications, is thoroughly discussed, with clear recommendations on how to implement cryptographic solutions that consider critical system constraints like latency and bandwidth in power systems. The paper includes two case studies: the hardware requirements for cryptography and the impact on communications latency, offering practical insights into the challenges and solutions for securing DER systems. However, the paper does not specifically address vulnerabilities associated with IEEE 2030.5.

Sun *et al.* [37] provide a comprehensive analysis of cyberattack scenarios targeting smart inverters, highlighting the vulnerabilities that arise from their deployment in DER systems. The study focuses on the development and implementation of a signature-based Intrusion Detection System (IDS) to detect and mitigate cyber intrusions in real-time. The authors use a simulation environment to evaluate the effectiveness of the proposed IDS. The simulation results, derived from two case studies involving flooding attacks and false command injection attacks, demonstrate the impact that cyberattacks can have on the stability and reliability of distribution systems with high solar energy source. The paper's approach primarily focuses on

the detection and mitigation of known attack patterns through signature-based methods. Although practical, this approach may be limited in addressing emerging or unknown threats, commonly referred to as zero-day attacks. Nevertheless, the study's emphasis on the cybersecurity of smart inverters aligns closely with the objectives of the IEEE 2030.5 standard, which aims to establish a secure and interoperable communication framework for DER systems. The vulnerabilities highlighted by Sun *et al.* underscore the importance of implementing robust security measures within the IEEE 2030.5 framework, particularly concerning the communication protocols used by smart inverters and other critical DER components. However, the narrower focus of their work does not align with the broader scope of the IEEE 2030.5 standard, which seeks to address a wide range of interoperability and security issues across the entire smart grid ecosystem.

Another study presented in [44] explores the trade-offs between implementing cybersecurity measures and maintaining power system performance (resilience) within a co-simulation environment known as SCEPTRE. This environment effectively integrates real network traffic between virtualized Distributed Energy Resource equipment and a DER management system (DERMS). The co-simulation platform allows for the realistic evaluation of cybersecurity defenses, including network segmentation, encryption, and moving target defence (MTD), assessing their impact on both cybersecurity metrics and grid services. The work demonstrates that implementing these security features does not significantly degrade the performance of grid-support functions, making the case for their inclusion in DER network designs. The SCEPTRE platform provides valuable insights into how these measures can be balanced against the need for reliable power system operations. However, while the paper addresses general cryptographic needs, it does not explore specific vulnerabilities related to IEEE 2030.5 in depth.

c) Industry-related literature: corporate Technical Reports, as referenced in [31], [41] and [50], establish two main goals (among others).

1) Benchmarking and Standards Development – In sectors where adhering to standards is imperative, these reports play a crucial role in shaping industry benchmarks. By openly discussing methodologies and results, a collective agreement on optimal practices and industry standards can be reached.
2) Informed Decision Making – Technical reports offer researchers valuable insights regarding the feasibility, advancements, and results of R&D initiatives. Such information is instrumental in directing investment choices, strategic envisioning, and the judicious allocation of resources.

d) Implementations: in [16], for example, authors describe an implementation of the standard used for performance assessment of the communication. Meanwhile, [43] implements the standard to support a transactive demand response scheme for a HAN. The increased adoption of implementations in recent papers, as in [51] at 2021 to [60] at 2023, can be attributed to the recognition of IEEE 2030.5 as a widely accepted standard and its selection for testbeds and performance comparisons.

e) Secondary citations: the remaining documents are classified as *Secondary*, as they do not have IEEE 2030.5 as their primary focus. For example, Pala and Proserpio [20] describe a customer power management model that supports IEEE 2030.5. The work in [26] implements a middleware that supports IEEE 2030.5 to overcome IoT devices' restrictions, such as hardware constraints. Finally, van Kerkhoven *et al.* [34] implement a 6LoWPAN-based smart grid communication system to connect devices in compliance with IEEE 2030.5.

Different studies review communication standards used for smart grids. In [42], the authors present considerations on some of the most relevant communication protocols that can be applied to the cooperative control of multiple smart inverters. Meanwhile, Obi *et al.* [46] focus on a literature review of solutions adapted by power utilities to deal with problems caused by the large-scale adoption of DERs. They also focus on reviewing communication standards such as ANSI/CTA 2045, SunSpec Modbus, SAE J3072, IEEE 2030.5–2018 and OpenADR used to manage such solutions. In addition, they present a succinct description of each standard by summing up some specific details of each. However, the review approach by both studies is generic and does not have IEEE 2030.5 as the primary focus.

III. Applications and Communication Scenarios in IEEE 2030.5

The IEEE 2030.5 standard extends its utility beyond the realm of electric grid to embrace a multitude of service sectors. Its robust communication framework and design principles are applicable to the management of gas and water supply systems, among others. The standard's architecture adeptly supports the monitoring and control of diverse variables such as pressure, temperature, and flow, integral to these sectors. Employing a HAN underpinned by a Home Energy Management System (HEMS) enables centralized oversight and management of smart devices within a residential context. This facilitates enhanced control and the optimization of resource consumption across various utilities, underpinning the standard's adaptability in diverse service environments. A HEMS may manifest as either a standalone software or a composite hardware-software solution, operating in either a passive mode for monitoring or an active mode for responsive action.

The standard can be used on a HAN integrated or not with the utility's servers. In the first case, the HEMS acts as a HAN gateway to promote its integration with the utility's servers. In the second case, all control and monitoring of smart devices are restricted to the home environment, and no control is possible by the utility. As a consequence, there are several possible topologies for the interaction between the HEMS and the smart devices present at a HAN. Fig. 8a shows a HAN not integrated with the utility servers. In this case, the HEMS may act as a manager for all smart devices including the appliances, light bulbs, the power inverter, the smart meter and even

electric vehicles. Fig. 8b shows a HEMS acting as a gateway for an IEEE 2030.5 Utility server. Fig. 8c shows a more generic topology with a Gateway HAN interconnecting smart devices, a Gateway HAN and an IEEE 2030.5 Utility server. In contexts devoid of extensive smart devices or sophisticated energy management requirements, a basic HAN gateway could suffice. These configurations provides streamlined efficiency, potentially offering a cost-effective solution. However, as shown in Section VI, a HEMS might concurrently introduce multiple vulnerability points.

The two scenarios envisioned for communications between the utility and DER systems are direct DER communications and aggregator mediated communications, as shown in Fig. 7. In both circumstances, all requirements for communication and interconnection are defined by the utility, including the mandatory use of IEEE 2030.5-2018 [10].

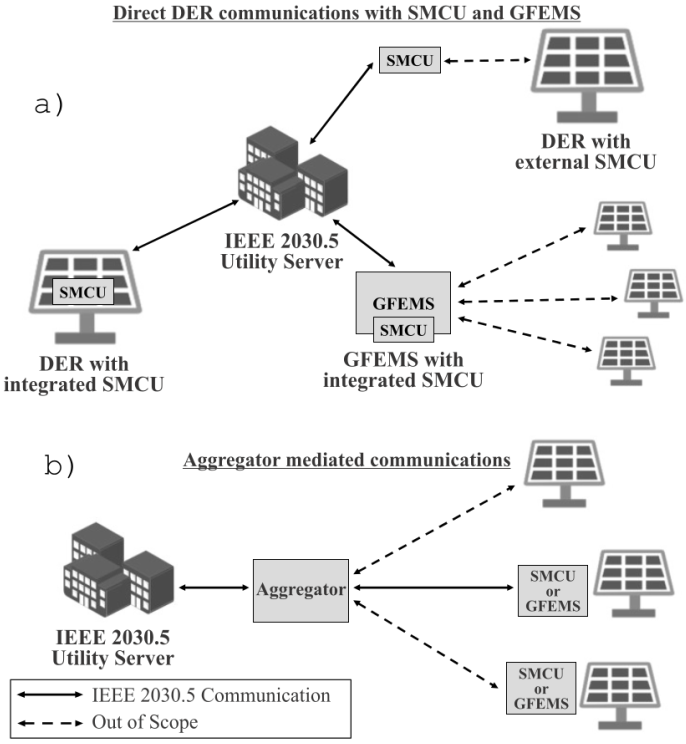


Fig. 7. The two scenarios envisioned for communications between the utility and DER systems. Adapted from [10].

In direct DER communications (without aggregators), the utility communicates with the DER system directly. This configuration is used when direct interaction between the DER and the utility is required for control and management purposes. In this scenario, two architectures are possible: DER with embedded or separate Smart Inverter Control Unit (SMCU)[3] and DER with Generating Facility Energy Management System (GFEMS)[3] [10]. In the first case, the smart inverter control is directly responsible for the communication between the DER and the utility. Therefore, it is represented individually on the utility's servers to identify a single DER. The SMCU can be integrated with the DER or reside external to the DER. The communication path between the SMCU and DER is outside the scope of this study. In the second case, a GFEMS is responsible for communicating multiple DERs with the utility. However, the utility views the entire array interconnected to the GFEMS as a single IEEE 2030.5 device [10].

In aggregator-mediated communications – where the DER does not communicate directly with the utility – the aggregator device is the intermediary in the communication between the utility and the various DERs distributed throughout the area under the management of the utility. The aggregator is then responsible for relaying any changes in the operational conditions for DERs or data requests to the affected systems and returning any needed information to the utility [10]. Each DER controlled by the aggregator appears as a separate IEEE 2030.5 device to the utility server [10]. Fig. 7a illustrates direct DER communication with SMCU and GFEMS. Here, the SMCU collects real-time energy data beneficial for billing and load forecasting. Concurrently, the GFEMS optimally manages multiple DERs, streamlining energy storage, release, and grid distribution. It is notable that aggregator-mediated communication with SMCU or GFEMS, as depicted in Fig. 7b, might utilize protocols other than IEEE 2030.5. However, such details exceed this study's scope. The preferred scenario varies based on each utility's unique requirements and preferences.

The forthcoming section will offer an in-depth exploration of the protocol, with a particular focus on detailing the packet structure and workflow, alongside highlighting key considerations in security.

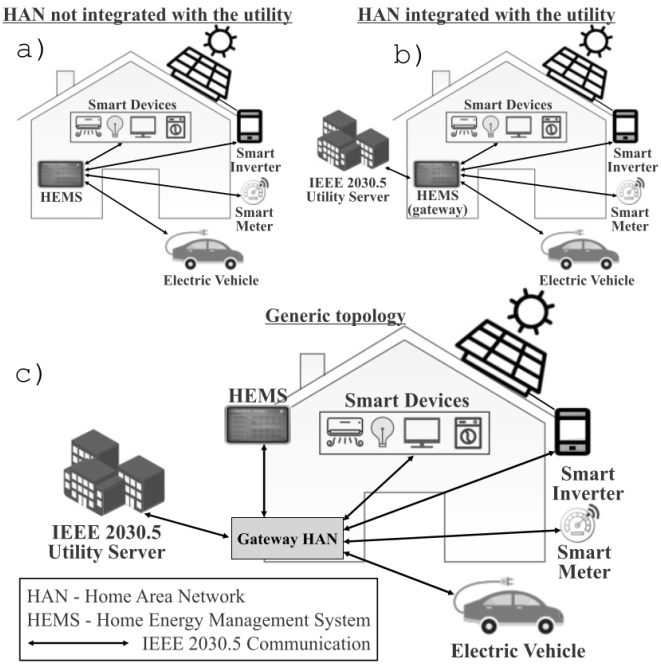


Fig. 8. Figures a), b) and c) show possible communication topologies between the HEMS and devices using IEEE 2030.5.

IV. An Overview of IEEE 2030.5

In this section, we provide an overview of the components of the IEEE 2030.5 standard. Later, in Section V, we discuss

[3]SMCU and GFEMS are terms used in Rule 21 Regulatory Documents.

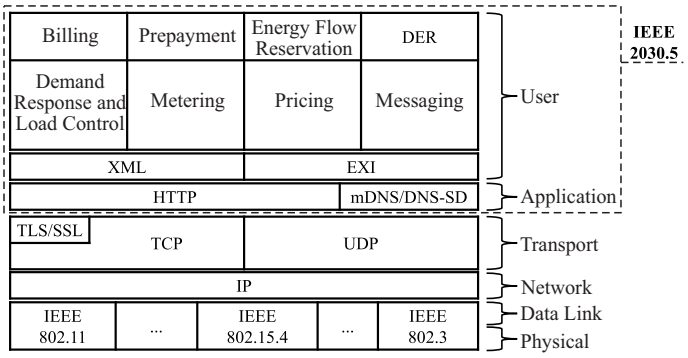


Fig. 9. Architecture of IEEE 2030.5-2018 communication stack. Adapted from [26].

some security issues associated with those components.

The IEEE 2030.5-2018 standard defines an application layer on top of TCP/IP providing functions to enable utility management of the end-user energy environment, including demand response, load control, time-of-day pricing, management of distributed generation, electric vehicles charging, etc [29]. Furthermore, this standard describes the mechanism for exchanging application messages, including error messages, and the security features used to protect the application messages [29].

In addition, since 2018, the standard provides support for IEEE 1547 [62], a standard for interconnection and interoperability between utility EPSs and DERs. The architecture of the IEEE 2030.5 communication stack is given in Fig. 9.

The protocol uses the concept of function sets. The function sets represent a minimum set of device functionalities and behaviors. The primary function sets (see Fig. 11) defined in the specification are metering, pricing, and demand-response load control [63].

Integral to the data exchange within these function sets is the Representational State Transfer (RESTful) architecture of IEEE 2030.5 [64] – which consists of a set of Create, Read, Update and Delete (CRUD) operations [63] – to access a given resource defined by a Uniform Resource Identifier (URI) [19]. IEEE 2030.5, like most web applications, defines a REST architecture built atop the Hypertext Transfer Protocol (HTTP). This architecture employs the GET, PUT, POST, and DELETE methods to realize CRUD operations. The HTTP protocol facilitates the conveyance of metadata, such as content-coding and media types. This metadata assists applications in determining the appropriate interpretation of the data [65].

The HTTP/1.1 header fields have been annotated by IEEE 2030.5-2018 with the following labels: mandatory, optional, and discouraged [4]. Examples of optional and discouraged are, respectively, Plug-in Electric Vehicle (PEV) Integration and Non-standard Data Models. Table II presents the headers classified as mandatory by IEEE 2030.5-2018.

The packet structure of the IEEE 2030.5 protocol is designed to encapsulate various operational commands and responses, utilizing XML and EXI formats for efficient data representation over HTTP transport. The emphasis on security operations within the IEEE 2030.5 protocol is highlighted by the standard's detailed guidelines on authentication, authorization, encryption, and integrity:

a) Authentication and Authorization: Authentication in IEEE 2030.5 employs a certificate-based mechanism for device and user validation, while authorization determines access levels and control within the system, managed through access control lists and roles.

b) Encryption: To maintain confidentiality, IEEE 2030.5 requires the use of Transport Layer Security (TLS) for encrypted communications between endpoints, protecting sensitive data such as pricing and consumption patterns.

c) Integrity: The integrity of message exchanges is ensured via cryptographic signatures, confirming that the data remains unaltered during transit.

The IEEE 2030.5 standard has two supplementary materials: IEEE 2030.5 XML Schema Definition (`sep.xsd` file) and IEEE 2030.5 WADL (`sep_wadl.xml` file). The IEEE 2030.5 XSD contains the definitions of the IEEE 2030.5 resources, attributes, and elements and their textual descriptions. In addition, the IEEE 2030.5 WADL includes the recommended URI structures and the use of HTTP methods associated with these objects [29]. For example: `/devices` represents the collection of devices and `/devices/{deviceId}` represents a specific device identified by its unique identifier.

TABLE II
HTTP HEADERS CLASSIFIED AS MANDATORY BY IEEE 2030.5.

Header	Used in message type
Accept	Request
Allow	Request
Content-Type	Request/Response
Date	Request/Response
Host	Request
Location	Response

A. Web Application Description Language

The Web Application Description Language (WADL) is an XML document that operates as a dictionary to describe RESTful web services. The WADL file contains the requirements that an HTTP request should include. In addition, it also consists of the URIs and the types of data expected in response to each request. Finally, the WADL allows any client possessing the WADL file to implement and make a valid request [65].

The IEEE 2030.5 WADL has the suggested URI structures and HTTP methods associated with these objects. Therefore, IEEE 2030.5 devices shall conform to the requirements defined in the WADL. Furthermore, all resource models shall validate the standardized IEEE 2030.5 XML namespace schema [65].

An XML Schema Definition (XSD) is a language for describing constraints and the structure of XML documents. An XML schema intends to define the legal building blocks of an XML document. A schema consists of metadata with the definitions of element types and declaration modes [65].

[4]"Discouraged" headers are advised against due to potential compatibility issues or deviation from best practices.

Describing and validating an XML document can be considered one of the main reasons for defining an XML schema. However, it is worth noting that besides validation, the XML schema has several other applications, such as allowing XML documents to be treated as objects within the programming universe [65].

While the primary function of an XML schema is to ensure the document adheres to a predefined structure, the security implications must also be considered. The integration of XML in power grid applications introduces vulnerabilities that need to be mitigated through proper schema design and validation practices, as highlighted in Section V-G.

B. Uniform Resource Identifier

A URI is a compact sequence of characters identifying an abstract or physical resource [66]. The following conventions are used for URI naming on IEEE 2030.5 [29]:

- URI elements should be at most four characters, but still recognizable to a knowledgeable engineer. Element names as short as one character are adequate, provided their meaning is clear.
- URI elements should contain only consonants, unless the inclusion of a vowel adds clarity, such as a leading vowel or well-known abbreviation.
- URI elements should be in all lower case.
- URIs must not exceed 255 bytes in length. In practice, URIs should be much smaller than 80 bytes.

C. Service Discovery

IEEE 2030.5 specifies DNS-based methods for service discovery, resource discovery, and hostname to IP address resolution [29]. A service is described as an application instance uniquely identified by host, port, and protocol, where the protocol, in this case, is IEEE 2030.5 plus its underlying transport bindings (*e.g.*, HTTP(S)/TCP/IP). DNS Service Discovery (DNS-SD) [67] uses existing DNS name syntax and message and record formats (PTR, SRV, TXT) to find instances of a given service within a given domain [29]. In IEEE 2030.5, DNS-SD is used to describe the location of function sets and groups of resources by supplying the host, port, and protocol of the supporting servers, along with more details provided by those servers. Furthermore, Multicast DNS (mDNS) [68] is used to perform DNS-like queries on the local link without any conventional unicast DNS server [29].

In DNS-SD, a pair of SRV and TXT records describes a service instance. Both records must have an identical Service Instance Name of the form `<Instance>.<Service>.<Domain>` [29]. In addition, the SRV record stores the hostname and port of the service, while the TXT record may contain additional information (such as a relative path) in text form. A service plus a path forms a URI and can locate a resource. A client discovers instances of a given service or resource type by sending a query for a DNS PTR record with the name `<Service>.<Domain>`, which returns a set of zero or more Service Instance Names of DNS SRV/TXT record pairs for the requested service or resource type [29]. Fig. 10 shows an example of DNS-SD flow to find a service instance.

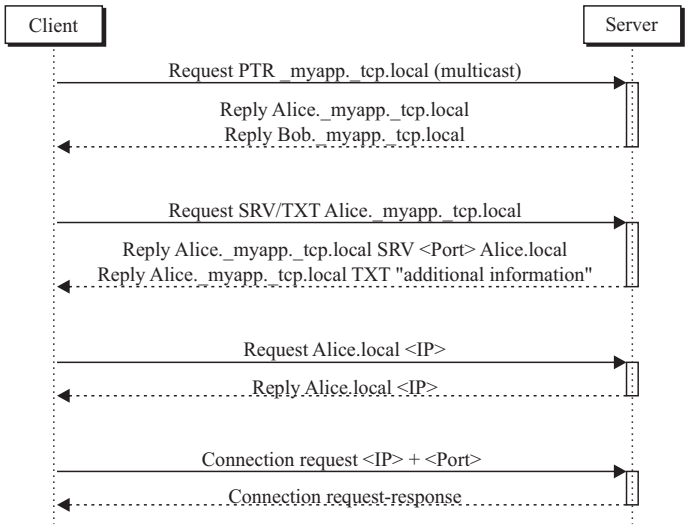


Fig. 10. DNS-SD flow to find a service instance.

Initially, a multicast DNS PTR query is performed to find the instances in the service network named "*myapp*". The string used in the query is "`_myapp._tcp.local`", where "`myapp`" is the service, "`tcp`" is the transport protocol and "`local`" is the domain. The response contains two instances: `Alice._myapp._tcp.local` and `Bob._myapp._tcp.local`. Each instance gives the information contained in the DNS SRV/TXT records. With the hostname – which for the first instance is `Alice.local` – it is possible to query for the IP address. With the IP address and the port, it is possible to start a connection to the "`myapp`" service provided by "`Alice`".

Following, each element of the Service Discovery is described.

1) Service Instance: IEEE 2030.5 establishes that a server should assign a unique `<Instance>` label of up to 63 bytes in UTF-8 form for each DNS SRV/TXT record pair that it advertises. In case of a name conflict, the Multicast DNS responder should assign a new name until the conflict is resolved. That is done by appending a decimal integer in parentheses to the `<Instance>` [29].

2) Service Name: The `<Service>` part of a Service Instance Name consists of the Service Name preceded by an underscore (_) followed by a period, plus a second DNS label specified by IEEE 2030.5 as `_tcp`. The Service Name used with IEEE 2030.5 DNS-SD is `smartenergy` which has been appropriately registered with the Assigned Numbers Authority (IANA). Therefore, an example of a valid Service Instance Name would be `device-0001111133._smartenergy._tcp.site.`, where `device-000001111133` is the `<Instance>` portion, `smartenergy` is the Service Name, `tcp` is the transport protocol, and `site` is the `<Domain>` component [29].

3) TXT Record: Table III lists the TXT (Text) record parameters utilized in DNS-based service discovery for IEEE

TABLE III
DNS TEXT RECORDS PARAMETERS USED IN IEEE 2030.5

Key=Value	Example
txtvers={#}	txtvers = 1
dcap={relative reference to DeviceCapabilities}	dcap = /dcap
path={relative reference to the function set}	path = /file
https={port}	https = 443
level={schema extensibility level indicator}	level = -S1

2030.5 [29], defining key-value pairs for service metadata, such as protocol version (txtvers), device capabilities (dcap), service path (path), secure communication port (https), and schema extensibility (level). These parameters enable devices to advertise and discover services within a smart grid network.

4) Subtype Queries: Subtype names work as filters that return the SRV/TXT record pairs describing a given function set [29] provided by a certain IEEE 2030.5 device. For example, if a device such as a smart meter also serves gas-metering data via mirroring, that device will register two subtype names: one for delivering metering data and one for the capability to receive metering data to mirror. The Metering Mirror function set provides a mechanism for constrained devices to post metering data to a metering server very efficiently [29]. The utility would have difficulty synchronizing the reading with the exact time when the meter is active to communicate. So the smart meter can use the *MirrorUsagePoint* resource on another device that provides this option and create an instance to send its measurements when it is active. The utility can read the measurements from the smart meter by accessing the other device on which the smart meter has created the instance. A client device can explore instances of a given function set by first performing a subtype query and then interrogating the Device Capabilities URIs to determine the URIs for that function set [29]. Subtype names are composed of a subtype string, followed by "`_sub._smartenergy._tcp.site.`". For example, the subtype name for the meter Usage Point function set shall be composed as "`upt._sub._smartenergy._tcp.site.`". Table IV lists the defined service subtype strings and corresponding IEEE 2030.5 function sets [29].

TABLE IV
SERVICE SUBTYPE STRINGS AND THEIR CORRESPONDING IEEE 2030.5 FUNCTION SETS, ADAPTED FROM [29].

Subtype	IEEE 2030.5 function set
bill	Billing
derp	Distributed Energy Resources
dr	Demand Response and Load Control
edev	End Device
file	File Download
msg	Messaging
mup	Metering Mirror
ppy	Prepayment
rsps	Response
sdev	Self Device
tm	Time
tp	Pricing
upt	Metering (Usage Point)

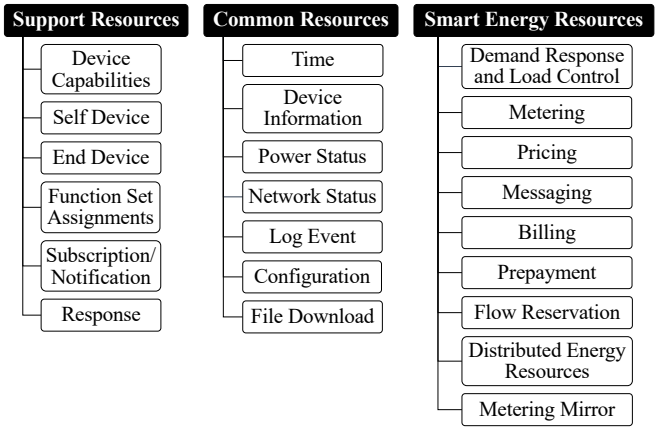


Fig. 11. IEEE 2030.5-2018 function sets.

D. Function Sets

Function sets are a logical grouping of resources that cooperate to implement IEEE 2030.5 features (*e.g.*, metering, demand response, and load control). They can be classified into three categories [29], as shown in Fig. 11:

- ***Support Resources*** – supply operational information to the end devices of an IEEE 2030.5 network or provide those end devices with services to manage and support their operation.
- ***Common Resources*** – represent the resources and function sets that provide general-purpose, non-domain-specific functionality.
- ***Smart Energy Resources*** – define the function sets specific to the domain of Smart Energy.

Query string parameters are parameters added to a URI to provide filtering/paging of list objects returned in query results [29]. The list paging mechanism allows GET requests to define the range of list items to be returned in a query result set. The general syntax of a paged query is as follows: `{URI}?s={x}&a={y}&l={z}`, [29] where :

- *{URI}* – represents the base URI used to address a list resource.
- *s* ("start") – denotes the first ordinal position in the list to be returned in the query result list as determined by the list's ordering.
- *a* ("after") – indicates that only items whose primary key occurs after the given date/time parameter should be included in the query result list.
- *l* ("limit") – used to set the maximum number of list items included in the query result list.

The following example demonstrates the use of query string parameters with a list resource. Consider the MyTypeList resource, shown below:

```
<MyTypeList href="http://h1/the/list" all="2"
    results="2">
  <MyType href="http://h1/instance/of/type/red">
    <timeStamp>100</timeStamp>
  </MyType>
  <MyType href="http://h2/instance/of/type/green">
    <timeStamp>200</timeStamp>
  </MyType>
</MyTypeList>
```

A GET to `http://h1/the/list?s=0&l=1` will return:

```
<MyTypeList href="http://h1/the/list" all="2"
    results="1">
  <MyType href="http://h1/instance/of/type/red">
    <timeStamp>100</timeStamp>
  </MyType>
</MyTypeList>
```

In the reply, the attribute *all* is used to indicate the total number of items in the list resource, while *results* indicate the number of items included in this particular subset of the list.

V. Security Components of IEEE 2030.5

By allowing remote control and monitoring of smart devices, smart grids become an obvious target for attackers aiming to disrupt critical infrastructure. For example, an attacker may try to disrupt the real-time balance between energy generation and consumption by means of falsifying consumption data [69]. On an extreme case, that might result in blackouts, which are a common goal of cyberwarfare. For instance, during the Russian-Georgian war in 2008, cyber attackers took out Georgia's power system [70]. In another example, in 2015, an attack on Ukraine's power system caused a blackout affecting more than 225,000 consumers [70].

In IEEE 2030.5, security is predominantly achieved by employing HTTP over TLS 1.2 [71], [72]. The TLS records are transported using TCP, where the TLS handshake mechanism provides mutual authentication based on device certificates or self-signed certificates. Additionally, the TLS Record Protocol ensures data confidentiality using symmetric key cryptography and data integrity through a keyed Message Authentication Checksum (MAC) [29]. Given the reliance on TLS, how certificates are generated and handled within a IEEE 2030.5 network is at the core of the security provided by the standard.

While TLS version 1.2 has been superseded by version 1.3, the cipher suite specified by IEEE 2030.5 is compliant with the newer version [31]. This means that the cipher suite adopted by IEEE 2030.5 is based on an ephemeral key exchange which provides perfect forward secrecy, ensuring that the future compromise of a device's private key cannot be used to break the cryptography of past sessions [31].

A. Device Credentials

There are three credentials per device in IEEE 2030.5: the Short Form Device Identifier (SFDI), the Long Form Device Identifier (LFDI), and a Personal Identification Number (PIN). The fingerprint of a device's certificate results from executing a SHA256 [73] hash operation over the whole DER-encoded certificate. Both the SFDI and the LFDI are derived from that fingerprint [29].

More specifically, the SFDI corresponds to the certificate fingerprint left-truncated to 36 bits. It is expressed as 11 decimal digits for display purposes, with an additional sum-of-digits checksum digit concatenated to the right (thus resulting in a total of 12 decimal digits). The SFDI identifies a device within a HAN or site domain [29].

The LFDI, in turn, corresponds to the certificate fingerprint left-truncated to 160 bits (20 octets). It is expressed as 40 hexadecimal digits divided into four groups. The LFDI is used when a globally unique identity is required, such as for sending an event alert back to a service provider associated with a particular device [29].

Since the SFDI and LFDI are derived from public information (*i.e.*, the device's certificate), they can be easily computed by an eavesdropper. Thus, a device may also have an additional 6-digit PIN code, which can then be shared out-of-band with a service provider in conjunction with the SFDI or LFDI [29].

For most communication scenarios defined in the standard, the SFDI and PIN are supplied separately. However, it may be convenient to provide a single *registration code* in certain cases, which is achieved by the simple concatenation of the SFDI and the PIN expressed as a decimal number [29].

Best practices for managing these identifiers include generating PINs and identifiers using cryptographically secure algorithms to ensure randomness and avoid predictable patterns. The standard ensures that SFDI and LFDI have sufficient entropy to uniquely identify devices within their respective contexts (local for SFDI and global for LFDI). PINs and registration codes must be transmitted over secure channels, using TLS, to prevent interception. Out-of-band methods can be employed to securely share PINs with service providers. Additionally, robust validation mechanisms should be implemented on the server side to verify the PINs provided by client devices, with incorrect PINs triggering security protocols to prevent unauthorized access. Local registration attributes and device credentials should be used to enforce strict access control, allowing only authenticated and authorized devices to interact with the network.

Regularly updating PINs and certificates is necessary to minimize the risk of compromise. Automated systems should be used to manage updates and reduce manual errors. Mechanisms to revoke and replace compromised PINs and certificates promptly should be implemented to ensure that all devices in the network are synchronized with the latest credentials [29].

B. Authentication

Resource access authentication is achieved by using HTTPS. It may be possible to use higher abstraction authentication methods on top of HTTP-only transactions, but this is out of scope for IEEE 2030.5 [29].

The use of TLS [72] requires that all hosts implementing HTTPS server functionality utilize a device certificate whereby the server offers its device certificate as part of the TLS handshake [29].

C. Authorization

Access Control List (ACL) attributes, shown in Table V, describe what information is used to determine whether access to a particular resource by a specific client is allowed or denied. An ACL can implement more granular access control based on various criteria (*e.g.*, client identity). Conceptually, an ACL exists for every single available resource. However, in practice, only specific resources with more complex access policies would likely require ACLs based on all attributes presented in Table V [29].

TABLE V
ACL ATTRIBUTES

Attribute	Type	Description
IPAddr	IPAddr	IP address of client
Port	Integer	Port of client
Method	Bitmap	Bitmap of which methods are supported: 0x1: GET 0x2: PUT 0x4: POST 0x8: DELETE 0x10: HEAD
AuthType	Integer	0x1: No authentication 0x2: User authentication 0x4: Self-signed certificate 0x8: Device certificate
DeviceType	Integer	Based on the `OBJECT IDENTIFER` of the digital certificate

ACL attributes provide a mechanism for granting and revoking privileges to use specified methods with a particular resource, applicable to all resources described in IEEE 2030.5. According to the security policy, all ACLs will be initialized appropriately at startup and subsequently modified according to registration and authentication. If a resource does not contain an ACL, access is granted to the resource unconditionally [29].

D. Registration

The access to certain resources may require a registration. Registration is the procedure whereby a server that houses a resource is notified that a certain client will access it in the future. The registration information conveys the client's SFDI and, optionally, its PIN, which uniquely identifies it in the given context [29].

Registration may occur sometime before the client tries to access a resource, using a website to register the information with a service provider, for example. The service provider will then deliver the information to the *EndDevice* server using some out-of-band mechanism, and the server will update its registration list accordingly [29].

There is also an alternative form of registration that is not done beforehand. Instead, the first time a devices needs to access the resource, it can request its registration with the server. This request then remains pending until, for example, it is approved by an administrator.

Registration for clients occurs via an *EndDevice* resource corresponding to the client, which resides on an Energy Services Interface (ESI) associated with the utility, third-party service, or premises owner provider that is trusted to perform registration [29].

Fig. 12 shows device authentication with registration procedure examples (client A is not in the server's ACL local registration list).

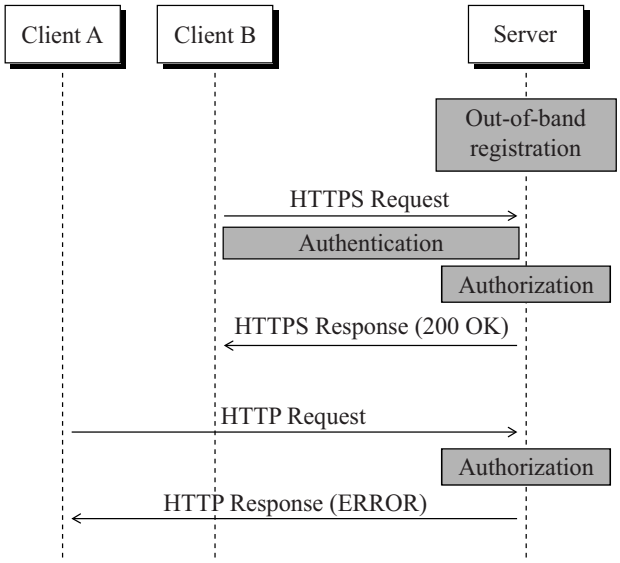


Fig. 12. Device authentication with registration procedure examples.

E. Public-Key Infrastructure

Public-Key Infrastructure (PKI) can be defined as the set of tools and processes required to perform the complete lifecycle management of a digital certificate issued by a Certificate Authority (CA) [29]. The X.509 standard defines the most commonly used format for public-key certificates [74].

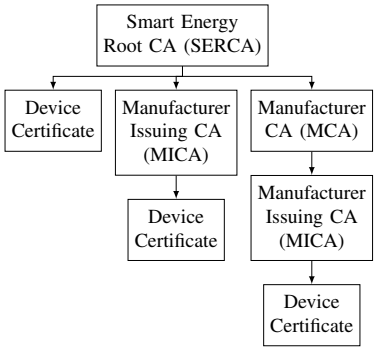
Every certificate also has a limited validity period. However, during that validity period, a certificate owner or CA that issued the certificate may declare it is no longer trusted. In these cases, the untrusted certificates must be revoked. The revogation is done by adding the untrusted certificate to a Certificate Revoked List (CRL).

Another method to convey information to users about revoked certificates is the Online Certificate Status Protocol (OCSP) [75]. Using this protocol, the client requests status information for a given certificate directly from the CA's revocation server instead of downloading the entire CRL and searching for the certificate of interest.

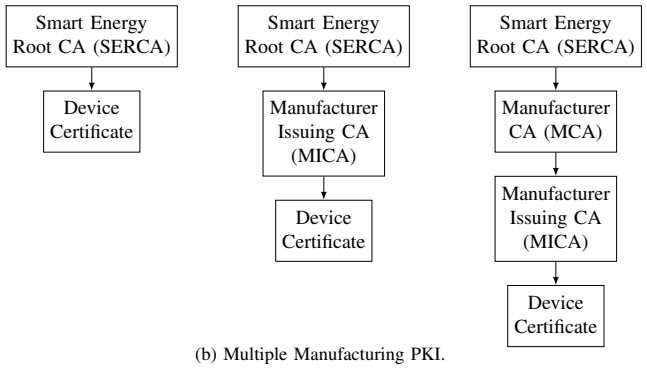
1) Manufacturing PKI: The IEEE 2030.5 standard specifies a PKI called Manufacturing PKI. The Manufacturing PKI issues certificates to devices during manufacture when the application is installed. These certificates are used during deployment and ongoing operation to authenticate the device with other IEEE 2030.5 devices implementing IEEE 2030.5 applications over TLS. It is expected that the market will implement one or more Manufacturing PKIs by the requirements outlined in this standard [29].

As illustrated in Fig. 13, any IEEE 2030.5 Manufacturing PKI should be a hierarchy with a depth of 2, 3, or 4 levels. At the top level, the Manufacturing PKI hierarchy should have one Smart Energy Root CA (SERCA). The elements that make-up the Manufacturing PKI are [29]:

- SERCA – the top-level (*root*) CA. A SERCA may issue device certificates on behalf of one or more manufacturers.
- Manufacturer CA (MCA) – an intermediate CA operated by a specific manufacturer to issue certificates for the Manufacturing Issuing CAs.
- Manufacturer Issuing CA (MICA) – an issuing CA that issues certificates to devices during the manufacturing



(a) Single Manufacturing PKI.



(b) Multiple Manufacturing PKI.

Fig. 13. Manufacturing PKI hierarchical structure examples.

process.

- Device Certificate – a digital certificate installed within a device that binds the device to its identity.

2) Certificate Management: All IEEE 2030.5 certificates are X.509 v3 certificates as defined in [76]. There are six classes of certificates that may be active in an IEEE 2030.5 deployment, depending on configuration and use, as follows [29]:

- **Device certificates** – issued under the Manufacturing PKI during manufacturing for purpose-built (aka "native") IEEE 2030.5 certified devices for operational objectives;
- **Device test certificates** – issued under the Manufacturing PKI during manufacturing to native IEEE 2030.5 certified devices for test purposes;
- **Additional certificates for IEEE 2030.5 devices** – one or more optional TLS server certificates issued by non-IEEE 2030.5 CAs to IEEE 2030.5 devices such as ESIs for use in complement to the device certificate;
- **Generic client certificate for non-native entities** – a TLS client certificate issued by a non-IEEE 2030.5 CA to a non-native entity;
- **Generic server certificate for non-native entities** – a TLS server certificate issued by a non-IEEE 2030.5 CA to a non-native entity;
- **Self-signed client certificate for non-native entities** – a TLS client certificate self-generated and self-signed by a customer or software.

In the context of IEEE 2030.5 standard communications, the authentication matrix provided in Table VI establishes the

TABLE VI
TLS AUTHENTICATION MATRIX.

		Server		
		Native IEEE 2030.5 application	**Generic server**	**Self-signed**
Client	**Native IEEE 2030.5 application**	IEEE 2030.5 Cert indef [1]	Optional OCSP	Not allowed
	Generic client	Optional OCSP	Not specified	Not specified
	Self-signed	Signature validation	Not specified	Not specified

[1] IEEE 2030.5 certificates are indefinitely valid, which means that only the signature validity of the chain of certificates is verified for this combination.

protocols for validating servers and applications, specifically prohibiting the use of self-signed certificates for server authentication within native IEEE 2030.5 applications. However, a client with a self-signed certificate is still able to communicate with a native application IEEE 2030.5 server. In other words, there are stricter requirements for the authentication of servers with clients than for the authentication of clients with servers. Under those circumstances, the ACL attributes listed in Table V offer a more comprehensive set of guidelines that detail the access parameters for any client, whether a server or an application, seeking to interact with protected resources. Consequently, the employment of self-signed certificates is contingent upon the communication context and the associated security policies [29].

For instance, a native IEEE 2030.5 application has the option to use OCSP for additional verification when interfacing with a Generic client certificate. However, self-signed certificates used by servers are typically not permitted when communicating with a native IEEE 2030.5 application client. The standard also considers certificates issued by the Manufacturing PKI as indefinitely valid, meaning that a native IEEE 2030.5 application will only validate the certificate signatures without performing any CRL or OCSP checks [29]. This underscores the standard's strict stance, which mandates that CAs shall not maintain CRLs or operate OCSP servers, and that clients and servers should not rely on these methods for certificate verification.

One of the reasons for not using CRL/OCSP is that such solutions would require the CA's servers to be somehow reachable by the IEEE 2030.5 devices. Notice that the CA's responsible for IEEE 2030.5 devices' certificates will usually not be managed by the utilities, but instead by the device manufacturers or even by third parties. However, there is no guarantee that all IEEE 2030.5 devices will have Internet access to make reliable use of such services [31], despite having connectivity with the utilities' servers to send measurements or request information, the used network infrastructure will not usually be connected to the public Internet, thus not allowing external entities to be reached.

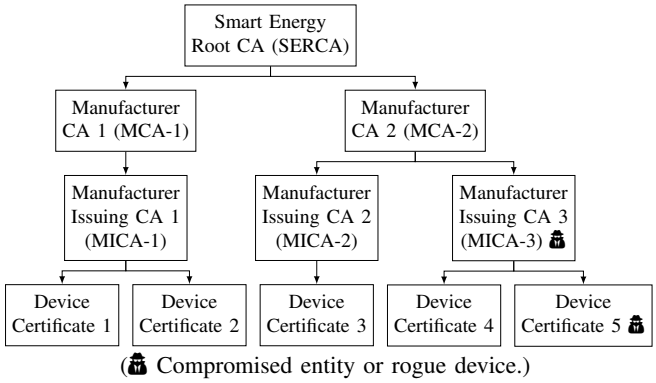


Fig. 14. Example of how a compromised Manufacturing PKI hierarchy can allow rogue devices.

F. Security Gaps in Certificate Management

From the previous section, two security gaps in the IEEE 2030.5 Manufacturing PKI [31] were identified:

1) the use of non-expiring certificates;
2) the explicitly prohibition of CRL and OCSP for validity checks.

Once issued, a device certificate has an unlimited lifetime, and it is always considered valid. Thus, if the device's private key is compromised, its certificate cannot be revoked.

To cope with these issues, device manufacturers are expected to use best practices to secure and protect their private keys. Moreover, servers or clients are allowed to maintain lists of blocked or allowed devices if the operator so chooses [31].

As IEEE 2030.5 devices are expected to be widely used, many of them will likely operate without user intervention and therefore will not be constantly monitored. Thus, episodes of credentials compromise may occur without the knowledge of an administrator. Additionally, there is no clear definition of who will be responsible for reporting compromised certificates [31]. Some issues with the workarounds often used to deal with those problems are discussed below.

Revocation of certificates through local lists (whitelists or blacklists) usually leads to inconsistency, because there is no guarantee that all devices will have the same information on their respective lists at all times [31]. The secure management of the local blacklists also becomes a problem, since, if an attacker is able to add fake entries to it, he or she may cause, for example, a Denial of Service. Additionally, even if there is a local policy to synchronize blacklists for all devices in a certain IEEE 2030.5 deployment, stolen credentials could be used to damage a different area [31].

This lack of a well-defined framework specifying the processes to be performed in a possible certificate compromise event is potentialized for MICAs and MCAs, as shown in the example of Fig. 14. Because MCAs and MICAs can generate and sign certificates for the system and there is no certificate revocation, if they are compromised by an attacker, there are no concrete means to prevent the emission of certificates for rogue devices that may harm the system. In addition, if a company operating an MCA becomes unfit for such activity, there are no definite means to render obsolete the use of the MCA certificate [31].

Besides those issues, it is also essential that the certificates have a limited validity period. With this feature, devices that are not updated — for example, to avoid the usage of cryptographic algorithms that become obsolete with time — are automatically disabled from integrating any system that performs certificate expiration verification. The same characteristic also allows certificates to be revalidated for reuse of long-life devices [31].

G. XML and WADL Security Concerns

The integration of WADL and XML in power grid applications introduces some security challenges that must be addressed to ensure the integrity and reliability in IEEE 2030.5 communications. These challenges arise from the inherent vulnerabilities in RESTful APIs and XML data handling, which can be exploited by attackers to compromise the system.

Firstly, vulnerabilities in RESTful APIs present significant security risks. Cross-Site Scripting (XSS) allows attackers to inject malicious scripts into the API, potentially compromising user interactions and accessing sensitive data. These attacks take advantage of the trust that system operators have in a web application, often intercepting web authentication cookies. The intercepted cookies are then used to gain access to controllers or web-based Human-Machine Interface (HMI) systems [77]. Additionally, broken access control can lead to unauthorized access to API endpoints, resulting in privilege escalation and data theft. Furthermore, Denial of Service (DoS) attacks can flood the API with requests, disrupting service and denying legitimate users access. These vulnerabilities highlight the importance of implementing robust security measures in the development and deployment of RESTful APIs.

Additionally, the authors in [77] point out the importance of sanitizing user input before storing or displaying it and of data type validation. Sanitization, in this context, refers to the process of cleaning and verifying user-provided data to ensure it does not contain malicious or harmful content. This prevents attacks such as code injection. The sanitization process includes removing dangerous characters, validating data, and escaping input. Removing dangerous characters eliminates or escapes special characters used in attacks, such as quotes and angle brackets. Data type validation ensures that the input is in the expected format, such as numbers, text, or dates. Input escaping transforms special characters into their safe representations, such as "<" into "`<`" for example.

Additionally, XML poses its own set of security issues, notably XML Injection attacks. Malicious XML data can be injected into the system, allowing attackers to execute arbitrary code or manipulate data. XML External Entities (XXE) attacks further exacerbate this risk by enabling attackers to read files or execute external commands on the system. To mitigate these risks, it is essential to validate XML data against the expected schema, ensuring that only legitimate data is processed.

Access control and authorization mechanisms are also critical in securing power grid applications. Strict access control ensures that only authorized users can access critical systems and data, while proper authorization checks at all API endpoints prevent unauthorized access. These measures help

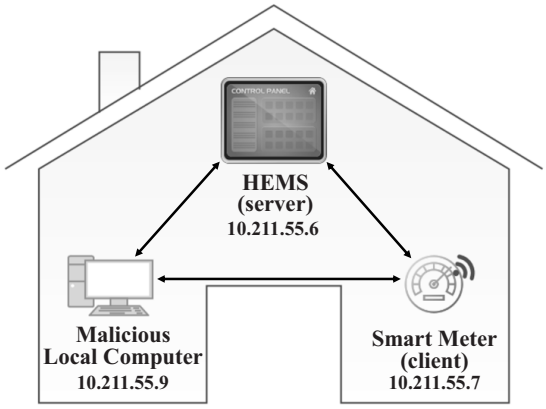


Fig. 15. Topology of the testing environment.

safeguard sensitive information and maintain the integrity of the system.

Beyond sanitization, another mitigation strategy in XML parsers used in power grid systems is to disable external entity expansion. External entity expansion is a feature in XML where entities defined outside of the current XML document are included and processed by the XML parser. This security measure prevents attackers from including malicious external entities in XML documents, which could lead to severe vulnerabilities such as sensitive data exposure, denial of service (DoS) attacks, or remote code execution. By disabling external entity expansion, power grid systems can protect against XML External Entity (XXE) attacks, which exploit the XML parser's capability to process external entities.

VI. Proof of Concept Attack

In this section, a proof of concept attack is described to demonstrate the practical implications of the security gaps of how IEEE 2030.5 handles digital certificates.

A. Test Topology

For this proof of concept, we use a test topology based on communication between a client device (smart meter) and a HEMS, as illustrated in Fig. 15. Both devices have digital certificates to operate secure communication generated according to the IEEE 2030.5 standard specification. There is also the entity of a local computer in the test topology, representing a malicious network device that attempts to perform harmful actions on the network.

Each device is implemented by a Virtual Machine (VM) running Linux. The smart meter is implemented in a virtual machine running a Posix system called *client*, which runs a C implementation of a simplified IEEE 2030.5 client developed by [78] and [79]. We used XCA [80] to create a root CA (and its self-signed digital certificate), in order to emulate the Smart Energy Root CA (SERCA). Then, this root CA was used to issue the HEMS digital certificate. We then added the CA's digital certificate to the smart meter's list of trusted certificates. The CURL tool was used to perform HTTPS requests to IEEE 2030.5 resources.

The HEMS is represented by a VM called *server*, which runs Python 3.8.5 and the Flask microframework [81]. Flask allows the creation of RESTful Applications Protocol Interfaces (APIs) in a simple and agile way. Flask also implements mutual authentication over TLS, where the server verifies the digital certificate presented by the client device. Since our goal is to provide a simple proof of concept, we only implement a few basic HEMS functions, such as *EndDevice*, *Register* and *TariffProfile*.

The malicious local computer is represented by a VM named *server-devil*, where Flask is used to implement any fake HEMS function (as generating fake messages of excessive or deficient power consumption data). This malicious computer also runs the HPING3 tool [82]. This tool can be used to execute a TCP SYN flood attack [83]. This will overload the legitimate HEMS on the network, causing it to stop responding to requests for smart meters. Although we acknowledge that there are countermeasures to prevent the TCP SYN Flooding Attack, here we use it as a simple example of a Denial of Service (DoS) attack. In practice, an attacker might resort to other approaches as detailed explained in [84] to the same effect.

B. Assumptions

We assume that the attacker is in the same subnet as the HEMS and is capable of capturing packets of legitimate communication between the HEMS and the smart meter. In a practical execution of this attack, this could be achieved in a number of ways. For example, the attacker may have previously compromised another device connected to the same subnet. If the communication network is wireless, the attacker might also be able to connect and use its own device remotely.

C. Scenarios

We consider three different scenarios:

- Scenario 1 – No attack. This illustrates the normal behavior of a smart meter to HEMS communication.
- Scenario 2 – Compromise of the HEMS' digital certificate.
- Scenario 3 – Compromise of the smart meter's digital certificate.

1) Scenario 1: Initially, the smart meter connects to the HEMS to verify which functions sets are available. For that, the smart meter requests the *DeviceCapability* (dcap) resource of HEMS. This requires mutual authentication between the parties using TLS. Fig. 16 shows this communication, with relevant information in red. First, we can see that the HEMS has an active RESTful interface listening on port 8443. The smart meter then requests the `dcap` resource of the HEMS, using the Linux CURL tool. Mutual authentication through TLS is successfully achieved and, then, the HEMS sends the requested resource to the smart meter.

Based on that reply, the smart meter discovers that the HEMS has the *EndDeviceList* function set. After that, it needs to confirm that it is registered with the HEMS. This is done by utilizing the `register` parameter of the

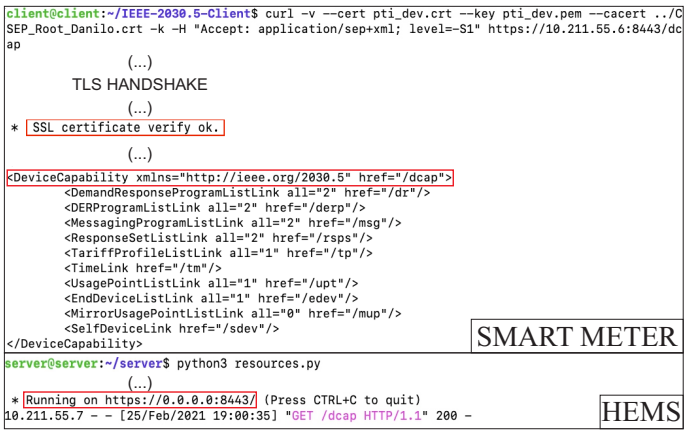


Fig. 16. *DeviceCapability* resource.

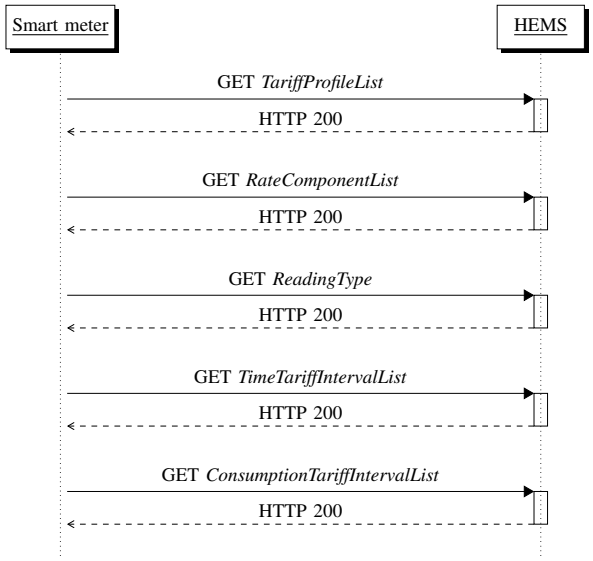


Fig. 17. The message exchange flow to check the consumption tariff.

`client_test` routine of the IEEE 2030.5 client implementation. Fig. 21 shows this registry verification process. First, the `client_test` application calculates the LFDI and SFDI of the smart meter. Then, the digital certificates of the trusted CA are loaded, and the devices are mutually authenticated. In case of failure, communication is interrupted. Otherwise, the message exchange between the devices is initiated. Finally, as the smart meter's SFDI/LFDI/PIN was previously registered with the HEMS, the application confirms that it can access the HEMS' resources. It is important to note that the PIN is optional for registration. In this test, we used a PIN "111115".

The client now proceeds to check the energy price. The cost of energy may vary depending on the time. At peak consumption times, the price is higher to inhibit excessive consumption that could overload the electrical system. Therefore, energy price information helps the homeowner control the consumption and final amount of the electricity bill. The message exchange flow in IEEE 2030.5 to obtain the tariff is shown in Fig. 17.

Fig. 18 shows these message exchanges between the smart meter and the HEMS in our tests. Before starting the exchange

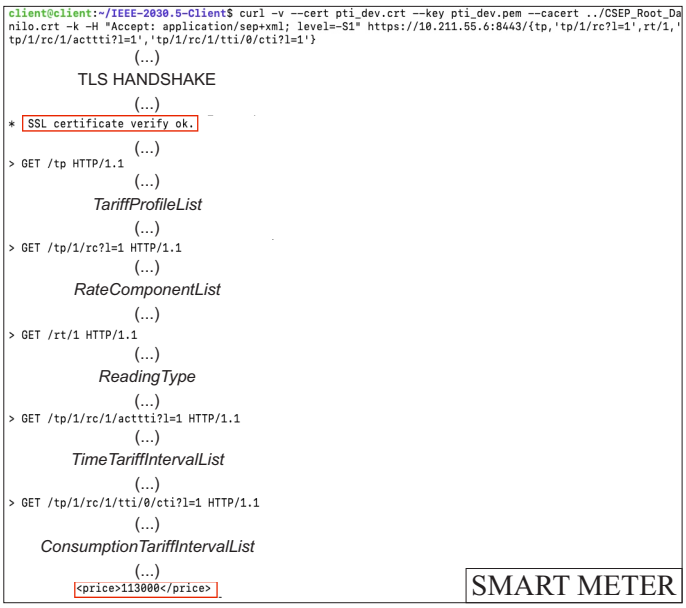


Fig. 18. Energy price request by smart meter.

of messages, mutual authentication is performed. Upon successful authentication, the exchange of messages is initiated and, hence, the smart meter considers that the received information is true (in this case, the tariff value is 113,000 currency units, highlighted in a red frame).

2) Scenario 2: In this scenario, we assume that an attacker has compromised the private key associated with the HEMS' digital certificate. Consequently the attacker is able to impersonate the HEMS by presenting its digital certificate in communications with the smart meter. As discussed in Section V-F, The explicit prohibition of CRLs and OCSP for validity checks is clearly stated in the IEEE 2030.5 standard. As a result, it is not possible to revoke its certificate. Thus, if the HEMS's private key is compromised, its certificate cannot be revoked. Thus, the false HEMS can provide a false value for the energy price. More specifically, we assume that the false HEMS presents a lower energy price to the smart meter, which incentives consumption. During a period of peak demand, that might be used to overload the power grid.

The malicious device initiates a DoS attack against the HEMS using the HPING3 tool [82]. From then on, the smart meter can no longer communicate with the HEMS to check the energy price and the evil device can impersonate the HEMS. This is illustrated in Fig. 19.

We assume that the smart meter executes a new service discovery, as discussed in Section IV-C, to find an alternative device that provides the energy price resource, thus obtaining the connection information for the rogue HEMS.

Fig. 20 shows the communication between the smart meter and the fake HEMS. Notice how the energy price sent to the smart matter has changed (to 105,000) with respect to Scenario 1. This attack can instruct residents to increase consumption when the power grid is in peak demand.

3) Scenario 3: In this scenario, we assume the smart meter has its private key compromised (see the challenge results

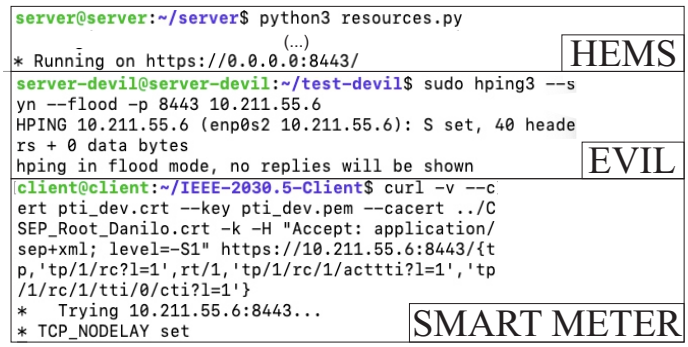


Fig. 19. Illustration of the DoS attack on HEMS. The smart meter is unable to connect the real HEMS once the attack is started.

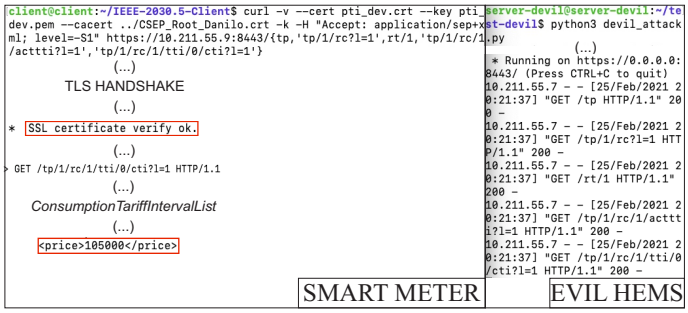


Fig. 20. Sending false consumption tariff to smart meter.

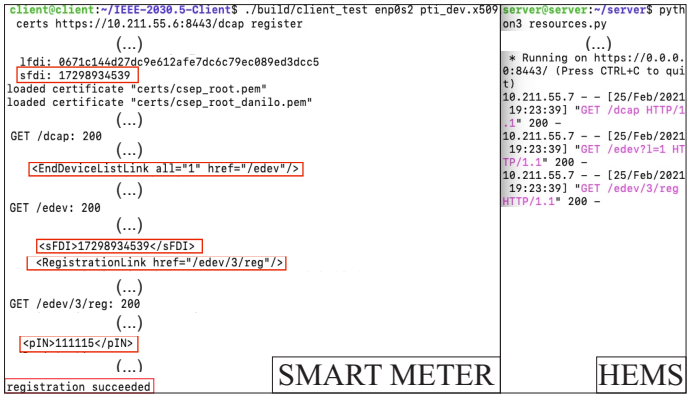


Fig. 21. Smart meter registration check.

mentioned in [85] for an example). Afterward an attacker can impersonate the smart meter and initiate communication with the HEMS providing false meter reading information that can cause financial losses to the utility.

To this end, the attacker initiates a DoS attack against the smart meter to prevent it from communicating with the HEMS. From then on, the attacker initiates communication with the HEMS to send the false measurement information. It provides the HEMS with the legitimate certificate of the real smart meter and uses the smart meter's private key to establish an authenticated TLS connection. Because the certificate is correctly signed by the CA and there is no verification of validity or revocation, authentication always succeeds. After that, the attacker transmits a measurement with a falsified value (in this example, a value of 5), different from the real

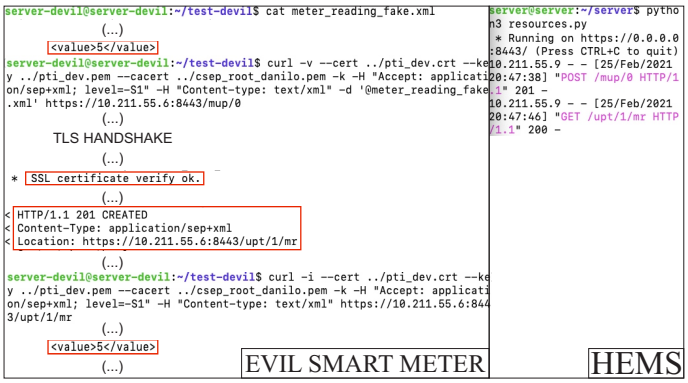


Fig. 22. Sending false meter reading to HEMS.

consumption. Because the meter passed authentication, the HEMS accepts the measurement value and records it so that the utility can read it at a future time — for example, for billing the client. Those communication steps are illustrated in Fig. 22.

D. Practical Impacts

Our proof of concept attack is divided into two main components. Initially, the attack involves compromising either the digital certificate of the Home Energy Management System (HEMS) or that of the smart meter. This breach sets the stage for the subsequent phase, a Denial of Service (DoS) attack, which specifically targets and overloads the legitimate HEMS. Detailed descriptions of these attack scenarios are provided in this section, under scenarios 2 and 3, and are illustrated in Figs. 19, 20 and 21. Once the exploitation of the vulnerability is successful, the attacker is then capable of performing a series of actions, and the potential impacts and consequences are also discussed here.

1) Data Manipulation:

- **Impact:** attackers intercepting and altering communications can inject false data, leading to incorrect billing, misleading demand response systems, or unbalancing the grid load.
- **Consequence:** such manipulations can degrade the reliability and efficiency of the grid, causing operational inefficiencies and instability, raising the risk of catastrophic failures or systematic disruptions.

Disruption of Demand Response Programs

- **Impact:** inaccurate data from compromised devices disrupts programs adjusting energy distribution during peak times.
- **Consequence:** reduced effectiveness of these programs can lead to power over or under-generation and increased operational costs.

Billing Errors

- **Impact:** compromised data integrity may result in incorrect energy usage reporting.
- **Consequence:** this can lead to financial discrepancies and erosion of consumer trust due to billing inaccuracies.

Load Balancing Issues

- **Impact:** falsified data may lead to load balancing mismanagement within the grid.
- **Consequence:** this can cause unexpected loads, damaging infrastructure and causing energy wastage.

VII. Other Security Issues and Possible Solutions

This section explores other critical security dimensions of the IEEE 2030.5 standard, fundamental in safeguarding DER communications. To that end, we review a number of references related to security issues in Smart Grids, in general, as well as more specifically in the IEEE 2030.5 standard.

A. Guidelines for Smart Grid Cyber Security

Since its inception in 2010, NIST's guidelines for Smart Grid operation [86] have laid the groundwork for strategic, architectural, and operational cybersecurity practices within the Smart Grid field. It was developed by members of the Smart Grid Interoperability Panel and the Smart Grid Cybersecurity Committee. It outlines, among other topics, comprehensive security requirements and extensive privacy considerations. It emphasizes Security and Risk Assessment, Authorization, Operational Continuity, and addresses Physical and Environmental Security alongside practical scenarios. Yet, in the same work, the authors delve into Smart Grid Cryptography and Key Management, highlighting issues like Certificate Revocation and Expiration, and introduce a vulnerability matrix to identify and mitigate security risks. This comprehensive approach by NIST has significantly contributed to shaping future frameworks for the Smart Grid, notably by presenting use cases and example scenarios.

Following the publication of NIST's guidelines, subsequent research and practical applications have built upon this foundation, identifying and addressing new security vulnerabilities, thereby enhancing and extending the cybersecurity measures for Smart Grids.

B. Autonomous Operational Domains

The work in [111] presents a taxonomy of autonomous domains within the DER communication infrastructure, their associated security vulnerabilities (SV), and hardening recommendations. Fig. 23 presents these domains and vulnerabilities in a hierarchical tree structure, and in Table VII, we extend and detail potential solutions for each SV. As these entities engage in bi-directional communication flows, their exposure to cyber risks escalates, necessitating a comprehensive assessment of potential vulnerabilities.

For instance, Third-party Aggregators and Virtual Power Plants, which are integral to demand-response coordination and energy dispatch, may face denial of service attacks that incapacitate their monitoring and control capabilities. Similarly, DER vendors and operators are susceptible to spear phishing attacks that could compromise IEEE 2030.5 servers, altering DER parameters to the detriment of grid stability. The Electric Power System (EPS) Operator Area, responsible for maintaining grid balance and stability, could be targeted by advanced persistent threats, further amplifying the risks

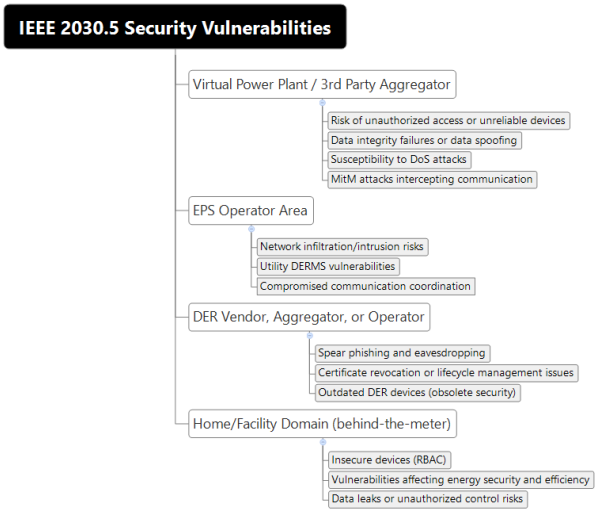


Fig. 23. Hierarchical tree of IEEE 2030.5 security vulnerabilities across smart grid domains, organized by domain as presented in [111].

to the broader energy infrastructure and the Home/Facility Domain, operating behind-the-meter, must contend with the possibility of insecure DER devices, which can be manipulated to authorize external control, leading to privacy breaches and service disruptions.

In the next subsections, we will discuss each of those entities and domains in more detail. To organize this discussion, those subsections are structured according to the tree shown in Fig. 23.

C. Virtual Power Plant or 3rd Party Aggregator

A real or traditional power plant is a physical facility that generates electricity from various energy sources, such as coal, natural gas, nuclear, hydro etc. A VPP, on the other hand, does not have a centralized physical infrastructure. Instead, it consists of a network of DERs, like rooftop solar panels, small wind turbines, battery storage systems, and demand response units. These resources are spread across different locations but are aggregated and managed through some software to act as a single, coordinated energy resource.

This integration of many resources exposes these systems to heightened cyber threats, notably Distributed Denial-of-Service (DDoS) attacks [112]. These vulnerabilities, demonstrated by significant cyber incidents, underscore the need for enhanced security within the DER ecosystem. Recently, the ethical hack described in [5] involved exploiting vulnerabilities in the API of a VPP. The attacker generated and manipulated tokens signed with weak 512-bit RSA keys. By cracking the RSA key, the attacker was able to forge valid API tokens, gaining unauthorized access to the VPP system, highlighting the risks of using outdated cryptographic standards.

Among the potential solutions found on the literature, we highlight the ones shown in in bold in Table VII, as they provide critical insights into these challenges, offering distinct perspectives and solutions. Those are discussed in more details in the following paragraphs.

TABLE VII
SECURITY VULNERABILITIES ASSOCIATED WITH IEEE 2030.5 IN SMART GRID AUTONOMOUS OPERATIONAL DOMAINS.

Domains	Security Vulnerabilities (SV)	Potential Solutions for each SV
Virtual Power Plant or 3rd Party Aggregator	1) Risk of unauthorized access or non reliable devices. 2) Data integrity failures or data spoofing leading to incorrect operational decisions. 3) Susceptibility to DoS attacks. 4) MitM attacks that intercept and potentially alter communication between the aggregator and DERs.	1) [87], [88], **[89]**. 2) **[31]**, [90], [91]. 3) **[92]**, **[93]**, [94]. 4) **[31]**, **[39]**, [95].
EPS Operator Area	1) Network infiltration/intrusion risks within IT networks. 2) Vulnerabilities within Utility DERMS affecting DER management and grid stability. 3) Compromised communication leading to operational lack of coordination.	1) **[89]**, **[96]**, [97], [98]. 2) **[7]**, [9], [99]. 3) **[100]**, [101].
DER Vendor, Aggregator, or Operator	1) Spear Physhing attacks and Eavesdropping, attacker listens to confidential info expect stealing sensitive data. 2) Certificate revocation or life cycle management issues. 3) Outdated DER devices (obsolete security design), leaving them susceptible to known exploits.	1) [102], [103]. 2) [89] , **[104]**, **[105]**. 3) **[27]**, [89], [94].
Home/Facility Domain (behind−the−meter)	1) Insecure devices allowing external access (RBAC). 2) Vulnerabilities affecting energy security and efficiency. 3) Devices risks leading to data leaks or unauthorized control.	1) **[103]**, **[106]**. 2) [107]. 3) **[108]**, [109], **[110]**.

a) Adversary-Based Assessments and Gap Analysis: The authors in [31] and [39] highlight common security threats, such as Packet Replay, Man-In-The-Middle (MITM), and DoS attacks. These reports critique the existing cryptographic standards and the over-reliance on outdated encryption mechanisms. Both emphasize the crucial gap in comprehensive Certificate Policy (CP) and robust certificate revocation mechanisms, which might allow compromised devices to remain active within the network, posing a significant risk to the security integrity of DER systems.

b) Recommendations for Enhancing Security: While addressing vulnerabilities, both reports propose common recommendations to improve DER security.

- Update encryption algorithms to better protect data in transit.
- Establish ecosystems that support certificate revocation lists (CRLs) or utilize Online Certificate Status Protocol (OCSP) to enhance trust and verification processes.
- Standardize interfaces between DER networks and utility servers to ensure consistent and secure communication.

Additionally, [39] delves into the integration of emerging technologies to strengthen DER communications, including:

1) **Mobile Trusted Module:** Ensures only verified software execution, thus mitigating firmware tampering risks.
2) **Mobile Device Management Software:** Provides a platform for managing and securing mobile devices, crucial for enforcing security policies remotely in DER systems.
3) **Per-Application VPN:** isolates application data into separate VPN tunnels.
4) **ARM TrustZone:** Segregates system resources into secure and non-secure zones, preventing unauthorized access.
5) **Post-Quantum Crypto:** Introduces encryption techniques resilient to quantum computing attacks, securing future communications. Employs decentralized infrastructure to enhance certificate security and prevent man-in-the-middle attacks.

The integration of DERs into smart grids, managed by Virtual Power Plants or third-party aggregators, introduces plenty of cybersecurity challenges. As DERs become increasingly reliant on communication networks for voltage regulation and coordination, the risks associated with cyberattacks grow. The work on [92] highlights how VPPs depend on information and communication technologies to manage and regulate voltage across DERs, making these systems vulnerable to attacks such as DDoS and data manipulation. In turn, the work on [93] provides complementary insights, focusing on the impact of cyberattacks on Renewable Generation (ReGen) plants and emphasizing how vulnerabilities in aggregator systems can directly disrupt voltage control coordination and compromise grid stability.

While [92] demonstrates that DDoS attacks targeting VPPs degrade operational performance by delaying or blocking critical updates to voltage regulation parameters, their work also reveals that disruptions in IEEE 2030.5-enabled communication pathways within VPP architectures can escalate into widespread instability. The work on [93] extends this understanding by analyzing how cyberattacks, such as time-varying delays and manipulated control signals in ReGen plants, exploit weaknesses in aggregator systems. Their findings show that small-scale UDP floods may introduce negligible delays, but larger-scale attacks can cause multi-hour disruptions, significantly increasing power losses and threatening

grid stability.

Additionally, [93] raises specific concerns regarding the manipulation of droop values in ReGen plants. They demonstrate through simulations that extreme droop value manipulations can trigger cascading failures, such as severe voltage oscillations and overvoltage conditions, forcing DER shutdowns. These scenarios illustrate practical vulnerabilities in IEEE 2030.5-based communication frameworks and align with the broader framework for vulnerability indexing proposed by [92], which can prioritize critical DER nodes for enhanced protection.

Both studies propose actionable solutions to mitigate these risks. In [92], authors advocate for a structured vulnerability assessment index, enabling operators of VPPs and aggregator systems to identify and secure critical DER components. On the other hand, [93] focuses on implementation-level countermeasures such as DDoS scrubbing centers, which filter malicious traffic while maintaining low latency, and IPsec protocols to ensure the confidentiality and authenticity of communications between ReGen plants and aggregators. Together, these strategies create a multi-layered approach to securing voltage control coordination.

These findings underscore the need for IEEE 2030.5 to incorporate additional safeguards to address vulnerabilities in VPPs and third-party aggregators:

- **Enhanced Security Protocols:** [93] recommends integrating IPsec for secure and authenticated communication, addressing the risks of eavesdropping and tampering in IEEE 2030.5.
- **Vulnerability Prioritization:** [92] proposes a vulnerability index that offers a systematic method for identifying and protecting key IEEE 2030.5 nodes in VPP architectures.
- **Real-Time Monitoring:** both works emphasize the importance of real-time monitoring tools and attack simulations to evaluate the resilience of IEEE 2030.5-based systems under evolving cyber threats.

In addition to the works previously mentioned, [90], [91], [94], [95] also provide relevant studies that cover one or more SVs shown in Table VII.

D. EPS Operator Area

An Area EPS Operator is responsible for managing and operating the electrical power system within a specific geographical region, ensuring the balance between electricity supply and demand, and maintaining grid stability and reliability. A study in [7] analyzes cyber-resilience in microgrid systems, with a focus on the IEEE 2030.5 standard. The research presents a simulated testbed using OpenDSS for modeling PV/Inverter interactions within a cyber-physical resiliency framework, emphasizing secure communication protocols, vulnerabilities in Utility DERMS, and the risks of compromised communication leading to operational lack of coordination.

The study highlights significant vulnerabilities in CSIP implementations, such as MITM and SSL/TLS downgrade attacks. It introduces a resilience scoring system that considers both topological and physical factors, offering a quantitative measure of a microgrid's ability to withstand cyber threats. However, while the scoring system is a valuable tool for strategic microgrid design and rapid response planning, the study does not provide specific countermeasures for these identified vulnerabilities, particularly in contexts beyond military scenarios, which may limit its broader applicability.

Both [96] and [100] highlight the growing attack surface due to the increasing penetration of DERs and their reliance on communication protocols like IEEE 2030.5. The work by Ravi *et al.* [100] identifies key vulnerabilities, such as:

- Lack of encryption in communication channels, exposing DER data to interception and tampering.
- The use of outdated protocols (e.g., HTTP and Modbus) in some DER devices, which do not meet the security standards recommended by IEEE 2030.5.
- The risk of Distributed Denial of Service (DDoS) attacks disrupting the availability of DER systems in the EPS Operator Area.

Similarly, Lai *et al.* [96] emphasize the difficulty of distinguishing malicious events from operational anomalies in DER systems. This challenge is exacerbated by the intermittent nature of DER data and the variability introduced by renewable energy sources.

To address these challenges of intrusion detection system, Lai *et al.* [96] propose a hybrid IDS that integrates physical data with network-level cyber data. This approach leverages:

- Deep packet inspection tools tailored for protocols such as Modbus, DNP3, and IEEE 2030.5.
- Machine learning models to reduce false positives and identify zero-day attacks.
- Cyber-physical correlation to enhance the accuracy of anomaly detection.

On the other hand, Ravi *et al.* [100] stress the importance of implementing a PKI for DER authentication and authorization, as outlined in IEEE 2030.5. Their experiments demonstrate the feasibility of employing advanced encryption algorithms, such as AES-256, in resource-constrained DER devices.

The findings from these studies underline several implications for enhancing the implementation of IEEE 2030.5 in the EPS Operator Area:

- **Enhanced Protocol Filters:** intrusion detection systems must incorporate protocol-specific filters for IEEE 2030.5 to ensure comprehensive monitoring of DER communications [96].
- **PKI-Based Security Frameworks:** adoption of X.509v3 digital certificates and TLS 1.2 encryption for DER devices should be mandatory to ensure secure communication, as demonstrated in [100].
- **Resilient System Architecture:** decentralized access control mechanisms and role-based permissions, as highlighted by Ravi *et al.* [100], can mitigate risks associated with centralized points of failure.
- **Integrated Cyber-Physical Models:** the hybrid IDS proposed by Lai *et al.* [96] should be further developed to provide real-time insights into both cyber and physical layers.

Beyond those works, additional studies such as [9], [97]–[99], [101] are also pertinent to topics shown in Table VII.

E. DER Vendor, Aggregator, or Operator

These entities manage and control individual DERs or groups of DERs. A DER Vendor provides the technology (*e.g.*, solar panels or batteries), an Aggregator pools multiple DERs to act as a larger resource, and an Operator manages the operation of these resources within the grid. In this scenario, Baker *et al.* [27] point out some issues in DER Vendor, Aggregator, or Operator autonomous entities. Originally, DER devices were designed to be static, lacking the necessary defenses to address evolving threats. This gap in design leaves them unprepared against sophisticated cyber attacks. The situation is exacerbated by the reliance on public and poorly-secured networks for communication, amplifying the risk of unauthorized access and data breaches, making the entire energy infrastructure more susceptible to advanced persistent threats (APTs). These APTs, characterized by their stealth, continuity, and complexity, aim to disrupt grid operations and achieve more sophisticated goals.

The expanding integration of DERs within the grid increases the system's vulnerability to Advanced Persistent Threats (APTs), as these devices were originally designed without adequate defenses against evolving cyber threats. IEEE 2030.5 introduces several security measures to mitigate these risks, categorized below into Protocol Implementations and Client Communications.

a) Protocol Implementation:

- **HTTP over TLSv1.2** ensures secure data transmission, protecting against spear phishing and eavesdropping by encrypting communications. This is critical in preventing attackers from intercepting and stealing sensitive information during transit.
- **X.509 device certificates** provide robust authentication, addressing challenges related to certificate revocation and lifecycle management. This ensures that only authorized devices are allowed network access, reducing the risk of compromised or expired certificates.
- **PKI authentication** is used to verify device identities, safeguarding the grid against unauthorized access, particularly from outdated DER devices with obsolete security designs. This measure ensures that only secure and validated devices can communicate within the network.

b) Client Communications:

- **Randomized polling intervals** and **pre-defined polling schedules** are employed to obscure predictable communication patterns, making it difficult for attackers to exploit timing vulnerabilities, especially in outdated DER devices.
- **Scheduling of future events** reduces the need for continuous communication, thereby decreasing the network's exposure to potential attacks. This controlled communication approach not only minimizes the attack surface but also helps protect against unauthorized access and interference.

Also, the authors in [105] introduce a Keyless Infrastructure Security Solution (KISS). KISS leverages the robust immutability features of distributed ledger technologies (DLTs) combined with a calendar hash system to offer mechanisms to store and maintain digital data fingerprints that can later be used to validate and assert data provenance. Their approach is designed to enhance data integrity and trust within the grid's communication channels through a decentralized architecture, thereby mitigating the risks associated with centralized systems prone to single points of failure. KISS facilitates the establishment of trust relationships among grid participants via digital identities and lifecycle management, without necessitating significant modifications to existing infrastructure.

On the other hand, Mahmood et al. [104] proposed a certificate verification scheme called FONICA, designed to enhance efficiency in fog computing environments by reducing storage consumption, communication overhead, and latency for edge devices, which is crucial for DER vendors, aggregators, or operators managing numerous devices. FONICA acts as an Intermediate Certification Authority, issuing short-lived certificates (SLC) to edge devices, ensuring secure communication and immediate revocation of certificates when necessary. The scheme significantly outperforms existing methods like CRL and OCSP, particularly as the number of edge devices increases, making it suitable for energy-efficient applications. Overall, FONICA addresses critical security issues while minimizing communication overhead, thus contributing to sustainable communication in DER vendor, aggregator, or operator environments.

Both studies prioritize data integrity and security, supporting real-time applications with distinct approaches. KISS enables real-time validation by signing critical functions, while FONICA ensures secure communication through chain-of-trust verification. Both methods are scalable and flexible, with KISS integrating seamlessly into existing SCADA systems and FONICA leveraging fog computing architecture. Regarding security, KISS prevents data tampering but does not guard against denial-of-service or phishing attacks, whereas FONICA offers broader protection, including efficient certificate verification.

Other relevant approaches in DER vendor, aggregator, or operator domain include [89], [94], [102] and [103].

F. Home/Facility Domain

The integration of Home/Facility Domain within the smart grid framework has significantly enhanced the coordination between power flow, information flow, and business operations, garnering considerable interest for its intelligent and convenient features. However, this advancement has also exposed numerous security vulnerabilities that necessitate rigorous investigation. Researchers have identified several critical security issues within the smart home ecosystem, including the authentication of device users, access control for smart home devices, and the secure interconnectivity of these devices. Moreover, the protection of privacy emerges as a pressing challenge that requires immediate and focused attention.

The authors in [108] propose a privacy protection scheme for smart meters in smart home networks using consortium

blockchain. This scheme safeguards user privacy and data leakage without relying on bilinear pairing and exponential operations, previously utilized by the authors in [113], to minimize computational costs. It offers reduced verification and communication overhead and employs consortium blockchain's distributed storage to address centralized storage's single-point failures and tampering issues. The scheme achieves Byzantine fault-tolerant consensus by designating community area gateways as pre-selected nodes rather than involving all network nodes, significantly lowering network overhead.

The work presented in [110] introduces a decentralized attribute-based signcryption scheme tailored for secure data sharing, capable of supporting user revocation and managing large attribute sets. This scheme emerges in response to the limitations of traditional attribute-based access control systems [114], [115], which typically depend on a unique data storage and are susceptible to being overwhelmed and vulnerable to key escrow issues within a single authority framework. To counteract these challenges, the scheme decentralizes attribute-based encryption, potentially enhancing system resilience.

The communication between the HEMS and the HAN may compromise user's power and personal sensitive information, potentially exposing privacy through detailed data like working hours, times of absence, and household appliance usage [116]. Such breaches could lead to property damage for users or the power company. Centralized storage for power data in smart homes, using a central node or gateway, introduces significant risks due to the challenge of establishing a universally trusted aggregator. This setup is susceptible to data loss from central node failures and tampering through cyberattacks.

In this approach, users are empowered to generate their own private keys, while authorities are responsible for producing private keys for the cloud server. Data owners contribute by creating both the signing public and private keys for attribute sets and generating ciphertexts. This arrangement ensures that the cloud server can only successfully verify and partially decrypt ciphertexts when the attribute sets presented by users align with the established signcryption policy. The scheme simplifies the process of user revocation by requiring only the deletion of the corresponding private keys from the cloud server.

A key advantage of this scheme is its efficiency as it reduces the computational load on Remote Terminal Units (RTUs) during the signcryption phase by outsourcing intensive computational tasks to third parties. These entities, external to the core communication or data exchange between the HEMS and the HAN, minimize the computational burden on users' side. Consequently, even if a user's attributes comply with the access policy, revocation ensures they cannot decrypt any ciphertext, thereby maintaining the system's security integrity.

The work in [103] proposes a fine-grained access control scheme based on blockchain and Attribute-Based Access Control (ABAC) to enhance data sharing in smart grids. It addresses the issue of unauthorized access, which discourages entities from sharing their data, thus limiting the potential value of that data. The solution employs smart contracts for automated policy evaluation and utilizes the Interplanetary File System (IPFS) for off-chain storage, ensuring reliable data management. The experimental results demonstrate the feasibility and effectiveness of the proposed scheme in ensuring secure and accountable data sharing.

Moreover, the authors in [106] propose a novel hybrid Role-Based Access Control (RBAC) model that integrates offline deep reinforcement learning (RL) and Bayesian belief networks to enhance security in organizational access control systems. It addresses inefficiencies in static RBAC management by dynamically improving policies based on user behavioral history. The model is implemented within a Home-/Facility Domain, demonstrating significant improvements in security accuracy and efficiency. The research highlights the effectiveness of the RL agent in decision-making for user authorization, maximizing cumulative rewards while minimizing false positive and false negative rates.

Both studies emphasize the importance of ABAC/RBAC in managing access to resources within the smart grid ecosystem. This is crucial for ensuring that only authorized users can access specific data and perform certain actions, enhancing security and compliance. For example, an attacker with unauthorized access could interfere with grid-support operations, such as voltage regulation and frequency control, which are critical for maintaining grid stability. This could result in widespread disruptions and compromise the reliability of the smart grid.

Other works related to this aspect include [107] and [109].

G. Other Security Solutions

It is possible to find in the literature several proposals of potential solutions to enhance security and to fill existing gaps on IEEE 2030.5. Those include technologies or solutions for physical security — as a way of reducing the risk of a device having its private key compromised — as well as alternative trust mechanisms.

1) Trusted Execution Environments: in [35], the authors highlight the role of the Trusted Execution Environment (TEE) as a secure second layer within a primary processor. These measures help to ensure the safe storage and processing of sensitive data in an isolated and safe environment. Acting as a shield, the TEE counters software attacks using the Rich Execution Environment (REE), thereby enhancing security. The TEE controls access to memory and hardware areas using hardware-supported safeguards and a unique software layer. This structure improve the secure execution of authenticated applications, help avoiding against threats external to the TEE.

In contexts demanding stronger security, such as systems handling sensitive data or financial transactions, the TEE provides an additional layer of trust and protection. Its incorporation upholds data integrity, preserves confidentiality, and guarantees the execution of critical tasks in a tightly-regulated environment.

Among several features of the TEE platform, the following are particularly noteworthy:

- Trusted applications (TAs) either digitally sign or, at a minimum, generate a hash digest for all measurements before transferring them to the REE. This mechanism

deters the REE from tampering with or producing inauthentic measurements.
- The system possesses the capability to transmit authenticated measurements using industry-standard protocols, such as IEEE 2030.5.

2) OTrP: the Open Trust Protocol (OTrP) is a security protocol designed to bolster the trustworthiness of TEEs. When considering the IEEE 2030.5 standard, the OTrP emerges as a potential solution to bridge security gaps, ensure data integrity and protect operations within the grid's communication systems.

In [35], the authors propose a solution leveraging the OTrP [117]. This protocol utilizes preallocated certificates within TEE environments, allowing for trusted key and certificate chain revocation status. Notably, it achieves this without the need for its own external OCSP service call. Additionally, OTrP facilitates certificate renewal and offers other essential features, as detailed below:

a) TA protection: A Trusted Application will be delivered in an encrypted form. This encryption is an additional layer within the message encryption and the TA binary is encrypted for each target device with the device's TEE Service Provider Attestation Identity Key.

b) Compromised CAs: If the root CA for the TAM (Trusted Application Manager) certificates is compromised, there is an expectation that device OEMs (Original Equipment Manufacturers) should have a mechanism to update the trust anchor. Any compromise at the intermediate CA level can be addressed by OCSP validation checks within the protocol itself. A TEE must validate certificate revocation pertaining to a TAM certificate chain, ensuring that any compromised certificates are properly recognized and handled. If the root CA of TEE device certificates is compromised, the affected devices might be rejected by a TAM. This decision rests with the TAM's implementation and specific policy. TFW (Trusted Firmware) and TEE (Trusted Execution Environment) device certificates are typically designed to last longer than the actual lifetime of a device. Conversely, a TAM certificate generally has a moderate lifetime, ranging from 2 to 5 years, necessitating renewal or rekeying.

3) Other Trust Alternatives: Aside from the TEE proposed in [35], Trusted Computing (TC) solutions that have been developed for small devices offering potential frameworks that can be leveraged for trust management in smart inverters. The prevailing TC architectures that hold promise for this application include Secure Elements, TPMs, Mobile Trusted Module (MTM) Standard [118], Blockchain PKI [31] and ARM TrustZone [119]. These technologies indicate a pathway toward strengthening trust and security within DER systems and beyond.

Encouragingly, recent research in penetration testing by EPRI (Electric Power Research Institute), utilizing a reference architecture from Cable Labs, has demonstrated potential advancements in resistance to DER (Distributed Energy Resources) key extraction. These discoveries provide hope for bolstering the security measures and trustworthiness of current systems [120].

VIII. Conclusion

In this paper, we provided a tutorial-style introduction to the IEEE 2030.5-2018 standard and an overview of its related scientific literature. Our presentation of the standard covered its main application scenarios, the possible architectures it supports, its communication protocols and data models. In particular, we covered the main technical aspects of the standard, including:

- Communication scenarios and topologies supported by the standard (Standalone HAN, Integrated HAN, Mixed Topologies, etc);
- The application-layer protocols used by the IEEE 2030.5: its usage of RESTful interfaces over HTTPS, including details on the main endpoints and their semantics;
- The concept of Function Sets and a list of the function sets defined by the standard (as well as their semantics);
- How the standard uses XML Schema Definitions (XSD) and Web Application Description Language (WADL) to provide dynamic definitions of the resources available on the network devices;
- How the standard leverages DNS-SD and mDNS to allow the dynamic discovery of devices and their services;
- Details on the usage of TLS 1.2 by the standard; and
- Details on the Public-Key Infrastructure (PKI) used by the standard, including particularities on how it handles certificates.

Our main emphasis was on the security aspects of the standard: we discussed how the IEEE 2030.5-2018 secures its communications by means of TLS and HTTPS, as well as the specificities of how the standard handles digital certificates among its devices. Our analysis of this last aspect, in particular, revealed a notable security flaw related to certificate management within the Manufacturing PKI.

This vulnerability is associated with the standard's reliance on non-revocable and non-expiring certificates, compounded by its explicit prohibition against using CRL or OCSP, posing significant security threats. We showed how a real attack can target this vulnerability and its potential effects. In response, we suggested potential remedies and new methods, including the adoption of cutting-edge cryptographic techniques and secure communication protocols, to address these vulnerabilities.

We hope this overview of the standard — and, particularly, of its possible security gaps — may foster research on improved security solutions for IEEE 2030.5. We envision possible solutions may explore either architectural aspects of the standard — *i.e.*, propose alternative network architectures that allow the communication between devices and CA servers (even if indirectly) — or alternative certification approaches, such as those presented in Section VII-G.

Future research directions should include the exploration of blockchain technology for heightened security and decentralization [55], the investigation into quantum-resistant cryptographic methods to counteract the threat of quantum computing [61], and the development of improved certificate management and device authentication mechanisms. The integration of machine learning for anomaly detection [49] and the employment of advanced hardware security modules present

promising strategies to safeguard against emergent cyber risks. These avenues not only aim to bolster the security of the IEEE 2030.5 standard against sophisticated threats but also ensure its resilience and adaptability amidst the fast-evolving smart grid technology landscape.

REFERENCES

[1] T. Adefarati and R. Bansal, "Chapter 2 - Energizing Renewable Energy Systems and Distribution Generation," in *Pathways to a Smarter Power System*, A. Taşcıkaraoğlu and O. Erdinç, Eds. Academic Press, 2019, pp. 29–65.

[2] Associação Brasileira de Energia Solar Fotovoltaica (ABSOLAR). (2024) Energia solar cresce no brasil em 2024. Accessed: 2024-08-23. [Online]. Available: https://www.absolar.org.br/noticia/energia-solar-cresce-no-brasil-em-2024-e-ultrapassa-39-gw-afirma-absolar/

[3] Australian PV Institute, "Solar PV data analysis," https://pv-map.apvi.org.au/analyses, Australian PV Institute, 2023, accessed: 2023-03-31.

[4] A. Richter, E. van der Laan, W. Ketter, and K. Valogianni, "Transitioning from the traditional to the smart grid: Lessons learned from closed-loop supply chains," *International Conference on Smart Grid Technology, Economics and Policies (SG-TEP)*, pp. 1–7, 2012.

[5] R. Neal, "How hackers could target virtual power plants," 2024, accessed: 2024-08-19. [Online]. Available: https://rya.nc/vpp-hack.html

[6] California Energy Commission, "Rule 21 Smart Inverter Working Group," https://www.cpuc.ca.gov/Rule21/, accessed: 2023-08-24.

[7] P. S. Sarker, V. Venkataramanan, D. S. Cardenas, A. Srivastava, A. Hahn, and B. Miller, "Cyber-Physical Security and Resiliency Analysis Testbed for Critical Microgrids with IEEE 2030.5," *Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, pp. 1–6, 2020.

[8] California Public Utilities Commission, "Smart Inverter Working Group," 2020.

[9] A. Vosughi, A. Tamimi, A. B. King, S. Majumder, and A. K. Srivastava, "Cyber–physical vulnerability and resiliency analysis for DER integration: A review, challenges and research needs," *Renewable and Sustainable Energy Reviews*, vol. 168, p. 112794, 2022.

[10] Common Smart Inverter Profile Working Group, "Common Smart Inverter Profile: IEEE 2030.5 Implementation Guide for Smart Inverters," https://sunspec.org/wp-content/uploads/2018/03/CSIPImplementationGuidev2.003-02-2018-1.pdf, 2018.

[11] "IEEE guide for smart grid interoperability of energy technology and information technology operation with the electric power system (eps), end-use applications, and loads," *IEEE Std 2030-2011*, pp. 1–126, 2011.

[12] I. Stefani, V. Stokic, S. Dzaleta, and B. Brbaklic, "Cyber-physical security and resiliency analysis testbed for critical microgrids with IEEE 2030.5," in *Proceedings of the 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, MSCPES 2020*. IEEE, 2020, pp. 1–6.

[13] R. Simpson, "IEEE 2030.5-2013 (Smart Energy Profile 2.0) - An Overview for KSGA," Online presentation, available at https://www.robbysimpson.com/prezzos/IEEE_2030_5_Seoul_Simpson_20150424.pdf, 2015, accessed: August 28, 2024.

[14] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[15] V. Kounev and D. Tipper, "Advanced Metering and Demand Response communication performance in Zigbee based HANs," *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 31–36, 2013.

[16] M. Ghalib, A. Ahmed, I. Al-Shiab, Z. Bouida, and M. Ibnkahla, "Implementation of a Smart Grid Communication System Compliant with IEEE 2030.5," *IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, 2018.

[17] E. L. C. Macedo, E. A. R. de Oliveira, F. H. Silva, R. R. Mello, F. M. G. França, F. C. Delicato, J. F. de Rezende, and L. F. M. de Moraes, "On the security aspects of internet of things: A systematic literature review," *Journal of Communications and Networks*, vol. 21, no. 5, pp. 444–457, 2019.

[18] IEEE, "IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard (Draft)," *IEEE P2030.5/D1, June 2013*, pp. 1–348, 2013.

[19] IEEE, "IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard," *IEEE Std 2030.5-2013*, pp. 1–348, 2013.

[20] D. Pala and G. Proserpio, "Model-driven development of a standard-compliant Customer Energy Manager," *International Symposium on Smart Electric Distribution Systems and Technologies (EDST)*, pp. 324–328, 2015.

[21] S. T. Bushby and D. G. Holmberg, "Standardization of Smart Grid Customer Interfaces," *Distribution and Utilization*, vol. 32, 2015.

[22] A. Nagarajan, B. Palmintier, and M. Baggu, "Advanced inverter functions and communication protocols for distribution management," *IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, pp. 1–5, 2016.

[23] D. J. Sebastian and A. Hahn, "Exploring emerging cybersecurity risks from network-connected DER devices," *North American Power Symposium (NAPS)*, pp. 1–6, 2017.

[24] C. Lai, N. Jacobs, S. Hossain-McKenzie, C. Carter, P. Cordeiro, I. Onunkwo, and J. Johnson, "Cyber security primer for DER vendors, aggregators, and grid operators," Sandia National Laboratories, Tech. Rep., 2017.

[25] IEEE, "IEEE Draft Standard for Smart Energy Profile Application Protocol," *IEEE P2030.5/D1, September 2017*, pp. 1–342, 2017.

[26] Y. Lu, Y. Ding, Q. Duan, X. Li, and Y. Tian, "Upper-Middleware Development of Smart Energy Profile 2.0 for Demand-Side Communications in Smart Grid," *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, pp. 306–310, 2018.

[27] J. Baker, P. G. Cordeiro, T. Doepke, S. Hossain-McKenzie, C. M. Howerter, N. Jacobs, D. Jose, C. F. Lai, and J. Zhao, "General Requirements for Designing and Implementing a Cryptography Module for Distributed Energy Resource (DER) Systems," Sandia National Laboratories, Tech. Rep., 2018.

[28] IEEE, "IEEE Approved Draft Standard for Smart Energy Profile Application Protocol," *IEEE P2030.5/D2, March 2018*, pp. 1–358, 2018.

[29] "IEEE standard for smart energy profile application protocol," *IEEE Std 2030.5-2018 (Revision of IEEE Std 2030.5-2013)*, pp. 1–361, 2018.

[30] B. Li, B. Jia, W. Cao, S. Tian, B. Qi, Y. Sun, W. Zhu, and A. Zheng, "Application Prospect of Edge Computing in Power Demand Response Business," *Dianwang Jishu/Power System Technology*, vol. 42, no. 1, pp. 79–87, 2018.

[31] J. Obert, P. Cordeiro, J. Johnson, G. Lum, T. Tansy, M. Pala, and R. Ih, "Recommendations for trust and encryption in DER interoperability standards," Sandia National Laboratories, Tech. Rep., 2019.

[32] O. T. Soyoye and K. C. Stefferud, "Cybersecurity Risk Assessment for California's Smart Inverter Functions," *IEEE CyberPELS (CyberPELS)*, pp. 1–5, 2019.

[33] F. Seitenfus, C. Barriquello, L. Neves Canha, A. Pedretti, T. Silva Santana, and Z. Nadal, "Simulation and analysis of OpenADR agents using VOLTTRON platform," *IEEE PES Conference on Innovative Smart Grid Technologies, ISGT Latin America 2019*, pp. 1–6, 2019.

[34] J. van Kerkhoven, N. Charlebois, A. Robertson, B. Gibson, A. Ahmed, Z. Bouida, and M. Ibnkahla, "IPv6-Based Smart Grid Communication over 6LoWPAN," *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, 2019.

[35] D. J. Sebastian, U. Agrawal, A. Tamimi, and A. Hahn, "DER-TEE: Secure distributed energy resource operations through trusted execution environments," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6476–6486, 2019.

[36] A. K. Jain, A. Nagarajan, I. Chernyakhovskiy, T. Bowen, B. Mather, and J. Cochran, "Evolution of Distributed Energy Resource Grid Interconnection Standards for Integrating Emerging Storage Technologies," *North American Power Symposium (NAPS)*, pp. 1–6, 2019.

[37] C. Sun, R. Zhu, and C. Liu, "Cyber Attack and Defense for Smart Inverters in a Distribution System," *CIGRE Study Committee D2 Colloquium, Helsinki, Finland*, 2019.

[38] R. S. de Carvalho and D. Saleem, "Recommended Functionalities for Improving Cybersecurity of Distributed Energy Resources," *Resilience Week (RWS)*, vol. 1, pp. 226–231, 2019.

[39] J. T. Johnson, "PV Cybersecurity Final Report." Sandia National Laboratories, Tech. Rep., 2019.

[40] S. K. Goudos, P. Sarigiannidis, P. I. Dallas, and S. Kyriazakos, "Communication protocols for the IoT-based smart grid," in *IoT for Smart Grids*. Springer, 2019, pp. 55–83.

[41] J. Mater, S. Kang, and R. Simpson, "Iec 61850 and IEEE 2030.5: A comparison of 2 key standards for DER integration: An update," Quality Logic, Tech. Rep., 2019.

[42] A. M. dos Santos Alonso, L. Carlos Afonso, D. I. Brandao, E. Tedeschi, and F. P. Marafão, "Considerations on Communication Infrastructures for Cooperative Operation of Smart Inverters," *IEEE 15th Brazilian*

Power Electronics Conference and 5th IEEE Southern Power Electronics Conference (COBEP/SPEC), pp. 1–6, 2019.

[43] J. Fattahi, M. Samadi, M. Erol-Kantarci, and H. Schriemer, "Transactive Demand Response Operation at the Grid Edge using the IEEE 2030.5 Standard," *Engineering*, vol. 6, no. 7, pp. 801–811, 2020.

[44] J. Johnson, I. Onunkwo, P. Cordeiro, B. Wright, N. Jacobs, and C. Lai, "Assessing DER network cybersecurity defences in a power-communication co-simulation environment," *IET Cyber-Physical Systems: Theory and Applications*, vol. 5, no. 3, pp. 274–282, 2020.

[45] J. P. Ogle, M. Touhiduzzaman, Q. H. Nguyen, and P. Thekkumparambath Mana, "CReST-VCT System Integration Framework," Pacific Northwest National Lab.(PNNL), Tech. Rep., 2020.

[46] M. Obi, T. Slay, and R. Bass, "Distributed energy resource aggregation using customer-owned equipment: A review of literature and standards," *Energy Reports*, vol. 6, pp. 2358–2369, 2020.

[47] P. K. Gautam, R. G. Cinar, and C. R. Clarke, "Testbed demonstration for distribution grid controls with high DER integration," in *2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, 2020, pp. 1–5.

[48] J. Johnson, B. Fox, K. Kaur, and J. Anandan, "Evaluation of interoperable distributed energy resources to IEEE 1547.1 using sunspec modbus, IEEE 1815, and IEEE 2030.5," *IEEE Access*, vol. 9, pp. 142 129–142 146, 2021.

[49] A. Singh, "Distributed intrusion detection system for modbus protocol," Master's thesis, Iowa State University, 2020.

[50] S. Ishikawa, "Integrating system to edge-of-network architecture and management for shines (seams) technologies of high penetration grids," Hawaiian Electric Company, Inc., Tech. Rep., 2020.

[51] J. Kim, K. Park, B. Ahn, J. Chor, Y. Noh, D. Won, and T. Kim, "Real-time hardware-in-the-loop distributed energy resources system testbed using ieee 2030.5 standard," in *2021 IEEE PES Innovative Smart Grid Technologies - Asia (ISGT Asia)*, 2021, pp. 1–5.

[52] T. Slay and R. B. Bass, "An energy service interface for distributed energy resources," in *2021 IEEE Conference on Technologies for Sustainability (SusTech)*, 2021, pp. 1–8.

[53] M. Ansari, L. H. Dahaj, and M. Ansari, "A practical three-layer energy management framework for future distribution systems," in *2021 North American Power Symposium (NAPS)*, 2021, pp. 01–06.

[54] P. Sharma, A. Riepnieks, A. Reiman, A. Singh, R. Melton, J. Ogle, and C. Allwardt, "Model-based interface design for smart field-device integration," in *2022 IEEE Rural Electric Power Conference (REPC)*, 2022, pp. 31–37.

[55] M. A. Alsaid, "A privacy-preserving strategy for the trust layer of the energy grid of things distributed energy resource management system," Master's thesis, Portland State University, 2022.

[56] C. Nguyen, "Interoperability profile for electric vehicle fleet managed charging," *National Institute of Standards and Technology (NIST)*, 2022.

[57] T. Slay, J. M. Acken, and R. B. Bass, "Incentivizing distributed energy resource participation in grid services," in *2022 IEEE Conference on Technologies for Sustainability (SusTech)*. IEEE, 2022, pp. 86–91.

[58] C. E. Piggott, Z. Caruso, and N. G. Nenadic, "Low-cost communication interface between a smart meter and a smart inverter," *Energies*, vol. 16, no. 5, p. 2358, 2023.

[59] QualityLogic, "IEEE 2030.5 test tools," https://www.qualitylogic.com/industries/smart-energy/smart-energy-test-tool-solutions/ieee-2030-5-test-tools/, 2023, accessed: 2023-10-02.

[60] VOLTTRON Development Team, "Volttron IEEE 2030.5 agent," https://volttron.readthedocs.io/en/releases-7.x/index.html#, 2023, accessed: 2023-10-02.

[61] K. Nakka, S. Ahmad, T. Kim, L. Atkinson, and H. M. Ammari, "Post-quantum cryptography (pqc)-grade IEEE 2030.5 for quantum secure distributed energy resources networks," in *2024 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2024, pp. 1–5.

[62] IEEE, "IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces," *IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003)*, pp. 1–138, 2018.

[63] Zhen Zhao, K. Agbossou, and A. Cardenas, "Connectivity for Home Energy Management applications," *IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, pp. 2175–2180, 2016.

[64] R. T. Fielding and R. N. Taylor, "Principled design of the modern Web architecture," *Proceedings of the 2000 International Conference on Software Engineering. ICSE 2000 the New Millennium*, pp. 407–416, 2000.

[65] R. Jacobsen and S. Mikkelsen, "Infrastructure for Intelligent Automation Services in the Smart Grid," *Wireless Personal Communications*, vol. 76, pp. 125–147, 2014.

[66] T. Berners-Lee, R. T. Fielding, and L. M. Masinter, "Uniform Resource Identifier (URI): Generic Syntax," RFC 3986, Jan. 2005. [Online]. Available: https://rfc-editor.org/rfc/rfc3986.txt

[67] S. Cheshire and M. Krochmal, "DNS-Based Service Discovery," RFC 6763, 2013.

[68] Stuart Cheshire and Marc Krochmal, "Multicast DNS," RFC 6762, RFC Editor, RFC 6762, 2013, available from: https://www.rfc-editor.org/rfc/rfc6762.txt.

[69] M. Z. Gunduz and R. Das, "Analysis of cyber-attacks on smart grid applications," in *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*, 2018, pp. 1–5.

[70] M. M. Hossain and C. Peng, "Cyber–physical security for on-going smart grid initiatives: a survey," *IET Cyber-Physical Systems: Theory Applications*, vol. 5, no. 3, pp. 233–244, 2020.

[71] E. Rescorla, "HTTP Over TLS," RFC 2818, May 2000.

[72] E. Rescorla and T. Dierks, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246, Aug. 2008.

[73] T. Hansen and D. E. E. 3rd, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)," RFC 6234, May 2011. [Online]. Available: https://rfc-editor.org/rfc/rfc6234.txt

[74] J. D. Ardigo, "Modelo de Infra-estrutura de Chaves Públicas como Organização Virtual para Processos de Avaliação Somativa à Distância ," Ph.D. dissertation, Universidade Federal de Santa Catarina, 2004.

[75] M. Myers and H. Tschofenig, "Online Certificate Status Protocol (OCSP) Extensions to IKEv2," RFC 4806, Feb. 2007. [Online]. Available: https://rfc-editor.org/rfc/rfc4806.txt

[76] S. Boeyen, S. Santesson, T. Polk, R. Housley, S. Farrell, and D. Cooper, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 5280, May 2008.

[77] E. Sohl, C. Fielding, T. Hanlon, J. Rrushi, H. Farhangi, C. Howey, K. Carmichael, and J. Dabell, "A field study of digital forensics of intrusions in the electrical power grid," in *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*, 2015, pp. 113–122.

[78] Eletric Power Reearch Institute, "IEEE-2030.5-Client," https://www.epri.com/research/products/000000003002014087.

[79] J. Johnson, "IEEE-2030.5-client," https://github.com/catch-twenty-two/ieee-2030.5-client.

[80] C. Hohnstadt, "X - Certificate and Key Management," https://hohnstaedt.de/xca/index.php, 2021.

[81] A. Ronacher, "Flask," https://flask.palletsprojects.com/en/1.1.x/.

[82] S. Sanfilippo, "Hping," http://www.hping.org/.

[83] W. Eddy, "TCP SYN Flooding Attacks and Common Mitigations," RFC 4987, Aug. 2007. [Online]. Available: https://rfc-editor.org/rfc/rfc4987.txt

[84] P. Jafary, "Cyber-security solutions for ensuring smart grid distribution automation functions," Master's thesis, Tampere University of Technology, 2018.

[85] L. Goubin, P. Paillier, M. Rivain, and J. Wang, "How to reveal the secrets of an obscure white-box implementation," *Journal of Cryptographic Engineering*, vol. 10, pp. 49–66, 2020.

[86] N. I. of Standards and T. (NIST), "Guidelines for smart grid cyber security," U.S. Department of Commerce, Tech. Rep., 2014, accessed: February 15, 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2014/nist.ir.7628r1.pdf

[87] S. K. Venkatachary, J. Prasad, R. Samikannu, A. Alagappan, and L. J. B. Andrews, "Cybersecurity infrastructure challenges in iot based virtual power plants," *Journal of Statistics and Management Systems*, vol. 23, no. 2, pp. 263–276, 2020.

[88] E. Koza and A. Öztürk, "A literature review to analyze the state of the art of virtual power plants in context of information security," *Environmental Informatics*, pp. 49–69, 2021.

[89] S. N. G. Gourisetti, D. J. Sebastian-Cardenas, B. Bhattarai, P. Wang, S. Widergren, M. Borkum, and A. Randall, "Blockchain smart contract reference framework and program logic architecture for transactive energy systems," *Applied Energy*, vol. 304, p. 117860, 2021.

[90] I. Onunkwo, "Recommendations for data-in-transit requirements for securing DER communications." Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2020.

[91] J. T. Johnson, "Design and evaluation of a secure virtual power plant." Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2017.

[92] J. Chen, J. Yan, H. Du, M. Debbabi, and M. Kassouf, "Vulnerability analysis of virtual power plant voltage support under denial-of-service attacks," in *2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2023, pp. 1–5.
[93] K. Shahid, E. Kidmose, R. L. Olsen, L. Petersen, and F. Iov, "On the impact of cyberattacks on voltage control coordination by regen plants in smart grids," in *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2017, pp. 480–485.
[94] A. P. Kuruvila, I. Zografopoulos, K. Basu, and C. Konstantinou, "Hardware-assisted detection of firmware attacks in inverter-based cyberphysical microgrids," *International Journal of Electrical Power & Energy Systems*, vol. 132, p. 107150, 2021.
[95] D. J. S. Cardenas, *Cyber risk analysis and threat mitigation strategies against Distributed Energy Resources and Internet of Things infrastructure attacks*. Washington State University, 2021.
[96] C. Lai, A. R. Chavez, C. B. Jones, N. Jacobs, S. Hossain-McKenzie, J. B. Johnson, and A. Summers, "Review of intrusion detection methods and tools for distributed energy resources," Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2021.
[97] K. Yan, X. Liu, Y. Lu, and F. Qin, "A cyber-physical power system risk assessment model against cyberattacks," *IEEE Systems Journal*, 2022.
[98] J. Johnson, J. R. Hoaglund, R. D. Trevizan, T. A. Nguyen *et al.*, "Physical security and cybersecurity of energy storage systems," *US DOE Energy Storage Handbook; Sandia National Laboratories: Albuquerque, NM, USA*, 2020.
[99] P. S. Sarker, V. Venkataramanan, D. S. Cardenas, A. Srivastava, A. Hahn, and B. Miller, "Cyber-physical security and resiliency analysis testbed for critical microgrids with IEEE 2030.5," *8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, MSCPES 2020 - Proceedings*, no. October 2022, pp. 1–6, 2020.
[100] R. S. Ravi, A. Jolfaei, D. Tripathy, and M. Ali, "Secured energy ecosystems under Distributed Energy Resources penetration," *Internet of Things and Cyber-Physical Systems*, vol. 2, no. November, pp. 194–202, 2022. [Online]. Available: https://doi.org/10.1016/j.iotcps.2022.10.002
[101] G. Fragkos, J. Johnson, and E. E. Tsiropoulou, "Centralized and decentralized distributed energy resource access control implementation considerations," *Energies*, vol. 15, no. 17, p. 6375, 2022.
[102] C. Carter, I. Onunkwo, P. Cordeiro, and J. Johnson, "Cyber Security Assessment of Distributed Energy Resources," *Photovoltaic Specialist Conference (PVSC)*, pp. 2135–2140, 2017.
[103] X. Liang, N. An, D. Li, Q. Zhang, and R. Wang, "A blockchain and abac based data access control scheme in smart grid," in *2022 International Conference on Blockchain Technology and Information Security (ICBCTIS)*. IEEE, 2022, pp. 52–55.
[104] S. Mahmood, M. Gohar, J.-G. Choi, S.-J. Koh, H. Alquhayz, and M. Khan, "Digital certificate verification scheme for smart grid using fog computing (fonica)," *Sustainability*, vol. 13, no. 5, p. 2549, 2021.
[105] D. Sebastian-Cardenas, S. Gourisetti, M. Mylrea, A. Moralez, G. Day, V. Tatireddy, C. Allwardt, R. Singh, R. Bishop, K. Kaur *et al.*, "Digital data provenance for the power grid based on a keyless infrastructure security solution," in *2021 Resilience Week (RWS)*. IEEE, 2021, pp. 1–10.
[106] G. Fragkos, J. Johnson, and E. E. Tsiropoulou, "Dynamic role-based access control policy for smart grid applications: an offline deep reinforcement learning approach," *IEEE Transactions on Human-Machine Systems*, vol. 52, no. 4, pp. 761–773, 2022.
[107] Y. Dafalla, B. Liu, D. A. Hahn, H. Wu, R. Ahmadi, and A. G. Bardas, "Prosumer nanogrids: A cybersecurity assessment," *IEEE Access*, vol. 8, pp. 131 150–131 164, 2020.
[108] S. Zhang, J. Rong, and B. Wang, "A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain," *International Journal of Electrical Power & Energy Systems*, vol. 121, p. 106140, 2020.
[109] S. Lakshminarayana, J. Ospina, and C. Konstantinou, "Load-altering attacks against power grids under covid-19 low-inertia conditions," *IEEE Open Access Journal of Power and Energy*, vol. 9, pp. 226–240, 2022.
[110] Y. Ye, L. Zhang, W. You, and Y. Mu, "Secure decentralized access control policy for data sharing in smart grid," in *IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2021, pp. 1–6.
[111] J. Johnson, "DER security considerations to enable grid services." Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2022.
[112] K. Leswing, "A massive cyberattack knocked out major websites across the internet," *Business Insider*, vol. 21, 2016.
[113] S. Zhang, Y. Zhao, and B. Wang, "Certificateless ring signcryption scheme for preserving user privacy in smart grid," *Autom Electr Power Syst*, vol. 42, no. 3, pp. 118–123, 2018.
[114] Y. Liu, W. Guo, C.-I. Fan, L. Chang, and C. Cheng, "A practical privacy-preserving data aggregation (3pda) scheme for smart grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1767–1774, 2018.
[115] R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar, and J. J. Rodrigues, "SDN-enabled multi-attribute-based secure communication for smart grid in iiot environment," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2629–2640, 2018.
[116] J. E. Rubio, C. Alcaraz, and J. Lopez, "Recommender system for privacy-preserving solutions in smart metering," *Pervasive and Mobile Computing*, vol. 41, pp. 205–218, 2017.
[117] M. Pei, N. Cook, M. Yoo, A. Atyeo, and H. Tschofenig, "The open trust protocol (otrp)," IETF, Internet-Draft, 2016.
[118] Trusted Computing Group, "TCG mobile trusted module 2.0 use cases version 1.0," 2010, accessed: 2024-08-23. [Online]. Available: https://trustedcomputinggroup.org/wp-content/uploads/TCG-Mobile-Trusted-Module-2-0-Use-Cases-v1-0.pdf
[119] ARM Limited, "Arm security technology: Building a secure system using trustzone technology," ARM Limited, Tech. Rep., April 2009, PRD29-GENC-009492C – Accessed on 2024-03-31. [Online]. Available: https://documentation-service.arm.com/static/5f212796500e883ab8e74531?token
[120] J. Obert, P. Cordeiro, J. T. Johnson, G. Lum, T. Tansy, N. Pala, and R. Ih, "Recommendations for trust and encryption in DER interoperability standards," Sandia National Lab.(SNL-NM), Albuquerque, NM (United States); Kitu Systems, Tech. Rep., 2019.

Diego Passos received his B.Sc., M.Sc. and D.Sc. degrees in Computer Science from Universidade Federal Fluminense (UFF), Rio de Janeiro, Brazil in 2007, 2009 and 2013, respectively. From 2013 to 2014, he worked as a postdoctoral fellow researcher at the same university. He is currently a professor at Instituto Superior de Engenharia de Lisboa (ISEL), Portugal. His research interests include multihop wireless networks, network coding, and wireless routing.

Cledson de Sousa earned his D.Sc. in Computing from Universidade Federal Fluminense (UFF), Brazil, in 2019, following his B.Sc. and M.Sc. degrees in Telecommunications Engineering from UFF in 1997 and 2013, respectively. With over 30 years of experience in the telecommunications industry, he has served as an associate professor in the Telecommunications Engineering Department at UFF since 2021. His research interests focus on wireless sensor networks and Channel State Information (CSI).

Rafael Caveari Gomes received the bachelor's degree in telecommunications engineering from Universidade Federal Fluminense (UFF), Brazil, in 2014, where he is currently pursuing the M.Sc. degree in computer science. He is presently a Lieutenant of the Brazilian Navy. His research interests include network security and smart grid communications.

Danilo Fernandes de Assis received his bachelor's degree in computer engineering from Universidade Federal de Itajubá (UNIFEI), Brazil, in 2009, and Master's degree in computer science from Universidade Federal Fluminense (UFF), Brazil, in 2021. His research interests include network security and smart grid communications.

Fernanda Gonçalves de Oliveira Passos is currently a professor at Instituto Superior de Engenharia de Lisboa (ISEL), Portugal. She is also a researcher in COPELABS of the Universidade Lusófona in Lisboa, Portugal, and also collaborates with the Smart Grid Computing Laboratory and MídiaCom Laboratory of the Universidade Federal Fluminense (UFF), in Brazil. She holds a Bachelor's Degree in Computer Science (2008), a Master's Degree in Computer Science (2010) and a D.Sc. in Computer Science (2014), all from UFF. Her research interests include parallel and distributed computing, autonomic computing, grid/cloud/-fog/edge computing, Internet of things, and smart cities.

Célio Albuquerque received the B.S. and M.S. degrees in electrical and electronics engineering from Universidade Federal do Rio de Janeiro, Brazil, in 1993 and 1995, and the M.S. and Ph.D. degrees in information and computer science from the University of California at Irvine in 1997 and 2000, respectively. From 2000 to 2003, he served as the networking architect for Magis Networks, designing high-speed wireless medium access control. He is currently a full professor at the Computer Science Department of Universidade Federal Fluminense, Brazil. His research interests include wireless networks, network security, Smart Grid communications, Internet architectures and protocols, multicast and multimedia services.