Adaptive and Proactive Security Assessment on Energy Delivery Systems

Website: http://cred-c.org/researchactivity/edssecassess

Researchers (ASU): Carlos Rubio-Medrano, Josephine Lamp, Vu Coughlin, Ziming Zhao, Anna Scaglione, and Gail-Joon Ahn

Industry Collaboration:

- Currently seeking collaborators from industry, power utilities, or national labs. Contact Carlos Rubio-Medrano to discuss how you can engage or collaborate with our research team.
- Lawrence Berkeley National Laboratory
- Pacific Northwest National Laboratory

Description of research activity: Our approach is described as follows: first, we provide support for the creation of dedicated repositories depicting security requirements, which are to be modeled leveraging *ontological* representations, in such a way that an unambiguous and comprehensive description of requirements, as well as common vulnerabilities and exposures (CVEs) (Mitre 2016), is synthesized cohesively. Using ontologies, the relationships between different security concepts can be better modeled, thus allowing for the exploration and discovery of similar and complimentary requirements obtained from different sources. We have identified already a starting collection of documents which we plan to enhance over time as a result of our interactions with both industry and academic partners, in such a way that our requirements repository is effectively constructed from source materials that are deemed as relevant by the EDS and cybersecurity communities.

Second, we introduce an approach based on multi-view analysis (Lee and Gandhi, Ontology-based active requirements engineering framework 2005), to allow for different stakeholders in EDS, who may have different security requirements, to assess the security of EDS based on their unique viewpoints.

Figure 1 presents a graphical depiction, adapted from a previous one (Lee, Gandhi and Ahn, Certification process artifacts defines as measurable units for software assurance 2007), that shows how security officials and system practitioners may obtain different information from a given ontology according to their different points of view, by *traversing* the different relationships, a.k.a., *links*, that are associated with the entities being modeled in a given ontology.

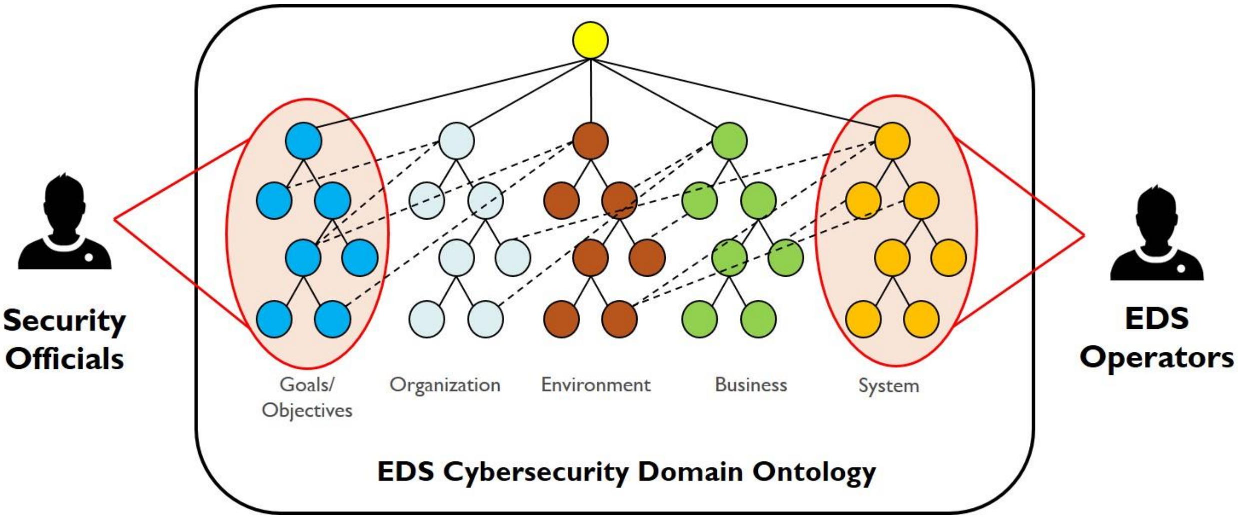

Figure 1. Multiple viewpoints for analyzing security requirements based on ontologies.

Third, even though stakeholders may have different needs and different security requirements, some security requirements may be related and share some common elements. Therefore, it is imperative to analyze the relationship links between different security requirements and extract the required assessment tasks for them, using an approach based on multi-link analysis (Lee, Gandhi and Ahn, Certification process artifacts defines as measurable units for software assurance 2007). As an example, Figure 2 shows a security requirement, derived from different documents on cybersecurity guidelines for EDS, that suggests the implementation of different network security zones, each of them in turn representing its own security domain, in order to restrict network communications between system devices. This way, even when an attacker may have been able to compromise a given component such as an intelligent electronic device (IED), the extent of the attack, as well as its possible consequences, may be contained by preventing other devices within the system from falling under the attacker's control. As suggested by Figure 2 such a requirement may in turn be implemented by a network partitioning strategy. For instance, a set of security-sensitive IEDs in a given EDS setting may be grouped together into a network partition corresponding to a security domain allowing for internal communication, but disallowing any external communication with other partitions, e.g., a partition containing other IEDs. Partitions may be defined beforehand taking into account the system-level purpose of each of its constituent devices as well as the level of trust placed on them. Later in this document, we will describe an approach for enforcing security requirements of this kind by leveraging technologies for network packet collection and analysis, as well as traffic rerouting.

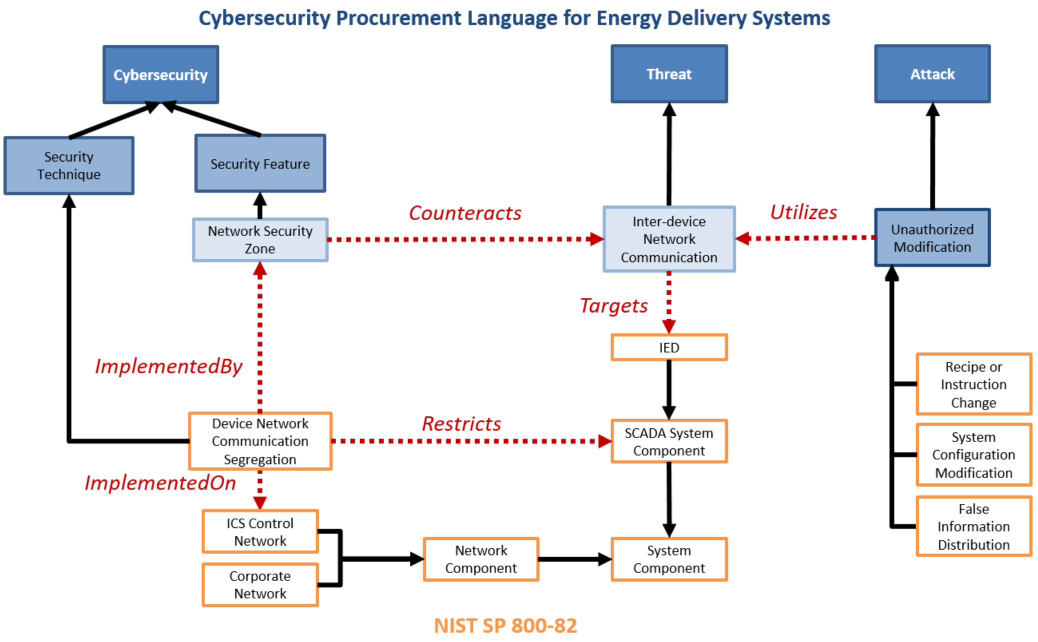
Cybersecurity Procurement Language for Energy Delivery Systems
Cybersecurity
Threat
Attack
Security Technique
Security Feature
Counteracts
Utilizes
Network Security Zone
Inter-device Network Communication
Unauthorized Modification
Targets
IED
ImplementedBy
Recipe or Instruction Change
Restricts
Device Network Communication Segregation
SCADA System Component
System Configuration Modification
ImplementedOn
ICS Control Network
False Information Distribution
Network Component
System Component
Corporate Network
NIST SP 800-82

Figure 2: Multi-link analysis for a security requirement restricting network communications.

Fourth, we will provide support for the automation of different security assessment tasks by introducing an approach based on *process-driven workflows*, which are to leverage the aforementioned multi-view and multi-link analysis. Such workflows are constructed by linking together a series of adaptive and proactive software modules that *collect* security-relevant data directly from EDS, e.g., by intercepting network traffic related to information input/output and command output, as well as modules that are intended to *process* such information for automated security assessment, e.g., by implementing security checks that can detect deviations indicating a potential vulnerability or even an attack being underway.

Within our proposed framework, both *collecting* and *processing* modules will be developed based on the requirements contained within our repository, thus effectively creating a collection of modules from which customized workflows can be later *instantiated* by following the results obtained from running the aforementioned multi-view and multi-link analysis techniques, thus allowing practitioners to dynamically run their own custom-made workflows. As an example, leveraging Figure 2 a security analysis based on our proposed techniques may result in the aforementioned requirement restricting communication between different network partitions enclosing IEDs. Such a requirement may be in turn implemented by a dedicated *interceptor* module that monitors and retrieves network traffic, which is then forwarded to a *checker* module that verifies that the source and destination IP addresses contained in a network packet do not correspond to an attempt to establish a disallowed communication between partitions. If an *offending* packet is found, a security alert can be raised as a result. An alternative technique may also include detecting unexpected or unauthorized protocols, e.g., DHCP in a network environment consisting of static IP addresses only. At runtime, these *interceptor* and *checker* modules may be selected from our module collection to create a dedicated workflow as a result of an analysis that implements the aforementioned requirement restricting network traffic for EDS devices. Since each EDS deployment may exhibit different network configurations with respect to number of devices and IP addresses assigned to them, a previous configuration step may be required before the newly-created workflow can be set to run. In addition, as mentioned above, different monitoring techniques may be implemented to detect violations to a given security requirement. This way, a robust approach may be in place, allowing for security alerts issued by different modules to be combined together and presented to an EDS operator for better decision making, thus potentially preventing false positives, and complicating attacks directed to disrupt our approach by producing misleading input to a specific data collection module.

For the purposes of data collection and forwarding, we will explore how software-defined networks (SDN) (Hu 2014) can be leveraged to observe, control and analyze network packets within EDS. As an example, we have envisioned an approach in which network monitoring rules, expressed in the scripting language of the well-known Bro framework (PAXSON 1999), can be translated into compatible SDN traffic rules and configuration settings, in such a way that not only are offending packets detected, but on-the-fly modifications to the set of network flows are possible, allowing for implementing a first-response countermeasure as described before in this document. Figure 3 shows how the aforementioned security requirement disallowing network communication between IEDs can be implemented by leveraging this idea: a Bro Script (1) implements a traffic policy restricting communication between different partitions (2). In addition, an *interceptor* SDN application (3) populates the flow tables implemented by each SDN-based switch in order to forward suspicious to the SDN controller and ultimately to the SDN application itself. A suspicious packet may in turn be processed by means of a *checker* module (4) implementing the Bro Monitoring Framework. When a suspicious packet is found to be in violation of the traffic policy, our SDN Application can then either raise an alert to EDS operators or implement a series of updates to the switch tables (using the SDN control and data planes) to prevent such a traffic flow from taking place, thus implementing a first-response that may give time for analyst to further process the incident.

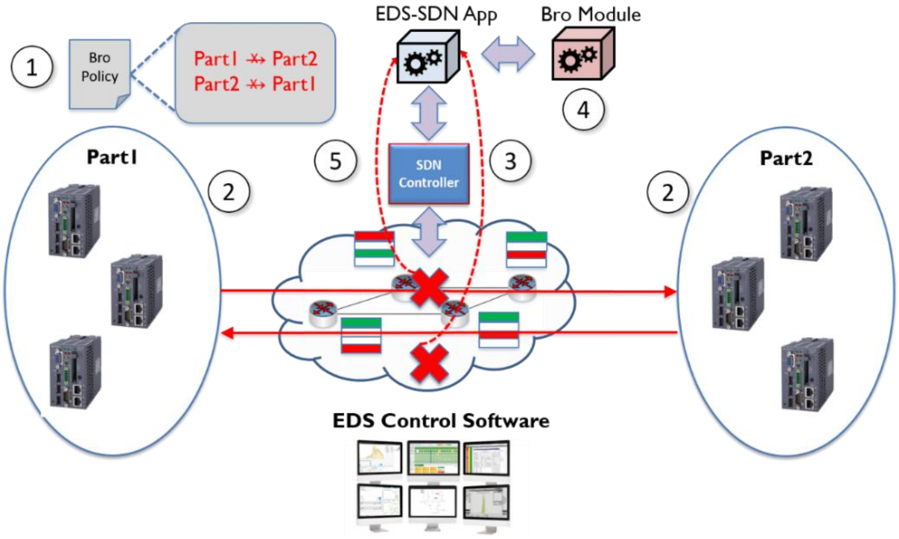

Figure 3. Enforcing network policies by using an SDN-Bro approach.

Figure 4 presents an architectural depiction of the *EDS Security Automated Tool* (EDS-SAT), a proposed implementation of our approach. Domain experts and developers are to be in charge of collecting and updating security requirements as mentioned before (1), and the requirements are in turn handled by means of a dedicated repository (2). Next, such requirements, along with information obtained from data collected directly from EDS infrastructure are fed to our proposed process-driven workflows, which in turn implement security assessment duties (3) (4) (5). Later, EDS domain experts and security officers may leverage the information provided by such tools and the proposed processing framework to perform various types of security-related assessment based on continuous real-time information. Finally, new security measures in the EDS domain may be elaborated based on the information obtained from our proposed tool (7).

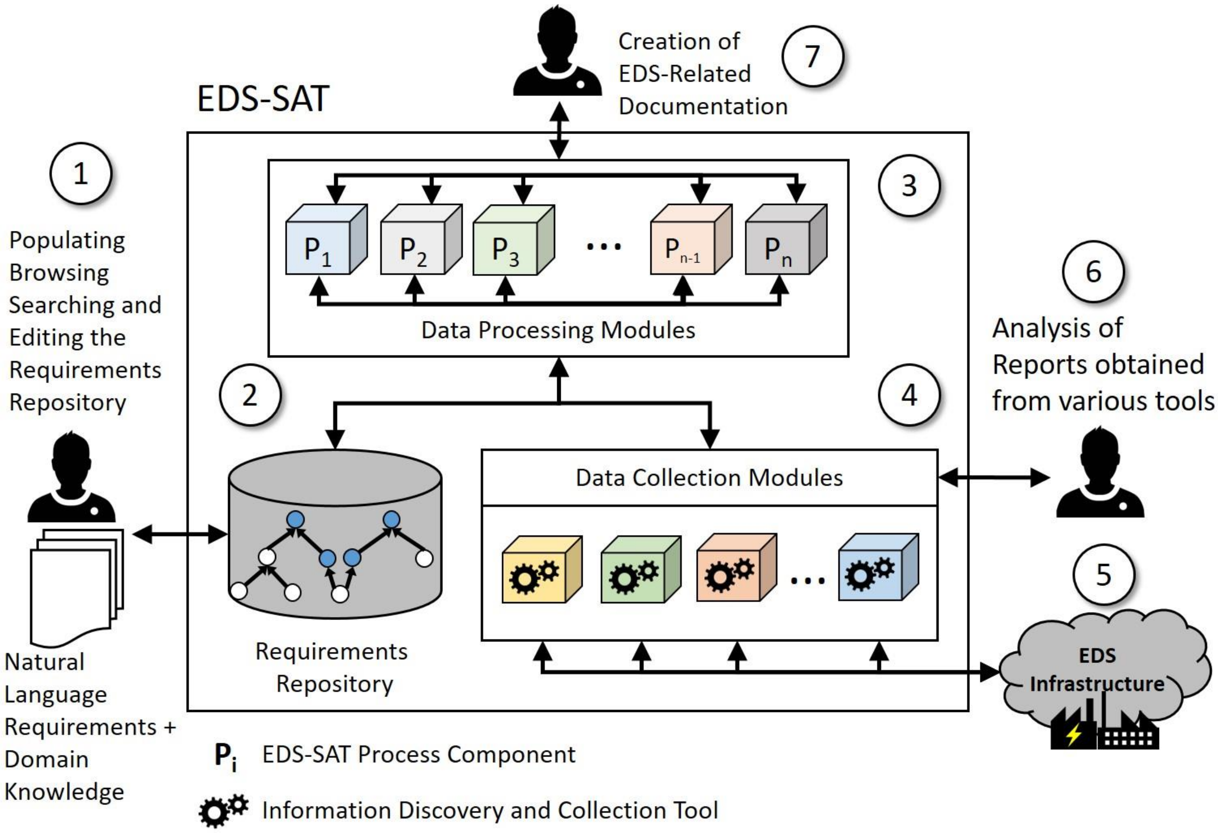
Creation of EDS-Related Documentation
7
EDS-SAT
1
3
P1
P2
P3
...
Pn-1
Pn
Data Processing Modules
6
Analysis of Reports obtained from various tools
Populating Browsing Searching and Editing the Requirements Repository
2
4
Data Collection Modules
...
5
EDS Infrastructure
Natural Language Requirements + Domain Knowledge
Requirements Repository
Pi EDS-SAT Process Component
Information Discovery and Collection Tool

Figure 4 An architectural depiction of EDS-SAT, a tool for automated security monitoring.

We have envisioned different use cases an operator may employ to use our proposed EDS-SAT tool: first, the attainment of knowledge specific to security requirements about security and EDS system components. Second, leveraging its data monitoring capabilities to gain an understanding of the current system state. Third, using its security assessment capabilities combining the previous two use cases to help assess the system and determine potential improvements needed to protect the system. Fourth, leveraging its first-response countermeasure tools, as shown in Figure 3, to collect evidence of security incidents for further decision making. Figure 5 shows an example following the first and second use case, in which an EDS operator may want to determine what security techniques are specifically related to network security, along with the system components such techniques would be implemented on (1). The operator would pose a question to the EDS-SAT tool asking about network security techniques, which would be automatically translated into a query and search through the security requirements and relationships contained within our ontology to find relevant requirements for the user (2). Next, a data collection module would be utilized to pull data measurements from the system related to networking configurations, and a data processing module would compare such measurements against the expected configurations described in the previously pulled system requirements (3). Finally, the tool would return information related to network security requirements and the components they should be applied to, along with any configuration mismatches and potential security techniques or other improvements that could be added to the system to mitigate potential threats (4).

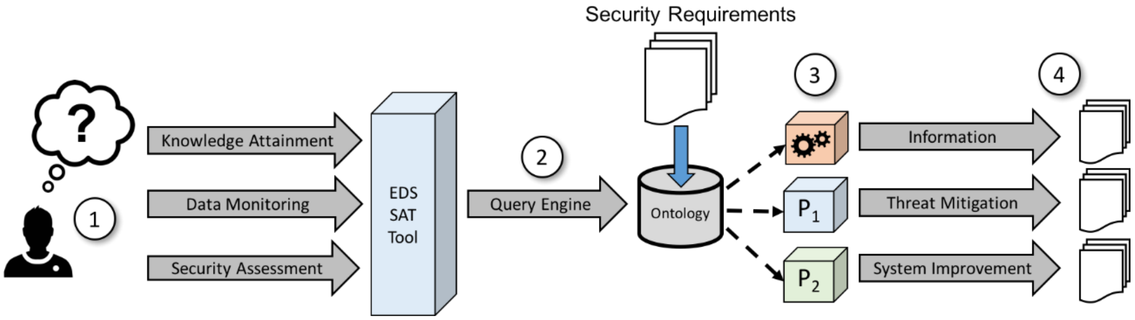

Figure 5: A detailed depiction of the workflow and use of our proposed EDS SAT Tool.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
In this new activity, we will build a security assessment framework and corresponding systems as follows: first, we will provide support for the efficient monitoring of security-related data, in such a way that the effective assessment of security risks in the context of automated EDS deployments can be achieved as a result, thus allowing for operators to evaluate the state of their EDS infrastructure against a well-defined set of security requirements. Additionally, our approach supports better management of security incidents, e.g., prevention, detection and mitigation, by allowing for security officials to provide data-based evidence that informs the development and implementation of new protective measures to reduce risk, e.g., by providing quantifiable data such that the effectiveness of new technologies for risk reduction can be evaluated and informed decision made to improve OT cyber-security.

Summary of EDS gap analysis: 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, such a process has also opened the door for sophisticated attacks that included a well-thought out combination of strategies at various levels of abstraction. Whereas previous approaches have been proposed for detecting ongoing attacks, they typically hold a limited scope and lack a well-defined foundation for incorporating security requirements from a broader knowledge base, therefore, they fall short in representing policies that can effectively tackle the distributed and heterogeneous nature of EDS and cannot provide an accurate detection of policy deviations, which can potentially indicate when an attack as the ones described before is underway. With this in mind, this project provides an approach for modeling security requirements based on cybersecurity guidelines for EDS, and later using them to implement an adaptive and customizable framework for the collection and processing of EDS data, thus supporting automated security monitoring, assessment, as well as the implementation of first-response countermeasures as a result, which can assist security officials and operators in effectively preventing and mitigating security incidents.

Full EDS gap analysis: Industrial control systems (ICS), including those in energy delivery systems (EDS), are increasingly characterized by a cyber-infrastructure that impacts assets from control rooms to intelligent field devices. This infrastructure, known as *operational technology* (OT), enables monitoring, control, resource optimization, and flexible on-demand reconfiguration. OT also provides enhanced reliability, scalability, and affordability. However, there is growing concern that OT exposes an increasing attack surface that may be potentially exploited to cause outages, system damage, or hazardous conditions, as observed in the recent attack against the Ukraine power grid (Lee, Assante and Conway March 2016).

System operators develop enforceable security policies and requirements to address these concerns, but there is a lack of tools to measure that the system complies with such policies and requirements (here, we use “compliance” with respect to a security policy of an operational system, as opposed to regulatory compliance). It is necessary to systematically resolve conflicts that inevitably arise in the presence of multiple policies, and to identify when observed system behavior violates those policies. In addition, there is a need to provide tools that can react to policy violations and implement automated first-response countermeasures, giving time for operators and security officials to further analyze the incident and determine a plan of action. This in turn requires a foundational methodology that would serve as the baseline to develop the above-mentioned tools.

Our proposed project addresses these identified gaps as follows. We first provide support for the creation of dedicated repositories describing security requirements, modeled in an ontology, which in our usage defines a set of representational primitives to model a domain of knowledge (Gruber 2009). The primitives are typically classes, attributes, and relationships, including information about their meaning and constraints on their logically consistent application. We then introduce a multi-view analysis capability that permits different EDS stakeholders to assess system security according to their specific viewpoints. We next analyze the links between different security requirements and extract the assessment tasks, using a multi-link analysis approach. Finally, we provide support for process-driven workflows to automate different security assessment tasks.

With respect to the foundational methodology, it is essential to rigorously analyze rules and goals for computation, access, service, and trust, in order to detect and respond to policy violations. We must also continuously monitor security-sensitive operations that drive preventive and corrective actions, and assess the effectiveness of this monitoring with well-defined metrics and measures. However, security assessment in EDS is tremendously complicated due to the distributed, highly-interconnected and heterogeneous nature of EDS. In addition, the security of EDS relies on multiple large, dense, highly-customized and sometimes conflicting requirements, which may ultimately result in the existence of subjective interpretations, and non-standard implementations.

Our project builds upon and extends the following related work.

In the context of gathering security requirements, Lee et al. (Lee, Gandhi and Ahn, Certification process artifacts defines as measurable units for software assurance 2007) built a multidimensional model to capture *verification and validation (V&V)* methodologies, focused on the automation of the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP). In their approach, a domain ontology was developed to comprehensively model DITSCAP criteria and requirements, as well as the knowledge and entities relevant to the domain that effectively emulate the DITSCAP measurements and certification process.

In the context of EDS, PBCONF (EPRI 2017) is a security policy configuration framework tailored for modern and legacy EDS devices that combines system-wide ontology representations with dedicated translation engines, so that policies can be automatically configured and distributed remotely to address the interoperability challenges of various remote access control methods imposed by different vendors.

In addition, several approaches have been proposed using ontologies to model system management such as resources and network configurations (Garcia, Paricio and Gosch 2010). Also, there are a few approaches related to modeling security standards. Fenz et al. (Fenz, Plieschnegger and Hobel 2016) mapped the ISO 27002 Information Security standard into an ontology for supporting compliance verification, and Santodomingo et al. (Santodomingo, et al. 2013) modeled the IEC 61850 standard and CIM standards as an ontology, in order to create a normalized reference for electrical power sensors and measurements that aid in the exchange of configuration files that are often necessary between the two standards. In addition, Kim and Lee (Kim and Lee 2015) created an ontology representation of security requirements that was used to identify the root causes of security threats: attack goal models were developed in terms of relationships between security concepts and events, and then inter-linked to physical, information and cognitive layers within the ontology.

These existing approaches are inadequate to address the particular aspect of OT cyber-security in the following ways. First, they are narrower in scope than our proposed project, and are focused on the creation and use of policy representations by means of requirements elicitation and representation that are tailored to very specific purposes. Therefore, they are not suitable for representing heterogeneous and diverse security policies applicable to the security requirements of distributed and heterogeneous EDS infrastructures. Second, they provide little support for the introduction of automated monitoring schemes to detect policy deviations resulting from a given EDS system not meeting a set of expected security requirements.

The state of the art in detecting policy deviations in OT systems has mostly focused on *intrusion detection systems* (IDS) (Debar 1999). For instance, Koutsandria et al. (Koutsandria, et al. 2015) presented an approach intended to collect and monitor a combination of both *cyber-based* data, e.g., network packets depicting command input/output, and *physical* data, e.g., field measurements obtained from EDS devices. In addition, Krauß and Thomalla (Krauß 2016) attempted to combine IDS and ontology modeling based on the common vulnerabilities and exposures (CVEs) (Mitre 2016) that models networks, system components, and security events, and recognizes attack types and vulnerabilities drawn from IDS alerts. At runtime, the system scans log files and network traffic to send out alarms, and a reasoning engine translates them back into the ontology through the creation of new entities and relationships depicting system vulnerabilities, alerts, attacks and overall system architecture information. In terms of security assessment and risk analysis models, Jauhar et al. (Jauhar 2015) 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. It was also used as a risk analysis tool to assess smart grid system risks. For such a purpose, they generated argument graphs to visually represent each attack scenario based on the integrated information contained within their model. Similarly, Anwar et al. (Anwar 2008) 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 whether potential anomalies indicate security risks.

These approaches effectively detect attacks specifically intending to disturb the operation of EDS infrastructure, but lack a well-defined foundation for obtaining and enforcing security requirements. Our proposed project introduces a more extensive approach that incorporates a broader knowledge base of cybersecurity concepts. It involves multiple sources such as security standards that are also applicable to the wider range of EDS systems, multiple vendor environments, and heterogeneous implementations. In addition, we provide means for security requirements to serve as a reference for automatically detecting policy deviations.

Recently, emerging technologies have attracted the attention of EDS researchers for the purposes of enforcing security policies. Within those technologies, Software-defined networks (SDN) (Lantz 2010) have recently received considerable attention due to the flexibility of its network management paradigm. In such a context, Dong et al. (Dong 2015) studied the impact of implementing SDN within smart grids. Describing a simple SDN implementation within a SCADA system, potential opportunities of SDN-enabled smart grids are elucidated, such as the opportunity for detection and analysis of cyber-attacks, along with significant challenges that may be newly introduced. In addition, Maziku and Nicol (Maziku 2015) utilized SDN principles towards the application of a resilient smart grid that can protect against DOS attacks. Specifying criticality scores in relation to IED placement within the network, OpenFlow controllers appraise the network when it is under attack, and based on input including network topology and system requirements, determine how to mitigate the effects of such attacks using SDN capabilities. In addition, out of the scope of EDS, but also aimed to the enforcement of security policies, the work of Hu et al. (Hu 2014) introduced *state-aware* firewalls leveraging SDN architectures. In their approach, a centralized SDN controller is in charge of distributing network traffic rules to SDN-enabled switches in such a way that security policies based on the *state* of connections can be properly enforced at runtime, allowing for *offending* packets to be forwarded to a specific SDN application for further processing.

Besides the benefits for policy enforcement as discussed before, SDN-based architectures may also provide support for the implementation of advanced data collection techniques for both cyber as well as physical data, which can be later used for the purposes of policy-based monitoring. As an example, a data collection strategy may be implemented by an SDN application, allowing for relevant network packets to be collected by switches based on traffic flow entries, and ultimately forwarding them for further processing to a predefined location. This way, SDN may provide an approach in which minor changes to existing network settings are required for the purposes of data collection, thus providing a *non-intrusive* solution that may better accommodate existing EDS cyber-infrastructures. Such a feature has not been explored by previous approaches in the context of EDS yet.

Secondly, SDN-based architectures may also provide support for implementing *first-response countermeasures* as a result of violations to security policies. As an example, any unintended traffic flows between EDS devices, as detected by a monitoring scheme, may be shut down automatically by allowing an SDN controller to push new traffic flow rules to all relevant switches within the SDN data plane. This way, an automated response may be implemented in a prompt way, allowing for EDS operators and security officials to later analyze the incident in detail for any security-related consequences. As with our previous discussion, this feature is yet to be described in the literature.

In summary, it is essential to develop a well-defined, systematic, and practical engineering methodology that incorporates innovative design principles, modeling techniques, and sound theoretical background, in such a way that it enables organizations to more efficiently optimize and evaluate their security postures and practices. The ultimate goal is the development of tools that create and enforce an EDS OT environment that is better protected from threats, and better able to respond to apparent security violations. With this in mind, we aim to provide a consolidated representation of security requirements extracted from different sources, in order to allow for dedicated analysis procedures to be conducted based on them, thus allowing security practitioners to better identify requirements and properly assess the security state of EDS deployments. This potentially alleviates the problems introduced by the existence of multiple and difficult-to-digest documents, and also removes the existence of subjective and non-standard interpretations between stakeholders. In addition, we also aim to create a framework for the automated collection and processing of security-relevant data, such that a combination of both physical and cyber-related information obtained directly from EDS infrastructures can be compared against security requirements, providing an integrated and logically-centralized approach for the detection and first-response reaction to potential security vulnerabilities and policy violations.

Bibliography

Anwar, Zahid and Shankesi, Ravinder and Campbell, Roy H. 2008. "Automatic security assessment of critical cyber-infrastructures." *2008 IEEE International Conference on Dependable Systems and Networks With FTCS and DCC (DSN).* Anchorage, Alaska, USA: IEEE. 366--375.

Debar, Herve and Dacier, Marc and Wespi, Andreas. 1999. "Towards a taxonomy of intrusion-detection systems." Edited by Elsevier. *Computer Networks* (Elsevier) 31 (8): 805--822.

Deng, Juan, Hongxin Hu, Hongda Li, Zhizhong Pan, Kuang-Ching Wang, Gail-Joon Ahn, Jun Bi, and Younghee Park. 2015. "VNGuard: An NFV/SDN Combination Framework for Provisioning and Managing Virtual Firewalls." *IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN).*

Dong, Xinshu and Lin, Hui and Tan, Rui and Iyer, Ravishankar K. and Kalbarczyk, Zbigniev. 2015. "Software-defined networking for smart grid resilience: Opportunities and challenges." *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security.* ACM. 61-68.

EPRI. 2017. *PBCONF: Secure Policy Based Configuration Framework.* January 31. Accessed January 31, 2017. http://publish.illinois.edu/iti-pbconf/framework/.

Fenz, Stefan, Stefanie Plieschnegger, and Heidi Hobel. 2016. "Mapping information security standard ISO 27002 to an ontological structure." *Information & Computer Security* 24 (5): 452-473.

Garcia, Alvaro, Juan Paricio, and David Gosch. 2010. "An intelligent agent-based distributed architecture for Smart-Grid integrated network management." *IEEE 35th Conference on Local Computer Networks.* IEEE. 1013-1018.

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

Hu, Hongxin and Han, Wonkyu and Ahn, Gail-Joon and Zhao, Ziming. 2014. "FlowGuard: Building Robust Firewalls for Software-Defined Networks." *ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN).* Chicago, IL, USA.

Jauhar, Sumeet and Chen, Binbin and Temple, William G and Dong, Xinshu and Kalbarczyk, Zbigniew and Sanders, William H and Nicol, David M. 2015. "Model-Based Cybersecurity Assessment with NESCOR Smart Grid Failure Scenarios." *2015 IEEE 21st Pacific Rim International Symposium on Dependable Computing (PRDC).* Zhangjiajie, China: IEEE. 319--324.

Kim, Bong-Jae, and Seok-Won Lee. 2015. "Conceptual framework for understanding security requirements: A preliminary study on Stuxnet." *Requirements Engineering in the Big Data Era* (Springer) 135-46.

Koutsandria, Georgia, Reinhard Gentz, Mahdi Jamei, Anna Scaglione, Sean Peisert, and Chuck McParland. 2015. "A Real-Time Testbed Environment for Cyber-Physical Security on the Power Grid." *First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy (CPS-SPC '15).* Denver, Colorado, USA: ACM. 67--78.

Krauß, Daniel, and Christoph Thomalla. 2016. "Ontology-based detection of cyber-attacks to SCADA-systems in critical infrastructures." *2016 International Conference on Digital Information and Communication Technology and its Applications .* 70-73.

Lantz, Bob, Brandon Heller, and Nick McKeown. 2010. "A network in a laptop: rapid prototyping for software-defined networks." *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks.* ACM.

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

Lee, Seok-Won, and Robin Gandhi. 2005. "Ontology-based active requirements engineering framework." *APSEC.* IEEE.

Lee, Seok-Won, Robin A Gandhi, and Gail-Joon Ahn. 2007. "Certification process artifacts defines as measurable units for software assurance." *Software Process: Improvement and Practice* (John Wiley & Sons, Ltd) 12: 165-189.

Maziku, Hellenhe and Nicol, David M. 2015. "Modeling a Cyber Resilient Smart Grid using Software Defined Networks."

Mitre. 2016. *Common Vulnerabilities and Exposures.* Accessed December 12, 2016. https://cve.mitre.org/.

PAXSON, Vern. 1999. "Bro: a system for detecting network intruders in real-time." *Computer networks* 31 (23): 2435-2463.

Santodomingo, Rafael, Sebastian Rohjans, Mathias Uslar, Josè A. Rodríguez-Mondèjar, and Miguel A. Sanz-Bobi. 2013. "Facilitating the automatic mapping of IEC 61850 signals and CIM measurements." *IEEE Transactions on Power Systems* 28 (4): 4348-4355.