National College of Ireland

Quantitative security assessment of power-grid using Common Vulnerability Scoring System (CVSS) and attack traffic analysis

MSc Research Project
Cyber Security

Vinayak Mate
Student ID: x20214791

School of Computing
National College of Ireland

Supervisor: Mr. Michael Prior

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Vinayak Mate
Student ID:	x20214791
Programme:	MSc in Cybersecurity **Year:** 2021-22
Module:	MSc Research Project
Supervisor:	Michael Prior
Submission Due Date:	15 August 2022
Project Title:	Quantitative security assessment of power-grid using Common Vulnerability Scoring System (CVSS) and attack traffic analysis
Word Count:	6232
Page Count:	20

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Vinayak Mate

Date: 15 August 2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Quantitative security assessment of power-grid cyber-physical system (CPS) using Common Vulnerability Scoring System (CVSS) and attack traffic analysis

Vinayak Mate
x20214791

Abstract

Systems that closely collaborate between computational, network, physical and many-a-times human components to perform their functional and operational tasks are called Cyber-Physical Systems (CPS). Power-grids form a core electricity infrastructure on a large geographical scale making it a critical national infrastructure. The close integration of components in power grids is based on Supervisory Control and Data Acquisition (SCADA) and Internet-of-Things (IoT) systems for smart process control and actions. Past few decades have shown the power grids targeted by bad actors to cripple national infrastructures. Some of the known reported attacks are on Ukrainian power system in 2015 and 2016, and the Stuxnet attack on SCADA systems of Iranian grid in 2005. These attacks have shown a requirement for developing a security assessment methodology for power grids infrastructures and its specific components.

While multiple security and threat assessment methodologies are available, Common Vulnerability Scoring System (CVSS) is a method that provides a quantitative assessment of the model making it easily actionable by the security teams. This study proposes to build a CVSS marking system for components of power grid and the impact an attack on a component can have on its CVSS score. First a CVSS model for a power grid system is proposed to form a base line score for the components. Then simulated attacks are performed on the component (Smart Meter) to evaluate the changes in its CVSS score. The updated score will more accurately represent the component's status for the specific environment it is deployed in.

The experimental results show the CVSS score can be successfully customized to the environment based on the results achieved through simulated attack dataset analysis. Both the selected CVEs saw their CVSS score updated from 7.5 to 9.3 and 4.6, and from 8.8 to 8.8 and 4.8 respectively for the SYN flood and PortMap attack data analysed. This shows an improvement in the identification of vulnerability characteristics, its quantification and will help in prioritization of remediation activities.

Keywords: Cyber-physical systems (CPS), power-grid, Common Vulnerability Scoring System (CVSS), smart meters.

1 Introduction

1.1 Project Background

The past few decades have shown exponential growth of cyber-physical systems (CPS) in various areas of our life. Electrical power grids and smart grids, smart cars and transportation systems, health and medical care devices, oil and gas extraction-distribution systems, etc., all employ CPS on different scales. The growth of CPS usage has improved the

operability in these fields over traditional systems but has also resulted in introduction of new security challenges. These systems are deployed in critical national infrastructures and in most ways have a direct impact on human lives. It is expected of these systems to be free of vulnerabilities to avoid any attack from external bad actors as well as prevent internal issues like misconfiguration, accidental damage, etc. Until recently, CPS systems were deployed in an isolated architecture where interconnectivity between the CPS components was not connected with the outside world. This provided an inherent security from outside bad actors by air-gapping the CPS with any data or command inputs or outflows to the external network. To provide real-time monitoring, remote management and improve operations, a transition to smart CPS systems was done where connection with external network was implemented. An example is installation of smart meters in homes for monitoring electricity consumption. While this move provided improvements in multiple areas for CPS operations, it also introduced potential attack possibilities by increasing the attack surface.

1.1.1 CPS in Power Grids

Power grids are one of the core implementations of the CPS. They consist of multiple components that can be grouped into three major categories based on their functionality. The power generation group, the distribution and transmission substations, the control centre and, consumer devices (Figure 1). The power generation group consists of the primary and secondary power generation stations. The controller for each generator is controlled through the power generation control centre which controls power output, shutdown, and other operations. The transmission group is responsible for carrying high voltage (HV) power to the distribution substations. Distribution Substation performs the function of transporting power to consumer homes and hence consist low power cables and transformers. Smart meters in consumer homes record the power consumption and relay the information to the distribution substation. The key element of the modern smart power grids are the Controllers present at each substation. These controllers utilize Supervisory Control and Data Acquisition (SCADA) and Programmable Logic Controller (PLC) systems for process control, decision making and resulting actions. The controller network is remotely monitored and managed from the power grid's command centre based in the internal utility network. It uses collection of applications for alert reporting, event logging and management, integrity checking and storage of information in a database. (Mavridou and Papa, 2012)

The controllers that form an essential element of smart grids utilizes multiple technologies. These are Advanced Metering Infrastructure (AMI), substations, and synchrophasor systems (Figure 2). A critical element is AMI as it constitutes the core characteristic of the modern smart grid, controlling smart meters, data collectors and loggers, etc. SCADA is an industrial type of system with main function being to monitor and control automation processes. Master Terminal Unit (MTU), Remote Terminal Units (RTUs) or Programming Logic Controllers (PLCs), communication and transport networks and Human Machine Interface (HMI) are the major elements of the SCADA system. Lastly, synchrophasor system is used for performing different electrical measurements like current, voltage and frequency, power produced/delivered, power received from the consumer generators, etc. (Mavridou and Papa, 2012)

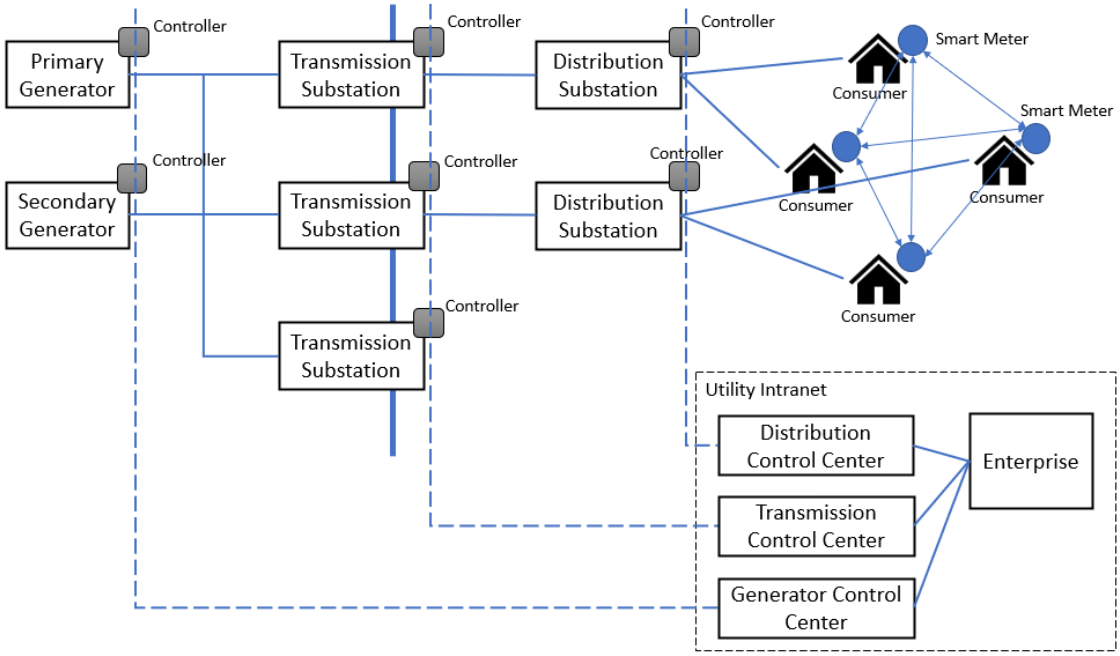


Figure 1: Power Grid block diagram

1.1.2 Common Vulnerability Scoring System (CVSS) for security assessment

A widely used security assessment method in software industries is CVSS system. It is an open framework owned and maintained by an US-based non-profit organization Forum for Incident Response and Security Teams (FIRST.Org, Inc.). It is used for standardizing vulnerability metrics based on common characteristics of the vulnerability and the severity of its impact on the target system. The overall CVSS scoring is based on three primary metric groups – Base, Temporal, and Environmental metrics.

Base metrics are partitioned into two groups – Exploitability and Impact. Exploitability metrics define the core characteristics of the component that may potentially make it vulnerable to cyber-attacks. Impact metrics define the impact of the vulnerable component on the Confidentiality, Integrity, and Availability (CIA) of the system. Environmental metrics are used to customize the vulnerability details for the specific environment of the component. Table 1 describes the CVSS metrics in detail.

CVSS Metric Group	**Description**
Base Metrics	
Exploitability Metrics	
Attack Vector (AV)	How or ways of exploiting the vulnerable component
Attack Complexity (AC)	Difficulty of exploiting the vulnerable component
Privileges Required (PR)	If and how many times authentication is required for exploiting the vulnerability
User Interaction (UI)	Is user interaction (excluding the attacker) required for successful exploit
Scope (S)	Does the vulnerability (on successful exploit) impact other components

Impact Metrics	
Confidentiality Impact (C)	Is there an impact on the confidentiality of the component
Integrity Impact (I)	Is there an impact on the integrity of the component
Availability Impact (A)	Is there an impact on the availability of the component
Temporal Metrics	
Exploit Code Maturity (E)	Does the method for exploit exist
Remediation Level (RL)	Is a remediation available and it is in which state
Report Confidence (RC)	What is the level of confident in the existence and credibility of the vulnerability
Environmental Metrics	
Collateral Damage Potential	A measure of the potential loss or impact if the vulnerability is exploited, similar to Exploitability Metrics
Target Distribution	A measure of the proportion of the vulnerable component
Impact Subscore Modifier	A measure of the specific security requirements for CIA. This metric enables customizing the environmental score based upon the environment

Table 1: CVSS metrics and their description

Another advantage of CVSS is it can be represented in form of a textual vector string for any score enabling its usage in programmatic implementation. The quantified CVSS score represents vulnerabilities on a standard scale of 0-10. Table 2 describes the severity scale for CVSS v3.0 score.

Severity	Base Score Range
None	0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Table 2: CVSS 3.0 severity rating scale

1.2 Motivation

The varied nature of CPS components and their applications has posed a challenge for the design and security teams to create a defined security model for the power grid systems. Moreover, interconnectivity with the external network for remote management, real-time monitoring, and smart control, has increased the attack vectors in the power grid CPS. This has been reflected in the recent attacks that have been reported on major power grid infrastructures across the globe. A 2015 report by French Institute of International Relations (IFRI) reported that the attacks on power grids increased by 350% between 2014 to 2015 out of which 125% were classified as “Zero day” vulnerabilities. Which means the attack vectors were exposed before a remediating fix was made available by the vendors. (Desarnaud, no date).

While Security Incident and Event Management (SIEM) solutions are available to monitor CPS systems, they are mostly reactive in nature. As a proactive solution, the vulnerability scanners and tools provide information of vulnerable components but only after the vendor has published that information to the vulnerability catalogue. Previous research in this field have utilized complex threat modelling methodologies to identify and grade vulnerabilities in the grid. There is a requirement to have a solution that will allow power grid security teams to perform an assessment of their CPS infrastructure and obtain the result in a simple, quantified form.

1.3 Research question

What quantitative security framework can be implemented by electric power grid companies to assess and mature security of cyber-physical systems?

a. Develop a quantitative assessment model of power grid components using CVSS method forming a baseline.
b. Analyse the impact of attack on the component and check how it affects the baseline CVSS score of that component.

2 Related Work

2.1 Current state-of-art in the security assessment of CPS

To create a security assessment method for power grid CPS systems, it is essential to understand the components of CPS from a security perspective. (Humayed *et al.*, 2017) discusses the primary components of CPS, and carry the discussion forward in terms of security by using vulnerabilities, attacking those vulnerabilities, perceived threats, and controls in CPS. An abstract of power grid is constructed by authors to identify the attack vectors and mitigation methods. A limitation of this paper is that it a more generic look at CPS security and discusses only two areas for power grids – vulnerabilities in grid communication and smart meters.

Delving further, (Sun, Hahn and Liu, 2018) focuses on specific areas of power-grid security in four stages – smart technologies and their review, industrial security practices and standards, solutions for security vulnerabilities, and lastly, usage of security test-beds for power grids. Test-bed simulations are used to identify security challenges and remediating them through real-time monitoring techniques. The testbed attack simulation inspires the attack dataset analyses that this paper is proposing for customizing the CVSS metric.

2.2 Security assessment methods for power grids

(Orojloo and Azgomi, 2014) propose a quantitative model for security assessment of the power grid using semi-Markov chain. Focussing on the linkages between the CPS components, quantitative weightage is provided to each component based on its interconnectedness and interdependence, attacker expertise, output reward from a successful attack, ease of access, etc. A similar approach is adopted in CVSS methodology that is being proposed in this research paper.

(Burmester, Magkos and Chrissikopoulos, 2012) have used a traditional Byzantine model to simulate attack behaviour in a threat-based model. Byzantine model bases its

security assessment on the organizational security policies that will be implemented to secure the grid. This model supports formal analysis and security proofs that may see direct implementation in an actual power grid, but the paper performs only a theoretical modelling approach with no assessment or analyses of CPS data.

In (Ten, Liu and Govindarasu, 2007), the authors have proposed SCADA vulnerability assessment framework based on Attack Trees. It is widely used threat modelling methodology where attack patterns are charted in a tree form. The root of the tree forms the objective of the attack (which is a grid component), leaves form the various ways of attacking the component, and branches form the path that the attack can utilize. This model is a static assessment but provides detailed insight into modelling methodologies and their implementation.

(Khalid *et al.*, 2018) follows a novel method of assigning quantitative values to grid components. The weightages are assigned in terms of the Confidentiality, Integrity, Availability triad which is one of the most common security approaches. Additionally, this method also makes allocation of human factor.

(Aigner and Khelil, 2020) propose a development of framework for measuring security with the purpose of addressing the complexity of the CPS. The weightage is assigned based on component's Exploitability Factor (EF), Scaling Factor (SF), and Asset Evaluation (AE). The security model is constructed using STRIDE method (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privileges). Authors have not considered any change in the characteristic of the component and only proposed a theoretical concept.

2.3 Securing assessment methods employing Common Vulnerability Scoring System (CVSS)

(Stellios, Kotzanikolaou and Grigoriadis, 2021) paper creates a threat model using Common Vulnerabilities and Exposures (CVE) and CVSS methods. Further, false positives are reduced in the model by prioritizing attack paths in terms of extent of risk. Post-patching the three critical test components, it is observed that there is significant reduction in the risk posed in cyber and cyber-physical test components which was 100% for Very High risks, 25% for High risks, and 35% for Moderate/Low risks.

(Li et al., 2019) focuses on utilizing the CVSS and Attack Trees (AT) to solve the attack quantification problem in Distribution Automation Systems (DAS). Evaluating the proposed model using seven distinct attack paths, it was observed that successful attack on Distribution Automation Systems (DAS) has maximum probability of 0.5896 which is higher than 50% and shows better results compared to Bayes method. A higher probability attack path means higher priority for mitigation through patching, configuration change, etc. A limitation of this framework is despite using attack trees, it does not support generating attack path graphs.

(Duy Le *et al.*, 2021) construct a Graphical Security model (GrSM) based on CVSS attack analysis to review a smart grid. Using single-path and multiple-path attack graphs, the model identified that for power grid case study, among 125 attack paths, there are 16 Almost Certain, 27 Likely, and 28 Possible attack paths. The study proposes to utilize this approach to educate security teams to identify which paths (and the devices on these paths) to patch first.

(Wang *et al.*, 2011) propose an improvement to the CVSS system by supplementing it with additional parameters of Server Type and OS Type. This paper takes a deep dive into the formulation of CVSS scoring by exploring the rationale behind weightages assigned to each parameter, its respective options and how they impact the overall score of a vulnerability. This paper does not evaluate the application of the proposed improvements for a particular

CPS application but provides a thorough understanding of the mathematical workings of the CVSS method.

(Venkataramanan *et al.*, 2019) propose a Cyber-Physical Resiliency Metric (CPRM) based on CVSS for quantifying the impact of cyber-vulnerabilities on microgrid resiliency. CPRM. The resiliency metric computes in real time, as the metric score changes when an attack is in progress (example, the attacker tries to elevate privileges) and allows operator to act immediately. Using case study of Ukraine power grid cyber-attack, the authors demonstrate an improvement of ModImpact (for component Modified after Impact) score from 6.4 (as assigned by CVSS) to 7.1 (as assigned by the proposed CPRM). This paper shows a mathematical approach to updating the CVSS scoring with respect to the application environment.

2.4 Summary

In conclusion, it is observed that Common Vulnerability Scoring System is a widely used industry standard for assessing the security of power grids. It is also seen that CVSS is combined with other threat and security modelling methodologies that are employed based on the application. While current research indicates a few models are available for power grid security and design teams to employ in their environment, there is need to formulate a methodology that can be customized to specific needs of a power grid. It is important to note that every power grid is different, the aim of this research is to propose a method that is easy to simulate in the lab environment available at power grids making it unique to each environment.

3 Research Methodology

The first step starts with modelling a power grid substation and its components. These components are the target of cyber-attacks which aim to exploit the vulnerabilities present in these components. The vulnerabilities can be introduced by vulnerable software/firmware used in the component, incorrect configuration implemented, or human error during business operations. This brings us to the second step where an appropriate security assessment method is chosen to identify the secure level of the component which will be the baseline metric. The used in this research is Common Vulnerability Scoring System (CVSS). While multiple threat modelling methods are available, Common Vulnerability Scoring System (CVSS) is chosen due to its ability to identify specific threats that are applicable to an environment. This enables customizing the environmental factors of the score that affect or are applicable to the power grid component. Power grid components modelled in first step are given a CVSS score using known vulnerabilities that will form the baseline metric. In the third step, the CVSS score is enhanced using environmental metric of CVSS score. This is done by carrying out simulation attacks on a power grid component using a virtual lab environment and capturing the attack data in a dataset. The fourth step involves performing statistical analysis of the attack data with respect to the normal traffic data and utilizing the scores to modify the environmental metric of the CVSS score.

3.1 Power grid model and vulnerable components

Out the variety of components present in a Power Grid, the smart meter is selected as the test component for the CVSS scoring of vulnerabilities, data collection, and evaluation of the proposed methodology. Smart meters utilize both physical wired connections of Zigbee standard and IEEE 802.15.4g Low-Rate Wireless Personal Area Network (LR-WPAN) standard for wireless communication at 900Mhz or 2.4GHz frequencies. DoS attacks pose a serious threat to Smart Meters in form or SYN flood attacks, Port Scan attacks, UDP packet flood attacks, etc. Also, since meters are public facing, they are also exposed to physical tampering. Fig. 2 represents a subset of a power grid substation and attack vectors for a Smart Meter.

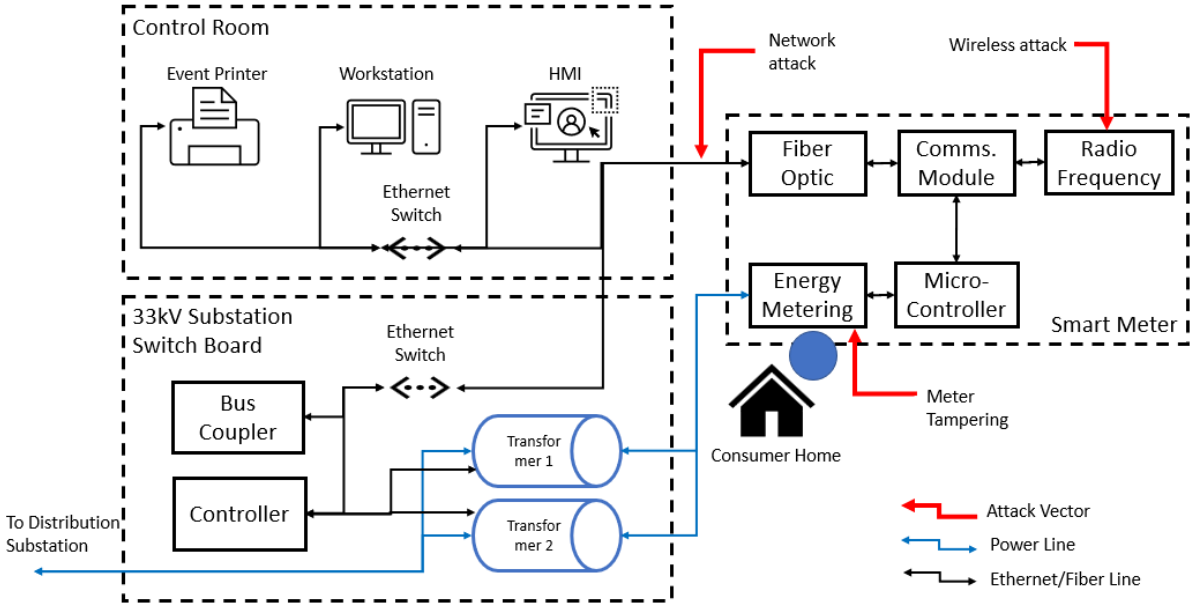


Figure 2: Power grid model with Smart Meter attack vectors

3.2 Common Vulnerability Scoring System (CVSS)

There are multiple threat modelling methodologies available, with each having their strengths depending on the environment and application of the method. The commonly used ones are STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial-of-Service, and Elevation of Privilege), PASTA (Process for Attack Simulation and Threat Analysis), Attack trees, and CVSS. Table 3 provides the comparison of the threat modelling methods and the advantages and disadvantages of each (*Choosing the Right Threat Modeling Methodology*, no date). While each methodology has its own advantages, CVSS is suitable for this research for two reasons:

a. It quantifies the vulnerabilities based on its characteristics, and
b. Provides the ability to customize the

Type	STRIDE	PASTA	Attack Trees	CVSS
Methodology	Data flow diagrams	Attacker focussed seven-step risk analysis	Graphical method with tree root as attack objective and branches/leaves as attack paths/vectors	Uses base and environmental characteristics of vulnerabilities

Focussed on	Software vulnerabilities	Risk to assets and business	Software and Infrastructure	Software and Infrastructure
Advantages	1. Identifies vulnerabilities in each STRIDE category	1. Incorporates business impact analysis 2. Works best with aligned with business strategic objectives	1. Uses attacker behaviour to plot vulnerabilities in a system. 2. Can be used to reduce attack surface if used during development	1. Provides a quantification for vulnerabilities. 2. Accommodates environmental factors 3. Simplified calculation
Disadvantages	Does not provide vulnerability severity quantification	Provides quantification only when used with other methods	Provides quantification only when used with other methods	Security teams need to develop their own method for updating environmental score

Table 3: Comparison of Threat Modelling methods

The CVSS consists of the Base, Temporal, and Environmental Score.

The Base Score is the characteristics of the component vulnerability. It is derived from the Exploitability sub score and Impact sub score equations. (*CVSS v3.0 Specification Document*, no date)

If (Impact sub score <= 0) 0 else,

Scope Unchanged Round up (Minimum [(Impact + Exploitability), 10])

*Scope Changed Round up (Minimum [1.08 * (Impact + Exploitability), 10])*

and the Impact sub score (ISC) is defined as,

Scope Unchanged $6.42 * ISC_{Base}$

Scope Changed $7.52 * [ISC_{Base} - 0.029] - 3.25 * [ISC_{Base} - 0.02]^{15}$

Where,

$$ISC_{Base} = 1 - [(1 - Impact_{Conf}) * (1 - Impact_{Integ}) * (1 - Impact_{Avail})]$$

And the Exploitability sub score is,

*8.22 * AttackVector * AttackComplexity * PrivilegeRequired * UserInteraction*

The Environmental score are used to refine the Base Score to accurately reflect the component environment. In case of power grid, the exploitability of the vulnerability from the environmental factors will be used to determine the impact on the Base score.

The Environmental Score is defined as:

If (Modified Impact Sub score =< 0) 0 else,

If Modified Scope Unchanged Round up(Round up (Minimum [

*(M.Impact + M.Exploitability), 10]) * Exploit Code Maturity * Remediation Level * Report Confidence)*

If Modified Scope Changed Round up(Round up (Minimum [1.08

** (M.Impact + M.Exploitability), 10])*

** Exploit Code Maturity*

** Remediation Level*
** Report Confidence)*

And the modified Impact sub score is defined as,

*If Modified Scope Unchanged 6.42 * [$ISC_{Modified}$]*
*If Modified Scope Changed 7.52 * [$ISC_{Modified}-0.029$] – 3.25 * [$ISC_{Modified}-0.02$]^15*
Where,
$ISC_{Modified} = Minimum[[1-(1-M.I_{Conf} * CR)*(1-M.I_{Integ} * IR)*(1-M.I_{Avail} * AR)],0.915]$

The Modified Exploitability sub score is,

*8.22 * M.AttackVector * M.AttackComplexity * M.PrivilegeRequired * M.UserInteraction*

3.3 Data analysis

With the aim to test common network attacks, the attack data traffic is selected from two datasets depicting two common attack types – DoS attack performed by SYN packet flooding and port scan attack through PortMap. Another dataset of Ideal data traffic was used as a control set. All three datasets contained multiple attributes, but the attributes of interest were Sent Packets and Received Packets (also termed as Packets Forwarded and Packets Received).

As part of Data Clean-up, the datasets were checked for any missing values and the only missing values observed were in Backward Packets. This is expected as the component being subjected to attack will fail to respond to all the packets it receives during an attack simulation test. A Pearson Correlation test was performed of the attributes to identify collinearity between the Sent and Received packets as a Sent packets will be dropped by the test component during a DoS attack depicting impact on Availability. Pearson's Correlation test was selected as:

a. the analysed data is bivariate, and all the variables are quantitative,
b. the variables are normally distributed with minimal outliers, and
c. the relationship is expected to be linear.

The Table 4 describes the methodology used to assign ordinal weightage to the analysis results.

Pearson's coefficient 'r' value	**Strength**	**Inference**	**Methodology**	**Ordinal Score for CVSS**
Greater than 0.5	High	No. of Sent Packets = No. of Received Packets	Low to No Impact on Test Component	Low
Between 0 to 0.5	Moderate	No. of Sent Packets < No. of Received Packets	High to Moderate Impact on Test Component	High
0 or Negative 'r' value	No Correlation	-	-	None

Table 4: Ordinal scoring based on Pearson's Coefficient 'r'

4 Design Specification

4.1 Architecture Design

The quantitative assessment framework designed here is performed in four stages of employing the CVSS 3.0 scoring method, and attack traffic data analysis as shown in Fig. 2. The stages are Baseline score for a component, CVSS score deconstruction, attack traffic analysis, and CVSS score modification. These stages are briefly discussed in the Methodology section.

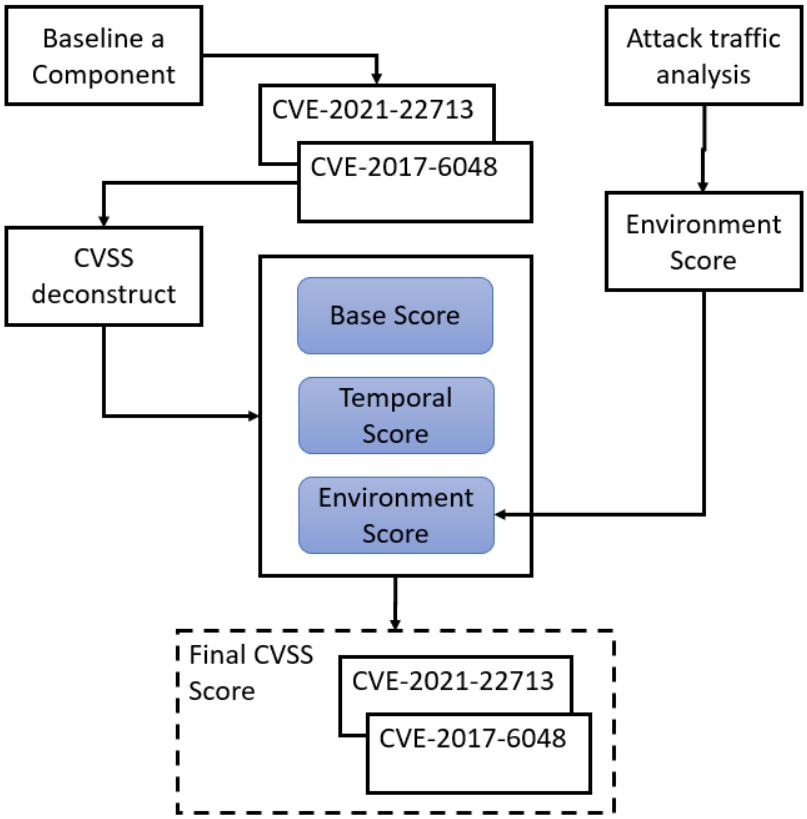


Figure 3. Methodology flowchart

4.2 Model Implementation

The component chosen for the analysis is a Smart Meter. Using the Common Vulnerabilities and Exposures database[1], the vulnerability released for smart meters were identified. The vulnerabilities identified were broken down into their characteristic Base, Temporal, and Environmental scores. This score was marked for updates based on the environmental factors specific to the smart meter.

The environmental factors were determined based on the attack susceptibility on the Smart Meter. Network based attacks were chosen for the analysis. The attack methods selected were a DoS attack attempted through SYN packet flooding and PortMap attack for port scanning. The datasets for attack traffic were obtained from the DDoS Evaluation

[1] https://www.cve.org/Downloads

Dataset (CIC-DDoS2019)[2] research conducted by the Canadian Institute of Cybersecurity based in University of New Brunswick, Canada (Sharafaldin *et al.*, 2019). This data was statistically analysed with respect to ideal traffic expected during a day-to-day Smart Meter operation. The ideal traffic dataset was obtained from Firewall Dataset[3] collated by University of California Irvine (UCI) Machine Learning Repository (Ertam and Kaya, 2018).

The Ideal traffic dataset has 65532 records whereas the SYN attack and PortMap attack datasets have 4320541 and 191694 records respectively. The statistical analysis performed was utilized assigned ordinal weightage in terms of "Low/Medium/High" and implemented in the Modified Impact Availability ($M.I_{Avail}$) and Modified Impact Integrity ($M.I_{Integ}$).

5 Implementation

5.1 Component Selection and CVSS Baseline

The components selected for the implementation are meters PowerLogic meters from Schneider Electric and SenNet meters from Satel Iberia. The vulnerabilities selected to establish the baseline scores are CVE-2021-22713 at *BaseScore* 7.5 and CVE-2017-6048 at *BaseScore* 8.8 impacting PowerLogic and SenNet meters respectively. The metric details of the vulnerabilities are in Table 5 and the detailed description below. The *BaseScore* was established using module CVSS3 of the CVSS Python library[4].

CVE-2021-22713: Memory buffer overflow vulnerability present in PowerLogic ION8650, ION8800, ION7650, ION7700/73xx, and ION83xx/84xx/85xx/8600. Successful exploitation may cause the meter to reboot. (*NVD - CVE-2021-22713*, no date)

CVE-2017-6048: This CVE was released for a command injection issue in SenNet Data Loggers and Electric Meters. Versions impacted are Optimal Datalogger v5.37c-1.43c and prior, SenNet Solar Datalogger V5.03-1.56a and prior, and SenNet Multitask Meter V5.21a-1.18b and prior. Successful exploitation may result in attack gaining full access to the meter. (*NVD - CVE-2017-6048*, no date)

Name	Impact	Base Score	CVSS Vector
CVE-2021-22713	Availability	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2017-6048	Availability, Integrity, Confidentiality	8.8	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Table 5: CVE Baseline

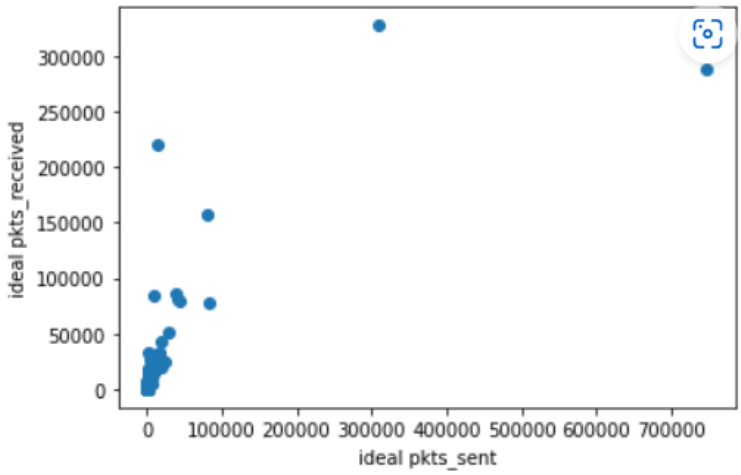
[2] https://www.unb.ca/cic/about/index.html
[3] https://archive.ics.uci.edu/ml/datasets/Internet+Firewall+Data
[4] https://pypi.org/project/cvss/

5.2 Attack traffic dataset analysis and Weighted Environment Score

Performing the Pearson's Correlation test on all three datasets, the aim to find collinearity between the Forward and Backward packets as the number of packets sent and received will vary as per the network attack scenario. A significant correlation will show that sent packets are not impacted by the received packets and an inference can be drawn that the network attack is not impacting the Availability or Integrity or Confidentiality of the test component. The exact impacted area will be decided by the impact of vulnerability being baselined in the first step. A non-significant or low correlation will show that the test component is impacted and hence is not able to respond to the received packets resulting in a drop in the sent packets.

A Scatter Plot was plotted and the Pearson's coefficient for correlation 'r' was calculated between Forward and Backward packets for all three datasets.

For Ideal traffic dataset, a significant linear correlation was observed with r = 0.7715 as seen in Fig. 4a and 4b.



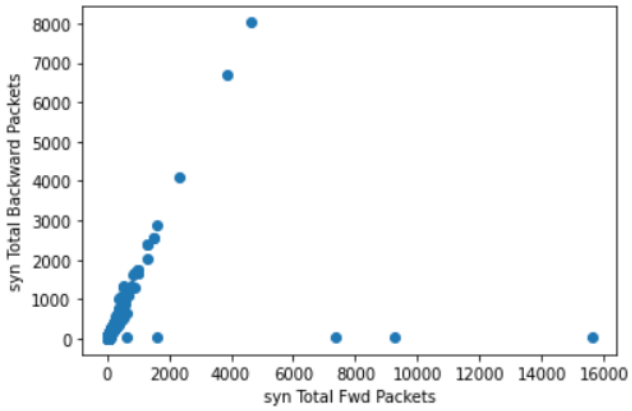
There seems to be a significant relation between two variables with a correlation of 0.77154954

Figure 4a: Scatter plot for Ideal traffic

```
The pearson's coeffient of the x and y inputs are:
 [[1.         0.77154954]
 [0.77154954 1.        ]]
```

Figure 4b: Pearson's coefficient for Ideal traffic

For SYN attack traffic dataset, a linear correlation was observed with r = 0.4423 with few outliers as seen in Fig. 5a and 5b.



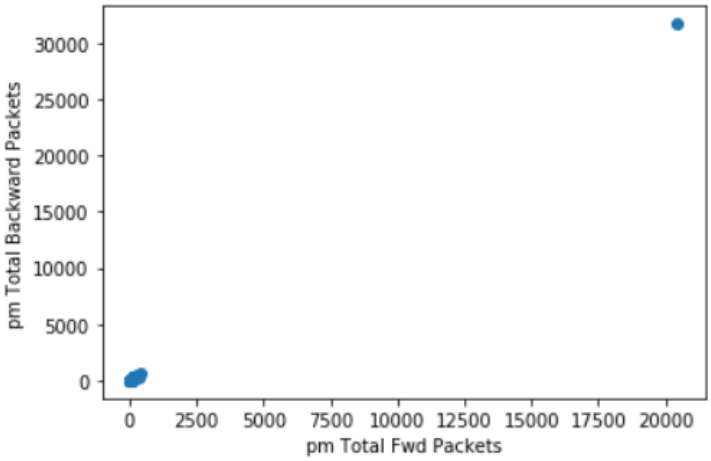
Except few outliers, there is a linear relationship between two variables. The correlation is low because of few outliers.

Figure 5a: Scatter plot for SYN attack traffic

```
The pearson's coeffient of the x and y inputs are:
 [[1.         0.44239957]
 [0.44239957 1.        ]]
```

Figure 5b: Pearson's coefficient for SYN attack traffic

For PortMap traffic dataset, a very high linear correlation was observed with r = 0.9997 as seen in Fig. 6a and 6b.



Except one outlier, all the variables are centered around zero. Correlation is also very high, i.e. 0.99973336

Figure 6a: Scatter plot for PortMap traffic

```
The pearson's coeffient of the x and y inputs are:
 [[1.         0.99973336]
 [0.99973336 1.        ]]
```

Figure 6b: Pearson's coefficient for PortMap traffic

5.3 Applying CVSS Environmental Score

The CVSS Environmental Score metrics are Exploitability Metrics, Impact Metrics, and Impact Subscore Modifiers. The Exploitability Metrics have the same variables as the Base Score and hence are not being modified. The variables of Impact and Impact Subscore Metrics and their possible values are given in the Table 6a and 6b respectively.

Impact Metrics	
Variable	Values
Confidentiality Impact (MC)	Not Defined/None/Low/High
Integrity Impact (MI)	Not Defined/None/Low/High
Availability Impact (MA)	Not Defined/None/Low/High

Table 6a: Impact Metrics – variable and values

Impact Subscore Modifiers	
Variable	Values
Confidentiality Requirement (CR)	Not Defined/None/Low/High
Integrity Requirement (IR)	Not Defined/None/Low/High
Availability Requirement (AR)	Not Defined/None/Low/High

Table 6b: Impact Subscore Modifiers – variables and values

In this step, ordinal weightage is assigned to the SYN attack and PortMap attacks based on the statistic analysis. The ordinal values are Not Defined, None, Low, and High. A low correlation coefficient value of Pearson's analysis means the number of packets sent or responded to is lower than number of packets received. This means the test component is highly impacted and hence 'High' impact is assigned. Following similar methodology of assigning ordinal weightage, the Table 7 is formulated.

'r' value (Attack type)	Methodology	Ordinal Score for CVSS
0.04423 (SYN)	High to Moderate Impact on Test Component	High
0.9997 (PortMap)	Low to No Impact on Test Component	Low

Table 7: The tested Pearson's Coefficient 'r' and the assigned score

The variables that are impacted is dependent on the vulnerability. For CVE-2021-22713, only Availability is impacted, hence the Availability Impact (MA) and Availability Requirement (AR) is set to "Low" for PortMap attack and "High" for SYN attack. For CVE-2017-6048, all three Availability, Integrity, and Confidentiality is impacted, hence all three variables of the metric will be modified accordingly. The CVSS vector is updated for CVEs and the results are documented.

6 Evaluation

Post implementation of the proposed methodology, four distinct results we obtained from the experiments conducted. These are the change in severity score of CVE-2021-22713 from attack analysis of SYN and PortMap attack and the change in severity score of CVE-2017-6048 from the same two attacks. The updated CVSS vector was passed as input to the CVSS module in python code, and the results are documented below.

6.1 Experiment 1 - CVE-2021-22713 with SYN attack

SYN attack showed a 'High' impact on the test component and since Base score of this CVE was only impacting the Availability variables, the updated CVSS vector is

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/**MA:H/AR:H**

The vector was passed as input to CVSS module and the updated CVSS score is 9.3 and the severity is moved up to Critical. This shows that the Smart Meter is highly sensitive to SYN flood DoS attacks and the component should be high on the security team's priority list for remediation.

```
CVE-2021-22713 vector with SYN attack =  CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/AR:H/MA:H
CVSS score =  (7.5, 7.5, 9.3)
Severity is ('High', 'High', 'Critical')
```

Figure 7a: Updated CVSS score for CVE-2021-22713 with SYN attack

6.2 Experiment 2 - CVE-2021-22713 with PortMap attack

The PortMap attack showed a 'Low' impact after analysing its attack data traffic on the test component and since Base score impact of this CVE is only limited to Availability, the updated CVSS vector is

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/**MA:L/AR:L**

The PortMap Passing this vector through the CVSS calculation code, the updated CVSS score drops down to 4.6 and severity is reduced to Medium. The drop is severity shows that Smart Meter being tested have low susceptibility towards PortMap attacks.

```
CVE-2021-22713 vector with PortMap attack =  CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/AR:L/MA:L
CVSS score =  (7.5, 7.5, 4.6)
Severity is ('High', 'High', 'Medium')
```

Figure 7b: Updated CVSS score for CVE-2021-22713 with PortMap attack

6.3 Experiment 3 – CVE-2017-6048 with SYN attack

This CVE's Base score shows impact on all three Availability, Integrity, and Confidentiality variables. The SYN attack showed a 'High' impact on the test component and updating the appropriate variables gives the CVSS vector

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/**MC:H/MI:H/MA:H/CR:H/IR:H/AR:H**

The updated CVSS vector gives updated CVSS score as 8.8 which is same as the Base score. The severity too remains the same at High. The result depicts that the Smart Meter with this vulnerability have low sensitivity towards SYN flood attacks.

```
CVE-2017-6048 vector with SYN attack =  CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/CR:H/IR:H/AR:H/MC:H/MI:H/MA:H
CVSS score =  (8.8, 8.8, 8.8)
Severity is ('High', 'High', 'High')
```

Figure 7a: Updated CVSS score for CVE-2017-6048 with SYN attack

6.4 Experiment 4 - CVE-2017-6048 with PortMap attack

The PortMap attack depicted a Low impact on the test component and its impact on all three variables gives the CVSS vector as

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/**MC:L/MI:L/MA:L/CR:L/IR:L/AR:L**

The updated CVSS vector shows the updated score as 4.8 and the severity is downgraded to 4.8. This result shows the Smart Meter with this vulnerability has lower susceptibility towards PortMap attacks.

```
CVE-2017-6048 vector with PortMap attack =  CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/CR:L/IR:L/AR:L/MC:L/MI:L/MA:L
CVSS score =  (8.8, 8.8, 4.8)
Severity is ('High', 'High', 'Medium')
```

Figure 7a: Updated CVSS score for CVE-2017-6048 with PortMap attack

6.5 Discussion

By following the proposed methodology and experiments conducted, a table is drawn with the updated CVSS score for each CVE. The updated score accurately reflects the performance of test component when subjected to the specific attack type. This is possible because the attack datasets are created from the simulation of the attack in a testbed lab environment which should closely reflect the production environment where the component is placed.

SYN packet flood attacks are one of the most common type of DoS attacks carried out by bad actors and they also have large adverse impact on the attacked component. The experimental showed that the CVSS score, and severity increased when the SYN attack test was performed. Importantly, for CVE-2017-6048, the SYN attack score remained the same showcasing that the characteristic of the vulnerability (depicted through Base score) also plays a role in final CVSS score of the component. The PortMap attack is generally not used for DoS attack and hence appropriately reduces the CVSS score and severity for both CVEs by quite a large margin.

This points to an important factor of selecting the appropriate parameter for a given type of attack. In this research, Sent and Received packets are selected for uniformity, to show comparable results, and availability of resources. In a live production environment, the choice of parameters should differ from one attack analysis to another as appropriate, and it will also have a critical impact on outcomes achieved.

Name	Base Score	Base Severity	Attack Type	Updated CVSS Score	Updated CVSS Severity
CVE-2021-22713	7.5	High	SYN	9.3	Critical
			PortMap	4.6	Medium
CVE-2017-6048	8.8	High	SYN	8.8	High
			PortMap	4.8	Medium

Table 6: Updated CVSS score

Lastly, it is important to discuss the inherent limitations of the CVSS system. It is introduced due to predefined values for each variable-value combination in CVSS. Although it provides the advantage of standardization across the different platforms and vendors that use the CVSS system, it is important to note that only 101 outcomes are possible between the values of 0.0 to 10.0. Another critical factor is multiple scoring combinations produce the

same CVSS score resulting in ambiguity errors. Some numeric scores may also be omitted due the variable-value combinations not deriving those specific values.

7 Conclusion and Future Work

With Cybersecurity taking an increasingly central role in design, development and maintenance of modern technologies, its accurate implementation in critical infrastructure power grid systems is important. Especially, the chosen cybersecurity assessment methods should enable security teams to develop fully customize and form a perfect-fit implementation for their environment. With the objective of answering the question of what security framework can be implemented in power grids, this research proposes a quantitative methodology to assess security of power grid components using CVSS and attack traffic data analysis. The CVSS Base score provides a baseline for the security vulnerability of the power grid component and the environment specific modifications in the score are obtained through Environmental Score obtained by simulated attack traffic analysis generated for that component.

The Base scores of CVE-2021-22713 and CVE-2017-6048 were baselined at 7.5 and 8.8. A comparative statistical analysis was performed between the Received Packets and Sent Packets of the attack traffic datasets of SYN flood DoS attack and PortMap attack network traffic dataset. The analysis results were weighted and used to update the Environmental Metric variables. The updated CVSS score for CVE-2021-22713 was 9.3 with SYN flood attack and 4.6 with PortMap attack. With similar method, the CVSS score for CVE-2017-6048 remained same at 8.8 with SYN flood attack and with PortMap attack was updated to and 4.8. This analysis showed that the Smart Meters with vulnerability CVE-2021-22713 are more susceptible to DoS attack and less towards PortMap attack whereas the ones with vulnerability CVE-2017-6048 will show same impact for a DoS attack and lower impact for PortMap attack.

With this assessment methodology, we are successfully able to demonstrate that a better suited security assessment can be carried out for Power Grids. The methodology can be scaled up and applied to the variety of Power Grid components with their CVSS score modified with specific attacks for that component group simulated in a lab environment. This will provide a clear metric to the security teams of vulnerable components in their grid and their behaviour towards different attacks assisting them in prioritizing remediation activities and reporting.

Some improvements that can be implemented in this research are building a lab testbed for simulating attacks providing datasets with wider attack types. Additionally, multiple components can be placed in the testbed with simultaneous attacks performed on them to generate complex attack datasets. These sorts of attacks are increasingly becoming common in the world where multi-layered attacks are performed targeting more than one component. For enterprise implementation, an application can be developed that will automate steps in this methodology to provide easy assessment of the power grid environment.

8 References

Aigner, A. and Khelil, A. (2020) ‘A Scoring System to Efficiently Measure Security in Cyber-Physical Systems’, in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1141–1145. Available at: https://doi.org/10.1109/TrustCom50675.2020.00151.

Burmester, M., Magkos, E. and Chrissikopoulos, V. (2012) ‘Modeling security in cyber–physical systems’, *International Journal of Critical Infrastructure Protection*, 5(3), pp. 118–126. Available at: https://doi.org/10.1016/j.ijcip.2012.08.002.

Choosing the Right Threat Modeling Methodology (no date) *TechWell*. Available at: https://www.techwell.com/techwell-insights/2020/05/choosing-right-threat-modeling-methodology (Accessed: 13 August 2022).

CVSS v3.0 Specification Document (no date) *FIRST — Forum of Incident Response and Security Teams*. Available at: https://www.first.org/cvss/v3.0/specification-document (Accessed: 10 August 2022).

Desarnaud, G. (no date) ‘Cyber Attacks and Energy Infrastructures’, p. 60.

Duy Le, T. *et al.* (2021) ‘CVSS Based Attack Analysis Using a Graphical Security Model: Review and Smart Grid Case Study’, in Y.-B. Lin and D.-J. Deng (eds) *Smart Grid and Internet of Things*. Cham: Springer International Publishing (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), pp. 116–134. Available at: https://doi.org/10.1007/978-3-030-69514-9_11.

Ertam, F. and Kaya, M. (2018) ‘Classification of firewall log files with multiclass support vector machine’, in *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, pp. 1–4. Available at: https://doi.org/10.1109/ISDFS.2018.8355382.

Humayed, A. *et al.* (2017) ‘Cyber-Physical Systems Security—A Survey’, *IEEE Internet of Things Journal*, 4(6), pp. 1802–1831. Available at: https://doi.org/10.1109/JIOT.2017.2703172.

Khalid, A. *et al.* (2018) ‘Security framework for industrial collaborative robotic cyber-physical systems’, *Computers in Industry*, 97, pp. 132–145. Available at: https://doi.org/10.1016/j.compind.2018.02.009.

Li, E. *et al.* (2019) ‘Quantitative Model of Attacks on Distribution Automation Systems Based on CVSS and Attack Trees’, *Information*, 10(8), p. 251. Available at: https://doi.org/10.3390/info10080251.

Mavridou, A. and Papa, M. (2012) *A Situational Awareness Architecture for the Smart Grid*, *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*. Available at: https://doi.org/10.1007/978-3-642-33448-1_31.

NVD - CVE-2017-6048 (no date). Available at: https://nvd.nist.gov/vuln/detail/CVE-2017-6048 (Accessed: 15 August 2022).

NVD - CVE-2021-22713 (no date). Available at: https://nvd.nist.gov/vuln/detail/CVE-2021-22713 (Accessed: 15 August 2022).

Orojloo, H. and Azgomi, M.A. (2014) ‘A method for modeling and evaluation of the security of cyber-physical systems’, in *2014 11th International ISC Conference on Information Security and Cryptology*, pp. 131–136. Available at: https://doi.org/10.1109/ISCISC.2014.6994036.

Sharafaldin, I. *et al.* (2019) 'Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy', in *2019 International Carnahan Conference on Security Technology (ICCST)*, pp. 1–8. Available at: https://doi.org/10.1109/CCST.2019.8888419.

Stellios, I., Kotzanikolaou, P. and Grigoriadis, C. (2021) 'Assessing IoT enabled cyber-physical attack paths against critical systems', *Computers & Security*, 107, p. 102316. Available at: https://doi.org/10.1016/j.cose.2021.102316.

Sun, C.-C., Hahn, A. and Liu, C.-C. (2018) 'Cyber security of a power grid: State-of-the-art', *International Journal of Electrical Power & Energy Systems*, 99, pp. 45–56. Available at: https://doi.org/10.1016/j.ijepes.2017.12.020.

Ten, C.-W., Liu, C.-C. and Govindarasu, M. (2007) 'Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees', in *2007 IEEE Power Engineering Society General Meeting*, pp. 1–8. Available at: https://doi.org/10.1109/PES.2007.385876.

Venkataramanan, V. *et al.* (2019) 'Measuring and Enhancing Microgrid Resiliency Against Cyber Threats', *IEEE Transactions on Industry Applications*, 55(6), pp. 6303–6312. Available at: https://doi.org/10.1109/TIA.2019.2928495.

Wang, R. *et al.* (2011) 'An Improved CVSS-based Vulnerability Scoring Mechanism', in *2011 Third International Conference on Multimedia Information Networking and Security*, pp. 352–355. Available at: https://doi.org/10.1109/MINES.2011.27.