A Novel Vetting Approach to Cybersecurity Verification in Energy Grid Systems

Kalyan Perumalla
Computer Sc. and Mathematics
Oak Ridge National Laboratory
Oak Ridge, TN, USA
perumallaks@ornl.gov

Juan Lopez Jr.
Cyber & Applied Data Analytics
Oak Ridge National Laboratory
Oak Ridge, TN, USA
lopezj@ornl.gov

Maksudul Alam
Computer Sc. and Mathematics
Oak Ridge National Laboratory
Oak Ridge, TN, USA
alamm@ornl.gov

Olivera Kotevska
Computer Sc. and Mathematics
Oak Ridge National Laboratory
Oak Ridge, TN, USA
kotevskao@ornl.gov

Michael Hempel
Electrical & Computer Engg.
University of Nebraska-Lincoln
Omaha, NE, USA
mhempel@unl.edu

Hamid Sharif
Electrical & Computer Engg.
University of Nebraska-Lincoln
Omaha, NE, USA
hsharif@unl.edu

***Abstract*— The cybersecurity auditing for Operation Technology is critical and has been largely missing from the cybersecurity research, especially in the energy sector. In this paper, we present a novel "cybersecurity vetting" approach (CYVET) to the problem of verification and validation of cybersecurity in complex cyber-physical installations underlying modern energy grid systems.**

I. Introduction

In Information Technology (IT), cybersecurity auditing is a widespread practice to ensure privacy, security, and trust. However, for the field of Operation Technology (OT) as used in electric energy systems, this is a relatively novel concept. In fact, OT itself only recently began to embrace IT principles, with the push for automation and centralized control driving this development. OT operators are simply not yet used to the idea of cybersecurity. To ameliorate the gap, product vendors for field devices are advancing the field by incorporating more and more security features into their products. However, customers are often either unaware of them, or do not use them, or cannot use them because of unsatisfied device ecosystem dependencies. There is thus a disconnect between what is offered, what is possible post-deployment, and what the customer expects.

There is a vast lack of cybersecurity oversight and insight, from a certification and a customer perspective alike, for OT systems in the energy sector. With new features constantly being added to new and existing products, customers are predominantly unaware what their purchased solutions are capable of, or not capable of. They often do not know if their current systems meet their own cybersecurity requirements as well as industry standards. Many of these facets not only indirectly depend on device capabilities, but also on device deployment decisions – Does a newly added feature work in an existing context? Can it be used as envisioned? Does it interfere with other cybersecurity requirements? Does it produce side effects that may interfere with other requirements?

Hence, what is needed is a security vetting system designed to provide insight into deployed systems, the match of capabilities to requirements, adherence to certification requirements, and so forth. There are few systems currently available that provide these energy grid security capabilities. OT systems are increasingly cyber-enabled, increasingly complex, and increasingly interdependent. This rapidly accelerating trend poses a clear risk for asset owners to lose confidence and for cybersecurity risk to go undiscovered until exploited by malicious parties.

A. Background in Energy Grid

Our modern society depends on the uninterrupted availability of electricity, and yet the rapid pace at which cyber-enabled OT pervades the power grid establishes a target-rich and vulnerable environment for malicious actors and adversaries.

Current practices in power grid rely on vendor-supplied information for an asset owner to gauge system capabilities of solutions being deployed. But this ignores scenarios that are all too common. For example, installers do not strictly follow configuration requirements to enable or disable features to achieve the desired security posture. Vendors often present product features through an ecosystem-of-devices during sales discussions that do not necessarily match the ground truth of deployment. Furthermore, if such features depend on a distributed functionality that are unavailable in deployment, it leaves the asset owner with the impression that the purchased features are operational when they are actually not. Device configurations may change over time, or new feature additions arrive in the form of software upgrades but are not enabled. Other features increase the cybersecurity footprint but are not disabled because the owner in unaware of this change in posture.

In light of the aforementioned types of issues, the anticipated performance improvement from a vetting approach to security is immediate and significant. It is immediate because asset owners will immediately gain insight into how their deployment matches their expectations and they can take informed steps to remedy any shortfalls. The benefit is significant because the majority of the energy sector shares the common problem of a lack of insights into their OT cybersecurity capabilities and configuration. There is also a significant potential for cost savings and increase in reliability and availability of energy systems. Prospective asset owners, during grid security purchase process, will be able to evaluate systems independently of sales information and within the context of their existing OT requirements, reducing the possibility of cyberattacks that result in the disruption of power to customers and an inherent loss of confidence and reputation for the asset owner.

International standards bodies and industry societies specify security requirements in formats that are aimed at human consumption. Also, vendors describe their security features in human-readable formats. In order to reconcile the cybersecurity requirements (CR) with candidate vendor supplied features (VSF) in an automated way, both sides need to be mapped, reconciled, and tested in machine-readable forms. We here refer to this as a **vetting process**.

B. Our Contribution

In this paper, we present a semi-automated vetting process, called CYVET, for cybersecurity assurance in energy grids. The goal of our approach is to provide the electric energy utilities the confidence that what they think their cybersecurity countermeasures provide indeed matches what their system is actually capable of and configured for. Our approach is driven by two key insights:

(1) Cybersecurity is a complex endeavor that requires a broad community involvement. Large groups of security experts operate across the world to assemble, define, refine, and maintain key insights, guidelines, and instructions on requirements and best practices for achieving cybersecurity. They range from regional to international societies, and from domain-specific to domain-agnostic bodies. It is nearly impossible and unnecessary to duplicate the guidance provided by these international bodies, which is available in the form of detailed published documents (standards or draft standards). In our approach, we build on the foundational and established professional infrastructure of international standards by conforming to their time-tested and evolving specifications.

(2) By the same token, we cannot also ignore the painstaking efforts by many vendors in carefully documenting the many security features that they design, develop, test, implement and maintain for their field devices. The vendor security features are detailed in their user guides, training manuals and specification sheets. In our approach, we also consider it most effective to build on this immense body of knowledge already codified in such vendor documents.

II. STATE OF THE ART

Historically, cybersecurity effectiveness has been largely a compliance-based approach adopted from generally accepted audit practices, yet, rarely could an organization achieve 100% compliance. Compliance-based security has the following shortfalls:

1. Benchmark measurements are static (invalid as soon as a new patch is released, or configuration change is made)
2. Requires substantially significant evidentiary documentation to verify compliance
3. Focused on security controls
4. Labor-intensive to execute
5. Requires experienced workforce with a high-level of technical acumen.

With focus on security controls, for example, Critical Infrastructure Protection (CIP) standards are comprised of 8 primary standards which include 41 requirements and 164 sub-requirements for mandatory compliance for all of the major electric companies that make up the North American power grid.

The evolution of cybersecurity effectiveness migrated towards a continuous-monitoring based approach. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) [10], for example, relies on five concurrent and continuous functions (Identify, Protect, Detect, Respond, Recover) that provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. Continuous-monitoring security has the following shortfalls:

1. Complexity and high expense for monitoring tools
2. Focused on risk outcomes (space is not well understood by stakeholders)
3. Does not accommodate acquisition cycle verification of vendor-supplied features (VSF)
4. Implementation process lacks automation
5. Does not help measure cyber risk in tangible terms nor show Return of Investment (ROI) for improvements.

Many of the practices described in compliance-based and continuous-monitoring are still beneficial and are still practiced to in varying degrees by many organizations. However, neither approach can account for verifying the cybersecurity features of assets "prior" to acquisition and integration. The vetting framework accounts for this inconsistency and allows itself to be subsumed in currently practiced risk management practices.

Multiple standards bodies and professional associations such as the International Electrotechnical Commission (IEC) and International Society of Automation (ISA) are currently operational to specify, publish, and continually update electrotechnology and cybersecurity requirements for cyber-physical systems, but matching them to vendor features is not their purview.

Currently, vendors offer multiple security features, and operators have the option of disabling them or enabling them as is, with trust on vendor claims, as long as they do not functionally break the system. There is a very limited and

unreliable level of assurance that the features work as intended. The international standards to assist in resolving this risk assessment and mitigating steps continue to be in draft (for instance, IEC 62443-4-2 [11]). There is also an inadequate framework by which customers can assess the degree of conformance of a given VSF to CR. It is necessary to overcome the limitation in the state-of-the-art due to the following reasons:

- Security features need to be tested in the intended target environments prior to installation.
- Vendors determine their own security specifications and feature set that are not necessarily overseen by international standards. Vendors largely rely on Installation Qualification (IQ), Operational Qualification (OQ), and Performance Qualification (PQ), all inadequate in a complex cyber-physical system of heterogeneous, customized installations.
- Many cyber-physical systems are highly customized installations where independent, vendor-side testing is insufficient to assure secure operation.
- Vendor-supplied systems are often installed by third-party contractors; intended feature sets may not be enabled or desired feature sets may be disabled, unbeknownst to the vendor or the end customer. What was intended as a VSF to fulfill CR is now incomplete and presents a vulnerability.
- No current framework exists to verify cybersecurity conformance in the context of the unique topological architectures of cyber-physical systems such as point-to-point, series, series-star and multi-point (as documented in, for example, NIST SP-800-82 standardized topologies [12]).

As indicated previously, cybersecurity auditing for IT is a proven and effective method. However, for OT this is an entirely new concept, and we are not aware of any solution that accomplishes the goals. A great model example where an industry has recognized the need for verification and validation, and has been making great advances, is the medical and pharmaceutical industry. Examples include equipment providers [1], software providers [2], service providers [3], and in research and development, such as in system validation using modeling [4-6]. In the IT space, similar efforts to validating network configuration gave rise to a myriad of companies such as RestorePoint [7], Veriflow [8], or Forward Networks [9]. In the OT space, SigaSec [13] and Mission Secure, Inc. [14] have introduced cybersecurity technologies that provide insight after deployment but do not address VSF capabilities prior to deployment. These underscore the need to provide similar capabilities in the OT space to protect vital infrastructure such as power grid.

III. Novel Vetting Approach: Basic Idea

Our approach is designed to comprehensively address the disparity of requirements and capabilities by vetting vendor claims against device capabilities, as well as vetting customer requirements against device capabilities. This is a vital capability, particularly for the power grid and utilities.

The presented approach is designed to directly address the need to elevate the current industry capabilities to verify and validate OT cybersecurity and associated control system infrastructure. Our approach provides that needed capability, and is device- and architecture-agnostic, makig it broadly applicable across the energy sector. The goal is to deliver a cybersecurity verification and validation framework testing capability to verify and validate OT equipment, software and the underlying control system architecture. The primary objectives are:

(1) Verification: the synthesis and reconciliation of standards and vendor supplied features
(2) Validation: the generation, execution, and presentation of testing scripts of verified security features
(3) Demonstration: apply the developed technology capabilities for verification and validation at a relevant end-user facility in the energy sector.

The vetting-based capability exhibits the following characteristics: (1) interoperability, (2) scalability, (3) backward compatibility with regard to OT asset generational evolution across critical infrastructure domains, (4) compatibility with common methods in use (e.g. DOE C2M2 [15], NIST CSF [10], NERC CIP [16]) vendor agnostic, (5) semi-automated testing process, (6) equally useable by vendors and asset owners, and (7) comprised of readily manageable advanced tools, technologies and techniques that do not impede critical energy delivery functions.

The vetting process is illustrated with a concrete example that is very commonly encountered in the OT space. Consider the "Authenticator Management" portion (Fig. 1) of the *actual* security guidelines published by the Integrated Administration and Control System (IACS). The requirement numbered 5.7.1 specifies, in natural language, four key properties of OT components. Each requirement represents a complex technological aspect in a generalized, device-agnostic, technology-agnostic, and implementation-independent fashion. For instance, the 5.7.1(a) requires an initial authentication facility that is commonly realized either as a pair of default administrator account and password or as a hardware switch. The next requirements state the conditions to be satisfied by those authenticators. There are several such requirements that are contained in voluminous standards documents that run to hundreds of pages of specification. The requirements that are expressed in natural language form in such large cybersecurity specification documents.

The counterparts to these OT cybersecurity standards specifications are the vendor-provided user guides, technical manuals and specification sheets that document the exact cybersecurity features that were chosen for implementation by the vendor. Fig. 2 shows the *actual* authentication features built into the flow meter devices of the EJA-E series manufactured and sold by Yokogawa [17]. Once again, the documented features are extensive, but expressed in a completely different plane.

IACS Standard (pages 27-28)

5.7 CR 1.5 – Authenticator management
5.7.1 Requirement
Components shall provide the capability to:

- **(a) Support the use of initial authenticator content;**
- **(b) Support the recognition of changes to default authenticators made at installation time;**
- **(c) Function properly with periodic authenticator change/refresh operation; and**
- **(d) Protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.**

Fig. 1: Illustration of Cybersecurity Requirement Specification from a Standards Body

The state-of-the-art requires the involvement of a few human experts to (a) know the intricate details of all cybersecurity requirements already established by international cybersecurity experts, (b) locate the most relevant requirements, (c) locate all the relevant vendor-supported features on the actual devices, (d) reconcile the particular features with their corresponding standards, and (e) test the features for conformance with the requirements. This is an extremely challenging process prone to error, does not provide the desired levels of cybersecurity assurance, and does not scale with the volume of standards specifications, the variety of devices, the temporally evolving nature of requirements and features, and the complexity of dynamic behavioral dimensions to be addressed.

Yokogawa EJA-E Series Field Guide – Write Protection (pages 1-2)

Hardware Write Protection Switch (WR)
The HART communication EJA-E and EJX-A transmitters have a Write Protection (WR) switch located on the CPU Assembly Board next to the Burn Out (BO) switch. When the WR switch is in the "D" (Disabled) position, the transmitter will not allow parameter changes through the use of a handheld communicator, FieldMate, or range setting switch on the transmitter indicator (if equipped). When the WR switch is in the "E" (Enable) position, parameter changes will be allowed.
Software Write Protection (Password)
The EJA-E and EJX-A transmitters with HART communication have a Password that can be set to protect the configured parameters. The Hardware Write Protect switch takes precedence over the Password Protection.
Using FieldMate, the Password function can be Enabled or Disabled. When the Password function is Enabled, a 8-digit password will need to be entered to make any setting changes. This Password can be any 8-digit password the customer wants.
Once the password is set-up, anytime a change needs to be made, the unit will need to be un-locked using the chosen password. When the password is entered, the technician will have 10 minutes to make the changes needed.

Fig. 2: Illustration of Vendor Supplied Feature from an Actual Vendor's Device Technical Sheet

IV. Vetting Approach: Components

International standards bodies identify and codify the precise cybersecurity functionalities expected as CR. Vendors or manufacturers supply a variety of cyber-physical products that incorporate their own proprietary/customized implementations which are the VSF. The VSF fall into four categories: (1) some VSF that match some corresponding CR, (2) some VSF that weaken, violate or contradict some CR, (3) some VSF that augment or enhance the CR, and (4) some VSF that are irrelevant relative to CR.

While most VSF are broadly motivated or guided by CR, the cybersecurity of an assembled, heterogeneous, multi-vendor, cyber-physical system is often not assured by mere composition of VSF-rich products. Individual and assembled/configured components need to be **vetted** against the published CR of professional bodies. To comprehensively address the cybersecurity verification and validation problem for OT in power grids, the following are needed.

- The cybersecurity verification and validation problem needs to be attacked as a semi-supervised but automated process of *vetting* VSF relative to CR, with the goal of evolving towards fully automated vetting when the standards specification processes mature.
- Vulnerability and penetration testing are sometimes considered specific parts of cybersecurity of an operational system. In contrast, verification and validation of CR and VSF capabilities (features in hardware and software) must be performed *prior to* deployment of operational technology (OT) components independently.

Given a system of individual vendor-supplied components and their associated architectures, it needs to be determined whether, and to what extent, the system with a set of VSF conforms to CR. Moreover, the customer must be able to dynamically modify, refine, and enhance the vetting process **to meet the continually evolving CR and VSF advancements** that are naturally adopted by vendors and standardized by professional bodies. The vetting process involves two major, distinct components: **Tally-Vet** and **Test-Vet**.

(1) **Tally-Vet**: The published CR items need to be tallied, matched, and reconciled with corresponding items in the user manuals documenting the VSF from the manufacturers. This process encompasses the burden of finding the most relevant features from the VSF that either (a) satisfy some of the CR, (b) fall short of the CR, or (c) go beyond the CR as specified in the standard requirements. Note that this process is entirely restricted to published information and does not touch actual equipment or their operation. Thus, this component in the vetting process can be considered as off-line analysis, reconciliation, and rating.

(2) **Test-Vet**: Upon vetting the published information about the CR and VSF, the second major process involves the actual testing of the specific set of features in VSF in light of their corresponding items in CR. This involves actual testing with hardware and software in operation to vet the subject VSF items determined in the previous Tally-Vet component.

V. PRELIMINARY IMPLEMENTATION

A. Tally-Vet

Our initial implementation offers the users to compare the relevant sections of the VSF and CR files. The basic workflow is shown in Fig. 3. The system reads the Portable Document Format (PDF) files for CR and VCF, converts them as txt files, extracts page/line information for each given keyword, and matches the VSF and CR files by highlighting the occurrences of the keyword in a side-by-side PDFrenderer in a graphical user interface (GUI). The user interface is primarily targeted at human-readable formats. We automatically highlight the keywords in the document for ready recognition of matching features and requirements. The interface provides enhanced vetting experiences to categorize the relevant features from the VSF in accordance with the CR.

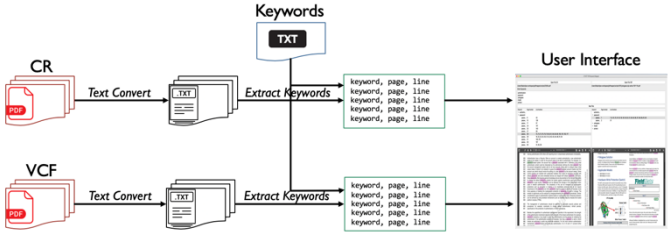

Fig. 3: Workflow of preliminary implementation

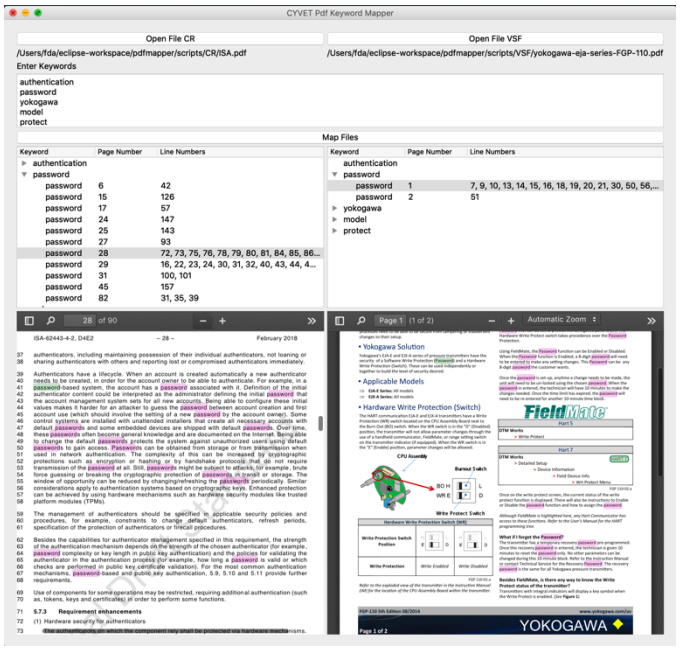

Fig. 4: Snapshot of working preliminary implementation

The user interface is developed in Python. The GUI components are imported from the widely available Qt 5 framework, which is portable to a wide range of operating systems. The PDF viewer component uses pdf.js open-source renderer engine to efficiently display on modern web browser technology. A screenshot of the interface is shown in Fig. 4: Snapshot of working preliminary implementation.

B. Natural Language Processing

We generate a summary of the text that conveys useful information without losing the overall meaning from the VSF documents. We implemented an automatic text summarization technique that transforms lengthy document into shortened text (see Fig. 5), using a Python-based toolkit (NLTK) for development and methods for tokenization, and for calculation of the sentence weights and average scores. These are initial results to show some of the possibilities of using natural language techniques in the vetting process.

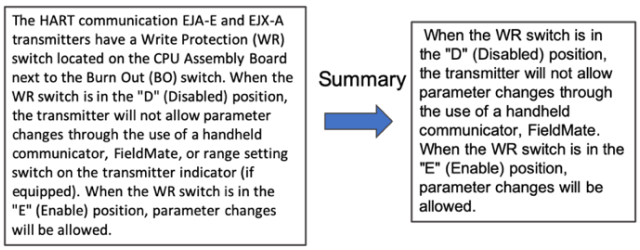

Fig. 5: Illustration of automatic text summarization tool

VI. CONCLUDING REMARKS AND FUTURE WORK

The philosophy behind our vetting approach is to directly support currently existing frameworks and risk assessment approaches that have been widely accepted, adopted, and implemented. For example, the Department of Energy (DOE)-developed Cybersecurity Capability Maturity Model (C2M2) [15] and the National Institute of Standards and Technology (NIST)-developed Cybersecurity Framework (CSF) [10] both represent approaches to assess the cybersecurity posture of an organization. The DOE C2M2 and NIST CSF allow an organization to benchmark their cybersecurity capability and aid stakeholders in developing a mitigation plan to address shortfalls based on an organization's strategic objectives. Both frameworks are self-assessment in application; both are abstract in order to accommodate broad applicability across critical infrastructure sectors with regard to organization types, structures, sizes, and industries. However, neither approach provides a verifiable approach to validate VSF against CR based on published and widely accepted standards (e.g. NERC CIP [16], IEEE). In many cases, especially in the last decade, heavy automation and internetworking capabilities have led to significant growth in "cybersecurity feature"-rich products to differentiate among competitors and establish competitive advantage. Indeed, this becomes critical in a market that has longer than usual product life cycles that are on the order of 10 to 15 years, made even more challenging by the introduction of counterfeit components in the supply chain [17].

ACKNOWLEDGEMENTS

This research has been supported by a project sponsored by the Cyber Security for Energy Delivery Systems program of the Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response.

References

[1] Distek, Inc. Validation and Qualification Services, www.distekinc.com/support/validation-and-qualification

[2] EngiLifeSciences, Compliance Solutions, www.engilifesciences.com/compliance-solutions/medical-device-software-compliance-services

[3] Andrews-Cooper, www.andrews-cooper.com/what-we-do/product-development/medical/expertise/automating-design-verification

[4] Mark Crawford, "Validation and Verification for Medical Devices", www.asme.org/engineering-topics/articles/manufacturing-design/validation-verification-for-medical-devices

[5] Silva, L. C., et al (2015), "A Model-Based Approach to Support Validation of Medical Cyber-Physical Systems," Sensors 15(11), 27625–27670

[6] Patricia Weide (1994), "SOFTWARE: Improving Medical Device Safety with Automated Software Testing", Medical Device and Diagnostic Industry Magazine

[7] Restorepoint, www.restorepoint.com/restorepoint/automate-network-compliance-audits

[8] Veriflow www.veriflow.net

[9] Forward Networks, www.forwardnetworks.com

[10] National Institutre of Standards and Technology, Cybersecurity Framework www.nist.gov/cyberframework/framework

[11] ISA for Security for Industrial automation and control systems www.isa.org/store/ansi/isa-62443-4-2-2018,-security-for-industrial-automation-and-control-systems,-part-4-2-technical-security-requirements-for-iacs-components/62990952

[12] NIST Guide to Industrial Control Systems SP 800-82 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[13] SigaSec, Cyber Security Intelligence www.cybersecurityintelligence.com/sigasec-siga-3892.html

[14] Mission Secure Inc. [Online] https://www.missionsecure.com

[15] Department of Energy Cybersecurity Capability Maturity Model Program www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0

[16] North American Electric Reliability Corporation (NERC), CIP Standards www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[17] Yokogawa (2104), "Caution: Beware of counterfeit Yokogawa products," Press Release 12