A Microgrid Ontology for the Analysis of Cyber-Physical Security

Matthew Backes, Ken Keefe, Alfonso Valdes
Information Trust Institute
University of Illinois at Urbana-Champaign
Urbana, Illinois, USA
{mbackes2, kjkeefe, avaldes}@illinois.edu

***Abstract*—The IEC 61850 protocol suite for electrical substation automation enables substation configuration and design for protection, communication, and control. These power system applications can be formally verified through use of object models, common data classes, and message classes. The IEC 61850-7-420 DER (Distributed Energy Resource) extension further defines object classes for assets such as types of DER (e.g., energy storage, photovoltaic), DER unit controllers, and other DER-associated devices (e.g., inverter). These object classes describe asset-specific attributes such as state of charge, capacity limits, and ramp rate. Attributes can be fixed (rated capacity of the device) dynamic (state of charge), or binary (on or off, dispatched or off-line, operational or fault state). We sketch out a proposed ontology based on the 61850 and 61850-7-420 DER object classes to model threats against a microgrid, which is an electrical system consisting of controllable loads and distributed generation that can function autonomously (in island mode) or connected to a larger utility grid. We consider threats against the measurements on which the control loop is based, as well as attacks against the control directives and the communication infrastructure. We use this ontology to build a threat model using the ADversary VIew Security Evaluation (ADVISE) framework, which enables identification of attack paths based on adversary objectives (for example, destabilize the entire microgrid by reconnecting to the utility without synchronization) and helps identify defender strategies. Furthermore, the ADVISE method provides quantitative security metrics that can help inform trade-off decisions made by system architects and controls.**

***Index Terms*—IEC 61850, microgrids, cyber-physical security evaluation, common information model**

I. Introduction

Cyber attacks against industrial control systems (ICS), of which modern energy delivery systems (EDS) are an important class, are of increasing concern, with some high-profile attacks receiving significant media attention [1][2][3]. Automation such as supervisory control and data acquisition (SCADA) has been part of these systems for decades. ICS are susceptible to physical disturbances, benign device misoperation, and cyber attacks [4]. Proper control must consider the possibility of each of these types of scenarios and how to differentiate between benign and malicious events.

EDSs function on a control loop consisting of measure-analyze-control. Measurements are collected on a variety of Intelligent Electronic Devices (IED), such as relays. IEDs are capable of a significant degree of local analysis and response. Whether local or centralized, the analysis determines whether the system is in a safe operating state, and issues control commands to field devices. These can be to dispatch generators, change transformer settings, or, in the case of a fault, trip one or more breakers to isolate the faulted part of the system. A cyber attack or malfunction that disrupts controller response can lead to dangerous conditions as well as significant damage to expensive, difficult-to-replace equipment.

Our main contribution is the development of an ontology to specify a microgrid design, using the ontology to build an executable, state-based attack graph by using the ADVISE Meta modeling framework [5]. ADVISE Meta models take a block diagram representation of a system, system characteristics, adversarial capabilities, and metric definitions to produce quantitative security results that inform system architecture and attack mitigation strategies. For constructing the block diagram and defining system characteristics, we will develop an ontology for microgrids that is based upon the IEC 61850 [6] and Common Information Model (CIM) standards ([7], [8], and [9]). These standards offer an information model and data object model for power systems and their applications. IEC 61850 is meant to be applied in the substation environment, but we employ its device modeling capabilities in the context of a microgrid. The CIM is used to provide a basis for the domains of our ontology, and for the physical system modeling. Another ADVISE input is adversarial capability. We will use standard profiles for this part of our models. The final input is security metric definitions.

The rest of the paper is outlined as follows. Section II defines microgrid systems, states assumptions made in this work, and introduces an example microgrid system. Section III describes the contributions of IEC 61850 and the CIM to the microgrid ontology this work develops. Section IV describes the current progress of the ontology this work is developing. Section V briefly describes the ADVISE method and demonstrates it on part of the example from Section II. We describe related work in Section VI and conclude in Section VII.

II. Microgrids

Microgrids have emerged as an important component of smart grids. Definitions of microgrids vary, but for our purposes, microgrids include the following components.

- A point of interconnection (POI) to a larger utility system. Depending on the mode of operation, the microgrid may get some or all of its power from the utility, or feed power back to the utility system, or disconnect from the utility (this last mode of operation is referred to as *islanded*).
- A variety of distributed energy resources (DER), with varying capacities and characteristics, such as ramp rate.
- Intelligent loads that respond to requests from the system for rapid demand response.
- A subset of loads identified as critical, for which the control and response mechanism must serve as long as possible.
- A microgrid controller, which may be centralized or distributed and makes decisions, including ones on dispatch of DER, regulation of power flow between the microgrid and the utility or islanding from the utility, and shedding of load.
- A measurement and control network that collects measurements at numerous points in the system, communicates these to the controller, and communicates control commands from the controller to the required nodes.

Microgrids have been promoted as a means to integrate community-scale renewables as an alternative to grid-scale approaches (in the microgrid case, local photovoltaic (PV) versus a centralized PV farm). By building in an islanding capability in the form of microgrids, regional electrical systems may be more robust against events such as major storms, and may be easier to reconstitute from component microgrids. On the negative side, microgrids present challenges of voltage and frequency stability due to their smaller size and lack of rotational inertia [10]. As with conventional transmission and distribution grids, microgrids must include system protection, which is the ability to rapidly detect and isolate a system fault. Protection schemes in modern electrical systems depend on networked communications between relays with overlapping zones of responsibility.

We will use the microgrid network topology illustrated in Figure 1. The microgrid is able to island and connect to the utility distribution system via a single POI. We incorporate a synchronous natural gas generator and power-electronics interfaced battery storage, along with a single critical load and a single non-critical (or interruptible) load. We assume that the microgrid operates under a modern configuration, communication, and control framework, in our case the IEC 61850 standard and DER extensions to that standard.

III. IEC 61850 AND CIM

The CIM is a suite of standards that allow for the definition and exchange of power system data between organizations and applications. The IEC standard 61970-301 [11] defines the base semantic model that describes the components of a power system model at an electrical level and describes the relationships between components. The CIM is maintained as a Unified Modeling Language (UML) model. The UML is used for modeling components within a software development lifecycle, including data structures, system interactions, and use cases. We will employ the CIM as a basis for the domains of our ontology, as well as for the physical modeling of the power system.

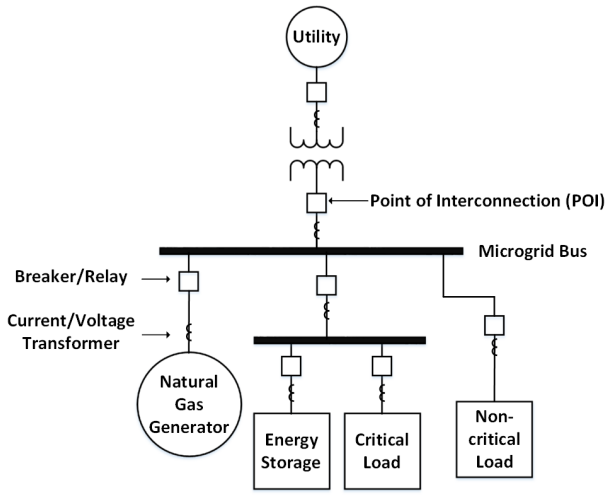

Fig. 1. A reference microgrid topology used as a basis for the preliminary ontology development.

The IEC standard 61850 was introduced as a standard for substation automation systems, with the aim to standardize communications and enable interoperability of IEDs. While IEC 61850 provides a comprehensive information model of substation automation components, it is also useful for the modeling of microgrid components. Many of the components overlap between the substation automation and microgrid domains, and IEC working groups are extending the standard to cover functions outside of substation automation. One such extension is IEC standard 61850-7-420 for DERs [12]. We will utilize the comprehensive information models of the base standard and its extensions in the context of a microgrid.

61850 also includes a number of message classes. For our purposes, the important ones are Sampled Values (SV), by which system measurements are communicated to merging units at the rate of 80 values per grid cycle (60 Hz in the U.S., resulting in an SV with a rate of 4800 Hz), and Generic Object Oriented Substation Events (GOOSE), which are used to communicate status values (breaker open or closed) as well as commands to trip a breaker or to block a trip from taking place. 61850 contains concepts of a process bus, station bus, and merging unit, but as they do not impact our modeling at this stage, we do not address them in this work.

While there is overlap between the CIM and IEC 61850, the aim of this paper is not to address the harmonization of the standards, but rather to select the best features from each standard and adopt them for our microgrid ontology. For example, CIM offers a comprehensive information model of physical components, and organizes them into classes, objects, and attributes. Inheritance is also expressed in the standard and it lends itself well to the building of an ontology. IEC 61850 offers comprehensive device object modeling, and since we are interested in executing attacks against devices within a

microgrid, we have adopted this strength in our model.

IV. Ontology

As defined in [13], in the context of information sciences, an ontology defines a set of representational primitives with which to model a domain of knowledge. The representational primitives typically include information about their meaning and constraints on their logically consistent application.

The core CIM is maintained as a UML model. It defines the components of a power system as classes and defines three relationships between the classes: inheritance, association, and aggregation. The parameters within each class are also defined. This provides us with a foundation for a generic model that can represent all aspects of a power system.

Harmonization of the CIM and 61850 is being addressed by IEC Working Group 19 and the Electric Power Research Institute (EPRI) [14]. We will base our preliminary ontology on the CIM physical model, as it is an information model, and we will use the IEC 61850 standard for its communication, control, and monitoring functions. These will be layered on top of the CIM physical model. We do not claim that this ontology definition is exhaustive; it is certainly far from it. However, we want to define the building blocks of the microgrid ontology, and then describe one specific application with the microgrid control system. Our microgrid ontology does not currently spell out specific cyber components, such as firewalls, HMIs, etc. This class of components are being considered by IEC technical committees. The ADVISE model is able to represent these components and the base ADVISE ontology begins to express fundamental ancestor types, such as *Server*, *Firewall*, and *Network*. As we develop the ontology further, we plan to incorporate these elements.

Classes in CIM are grouped together into packages dependent on their role within the power system. The core standard contains eight main packages plus a global domain package that defines data types. The *Core*, *Wires*, and *Topology* packages contain all the basic classes for defining the physical characteristics of a power network. The *Core* package contains the parent *PowerSystemResource* (*PSR*) class, from which all other classes concerned with the physical properties of the network inherit. In addition, there are *Generation*, *LoadModel*, *Measurement*, *Outage*, and *Protection* packages. Figure 2 shows a high-level example of the CIM UML model. It can be seen that the *Measurement*, *Dynamics* (a subset of *Generation*), and *Core* packages are utilized.

The *IdentifiedObject* class is the root class for this particular branch of the CIM class hierarchy, and key CIM classes in this reference microgrid hierarchy are:

- *PowerSystemResource*, used to describe any resource within the power system, whether it is a physical piece of equipment or an organizational entity such as *ControlArea*.
- *Equipment*, which refers to any piece of the power system that is a physical device, whether it be electrical or mechanical.

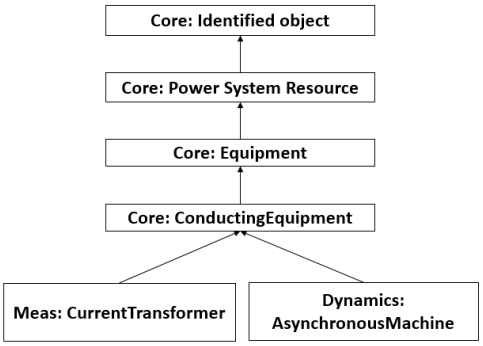

Fig. 2. High-level representation of CIM base ontology that relates to the reference microgrid.

- *ConductingEquipment*, used to define types of Equipment that are designed to carry current or that are conductively connected to the network.

The current transformer (CT) class is used to measure current on an electrical conductor, but does not map to a piece of *ConductingEquipment* in the CIM. Instead, a *Measurement* instance, representing a SCADA measurement from the CT, is associated with the *Terminal* on the *Breaker*. The *AsynchronousMachine* class maps to a single piece of conducting equipment. When operating as a generator, the *AsynchronousMachine* object must have an association with an instance of *GeneratingUnit*. For the reference microgrid, the *GeneratingUnit* will be the battery storage.

IEC 61850 provides a comprehensive library of semantic models known as *logical nodes (LN)*, although there is a lack of concrete semantic information attached to the LNs. However, relations between two logical nodes can be defined from a particular context. Therefore, we extend the IEC 61850 ontology to provide such contextual information, which defines logical relations between logical nodes within a microgrid. In addition, we utilize the IEC 61850-7-420 DER extension standard to include logical nodes that are related to DERs. As an example, the MMXU measurement logical node will be used by the microgrid controller to make a decision regarding resynchronization of the POI breaker, which uses the logical node XCBR.

To augment the CIM model with IEC 61850, we will relate LNs to PSRs by defining a relationship between the microgrid functions and the PSR that is providing the requested function. We will use the IEC 61850 Logical Node Groups to define our functions in this ontology. Those groups are listed in Table 1 of the IEC 61850-7-4 standard. The list below enumerates the logical node groups that are most applicable in the microgrid context. These groups contain specific LNs that control systems within a microgrid would need to utilize.

1) Automatic and supervisory control.
2) Distributed energy resources.
3) Metering and measurement.
4) Protection functions.
5) Instrument transformer and sensors.

Next, we expand the CIM *SCADA* class and *PSR* to include intelligent electronic devices of the types Relay, Microgrid Controller, and Battery Controller. The microgrid controller makes dispatch decisions for all the resources within the microgrid, and responds to requests from the utility distribution management system (DMS). The battery controller can receive commands from the microgrid controller, as well as make decisions based upon local measurements. A relay controls circuit breakers which determine which electrical connections are open and closed. Figure 3 shows how the IEDs are introduced into the CIM base ontology, and a small subset of LN connections are shown in red to detail where the IEDs are monitoring and controlling within the reference microgrid.

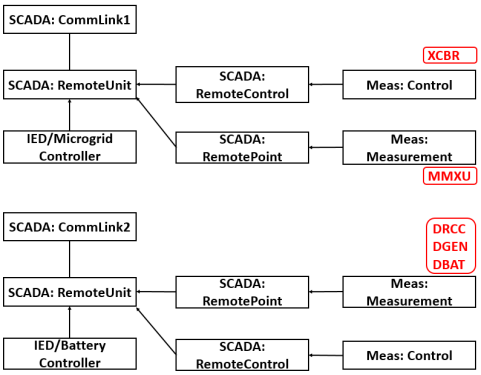

Fig. 3. Introducing DER and microgrid control systems into the reference ontology, and mapping to the corresponding LNs (red).

The LNClass allows the specification of a 61850 function for a particular domain. For example, the 61850 DER extension introduces a LN class called DER Unit Controller LNs. The DER device controller defines the operational characteristics of a single DER device. These characteristics can be either fixed or dynamic attributes. Example LNs within this class include DER Supervisory Control (DRCC) and DER Unit Generator (DGEN). DRCC has, among others, a fixed attribute of maximum real and reactive power the generator can output. DGEN has, among others, a dynamic attribute of "generator is synchronized to the EPS." These and other LNs allow the controllers within in a microgrid to correctly operate the system to maintain stable voltage and frequency. Figure 4 shows the interaction of the microgrid controller with other PSRs, and some example LNs are shown in red.

To motivate our creation of an ADVISE model, we briefly describe an example cyber attack within a microgrid. A particularly destructive attack is to cause the microgrid to connect to the utility when the two systems are not tightly aligned in voltage, frequency, and phase angle. A microgrid that has operated in island mode for a time may be at nominal frequency and voltage, but not aligned in phase angle with the utility system. The microgrid controller issues power injection commands to the assets within its control to align its phase angle to that of the utility according to IEEE Std. 1547 [15]. The control commands are based on measurements that come from the MMXU logical nodes, and in actual operation are

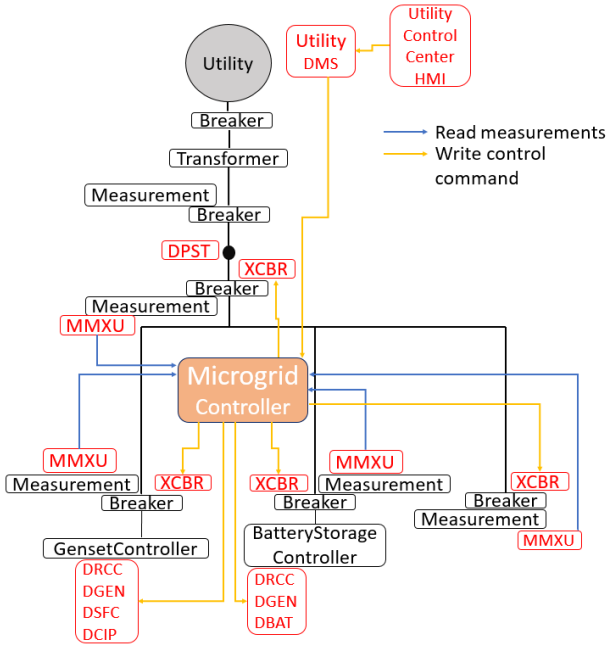

Fig. 4. Relationships between IEDs and the associated LNs within the reference microgrid.

reported at 61850 merging units. Our attack assumes that an adversary can inject false measurements into a merging unit, perhaps through a compromise of utility substation HMI systems, as was one of the attack vectors in Ukraine [2]. In our ontology, this is modeled as altering dynamic attributes of the MMXU LN. We next describe how an ADVISE model built from this ontology can be used to model this attack.

V. ADVISE

The microgrid ontology introduced in this paper is intended to be used for the construction of ADVISE models, with the ultimate purpose of evaluating the cyber-physical security ramifications of various design decisions. We provide a brief

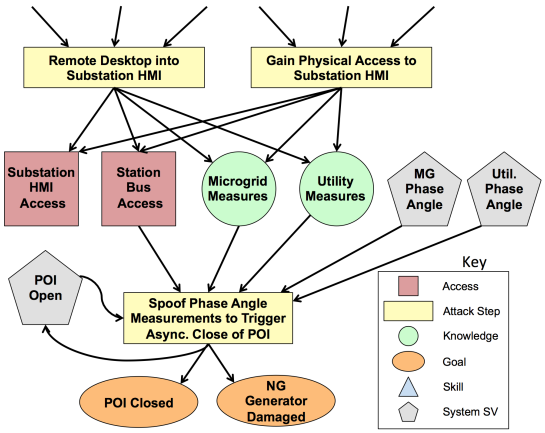

Fig. 5. An example fragment of the generated AEG from Figure 1.

overview of ADVISE and discuss how our microgrid ontology can be used to generate useful ADVISE models.

A. Overview of ADVISE Formalism

ADVersary VIew Security Evaluation (ADVISE) models [16] define an attack execution graph (AEG) that formally expresses the potential attack paths of an adversary attacking the system. Within the AEG, the state of an adversary's progress is stored in several types of state variables:

- *Access* elements define access domains.
- *Knowledge* elements define items of information.
- *Skill* elements define abilities.
- *Goal* elements define objectives.

The value of these state variables identify what the adversary possesses at a given time. Access, knowledge, and goals are boolean, with `TRUE` indicating that the adversary has obtained the item. Skills are integers between 0 and 1000, with greater numbers indicating a greater proficiency. Additionally, there is a *System State Variable* element type, which defines state variables not tied to the adversary, e.g., the frequency of the microgrid bus. System state variables may be integers, booleans, floats, or character types.

Figure 5 shows a fragment of the attack execution graph based on the microgrid example in Figure 1. Incoming arcs to an attack step mean that the state variable is used by the precondition expression of the attack step and outgoing arcs mean that the value of the state variable may be altered by an outcome of the attack step being attempted. When these attack steps are chained together, they form the attack paths possible in the model.

An ADVISE model also contains an adversary profile, which describes an adversary's interest or aversion to *cost*, *detection*, and *payoff*, as well as an adversary's initial state (state variables in the AEG he possesses at the beginning of simulation), and how many steps into the future an adversary can consider when planning his attack.

Using discrete-event simulation, custom quantitative metrics about the system performance, adversary behavior, operator costs, and more can be estimated. The quantitative results gathered in this way should not be used as absolute measures, since model input parameters may be inaccurate, but results can be used to make relative comparisons and sensitivity analysis can help users understand the effect of input parameters.

A more detailed explanation of ADVISE is available in [17].

B. ADVISE Model Generation

Realistic ADVISE models can grow large quickly, require a wide array of input parameters, and be too complex for manual construction. To alleviate these problems, the ADVISE Meta Modeling [5] approach has been developed. ADVISE Meta uses an ontology containing

1) A set of component types
2) A set of relationship types
3) A set of AEG fragments
4) A set of rules linking component and relationship instances to AEG fragment instances

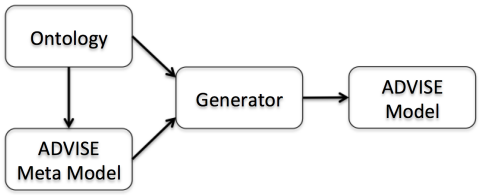

Fig. 6. The relationships between different parts of the ADVISE model generation process. The ontology provides available types for elements in the meta model's system diagram. The generator uses information specified in the ontology and the meta model to create an ADVISE model.

Using sets 1 and 2 from the ontology, the user constructs a meta model. An ADVISE Meta Model contains a high-level block-diagram of the system to be studied. The system diagram is composed of component instances as nodes and relationship instances as arcs between two nodes. The ADVISE Meta generator then applies the rules in set 4 to generate and connect instances of AEG fragments from set 3. This results in a complete ADVISE model of the system. Figure 6 shows the connections among the different pieces of the ADVISE model generation workflow.

For space reasons, the Figure 5 omits many more incoming and outgoing arcs from all of the elements in the diagram. In this fragment, the adversary may gain access to the utility's HMI, including the microgrid and utility measurements accessible by the HMI, by using remote desktop to access it remotely or by gaining physical access to the HMI. Once the adversary has access to the HMI, if the service phase angles (from the MMXU LN) of the microgrid and the utility buses are out of sync, the adversary can launch a spoofing attack that will fool the POI breaker into closing in an unsafe state and potentially damaging equipment, such as the natural gas generator. Another consequence of such an attack can be the loss of service to a critical load.

The effect of attempting any attack step in an AEG is stochastic, so it is not guaranteed that the adversary will be successful in obtaining their goal. For the *Spoof Phase Angle Measurements to Trigger Async. Close of POI* attack step, the outcome that gets selected during simulation depends on the magnitude of the difference of the microgrid and utility phase angles. IEEE 1547 specifies that the POI may close if the microgrid and utility are within 10° in phase angle. The adversary may spoof measurements so as to indicate that this condition is met, thereby enabling a potentially damaging POI close. If the true phase angle difference is within this limit, the spoofed measurement attack may result in a decision to close the POI, but otherwise does no harm to equipment. However, if the difference of phase angles is significant ($> 25^\circ$), then the adversary has a 90% chance of damaging the natural gas generator as well as opening the relay that protects the energy storage system. This also results in the critical load not being served. For this hypothetical attack step, there is always a 10% chance that the adversary will fail to achieve anything.

VI. Related Work

The CIM is maintained as a UML model, and therefore provides a base ontology in which one can describe the physical properties of a power system. In 2015 EPRI published an updated technical report about harmonization between CIM and 61850 [14]. In this technical report a detailed analysis of the harmonization problem is addressed. One of these recommendations is the use of the Web Ontology Language (OWL) [18] for the representation of semantic correspondences.

Other work has also been interested in integrating the CIM and IEC 61850 standards. The COLIN methodology is introduced in [19] to integrate utility standards. They take the CIM as the basic domain ontology, and transform other standards to the OWL ontologies. Their approach develops mappings between the standards, but many of these mappings require domain experts to verify. There has also been work in being able to solve the mismatches between CIM and 61850 automatically and without modifying the original standards [20]. They also use OWL, but then develop a tool which adds the required statements to complete the inferences obtained by an OWL reasoner. This work was extended in [21].

VII. Conclusion

The CIM describes components and component relations in a power system, using a formal UML model that is amenable to formal analysis. In this work-in-progress, we have sketched out an ontology for a microgrid, augmented to include IEC 61850 Logical Nodes. This ontology is the basis of an adversary model using the ADVISE methodology. We use the ontology to describe how a cyber attack against critical measurements can cause a dangerous reconnection of an islanded microgrid to the utility, which is an improper change of component attributes (MMXU LN values) in the ontology. We plan to extend this work to leverage the capabilities of ADVISE to model complex attack paths with assumptions about attacker objectives. The attacker wishes to inflict maximum system cost (equipment damage, loss of critical load) within constraints of attack path length and adversary cost. As such, the ADVISE model built from this ontology enables an attacker-defender game theoretic model.

Acknowledgment

The work described here was performed with funding from the Dept. of Energy (DOE) under Cooperative Agreement DE-OE0000831, under subcontract to ABB US Corporate Research Center. The views expressed are those of the authors.

Disclaimer

References

[1] D. Kushner, "The real story of Stuxnet, year=2013, pages=48-53, volume=50, month=March,," *IEEE Spectrum*.

[2] R. Lee, M. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," E-ISAC Report, March 2016.

[3] ICS-CERT, "Jsar-12-241-01: Shamoon/distrack malware," Industrial Control Systems Cyber Emergency Response Team, August 2012.

[4] A. Kushner, S. Amin, and S. Sastry, "Research challenges for the security of control systems," *Proceedings of the 3rd Conference on Hot Topics in Security*, pp. 1–6, 2008.

[5] B. Feddersen, K. Keefe, W. H. Sanders, C. Muehrcke, D. Parks, A. Crapo, A. Gabaldon, and R. Palla, "Enterprise security metrics with the advise meta model formalism," in *Proceedings of the 9th International Conference on Emerging Security Information, Systems, and Technologies*, Venice, Italy, Aug. 23 2015, pp. 65–66.

[6] *Communication networks and systems in substations - Basic communication structure for substation and feeder equipment,* IEC Standard 61850-7, August 2010.

[7] *Common Information Model: Energy management system application program interface,* IEC Standard 61970, December 2013.

[8] *Common Information Model: Application integration at electric utilities - System interfaces for distribution management,* IEC Standard 61968, March 2013.

[9] *Framework for energy market communications,* IEC Standard 62325, February 2005.

[10] A. Ulbig, T. Borsche, and G. Andersson, Impact of Low Rotational Inertia on Power System Stability and Operation, *axXiv preprint arXiv:1312.6435*, 2013.

[11] *Common Information Model: Energy management system application program interface - Part 301: Common information model (CIM) base,* IEC Standard 61970-3-1, December 2013.

[12] *Communication networks and systems for power utility automation: Basic communication structure - Distributed energy resources logical nodes,* IEC Standard 61850-7-420, March 2009.

[13] T. Gruber, *The Encyclopedia of Database Systems,* L. Liu and M.Tamer Ozsu (Eds.), Springer-Verlag, 2009.

[14] *Harmonizing the International Electrotechnical Commission Common Information Model (CIM) and 61850 via a Unified Model: Key to Achieve Smart Grid Interoperability Objectives.* EPRI, Palo Alto, CA, 2010. 1020098.

[15] *IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems,* IEEE Standard 1547, July 2003.

[16] E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders, and C. Muehrcke, "Model-based security metrics using ADversary VIew Security Evaluation (ADVISE)," in *Proceedings of the 8th International Conference on Quantitative Evaluation of SysTems (QEST 2011)*, Aachen, Germany, Sept. 5–8, 2011, pp. 191–200.

[17] E. LeMay, "Adversary-driven state-based system security evaluation," Ph.D. dissertation, University of Illinois at Urbana-Champaign, Urbana, Illinois, 2011.

[18] W3C. (2012) Owl Web Ontology Language guide. [Online]. Available: https://www.w3.org/TR/owl2-overview/

[19] M. Uslar, "Ontology-based integration of IEC TC 57 standards," *Workshop proceedings of the I-ESA 2008 conference,* Fraunhofer IPK Berlin, pp. 31–34, 2008.

[20] R. Santodomingo, J. A. Rodriguez-Mondejar, and M. Sanz-Bobi, "Ontology matching approach to the harmonization of CIM and IEC 61850 standards," *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on.*, pp. 55–60. [Online], October 2010.

[21] R. Santodomingo, S. Rohjans, M. Uslar, J. A. Rodriguez-Mondejar, and M. Sanz-Bobi, "Facilitating the automatic mapping of IEC 61850 signals and CIM measurements," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4348–4355], November 2013.