On Automated and Standardized Asset, Vulnerability and Patch Management in the Power Grid

Qi Liu, Arman A. Attar, Kaibin Bao, Peter Noglik, Martin Gottschalg, Veit Hagenmeyer, *Member, IEEE*

***Abstract*—Proper and timely vulnerability and patch management depend on a comprehensive, accurate and easily maintainable asset inventory, which in turn rests on standardized and automated information gathering procedures. In practice, the information gathering process may not provide all information required to determine if a device is vulnerable and the criticality of patching it. This considerably slows down the patch processes. Challenges in information gathering arise due to the heterogeneity of devices and systems deployed in an environment like the power grid and the lack of standardized protocols across the industry. In this article, we examine existing popular protocols, and identify their deficiencies for asset information gathering. We highlight the challenges in automated vulnerability and patch management through our experiments, in which we also evaluate and compare commercial products. Following this, we propose a new schema to streamline the information gathering process and improve the consistency during information gathering across devices of various vendors, which would ultimately contribute to proper and timely vulnerability and patch management.**

***Index Terms*—Asset inventory, vulnerability management**

I. Introduction

Proper asset, vulnerability and patch management are critical to a strong resilience against cyber threats in grid operators' operational technology (OT) networks. Currently, there is no well-adopted open technical solution to manage assets, their firmware and software state and the deployed configuration. In commercial solutions, the asset information gathering step alone relies on hand-crafted information scraping mechanisms. Asset discovery, as the first step of vulnerability & patch management, seeks to identify all assets in an organization. Conventionally, asset discovery is done manually through audits and reports. These inventories are not necessarily updated regularly, leading to gaps in visibility.

In practice, vulnerability & patch management is a laborious and error-prone process especially for large organizations, as it involves extensive manual effort to gather, analyze, and organize information from a variety of sources and ad-hoc document formats [1]. Typical sources include vulnerability tracking databases like NIST NVD (National Vulnerability Database) [2], national/international CERT advisories, product vendor security advisories. The number of published vulnerabilities has been increasing each year rapidly. This overwhelms security teams, increases the risk of human error.

The authors gratefully acknowledge funding by the German Federal Ministry of Research, Technology and Space (BMFTR) within the Kopernikus Project ENSURE 'New ENergy grid StructURes for the German Energiewende'. We thank Michael Gratza from TenneT, Bastian Bauhaus from Stadtwerke Kiel, Marc Jachenholz, Alen Murtovi from Westfalen Weser Netz, and Max Dauer, Anne Bauer from Siemens AG for their participation in our discussions.

Undoubtedly, organizations would greatly benefit from standardization and automation of the entire vulnerability & patch management process, which enables ongoing oversight of identified and addressed vulnerabilities. Continuous monitoring can significantly reduce the time window that attackers have to exploit a vulnerability, comparing to the traditional approach, in which vulnerabilities are addressed when identified through scheduled scans and left unaddressed between scans. The Common Security Advisory Framework (CSAF) [3] was introduced to address the problem that advisories including those provided by product vendors themselves are often incomplete and have a range of non-standardized formats. CSAF reduces the operational complexity and enhances the scalability of vulnerability tracking and management with a standardized advisory format and distribution method. It defines a number of attributes deemed as required to identify product versions affected in a vulnerability disclosure.

However, CSAF does not address the problems occurring during information gathering. That is, data formats of asset information and the procedure for information querying are not standardized. In other words, although CSAF seeks to standardize several aspects of vulnerability disclosure & patch management, it does not give a guideline to support the asset discovery step, and hence fails to provide a CSAF consuming organization with clear visibility into their infrastructures. Without a clear visibility, vulnerable products in an organization's infrastructures may not be identified timely, leading to incomplete vulnerability & patch management cycle.

Together with participants from power electronics vendors and grid operators in Germany, we have built a test environment, which includes representative equipment — protection relays, controllers, switches — across multiple vendors and generations. In particular, we include several popular devices for grid automation, protection and control, e.g., Hitachi RTU530, Siemens SIPROTEC and Siemens SICAM A8000. We employed popular protocols like SNMP, MMS (IEC 61850), OPC UA, and RESTCONF to query these devices, i.e., information gathering for asset discovery. Then we connected to other data sources like vulnerability databases and the emerging Digital Product Passport. We also looked at engineering tools for fleet, device, and configuration management to understand how patches are currently performed. We found that it is difficult to realize automation and deployment at scale due to high complexity.

In this study, we make the following contributions. First, we examine existing protocols used for asset, vulnerability, and patch management in practice. Second, we analyze concepts and technologies closely related to asset, vulnerability and patch management. Third, we evaluate and compare commer-

This article has been accepted for publication in IEEE Transactions on Power Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2026.3725276

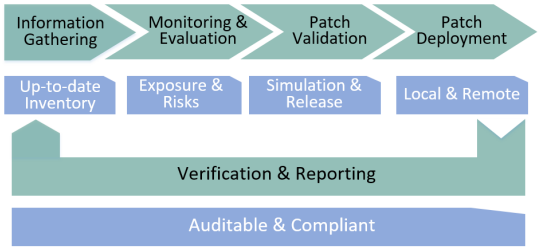

Fig. 1: A structured path forward according to IEC 62443-2-3.

cial products for asset, vulnerability and patch management. Finally, we propose a new schema that may help streamline asset information gathering process.

II. Analysis of Existing Technologies

While the convergence of IT and OT domains brings substantial benefits in terms of automation and monitoring, it also introduces challenges in security and lifecycle management. There is an urgent need for structured OT asset, vulnerability and patch management to ensure visibility, reduce cyber risk, and maintain grid reliability. Grid operators face numerous challenges in effective asset and patch management across their OT landscape. Many struggle with incomplete or inconsistent asset inventories due to a lack of standardization. The lack of automation makes it difficult to ensure that all devices are secure, and operating with validated settings. Advances on asset, vulnerability and patch management are not discussed in scientific literature often. Hence, in the following, we compile a list of topics related to asset, vulnerability and patch management, including guidelines, technical protocols, related concepts and commercial products.

A. Standards and guidelines for the management process

IEC 62443-2-3 [4] focuses on security for OT systems, provides guidance on patch management for industrial automation and control systems (IACS), and is applicable to power generation, transmission, distribution systems. Power grid, as a critical IACS environment, includes SCADA systems, protection relays, RTU etc.; all require patch management per IEC 62443-2-3. In Figure 1, we show a structured approach to vulnerability & patch management in industrial environments aligned with IEC 62443-2-3. The proposed process consists of five iterative steps: information gathering, monitoring & evaluation, patch validation, patch deployment, verification & reporting. First, we perform information gathering to identify each device installed in our infrastructure. Second, we evaluate whether there are vulnerabilities in those devices, assess the risk based on certain context. Third, a patch needs to be properly validated in realistic conditions before its release. Then, approved patches are distributed in a secure manner. Finally, continuous verification of changes and reporting them in an audit-proof way conclude the process. Note that Figure 1 is protocol-agnostic.

NIST SP 1800-5 [5] covers topics spanning traditional physical asset tracking, IT asset information, vulnerability and compliance information. It aims to help asset owners query their systems, gain insight into their asset, accurately assess risk, and respond quickly to threats. Although it is not specific to power grids, the introduced concepts and principles are applicable to power grids. Standards and guidelines for asset, vulnerability and patch management specify how the entire process should be conducted. However, they do not provide direct support for the implementation or directly address problems occurring during the implementation.

Through our project, we have interacted with major power electronics vendors like Hitachi Energy, Siemens AG, and several grid operators in Germany. We found that, although the steps presented in Figure 1 seem straightforward, implementing them in real, complex infrastructures like a power grid faces many obstacles.

B. Technical Protocols

Popular technical protocols used for gathering asset information include SNMP, IEC 61850, OPC-UA, NETCONF and RESTCONF. **SNMP** [6] is a widely employed protocol for management and monitoring of devices within a network, and enables network administrators to manage their configurations and resolve network-related problems. In power grid domain, SNMP is often used in substation communication networks. SNMP consists of several key components including management information base (MIB), which serves as a database outlining the structure of data manageable through SNMP. MIB comprises objects that symbolize different parameters such as device uptime. It has a hierarchical structure, with each object being designated by an Object Identifier (OID).

IEC 61850 [7] is extensively used in substations and power grid to enable communication among diverse devices. It emphasizes on facilitating interoperability among devices from various manufacturers within a substation, and outlines the communication framework and data models necessary for the automation of power systems. **OPC UA** [8] is a platform-agnostic, secure communication standard developed for industrial automation and IoT applications. In the context of power grid, it is often adopted in power generation plants. It offers a more adaptable, extensible, and standardized information model, which enables the description of devices and systems through objects, variables, and their relationships.

NETCONF [9] is broadly used for managing the configurations of network devices. It offers a uniform approach for configuring, monitoring, and managing devices across a network, and facilitates the retrieval, modification, and monitoring of network device configurations in a standardized manner. NETCONF employs a data modeling language called YANG [10] to specify the configuration data. YANG defines exactly what data a network device can accept, how that data is structured, and what constraints it must follow. In a typical YANG model, data is organized in a logical, tree-like structure using elements like containers, lists, and leaf nodes. While a container groups related nodes together, a list includes entries uniquely identified by a key.

RESTCONF [11] uses REST principles and HTTP to manage network devices. It aims to offer a lightweight substitute to NETCONF for managing network configurations and obtaining data from devices. RESTCONF also employs

TABLE I: Comparison of Commercial Products for OT Asset, Vulnerability and Patch Management

Tool	Data Collection Mode	Protocol Coverage	Key Attributes Collected	CPE	CSAF
Microsoft Defender for IoT	Passive sensors with optional endpoint agents	40+ OT/IoT protocols (e.g., IEC 61850, SNMP, HTTP)	Manufacturer, firmware version, serial number	✓	✓
Tenable OT Security	Hybrid (passive & active read-only queries)	Modbus, OPC, DNP3, and IoT protocols	Firmware, user accounts, hotfix history, config states	✓	✓
Nozomi Guardian	Active scanning & passive network-based monitoring	200+ OT/IoT protocols (regularly updated)	Firmware, throughput, session analysis, process values	✓	✓
Siemens OT Companion	Cloud-hosted asset platform & IoT gateway with polling	Multi-vendor OT protocols via Siemens infrastructure	Firmware metadata, vendor -specific lifecycle info	✓	✓

YANG data models to define and organize configuration and operational data for network devices. RESTCONF is highly suitable for environments, in which automation, scalability, and ease of integration are key considerations. NETCONF and RESTCONF currently have a low adoption maturity in power grids, which however is expected to grow in the future due to aforementioned benefits. One of the adoption barriers is the lack of YANG model related to power grids. We address this problem by introducing a new YANG model in Section III.

Listing 1: CPE Naming Scheme

```
cpe:2.3:<part>:<vendor>:<product>:<version>:
        <update>:<edition>:<language>:<sw_edition>:
        <target_sw>:<target_hw>:<other>
```

C. Related Concepts

Asset Administration Shell (AAS) serves as a fundamental concept within the Industry 4.0 ecosystem [12]. It offers a standardized method for depicting physical assets in the digital realm; an AAS retains all essential data regarding the asset. Its applications in power grids include substation digital twins, grid equipment lifecycle management etc. AAS focuses on how to model a device with data. In asset, vulnerability and patch management, the focus of information gathering is on creating a data schema for the communication protocols or defining a communication interface that can be used to transmit primarily security-relevant data correctly and consistently. Our data schema (in Section III) should also be applicable to AAS, whose focus is on modeling a device with data, but not on how the data is transmitted to AAS.

Common Platform Enumeration (CPE) [2] is a systematic naming convention that offers a standardized method for identifying and categorizing hardware, software, and firmware platforms. It is extensively used in security systems to assist in identifying and managing vulnerabilities. CPE was developed to address the need for standardized names for IT products and platforms that are suitable for machine interpretation and processing. The CPE naming scheme is shown in Listing 1. Security tools and databases employ CPE identifiers to cross-reference known vulnerabilities with the products they affect.

While the CPE Product Dictionary maintained at NIST [2] serves as a single source of vulnerability information, another framework called **Common Security Advisory Framework** (CSAF) [3] adopts a decentralized approach to share and consume vulnerability information, reducing the risk of single point of failure. CSAF offers a unified structure for the formatting and distribution of security information across various industries, vendors, and organizations. It facilitates the upstream security intelligence community in sharing information regarding vulnerabilities. In the downstream context, CSAF empowers consumers of vulnerability information to consolidate security advisories from various providers [1].

D. Commercial Products

In recent years, some commercial products for asset, vulnerability and patch management have been developed. We compare some popular commercial solutions in Table I.

Microsoft Defender for IoT provides passive network monitoring through on-premise OT sensors with optional endpoint agents. It enables real-time asset discovery and vulnerability management across IoT and OT networks [13]. It has an extensive protocol coverage, and supports CPE-based vulnerability mapping and CSAF-style advisory ingestion. **Tenable OT Security** employs a hybrid approach—combining passive sensors with read-only, protocol-native active querying for safe inventory extraction [14]. It collects metadata including firmware versions and configuration parameters. It supports CPE-based matching as well as CSAF-style exportable reports. **Nozomi Guardian** is a passive OT and IoT monitoring platform that provides real-time asset inventory, vulnerability assessment [15]. It builds comprehensive asset profiles with attributes such as firmware version, operational data. **Electrification X - OT Companion by Siemens** is a cloud-based platform for scalable and secure OT asset management [16]. It enables real-time visibility across multi-vendor OT and IoT devices, focusing on firmware inventory, lifecycle metadata. CPE identifiers are used for vulnerability correlation, and the system facilitates CSAF-aligned advisory generation. These four commercial products all directly include power grids in their application domain.

III. Our Experiments

A. Design

With the number of devices and vulnerabilities in most organizations increasing, the traditional way of asset, vulnerability and patch management becomes infeasible. The process of collecting, analyzing, and organizing information from various sources needs to be streamlined and standardized. In our study, we aim to find out what hinders timely asset, vulnerability and patch management most, and come to the conclusion

This article has been accepted for publication in IEEE Transactions on Power Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2026.3725276

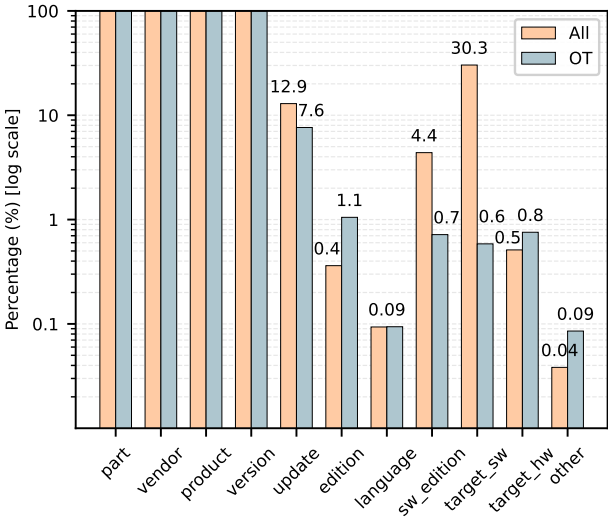

Fig. 2: CPE 2.3 attributes' adoption in practice.

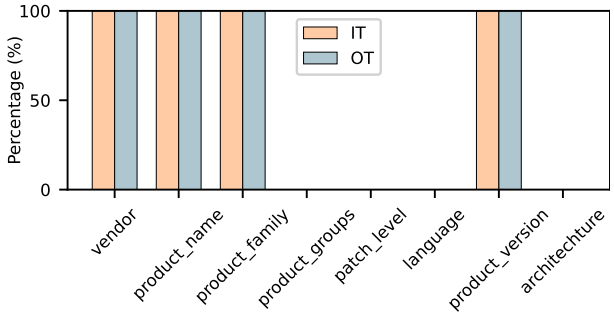

Fig. 3: CSAF attributes' adoption in practice.

that there are mainly three problems. First, data formats of asset, vulnerability and patch information are not standardized. Second, data sources of vulnerability and patch information are not clearly and exclusively defined. Third, the procedure for information exchange is not standardized. We analyzed the most important sources of vulnerability and patch information, i.e., CPE and CSAF, which both target the first two problems. We are interested in the question which attributes specified in CPE and CSAF are really adopted by product vendors.

Our analysis of all CPE entries in the CPE Product Dictionary [2] shows that each attribute was used at least a few times, both for IT and OT products (see Figure 2). It reveals that only the first four attributes were always assigned a value when a CPE entry was created, while the adoption of the rest of attributes lag far behind, to varying degrees. Further, our analysis of CSAF documents provided by the US CISA [17] shows that only a few of all attributes deemed as required by the CSAF Specification [3] are actually used in those CSAF advisories (see Figure 3). It reveals that half of the attributes were never considered when a CSAF advisory was created, both in IT and OT domain. However, the list of CSAF documents provided by CISA is only a small subset of all existing CSAF documents. Note that CSAF uses a decentralized approach to share and consume vulnerability and patch information. Hence we further collected and analyzed CSAF documents from other providers like the German BSI Security Agency, Siemens, Hitachi Energy etc.; our analysis delivers the same result: Currently, only four attributes specified in CSAF are really adopted by vendors.

In our study, we conducted a survey to investigate how well the asset, vulnerability & patch management cycle is organized and performed in industrial organizations. However, we end up having very low participation, not due to lack of interest, but due to security concerns and the absence of clear ownership in patching responsibilities. Through our own experiments in our test environment, which includes representative equipment — protection relays, controllers, switches — across multiple vendors and generations, we find that the step of asset discovery & inventory alone is difficult to automate. This is due to the fact that different products use different protocols for asset information gathering, with the most popular ones being SNMP, IEC 61850, and OPC UA.

Further, each vendor may have a different implementation of the same protocol. For instance, when using SNMP to query a certain piece of information, e.g., software revision, we may expect that it has a "standard" OID as defined in ENTITY-MIB [18]. However, devices from vendors like Siemens and Hitachi Energy employ a different OID. That is, retrieving a firmware version from a device via SNMP can be a manual exercise. In other words, we find that device information, firmware versions, patch availability etc. are in different shapes, formats, and have different naming conventions from vendors. It is therefore very difficult to realize automation and deployment at scale due to high complexity.

In order to develop a structured, vendor-independent process for information gathering across various devices from different vendors, we propose a new vendor-agnostic schema based on the data modeling language YANG. We present a list of attributes relevant for vulnerability & patch management in the Table II, which is a simplified version of the full table that we put in our Gitlab repository[1] due to its size. Note that the scope of this table and our paper is limited to vulnerability & patch management; we do not provide a complete information model supported by underlying protocols. This list of attributes result from discussions with participants from power electronics vendors and grid operators; they are primarily based on CSAF attributes and CPE attributes. Besides, we include attributes like `serial number` due to its importance in power system security, which we refer to IEC 62351. This attribute is important for individual asset identification and tracking, as it is often not possible to patch an entire fleet at the same time due to safety-critical operations in power grids.

We believe that these attributes form a complete asset fingerprint critical for automated vulnerability and patch management. Missing some of these critical attributes would create gaps. That is, for instance, edition-specific vulnerabilities may be missed without the `product edition` attribute. Runtime vulnerability and exploitation context cannot be assessed in the absence of the `software environment` attribute. Without the `product update` attribute, remediation cannot be verified. We map these attributes also to their counterparts in popular protocols like SNMP and IEC 61850. We chose these protocols, as they are either typically used for asset

[1] https://gitlab.kit.edu/kit/iai/rsa/ensure3b233

This article has been accepted for publication in IEEE Transactions on Power Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2026.3725276

TABLE II: Protocol Mapping.

Attributes	Prod. type	Manu.	Prod.	Prod. family	Prod. model	Serial num.	Prod. update	Prod. edi.	Lang.	Soft. rev.	Soft. env.	Hard. rev.	Hard. arch.
CSAF		vendor	prod. _name	prod. _family	prod. _groups		patch _level		lang.	prod. _ver.			arch.
CPE	part	vendor	prod.				update	edi.	lang.	ver.	target _sw		target _hw
ENTITY-MIB		∼1.12	∼1.13			∼1.11				∼1.10		∼1.8	
SNMP-Siemens S7 Automation		%1.0	%1.0							%1.0		%1.0	
SNMP-Hitachi Energy RTU										ß			
IEC 61850 (Objects)		LN. vendor	LP. model			LP. serNum				LN. swRev		LP. hwRev	
YANG (ietf-hardware)		IH/mfg -name	IH/model -name			IH/serial -num				IH/firm. -rev		IH/hard -rev	
YANG (our proposal)	CS/prod. -cat.	CS/ vendor	CS/prod. -name	CS/prod. -family	CS/prod. -group	CS/serial. -num.	CS/patch -level	CS/prod. -edi.	CS/ lang.	CS/prod. -ver.	CS/prod. -env.	CS/hard. -rev.	CS/ arch.

Note: arch. = architecture, cat. = category, CS = /ensure-cyber-asset:cyber-asset/network-elements/network-element, edi. = edition, env. = environment, firm. = firmware, hard. = hardware, IH = /ietf-hardware:hardware/component, lang. = language, LN = LLN0.NamPlt, LP = LLN0.PhyNam, LSN = LLN0/Sub1.NamPlt, LSP = LLN0/Sub1.PhyNam, manu. = manufacturer, num. = number, prod. = product, rev. = revision, soft. = software, ver. = version; ∼ = .1.3.6.1.2.1.47.1.1.1., % = 1.3.6.1.2.1.1., ß = 1.3.6.1.4.1.27527.10.3.2.1.2.1

discovery, e.g., SNMP, or popular protocols in power grids that can deliver some information needed for asset management, e.g., IEC 61850.

Table II demonstrates that existing protocols have fragmented attribute coverage; it is not possible to get a complete asset inventory from any single protocol alone. Further, as aforementioned, SNMP implementations vary by vendor: Siemens S7 covers 4 attributes; Hitachi RTU covers only 1. As a consequence, security advisories may not map precisely to affected assets, leading to false negatives (i.e., missing vulnerable systems). Organizations with mixed vendor environments cannot rely on vendor-specific protocols for unified asset management; they must either build complex integration layers to aggregate fragmented data, or adopt a new, comprehensive model. The cost of inaction is incomplete asset visibility, which directly impacts security posture, compliance, and operational resilience.

Listing 2: Cyber Asset YANG Module Snippet

```
module ensure-cyber-asset {
  namespace "urn:ensure:params:xml:ns:yang:
  ensure-cyber-asset";
  prefix ca;
  /* ... */
  grouping common-entity-attributes {
    leaf product-category {
      type identityref; {base product-category-type;}
      config false; mandatory true; }
    leaf vendor {
        type string; config false; mandatory true;}
    leaf product-name {
        type string; config false; mandatory true;}
    leaf product-version {
        type string { length "1..64";
         pattern '\d+(\.\d+)*([.-][a-zA-Z0-9]+)*';}
        config false; mandatory true; }
    leaf patch-level {
        type string; config false; mandatory true;}
    /* ... */
  }
  /* ... */
  container cyber-asset {
    uses common-entity-attributes;
    container components {
      list component {
        key "component-id";
        leaf component-id { type string;}
        uses common-entity-attributes;}
/* ... */
```

As neither the YANG module for network discovery [19] nor the YANG module for hardware [20] includes all attributes deemed as required by us, we create a new YANG module based on the previous two YANG modules, and present a snippet of our module in Listing 2. We put the whole module in our Gitlab repository due to its size. Table II shows that our YANG model provides a complete attribute mapping for asset identification. In Listing 2, an important subset of attributes mandatory to all entities defined in this module are presented. The `common-entity-attributes` grouping is this module's core part; it includes key asset metadata fields, enabling vulnerability matching. The type enforcement, mandatory constraint, incorporated patterns ensure data completeness and consistency. The `cyber-asset` container with hierarchical data structure shows asset/component organization.

This module provides a standardized, machine-readable schema for cyber asset inventory that enables automated vulnerability management. It aims to solve the fundamental problem that security teams cannot protect what they cannot accurately identify and track. Existing approaches typically suffer from the following limitations: 1) incomplete, fragmented asset data, 2) inconsistent formats across tools, 3) manual spreadsheet updates, 4) no component-level detail. Our proposed YANG module addresses these limitations by 1) using mandatory fields to ensure completeness, 2) merging critical asset attributes into a single canonical schema, 3) sup-

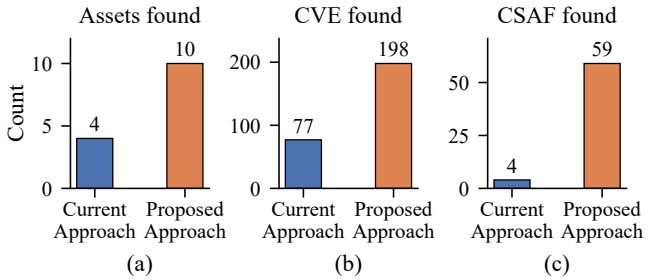

Fig. 4: Comparison of current [6] and proposed approaches.

porting automated NETCONF/RESTCONF API, 4) enabling full component tree tracking.

Further, this schema helps to satisfy the standards discussed in Section II-A. In particular, it complies with NIST SP 1800-5's asset management requirements by providing standardized attributes and type constraints to ensure data consistency, and enabling lifecycle tracking (via the attributes `acquisition-date`, `end-of-support-date`). It supports automated data collection via NETCONF/RESTCONF API to eliminate manual spreadsheet-based inventory. It also satisfies requirements introduced in IEC 62443-2-3 by incorporating OT-specific device types (via the attribute `iacs-device-type`), security zone levels (via the attribute `iacs-zone`) etc.

B. Validation

In our experiments, we have developed and implemented a test program that allows us to demonstrate how much the implementation of our information schema would help to complete the list of discoverable assets and associated vulnerabilities and security advisories in a network. Our test program first 1) performs a network scan in the local network for asset discovery, and outputs a list of assets found. Then, for each asset found, it takes the asset information obtained from the scan, 2) checks against the CVE database using the NVD CVE API, and outputs a list of CVE entries found. Further, it 3) checks against a list of well-known CSAF providers curated by the German Federal Office for Information Security, and outputs a list of CSAF advisories found.

We show the result obtained in our test environment in Figure 4. Our test environment consists of 13 devices inside an isolated OT network, including popular devices for grid automation, protection and control, e.g., Hitachi RTU530, Siemens SIPROTEC. Current approach refers to asset discovery via SNMP [6], while proposed approach assumes implementation of our YANG module. Note that we are not device vendors, and cannot directly implement it into the devices. Currently we can only resort to converting collectable information into a json file with the format defined in the YANG schema by ourselves, and assuming it is directly from the device. Figure 4 (a) shows that more than half of the devices in the network were not discovered through current approach; even for discovered assets, asset information can be incomplete. As a consequence, only a small portion of CVE entries and a fraction of CSAF entries can be discovered via current approach in comparison with our proposed approach, shown in Figure 4 (b) and (c).

IV. Conclusion

In this paper, we introduce and discuss a number of guidelines, concepts and products closely related to asset, vulnerability and patch management. In our study, we have built a test environment, and employed popular protocols for asset discovery. We found device information in different formats, and with different naming conventions based on vendors; it is very difficult to realize automation and deployment at scale due to high complexity. That is, retrieving critical information like firmware version from devices can be a laborious exercise. Hence we propose a new vendor-agnostic YANG schema for a structured information gathering across various devices from different vendors. We believe that it would provide a foundation to realize complete, accurate, queryable, real-time asset inventory, and fully automated CVE and CSAF matching.

References

[1] J. Lee. "How csaf 2.0 advances automated vulnerability management." Last accessed: March 2026. [Online]. Available: https://www.greenbone.net/en/blog/how-csaf-2-0-advances-automated-vulnerability-management/.

[2] NIST. "Official common platform enumeration (cpe) dictionary." Last accessed: March 2026. [Online]. Available: https://nvd.nist.gov/products/cpe.

[3] OASIS. "Common security advisory framework (csaf)." Last accessed: March 2026. [Online]. Available: https://www.csaf.io/.

[4] International Electrotechnical Commission, *Security for industrial automation and control systems – part 2-3: Patch management in the iacs environment*, 2015.

[5] National Institute of Standards and Technology, *It asset management*, 2018. [Online]. Available: http://doi.org/10.6028/NIST.SP.1800-5.

[6] J. D. Mark Fedor Martin Schoffstall and J. Case, *A simple network management protocol (snmp)*, 1990. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc1157.

[7] International Electrotechnical Commission, *Iec 61850*, 2004. [Online]. Available: https://iec61850.dvl.iec.ch/.

[8] OPC Foundation, *Opc unified architecture specification*, 2006. [Online]. Available: https://reference.opcfoundation.org/.

[9] A. B. Rob Enns Martin Bjoerklund and J. Schoenwaelder, *Network configuration protocol (netconf)*, 2011. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc6241.

[10] IETF. "YANG - a data modeling language for the network configuration protocol (NETCONF)." Last accessed: March 2026. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6020.

[11] M. B. Andy Bierman and K. Watsen, *Restconf protocol*, 2017. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc8040.

[12] Plattform Industrie 4.0, *Details of the asset administration shell, part 1*, 2022. [Online]. Available: https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/Details_of_the_Asset_Administration_Shell_Part1_V3.pdf?__blob=publicationFile&v=1.

[13] Microsoft, *Microsoft defender for IoT documentation*, https://learn.microsoft.com/en-us/azure/defender-for-iot/, Accessed: March 2026.

[14] Tenable, *Tenable OT security overview*, https://www.tenable.com/products/ot-security, Last accessed: March 2026.

[15] N. Networks, *Nozomi guardian product page*, https://www.nozominetworks.com/products/guardian, Last accessed: March 2026.

[16] Siemens, *OT Companion*, https://www.siemens.com/global/en/products/energy/medium-voltage/iot-applications-and-cybersecurity/ot-companion.html, Last accessed: March 2026.

[17] Cybersecurity and Infrastructure Security Agency. "CISA CSAF repository." Last accessed: March 2026. [Online]. Available: https://github.com/cisagov/CSAF.

[18] IETF. "ENTITY-MIB." Last accessed: March 2026. [Online]. Available: https://mibs.observium.org/mib/ENTITY-MIB/.

[19] IETF. "YANG tree, module: Ietf-network-inventory@2025-02-03." Last accessed: March 2026. [Online]. Available: https://www.yangcatalog.org/yang-search/yang_tree/ietf-network-inventory@2025-02-03.

[20] IETF. "YANG tree, module: Ietf-hardware@2018-03-13." Last accessed: March 2026. [Online]. Available: https://www.yangcatalog.org/yang-search/module_details/ietf-hardware.