Towards Adaptive and Proactive Security Assessment for Energy Delivery Systems

Josephine Lamp, Carlos E. Rubio-Medrano, Ziming Zhao and Gail-Joon Ahn
The Center for Cybersecurity and Digital Forensics
Arizona State University
Email: {jalamp, crubiome, zzhao30, gahn}@asu.edu

***Abstract*—Recently, *energy delivery systems* (EDS) have undergone an intensive modernization process that includes the introduction of dedicated cyber-infrastructures for the purposes of monitoring, control, and optimization of resources. While extremely convenient, the introduction of software-based control over computer networks has also opened the door for the exploitation of non-trivial security vulnerabilities by malicious third-parties. As demonstrated by recent incidents, EDS systems worldwide are vulnerable to sophisticated attacks that include a well-thought out combination of strategies at various levels of abstraction. In such a context, a comprehensive solution supporting automated monitoring and assessment, that can assist security officials in effectively preventing and mitigating such attacks, is highly desired. With this in mind, this paper presents an ongoing effort that takes security requirements obtained from existing documents on guidelines and best practices on EDS, and implements a *proof-of-concept* framework based on adaptive and customizable software modules that collect and process security-relevant data for assuring the security of EDS.**

I. Introduction

Energy delivery systems (EDS) include the critical network of processes, electronic devices, and communication and control mechanisms that manage the transport of energy, and are an important asset to the economies of towns, states and countries [1]. In recent years, EDS have been transferring to electronic systems due to the vast opportunities available through the implementation and use of digital technology, such as the increased reliability, flexibility, resilience and efficiency of the system [2]. However, as this automation occurs, along with the great benefits attainable, there are also new threats, i.e., cyberattacks, that may compromise the security of EDS deployments resulting in devastating consequences. As an example, an attack tailored to disrupt the EDS infrastructure of Ukraine took place in December 2015, allowing for attackers to perform a sophisticated multi-stage operation to infiltrate the infrastructure-controlling system of regional electric companies, resulting in severe power outages for multiple hours to an estimated 225,000 customers [3].

To mitigate threats of this kind, organizations such as the U.S. Department of Energy (DOE), the Energy Sector Control Systems Working Group (ESCSWG), the International Electrochemical Commission (IEC), IEEE, North American Electric Reliability Corporation (NERC) and the National Institute of Standards and Technology (NIST), have released documentation and manuals specifying security best practices for EDS systems, as well as regulations and standards that energy distribution organizations need to comply with. As such information may be indeed valuable for properly securing EDS deployments, they are often a lengthy number of pages and contain a wide range of complicated security specifications. As a result, and due to the inherent complexity involved in EDS systems, e.g., the heterogeneity of devices, systems and communication connections, the application and understanding of this information may be difficult to digest for security officers, EDS operators and stakeholders. This serves as a severe drawback, as it can inhibit diverse operators to understand and perform system evaluations such as risk assessment techniques. Furthermore, it is often difficult to determine the potential security consequences that may occur as a result of not implementing or missing a piece of the regulations.

While existing approaches in the literature focus mainly on providing partial solutions for intrusion detection [4], risk analysis [5] and system management [6], it is critical to seek a broader approach for security monitoring and assessment that goes beyond the identification of potential system flaws and threats. To address this eminent challenge, we aim to combine reputable organizational and governmental security requirements, standards and best practices, in order to produce a framework composed of a set of processing modules and tools that can support complex decision making, optimization and evaluation processes to effectively mitigate the consequences associated with potential security vulnerabilities and threats. In addition, we also present our ongoing work in developing a supporting knowledge ontology that intelligently represents security requirements, concepts, EDS system components, and their inter-relationships. Using this ontology, we then provide an illustrative example on how to effectively leverage the knowledge extracted from the aforementioned sources using our framework, in such a way that a security assessment and mitigation analysis can be carried out to prevent the successful deployment of attacks such as the one to the Ukrainian EDS infrastructure mentioned before.

This paper is organized as follows: we start by briefly reviewing some important background topics, along with a running example and some other key considerations for our approach in Section II. Our approach is described in Section III, followed by some related work behind the inspirations for our approach in Section IV. In Section V, we conclude the paper with the future direction of our work.

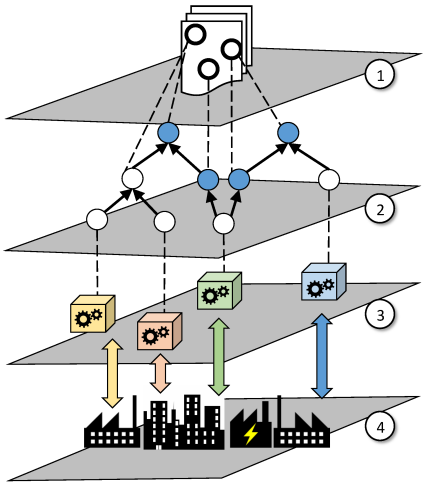

Fig. 1. A multi-layer framework for automated security monitoring and assessment in EDS: documents describing security requirements and best practices for EDS (1) are captured into ontological representations (2), which are later used to create and instantiate dedicated software modules (3) collecting and processing data obtained from EDS infrastructures (4).

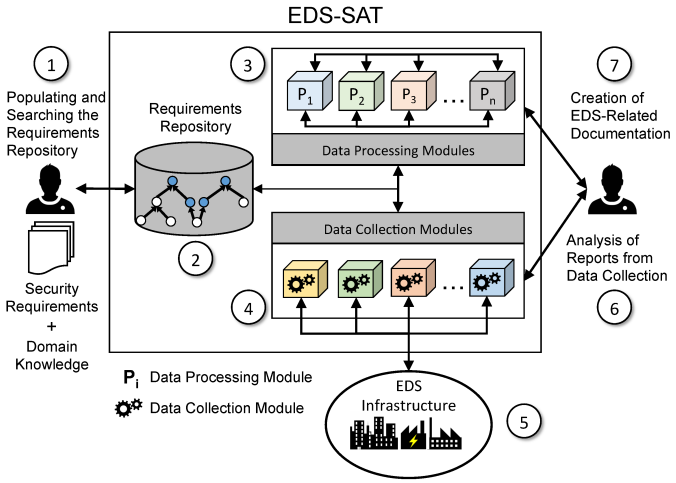

Fig. 2. An architectural depiction of EDS-SAT: domain experts maintain a collection of security requirements (1) of which an ontology repository is built off of (2). Dedicated software modules implement monitoring and assessment tasks (3), leveraging data collected from EDS infrastructures (4, 5). Finally, data and system reports can be analyzed (6) and produced as a result (7).

II. Background

The Ukrainian EDS Attack. The results of successful cyber attacks on EDS infrastructures have had devastating consequences. As mentioned in Section I, a recent attack on the EDS cyber-infrastructure deployed in Ukraine [3] allowed for hackers to perform a multi-stage operation over the span of several months that ultimately resulted in infrastructure-controlling systems being completely manipulated in a remote way from an undisclosed location. For such a purpose, the attackers used multiple attack *vectors*, including malware, credential harvesting, and spear phishing, ultimately resulting in a case of *denial of service* (DoS). Afterwards, multiple security vulnerabilities were identified as the root cause that allowed for the attack to be successfully performed, including the lack of *two-factor authentication* between the business network and the *virtual private network* leading to the *industrial control system* (ICS), as well as a lack of continuous monitoring for abnormalities within the ICS network, which included a remote access permission through a firewall.

III. Our Approach: Security Assessment for EDS

As introduced in Section I, the protection of EDS is dependent on the supporting software, external devices, users, along with the correct implementation of security best practices, as well as the continuous monitoring of the state of the system and its operations. This includes a strong understanding of security requirements, guidelines and standards outlined in reputable governmental and organizational documentation that define high quality policies of service and trust, and a supporting implementation that offers an accurate view and awareness of the current state of the system. With this in mind, we propose an approach for a multi-layer framework that can support complex decision making, system optimization and evaluation efforts of current system security measures in order to effectively mitigate the consequences associated with potential security threats. The components of such a framework are realized in four connected layers as depicted in Fig. 1. Layer 1 contains the most relevant documentation on security best practices within EDS and large heterogeneous systems. These documents are then be combined and summarized intelligently into an ontological representation (Layer 2) in order to create well-defined representations that serve as the supporting knowledge structures for our approach. The ontology shown in Fig. 3. will be further described later in this section. Building on top of such ontology, an extensible framework that supports different software modules to handle system monitoring and automated security assessment will be developed as depicted in Layer 3. Finally, real-time data originating directly from the EDS infrastructure are collected and fed to the supporting software modules, to ensure dynamic views of the system and to be used in module processing to facilitate user decisions based on accurate current system states (Layer 4). Fig. 2 illustrates the proposed architecture of a software implementation of the multi-layered framework shown in Fig. 1, coined the EDS Security Assessment Tool (EDS-SAT).

In this section, we further describe how our ontology models the knowledge contained within EDS documentation, which combines it into a coherent and comprehensive representation. In addition, we also discuss use cases that leverage our proposed framework for meeting the goals described earlier in this paper. Finally, we exemplify a scenario in which our approach can be used to perform a comprehensive security assessment including identifying, analyzing and mitigating system vulnerabilities and related risks associated with attacks such as the one affecting the EDS infrastructure in Ukraine as discussed in Section II.

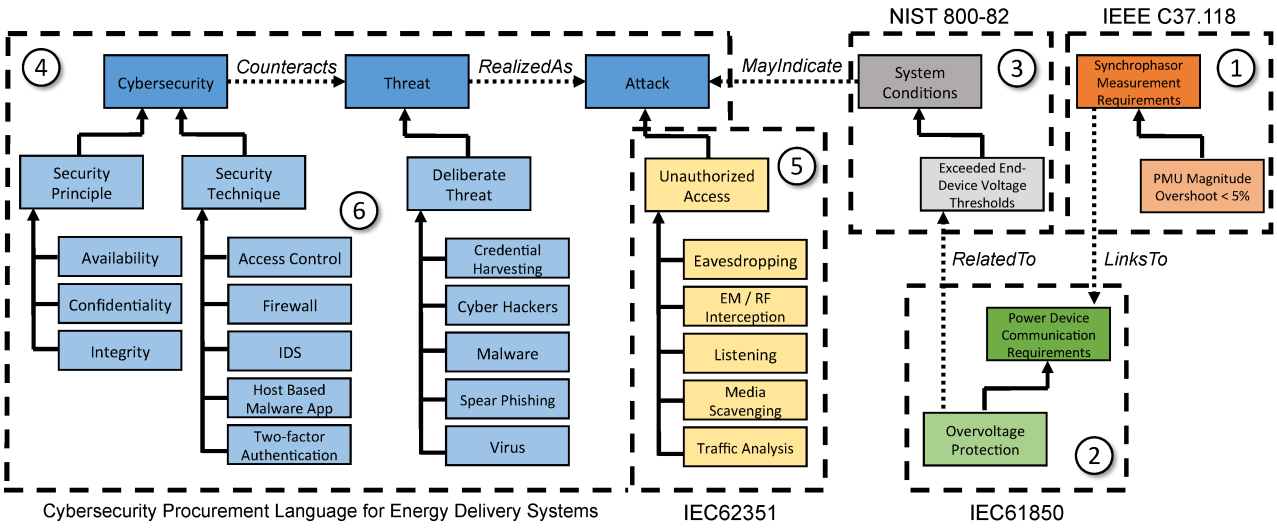

Fig. 3. A partial depiction of our ontology based on several documents from multiple domains, containing system and security requirements for EDS.

A. An Ontology for EDS Cybersecurity

Methodology. Towards the development of our ontology, important high level entities identifying key players in the EDS and cybersecurity domains were constructed, along with the defining links that relate these entities to one another, following the Onto-ActRE methodology described in [7], which defines a systematic process to effectively model and incorporate diverse contexts including technical and nontechnical factors involved within a software-intensive system. We also leveraged *natural language processing* (NLP) [8] techniques for automated document processing. As an example, Fig. 3 depicts a scenario in which different EDS entities including attacks, threats, cybersecurity concepts and system conditions are represented as ontological constructs. In such a case, the larger parent categories, e.g., *Threat* and *Power Device Communication Requirements*, are broken down into subtypes and specializations such as subcategories of threats for the former and overvoltage power requirements for the latter.

Documents Included. We selected the *Cybersecurity Procurement Language for Energy Delivery Systems* [1] published by the Energy Sector Control Systems Working Group (ESCSWG) to serve as the primary reference for the base level of knowledge contained within our ontology, due to its comprehensive and detailed coverage of a wide range of security features and techniques, that would act as a good foundation knowledge structure to expand with the inclusion of other documents. In subsequent steps, we are in the process of modeling additional documents such as the IEC 62351 standard [9], the NIST 800-82 special publication [10], the electrical engineering domain documents of the IEC 61850 standard [11] and the IEEE C37.118 standard [12]. These documents include a total of over 1260 pages in length, ranging in size from 30 to 600 pages each, and contain different system scopes, focuses, purposes and security requirements. The information extracted from these documents is systematically represented within our ontology, a subset of which is illustrated in Fig. 3. It eventually helps EDS engineers to overcome difficulties in synthesizing and comprehending such diverse documents. Moreover, as a validation step, we plan to receive industry and EDS stakeholder feedback on the relevance of the inclusion of such documents, as well as suggestions to additional documentation to be added, to expand the ontology's breadth and applicability.

B. Intended Use Cases

Knowledge Representation and Understanding. Our proposed framework is aimed to support the knowledge representation and understanding of EDS system components, attacks, threats and vulnerabilities contained within a given EDS system, along with security techniques and countermeasures. As an example, an end-user, i.e., a security officer, should be allowed to leverage our proposed ontology to gain an understanding of any applicable documentation, standards and security measures. Potential results may include a description of system components along with attainable security measures, relations between security principles, and their corresponding security techniques, as well as relations between security documents, and the EDS components and techniques that may be covered by them.

Data Collection and Monitoring. In addition, as mentioned in Section III, real-time data are collected from EDS infrastructures to provide a view of the current system state by recurring to a combination of both command input/output as well as physical data, i.e., sensor data. In this way, we aim to identify potential vulnerabilities and threats that may be unknown to end-users beforehand, specifically by comparing such current state against the directives specified by the security requirements included within our proposed ontology. As an example, a dedicated collection module such as the one depicted in Fig. 2 (4) is designed to gather data directly from EDS field deployments. Later, such data are forwarded to a processing module as shown in Fig. 2 (3) that compares it against a set of rules depicting acceptable ranges of values

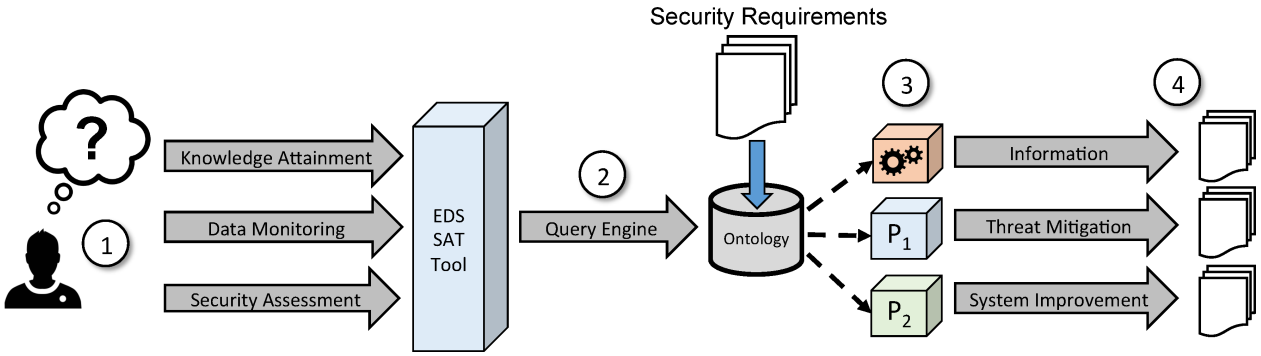

Fig. 4. A detailed depiction of our proposed framework: a stakeholder request is translated into a SPARQL query (1), which is then run against our proposed ontology repository (2). Based on the pulled results, a set of collection and/or processing modules, as described in Section III and Fig. 2, are set to run (3), thus allowing for the generation of relevant information for the user, which is then returned back in an appropriate format, e.g., a description of relevant system components, security principles, solutions to mitigate threats, and/or ways to improve the EDS system (4).

for correct operation, raising a security alert if improper values are found. Such rules are expected to be extracted from the security requirements contained in our ontology. As an example, following requirements contained within the NIST 800-82 standard, network communication between EDS devices can also be monitored to avoid unintended inter-device communication, e.g., network packets flowing from *intelligent electronic devices* (IEDs) to *programmable logic controllers* (PLCs) can be intercepted to prevent the former from being used as an attack vector to compromise the latter.

Security Assessment and Mitigation. Furthermore, our proposed framework is also utilized to perform an assessment of security within EDS by relating system risks, threats and vulnerabilities with system components, along with how such threats can be mitigated through the implementation of security techniques or principles. Moreover, leveraging the collection of real-time data within a given EDS deployment, a proper analysis of the current state of the system with respect to requirements and risks can be better obtained, allowing for subsequent mitigation techniques to be developed. As an example, a dedicated processing module, such as the one depicted in Fig. 2 (3), evaluates the most susceptible areas of the system by applying additional risk analysis methodologies that use the information pulled from our proposed ontology and leveraging well-established techniques such as the *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (OCTAVE) criteria [13]. In this way, the assignment of criticality scores to entities contained within the ontology such as system components and potential threats can be used to help identify the most susceptible areas of the system as well as to help in the determination of the trade-offs of implementing specific security techniques for mitigation.

Collaborative Development. Fig. 4 presents a sample scenario depicting how a security officer or system stakeholder starting with a specific goal in mind can leverage our proposed approach, generally aligned with the three use cases described before. As mentioned in Section III, we envision our framework supporting the development of software modules that implement automated monitoring and assessment techniques, which can then be customized to work with the specific settings of particular EDS deployments, e.g., network and EDS device configurations. Such modules should correspond to either well-known or experimental security techniques, as the ones depicted in Fig. 3. We also envision their creation as a collaborative effort within the EDS community, allowing for our framework (and our proposed ontology) to serve as a common foundation for designing, developing, testing and sharing solutions over time, in such a way that common vulnerabilities and threats within the community can be better addressed and solved. For such a purpose, our proposed ontology may be used as a common reference to locate security requirements, e.g., detection and response to threats and attacks, that need to be addressed by allowing partners to leverage existing or future processing modules.

C. A Sample Scenario: the Ukrainian EDS Attack

In order to exemplify the usefulness of our approach and its applicability towards supporting the goals described in this paper, we demonstrate a sample progression and application of our framework within real-life scenarios before and after an attack as the one mentioned in Section II, has occurred.

Pre-Attack Scenario. In order to aid in prevention of large-scale attacks, our framework may be used to perform a security assessment by utilizing views of the current system state, which may be in turn obtained from data returned by data collection modules, thus helping to identify potential security vulnerabilities. For example, within an EDS infrastructure such as the one in Ukraine, our framework may be leveraged as follows: initially, a data collection module, such as the ones depicted in Fig. 2 (4), obtains data from different areas of the grid and compares the measurements to expected thresholds amalgamated from security and electrical engineering requirements contained within our proposed ontology. More specifically, the module may receive information that the input step magnitude reported from *phasor measurement unit* (PMU) sensors deployed within the grid is overshot by more than 5%. Pulling a requirement from the IEEE C37.118 standard, the module identifies this as an improper value, as according to such security requirement, the magnitude should not be overshot by more than 5%.

As a result, an alert is raised and the potential security consequences e.g., the different types of attacks, of such an abnormally high value may be investigated by referring back to our ontology repository. Starting at the aforementioned requirement specified in the IEEE C37.118 standard, our proposed query engine traverses links in the ontology to identify and return the *Unauthorized Access* attack entity. Later, from the IEEE requirement shown in Fig. 3 (1), the query engine follows links to the IEC 61850 standard that identifies PMUs as logical nodes and specifies overvoltage protection requirements (Fig. 3 (2)). Such requirement is in turn related to the NIST 800-82 special publication that states exceeded voltage thresholds may indicate an attack, as shown in the connection to the *System Conditions* entity displayed in Fig. 3 (3), which is then linked to the *Cybersecurity Procurement Language for Energy Delivery Systems* document (Fig. 3 (4)) that provides the general *Attack* entity. Finally, our proposed engine follows the *Attack* entity down into its sub-entity of the *Unauthorized Access* attack type, as specified by the IEC 62351 standard, shown in Fig. 3 (5).

After the identification of such attack type, a risk analysis appraisal may be performed by utilizing another processing module in the context of our proposed framework. As an example, the previously mentioned OCTAVE risk analysis methodology provides a general approach that can identify, assess and manage security risks within a system, but does not come with its own tools or specific methods in order to enact the risk analysis criteria [6]. Therefore, our framework can be used to provide the tools necessary for performing such a risk analysis process. To start, critical system components are identified by allowing our query engine to retrieve requirements and system specifications following the link traversal approach discussed before. For example, our query engine may return the following requirements: the IEC 61850 standard elucidates communication and performance requirements related to important end devices including PLCs and IEDs, and similarly the NIST 800-82 describes PLCs and IEDs as key EDS system components and gives cybersecurity requirements related to their protection. As such, PLCs and IEDs would be identified as critical system components.

Later on, by utilizing the information learned about the system state (through our framework's system monitoring capabilities), vulnerabilities can be identified following the OCTAVE criteria. For example, after the abnormally high PMU value was identified as potentially indicative of an attack, a processing module within our framework may then compare network configuration settings from the actual system to the expected configurations depicted in requirements documentation such as the *Cybersecurity Procurement Language for Energy Delivery Systems* and identify differences in the ICS network permissions that imply system vulnerabilities. In this way, our framework may aid in the identification of an improper permission configuration that allows remote access accessible through the firewall, among other vulnerabilities including the lack of two-factor authentication in the connection between the VPNs into the ICS from the business network, as well as the lack of continuous monitoring of the ICS network, all of which caused the afore-mentioned attack in Ukraine, as mentioned in Section II. Finally, synthesizing the previous information, and fulfilling the guidelines defined by the OCTAVE criteria, a strategic plan can be developed to mitigate the potential risks associated with each vulnerability. Using our framework as an auxiliary tool, as shown in in Fig. 2 (6, 7), a strategic list of steps for the implementation of security phases will be developed, thus potentially preventing a large-scale attack such as the one that occurred in real life.

Post-Attack Scenario. Following the use cases described in Section III-B, our framework can be also used to mitigate the consequences after an attack has occurred by gaining a better understanding of the specific, related threats and security measures that may serve as proper response techniques. For example, in the case of the Ukraine attack, *Unauthorized Access* (as shown in Fig. 3), was identified as an important vector that allowed for the attack to take place. With this in mind, information can be obtained from our proposed ontology describing the deliberate threats that may be realized from such an attack type. Leveraging our query engine once again, exploration of our requirements ontology may include the entities of *Credential Harvesting*, *Cyberhackers*, *Malware*, and *Spear Phishing*, among others, all of them representing key threats to the EDS infrastructure. Later on, a subsequent query processed by our engine may include the specific techniques that may counteract such threats, returning a long list of entities including *Firewall*, *IDS*, and *Two-factor Authentication* as depicted in Fig. 3 (6). By referring to our approach, and by implementing the aforementioned techniques, EDS infrastructures may be better protected from future attacks utilizing similar vectors.

IV. Related Work

Intrusion Detection. Recently, several solutions depicting *intrusion detection systems* (IDS) for EDS have been introduced in the literature. As an example, Koutsandria et al. [4] presented an approach to handle a combination of both cyber-based data, e.g., network packets depicting command input/output, as well as physical data, i.e., field measurements, obtained from EDS devices. While extremely convenient to detect attacks disturbing the operation of EDS infrastructure, their approach lacks a well-defined foundation for obtaining and enforcing security requirements, e.g., network monitoring rules and data range values, such as the one we have proposed by means of our ontological repository. In addition, combing IDS and ontology modeling, Krauß and Thomalla [14] developed an approach linking networks, system components, security events, attack types and vulnerabilities drawn from IDS alerts. The combination of an ontology and IDS is similar to the ideology of our framework as described in Section III. However, our framework takes a broader approach, in which the use of exploration techniques within our query engine, as well as the use of multiple monitoring and processing modules can provide support for meeting a larger variety of security requirements applicable to a wide range of EDS systems.

Security Assessment. In terms of security assessment and risk analysis, Jauhar et al. [5] developed a security assessment model that utilized failure-scenarios developed by the US National Electric Sector Cybersecurity Organization Resource (NESCOR), originally documented to identify threats to smart grid systems. Such a model was also used as a risk analysis tool to assess smart grid system risks by generating argument graphs to visually represent each attack scenario based on the integrated information contained within their model. Similarly, Anwar et al. [15] developed a framework that models elements of an electric power grid using predicate logic and performs assessment of the system based on attack graphs by determining if potential anomalies indicate a high risk security problem. Although our approach can also be leveraged to implement risk analysis based on attack scenarios as the ones just discussed, we are proposing a broader framework in which various security assessment techniques, as well as data collection strategies, can be integrated through additional processing modules, such that our framework can be adapted to meet the needs of a diverse set of EDS infrastructures.

V. Conclusions and Future Work

In this paper, we have presented our ongoing efforts towards developing an ontology from a set of documents covering a diverse range of domains, along with a set of collection and processing modules that use real-time data to provide insight on the system state, all incorporated within the framework to aid in knowledge attainment, monitoring, security assessment and mitigation based on EDS operator requests. This way, our approach provides effective means for representing multiple security requirements, at the same time it supports the better assessment of vulnerabilities and incidents, which can eventually lead to the detection of damaging attacks, as well as the deployment of proper countermeasures as a response. Whereas the illustrative discussions in this paper were mostly based in electrical EDS infrastructure, we believe our approach can be easily extended to cover other areas within the EDS spectrum, namely the gas and oil industries, among others. As of today, we are working towards enhancing our ontology presented in Section III. In addition, we are constructing a chain of toolkits depicted in Fig. 2, which will allow for EDS engineers to develop their own processing modules to leverage existing and newer functionality for better security-related analysis and decision making. Future work will be also directed towards enhancing our query engine to include *state-of-the-art* techniques for ontology exploration and analysis. Finally, we plan to evaluate our approach including a set of attack scenarios, as well as a monitoring and collection infrastructure for both cyber-based and physical data, in an effort to provide tangible evidence of the suitability of our approach for effectively assessing the security of EDS deployments.

Acknowledgment

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780.

Disclaimer

References

[1] Energy Sector Control Systems Working Group (ESCSWG), "Cybersecurity Procurement Language for Energy Delivery Systems," April 2014. [Online]. Available: https://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

[2] U.S. Department of Energy, "2014 Smart Grid System Report," August 2014. [Online]. Available: http://energy.gov/sites/prod/files/2014/08/f18/SmartGrid-SystemReport2014.pdf

[3] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the ukrainian power grid," *SANS ICS Report*, 2016.

[4] G. Koutsandria, R. Gentz, M. Jamei, A. Scaglione, S. Peisert, and C. McParland, "A real-time testbed environment for cyber-physical security on the power grid," in *Proc. of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*, ser. CPS-SPC '15. New York, NY, USA: ACM, 2015, pp. 67–78.

[5] S. Jauhar, B. Chen, W. G. Temple, X. Dong, Z. Kalbarczyk, W. H. Sanders, and D. M. Nicol, "Model-based cybersecurity assessment with nescor smart grid failure scenarios," in *IEEE 21st Pacific Rim International Symposium on Dependable Computing (PRDC)*. IEEE, 2015, pp. 319–324.

[6] S.-W. Lee, R. A. Gandhi, and G.-J. Ahn, "Certification process artifacts defined as measurable units for software assurance," *Software Process: Improvement and Practice*, vol. 12, no. 2, pp. 165–189, 2007.

[7] S. W. Lee and R. A. Gandhi, "Ontology-based active requirements engineering framework." in *APSEC*, 2005, pp. 481–490.

[8] G. G. Chowdhury, "Natural language processing," *Annual review of information science and technology*, vol. 37, no. 1, pp. 51–89, 2003.

[9] International Electrochemical Commission, "IEC TC57 WG15: IEC 63251 Security Standards for the Power System Information Infrastructure," June 2012. [Online]. Available: http://www.iec.ch/smartgrid/standards/

[10] NIST, "NIST Special Publication 800-82 Revision 2 Guide to Industrial Control Systems (ICS) Security," May 2015. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[11] International Electrotechnical Comission (IEC), "Core IEC Standards," 2017. [Online]. Available: http://www.iec.ch/smartgrid/standards/

[12] IEEE, "C37.118.1-2011 - IEEE Standard for Synchrophasor Measurements for Power Systems," 2017. [Online]. Available: https://standards.ieee.org/findstds/standard/C37.118.1-2011.html

[13] C. Alberts and A. Dorofee, "Octave-the operationally critical threat, asset, and vulnerability evaluation," *Canegie Mellon University–Software Engineering Institute*, 2001.

[14] D. Krauß and C. Thomalla, "Ontology-based detection of cyber-attacks to scada-systems in critical infrastructures," in *Digital Information and Communication Technology and its Applications (DICTAP), 2016 Sixth International Conference on*. IEEE, 2016, pp. 70–73.

[15] Z. Anwar, R. Shankesi, and R. H. Campbell, "Automatic security assessment of critical cyber-infrastructures," in *IEEE International Conference on Dependable Systems and Networks With FTCS and DCC (DSN)*. IEEE, 2008, pp. 366–375.