Proceedings of the 54th Hawaii International Conference on System Sciences | 2021

Cybersecurity Risk Assessment Framework for Externally Exposed Energy Delivery Systems

Sri Nikhil Gupta Gouresetti[1], Md Touhiduzzaman[2], Travis Ashley[1], Seemita Pal[1], Penny McKenzie[1], Bev Johnson[1] [1]Pacific Northwest National Laboratory, [2]Washington State University
sri@pnnl.gov

***Abstract*—Securing the energy delivery system (EDS) from complex, nonlinear, and evolving cyber threats requires a complex set of changing and interwoven classes of technologies, policies, relationships, and personnel. One key area in this technological milieu is assessment methodologies to compare information, gathered by a variety of means, about networked devices with publicly known possible threat information about said devices. This information is used to generate risk-based characterizations that allow for the adjudication and proper corresponding management action chains to be assigned. To address the current cybersecurity needs in the operational technology (OT) domain, we developed a novel relative-risk assessment framework and a software application called MEEDS that can detect exposed OT systems. This paper presents the detailed architecture of relative-risk assessment framework methodology and its integral role in the MEEDS software. The efficacy of the presented framework is demonstrated by testing with the real-world systems and vulnerabilities pertaining to the industrial control systems (ICS) in critical infrastructures.**

***Index Terms*—web spiders, operational technology, cybersecurity, industrial control systems, energy delivery systems, OT cybersecurity**

I. Introduction

Operational technology (OT) is increasingly being connected to facilitate remote control and coordination, increased performance, physical security, productivity, optimized energy management, and many more functions. Examples of OT include devices such as programmable logic controllers (PLCs) and supervisory control and data acquisition (SCADA) systems. [1]. These OT systems present in the electricity infrastructure are frequently referred to as energy delivery systems (EDS) [2]. However, the advent of connected technologies is causing the convergence of the traditional information technology (IT) and OT systems, increasing the overall risk for critical infrastructure systems [3] such as the power grid.

Securing the power grid from complex, nonlinear, and evolving cyber threats requires continuous monitoring to identify, detect, and respond to threats and vulnerabilities of critical cyber assets. EDS devices are often inadvertently exposed to the public-facing internet, which can create vulnerabilities in one or more devices. Threat actors can exploit these vulnerabilities to gain access to the utility network. Once inside the utility network, the adversary can execute commands or control actions intended to cause faulty operation or damage to the system. It is essential to continuously monitor and detect any exposed or misconfigured devices so that owners, operators of EDS, and the associated utility can mitigate potential cyber risks. In the recent years, there have been significant amount of research in the digital forensics domain [4] [5]. In the digital forensics processes, the forensic analyzer performs in-depth analysis of devices and data within the legal context, such as a criminal investigation or civil enquiry. But only a small number of analyzers focus on the EDS domain. Furthermore, the ongoing growth in the number of devices and storage volume requiring analysis puts immense pressure on timely analysis.In response to the above challenges, this paper presents a high-level overview of a system called Mitigation of External Exposure of Energy Delivery Systems (MEEDS) and provides an in-depth overview of its relative-risk assessment component[1]. MEEDS is designed to help critical infrastructure owners identify exposed and vulnerable OT systems.

In 2014, researchers discovered more than two million control system devices directly connected to the internet [12]. These exposures can be exploited by adversaries to initiate adverse events and cyberattacks to disrupt operations, cause equipment malfunction or damage, or even cause personnel injury and loss of life. Time after time, it has been evident that EDSs are becoming a prime target for cyberattacks. This can be observed from cyber incidents such as those reported in Ukraine in December 2015 [24] and December 2016 [25]. The convergence of OT and IT systems resulted a need for enhanced monitoring, control, visibility, and flexibility in EDS operation.

Recently, researchers have been adopting different existing frameworks and standards such as the Cybersecurity Capability Maturity Model (C2M2) [7] [6], National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) [8] [9], Cyber Security Evaluation Tool (CSET®), International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) Standard 31010 to address the cybersecurity gap in OT systems. In all these frameworks, risk assessment is a missing piece that is required to evaluate the risks associated with critical infrastructure facilities. So, there is an urgent need to develop a relative-risk assessment framework for internet-facing EDSs that utilities can use within their electronic perimeter and implement timely responses for mitigating cyber risks.

MEEDS is designed to integrate with web spider databases such as Shodan [26] to detect and identify EDS equipment that may be exposed to the public internet. MEEDS is designed

[1]This study has been conducted at the Pacific Northwest National Laboratory is operated for the U. S. Department of Energy by the Battelle Memorial Institute under Contract DE-AC05-75RL01830.

URI: https://hdl.handle.net/10125/71455
978-0-9981331-4-0

to enable utilities to proactively respond to this information and secure their networks by mitigating risks arising for the exposed and vulnerable devices, both internally and externally. Furthermore, the final version of MEEDS will have a built-in relative-risk assessment method (presented in this paper) that will qualitatively recommend associated risk levels for the detected exposures. In this paper, we demonstrate MEEDS's relative-risk assessment framework, which is capable of analyzing network characteristics and communication pathways of publicly exposed EDSs. This relative-risk assessment framework uses vulnerability calculations based on the approaches developed by NIST. Here are the key contributions and characteristics of the present work:

- The framework provides a novel approach to dynamically construct relative-risk metrics for EDS devices from a service banner.
- This framework does not require direct interaction with the inspected services, which ensures identification of externally exposed devices without affecting EDS OT operations.
- The framework is nonintrusive and designed with security best practices. Since MEEDS is not designed to scan the internal networks, it does not require for the devices to have any specific open ports. It is important to note that the goal of MEEDS is to detect and enumerate externally exposed systems and their parameters such as vulnerabilities, open ports, etc. However, if the system is not exposed, other mechanisms (such as scanning tools) should be used alongside MEEDS.
- The framework is designed to run inside the MEEDS software[2] and collectively, they are divided into client and server components. MEEDS server component is designed to run on a computer with internet accessibility while the lightweight clients are designed to run on any computer within the network and with the means to have periodic or continuous reach-outs to the MEEDS server.

II. Literature Review

A. Overview of Web Spiders

Web spiders could be proprietary or open-source software systems connected to web-based search engines and databases. These web spiders facilitate the discovery of thousands of internet-facing information communication technologies, including vulnerable internet-facing EDSs. These web spiders sort the discovered information into categories associated with the device's banner and stores that data in their respective databases. Often, these web spiders have an attribute called filters that can enumerate common vulnerabilities in legacy and misconfigured industrial control systems (ICSs)/EDSs (e.g., use of default usernames and passwords, weak encryption, lack of encryption and authentication, lack of authentication in the Ethernet/IP). Attackers could take advantage of these web spiders and techniques such as Google dorking[3] to illegally gain access to OT networks. However, MEEDS can use those data sources to proactively discover the exposures and mitigate them before cyber attackers can attempt any malicious actions. MEEDS uses the application programming interface (API) of those web spiders to extract information from their associated databases. Using these API connections, MEEDS generates detailed cybersecurity vulnerability reports, provides near-real-time alerts, and keeps track of historical results.

1) Shodan [26]: Shodan is an internet intelligence organization that collects information about devices that are publicly available on the Internet, including EDSs that are part of the U.S. power grid infrastructure. The resulting data is made available through a web-based search engine, a developer API, and an enterprise platform. The main unit of data is the banner, which contains information about the device such as operating system, software, and geographic location. The information can be used to determine the purpose and function of a specific device. To use this search engine, the technical user is expected to have knowledge about banners, ports, and services to obtain information about relevant connected devices facing the public internet. When queried, the search engine taps its database to generate responses. The search engine is a query-based system that uses the existing information already stored in its database. The search filters can enumerate common vulnerabilities in legacy and misconfigured ICSs/EDSs (e.g., weak encryption or lack of encryption and authentication). A knowledgeable user with enterprise access can use custom queries to enumerate critical systems that have vulnerabilities and are susceptible to cyber exploitation. The user can employ those capabilities to monitor their internet-facing infrastructure and strengthen their cyber defenses. It has been evident from [10] and [11] that the researchers have been exploring ways to using the search engine to perform vulnerability analysis and assessment for internet-facing services.

2) Project SHINE [12]: Project SHINE (SHodan INtelligence Extraction), a major effort by Infracritical, was designed to catalog internet-facing SCADA and EDS devices. Project development started in mid-2008 and ended in 2014; SHINE found more than 2 million control system devices directly connected to the internet [13] [12]. Project SHINE built search queries using the names of 182 SCADA suppliers and their leading products [14]. The project discovered multiple SCADA and EDS devices from over 60 vendors worldwide. It reportedly discovered some 2000 to 8000 new exposed devices each day. Suitable and meaningful search terms to identify control system devices from their metadata were used to extract information about the devices that were directly exposed to the public internet. These devices included traditional SCADA/EDS equipment, such as remote terminal units (RTUs), PLCs, intelligent electronic devices (IEDs)/sensor equipment, SCADA/human-machine interface (HMI) servers, distributed control systems, and other nontraditional SCADA/EDS devices. Many of the discovered devices

[2]MEEDS client system specifications/requirements: 2 GB RAM, 500 MB disk space, min of 450 MHz 32-bit or 64-bit processor, Windows 7 or newer operating system, HTTP and SSL communication protocols; MEEDS server system specifications/requirements: 4 GB RAM, 10 GB disk space, min of 1 GHz 32-bit or 64-bit processor, Windows 7/2008 R2 or greater, HTTP and SSL communication protocols, PostgreSQL version 10 or higher; Average query execution time: less than 30 seconds per 100 queries per /24 sub-net

[3]Google Dorking: In this technique, hackers use google search engine and similar software/applications to discover security gaps or vulnerabilities in software and system configuration

also revealed their hardware and firmware metadata, which could provide information about the documented security flaws associated with the devices. While the project found thousands of potentially vulnerable devices, the level of vulnerabilities and the criticality of the systems were not validated.

3) Expanse Inc. (Expander) [15]: Expanse Inc is a cybersecurity start-up company that provides a solution that continuously monitors the internet to collect information about all public-internet connected devices. Expanse Inc's product, known as Expander, is closed to the general public. Its customers are typically large organizations, and the product can cost anywhere from $250,000 to $1 million per year. Expander scans the public internet looking for exposed devices, and alerts its customers about rogue or unprotected devices within an hour of finding them. The digital assets of the customer are displayed on a map to show the true network boundary and inform the customer of other exposures. Although the product can see all the connected devices, it shows only the devices that are on the customer's network and not on other networks. This is to prevent any kind of malicious use of the gathered information. Expanse's product is a software-as-a-service, web-based product that also offers customer-specific application programming interface (API) integration. Its customer base includes PayPal, Capital One, CVS, other banking and financial services, IT manufacturing, commercial real estate, software, health care, and government agencies [16].

4) Censys [17]: Censys is a cloud-based service that continually scans the public address space and provides an up-to-date snapshot of the hosts and services running across the public Internet Protocol version 4 (IPv4) address space through a search engine and API [18]. The search results provide information about the devices that respond, including details about their software or configuration [19]. Censys produces structured data about each host and protocol, which are post-processed to enable researchers to programmatically define additional attributes that identify device models and tag security-relevant properties of each host. Search queries using software- or configuration-related details about a new security flaw can reveal how widespread it is, and provide information about the devices that are identified as affected by the flaw. Censys centralizes the mechanical aspects of scanning to expose data to researchers through a public search engine, Representational State Transfer (REST) API, publicly accessible tables on Google BigQuery, and downloadable data.

5) Reposify [20]: Reposify is a search engine that, by performing HTTP requests, can provide insight into a multitude of devices that may be connected to the public internet. The search engine is based on a custom API that not only discovers new devices, but can also determine what inherent vulnerabilities the connected devices may have. Reposify can also determine a device's relationship with other devices and people, and whether other technologies may be connected, such as an operating system, a database, or a web server. The pricing structure is slightly different because they offer a free version of the tool that does not include the "Global Asset Discovery" feature, which is aimed at inspecting and indexing assets-on-demand. The company is working with a few cybersecurity and business intelligence companies. The queries generated using Reposify are limited to the address range provided and specific ports and protocols. Only one query request can be active at one time, which limits the number of requests, and there is a maximum of 65,536 unique addresses per query.

6) Thingful [21]: Thingful is a search engine that shows the locations of data-emitting devices on an interactive map, and provides information about the types of data these devices emit and the online conversations that arise around them. The devices are grouped into categories, such as transportation, energy, or residential. Unlike the other internet search engines described in this section, Thingful builds its data set from sensor data sources on the web instead of pinging public IPv4 addresses [22]. The Thingful application has certain limitations. For example, access to its data is provided only via a dedicated user interface [23], and it does not provide information about SCADA/EDS devices in any of its queries.

B. Overview of CVE and CVSS

The Common Vulnerability Scoring System (CVSS) is a vulnerability evaluation and scoring system developed by FIRST (Forum of Incident Response and Security Teams) that quantitatively evaluates system vulnerability [27]. The CVSS considers known vulnerabilities in devices (known as Common Vulnerabilities and Exposures, or CVEs) and tries to assess the effect of the vulnerability by looking at parameters such as complexity of attack vector, confidentiality, integrity, and availability impacts. The CVSS score has three metric groups: base, temporal, and environmental.

The "base" metric group quantifies the intrinsic characteristics of a vulnerability in term of two sub-scores: exploitability sub-score and impact sub-score. The base metric attributes can be collected from the information provided by product vendors, where the vulnerability has been discovered. Unlike temporal and environmental score attributes, the base score attributes are constant across different user environments and time points. The CVSS base score is calculated as follows:

$$Base\ Score = round\_to\_1(((0.6 * Impact) + (0.4 * Exploitability) - 1.5) * f(Impact)) \quad (1)$$

Here, $Impact$ calculation is based on confidentiality, availability, and integrity, and $Exploitability$ is based on access vector, access complexity, and authentication. The CVSS base scores range from 0 to 10, with 0 indicating a threat of the lowest significance and 10 indicating a threat of the highest significance. Qualitative severity rankings of "Low," "Medium," and "High" for CVSS base score ranges are provided by the National Vulnerability Database (NVD) and are shown in Table I.

TABLE I
NVD VULNERABILITY SEVERITY RATING FOR CVSS BASE SCORE

CVSS Base Score Rating	
Severity	**Base Score Range**
Low	0.00-3.9
Medium	4.0-6.9
High	7.0-10.0

C. Other Related Research and Tools

Cybersecurity risks require proper metrics for risk assessment so that one can evaluate the potential effects of the exposed EDS on the OT side, and multiple research efforts have explored improved techniques [28] [29] [30] [31]. Cherdantseva et al. [34] comprehensively surveyed several existing cybersecurity risk assessment methods targeting ICSs such as SCADA systems. In [32], the authors introduced a new type of cyber risk metrics system that uses both the engineering operations and economic impacts of cyber attacks on systems. Also, in [33], the authors proposed a framework that identifies software risks and proposed organizational risk mitigation strategies. It is evident from [32] and [33] that while the cyber risks can be calculated as $risk = likelihood * consequences$ or a form of such equation, simply analyzing because of the risk (or likelihood of an attack) may not be sufficient. As part of the cyber risk analysis, the associated financial implications would need to serve as one of the key components. Furthermore, techniques have been introduced to incorporate the CVSS metrics against cyberattacks in EDSs [35]. In the network asset discovery and vulnerability assessment domain, several tools are available, such as Nessus [36], pOf [37], PRADS [38], NMAP [39], ZMAP [40], and others. However, it is important to note that not all of those tools can be safely used in the OT environment.

Cybersecurity risk assessment and management is often performed in two main areas: 1) organizational policy-based analysis; 2) organizational network and systems based analysis. Tools, processes, and methodologies such as the NIST cybersecurity framework (CSF) [9] [8], CSET [41], C2M2 [6] [7] are designed to assist with organizational policy-based analysis. Other similar policy-driven risk assessment and management frameworks can be found in [42], [43], [44], [45], [46], [47]. On the other hand, tools such as MEEDS, NMAP, Nessus, etc. are designed to address organizational network and system analysis. In other words, MEEDS and its built-in relative-risk assessment framework is designed to address several objectives listed in the above cited policy-based analysis framework. MEEDS can assist with:

- ID.RA-1, ID.RA-2, ID-RA5, and ID-RA6 sub-categories from NIST CSF's *Risk Assessment (RA)* category under the *Identify (ID)* function.
- PR.IP-12 sub-category from NIST CSF's *Information Protection Processes and Procedures (IP)* category under the *Protect (PR)* function.
- DE.AE-2, DE.AE-3, DE.CM-1, and DE.DP-5 sub-categories from NIST CSF's *Anomalies and Events (AE), Security Continuous Monitoring (CM), Detection Processes (DP)* categories under the *Detect (DE)* function.
- RS.AN-3 sub-category from NIST CSF's *Analysis (AN)* category under the *Respond (RS)* function.

III. Overview of MEEDS Relative-Risk Assessment Framework

Risk assessment is the first and most critical component of risk management. Risk assessment involves identifying, quantifying, and prioritizing EDS device security risks in the OT network. By conducting a risk assessment that targets the externally exposed EDS, energy utilities can determine the overall vulnerability of their devices and develop prioritized mitigation strategies. As stated in the previous section, web spiders extract a lot of system-specific parameters through banner grabbing technique. MEEDS uses some of those banner parameters (showed in later parts of this section) to perform relative-risk analysis. The presented risk assessment framework for EDS performs an in-memory mapping of CVE entries that are found by querying the web spider databases. To achieve this, the relative-risk framework compiles a list of all known exposed EDS devices and their CVE IDs into a single input file by retrieving and processing data from the national vulnerability database (NVD) in near-real-time.

The framework presented here calculates relative-risks by categorizing the exposed EDS devices in an OT network according to their respective CVSS scores. This categorization will provide information regarding network characteristics and communication pathways. To achieve this assessment goal, initially, (i) multiple EDS devices (e.g., PLC, RTU, SCADA) are queried through MEEDS (note that, as stated previously, MEEDS uses the web spider databases as one of the data sources in the back end[4]) to gather the banner information of the exposed devices. (ii) Next, a classification is done to identify whether the exposed banner is actually an EDS (this step eliminates false positives). (iii) From those identified device banners, only the banners with CVE IDs are extracted. Note that not all the exposed device banners will have CVEs, while some banners may contain multiple CVEs. In the absence of a CVE ID, Equation 1 can be used to calculate the vector string and the CVSS score using the banner information returned by the web spider (through MEEDS) queries. (iv) Finally, an aggregated CVSS score is calculated for the discovered devices and they are categorized into respective risk categories (see Fig.1).

A. Web Spider Queries

Web spiders perform an intensive, per-target scan on physical (Open Systems Interconnection [OSI] layer 1) devices, network (OSI layer 3) protocols, and transport (OSI layer 4) protocols. Some web-spider-scan APIs evaluate two scanning configurations: (1) an EDS port scan and (2) an EDS device scan. These two scanning configurations scan the EDS network immediately upon request by using the on-demand scanning capabilities of the API. Table II lists the queries from those two scan API configurations.

B. Classify Device Categorization

Querying through MEEDS generates potential device banners. However, those banners are not always related to EDS ports. For example, for queries such as *PLC* through MEEDS,

[4]MEEDS relies on multiple external datasources such as the web spider databases, national vulnerability database, etc. To successfully make the data retrieval calls using the application programming interfaces (APIs) of those external sources, certain ports should be open on the system that runs MEEDS. For example: since the MEEDS queries are executed through HTTPS calls, port 43 should be open to execute the queries and receive the data from the external sources.

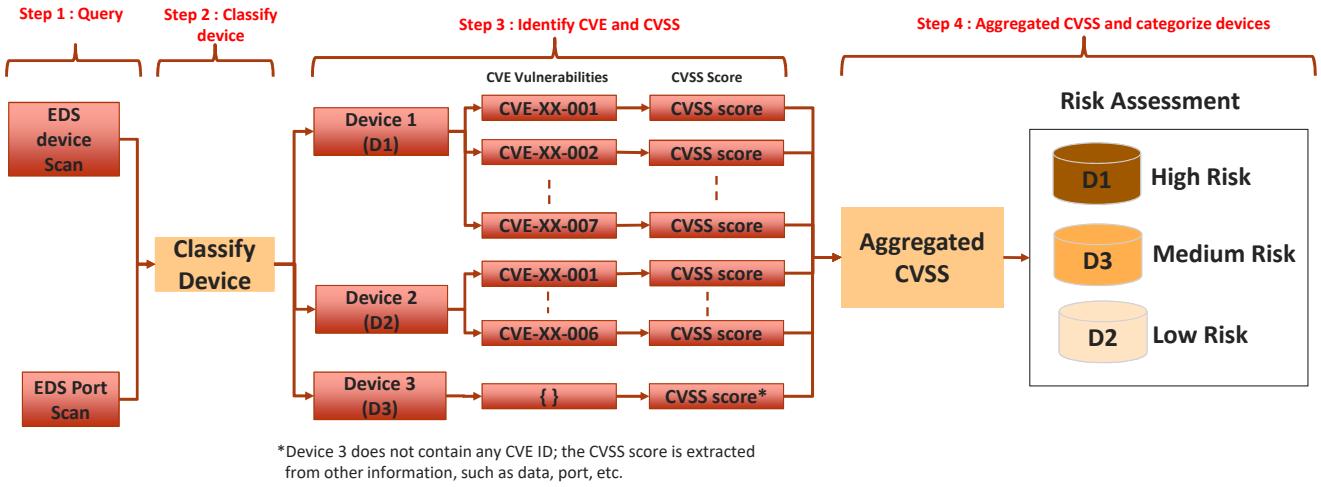

Fig. 1. High-level overview of proposed MEEDS relative-risk assessment framework

TABLE II
STANDARD PORT CONFIGURATION QUERIES

EDS Port Scan		EDS Device Scan
Port	**Service**	**Devices**
21	FTP	PLC
22	SSH	RTU
23	Telnet	SCADA
502	Modbus TCP	HMI
102	S7/MMS/ICCP/IEC 61850	PAC
4712	C37.118	Relay
4840	OPC	DNS
20000	DNP3	Smart Meter

it sometimes generates http and ftp banner information that is not directly related to the PLC. Instead, that information refers to the handshaking process and related data pertaining to the PLC. Hence, an appropriate device categorization is necessary to eliminate banners that are not related to EDSs.

In the presented research, classifying a device type based on its banner is achieved using regular expressions (RegEx) on the *data value* attribute of the banner. That information is uniquely indicative of a device type; therefore, a device cannot be categorized if the RegEx does not find a match in the banner's metadata. False positives are eliminated or reduced by issuing search terms that are multifaceted and distinctive to a targeted banner. Search filters are applied to the queries to limit/scope the results related to the exposed devices, and the data fields of the returned banners are queried using a RegEx dictionary. RegEx terms of the targeted device type are used to query the banners in the sequential order of dictionary entries using a tiered approach. Finally, banner classification is complete upon a successful match, although succeeding RegEx queries could also match. Search terms are created and combined to produce a RegEx dictionary for each device type by examining the data properties of the banners and identifying consistent and unique properties. Fig.2 provides a simple example of device classification methodology for the PLC query. In this case, a total of 238 banners were found. From those banners, 120 banners have RegEx "*PLC Name:*", 58 banners have RegEx "*PLC Type:*", and 4 banners have RegEx "*Unit ID:*". Hence, out of 238 exposed banners, 182 are related to the PLC.

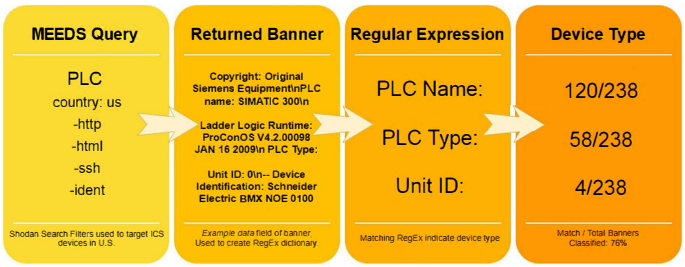

Fig. 2. Example flowchart of device classification for PLC query

C. Identify CVE

To identify CVEs, the banner information of the detected (potentially exposed) EDS is analyzed. In the first step, the MEEDS relative-risk assessment framework checks whether the banner has any CVEs. If the CVEs exist, they are used to query the NVD [27] to extract the corresponding CVSS scores.

As mentioned previously, not all banners will have CVEs, so it is not always possible to extract the CVSS scores. To get the CVSS scores of unassociated CVEs, the MEEDS framework generates a vector string by analyzing the metadata of that banner.

The following steps provide an example of how to construct a CVSS vector string by analyzing the banner information. Please note that the value assignments below are illustrative and the end user can assign these factors according to their environment. MEEDS is designed to be flexible, to fit any EDS environment.

- **Attack Vector (AV)**: This metric reflects the process of vulnerability exploitation. For example, the metric value "*network (N)*" indicates that the vulnerability can be exploited through network access. Because the exposed device is found through MEEDS, the vulnerability is remotely exploitable. This framework always assigns *network (N)* to the AV metric.

- **Attack Complexity (AC)**: This metric measures the complexity of the attack required to exploit the vulnerability once an attacker has gained access to the target system. The web spider banner contains a property/attribute called *tag*, and it returns a value such as VPN, ICS, etc. This *tag* describes the purpose of the device. Assuming that most of the ICSs in the energy domain might be strongly protected through the firewall and different types of security mechanisms, if the tag properties return *ics*, this framework assigns *high (H)* to the AC vector; if not, the framework assigns *Low (L)*.
- **Authentication (AU)**:This metric measures the number of times an attacker must authenticate to a target in order to exploit a vulnerability. The framework assumes that the vulnerable command is only available after successful single authentication and assigns *Single (S)* to the AU vector.
- **Confidentiality (C)**: Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized users. This framework assigns *Low (L)* to the C vector based on the assumption that in the EDS domain, unauthorized disclosure of information could be expected to have limited adverse effects on organizational operations, organizational assets, or individuals.
- **Integrity (I)**: The Integrity metric measures the effect on integrity of a successfully exploited vulnerability. The MEEDS framework assumes that a complete loss of system protection will compromise the entire system, and therefore assigns *Complete (C)* to the I vector.
- **Availability (A)**: A loss of availability is the disruption of access to or use of information or an information system. This metric measures the effect on availability of a successfully exploited vulnerability. In the OT domain, availability is given the topmost priority to maintain system operations. This framework assigns *Complete (C)* to the A vector.

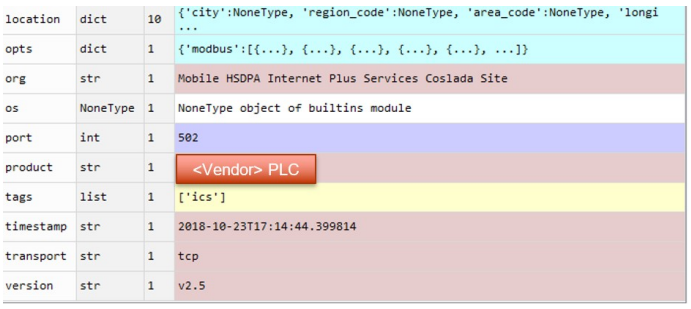

Fig. 3. Banner information of exposed PLC without a CVE ID

The following scenario illustrates the process of CVSS string constructions using the presented framework. Fig. 3 shows a snapshot of banner information of an exposed PLC that does not contain any CVEs, and Table III describes the process for constructing a CVSS vector string by analyzing the exposed PLC banner information. The overall vector string of this banner is $(AV:L/AC:H/Au:S/C:P/I:C/A:C)$ and the CVSS score is calculated as shown below:

$Impact = 10.41*(1-(1-0.275)*(1-0.666)*(1-0.666)) = 9.53$

$Exploitability = 20 * 0.395 * 0.35 * 0.56 = 1.5484$

$BaseScore = round_{[0-1]}(((0.6 * 9.53) + (0.4 * 1.5484) - 1.5) * 1.176) = 5.6$

TABLE III
CREATE VECTOR STRING BY ANALYZING BANNER

Vector	Metric Value	Metric Score	Explanation
AV	Network (N)	1.0	Modbus protocol uses Port 502 and this port is open in the Modbus server
AC	High (H)	0.35	The tag mentioned in this banner is "ICS"; therefore, it is strongly protected through the firewall and different types of security mechanisms.
AU	Single (S)	0.56	The PLC uses single authentication.
C	Partial (P)	0.27	Access to some system files is possible, but the attacker does not have any control over what is obtained
I	Complete (C)	0.66	Total compromise of system integrity
A	Complete (C)	0.66	Total shutdown of the affected PLC

MEEDS Risk Assessment Algorithm

Input: (a) A list of NVD database file, $x =$ $\{NVD_{2006}.json, NVD_{2007}.json, \ldots, NVD_{2019}.json\}$

(b) A list of downloaded Shodan search queries, $y =$ $\{PLC.json \ldots., SCADA.json\}$

Output: The CVSS score and vector string of exposed EDS devices

 # Load and extract the entire CVE information from the NVD database

For i in x:
  NVD = load the CVE item of json data;
  For j in $number\ of\ NVD$:
    Temp_score = Identify base score
    Vector = Identify vector string
    If $Temp\_score < 3.9$, set Impact ='*low*';
    Else if $Temp\_score < 6.9$, set '*medium*';
    otherwise set '*high*'
    Final_dictionary = (Temp_score, Impact, Impact)

 # Extract the Shodan queries data and identify the exposed OT devices with categorization

For i in y:
  Attr = rear the Shodan data and split all the banner
  For j in $number\ of\ Attr$:
    If 'Vulns' in j: # check 'vulns' exists or not
      Value = Attr.append('Vulns')
      For i in number of vulns: # count number of exposed
        If vulns = = Final_dictionary
          Result = (i, Temp_score, Vector)
    Else Value = Result # create vector string and get result using CVSS equation

D. Calculate Aggregated CVSS

An exposed device that has multiple CVEs will be categorized into three vulnerability risk categorization buckets: high, medium, and low. This categorization is applied to the vulnerabilities of the exposed device based on the CVEs and does not evaluate the device as a whole. The CVEs found to be associated with a device are evaluated by their CVSS scores using the *device categorization algorithm*, which produces a weighted average CVSS score for the device. The range of weighted arithmetic mean CVSS scores for low risk categorization is 0.0-3.9; medium risk categorization

is 4.0-6.9; high risk categorization is 7.0-10.0. The device categorization algorithm uses the following arithmetic mean formula:

$$Risk\ categorization\ score, R_d = \frac{\sum_{i=k}^{b}(y_i w_i)}{\sum_{i=k}^{n} y_i}$$

where

y = count of CVSS score
w = weight of CVSS score $(3.9, 6.9, 10.0)$
n = High categorization
k = Low categorization

IV. Experimental Results

In this work, we conducted several experiments and tests to validate the proposed framework. In this section, we present the results of these experiments and the associated data to confirm high performance of the proposed MEEDS framework in terms of execution time and the false/true positive rates. The experimental analysis mostly focused on PLCs, RTUs, and SCADA systems, because those are the most common and some of the most significant systems in an OT environment.

A. Analysis

For the experimental analysis, the search terms that were used in the queries are *"PLC," "RTU,"* and *"SCADA."* Although the generated data is accessible through simple queries, the data is obfuscated (see Fig. 4, Fig. 5, and Fig. 6) for privacy and confidentiality. A particular exposed device falling under a class (such as RTU, PLC, etc.) is named "device 1, device 2…device *n*." Each device has a banner with zero or more CVEs. Fig. 4, Fig. 5, and Fig. 6 show snapshots of output from the queries *"PLC," "RTU,"* and *"SCADA."* These figures show that most exposed devices for a particular query contain multiple CVEs. For example, for *PLC* queries, device 1 contains 15 CVEs; four of them are rated high criticality, ten are rated medium criticality, and one is rated low criticality.

The extracted information is not associated with a specific network, geographical location, facility, vendor, or threat. The results of these queries were each stored in multiple JavaScript Object Notation (.JSON) files, resulting in approximately 100 different exposed devices per file. The CVEs associated with an exposed device are a field that the query results return along with the CVSS v2.0 base score. This CVSS v2.0 base score is then used to categorize the CVE by following the rating rubric shown in Table IV. To query CVEs in the NVD and gather the CVSS v2.0 vectors, a locally stored copy of NVD is loaded into a Python script to search the CVE.

Table IV shows the overall device criticality of the exposed device after aggregating all CVSS scores. Note that the table only represents PLC queries. After device classification, this framework identified a total of eight exposed PLCs out of 100 devices, and each of the exposed devices has multiple CVEs. Out of those eight exposed devices, five devices fall in the medium criticality range and three devices fall in the high criticality range. It is important to note that most of the OT devices are critical towards maintaining secure operations. Therefore, the corresponding CVSS associated with the OT-related vulnerabilities are often high enough to be categorized as medium or high. This pattern is also reflected in table IV where all the exposed PLC devices fall under the medium and high criticality categories.

```
Device No: 1,  CVE ID = CVE-2012-2336  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:N/I:N/A:P)')
Device No: 1,  CVE ID = CVE-2009-4143  (10.0, 'high', '(AV:N/AC:L/Au:N/C:C/I:C/A:C)')
Device No: 1,  CVE ID = CVE-2009-4142  (4.3, 'Medium', '(AV:N/AC:M/Au:N/C:N/I:P/A:N)')
Device No: 1,  CVE ID = CVE-2009-4018  (7.5, 'high', '(AV:N/AC:L/Au:N/C:P/I:P/A:P)')
Device No: 1,  CVE ID = CVE-2009-3293  (7.5, 'high', '(AV:N/AC:L/Au:N/C:P/I:P/A:P)')
Device No: 1,  CVE ID = CVE-2012-0788  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:N/I:N/A:P)')
Device No: 1,  CVE ID = CVE-2013-2110  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:N/I:N/A:P)')
Device No: 1,  CVE ID = CVE-2012-3499  (4.3, 'Medium', '(AV:N/AC:M/Au:N/C:N/I:P/A:N)')
Device No: 1,  CVE ID = CVE-2012-0031  (4.6, 'Medium', '(AV:L/AC:L/Au:N/C:P/I:P/A:P)')
Device No: 1,  CVE ID = CVE-2008-2829  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:N/I:N/A:P)')
Device No: 1,  CVE ID = CVE-2012-2386  (7.5, 'high', '(AV:N/AC:L/Au:N/C:P/I:P/A:P)')
Device No: 1,  CVE ID = CVE-2008-5814  (2.6, 'low', '(AV:N/AC:H/Au:N/C:N/I:P/A:N)')
Device No: 1,  CVE ID = CVE-2012-0057  (6.4, 'Medium', '(AV:N/AC:L/Au:N/C:P/I:P/A:N)')
Device No: 1,  CVE ID = CVE-2012-0789  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:N/I:N/A:P)')
Device No: 1,  CVE ID = CVE-2017-16642  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:P/I:N/A:N)')
Device No: 2,  CVE ID = CVE-2018-15473  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:P/I:N/A:N)')
Device No: 2,  CVE ID = CVE-2017-15906  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:N/I:P/A:N)')
Device No: 3,  CVE ID = CVE-2018-15473  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:P/I:N/A:N)')
Device No: 3,  CVE ID = CVE-2017-15906  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:N/I:P/A:N)')
Device No: 4,  CVE ID = CVE-2018-15473  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:P/I:N/A:N)')
Device No: 4,  CVE ID = CVE-2017-15906  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:N/I:P/A:N)')
```

Fig. 4. PLC device output file

```
C:\Users\touh932\Desktop\PNNL_WORK\shodan_code\MEEDS code\nvd_data\nvdcve-1.0-2017.json
C:\Users\touh932\Desktop\PNNL_WORK\shodan_code\MEEDS code\nvd_data\nvdcve-1.0-2018.json
C:\Users\touh932\Desktop\PNNL_WORK\shodan_code\MEEDS code\nvd_data\nvdcve-1.0-modified.json
C:\Users\touh932\Desktop\PNNL_WORK\shodan_code\MEEDS code\nvd_data\nvdcve-1.0-recent.json
Device No: 1,  CVE ID = CVE-2018-15473  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:P/I:N/A:N)')
Device No: 1,  CVE ID = CVE-2017-15906  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:N/I:P/A:N)')
Device No: 2,  CVE ID = CVE-2018-15473  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:P/I:N/A:N)')
Device No: 2,  CVE ID = CVE-2017-15906  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:N/I:P/A:N)')
Device No: 3,  CVE ID = CVE-2018-15473  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:P/I:N/A:N)')
Device No: 3,  CVE ID = CVE-2017-15906  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:N/I:P/A:N)')
```

Fig. 5. RTU device output file

```
Device No: 1,  CVE ID = CVE-2017-3167  (7.5, 'high', '(AV:N/AC:L/Au:N/C:P/I:P/A:P)')
Device No: 1,  CVE ID = CVE-2017-9798  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:P/I:N/A:N)')
Device No: 1,  CVE ID = CVE-2017-3169  (7.5, 'high', '(AV:N/AC:L/Au:N/C:P/I:P/A:P)')
Device No: 1,  CVE ID = CVE-2016-2161  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:N/I:N/A:P)')
Device No: 1,  CVE ID = CVE-2016-8612  (3.3, 'low', '(AV:A/AC:L/Au:N/C:N/I:N/A:P)')
Device No: 1,  CVE ID = CVE-2016-4975  (4.3, 'Medium', '(AV:N/AC:M/Au:N/C:N/I:P/A:N)')
Device No: 1,  CVE ID = CVE-2018-1283  (3.5, 'low', '(AV:N/AC:M/Au:S/C:N/I:P/A:N)')
Device No: 1,  CVE ID = CVE-2017-16642  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:P/I:N/A:N)')
Device No: 1,  CVE ID = CVE-2016-8743  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:N/I:P/A:N)')
Device No: 1,  CVE ID = CVE-2018-15132  (5.0, 'Medium', '(AV:N/AC:L/Au:N/C:P/I:N/A:N)')
```

Fig. 6. SCADA device output file

TABLE IV
Device Criticality of Exposed PLCs

PLC Devices	Bann-ers	No. Banner Criticalities According to CVSS v2			Weighted Avg. Score	Device Criticality
		High	Med	Low		
Device 1	15	4	10	1	7.52	High
Device 2	6	2	1	3	6.43	Medium
Device 3	5	3	2	0	8.76	High
Device 4	4	0	1	3	4.65	Medium
Device 5	2	0	1	1	5.40	Medium
Device 6	3	2	1	0	8.95	High
Device 7	2	0	2	0	6.9	Medium
Device 8	10	2	6	3	6.20	Medium

B. Device Behavior during Assessment

Web spiders query for the banner information of exposed devices through a scanning technique that reviews a target attribute via TCP (SYN, SYN-ACK, ACK) three-part hand-

shaking [48] [49][5]. Nonintrusive scanning techniques have fewer negative effects on device functionality because these techniques allow a scanner to scan the network without interfering with the server or client. Also, the messages (i.e., banner information) of some of the web spider scanners are small, and therefore do not raise any flags in the EDS defense systems [48]. By extracting the banner information from web spiders, the MEEDS framework can perform relative-risk assessment of the externally exposed devices without affecting EDS OT operation.

V. Conclusion

The main objective of the MEEDS relative-risk assessment framework is to use data of exposed OT devices from multiple sources (web spiders, CVE, NVD, etc.) and calculate the relative-risk scores of the exposed devices in such a way that the device operators can easily understand which devices need to be prioritized for mitigating the exposures. Using the presented qualitative relative-risk assessment and scoring framework that will be integrated into MEEDS software, some of the risks associated with inadvertent OT exposures arising from IT and OT convergence could be addressed. As articulated in the previous sections, MEEDS uses a novel, non-intrusive process of enumerating the exposures to help the end users to better manage the overall risk of their network and help them address the CVEs. Furthermore, MEEDS along with the presented framework will facilitate the implementation of a well-informed mitigation plan[6] and continuously monitor the network throughout its life cycle.

References

[1] Gartner, *Gartner Glossary: Operational Technology*, 2018. Available at: https://www.gartner.com/it-glossary/operational-technology-ot/.

[2] U.S. Department of Energy, *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, 2011.

[3] NIAC (National Infrastructure Advisory Council), *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*, 2018. Available at https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf.

[4] O'Sullivan, W., Choo, K. K. R., Le-Khac, N. A. (2020). Defending IoT Devices from Malware. In Cyber and Digital Forensic Investigations (pp. 5-29). Springer, Cham.

[5] Pour, M. S., Bou-Harb, E., Varma, K., Neshenko, N., Pados, D. A., Choo, K. K. R. (2019). Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize Internet-scale IoT probing campaigns. Digital Investigation, 28, S40-S49

[6] U.S. Department of Energy, *Cybersecurity Capability Maturity Model (C2M2) Program*.

[7] Pacific Northwest National Laboratory, *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*tool: https://esc2m2.pnnl.gov/.

[8] Pacific Northwest National Laboratory, Facility Cybersecurity web tools. Available at https://facilitycyber.labworks.org/.

[5]Note: depending on the web spiders or other method of banner grabbing, they may use nonintrusive, passive scanning or intrusive active scanning techniques.

[6]MEEDS software and the presented relative-risk assessment framework provides network intelligence information to the user. That information includes exposed systems enumeration, vulnerabilities (CVEs) and CVSS, ports, protocols, and estimated device types in addition to IPs. Furthermore, the presented relative-risk method is embedded into the MEEDS software to annotate estimated qualitative relative-risks to the exposures. The user has complete ability to adjust them based on their requirements. In summary, the user can use the MEEDS output data to develop a risk-informed mitigation plan combined with economic and organizational factors as discussed in [32].

[9] National Institute of Standards and Technology (NIST), *Cybersecurity Framework*. Available at https://www.nist.gov/cyberframework.

[10] Genge, B., Enăchescu, C., ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services. Security and communication networks, 9(15), 2696-2714.

[11] Al-Alami, H., Hadi, A., Al-Bahadili, H., Vulnerability scanning of IoT devices in Jordan using Shodan, IEEE International Conference on the Applications of Information Technology in Developing Renewable Energy Processes Systems (IT-DREPS) (pp. 1-6), December 2017.

[12] Infracritical. *Project SHINE (SHodan INtelligence Extraction) Findings Report*, October 1, 2014. SlideShare available at https://www.slideshare.net/BobRadvanovsky/project-shine-findings-report-dated-1oct2014.

[13] OSIsoft, DoD: GSA/DoD Control Systems Cyber Policy and Strategy. Available at https://www.energy.gov/sites/prod/files/2017/04/f34/fupwg_spring17_haegley.pdf.

[14] Fairley P. 2014. "Internet-Exposed Energy Control Systems Abound." *IEEE Spectrum* webpage: https://spectrum.ieee.org/energywise/energy/the-smarter-grid/thousands-of-control-systems-connected-to-the-internet.

[15] Expander, Available at https://expanse.co/

[16] Business Wire. 2017. "Qadium Announces $40 million in Series B Funding, Led by IVP." Available at https://www.businesswire.com/news/home/20170831005455/en/Qadium-Announces-40-million-Series-Funding-Led.

[17] Censys, Available at https://censys.io/.

[18] Durumeric Z., D. Adrian, A. Mirian, M. Bailey, and A. Halderman. 2014. "A Search Engine Backed by Internet-Wide Scanning." In *CCS '15 Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 542-553, USA, Oct 2015.

[19] Lee S., S. H. Shin, and B. H. Roh, "Abnormal Behavior-Based Detection of Shodan and Censys-Like Scanning," *Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*, Milan, 2017.

[20] Reposify, Available at https://www.reposify.com/.

[21] Thingful, Available at https://www.thingful.net/.

[22] Tran N. K., Q. Z. Sheng, M. A. Babar, and L. Yao. 2017. "Searching the Web of Things: State of the Art, Challenges, and Solutions." *ACM Computing Surveys* 50, 4, Article 55, August 2017.

[23] Shemshadi A., Q. Z. Sheng, W. E. Zhang, A. Sun, Y. Qin, and L. Yao. "Searching for the Internet of Things on the Web: Where It Is and What It Looks Like." *ACM Computing Surveys*, Vol. 50, No. 4, Article 55.

[24] Electricity Information Sharing and Analysis Center (E-ISAC)/SANS Institute, *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*, March 2016.

[25] Dragos.com, *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations*, 2017.

[26] Matterly J. Shodan, http://www.shodan.io [Accessed in 2019].

[27] National Institute of Standards and Technology, National Vulnerability Database. Available: https://nvd.nist.gov/vuln/data-feeds.

[28] E. Ciapessoni, D. Cirio, G. Kjølle, S. Massucco, A. Pitto, and M. Sforna, "Probabilistic Risk-Based Security Assessment of Power Systems Considering Incumbent Threats and Uncertainties," *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2890-2903, 2016.

[29] G. A. Francia III, D. Thornton, and J. Dawson, "Security best practices and risk assessment of SCADA and industrial control systems," in *Proc. 16th Colloquium Inf. Syst. Security Educ.*, USA, 2012.

[30] J. E. Y. Rossebø, R. Wolthuis, F. Fransen, G. Björkman and N. Medeiros, "An Enhanced Risk-Assessment Methodology for Smart Grids," *Computer*, vol. 50, no. 4, pp. 62-71, 2017.

[31] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "CPIndex: Cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 566–575, Mar. 2015.

[32] Ruan, K. "Introducing cybernomics: A unifying economic framework for measuring cyber risk", *Computers & Security*, Vol 65, pp. 77–89, 2017 black

[33] Biswas, B. and Mukhopadhyay, A. (2018), "G-RAM framework for software risk assessment and mitigation strategies in organisations", Journal of Enterprise Information Management, Vol. 31 No. 2, pp. 276-299. https://doi.org/10.1108/JEIM-05-2017-0069

[34] Y. Cherdantseva, P. Burap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for SCADA systems," *Computers and Security*, pp. 1-27, 2016.

[35] V. Venkataramanan, A. Hahn and A. Srivastava, "CP-SAM: Cyber-Physical Security Assessment Metric for Monitoring Microgrid Resiliency," in *IEEE Transactions on Smart Grid* vol. 11, no. 2, pp. 1055-1065, March 2020, DOI: 10.1109/TSG.2019.2930241.

[36] Rogers R. *Nessus network auditing*. Syngress Publishing: Rockland, Massachusetts, USA, 2008.

[37] Zalewski M. *p0f v3: Passive Fingerprinter*, 2012. http://lcamtuf.coredump.cx/p0f3/ [Accessed in December 2014].
[38] Fjellskal E. B. *Passive Real-Time Asset Detection System,* 2009. Available at: http://gamelinux.github.io/prads/.
[39] Nmap, 2014. http://nmap.org/.
[40] Durumeric Z., Wustrow E., and Halderman J. A. "Zmap: fast internet-wide scanning and its security applications." *Proceedings of the 22nd USENIX Conference on Security, SEC'13*, USENIX Association, Berkeley, CA, USA, 2013; 605–620.
[41] Cyber Security Evaluation Tool: https://us-cert.cisa.gov/ics/Assessments
[42] Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
[43] CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): https://www.cisecurity.org
[44] American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
[45] ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
[46] ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements: https://www.iso.org/standard/54534.html
[47] NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (including updates as of January 22, 2015). https://doi.org/10.6028/NIST.SP.800-53r4.
[48] Bodenheim R. *Impact Of the Shodan Computer Search Engine on Internet-Facing Industrial Control System Devices,* thesis, Air Force Institute Of Technology, 2014.
[49] Bodenheim R., J. Butts, S. Dunlap, and B. Mullins, "Evaluation of the Ability of the Shodan Search Engine to Identify Internet-Facing Industrial Control Devices." *International Journal of Critical Infrastructure Protection*, vol. 7, no. 2, p.114-123, 2014. DOI: 10.1016/j.ijcip.2014.03.001.