World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:18, No:4, 2024

A Proposal for a Secure and Interoperable Data Framework for Energy Digitalization

Hebberly Ahatlan

***Abstract*—**The process of digitizing energy systems involves transforming traditional energy infrastructure into interconnected, data-driven systems that enhance efficiency, sustainability, and responsiveness. As smart grids become increasingly integral to the efficient distribution and management of electricity from both fossil and renewable energy sources, the energy industry faces strategic challenges associated with digitalization and interoperability — particularly in the context of modern energy business models, such as virtual power plants (VPPs). The critical challenge in modern smart grids is to seamlessly integrate diverse technologies and systems, including virtualization, grid computing and service-oriented architecture (SOA), across the entire energy ecosystem. Achieving this requires addressing issues like semantic interoperability, Information Technology (IT) and Operational Technology (OT) convergence, and digital asset scalability, all while ensuring security and risk management. This paper proposes a four-layer digitalization framework to tackle these challenges, encompassing persistent data protection, trusted key management, secure messaging, and authentication of IoT resources. Data assets generated through this framework enable AI systems to derive insights for improving smart grid operations, security, and revenue generation. Furthermore, this paper also proposes a Trusted Energy Interoperability Alliance as a universal guiding standard in the development of this digitalization framework to support more dynamic and interoperable energy markets.

***Keywords*—**Digitalization, IT/OT convergence, semantic interoperability, TEIA alliance, VPP.

I. Introduction

DIGITALIZING energy systems to improve smart grids goes beyond monitoring hardware infrastructure via the internet and collecting telemetry to establish operational trends. The digitalization process involves the transformation of traditional energy infrastructure into interconnected, data-driven, and technology-enabled systems [1]. Energy infrastructure digitalization aims to make energy generation, distribution, and consumption more efficient, sustainable, and responsive to changing demands.

Digitalization is a complex task with evolving attributes and demands. It requires methodical solutions to enable the energy industry to scale efficiently and interoperate across the complete smart grid. Data collection, transmission, and analytics are foundational elements of the digitalization process, but their value is not fully realized without a secure, interoperable layer permeating the entire energy infrastructure.

The key digitalization challenge for smart grids today is the smooth integration of diverse technologies and systems, including virtualization, grid computing, and SOA, across the energy ecosystem. In addition, a digitized energy framework needs to tackle semantic interoperability [2] where different systems may interpret data differently, making it crucial to establish common data models and ontologies for the consistent understanding and exchange of information [3].

Furthermore, digitalization needs to solve the challenge of scaling interoperable data fabrics — as smart grids expand and incorporate more renewable energy sources and distributed energy resources, the systems must be capable of accommodating growth without sacrificing performance or security. Finally, digitalization efforts must include regulatory and governance harmonization across regions and nations to invigorate international smart grid interoperability [4].

Solving these challenges means that data assets need to be secure, verified, and independent of multidimensional IoT device and data incompatibility. Rich data that are fully protected enable AI systems to derive dependable valuable business insights to improve the operation, security, revenue generation, and scalability of smart grids.

Smart grids, and the innovative business entities that support them, such as VPPs, are expected to propel data-driven energy economies; but in parallel, smart grids must be secure and interoperable to support AI systems and panoramic infrastructure monitoring [5]. Complex networks of devices, sensors, control systems, and data sources require a clear digitalization and interoperability standard to guide the design of infrastructure across the smart grid.

To ensure the efficient digitalization, security and interoperability of smart grids, a secure, interoperable digitalization model is proposed to address diverse energy entities, objectives, and potential threats. This model can serve as an energy digitalization standard for secure communication, interoperability, and risk management in a highly interconnected and dynamic energy system.

II. Secure and Interoperable Digital Energy Orchestration Framework

The digitalization framework aims to facilitate secure communication and collaboration. It will enable flexibility and innovation within energy systems, supporting various protocols, legacy devices, and data governance approaches. The digitalization model is organized into four layers to address the various challenges posed by the complex and interconnected nature of smart grid systems.

Hebberly Ahatlan is with Intertrust Technologies, Milpitas California 95035 USA (phone: 408-616-1600; fax: 408-616-1626; e-mail: Heb@intertrust.com).

TABLE I
ELEMENTS OF ENERGY DIGITALIZATION

Layer	Digitalization Elements
3	Robustness, renewal, compliance, interoperability
2	Trusted key management, authentication, governance, attestation
1	Security for signaling framework
0	Protected resources in the ecosystem

A. Layer 0: Energy Systems and Zero Trust

Zero trust principles are applied to assume no inherent security within the network. Resources in an energy system are identified and classified, including data, controls, and devices [6]. Entities' interactions with these resources are accounted for, forming a zero-trust approach.

This layer focuses on identifying and protecting resources within the ecosystem. Furthermore, it outlines frameworks for digital commands, action requests, and the responses from IoT devices with provenance that is verifiable in real time. In addition, zero trust architectures accommodate OT, IT, and hybrid IT/OT and deliver flexible schemes to provision privacy, confidentiality, and transparency across the entire IT/OT network.

B. Layer 1: Secure Messaging

Layer 1 focuses on secure messaging, where cryptographic keys play a crucial role in verifying message authenticity and integrity. Secure messaging includes commands, requests, and responses within energy systems. Information for verifying origin, integrity, and authority is captured. Cryptographic keys associated with legitimate originators are used to ensure message integrity. Each entity maintains a list of security associations with unique identifiers and shared keys.

C. Layer 2: Provisioning for Flexibility in Administering Disparate Digital Energy Systems

Layer 2 supports Layer 1 with advanced but flexible cryptographic key management policies and algorithms, making system administration easy and efficient. Furthermore, Layer 2 provisions for data protection from its origin to its destination. It assures that data are protected while in transit or at rest with technologies that not only protect the data tunnel, but also protect the data traversing through the communication channel as well as the nodes or network boundaries where data may change communication protocols.

In other words, it is critical to protect data beyond Transport Layer Security or Virtual Private Network schemes, for example. This allows for full data control and governance by different stakeholders who are responsible for a broad and diverse group of technical and business entities in the ecosystem.

D. Layer 3: Invigorating Provisions and Protections Described at the Lower Layers

Within this layer it is critical to establish measures designed to limit the scope of external interactions with the resources at Level 0, thereby assuring the systemic effectiveness of Layer 1. In addition, it is important to establish renewability within all the layers, so the layers' technical security algorithms can be seamlessly upgraded and adapted to incoming business requirements, technologies, or regulations. Energy systems are a strategic target for innovative cybercrime and need to adapt to fight new threats dynamically and need to comply with new local or national regulations in real time.

At Layer 3, software applications can function to establish common data models and ontologies that enable consistent understanding and transaction of information [7]. In addition, applications can be tuned to solve the challenge of scaling interoperable solutions without sacrificing performance or security.

The consolidated goal of all four layers is to focus on strict and minimal implementations of Layer 1, but allow for fast paced innovative evolution of Layer 0, Layer 2, and Layer 3. This approach is essential for making the entire digitized energy system framework achievable and organic.

III. SPECIFIC ATTRIBUTES FOR SMART GRIDS

Greater security and interoperability within smart grids that incorporate VVPs, EaaS, or other modern energy business models is achieved by focusing on the mechanisms of Layer 1 and Layer 2. Here are the details of the strategic provisions necessary in both layers:

- Persistent data integrity: To ensure the integrity and provenance of data, the digitized interoperability model employs persistent digital signatures using public keys or trusted blockchains. This strengthens cybersecurity measures, guarding against unauthorized data tampering.
- Rich identity: Rich identities involve uniquely identifying entities within the energy system. The digitized interoperability model assigns verifiable attributes to each identity. This is crucial for authenticity, provenance, and authority verification for commands and data, but there is more, these identities provide a comprehensive view of each device including its capabilities. This information empowers automated systems to make informed decisions, optimize device usage, and respond effectively to dynamic energy demands. Additionally, rich device identities support authentication and authorization processes, ensuring that only authorized devices participate in all energy operations.
- Policies: Policies are sets of rules that dictate automated decisions within the system. They can range from simple to complex and can be centralized or decentralized. Policies enable rapid actions while flagging anomalies that require deeper evaluation.
- Trusted assertions: The digitized interoperability framework allows users to validate statements, such as entity ownership, permissions, and control over resources. Assertions can include alternate names, credentials, and group memberships. Trusted assertions ensure that data and commands exchanged between entities are accurate, legitimate, and aligned with established policies.
- Secure messaging: Layer 1 deals with secure messaging, where messages are encapsulated to ensure origin verification, data integrity, and authority verification [8]. Cryptographic keys play a crucial role in this process.
- Security associations: Each entity maintains a list of

security associations that includes unique identifiers and shared keys. Message integrity is assured using these associations. Security associations is intimately connected to rich identities. For example, the identity of modular software platforms or IoT networks needs to be verified before secure associations are made between them. Subsequently, periodic mutual verifications of the authenticity of modules can be made by leveraging the list of security associations with its corresponding identifiers and shared keys.

- Trust layer: Layer 2 defines a trust scheme for how devices are introduced and managed within a smart grid. Devices added to the energy system must use different trust mechanisms, including supervisory entities, PKI-based authentication – such as Intertrust XPN, and keyless signatures with trusted blockchains [9]. The choice between PKI and blockchain approaches can depend on scalability and resistance to future quantum computing attacks.

IV. Layer 3 as the Connecting Lattice for Secure Digitized Energy Data

Layer 3 must be viewed as the superseding lattice that connects the functions of the lower layers and delivers a high grade of adaptability to ensure the smart grid data infrastructure can function efficiently and consistently. Layer 3 is critical for achieving greater security and interoperability within smart grids and larger energy systems. For smart city grids and other broader energy ecosystems, Layer 3 can help establish:

- Compliance and robustness rules (CRRs): CRRs are used to group policies for different types of devices and entities. They help rate the overall security and trustworthiness of an energy entity. CRRs describe required, specific, interoperable rules and actions, as well as optional rules and actions for optional capabilities. The digitalized interoperability framework provisions that all CCR rules and actions are followed consistently and updated regularly, enhancing system resilience and reliability. CRRs enable consistent adherence to security protocols, helping maintain system integrity and facilitating compliance with evolving regulations.
- Device robustness classification: Robustness is categorized based on trust layers, function, scope, and the ability to affect other entities. The precise identification and categorization of devices within the energy ecosystem ensures that each device is appropriately authenticated and authorized for its specific role. All four layers can participate in the device classification process and can cross-check each other. This classification helps assess the security and trustworthiness of devices and entities within the smart grids and energy systems.
- Event and action logging: Monitoring and logging of events and actions within the energy system are essential for security performance evaluation, anomaly detection, and the identification of illicit activities. This aspect is crucial for maintaining system integrity, and it is the key to provide a continuous record of system activities and interactions, enabling real-time monitoring, and security performance assessment.
- Renewability: In a dynamic energy system, where new entities appear and entity attributes change frequently, adaptability is key. Renewability involves upgrading security mechanisms and allowing entities to adopt more secure options without significant disruption. Renewability is of particular importance in the context of SOAs, because SOAs promote data sharing and accessibility, critical for managing and optimizing, for instance, renewable energy generation and distribution. SOAs allow real-time data exchange among renewable assets, grid operators, and energy management systems, facilitating better decision-making, predictive maintenance, and load balancing. Each attribute of SOAs requires flexible and efficient renewability.
- IT/OT convergence: The convergence of IT and OT is a transformative force in the digitization of energy infrastructures. IT/OT convergence bridges the gap between traditional operational systems (OT) responsible for energy generation, distribution, and management, and modern IT that enable data analytics, communication, and decision-making. Defining a common communication and data framework that bridges the historically distinct IT and OT domains is essential. Layer 3 prioritizes interoperability standards, robust security measures, and scalable technologies to facilitate the exchange of data and insights between these domains.
- TEIA Alliance: The Trusted Energy Interoperability Alliance (TEIA) guides the design and deployment of Layer 3 and provides a framework for Layer 0, Layer 1 and Layer 2. TEIA organizes the four layers of the digitalization framework into a neutral and coherent standard that provides adaptable digitalization and interoperability norms for energy systems and smart grids [10]. TEIA's goal is to foster secure digitized orchestration by guiding the design of trusted, complementary energy infrastructure components and interoperable monitoring and signaling systems. This will ensure greater compliance, privacy, and confidentiality across smart grids and modern energy business entities such as VPPs.

Today, energy systems are supported by innumerable devices and platforms that are often developed by different manufacturers with various communication protocols. To effectively orchestrate the digitalization, communication, and integration of these eclectic systems it is necessary to establish a methodical, scalable, and trusted digitalization framework. Furthermore, a digitalization framework must also encompass regulatory harmonization across countries to ease international interoperability and compliance efforts [11]. In this paper, we have outlined provisions for standardized digital energy orchestration mechanisms that could alleviate these challenges to create a global framework for smart grid digitalization and interoperability.

V. Conclusion

It is critical that all relevant participants in the digital energy economy feel safe and poised to efficiently scale smart grids. As technology evolves and new cyberthreats emerge, the ability to update and enhance security measures is crucial. Simplifying the orchestration and renovation of digital energy entities across private and public stakeholders, as well as across regions and international borders, can be achieved through collaborative standardization efforts, such as the one proposed here. A secure and interoperable data framework for energy digitalization can play a vital role in establishing guidelines that promote interoperability and security in energy systems. This is essential to foster vibrant and responsive energy markets, instrumental in achieving environmental goals, such as reducing carbon emissions and promoting clean energy sustainability [12].

Acknowledgment

Hebberly Ahatlan thanks Anahita Poonegar, Douglas Uptmor, David P. Maher, Julian Durand, Christopher Kalima, Ian McAdams, and the marketing and engineering teams at Intertrust Technologies for their input in the preparation of this paper.

References

[1] European Commission. Digitalization of the European Energy System, 2023. https://digital-strategy.ec.europa.eu/en/policies/digitalisation-energy

[2] IEC. IEC 61850 standard series and associated extensions, governing the interoperability in the Power Utility automation domain — ahead of semantic interoperability, 2023. https://iec61850.dvl.iec.ch/

[3] International Energy Agency. Tracking Clean Energy Progress, 2023. https://www.iea.org/reports/tracking-clean-energy-progress-2023

[4] The United Nations Economic Commission for Europe. Group of Experts on Energy Efficiency. Seventh session, item 5 of the annotated provisional agenda. Regulatory and policy dialogue addressing barriers to improve energy efficiency. Geneva, September 2020. https://unece.org/sites/default/files/2020-12/GEEE-7.2020.INF_.3.pdf

[5] World Economic Forum. Harnessing Artificial Intelligence to Accelerate the Energy Transition, White Paper. September 2021. https://www3.weforum.org/docs/WEF_Harnessing_AI_to_accelerate_the_Energy_Transition_2021.pdf

[6] H. Ahatlan, "Overcoming zero-trust environments for smart city data and devices," 2023 *17th Multi Conference on Computer Science and Information Systems* Porto, Portugal, July 2023. https://mccsis.org/wp-content/uploads/2023/07/CSC2023_R_026.pdf

[7] European Network of Transmission System Operators for Electricity. Common Information Model, 2023. https://www.entsoe.eu/digital/common-information-model/

[8] R. Czechowski, P. Wicher and B. Wiecha, "Cyber security in communication of SCADA systems using IEC 61850," *2015 Modern Electric Power Systems (MEPS)*, Wroclaw, Poland, 2015, pp. 1-7, doi: 10.1109/MEPS.2015.7477223. https://ieeexplore.ieee.org/document/7477223

[9] J. Durand, C. Kalima, "How is XPN different from a VPN." Intertrust Technologies, February 2023. https://www.intertrust.com/platform/xpn-faq/#faq-item-6

[10] The Trusted Energy Interoperability Alliance. Secure Interoperability Standard for energy, 2023. https://www.trusted-energy.org/

[11] M. Keller, "Smart Grid Standards and the Importance of Interoperability," Smart Electric Power Alliance, March 2022. https://sepapower.org/knowledge/smart-grid-standards-and-the-importance-of-interoperability/

[12] European Commission. European Green Deal: Energy Efficiency Directive adopted, helping make the EU 'Fit for 55,'July 2023. https://energy.ec.europa.eu/news/european-green-deal-energy-efficiency-directive-adopted-helping-make-eu-fit-55-2023-07-25_en

Hebberly Ahatlan, B.S. Electrical Engineering. UCLA, 2006, is an energy technology initiatives leader developing go to market plans for software platforms in the smart city and AI sectors. Currently he is a member of the marketing staff at Intertrust Technologies directing marketing strategies for smart grid security solutions.