

Firmware Analyzer of Intelligent Electronic Devices in Substations Based on Vulnerability Databases

Khoulood Gargouri¹ , Murat İskefiyeli² 

¹Institute of Science, Sakarya University, Sakarya, Türkiye, ror.org/04ttnw109

²Cyber Security Engineering, Sakarya University, Sakarya, Türkiye, ror.org/04ttnw109

Corresponding author:

Khoulood Gargouri, Sakarya University,
Institute of Science, Computer Engineering,
Cyber Security Program, Sakarya, Türkiye
khoulood.gargouri2@ogr.sakarya.edu.tr

Article History:

Received: 31.07.2025

Accepted: 08.09.2025

Published Online: 30.09.2025

ABSTRACT

In recent years, with the acceleration of digitalization, Intelligent Electronic Devices (IEDs) used particularly in energy transmission and distribution infrastructures have become one of the primary targets of cyber-attacks. This has made the detection and management of vulnerabilities in IEDs more challenging. Most energy system operators rely on security advisories published by vendors to identify security vulnerabilities. This study presents an approach aimed at automating this process. Manufacturer, model, hardware, and software version information of the devices is passively obtained from SCL files compliant with the IEC 61850 standard, and this data is correlated with the NVD, CWE, and vendor security bulletins to generate a comprehensive vulnerability report. In the implementations carried out in the CENTER-SAÜ test environment, the developed system was observed to produce accurate and complete results. The reports include the identified vulnerabilities and the risk level, attack vector, affected versions, patches and recommended mitigation measures for each vulnerability.

Keywords: Passive Vulnerability Scanning, Configuration Analysis, Intelligent Electronic Devices, Energy System

1. Introduction

Critical infrastructures are vital for national security, and their failure can significantly disrupt societal and economic order [1], [2]. In recent years, the proliferation of information and communication technologies has led to increased digitalization of operational technologies (OT) used in critical infrastructure sectors such as manufacturing, transportation, and energy, integrating them with Industrial Control Systems (ICS) [3]. ICS encompasses various subcomponents, including SCADA systems, Distributed Control Systems (DCS), and Programmable Logic Controllers (PLC) [4].

Given that the energy infrastructure underpins the continuity of other sectors, it is considered one of the most critical domains in scenarios of cyber warfare [3]. According to the statistics published by the Turkish Electricity Transmission Corporation (TEİAŞ), in 2023, the national transmission network managed by the organization comprised 74,441.6 km of high-voltage transmission lines [5] and 2,146 transformers [6]. Similarly, data from the Turkish Electricity Distribution Corporation (TEDAŞ) indicate that the total length of distribution lines reached 1,269,706.4 km in 2022 [7].

Securing these systems becomes even more apparent because of the vast geographical coverage and the high population served by energy transmission and distribution networks. However, these systems remain vulnerable to large-scale failures and cyber-attacks [8]. Past widespread power outages have demonstrated the practical impacts of these vulnerabilities. One of the most widely known events occurred on December 23, 2015, when cyber-attacks targeted three regional electricity distribution companies (Oblenergos) in Ukraine by disconnecting 7 units of 110 kV and 23 units of 35 kV substations from the grid. As a result, power outages affected approximately 225,000 customers for several hours [9], [10]. Consequently, cybersecurity of power systems has emerged as a critical research area [11].

Traditionally isolated, modern energy systems have become increasingly interconnected through IP-based communication protocols and open standards such as IEC 61850, designed for interoperability. While this transformation has facilitated many operational benefits, it has also introduced new security vulnerabilities. In particular, intelligent Electronic Devices (IEDs) play a pivotal role in grid control and protection functions. Cyber-attacks targeting these devices can disrupt the entire system's operation [12]–[14]. According to the U.S. National Institute of Standards and Technology (NIST), unpatched software represents one of the most significant vulnerabilities in any system [4], [15].

A report by the SANS Institute [16] indicates that ICS operators employ various tools and methods—including passive network monitoring and active vulnerability scanning—to detect software and hardware vulnerabilities within control system networks. Nevertheless, 61.2% of these operators also regularly monitor publicly disclosed security advisories and patch bulletins issued by vendors and relevant authorities. This study proposes a passive vulnerability detection (PVD)-based approach to automate this manual process. The proposed method processes vendor-issued security notifications for specific IEDs and transforms them into comprehensive, systematic vulnerability reports tailored to individual devices. This enables more efficient and timely tracking and management of security flaws.

Unlike active scanning methods, PVD can identify vulnerabilities without impacting system performance, yielding lower false positive rates [17], [18]. However, its effectiveness is highly dependent on the accuracy of the asset inventory. At present, many organizations lack complete or up-to-date inventories [19]. To address this challenge, the proposed approach analyzes IEC 61850 Substation Configuration Language (SCL) files to extract critical metadata—such as the manufacturer, model, hardware, and software versions of devices—and maps this information to a vulnerability database created for this work based on public databases (e.g., NVD and CWE) and vendor-issued security bulletins.

Moreover, the semi-automated tool developed in this study generates a list of vulnerabilities and a comprehensive report including risk levels, CWE classifications, affected versions, available patches, and recommended mitigation measures. This approach not only streamlines the manual analysis process but also holds the potential for constructing a broad vulnerability database across various vendors' IED products.

The primary contributions of this study are as follows:

- To our knowledge, this is the first study in the literature to perform vulnerability detection based on vendor-issued security advisories and bulletins. In doing so, it presents an innovative approach to identifying vulnerabilities specific to IEDs and addresses a notable gap in the existing body of research.
- Device-specific information has been automatically extracted from IEC 61850 configuration files and correlated with known vulnerabilities.
- A holistic vulnerability database using NVD, CWE, and vendor bulletins has been created.
- The proposed method introduces a passive alternative to active scanning techniques, eliminating associated performance risks.
- Experimental evaluations demonstrate the accuracy and applicability of the proposed approach.

This study aims to contribute to the early detection and management of security vulnerabilities in energy infrastructures via IEDs, while also offering a model that can be extended across different industry sectors.

The remainder of this study is structured as follows: First, fundamental concepts are defined. Next, vulnerability scanning techniques in ICS are examined in both technical and literature contexts, highlighting their strengths and limitations. Following that, the characteristics of IEDs, their vulnerability sources, and the types of attacks they enable are discussed. The study then explores the relevant aspects of the IEC 61850 standard, which governs the IEDs' communication structure and functional model. Subsequently, the proposed method, testing environment, and implementation process are described in detail. Finally, the results are evaluated, future research directions are suggested, and the study's key findings are summarized.

2. Fundamental Concepts

2.1. Vulnerability

The National Institute of Standards and Technology (NIST) defines a vulnerability as a “weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source” [20]. Essentially, vulnerabilities are defects in systems, applications, or services that allow attackers to circumvent security measures and perform unauthorized actions not intended by the original design [17], [21]. Known cybersecurity vulnerabilities and their related risks are systematically documented in the Common Vulnerabilities and Exposures (CVE) database [17], [22].

2.2. National Vulnerability Database (NVD)

The National Vulnerability Database (NVD) is a comprehensive platform for aggregating, managing, and distributing data on publicly known security vulnerabilities. Housing over 300,000 CVE entries, it is recognized as the largest and most extensively utilized vulnerability repository. Each CVE record within the NVD contains detailed information, including a description of the vulnerability, its risk score, severity rating, attack vector, and classification according to the Common Weakness Enumeration (CWE) framework [23]. As such, the NVD plays a crucial role in supporting the analysis and assessment of known security flaws.

2.3. Common Weakness Enumeration (CWE)

The Common Weakness Enumeration (CWE) is a structured classification of common software and hardware weaknesses that may result in security vulnerabilities. A weakness refers to a condition or flaw within software applications, firmware, hardware components, or services that, under specific conditions, can give rise to vulnerabilities. These weaknesses are typically introduced during the development process by the product's creators [24].

3. Literature Review

The security of smart grid systems is directly dependent on detecting and remedying software vulnerabilities in one of their core components: Intelligent Electronic Devices (IEDs). A majority of Industrial Control System (ICS) operators (more than 60%) rely on vendor-issued security advisories to track vulnerabilities and corresponding patches in their devices [16]. However, to date, no comprehensive study in literature aims to automate this process.

Most existing studies focus on comparing available vulnerability scanning tools or proposing new scanning techniques. For instance, El et al. (2017) evaluated Nessus and Burp Suite in the context of SCADA systems [25], [26], while McMahon et al. (2018) compared Nessus and OpenVAS for use in cyber-physical systems [27], [28]. Ecik (2021) experimentally compared Passive Vulnerability Detection (PVD) and Active Vulnerability Scanning (AVS), demonstrating that PVD offered higher accuracy and reduced scanning time [17]. The approach presented in this study builds upon PVD, supported by CPE and NVD databases, to develop a semi-automated method.

Similarly, Samtani (2016) conducted a vulnerability assessment of SCADA systems using passive and active techniques. He developed a Python script capable of automatically cross-referencing devices found on Shodan—based on manufacturer, product, and version information—with entries in the NVD [21]. However, this work did not conduct an in-depth evaluation of the accuracy or effectiveness of the methods employed.

Popular tools such as Nessus and OpenVAS, frequently used in ICS security assessments, were originally designed for Information Technology (IT) systems. Consequently, their capability to detect specific vulnerabilities in Operational Technology (OT) environments is limited, and their active scanning techniques pose risks of disrupting critical systems. Studies numbered [29]–[31] in the literature emphasize the necessity of developing more tailored, targeted security tools that account for the unique characteristics of ICS infrastructure.

In response to this need, several innovative research efforts have emerged. For example, Shirani et al. (2018) proposed a three-phase passive detection engine and a vulnerability database to identify flawed functions in ARM-based IED software [32], [33]. Xia et al. (2020) developed an ICS-specific vulnerability scanner based on OpenVAS that outperformed the traditional tool in effectiveness [14]. However, tools like OpenVAS still fail to identify vulnerabilities outside the network (e.g., local device firmware).

Lastly, several studies [34]–[39] have focused not on directly identifying IED vulnerabilities but on evaluating the cyber-attack risks that may arise from such vulnerabilities. Given the existing gaps, there is a critical need to develop automated, OT-specific systems that can passively correlate IED vulnerabilities using device-specific version and configuration data.

4. IEDs: Characteristics, Attacks, And Sources of Vulnerabilities

4.1. Definition and Characteristics of IEDs

Intelligent Electronic Devices (IEDs) are multifunctional units equipped with one or more processors, capable of receiving and transmitting data from external sources [40], [41]. These devices, enhanced with advanced microprocessors and communication technologies, perform core functions such as monitoring, control, protection, measurement, and communication in an integrated manner. In modern energy infrastructures, IEDs have become essential for remote monitoring and control, which is critical in enhancing system reliability and efficiency [40], [42].

IEDs are typically categorized into three main types: control, monitoring, and protection IEDs. Control IEDs process and transmit commands that direct system behavior, while monitoring and relaying, IEDs convert analog signals into digital data that can be shared across the network. Protection IEDs safeguard components such as transmission lines, transformers, and busbars, and ensure system integrity by operating circuit breakers during fault conditions [32], [43], [44].

Interoperability among IEDs is supported through open communication protocols such as Modbus, DNP3, IEC 60870-5, and notably IEC 61850, enabling integration across devices from different vendors [44], [45]. However, adopting Ethernet and TCP/IP-based communication technologies has exposed IEDs to network and internet connectivity, rendering them susceptible to cyber threats. The complexity of their software and hardware architecture further increases the likelihood of exploitable vulnerabilities. If an IED is compromised, attackers may inflict physical damage on critical systems, manipulate measurement data, or trigger cascading system failures with potentially catastrophic consequences [45].

In this context, the cybersecurity of IEDs is of paramount importance. Enhancing security requires the identification of vulnerabilities in both software and hardware components, followed by implementing appropriate preventive measures.

4.2. Common Sources of IED Vulnerabilities

Attackers often exploit one or more existing vulnerabilities within a device—including IEDs—to launch cyberattacks. Among these are non-software-related issues such as unchanged default passwords, weak password policies, lack of limits on failed authentication attempts, unrestricted packet rates, and the transmission of unencrypted or unsigned sensitive data [12], [45].

Table 1 presents various software-specific vulnerability sources associated with IEDs and potential exploitation methods that can be used to launch attacks. This study aims to identify and assess such vulnerabilities.

Table 1. Software-related vulnerability sources in IEDs and associated attack methods [12], [45].

Vulnerability	Description
Vulnerabilities arising from third-party software components and operating systems	Third-party software may not have undergone comprehensive security testing and could contain exploitable vulnerabilities. Once integrated into the target device, these vulnerabilities are transferred to the system. Examples include the TCP/IP stack [46], [47], security stack, and operating system [48], [49].
Debug and test features left in production versions	Displaying debug information may reveal device functionality, allowing attackers to understand internal behaviors. Backdoors enabled for debugging can be exploited to escalate privileges and access sensitive information.
Poor design and coding practices	This category includes a range of issues of varying complexity, such as insufficient input validation [50], race conditions [51], buffer overflows [52], [53], and memory leaks. Attack types depend on the specific vulnerability. For example: <ul style="list-style-type: none"> • If input validation is weak or missing, attackers may enter out-of-range values that the internal logic cannot handle, potentially causing device crashes. • Memory leaks can be exploited to exhaust system memory, rendering the device non-functional. • Buffer overflows may allow attackers to write outside allocated memory, leading to system crashes or code execution. • Absence of usage limits can be abused to consume computational resources and degrade performance.

4.3. Types of Cyberattacks Targeting IEDs

While Intelligent Electronic Devices (IEDs) play a critical role in the operation of energy systems, they have become increasingly vulnerable to cyber threats. A cyberattack on an IED often serves as the initial stage of a larger coordinated assault, aiming to gain control over the device and infiltrate other system components. Such attacks can generally be classified into five main categories [45]:

Direct Control of Actuators: Attackers may impersonate authorized operators and send direct commands to actuator IEDs, such as circuit breakers. These intrusions can lead to multiple outages or cascading failures within the grid [45]. Real-world examples illustrating the impact of such control manipulation include the 2007 Aurora vulnerability [54] and the 2015 cyberattacks on Ukraine’s power grid [55].

Measurement Manipulation Attacks: Energy management systems rely heavily on accurate measurements for decision-making. Manipulating data from IEDs can disrupt system stability and lead to erroneous operational decisions [45], [56]. Common examples include False Data Injection Attacks (FDIA) [57], [58], where fabricated data is used for state estimation, and Replay Attacks [59], in which previously recorded sensor data is retransmitted to mislead the system.

Resource Exhaustion and Response Delay Attacks: These attacks involve flooding IEDs with excessive data, consuming their communication and processing resources and rendering them nonfunctional. Time-sensitive systems, such as Denial-of-Service (DoS) attacks, can prevent the timely activation of corrective actions, potentially resulting in widespread system failures [45], [60].

Time Synchronization Attacks: Many critical applications within power grids rely on precise time data. Manipulating GPS signals can corrupt the timestamps of IEDs, leading to deviations in sampling and event detection processes [61]. By injecting spoofed GPS signals, attackers can cause receivers to calculate incorrect time offsets [62].

Attacks on Relay Protection Schemes: Cyberattacks may target individual relay IEDs and entire protection schemes [63]. In agent-based systems in particular, attackers may disrupt inter-relay communication to execute coordinated attacks. Such actions can undermine the stability of the power system and result in severe consequences [64], [65].

5. Vulnerability Scanning/Detection Techniques

Continuous and systematic scanning efforts are essential for identifying security vulnerabilities before they can be exploited [15]. Achieving such continuity and accuracy through manual methods is highly challenging. Therefore, using automated tools to detect vulnerabilities has become inevitable [18]. In modern systems, two primary and widely accepted scanning approaches are employed: Active Vulnerability Scanning (AVS) and Passive Vulnerability Detection (PVD) [21].

5.1. Active Vulnerability Scanning (AVS)

The active scanning approach identifies potential security vulnerabilities by transmitting data to systems and analyzing the responses [17], [18]. These responses reveal details such as software version and patch status. Techniques commonly used in this approach include port scanning, SQL injection testing, brute-force password attempts, and deployment of malicious payloads [18], [21].

Popular AVS tools include Nmap, Zmap, Burp Suite, SQLMap, Nessus, and OpenVAS [21]. However, due to its intrusive nature, AVS may introduce additional network load and potentially compromise the stability of industrial systems [66], [67]. Two incidents documented in the NIST (2023) report highlight the potential risks associated with AVS. In the first, a simple ping scan on a SCADA network caused a robotic arm in standby mode to activate and move uncontrollably. In the second case, a production line system crashed during an inventory scan, damaging a semiconductor wafer worth \$50,000. These examples demonstrate that active scanning techniques must be applied cautiously and under controlled conditions in ICS environments [15].

5.2. Passive Vulnerability Detection (PVD)

Unlike active methods, the passive approach does not interact directly with the network or systems. Instead, it gathers information about system components from existing data sources (e.g., network traffic, inventory records). The identified products are matched with CVE entries in vulnerability databases [15], typically through Common Platform Enumeration (CPE) identifiers [17]. PVD allows for continuous monitoring without compromising system stability. Vulnerability detection is generally conducted based on pre-established asset inventories or supported by traffic analysis tools.

5.3. Comparison of AVS and PVD Approaches

The advantages and limitations of both approaches are compared below across several criteria [17], [68]:

- **Coverage:** The detection capacity of AVS tools is limited by the integrated CVE database [17], [18]. For example, while the NVD contains over 300,000 CVEs [69], Nessus reportedly supports just over 100,000. In contrast, PVD can theoretically access the entire database.
- **Timeliness:** Creating AVS test scenarios takes time. PVD may also experience delays due to dependency on CPE updates in the NVD [17], [70].
- **Visibility:** AVS may miss components due to firewalls or offline systems. PVD is unaffected by such barriers [17].
- **Speed:** AVS can be time-consuming due to the depth of its scans, whereas PVD is faster as it utilizes pre-existing data [68], [71].
- **Scalability:** The performance of AVS is directly affected by network size, while PVD operates independently of this factor [17].
- **Side Effects:** AVS can increase network traffic and affect system stability. PVD is immune to such impacts [15], [71].
- **Scanning Frequency:** AVS is performed periodically, while PVD enables continuous monitoring [71].
- **Reliability:** Both methods may yield false positives or negatives. AVS errors may arise from incomplete scripts, while PVD may encounter inaccuracies due to CPE-based matching issues [17].

Given these advantages, this study focuses on passive vulnerability detection and proposes a method that performs vulnerability matching based on static information extracted from devices.

5.4. Challenges in CPE-Based Detection

The most employed technique in PVD is to match system components, identified via their CPE identifiers, with CVE-CPE records in vulnerability databases. However, this method presents several limitations [17], [72], [73]:

- **CVE Entries Without CPE Identifiers:** Some CVE records in the NVD lack corresponding CPE entries, which hinders the detection process and can lead to false negatives.

- **CPE-CVE Synchronization Gaps:** Are CVE records linked to CPE identifiers not listed in the CPE dictionary? Additionally, deprecated CPEs are sometimes still used in outdated CVE entries.
- **Inconsistent CPE Assignments:** Different sources (e.g., NVD, vendor advisories) may assign varying CPEs for the same product, complicating the assessment of data accuracy and currency.

For these reasons, this study does not rely solely on CPE-based detection. Instead, it incorporates alternative data sources—such as vendor advisories, Common Weakness Enumeration (CWE), and the NVD—to perform vulnerability correlation based on static information extracted from IEDs.

6. The Asset Inventory Problem

Maintaining a robust and up-to-date asset inventory is a fundamental requirement for ensuring the security of critical infrastructures, including energy systems [66]. Asset inventories form the foundation of various cybersecurity processes such as vulnerability scanning, risk management, configuration analysis, and system obsolescence tracking. However, professionals from both Information Technology (IT) and Operational Technology (OT) domains emphasize that building an accurate inventory is a costly, time-consuming, and challenging process [74], [75]. These difficulties have resulted in many industrial facilities lacking a comprehensive and current asset management system [19].

Four primary methods are commonly used for asset discovery: passive network scanning, active network scanning, configuration analysis, and physical inspection. Passive scanning detects devices by monitoring network traffic without interfering with the system. In contrast, active scanning communicates directly with devices to gain broader visibility, but it risks causing failures in OT environments. Configuration analysis identifies assets using static data retrieved from control systems, while physical inspection is typically employed in scenarios where automation is not feasible. Although it is thorough, this method is also labor-intensive [74].

Thanks to the IEC 61850 standard, particularly in digital substations, critical information such as manufacturer, model, hardware, and software versions can be obtained from configuration files. This standard facilitates more effective application of configuration analysis and helps reduce incompatibilities in heterogeneous environments [3].

In conclusion, this study proposes updating incomplete or inaccurate asset information by analyzing IED configuration files before vulnerability detection. This approach aims to enhance the accuracy and scope of passive vulnerability scanning.

7. IEC 61850 Standards: Definition, Modeling, and Configuration Language

IEC 61850 is a global standard developed by the International Electrotechnical Commission (IEC) and published in 2003, aimed at standardizing communication among Intelligent Electronic Devices (IEDs) used in substations [76]. It is not merely a communication protocol; it offers a comprehensive framework for the design, engineering, and operation of substation automation systems [77]. The standard includes detailed technical specifications for Ethernet-based communication, object-oriented data modeling, and application programming interfaces (APIs) [78]. This architecture facilitates device self-configuration, significantly reducing the burden of manual engineering tasks [76].

IEC 61850 defines device data within a hierarchical, object-oriented structure [78]. Physical devices are abstracted into Logical Devices (LD), which consist of multiple Logical Nodes (LN). Each Logical Node is associated with a specific power system function and comprises Data Objects (DO) that are structured according to Common Data Classes (CDC) and are described by various attributes (DA) subject to Functional Constraints (FC). This modeling approach enables all data objects to be uniquely addressable and accessible over the network via the MMS protocol defined in IEC 61850-8-1 [76], [79].

For instance, suppose we have a logical device named "AA1C1Q02A2" representing a specific IED, and we wish to determine its firmware version. To do this, it would be necessary to access and read the data object illustrated in Figure 1.

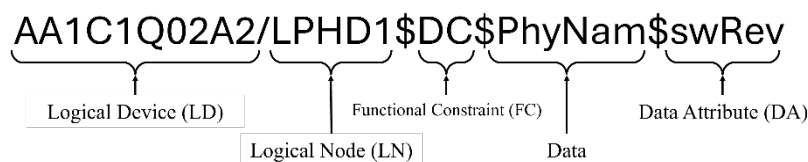


Figure 1. Object Naming Anatomy in IEC 61850-8-1.

One of the key components of the standard, the Substation Configuration Language (SCL), defines the configuration of IEC 61850 systems using an XML-based structure [76], [80]. SCL files provide detailed documentation of device specifications and system topology, facilitating interoperability among manufacturers [76], [81]. These files can be generated using commercial tools such as IEDScout [82] and PCM600 [83], or with open-source software such as IEDExplorer [84].

In this study, a passive vulnerability detection approach based on the analysis of device attributes via SCL files is adopted. This method offers a reliable foundation for assessing the security of IEC 61850-compliant IEDs.

8. Testbed Environment

Within the scope of this study, experimental analyses were carried out using the infrastructure of the National Testbed Center for Critical Infrastructures (CENTER-Energy), located at Sakarya University. CENTER-Energy provides a comprehensive testing environment where energy generation, transmission, distribution, and consumption can be realistically modeled, offering researchers a practical platform for conducting experimental studies on critical infrastructure security [85].

The testbed setup consists of two separate substations, TM-1 and TM-2. Energy generated by the production unit is transmitted through TM-1 at medium voltage, stepped up to high voltage for transfer to TM-2, and subsequently stepped down again for distribution. To ensure the safety of the power system throughout this process, protection components such as transformer differential relays, distance protection relays, and overcurrent relays are employed. Additionally, the field signals from circuit breakers and disconnectors are modeled using auxiliary relays. The TM-1 station is controlled using SICAM SCC SCADA, Siemens, ABB, and GE relays, along with a Siemens RTU; whereas the TM-2 station is supervised using an ABB Micro SCADA system, ABB and Schneider relays, and an ABB RTU [86].

The tests conducted in this study were specifically carried out on three different Intelligent Electronic Devices (IEDs) from ABB's Relion® series—REF615, REL650, and RET670—located in the TM-1 substation. The Relion® series consists of advanced IEDs that support protection, control, and monitoring functions in power systems based on the IEC 61850 standard [87]. These devices support features within the scope of IEC 61850, such as process data (measurements and status information), application data (protection activations, fault records), control commands, configuration information, setting groups, disturbance records, time synchronization, and inter-device GOOSE/SV messaging [77].

9. Methodology

9.1. Construction of a Vulnerability Database

To fulfill the objective of this study, a dedicated vulnerability database was developed based on security advisories published by a specific vendor for their particular device models. A passive vulnerability scanning method was adopted in this context. The conventional CVE–CPE correlation approach, commonly used in practice, exhibits several shortcomings. Notably, security advisories issued by manufacturers such as ABB typically do not reference Common Platform Enumeration (CPE) identifiers but provide model names, design standards, and details on hardware/software version. This makes it difficult to associate device-specific vulnerabilities with traditional vulnerability databases directly.

Furthermore, national vulnerability databases (e.g., NVD) focus primarily on third-party software components without specifying which devices incorporate these components. For instance, ABB has documented that its REL650 and RET670 devices with hardware version 2.1 are affected by vulnerabilities in the OpenSSL library—specifically CVE-2016-2177, CVE-2016-2178, CVE-2016-2182, CVE-2016-2183, CVE-2016-6304, and CVE-2016-6306 [88]. However, these CVE records do not reference the affected device models or manufacturers [89]–[94].

Therefore, in this study, a customized vulnerability database was developed based on technical documentation published by the vendor. This database includes device-specific technical details such as model, design standard, hardware, and software versions. Technical descriptions of the vulnerabilities were integrated from standard databases such as CWE and NVD to enrich the correlation and analysis process.

9.2. Parsing of SCL Files

The official IEC 61850 standard documentation, the HMI interfaces of ABB's REF615, REL650, and RET670 IED models within the CENTER Energy test environment, and the corresponding SCL files retrieved from these devices were examined. As a result of the analysis, it was determined that the following key information is embedded within specific data objects:

- Manufacturer information: "LPHD1\$DC\$PhyNam\$vendor"
- Model information: "LPHD1\$DC\$PhyNam\$model"
- Software version: "LPHD1\$DC\$PhyNam\$swRev"
- Serial number: "LPHD1\$DC\$PhyNam\$serNum"
- Order code (if available): "LDEV1\$EX\$NamPlt\$eOrdNum"
- Hardware revision (if available): "LINF1\$EX\$NamPlt\$eDevRev"

These data objects demonstrate that IEDs' fundamental identity and configuration information can be passively obtained from SCL files, without requiring active interrogation.

9.3. Filtering Process in the Vulnerability Database

By analyzing ABB's product manuals, technical documentation, and published security advisories, several insights were derived to guide the vulnerability filtering process for device-specific assessments:

- ABB markets the same IED models under different design standards (IEC, ANSI, and CN) [95], [96]. As a result, even when devices share the same version, the associated vulnerabilities and applicable patches may vary depending on the design standard [97].
- The unique alphanumeric order codes of ABB devices encapsulate critical information, including design standard identifiers. For instance, the second character of the order code signifies the design standard, where "A" indicates ANSI, "B" refers to IEC, and "C" represents CN. While design standards may not be explicitly specified in SCL files or HMI interfaces, they can be inferred from the order code [98], [99].
- ABB IEDs are categorized into specific product series (e.g., 615, 650, 670) [100] and also belong to the broader *Relion*® product family [87]. Security advisories may identify affected products by model, series, family name, or combinations thereof, such as "REF615," "Relion 650," "Relion 670 series," or "615 series IEC 5.0 FP1."

Accordingly, the software tool developed in this study was designed to account for all possible identifier variations to ensure no vulnerability is overlooked. The detection process yields more accurate and comprehensive vulnerability assessments by performing a cross-validation of all device-related parameters.

10. Utilized Tools

Various tools were employed in this study to extract configuration data from IEDs and conduct vulnerability analyses. The Python programming language was selected due to its flexibility and widespread use in cybersecurity applications. Vulnerability data was stored in a MySQL relational database for efficient querying and management.

The open-source and freely available IEDEplorer tool was used to acquire SCL files. This software supports MMS protocol communication with IEC 61850 devices and enables data reading/writing, reporting, and GOOSE message analysis [84].

In addition, the Nmap tool was employed to identify the IP addresses of IEDs within the network. Specifically, ARP scanning, which is considered a safe technique for Operational Technology (OT) environments [30], proved effective in detecting unknown device IPs.

11. Proposed Approach

This study proposes a three-stage methodology for detecting vulnerabilities in IEDs, as illustrated in Figure 2, consisting of: Preparation, Manual Operations, and Automated Processing.

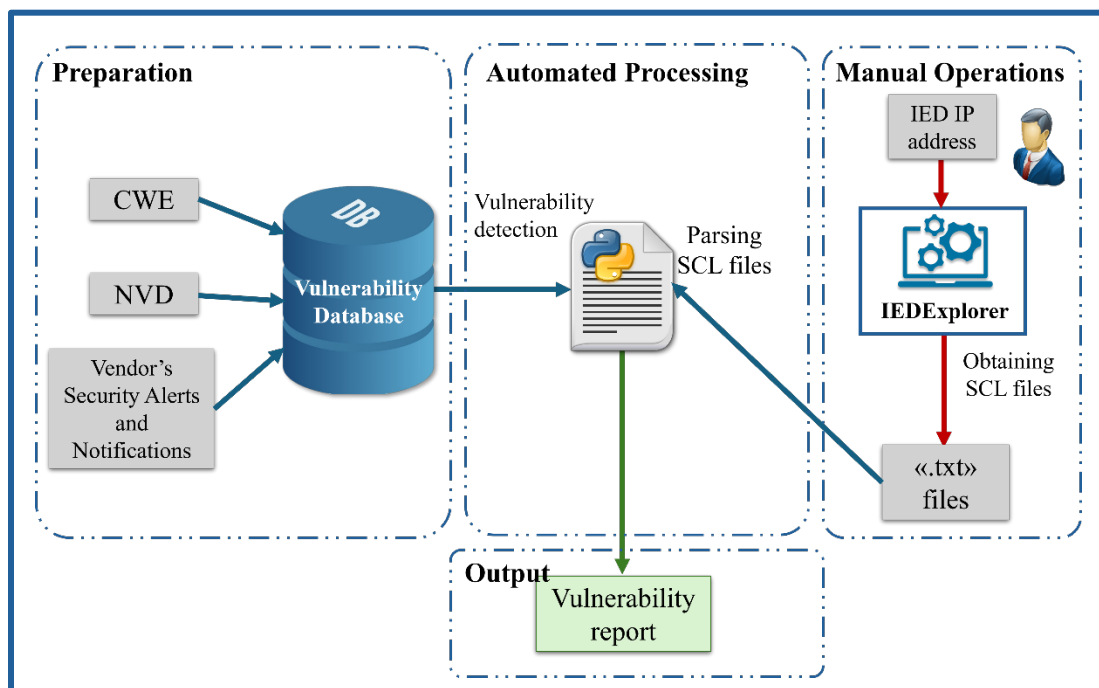


Figure 2. Overview of the Proposed Approach.

In the **Preparation** phase, a comprehensive vulnerability database was constructed by analyzing security advisories published by ABB and publicly available sources such as the National Vulnerability Database (NVD) and the Common Weakness Enumeration (CWE). This database includes CVE/CWE identifiers, vulnerability descriptions, affected models, firmware versions, patch details, and recommended mitigation strategies. Although the current implementation comprises a single table named “ABB,” it has been designed to be extensible to accommodate other manufacturers (e.g., Siemens, GE) in the future.

In the **Manual Operations** phase, the IP addresses of IEDs within the target system are identified via asset inventory or through a secure ARP scan. Each device is then accessed using the IEDEplorer tool, and its SCL file is extracted and saved in “.txt” format, named according to the device’s IP address. From this point forward, the analysis continues offline.

The flow of the **Automated Processing phase is as shown** in Figure 3. During this phase, the user is provided with three analysis options:

- In **single-device analysis**, the SCL file of the device corresponding to the entered IP address is parsed to extract device-specific information, such as model, manufacturer, and hardware/software versions. Unique identifiers like the order code determine the device’s design standard and product family. This information is then cross-referenced with the vulnerability database to identify applicable security issues. A device-specific vulnerability report presents the device information, its vulnerabilities, and recommended countermeasures.
- In **IP range analysis**, devices' data within a specified range is extracted, and all vulnerabilities are consolidated into a single report.
- In **manual information entry**, the user inputs the device information, which is then compared with the database to generate a security report.

The user can also specify the sorting criteria for vulnerabilities in the vulnerability report; sorting can be done by publication date (chronological) or CVSS score and can be selected in ascending or descending order.

This approach enables security vulnerabilities in IEDs deployed within digital substations to be effectively identified, providing cybersecurity professionals with detailed and device-centric remediation recommendations.

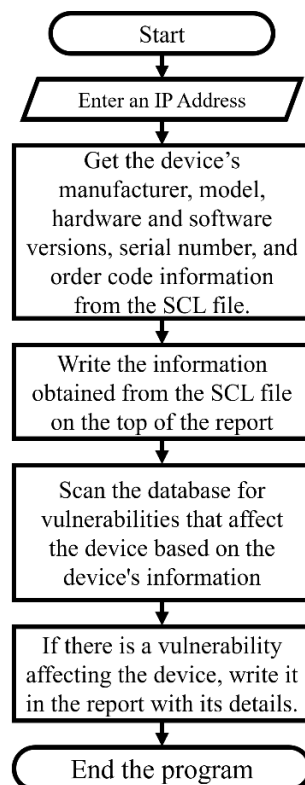


Figure 3. Automated processing flow.

12. Scan Results and Evaluation

The developed program was tested on ABB’s REF615, REL650, and RET670 models. The results of parsing the SCL files of these three devices and scanning their vulnerabilities are written to the vulnerability report created by the program, as shown in Figure 4. a–c.

As a result of the scanning process, no vulnerabilities were identified in the REL650 and RET670 models. However, seven medium-level security vulnerabilities were detected in the REF615 device of the IEC standard, 5.0 FP1 hardware version and 5.1.17 firmware version. These vulnerabilities were documented in detail, accompanied by their corresponding CVE and CWE identifiers, patch requirements and recommended mitigation strategies. An example of how one of the identified vulnerabilities in the REF615 device is presented in the report is illustrated in Figure 4.c.

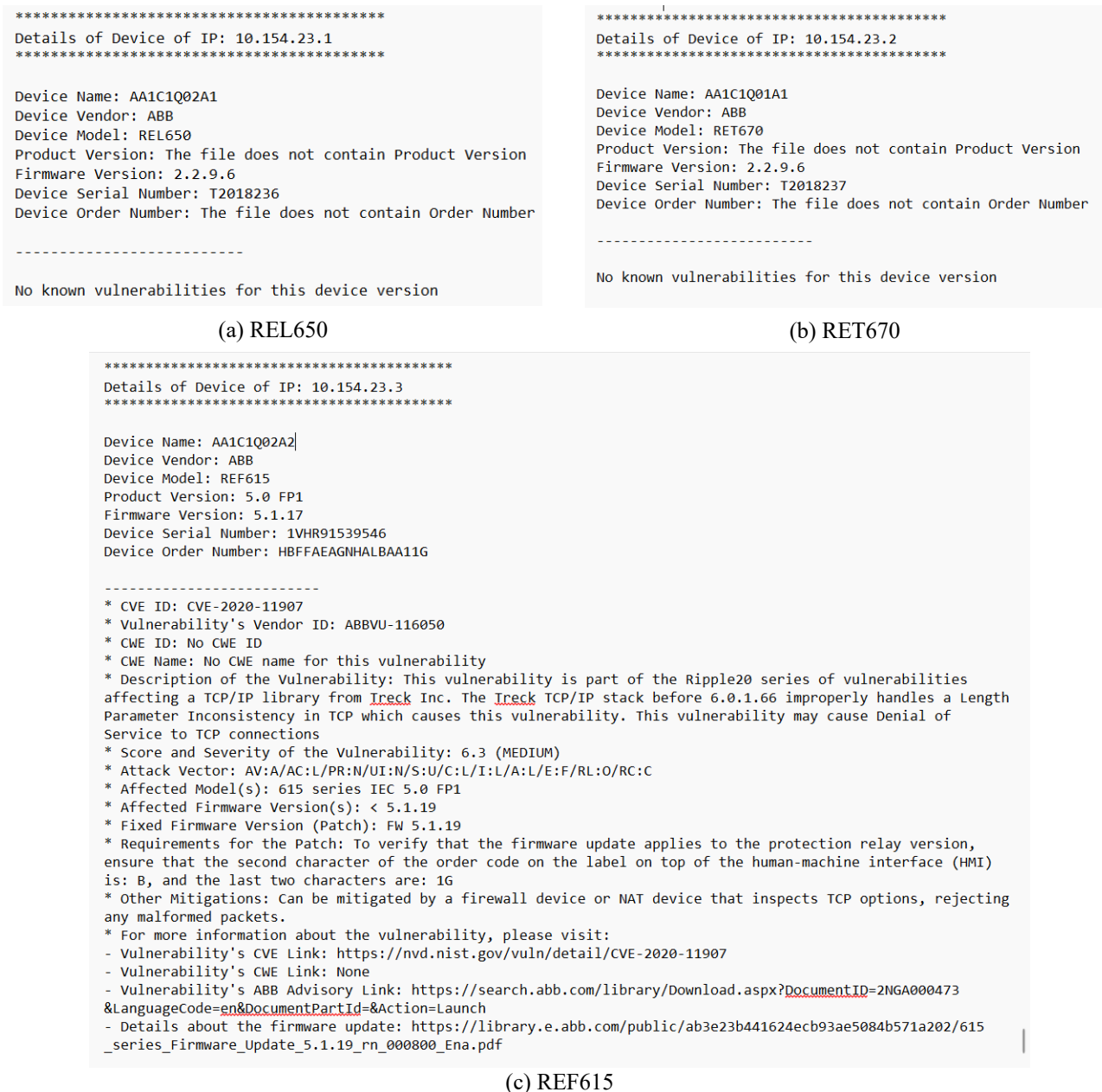


Figure 4. Device information extracted from parsing SCL files is an example of the result of vulnerability filtration.

The list of vulnerabilities identified in the REF615 device is summarized in Table 2.

Table 2. Summary of the vulnerabilities affecting REF615.

CVE ID	CWE ID and Name	CVSS score and Severity	Affected Firmware Version(s)	Patch
CVE-2020-11907	No CWE ID and Name for this vulnerability	6.3 (Medium)	5.1.19	FW 5.1.19
CVE-2020-11909	CWE-191: Integer Underflow (Wrap or Wraparound)	5.3 (Medium)	< 5.1.19	FW 5.1.19
CVE-2020-11910 And CVE-2020-11912	CWE-125: Out-of-Bound Read	5.3 (Medium)	< 5.1.19	FW 5.1.19
CVE-2020-11911	CWE-732: Incorrect Permission Assignment for Critical Resource	5.3 (Medium)	< 5.1.19	FW 5.1.19
CVE-2021-22283	CWE-665: Improper Initialization	6.2 (Medium)	< 5.1.20	FW 5.1.20
CVE-2024-8036	CWE-347: Improper Verification of Cryptographic Signature	5.9 (Medium)	All versions	No patch found

The accuracy of the devices’ information extracted from SCL files was verified through manual cross-checks using the Human-Machine Interfaces (HMIs) and the corresponding SCL files. When the vulnerability database was manually reviewed and compared with the results produced by the developed program, it was observed that the program delivered accurate and complete outcomes.

In conclusion, this study presents a semi-automated approach capable of processing vendor security advisories and generating comprehensive vulnerability reports for Intelligent Electronic Devices (IEDs) used in smart grid systems. By leveraging static device information extracted from SCL files, the developed tool successfully filtered CVE entries in the database and produced accurate results.

The primary challenge of this approach is analyzing the diverse documentation and reporting formats adopted by different manufacturers and transforming them into a unified and standardized database structure. This normalization process requires systematically examining each vendor’s device classifications and security advisories. However, once established, this database is a sustainable and reusable resource, offering significant value to the research community.

In the case of ABB, security advisories issued before 2025 were manually processed. Starting in 2025, however, adopting the Common Security Advisory Framework (CSAF) can enable the preparatory phase of the proposed approach to be automated in future studies.

13. Future Work

The findings of this study offer several avenues for future research, providing opportunities for both enhancement and expansion. Potential directions for further investigation include:

- Research can be conducted on methods that enable the automated retrieval of SCL files from IED devices using the IEDEXplorer tool. This would allow the data collection process to be fully automated, eliminating the need for manual intervention.
- The current scope, limited to devices in the CENTER Energy test environment, can be expanded by building a more comprehensive vulnerability database that includes various IED models from different vendors. This extended database would facilitate testing the developed program across a wider range of devices.
- To ensure the vulnerability database remains up-to-date, a component can be developed that regularly monitors newly published security advisories and automatically parses and integrates them into the database using web scraping techniques.
- The device information extracted from the SCL parsing process could be exported in various data formats and integrated into existing asset management systems within organizations. This would enable automatic updates of asset records based on the parsed data.
- The current implementation, focused solely on IED devices, may be expanded to generate vulnerability assessment reports for other ICS components. Although the proposed database structure and filtering algorithms are suitable for such an expansion, it is important to note that the IEC 61850 standard governs communication among IEDs. SCL files are

unique to this standard. Therefore, the primary challenge for non-IED systems is obtaining static device information. In this context, if an organization's existing asset inventory system is reliable and up to date, the necessary data can be sourced from there. Otherwise, alternative methods for acquiring such information must be researched and new approaches developed.

10. Conclusion

This study proposed a semi-automated approach for passively detecting software-specific vulnerabilities in Intelligent Electronic Devices (IEDs). IEC 61850-compliant Substation Configuration Language (SCL) files automatically extracted technical attributes such as manufacturer, model, hardware, and software versions. These attributes were then cross-referenced with entries from a database that was established in the context of this study, taking information from the National Vulnerability Database (NVD), the Common Weakness Enumeration (CWE), and vendor-issued security advisories to generate a comprehensive vulnerability report.

Compared to active scanning techniques, the proposed system offers a faster and less intrusive method of conducting security assessments, thus maintaining the operational continuity of Industrial Control Systems (ICS). Experimental results demonstrated that the developed program delivered accurate and complete outcomes. In addition to listing vulnerabilities, the system provides detailed information on each vulnerability, including descriptions, risk levels, attack vectors, affected versions, patches, and recommended mitigations.

This work is one of the few studies that automatically analyzes known vulnerabilities and generates device-specific security reports, enhancing cybersecurity in Operational Technology (OT) environments. Future work will focus on expanding the system to include devices from different vendors and integrating it with real-time monitoring solutions.

References

- [1] AFAD, *2014-2023 Kritik Altyapıların Korunması: Yol Haritası Belgesi*. 2014.
- [2] A. Pinto, L.-C. Herrera, Y. Donoso, and J. A. Gutierrez, "Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure," *Sensors*, vol. 23, no. 5, p. 2415, Feb. 2023, doi: 10.3390/s23052415.
- [3] P. E. Weerathunga and A. Cioraca, "Securing IEDs against cyber threats in critical substation automation and industrial control systems," in *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, Apr. 2017, pp. 1–20, doi: 10.1109/CPRE.2017.8090048.
- [4] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," Gaithersburg, MD, Jun. 2015. doi: 10.6028/NIST.SP.800-82r2.
- [5] TEİAŞ, "GRAFİK VI.I- TÜRKİYE İLETİM HAT UZUNLUKLARININ GELİŞİMİ (2013-2023)," 2024. [Online]. Available: <https://www.teias.gov.tr/turkiye-elektrik-uretim-iletim-istatistikleri>.
- [6] TEİAŞ, "GRAFİK VI.III- TÜRKİYE TRAFİKO ADETLERİNİN GELİŞİMİ (2013-2023)," 2024. [Online]. Available: <https://www.teias.gov.tr/turkiye-elektrik-uretim-iletim-istatistikleri>.
- [7] TEDAŞ, "2023 Yılı Türkiye Elektrik Dağıtım Sektör Raporu," 2024. [Online]. Available: <https://www.tedas.gov.tr/FileUpload/MediaFolder/25819eac-d024-4308-891a-d248db8c1e0a.pdf>.
- [8] A. Abedi, L. Gaudard, and F. Romerio, "Review of major approaches to analyze vulnerability in power systems," *Reliab. Eng. Syst. Saf.*, vol. 183, no. November, pp. 153–172, Mar. 2019, doi: 10.1016/j.res.2018.11.019.
- [9] CISA, "Cyber-Attack Against Ukrainian Critical Infrastructure," *ICS Alert*, 2021. <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01> (accessed Jul. 14, 2025).
- [10] ISA, "Ukrainian power grids cyberattack," *ISA's Flagship Publications*, 2017. <https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack>.
- [11] V. S. Rajkumar, M. Tealane, A. Stefanov, and P. Palensky, "Cyber attacks on protective relays in digital substations and impact analysis," *8th Work. Model. Simul. Cyber-Physical Energy Syst. MSCPES 2020 - Proc.*, 2020, doi: 10.1109/MSCPES49613.2020.9133698.
- [12] P. E. Weerathunga and A. Cioraca, "The importance of testing Smart Grid IEDs against security vulnerabilities," *69th Annu. Conf. Prot. Relay Eng. CPRE 2016*, pp. 1–21, 2017, doi: 10.1109/CPRE.2016.7914920.
- [13] IEEE, "Cybersecurity of Critical Infrastructure with ICS/SCADA Systems," *IEEE Public Safety Technology*. <https://publicsafety.ieee.org/topics/cybersecurity-of-critical-infrastructure-with-ics-scada-systems/> (accessed Jul. 15, 2025).
- [14] Y. Xia, J. Wang, C. Liu, and K. Yu, "Design and Implementation of Vulnerability Scanning Tools for Intelligent Substation Industrial Control System Based on Openvas," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 440, no. 4, p.

- 042031, Feb. 2020, doi: 10.1088/1755-1315/440/4/042031.
- [15] K. Stouffer *et al.*, “Guide to Operational Technology (OT) security,” Sep. 2023. doi: 10.6028/NIST.SP.800-82r3.
- [16] M. Bristow, “A SANS 2021 Survey: OT/ICS Cybersecurity.” [Online]. Available: <https://www.sans.org/white-papers/SANS-2021-Survey-OTICS-Cybersecurity/>.
- [17] H. Ecik, “Comparison of Active Vulnerability Scanning vs. Passive Vulnerability Detection,” in *2021 International Conference on Information Security and Cryptology (ISCTURKEY)*, Dec. 2021, no. December, pp. 87–92, doi: 10.1109/ISCTURKEY53027.2021.9654331.
- [18] D. Kennedy, J. O’Gorman, D. Kearns, and M. Aharoni, *Metasploit: The Penetration Tester’s Guide*. William Pollock, 2011.
- [19] B. Filkins and D. Wylie, “SANS 2019 State of OT/ICS Cybersecurity Survey,” 2019. [Online]. Available: <https://sansorg.egnyte.com/dl/6hWfMGKRKwqx>.
- [20] NIST, “Minimum security requirements for federal information and information systems,” 2006. doi: 10.6028/NIST.FIPS.200.
- [21] S. Samtani, S. Yu, H. Zhu, M. Patton, and H. Chen, “Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques,” in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, Sep. 2016, pp. 25–30, doi: 10.1109/ISI.2016.7745438.
- [22] CVE Numbering Authority (CNA), “Common Vulnerabilities and Exposures,” 2000. <https://www.cve.org/> (accessed Jul. 12, 2025).
- [23] NIST, “NVD Dashboard,” *NVD*, 2025. <https://nvd.nist.gov/general/nvd-dashboard> (accessed Jul. 17, 2025).
- [24] MITRE, “Common Weakness Enumeration (CWE).” <https://cwe.mitre.org/> (accessed Jun. 21, 2025).
- [25] M. El, E. McMahon, S. Samtani, M. Patton, and H. Chen, “Benchmarking vulnerability scanners: An experiment on SCADA devices and scientific instruments,” in *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, Jul. 2017, pp. 83–88, doi: 10.1109/ISI.2017.8004879.
- [26] M. EL, “Benchmarking vulnerability scanners: An experiment on SCADA devices and scientific instruments,” THE UNIVERSITY OF ARIZONA, 2017.
- [27] E. McMahon, M. Patton, S. Samtani, and H. Chen, “Benchmarking Vulnerability Assessment Tools for Enhanced Cyber-Physical System (CPS) Resiliency,” in *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, Nov. 2018, vol. 945, no. 05 0, pp. 100–105, doi: 10.1109/ISI.2018.8587353.
- [28] E. McMahon, “Benchmarking Vulnerability Assessment Tools for Enhanced Cyber-Physical System (CPS) Resiliency,” THE UNIVERSITY OF ARIZONA, 2018.
- [29] E. Samanis, J. Gardiner, and A. Rashid, “A Taxonomy for Contrasting Industrial Control Systems Asset Discovery Tools,” in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, Aug. 2022, pp. 1–12, doi: 10.1145/3538969.3538979.
- [30] L. Pöhler, M. Schuba, T. Höner, S. Hack, and G. Neugebauer, “An Open-Source Approach to OT Asset Management in Industrial Environments,” in *Proceedings of the 10th International Conference on Information Systems Security and Privacy*, 2024, vol. 1, no. Icissp, pp. 128–136, doi: 10.5220/0012362200003648.
- [31] NISTIR 7628, “Guidelines for smart grid cybersecurity,” Gaithersburg, MD, Sep. 2014. doi: 10.6028/NIST.IR.7628r1.
- [32] P. Shirani *et al.*, “BINARM: Scalable and Efficient Detection of Vulnerabilities in Firmware Images of Intelligent Electronic Devices,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10885 LNCS, 2018, pp. 114–138.
- [33] L. Collard, “Fingerprinting Vulnerabilities In Intelligent Electronic Device Firmware,” Concordia University, 2018.
- [34] Q. S. Qassim, N. Jamil, M. Daud, A. Patel, and N. Ja’affar, “A review of security assessment methodologies in industrial control systems,” *Inf. Comput. Secur.*, vol. 27, no. 1, pp. 47–61, 2019, doi: 10.1108/ICS-04-2018-0048.
- [35] H. Wen, “Vulnerability Assessment of Industrial Control System with an Improved CVSS,” *ArXiv Prepr.*, Jun. 2023, [Online]. Available: <http://arxiv.org/abs/2306.08631>.
- [36] M. Alonso, J. Turanzas, H. Amaris, and A. T. Ledo, “Cyber-physical vulnerability assessment in smart grids based on multilayer complex networks,” *Sensors*, vol. 21, no. 17, 2021, doi: 10.3390/s21175826.
- [37] W. Shang, T. Gong, J. Hou, J. Lu, and Z. Cao, “Quantitative Evaluation Method for Industrial Control System

- Vulnerability Based on Improved Expert Elicitation and Fuzzy Set Method,” *IEEE Access*, vol. 11, no. August, pp. 101007–101019, 2023, doi: 10.1109/ACCESS.2023.3314629.
- [38] S. Alhasawi, “ICSrank: A Security Assessment Framework for Industrial Control Systems (ICS),” Liverpool John Moores University, 2020.
- [39] U. D. Ani, J. Watson, H. He, P. Radanliev, and G. Epiphaniou, “Minimising cybersecurity risk exposures in industrial control system environments: a techno-human vulnerability analysis approach,” *J. Cyber Secur. Technol.*, vol. 00, no. 00, pp. 1–40, Nov. 2024, doi: 10.1080/23742917.2024.2421589.
- [40] C.-L. Hor and P. A. Crossley, “Knowledge Extraction from Intelligent Electronic Devices,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 3400 LNCS, no. November, 2005, pp. 82–111.
- [41] J. D. McDonald, “Substation automation. IED integration and availability of information,” *IEEE Power Energy Mag.*, vol. 1, no. 2, pp. 22–31, Mar. 2003, doi: 10.1109/MPAE.2003.1192023.
- [42] M. Abdulrazzaq and Y. Wei, “Industrial Control System (ICS) Network Asset Identification and Risk Management,” HALMSTAD UNIVERSITY, 2018.
- [43] B. M. R. Amin, M. J. Hossain, A. Anwar, and S. Zaman, “Cyber Attacks and Faults Discrimination in Intelligent Electronic Device-Based Energy Management Systems,” *Electronics*, vol. 10, no. 6, p. 650, Mar. 2021, doi: 10.3390/electronics10060650.
- [44] X. Huang, Z. Qin, and H. Liu, “A Survey on Power Grid Cyber Security: From Component-Wise Vulnerability Assessment to System-Wide Impact Analysis,” *IEEE Access*, vol. 6, pp. 69023–69035, 2018, doi: 10.1109/ACCESS.2018.2879996.
- [45] J. Wang and D. Shi, “Cyber-Attacks Related to Intelligent Electronic Devices and Their Countermeasures: A Review,” in *2018 53rd International Universities Power Engineering Conference (UPEC)*, Sep. 2018, pp. 1–6, doi: 10.1109/UPEC.2018.8542059.
- [46] NIST, “CVE-2020-11907 Detail,” *NVD*, 2020. <https://nvd.nist.gov/vuln/detail/CVE-2020-11907> (accessed May 07, 2024).
- [47] ABB, “TCP Predictability Vulnerability in Relion® 670 series version 2.0 ABB-VU-PGGA-1MRG019772,” 2016. [Online]. Available: <https://publisher.hitachienergy.com/preview?DocumentID=1MRG023264&LanguageCode=en&DocumentPartId=&Action=Launch>.
- [48] NIST, “CVE-2019-12256 Detail,” *NVD*, 2022. <https://nvd.nist.gov/vuln/detail/CVE-2019-12256> (accessed May 15, 2024).
- [49] ABB, “WindRiver VxWorks IPNet Vulnerabilities , impact on Relion 670 , Relion 650 , SAM600-IO series ABBVU-PGGA-Relion670-1MRG035814 ABBVU-PGGA-Relion650-1MRG035815 ABBVU-PGGA-SAM600-IO-1MRG035816,” 2020. [Online]. Available: <https://device.report/m/6b0850dd3f66a375b47f30730f75243a64672806995ae4acdb8d542aeb4649f.pdf>.
- [50] MITRE, “CWE-20: Improper Input Validation,” *CWE*, 2023. <https://cwe.mitre.org/data/definitions/20.html> (accessed Apr. 25, 2024).
- [51] MITRE, “CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization (‘Race Condition’),” *CWE*, 2023. <https://cwe.mitre.org/data/definitions/362.html> (accessed May 16, 2024).
- [52] MITRE, “CWE-120: Buffer Copy without Checking Size of Input (‘Classic Buffer Overflow’),” *CWE*, 2023. <https://cwe.mitre.org/data/definitions/120.html> (accessed Jun. 29, 2024).
- [53] MITRE, “CWE-121: Stack-based Buffer Overflow,” *CWE*, 2023. <https://cwe.mitre.org/data/definitions/121.html> (accessed May 16, 2024).
- [54] D. Salmon, M. Zeller, A. Guzman, V. Mynam, and M. Donolo, “Mitigating the Aurora Vulnerability With Existing Technology,” in *36th Annual Western Protective Relay Conference*, 2009, no. October 2009, pp. 1–7, [Online]. Available: https://cdn.selinc.com/assets/Literature/Publications/TechnicalPapers/6392_MitigatingAurora_MZ_20090918_Web.pdf.
- [55] NCCIC, “IR-ALERT-H-16-043-01AP CYBER-ATTACK AGAINST UKRAINIAN CRITICAL INFRASTRUCTURE,” 2016. [Online]. Available: https://nsarchive.gwu.edu/sites/default/files/documents/4164304/Department-of-Homeland-Security-NCCIS-ICS-CERT.pdf?utm_source=chatgpt.com.

- [56] S. Sridhar and M. Govindarasu, "Model-Based Attack Detection and Mitigation for Automatic Generation Control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014, doi: 10.1109/TSG.2014.2298195.
- [57] S. Mangalwedekar, S. K. Surve, and H. A. Mangalvedekar, "False Data Injection Attacks and detection scenarios in the power system," in *2015 Annual IEEE India Conference (INDICON)*, Dec. 2015, no. 8, pp. 1–6, doi: 10.1109/INDICON.2015.7443817.
- [58] E.-N. S. Youssef and F. Labeau, "False Data Injection Attacks Against State Estimation in Smart Grids: Challenges and Opportunities," in *2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE)*, May 2018, vol. 2018-May, no. 1, pp. 1–5, doi: 10.1109/CCECE.2018.8447683.
- [59] T.-T. Tran, O.-S. Shin, and J.-H. Lee, "Detection of replay attacks in smart grid systems," in *2013 International Conference on Computing, Management and Telecommunications (ComManTel)*, Jan. 2013, pp. 298–302, doi: 10.1109/ComManTel.2013.6482409.
- [60] R. Kalluri, L. Mahendra, R. K. S. Kumar, and G. L. G. Prasad, "Simulation and impact analysis of denial-of-service attacks on power SCADA," in *2016 National Power Systems Conference (NPSC)*, Dec. 2016, no. 1, pp. 1–5, doi: 10.1109/NPSC.2016.7858908.
- [61] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time Synchronization Attack in Smart Grid: Impact and Analysis," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 87–98, Mar. 2013, doi: 10.1109/TSG.2012.2227342.
- [62] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Dominguez-Garcia, "Spoofing GPS Receiver Clock Offset of Phasor Measurement Units," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 3253–3262, Aug. 2013, doi: 10.1109/TPWRS.2013.2240706.
- [63] R. Bulbul, Y. Gong, C.-W. Ten, A. Ginter, and S. Mei, "Impact quantification of hypothesized attack scenarios on bus differential relays," in *2014 Power Systems Computation Conference*, Aug. 2014, pp. 1–7, doi: 10.1109/PSCC.2014.7038497.
- [64] M. S. Rahman, H. R. Pota, and M. J. Hossain, "Cyber vulnerabilities on agent-based smart grid protection system," in *2014 IEEE PES General Meeting | Conference & Exposition*, Jul. 2014, vol. 2014-October, no. October, pp. 1–5, doi: 10.1109/PESGM.2014.6939298.
- [65] J. Zhang and Y. Dong, "Cyber attacks on remote relays in smart grid," in *2017 IEEE Conference on Communications and Network Security (CNS)*, Oct. 2017, vol. 2017-Janua, pp. 1–9, doi: 10.1109/CNS.2017.8228637.
- [66] M. Niedermaier, T. Hanka, S. Plaga, A. von Bodisco, and D. Merli, "Efficient Passive ICS Device Discovery and Identification by MAC Address Correlation," in *Proceedings of ICS & SCADA 2018*, Aug. 2018, pp. 21–30, doi: 10.14236/ewic/ICS2018.3.
- [67] A. Wedgbury and K. Jones, "Automated Asset Discovery in Industrial Control Systems - Exploring the Problem," 2015, pp. 73–83, doi: 10.14236/ewic/ICS2015.8.
- [68] R. Gula, "Passive Vulnerability Detection," *Netw. Secur. Wizards*, vol. 9, p. 7, 1999, [Online]. Available: https://markowsky.us/papers/net-papers/gula_passive_vulnerability_detection.pdf.
- [69] Tenable® Inc, "Plugins," 2025. <https://www.tenable.com/plugins> (accessed Jul. 17, 2025).
- [70] M. Gawron, F. Cheng, and C. Meinel, "PVD: Passive vulnerability detection," in *2017 8th International Conference on Information and Communication Systems (ICICS)*, Apr. 2017, pp. 322–327, doi: 10.1109/IACS.2017.7921992.
- [71] R. Deraison, R. Gula, and T. Hayton, "Passive vulnerability scanning: Introduction to NeVO," 2003. [Online]. Available: https://ouah.lescigales.org/passive_scanning_tenable.pdf.
- [72] L. Alberto, B. Sanguino, and R. Uetz, "Software Vulnerability Analysis Using CPE and CVE."
- [73] R. J. Thomas, J. Gardiner, T. Chothia, E. Samanis, J. Perrett, and A. Rashid, "Catch Me If You Can: An In-Depth Study of CVE Discovery Time and Inconsistencies for Managing Risks in Critical Infrastructures," in *Proceedings of the 2020 Joint Workshop on CPS&IoT Security and Privacy*, Nov. 2020, pp. 49–60, doi: 10.1145/3411498.3419970.
- [74] M. Bristow, "SANS White Paper - ICS Asset Identification: It's More Than Just Security," 2020. [Online]. Available: <https://www.sans.org/white-papers/39650/>.
- [75] N. Wallace and B. Proctor, "Passive Real-Time Asset Inventory Tracking and Security Monitoring of Grid-Edge Devices," in *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, Apr. 2018, vol. 2018-April, doi: 10.1109/TDC.2018.8440434.
- [76] R. E. Mackiewicz, "Overview of IEC 61850 and Benefits," in *2006 IEEE PES Power Systems Conference and*

- Exposition*, 2006, vol. 57, no. 57, pp. 623–630, doi: 10.1109/PSCE.2006.296392.
- [77] ABB, *615 series IEC 61850 Engineering Guide*, G. ABB, 2012.
- [78] A. Hadbah, T. S. Ustun, and A. Kalam, “Using IEDScout software for managing multivendor IEC61850 IEDs in substation automation systems,” in *2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Nov. 2014, pp. 67–72, doi: 10.1109/SmartGridComm.2014.7007624.
- [79] ABB, *630 series IEC 61850 Communication Protocol Manual*, A. ABB, 2009.
- [80] P. Lloret, J. L. Velasquez, L. Molas-Balada, R. Villafafila, A. Sumper, and S. Galceran-Arellano, “IEC 61850 as a flexible tool for electrical systems monitoring,” in *2007 9th International Conference on Electrical Power Quality and Utilisation*, Oct. 2007, pp. 1–6, doi: 10.1109/EPQU.2007.4424193.
- [81] SIEMENS, *SIPROTEC 5 Transformer Differential Protection 7UT82, 7UT85, 7UT86, 7UT87 V9.90 and Higher Manual*, 11.2024. SIEMENS, 2024.
- [82] Omicron, “IEDScout: Versatile software tool for working with IEC 61850 devices,” 2024. <https://www.omicronenergy.com/en/products/iedscout/> (accessed Jul. 10, 2025).
- [83] ABB, “Simplifying management of protection and control relays with PCM600 - Protection and control IED manager.” <https://new.abb.com/medium-voltage/digital-substations/software-products/protection-and-control-ied-manager-pcm600> (accessed Jul. 10, 2025).
- [84] Pavel Charvat, “IEDEXplorer,” 2013. <https://sourceforge.net/projects/iedexplorer/> (accessed Jun. 15, 2024).
- [85] Sakarya Üniversitesi, “Kritik Altyapılar Ulusal Test Yatağı Merkezi,” *CENTER-SAU*, 2023. <https://center.sakarya.edu.tr/> (accessed Jul. 20, 2025).
- [86] I. Ozcelik, M. Iskefiyeli, M. Balta, K. Ovaz Akpınar, and F. S. Toker, “CENTER Energy: A Secure Testbed Infrastructure Proposal for Electricity Power Grid,” in *2021 International Conference on Information Security and Cryptology (ISCTURKEY)*, Dec. 2021, no. December, pp. 149–154, doi: 10.1109/ISCTURKEY53027.2021.9654352.
- [87] ABB, “Relion protection and control.” <https://new.abb.com/medium-voltage/digital-substations/relion> (accessed Jul. 06, 2025).
- [88] ABB, “OpenSSL vulnerabilities in Relion® 650 series version 2.1 and Relion® 670 series version 2.1 ABB-VU-PGGA-1MRG024369 ABB-VU-PGGA-1MRG025160,” 2019. [Online]. Available: <https://publisher.hitachienergy.com/preview?DocumentID=9AKK107492A9254&LanguageCode=en&DocumentPartId=&Action=Launch>.
- [89] NIST, “CVE-2016-2177 Detail,” *NVD*, 2016. <https://nvd.nist.gov/vuln/detail/cve-2016-2177> (accessed Jul. 28, 2025).
- [90] NIST, “CVE-2016-2178 Detail,” *NVD*, 2016. <https://nvd.nist.gov/vuln/detail/cve-2016-2178> (accessed Jul. 28, 2025).
- [91] NIST, “CVE-2016-2182 Detail,” *NVD*, 2016. <https://nvd.nist.gov/vuln/detail/cve-2016-2182> (accessed Jul. 28, 2025).
- [92] NIST, “CVE-2016-2183 Detail,” *NVD*, 2016. <https://nvd.nist.gov/vuln/detail/cve-2016-2183> (accessed Jul. 28, 2025).
- [93] NIST, “CVE-2016-6304 Detail,” *NVD*, 2016. <https://nvd.nist.gov/vuln/detail/cve-2016-6304> (accessed Jul. 28, 2025).
- [94] NIST, “CVE-2016-6306 Detail,” *NVD*, 2016. <https://nvd.nist.gov/vuln/detail/cve-2016-6306> (accessed Jul. 28, 2025).
- [95] ABB, “Feeder protection and control REF615 IEC.” <https://new.abb.com/medium-voltage/digital-substations/protection-relays/feeder-protection-and-control/feeder-protection-and-control-ref615-iec> (accessed Jul. 15, 2025).
- [96] ABB, “Feeder protection relay REF615 ANSI.” <https://new.abb.com/medium-voltage/digital-substations/protection-relays/feeder-protection-and-control/feeder-protection-relay-ref615-ansi> (accessed Jul. 15, 2025).
- [97] ABB, “Firmware update releases for digital substation products.” <https://new.abb.com/medium-voltage/digital-substations/protection-relay-services/firmware-update-release> (accessed Jul. 06, 2025).
- [98] ABB, *Feeder protection relay REF615 ANSI Product Guide*. ABB Inc., 2007.

[99] ABB Oy., *Feeder Protection and Control REf615 Product Guide*. ABB Oy., 2010.

[100] ABB, *RELION® 615 SERIES: Feeder Protection and Control REF615 Application Manual*. ABB, 2021.

Authors Contributions

Acknowledgments

We would like to express our sincere gratitude to all who contributed to the development, implementation and maintenance of the Critical Infrastructures National Testbed Center (CENTER-Energy) for their efforts in establishing such a robust and practical experimental research environment that has significantly enriched this study. We would like to thank them especially for giving us the opportunity to conduct our experiments in such a well-equipped and realistic environment, which played a crucial role in the practical validation of this study.

Conflict of Interest Notice

The authors declare that there is no conflict of interest regarding the publication of this paper.

Ethical Approval

It is declared that during the preparation process of this study, scientific and ethical principles were followed, and all the studies benefited from are stated in the bibliography.

Availability of data and material

Not applicable / or link

Artificial Intelligence Statement

No artificial intelligence tools were used while writing this article.

Plagiarism Statement

This article has been scanned by iThenticate™.