Toward Automated Enforcement of Cyber-Physical Security Requirements for Energy Delivery Systems

Carlos E. Rubio-Medrano
Texas A&M University-Corpus Christi
carlos.rubiomedrano@tamucc.edu

Ziming Zhao
University at Buffalo
zimingzh@buffalo.edu

Gail-Joon Ahn
Arizona State University and Samsung Research
gahn@asu.edu

***Abstract*—The innovation and advances in power delivery and information technologies are bringing unmatched changes to energy delivery systems (EDS), automating the management and administration of mission-critical infrastructures, such as the power grid, the oil, and gas industries. While the benefits of these changes are unparalleled, cyberattacks at EDS are also at unprecedented levels, which may lead to consequences ranging from power outages to homeland security breaches. To securely connect and integrate large quantities of these components, the energy community has proposed roadmaps to update the way to plan and operate EDS. These roadmaps come with security requirements that specify the best practices along with regulations EDS and utility should comply with. However, there is a huge gap between these requirements and the actual enforcement. In this paper, we envision a framework that automates the security requirement enforcement so that natural language policies can be enforced without human intervention and with high confidence.**

***Index Terms*—energy delivery systems, automated requirement enforcement, ontologies**

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 are an important asset to the economies of towns, states and countries. 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 [1]. While the benefits of these changes are unparalleled, cyberattacks at EDS are also at unprecedented levels, which may lead to consequences ranging from power outages to homeland security breaches. In recent years, multiple attacks against EDS have occurred, including the Kyivoblenergo and the Prykarpattyaoblenergo attacks (2015) [2] and the Ukrenergo transmission station attack (2016) [3]. Moreover, there have been recent concerns that foreign actors may be already launching a series of attacks over EDS infrastructures in the United States and Europe [4]. As a response, and to ensure EDS are built on a trustworthy and secure foundation, the "Securing Energy Infrastructure Act" (S.174, 2019) highlights the need for urgent actions on EDS security [5].

Unfortunately, securing EDS is challenging and still has a long way to go. For instance, the cyber components of most EDS end devices, including distributed energy sources, are connected to grid operators via public internet channels. And, they typically do not support basic encryption or other security features due to limited processing capabilities. To securely connect and integrate large quantities of these components, the energy community has proposed a series of roadmaps, including the Cybersecurity Procurement Language for Energy Delivery Systems (CPLEDS) [1], published by the Energy Sector Control Systems Working Group (ESCSWG), the IEC 62351 standard [6], the NIST 800-82 special publication [7], the NERC Critical Infrastructure Protection (CIP) standards [8], the NISTIR 7628 smart grid guideline [9], the IEC 61850 standard [10], the IEEE C37.118 standard [11], among others. These roadmaps come with security requirements that specify the best practices along with regulations EDS and utility should comply with. Also, standards for new functions are also being updated on a national level through IEEE 1547/IEEE 1547.1, and they have been implemented in some state interconnection standards, including California and Hawaii [12] [13]. However, there is a huge gap between these requirements and the actual enforcement for the following reasons:

1) *Lack of formalization in security requirements.* Various organizations have released, potentially conflicting, documents specifying a series of security requirements. These documents are difficult for humans and machines to understand in that they are lengthy in natural language. That may ultimately result in subjective interpretations, non-standard implementations, and breakdowns among stakeholders;
2) *Impossible to enforce all requirements due to the complexity and conflicts.* EDS are diverse and complex with many components and configurations, it is usually impossible to enforce all the security requirements. Hence, it is imperative to design an approach to automatically identify the requirements that should be enforced with the highest priority. This consideration should take the requirements, vulnerabilities, and system status into account;
3) *Difficult to enforce due to the heterogeneous nature of EDS systems.* The distributed and highly-interconnected EDS include many different monitoring sensors, meters, and software systems from different vendors. It is difficult to implement a consolidated enforcement strategy as each device may support different paradigms and techniques.

Nevertheless, it is evident that security requirement enforcement is of great importance for EDS and utility to better detect, withstand and respond not only hazardous but also intentional

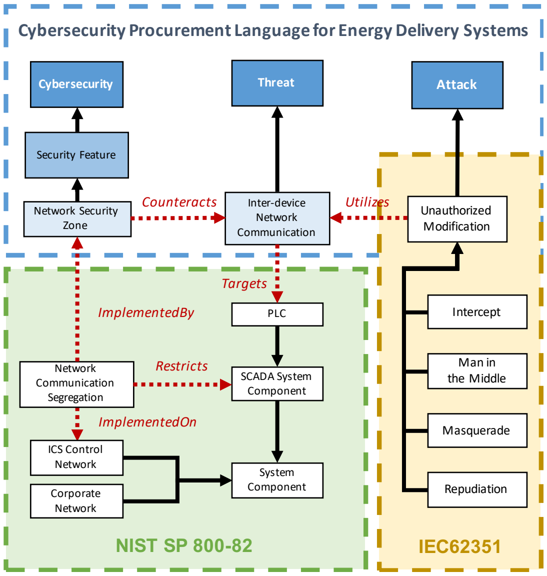

Fig. 1. An Ontology Depicting a Series of Documents for EDS [1], [6], [7].

attacks from both physical and cyber surfaces. In this paper, we envision a framework that automates the security requirement enforcement so that natural language policies can be enforced without human intervention and with high confidence. Our framework consists of 3 inter-dependent components:

1) Formalizing Cyber-Physical Security Requirements of EDS. The component includes novel approaches to extract and translate security requirements from natural language documents and provision them in a structural way; 2) Automating Data-driven Cyber-Physical Risk Assessment. The module has an automated risk assessment framework that combines security requirements from the ontology-based repository and real-time monitoring data from EDS; 3) Automatically Enforcing Security Requirements in EDS. This component include new designs and implementations of automated and provable enforcement mechanisms for security requirements at the network and device layers of EDS.

II. Formalizing Cyber-Physical Security Requirements of EDS

Security requirements for EDS are buried in many dense and lengthy documents, which are in different natural language styles. Also, the documents may present contradictory recommendations. Therefore, there is a need to automatically model, mine and synthesize such security requirements from multiple and potentially contradictory sources so that they can be presented in a structural way. To solve this issue, we will develop an automatic security requirement mining approach for locating, processing, and conflict-solving security requirements. The output is a consolidated, structural and ontology-based security requirement repository [14]–[17]. An example, featuring security requirements extracted from three source documents for the protection of programmable logic controllers (PLCs), is shown in Figure 1. As shown in Figure 2, our approach has the following modules:

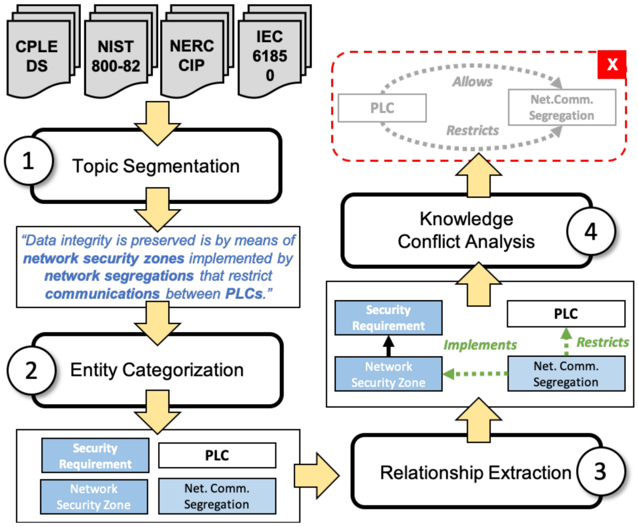

Fig. 2. Automatic Security Requirement Mining.

1) Document Collection. We will develop a web crawler to continuously collect relevant documents from reputable organizational sources in the EDS community, such as IEEE, NIST, NISTIR, IEC, and NERC, for instance [1], [6]–[11].
2) Topic Segmentation. In these documents the security requirement descriptions are usually interleaved with other unrelated discussions. To extract the security requirement sentences and paragraphs, we will design a multi-document long short-term memory (LSTM) approach for topic segmentation.
3) Entity Categorization. Within each source text, different synonyms and technical jargon are often used to refer to key entities relevant in the EDS context, e.g., cyber-physical devices and security techniques. We will design a morphology lexical semantics approach that not only synthesizes different forms used to refer to each entity among several source documents, but also categorizes and inserts the resulting standardized representation into its corresponding place within our ontology [18].
4) Relationship Extraction. The entities discovered in the previous step are related to each other by means of different action verbs scattered all over the source text. To address this, we will develop an approach for sentence-level relation extraction that employs convolutional neural networks (CNN) to embed the semantics of action verbs, allowing for standardizing relationships and automatically linking them to different sets of entities [19].
5) Knowledge Conflict Analysis. We will develop an approach that depicts a set of semantic pattern matching rules for discovering, evaluating, and eventually selecting or pruning conflicting entities and/or relationships [20].

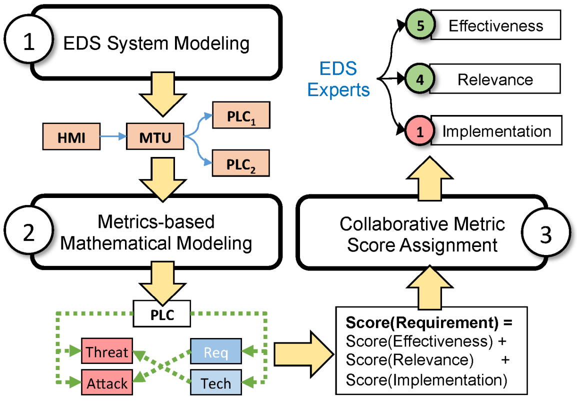

Fig. 3. Requirements-based Risk Assessment.

III. Automating Data-driven Cyber-Physical Risk Assessment

Because EDS are diverse and complex with many heterogeneous components and configurations [21], it is usually impossible to enforce all the security requirements. Hence, it is imperative to design an approach to automatically identify the requirements that should be enforced with the highest priority. This consideration should take the requirements, vulnerabilities, and system status into account. With that in mind, we propose an approach for the assessment of security risks for EDS that evaluates: i) the impendence and severity of threats and attacks targeting EDS; ii) the effectiveness and the quality of the implementation of any counteracting security requirements; iii) the input of experts in the EDS community [22]. Our approach, featured in Figure 3, will be composed of the following modules:

1) EDS System Modeling. The first step in our approach will include the construction of an abstract model that can accurately capture the topology and architectural design of EDS instances for risk quantification. That will include information about the functional relationships between devices within an EDS instance, which may be useful to understand how the risk of a specific device may be impacted by other devices it is related to. As an example, following Figure 3 (1), an MTU has a functional relationship with two PLCs, as it sends control commands to them, and receives data from them.
2) Metrics-based Mathematical Modeling. Using such information as an input, we will develop a set of metrics that characterize the likelihood, applicability and impact of threats and attack vectors, allowing for their accurate and comprehensive quantification. Conversely, we will develop metrics for measuring the effectiveness, relevance and the quality of implementation of security requirements and features. For each of these metrics, we will develop different numerical scoring schemes, which can accurately reflect both objective and subjective perceptions, as given by EDS practitioners, for each metric featured by our approach. Finally, we will define a set of mathematical formulations that combine the aforementioned scores along with the system modeling and functional relationships of an specific EDS instance, to obtain a quantifiable, comparable description of the current security state of an EDS device or subsystem.
3) Collaborative Score Assignment. We will introduce a platform for a collaborative ecosystem that supports the quantification of risk by providing an interconnected, live, community-based score tabulation scheme for the metrics described before, allowing for the EDS community to collaboratively decide on these scores and ranges based on changes in the threatscape and their expertise, resulting in standardized calibrated scores and accurate risk score calculations.

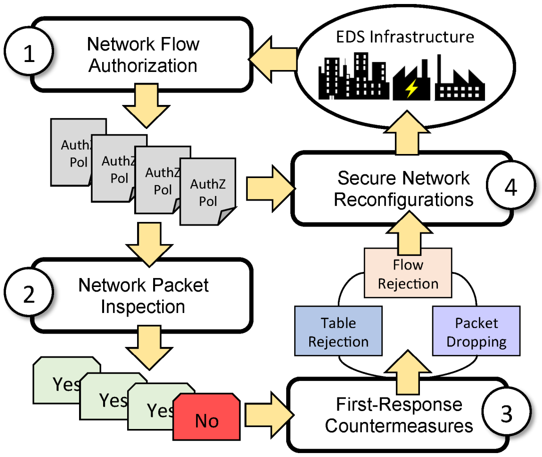

Fig. 4. Enforcing Security Requirements for EDS Networks with SDN.

IV. Automatically Enforcing Security Requirements in EDS

The effective protection of EDS depends on the correct enforcement of security requirements at the implementation level, as well as the continuous monitoring of the state of the system and its operations, However,, enforcing security requirements for EDS is difficult due to the existence of a variety of legacy cyber-physical systems, which typically come from different vendors and suppliers with a variety of configuration methodologies and techniques, and may not support security requirement enforcement directly and cannot be updated to do so. To solve this problem, we will develop a framework for enforcing security requirements for EDS at the network level, thus overcome the limitations at the device and system levels. Our approach, shown in Figure 4, incorporates software defined networking (SDN) [23] for network administration:

1) Network Flow Authorization. First, we will leverage the SDN paradigm to enforce a series of authorization policies restricting the set of communication flows between cyber-physical devices and sub-systems. As an example, authorization policies will restrict the network traffic from the Control to the Business sub-networks and vice versa within an EDS network, thus preventing any compromised hosts

within the Business sub-network from eventually reaching EDS devices.

2) Network Packet Inspection. We will design approaches for detecting anomalies in the direction and the their inner contents of network packets implementing the Modbus [24] and link layer protocols, such as ARP, which can be potentially abused for command or data injection attacks to EDS devices.
3) First-Response Countermeasures. Also, we will implement a series of first-response strategies to proactively react and reduce the impact and consequences of ongoing attacks to EDS networks. Such strategies include: i) rejecting the installation of new unauthorized communication flows in SDN-enabled switches; ii) rejecting any changes in the SDN network flow tables that may ultimately result in changes in the communication flows; and, iii) blocking anomalous network packets by instructing SDN-enabled switches to drop them from the network.
4) (4) Secure Network Reconfigurations. Finally, we will provide support for the prevention of future security vulnerabilities that arise from reconfigurations of the EDS network, e.g., the introduction of new communication flows between devices as a response to physical changes/emergencies within the EDS infrastructure. As an example, our approach will maintain the consistency between the flow authorization policies defined in Step 1 and the flow tables implemented by SDN-enabled switches, dropping new flows that happen to violate a rule in such a policy and preventing any modifications to the flow table entries. In addition, every time the flow table entries at switches are reconfigured, our approach will reject any changes that may introduce flows not authorized by an authorization policy.

V. Conclussions

In this paper, we have presented our vision towards the automated enforcement of security requirements in the context of EDS. Starting with an ontology from a set of documents followed by a set of collection and processing modules that use real-time data, a proper solution for knowledge attainment, monitoring, security assessment and mitigation is proposed. 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 and prevention of damaging cyberattacks, as well as the deployment of proper countermeasures.

References

[1] Energy Sector Control Systems Working Group (ESCSWG), "Cybersecurity Procurement Language for Energy Delivery Systems," April 2014.

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

[3] Dragos, Inc., "CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations," tech. rep., Dragos, Inc., 06 2017.

[4] The New York Times, "Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says." https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html, March 2020.

[5] A. S. King, "S.174 - Securing Energy Infrastructure Act." https://www.congress.gov/116/bills/s174/BILLS-116s174rs.pdf, 2019.

[6] International Electrochemical Commission, "IEC TC57 WG15: IEC 63251 Security Standards for the Power System Information Infrastructure," June 2012.

[7] NIST, "NIST Special Publication 800-82 Revision 2 Guide to Industrial Control Systems (ICS) Security," May 2015.

[8] North American Electric Reliability Corporation, "Critical Infrastructure Protection Standards," March 2019.

[9] National Institute of Standards and Technology, "NISTIR 6828 Rev. 1: Guidelines for Smart Grid Security," September 2014.

[10] International Electrotechnical Comission (IEC), "Core IEC Standards," 2017.

[11] IEEE, "C37.118.1-2011 - IEEE Standard for Synchrophasor Measurements for Power Systems," 2017.

[12] S. Chakraborty, "Making ieee std. 1547 fit for the future," tech. rep., National Renewable Energy Lab.(NREL), Golden, CO (United States), 2017.

[13] M. Ingram, D. J. Narang, B. A. Mather, and B. D. Kroposki, "Supplemental information for new york state standardized interconnection requirements," tech. rep., National Renewable Energy Lab.(NREL), Golden, CO (United States), 2017.

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

[15] J. Pullmann, N. Petersen, C. Mader, S. Lohmann, and Z. Kemeny, "Ontology-based information modelling in the industrial data space," in *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pp. 1–8, 2017.

[16] J. Lamp, C. E. Rubio-Medrano, Z. Zhao, and G.-J. Ahn, "The danger of missing instructions: A systematic analysis of security requirements for mcps," in *Connected Health: Applications, Systems and Engineering Technologies: CHASE-MedSPT2018, the IEEE/ACM 3rd International Conference on*, p. 6, ACM/IEEE, September 2018.

[17] A. M. Shaaban, C. Schmittner, T. Gruber, A. B. Mohamed, G. Quirchmayr, and E. Schikuta, "Ontology-based model for automotive security verification and validation," in *Proceedings of the 21st International Conference on Information Integration and Web-Based Applications and Services*, iiWAS2019, (New York, NY, USA), p. 73–82, Association for Computing Machinery, 2019.

[18] B. Levin and M. R. Hovav, *Morphology and Lexical Semantics*, ch. 12, pp. 248–271. John Wiley and Sons, Ltd, 2017.

[19] Y. Lin, S. Shen, Z. Liu, H. Luan, and M. Sun, "Neural relation extraction with selective attention over instances," in *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pp. 2124–2133, Aug. 2016.

[20] J. Zhang and N. M. El-Gohary, "Semantic nlp-based information extraction from construction regulatory documents for automated compliance checking," *Journal of Computing in Civil Engineering*, vol. 30, no. 2, p. 04015014, 2016.

[21] W. Knowles, D. Prince, D. Hutchison, J. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," *Int. journal of critical infrastructure protection*, vol. 9, pp. 52–80, 2015.

[22] T. Cruz, J. Proença, P. Simões, M. Aubigny, M. Ouedraogo, A. Graziano, and L. Yasakhetu, "Improving cyber-security awareness on industrial control systems: The cockpitci approach," in *13th Euro Conf. on Cyber Warfare and Sec.*, p. 59, 2014.

[23] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker, "Ethane: Taking control of the enterprise," in *Conf. on Applications, Technologies, Architectures, and Protocols for Computer Comm. (SIGCOMM '07)*, pp. 1–12, ACM, 2007.

[24] A. Swales *et al.*, "Open modbus/tcp specification," *Schneider Electric*, vol. 29, 1999.