Considerations for Secure Data Exchange to Achieve Cyber-Physical Situational Awareness in the Electric Grid

P. Cordeiro*, A. Chavez,
S. Hossain-McKenzie
Sandia National
Laboratories
*pgcorde@sandia.gov

A. Stenger, S. Bayless
Sierra Nevada
Corporation

R. Clark,
S. Behrendt
Tenable

J. Hawkins
Public Service
Company of
New Mexico

K. Davis
Texas A&M
University

2023 IEEE Power and Energy Conference at Illinois (PECI) | 979-8-3503-9940-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/PECI57361.2023.10197678

***Abstract*—Cyber-physical situational awareness (CPSA) is crucial for understanding the intricacies and relationships within the interconnected electric grid, especially with increasing distributed energy resource penetration. However, beyond developing the necessary cyber-physical data fusion techniques, another critical challenge to address is the multi-level, multi-owner data exchange process and its cybersecurity. Therefore, in this paper we explore the considerations for secure data exchange for performing CPSA analysis and present the current landscape alongside existing gaps, potential solutions, and next steps. Additionally, we present a case study related to the project team's CPSA sensor and implementation architecture development, called griDNA, and how these potential solutions could apply and form a secure data exchange framework.**

***Index Terms*—cyber-physical systems, electric grid, situational awareness, secure data exchange, cybersecurity**

I. Introduction

With the continually evolving cyber-physical grid and rising penetration of distributed energy resources (DERs), cyber-physical situational awareness (CPSA) is needed for holistic observability into the interconnected, decentralized electric grid [1]. Processes such as IEEE 1547 DER grid-support functions and communication-assisted protection schemes increase reliance on communications [2], [3]. The highly interconnected nature of the grid with growing, distributed grid-edge presence requires greater visibility into the cyber and physical system states. It is no longer sufficient for the grid to only monitor the physical power system – the cyber-physical system must be monitored and understood to efficiently operate the evolving, cyber-physical grid as well as respond to disturbances quickly and adaptively. Achieving CPSA in the grid is a challenging goal, especially due to the multi-level nature of the grid (e.g., establishing trust between utility, aggregator, customer levels), the lack of existent cyber-physical sensors to gather necessary concurrent data, and techniques to fuse cyber-physical data for full system CPSA.

As more DERs and smart technologies are connected to the traditional transmission and distribution grid, it is of paramount importance that grid operators have cyber-physical visibility into the connected system as a whole. The 2003 Northeast Blackout demonstrated the critical need for situational awareness across utility systems; furthermore, as cyber attacks increase in frequency and sophistication, this situational awareness can no longer be limited to the physical system dynamics [4], [5].

However, an important consideration in the multi-level and multi-owner grid is the ability to securely exchange necessary data for CPSA insights. For example, necessary data may already exist on communicating devices that vary in capability, from low-powered micro-sensors to high-powered server configurations; from custom to standardized transmission protocols; and from publicly broadcasting to certified, highly secure hardware. This diverse set of devices vary significantly in their cybersecurity capabilities. Other important considerations are sensor placement algorithms to ensure the necessary system observability; obtaining placement permission for new sensors, and whether communication is locally integrated or overlaid, are open, relevant questions to address. All in all, the security and integration considerations for achieving interconnected CPSA are critical to understand, especially as DER penetration and grid modernization increase.

In this paper, we will focus on exploring these considerations in terms of the state-of-the-art as well as remaining gaps. We will discuss these considerations for defining next steps for designing a CPSA sensor and implementation architecture, called griDNA. Section II will detail existing architectures and security solutions and Section III will dive into some of the remaining security concerns and gaps. Section IV describes potential solutions and Section V provides more details on griDNA introducing a case study to discuss its security needs and which potential solutions are most suitable for composing

This article has been authored by an employee of National Technology Engineering Solutions of Sandia, LLC under Contract No. DE-NA0003525 with the U.S. Department of Energy (DOE). The employee owns all right, title and interest in and to the article and is solely responsible for its contents. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this article or allow others to do so, for United States Government purposes. The DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan https://www.energy.gov/downloads/doe-public-access-plan. This material is based upon work supported by the Sandia Laboratory Directed Research and Development Project # 229434; SAND2023-11678C.

a secure data exchange framework. Finally, Section VI will discuss conclusions and future work.

II. Background

Constituents of the multi-level, multi-owner electric grid each exhibit specialized cyber-physical architectures built for particular purposes. Energy markets, utilities and DER owners carry out their missions with divergent bases of security requirements and outcomes. Utilities may rely on network separation, whether for legacy equipment with private, leased communication lines, or for air-gapped isolation of control equipment, for example [6]. Meanwhile, DER owners may have compulsory communications with contracted system maintainers and grid operators, enabled by unspecified network connections such as local wireless networking connected to an internet service provider [7].

Energy markets have begun to tackle security issues by using blockchain technologies; blockchain frameworks promise secure, transparent market transactions [8]. The surety of blockchain applications is under constant examination [9], as newly implemented use-cases succeed or fail.

III. Security Concerns for Data Exchange

The data exchange needed for cyber-physical situational awareness spans the operating power system state-space balancing production, loads and disturbances, and requires insight into even larger numbers of comparatively small, distributed generating systems. Given the availability of data needed to improve grid operation and integration of distributed generating resources, the challenge becomes identifying which information is of a protected class.

The system granularity allowing local inverter-based systems to support a stressed large-scale power grid, also poses a risk as an attack surface if left unprotected. For this application of deploying CPSA sensors, the sensors themselves and the networks where they are deployed must prevent access to certain classes of data and data synthesis, while other data remains publicly visible with protections against unauthorized modification.

New guarantees of data integrity and authenticity are necessary for the evolving, multi-faceted nature of power and ancillary service producers, consumers and intermediaries, amongst whom trust is not implicit.

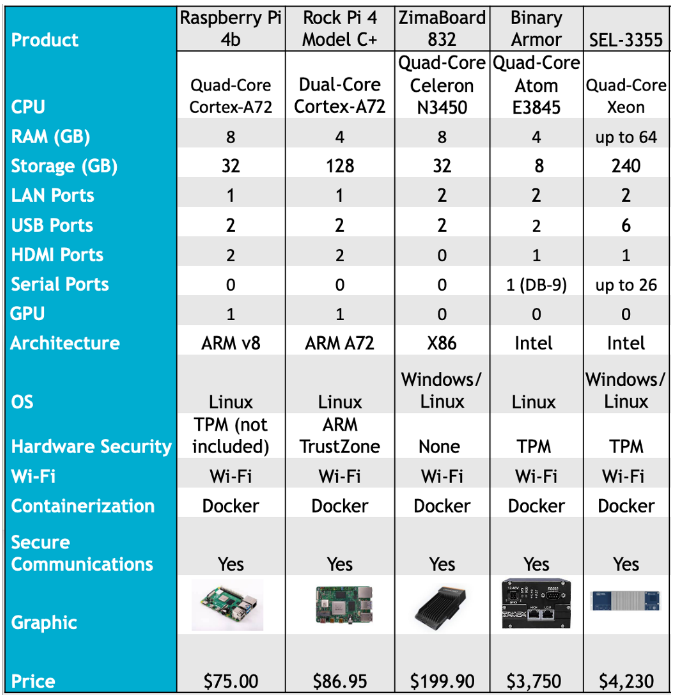
Technology for secure communications exists in assorted hardware, software and virtualization forms, tackling constraints such as translation, scalability, interoperability and latency, while seeking to satisfy confidentiality, integrity, availability, authenticity and non-repudiation. Sensors for CPSA may be further constrained to temporal access to data flows, or network segmentation and trust zones.

Secure data exchange will rely on cryptographic primitives and implementations rigorously vetted for the anticipated lifetime of the specific installations. For example, recommendations for key strengths and lifetimes are defined according to the accepted progression of successful attacks against types of keys. Recommendations for cryptographic algorithms are defined by the algorithms' strengths against demonstrated or anticipated attacks by conventional or quantum means. Additionally, a strong key management infrastructure is also an important requirement to ensure proper cybersecurity hygiene. Defining processes and procedures for key issuing, revocation, and recovery will be needed.

IV. Potential Solutions

A. Single Board Computer Options

Several single board computers (SBCs) are available that are capable of harnessing the necessary hardware and software to implement secure data exchange. These SBCs vary in resources, capabilities, and cost. The SBC chosen will depend on the capabilities needed, cost, and how well they can be integrated into existing environments. Low-cost SBCs may be sufficient for grid-edge devices that require minimal processing, whereas higher-cost industrial systems may be necessary when aggregating data and performing complex analysis across a large number of the deployed low-cost SBCs. Each of the SBCs will also need to interoperate with a diverse set of devices and protocols to be practical. DERs continue to evolve and the SBC system(s) selected will also need to adapt to those changes. Existing commercial-off-the-shelf hardware can be leveraged to collect and communicate data between DERs. To ensure secure communications between multiple parties, open source or commercial software can be integrated within the SBCs.



Product	Raspberry Pi 4b	Rock Pi 4 Model C+	ZimaBoard 832	Binary Armor	SEL-3355
CPU	Quad-Core Cortex-A72	Dual-Core Cortex-A72	Quad-Core Celeron N3450	Quad-Core Atom E3845	Quad-Core Xeon
RAM (GB)	8	4	8	4	up to 64
Storage (GB)	32	128	32	8	240
LAN Ports	1	1	2	2	2
USB Ports	2	2	2	2	6
HDMI Ports	2	2	0	1	1
Serial Ports	0	0	0	1 (DB-9)	up to 26
GPU	1	1	0	0	0
Architecture	ARM v8	ARM A72	X86	Intel	Intel
OS	Linux	Linux	Windows/ Linux	Linux	Windows/ Linux
Hardware Security	TPM (not included)	ARM TrustZone	None	TPM	TPM
Wi-Fi	Wi-Fi	Wi-Fi	Wi-Fi	Wi-Fi	Wi-Fi
Containerization	Docker	Docker	Docker	Docker	Docker
Secure Communications	Yes	Yes	Yes	Yes	Yes
Graphic					
Price	$75.00	$86.95	$199.90	$3,750	$4,230

Fig. 1: Hardware options for implementing secure data exchange.

The specifications for several systems that can serve as a sensor to securely exchange data are shown in Fig. 1. Each of these devices are capable of interoperating with one another which is important when a diverse set of sensors are deployed. The combination of Random Access Memory (RAM), Central Processing Unit (CPU), and storage are important to determine the software that can be supported for each board. For example, a sensor that harnesses software that is memory intensive may be narrowed down to only those devices that exceed a certain threshold of RAM. It should also be noted that many of the example sensors included here do have the ability to be expanded and customized to a variety of configurations. Additional low-cost modifications, such as increasing the storage capacity, are also available if required.

The number of communication ports is also an important feature since the sensors will need to serve as a bump-in-the-wire system while also communicating with the other sensors deployed. Universal Serial Bus (USB) to Ethernet dongles can be introduced as needed as a low-cost solution to increase the number of network communication ports. The number of USB ports and built-in Ethernet ports along with their speeds is another factor that can drive which SBC is selected. Additionally, if artificial intelligence (AI) algorithms are planned for an individual sensor, it may be beneficial to include sensors with a Graphics Processor Unit (GPU), Tensor Processing Unit (TPU) or other advanced processor architecture to enhance performance. Machine learning algorithms may be desired to assist in the detection of abnormal behavior which could be indicative of a cyber-physical attack. Also, to ensure that the sensors boot properly into a known good state that is secure or to have a trusted execution environment, it is important to deploy sensors that support technologies such as the Trusted Platform Module (TPM) or ARM TrustZone. These hardware security features could be used to securely store cryptographic keys or perform secure computations. Wireless communications will become more important as 5G and cellular communications are introduced into DER environments. Wi-Fi capabilities will be particularly important especially as the number of devices increase in regard to Industrial Internet of Things (IIoT).

Finally, to simplify the portability of custom or commercial software packages, it is important to include SBCs that support software containerization. Containerization technology allows new software packages to be rapidly integrated into deployed devices without requiring custom modifications to the software to function or cumbersome troubleshooting to integrate the software package when the underlying hardware platforms change. Note, the devices listed in Fig. 1 do not represent a comprehensive list of all potential options, but do provide a snapshot of the available options that can serve as viable options to deploy sensors that can securely exchange data.

B. Data Exchange and Type

With regard to power system data intended for public consumption, a popular idea for preventing unauthorized modification is that of using distributed ledgers incorporating cryptographic validation mechanisms. Transactions or other records can be secured in data structures such as chains or graphs preserving the integrity of data. These schemes are built to allow information owners the ability to select how information is shared. Some such arrangements may be infeasible in the realm of grid support functionality whereby a standard level of detail is necessary, however the methods of immutable ledgers remain a potential solution for securing published data that cannot be tampered with or maliciously modified.

Additionally, it is important to consider what type of cyber-physical data needs to be communicated between owners in a multi-owner system. For example, power system data could include measurements such as voltage, current, real and reactive power, and frequency at different buses as well as system topology including generator and load locations. These topology-focused measurements and information are often considered sensitive by the system owner and are typically not shared with external entities and/or other system owners. Therefore, by studying what type of data is available in a particular system, one can define what type or form of data can be shared across multiple owners. In the case of the topology-focused data, this detailed information could be shared with a single system to increase individual system situational awareness while only aggregate data (e.g., total real power generation, total load, average frequency) would be shared with external entities to enhance cohesive system operation. Similarly, for the cyber network data, it is important to assess what data is useful to share across system owners and does not release any sensitive information. For example, sharing information types of communication protocols, security alerts, and modes of operation/control (e.g., grid support functions) can benefit integrated, multi-owner systems.

Placement and roles of the griDNA sensors will dictate both data sharing and protection requirements. Encryption requirements of griDNA shared data will depend on each sensor's location and access privilege. For example, a griDNA sensor located within a physically protected area with only analog and digital inputs for reading system measurements, and no further communication interfaces to network-connected cyber-physical equipment, may be allowed to communicate with similarly situated griDNA sensors without encryption. Careful configuration of network segmentation, firewalls and data separation is required for these griDNA sensors' communications with next-level sensors/aggregators having greater access and communication privileges.

C. Data Encryption

For griDNA sensors requiring encryption, Transport Layer Security (TLS) is the *de facto* standard providing an encrypted tunnel for application data of any kind. The resources necessary for supporting TLS, such as an operating system with libraries for secure socket layer, pre-provisioning of Public Key Infrastructure (PKI) certificates, and internet connection for software and certificate status updates, may exceed the capabilities of lower end IoT devices implementing more elementary griDNA sensors.

MQTT, the lighter-weight popular IP-based IoT pub-sub communication protocol, provides optional, built-in end-to-end encryption with subscribers employing ad hoc (i.e. not PKI) username/password protection. Disadvantages to this approach include cumbersome password management as the number of subscribers increases. [10].

Named Data Networking (NDN) [11], a data-centric alternative to host-based communication architectures, provides security at the data level [12], employing per-packet signatures, schematized trust, and encrypting data at creation [13]. Data owners themselves establish requesters' data access rights. Examples of NDN in health apps [13] and IoT [14] have shown success with information-centric architecture. An example NDN certificate management system is proposed in [15].

As the implementation and discovery regarding griDNA sensors evolve through case study and demonstration projects, we propose for further consideration the exploration of rigorous criteria to be established for identifying and categorizing data protection agreements regarding cyber-physical data collection and fusion.

In the other direction, information about connected devices and users is often garnered silently, through mechanisms otherwise created to improve usability and experience. The concept of privacy budgets, as proposed by Google, addresses such fingerprinting by suggesting voluntary limits on the amount of information collected by sites from device configurations or user behaviors. Sites authorized to access CPSA sensors could presumably be required to abide by privacy budgets devised specifically for cyber-physical observability.

Secure data exchange by CPSA sensors will enable trusted observability and characterization of the cyber-physical system state. The path to solving the concerns surrounding secure data exchange will take into consideration several aspects of data protection. Trade-offs of diversely capable SBCs, software defined networks, and containerized solutions will be examined, wired and wireless access up to and including 5G and Wi-Fi 6 will be considered, observability analytics platforms will be studied, and X-As-A-Service will be explored for securing CPSA sensor data in flight and at rest.

V. Case Study for griDNA

To address the need for CPSA in the grid, we have proposed to develop griDNA, multi-level CPSA sensors and their implementation architecture, that collects cyber-physical data at varying, decentralized grid levels and applies advanced sensor data-fusion techniques, both locally and globally, to understand the cyber-physical system state, characterize interdependent systems, and inform comprehensive planning, operation, and mitigation decisions; Fig. 2 presents an overview. Specifically, the griDNA sensor will not only collect the cyber and physical data concurrently but also perform onboard fusion analysis in real-time.

However, we must address the secure data exchange multi-level and multi-owner challenges for achieving the griDNA goals. The initial use-case for the griDNA project is presented in Fig. 3 and Fig. 4. Fig. 3 shows an integrated transmission system (IEEE 39-bus) and distribution system (local 15-bus system [16]) with 3 photovoltaic (PV) systems (11MW, 1MW, 256kW). The green curves indicate division between two entities, the utility-owned and privately-owned assets. Fig. 4 shows a representative communication network for the integrated power system including network devices such as gateways and routers as well as the smart inverters for the grid-edge PV systems. The yellow circles represent the exemplar local griDNA sensor placements, the blue circles represent the enclave griDNA sensors, and the green circles represent the global griDNA sensors.

Next, we describe a potential griDNA sensor data collection and analysis scenario; this scenario is summarized in terms of sensor capability in Table I. Note, this scenario is described for a paper-study purpose and further details (e.g., data storage, type of insights, entity participation) will be detailed in future experiments and publications.

- The local griDNA sensors collect cyber-physical data and perform onboard data fusion analysis only using the collected, local data streams. The local griDNA sensors are trusted by the system owner and their insights are not shared with other entities.
- The enclave griDNA sensors can collect cyber-physical data and perform onboard data fusion analysis and, additionally, aggregate insights or specific data sets sent by local griDNA sensors within the same system. The enclave griDNA sensors are trusted by the system owner and their insights are not shared with other entities.
- The global griDNA sensor only aggregates insights (with high-level data fusion) sent by enclave griDNA sensors across different systems, owned by different entities. The global griDNA sensor is trusted by all system owners and its insights can be shared with all participating entities.

A. Secure Data Exchange Architecture Design for griDNA

For the griDNA application in the case study and scenario described in this section, we would like to formulate an initial secure data exchange architecture that applies the potential solutions described in Section IV. For this effort, we will divide the architecture into five main pieces and discuss how each of these solutions can be applied to achieve the secure data exchange goal.

griDNA Sensor Design: As presented in Section IV, SBCs of varying specifications are available for the different griDNA sensor scenarios. Hardware selection will rest upon the particular applications to be run in each scenario.

Where throughput, low latency and encryption are required, cryptographic hardware accelerators can be found in the form of special purpose processor cores, co-processors, or extension boards; cryptographic software accelerators are now available as an extension in many processors' Instruction Set Architectures (ISA) [17].

Specialized boards with pre-installed hardware accelerators and firmware suited to scenarios can be used where appropriate. Care must be taken with immutable hardware features that could be rendered outmoded with advances in technology.

Keystores holding devices' certificates may be password protected or securely held in TPMs or hardware security

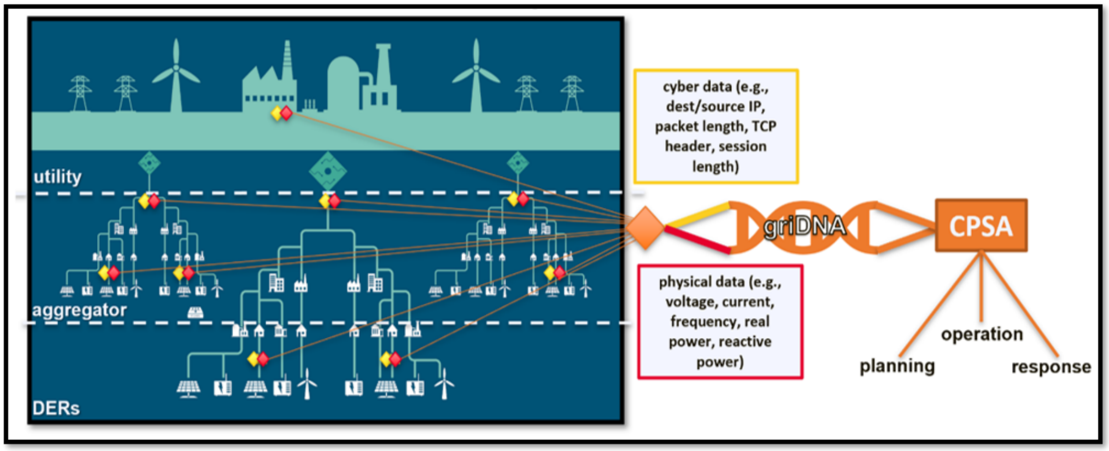

utility
aggregator
DERs
cyber data (e.g., dest/source IP, packet length, TCP header, session length)
physical data (e.g., voltage, current, frequency, real power, reactive power)
griDNA
CPSA
operation
planning
response

Fig. 2: Overview of griDNA multi-level CPSA sensors and implementation architecture vision.

TABLE I: Local, Enclave, and Global griDNA Sensor Summary for Data Sharing, Data Fusion (DF), and Local/Aggregate (Aggr.) Analysis Capabilities

Sensor Type	Collects Data?	Shares Data?	Local DF?	Aggr. DF?	Shares Local Insights?	Shares Aggr. Insights?
Local	Yes	Yes	Yes	No	Yes	Yes
Enclave	Yes	Yes	Yes	Yes	Yes	Yes
Global	No	No	No	Yes	No	Yes

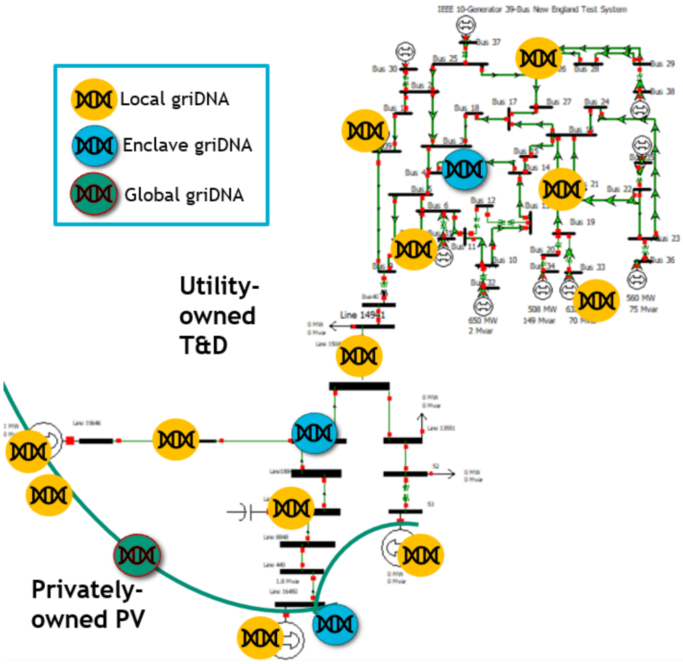


Fig. 3: Interconnected transmission and distribution system with grid-edge PV.

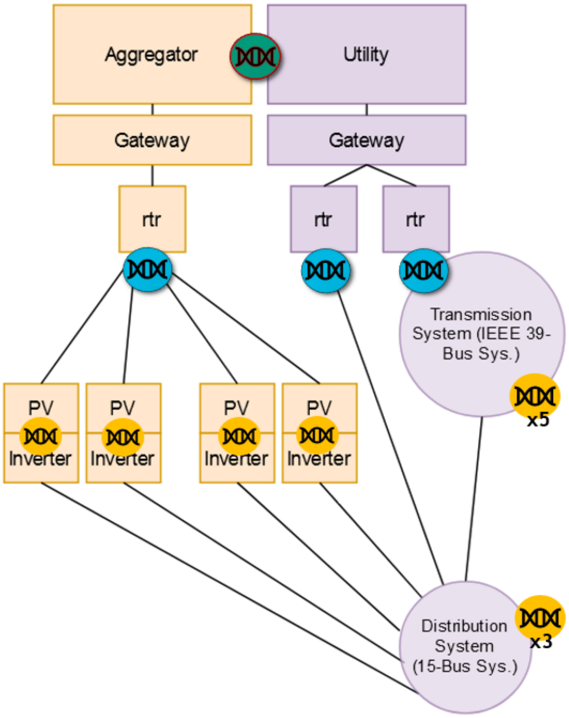


Fig. 4: Network for interconnected system with exemplar griDNA sensor locations.

modules (HSM) commensurate with the devices' security requirements.

Hardware and software solutions, as well as virtualization forms, such as software defined networking, containerization and X-As-A-Service, can be applied elsewhere as appropriate for satisfying portability, security and interoperability needs.

Local griDNA Sensor: Local sensors, collecting and analyzing data from one location/area using data fusion methods require sufficient hardware and software (described in prior section) to collect, store, and analyze data. Additionally, secure communication is needed between the local and enclave griDNA sensors as discussed in the additional features section.

Enclave griDNA Sensor: Enclave sensors, collecting and analyzing data from numerous local sensors with data fusion methods, will have the greatest demand for high throughput and low latency. Previous experiments on the project team's emulation system described throughput and latency benchmarks [18]. Enclave sensors will need to support secure communication to local sensors, where data and local insights are shared. Enclave sensors will also support secure communication to global sensors where only aggregate insights are shared and some data may need to be obfuscated.

Global griDNA Sensor: Global sensor design supporting full-scope aggregation and analysis with edge device deep learning could incorporate additional concepts from distributed, artifical intelligence (AI) and machine learning where greater efficiencies are needed. Examples of elastic inference with multi-capacity models, distributed inference via workload prediction, and efficiently distributed training based on importance sampling are considered in the work of [19]. The global sensors will, in general, have the most computational and storage resources available amongst the collection of sensors to perform analysis on the aggregated data.

Additional Features: Privacy-preserving data sharing methods including exchanging encrypted data, aggregating anonymous data, and pooling identified data in secure environments, are widely investigated for modern medical research [20].

Building from these three methods in the performance of anomaly detection for cyber-physical grid protection, an enclave griDNA sensor in a secure environment could logically pool identified data from local griDNA sensors; enclaves could exchange anonymous aggregated data for mid-range analytics and prediction; and the global griDNA sensor could exchange encrypted data with all enclaves for full-scale data fusion and analysis. Where necessary, anonymization should be used to the extent possible while still providing the ability to backtrack to the sources for appropriate response to physical and cyber issues.

Borrowing structures from data science, trees, chains and graphs can be put to use in preventing unauthorized modification of transactions or other records. Distributed ledgers such as the bitcoin blockchain employ Merkle Trees to efficiently prove a record to be a valid part of a previous commitment [21].

The Mnemosyne Logger [14] is a distributed, event-logging system built upon NDN and utilizes a directed acyclic graph structure to achieve an interlocking, immutable record of events. Unlike many blockchain implementations requiring computationally expensive proof of work, Mnemosyne requires proof of authenticity, providing high throughput and resiliency.

VI. Conclusions and Future Work

Secure data exchange for cyber-physical situational awareness of a multi-level, multi-owner electric grid requires consideration of appropriate methods of securing and integrating new and existing sources of characteristic data of the interacting cyber and physical state-spaces of the electric grid.

The griDNA sensors, the multi-level CPSA sensors currently under development, will contribute to the exploration of a set of solutions to the remaining challenges toward attaining the secure, cyber-physical awareness needed for an increasingly distributed and interconnected electric grid.

In this paper, we detailed the nature of these security challenges and proposed several potential solutions and design considerations for the griDNA sensor. We discussed these considerations, and persisting challenges, from the perspective of an integrated transmission, distribution, and PV system with exemplar griDNA sensor placements. In particular, we put forth the following concepts for an initial framework:

- We categorized and segmented the grid into three layers: (1) Local, (2) Enclave, and (3) Global. Each layer would have different owners of the data produced. The types of data to be shared between the layers and the requirements necessary to share the data were also discussed and defined;
- We discussed the hardware and software resources required for the various griDNA sensors placed at different locations within the transmission and distribution system (local, enclave, and global). Additionally, we provided candidate SBC options that can support the features needed by the griDNA sensors;
- We described several security considerations, such as host-based and data-centric security options and next generation communication options such as NDN and Wi-Fi 6;
- We described data security structures from the fields of data science, medical research and health apps that can be applied for the griDNA CPSA focus;
- We discussed deep learning efficiency methods of distributed AI for IoT that can be leveraged for griDNA distributed data fusion needs.

Ultimately, a high-level framework designed for secure data exchange in the grid is proposed in this paper that categorizes and segments the grid into different layers and defines specific hardware/software considerations and data exchange/structure considerations for each layer. In future work, we will build upon this framework by implementing some of the proposed solutions in a real-time cyber-physical emulation environment and assessing griDNA sensor operation. We will continue to define and iterate on the framework such that secure data exchange is achieved for enabling cyber-physical situational awareness in the electric grid.

Acknowledgements

We'd like to acknowledge the remainder of the griDNA Sandia team for their valuable discussion and review: Nicholas Jacobs, Adam Summers, Brian Wright, Logan Blakely, and Ryan Adams. Additionally, we are very grateful to the Sandia Resilient Energy Systems Mission Campaign for their funding and support of the griDNA project.

REFERENCES

[1] N. Jacobs, S. Hossain-McKenzie, A. Summers, C. B. Jones, B. Wright, and A. Chavez, "Cyber-physical observability for the electric grid," in *2020 IEEE Texas Power and Energy Conference (TPEC)*, 2020, pp. 1–6.

[2] D. G. Photovoltaics and E. Storage, "Ieee standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," *IEEE Std*, pp. 1547–2018, 2018.

[3] V. Terzija, G. Valverde, D. Cai, P. Regulski, V. Madani, J. Fitch, S. Skok, M. M. Begovic, and A. Phadke, "Wide-area monitoring, protection, and control of future electric power networks," *Proceedings of the IEEE*, vol. 99, no. 1, pp. 80–93, 2010.

[4] A. Muir and J. Lopatto, "Final report on the august 14, 2003 blackout in the united states and canada: causes and recommendations," 2004.

[5] K. E. Hemsley, E. Fisher *et al.*, "History of industrial control system cyber incidents," Idaho National Lab.(INL), Idaho Falls, ID (United States), Tech. Rep., 2018.

[6] A. J. McBride and A. R. McGee, "Assessing smart grid security," *Bell Labs Technical Journal*, vol. 17, no. 3, pp. 87–103, 2012.

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

[8] M. R. Hamouda, M. E. Nassar, and M. M. A. Salama, "A novel energy trading framework using adapted blockchain technology," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2165–2175, 2021.

[9] C. Herweijer, "Building Block(chain)s for a Better Planet," https://www3.weforum.org/docs/WEF_Building-Blockchains.pdf, 2018, [Online; accessed 22-Nov-2022].

[10] Steve, "Introduction to MQTT Security Mechanisms," http://www.steves-internet-guide.com/mqtt-security-mechanisms, 2022, [Online; accessed 16-Jan-2023].

[11] "Named Data Networking NDN Project Overview," https://named-data.net/project/, 2022, [Online; accessed 16-Jan-2023].

[12] "Named Data Networking," https://en.wikipedia.org/wiki/Named_data_networking, 2022, [Online; accessed 16-Jan-2023].

[13] "Sharing mHealth Data via Named Data Networking," https://web.cs.ucla.edu/~lixia/papers/ndnfit-icn-2016.pdf, 2022, [Online; accessed 23-Jan-2023].

[14] Liu, "Mnemosyne: An immutable distributed logging framework over named data networking," September 2021. [Online]. Available: https://doi.org/10.1145/3460417.3483375

[15] Z. Zhang, S. Y. Wong, J. Shi, D. Pesavento, A. Afanasyev, and L. Zhang, "On certificate management in named data networking," 2020. [Online]. Available: https://arxiv.org/abs/2009.09339

[16] R. Darbali-Zamora, J. Hernandez-Alvidrez, A. Summers, N. S. Gurule, M. J. Reno, and J. Johnson, "Distribution feeder fault comparison utilizing a real-time power hardware-in-the-loop approach for photovoltaic system applications," in *2019 IEEE 46th Photovoltaic Specialists Conference (PVSC)*, 2019, pp. 2916–2922.

[17] "AES Instruction Set," https://en.wikipedia.org/wiki/AES_instruction_set, 2023, [Online; accessed 23-Jan-2023].

[18] I. Onunkwo, "Recommendations for data-in-transit requirements for securing der communications." 10 2020. [Online]. Available: https://www.osti.gov/biblio/1876612

[19] "How to run a BILLION IoT devices w/ Mi Zhang — Stanford MLSys 41," https://www.youtube.com/watch?v=xy4sbZ4ev2k, 2021, [Online; accessed 5-Dec-2022].

[20] F. Wirth, "Privacy-preserving data sharing infrastructures for medical research: systematization and comparison," August 2021. [Online]. Available: https://doi.org/10.1186/s12911-021-01602-x

[21] "Merkle Tree," https://en.wikipedia.org/wiki/Merkle_tree, 2022, [Online; accessed 16-Jan-2023].