An Open-Source Approach to OT Asset Management in Industrial Environments

Luca Pöhler[a], Marko Schuba[b], Tim Höner[c], Sacha Hack[d] and Georg Neugebauer[e]
Department of Electrical Engineering and Computer Science, FH Aachen University of Applied Sciences,
Eupener Str. 70, 52066 Aachen, Germany

Keywords: OT, ICS, OT Security, Risk Management, Asset Management, Asset Discovery, Asset Inventory.

Abstract: The need for compliance and the growing number of IT security threats force many companies to improve their level of IT security. At the same time, new legal regulations and the trend to interconnect IT with automation environments (operational technology, OT) lead to the situation that IT security and OT security need to be approached at the same time. However, OT differs from IT in several aspects and many well-established IT security procedures cannot simply be copied to OT networks. As in IT the first step to establish an acceptable security level for OT is to perform a proper risk assessment. Available tools that support OT asset management are either expensive or they do not provide the functionality needed. In the context of this paper a new open-source approach to OT asset management is presented. The tool that was developed to collect OT assets considers the specific characteristics of OT devices, the sensitivity of production environments, and the typically rudimentary starting situation of many real-world machine operators while being free of charge at the same time.

1 INTRODUCTION

The global cybersecurity threat situation continues to stay critical (Crowdstrike, 2023). Operational technology (OT) environments are becoming increasingly attractive to threat actors. The German Federal Office for Information Security 2022 annual report on the state of IT security in Germany shows that attacks affecting OT are becoming more common. Examples include the state-sponsored attack on the power grid in Ukraine, the collateral damage caused by an attack on a satellite service controlling German wind turbines, rendering 5,800 turbines inaccessible, or the cyberattack on German oil traders (BSI, 2022, p.49 f).

To mitigate the risks of industrial plants and increase their resilience, it is necessary to approach the topic of OT security in a structured manner. The basis of a functioning information security management system - also in OT - is always a systematic risk management. This in turn requires knowledge of all IT and OT assets. In the field, asset management is still suboptimal and has high potential for improvement in both IT and OT. Especially in the OT environment, the knowledge of own OT assets is often poor. If at all, OT assets are inventoried in Excel files, a tedious, unreliable and expensive method of asset management.

The purpose of this paper is to present an open-source tool that can significantly improve asset management for OT in many organizations. The goal is to create an extensible, free and open-source tool that considers OT-specific characteristics and delivers similarly good results as commercial tools.

2 BACKGROUND

2.1 Operational Technology

Operational technology includes programmable systems and devices that interact with the physical environment. OT devices can detect changes in this environment or can trigger changes to it (NIST, 2023).

[a] https://orcid.org/0009-0007-5648-0559
[b] https://orcid.org/0000-0002-3302-3060
[c] https://orcid.org/0009-0006-0224-6292
[d] https://orcid.org/0000-0001-6624-0486
[e] https://orcid.org/0009-0008-0927-2324

Pöhler, L., Schuba, M., Höner, T., Hack, S. and Neugebauer, G.
An Open-Source Approach to OT Asset Management in Industrial Environments.
DOI: 10.5220/0012362200003648
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024)*, pages 128-136
ISBN: 978-989-758-683-5; ISSN: 2184-4356

Besides the application area of industrial plants - here OT systems are often referred to as Industrial Control Systems (ICS) - OT is also used in other areas, e.g., building automation or in vehicles. Even though the focus of this paper is on industrial plants, the term OT will continue to be used instead of ICS because the results can in principle be extended to other OT application areas.

2.2 OT Systems and Devices

OT systems and devices are often based on proprietary hardware and software and come from a multitude of manufacturers, including sensors and actuators, programmable logic controllers (PLC), supervisory control and data acquisition systems (SCADA), manufacturing execution systems (MES), or enterprise resource planning (ERP) systems (IEC 62441-1, 2013; Sauer et al., 2019).

Other typical devices in the OT area are Human Machine Interfaces (HMI) and Engineering Workstations (EWS).

2.2.1 OT and Related Protocols

In contrast to the private or office IT area, where TCP/IP is mostly used via Ethernet or WLAN, there are many different protocols in the OT area. Two prominent examples are Modbus and Profinet.

The Modbus serial protocol is now an open and very widely used protocol (Schneider Electric, 2022). Modbus is available in several variants, one of which is Modbus TCP (Transmission Control Protocol), that can transmit Modbus data units over the standard Internet protocols TCP and IP (Internet Protocol).

The Process Field Network (Profinet) protocol is the successor to the older Profibus protocol and is based on Ethernet TCP/IP (PI, 2023). Industrial Ethernet, as implemented by Profinet, has become the standard technology for automation systems and will replace the fieldbus implementations over time.

Due to the increasing implementation of OT protocols via TCP/IP, underlying protocols of classic IT are also becoming relevant, in particular Ethernet and the Address Resolution Protocol (ARP) (RFC 826, 1982).

2.3 OT Asset Management

In principle, it is essential in today's world to know which components are in use. Sensible risk management, for example, is only possible if you know exactly which systems you have and which software they use (Kassa, 2017), i.e. the security of IT or OT correlates with the knowledge of the assets.

2.3.1 Asset Management Process

Asset management is a continuous process that is more than just inventory. The process starts with the identification of the asset and the inclusion of this asset in the data management. To do this, the organization must first determine which systems are relevant. Once the asset is included, its information must be permanently maintained, checked and possibly updated. This means the information must be kept up to date, and possible changes, for example new threats, must be reacted to. Here, various processes come into play that, depending on the definition, belong to asset management or work closely together with it.

A well-known model for the life cycle of IT assets is the so-called IMAC model. In full, this is also referred to as IMAC/R/D (Bluhm, 2020). IMAC stands for Install, Move, Add and Change, with Remove and Dispose being added in the complete model, describing phases, or processes, that an asset usually passes throughout its life cycle.

In addition, there are processes that are either part of the asset management system, or at least closely linked to it.

Patch management is responsible for checking the version status of all installed software and identifying possible updates.

Closely related to patch management is vulnerability management. This monitors system vulnerabilities and categorizes them based on their impact and the likelihood that they will occur. If a vulnerability has a major impact on an organization and is also very likely to occur, it should be considered critical and should be dealt with as quickly as possible.

2.3.2 Reasons for OT Asset Management

The reason for the now fundamental importance of OT asset management is partly due to the fact that OT security has found its way into legislation.

In Germany, for example, there are requirements for OT asset management that can be derived directly from the IT-Sicherheitsgesetz 2.0 (IT Security Act 2.0; BSI, 2020) or the Maschinenverordnung (Machinery Ordinance; BMJ, 2021). At the European level, similar requirements follow from the Cyber Resilience Act (EU, 2023). In the USA, there are NIST recommendations on the same topic (NIST, 2023).

In general, asset management in OT must consider the specific characteristics of OT (cf. NIST, 2023).

While automated asset management tools are obviously efficient and avoid human error, organizations should consider how the tool collects information and whether the collection method (e.g., active scanning) may have a negative impact on their OT systems. If problems are expected here, NIST recommends that the organization consider manual processes to maintain current inventory.

3 STATE OF THE ART

The topic of OT asset management is a very practical one, which is why the state of the art includes work from the field of applied research as well as commercial solutions. The latter usually require licenses that need to be bought. In a few cases, free but limited demo version are available, however, those are not very useful in real use cases. In addition, not all information for the commercial tools is publicly available, so the accessible statements of the manufacturers must be relied upon.

3.1 Research on OT Asset Management

OT asset management is not a new topic. As early as 2005, ABB Switzerland Ltd. dealt with the "IT Asset Management of Industrial Automation" (Gelle, 2005). However, this was not a general solution to the problem, but a proprietary solution for ABB's own automation system 800xA. Similar solutions can be found from many manufacturers in the industrial sector. However, since very few integrators or operators of plants exclusively use a (single) product (variant) of a single manufacturer, these solutions are often not useable.

Other works like "A literature survey on asset management in electrical power [transmission and distribution] system" (Khuntia, 2016) or "Development of a concept for OT asset management in the production environment" (Koch, 2021) deal with the theoretical basics of asset management in OT. These are by no means to be neglected, but in practice they do not provide the necessary opportunity for a company to set up an asset management system.

Many projects such as "OT-asset CMDB Solutions" (Koskelo, 2020) look for the best solution for a specific purpose at an enterprise. This is certainly a good approach for the organization concerned, but not a transferable solution. As a result of the project, an asset management software is selected that is not free of charge.

3.2 Existing OT Asset Management Tools

Many existing solutions for OT asset management charge licensing fees. Some of these tools claim to have been developed specifically for OT. In the following sections, we will briefly introduce some of the tools. Interestingly, the promised functions are mostly the same.

The company Langner Communications GmbH from Norderstedt, Germany offers an asset management system especially for OT. It is neither freeware, nor an open-source solution. Langner promises that their tool OT-BASE "makes automation engineers, cybersecurity experts and maintenance staff more efficient" (Langner, 2023).

Verve Industrial Protection of Chicago, USA claims its Verve product provides the deepest, broadest and most efficient asset inventory management solution for OT (Verve, 2023). In doing so, Verve promises a particular depth of information retrieval about assets.

Industrial Defender from Foxborough, USA offers another software for asset and risk management (Industrial Defender, 2023).

Other fee-based asset management systems developed specifically for OT are:

- Asset Guardian (Asset Guardian, 2023)
- Claroty (Claroty, 2023)
- Dragos (Dragos, 2023)
- Microsoft Defender for IoT (Microsoft, 2023)
- Nozomi (Nozomi Networks, 2023)
- PAS Cyber Integrity (PAS, 2023)

Another asset management system is Snipe-IT (Grokability, 2023). Although it does not advertise that it is OT-compatible, it is open-source and at least the basic version is available free of charge. The tool does not offer asset recognition but would theoretically be extensible since it is open-source. It is very complex and offers many options that go more in the direction of commercial management. In the context of the project, it was therefore decided against Snipe-IT.

4 REQUIREMENTS FOR AN OPEN-SOURCE OT ASSET MANAGEMENT TOOL

As already mentioned, the development of the tool focused on practical applicability. Therefore, a case study was first conducted at a real company before the actual requirements analysis was implemented.

4.1 Case Study

To assess the current state of OT asset management in the industry, an interview was conducted with a German business. The company, which is anonymized here, has a history of more than a hundred years, tenths of thousands of employees, its headquarters in Germany and hundreds of locations worldwide. The enterprise manufactures equipment itself in the role of an integrator and is in turn an operator of equipment.

Due to the size of the enterprise, the asset management is organized in a distributed manner. Various systems and tools are used for this.

For manufacturing, i.e. OT, the company currently has no system for asset management. Machines, PLCs or sensors are managed using Excel lists or PDF files. There are also no strict protocols or processes to ensure that the data is up-to-date and complete. The responsibility to maintain the lists is entirely up to the employees. The industrial facilities are highly segmented and separated from the environment by an air gap. This separation is relied upon to minimize the risk of a successful attack on the OT.

However, the topic of asset management is becoming increasingly important for the company. It was affected by the Log4shell vulnerability in the Java library Log4j (IBM, 2021) and had to manually query which departments were affected. Currently, several OT asset management tools are being evaluated, but no tool had yet been found that could fully meet the requirements. The main complaint is the inadequate detection of assets. Even tools that promise automatic detection of the devices would only recognize about 50-60%. Often IT asset management systems would also sell themselves as OT-compatible, but due to lack of experience would encounter problems mainly with network segmentation. Another quality feature would be the ability to import existing Excel lists into the new system.

4.2 Requirements and Goals

Due to the poor experience of the case study company with commercial OT asset management solutions and because no suitable open-source software was available, it was decided to develop a new asset management software. The goal was not to compete in scope and performance with paid software such as OT-Base (see 3.2). Rather it should be shown that it is possible to build a good free tool within a short development time, which offers especially smaller companies the chance to improve their OT asset management. But also, for larger companies, like the one described in the case study, the development of an own OT asset management system can be an attractive option, because off-the-shelf solutions often need adaptations to the specific requirements.

Before implementation, a complete set of requirements was specified in collaboration with the case study enterprise and a company from the OT security sector. Through extensive interviews, requirements for the software could be derived in detail. The following figure 1 shows the conceptual structure of the application, which is explained in more detail in the following sections.

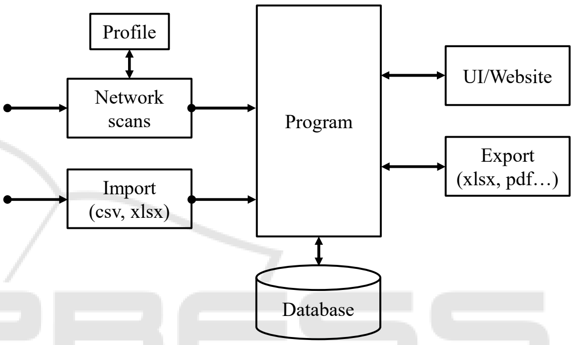

Figure 1: Conceptual structure of the application.

The specified requirements are only roughly outlined within the scope of this paper:

- Costs and licensing: the program to be created should be free of charge and available as open-source software.
- Use of inventory data: since the company already has data in the form of Excel files, it should be possible to continue using these. For this purpose, an Excel or CSV import is to be implemented. An export to standard formats such as Excel or pdf should be possible as well.
- Database connection: the asset information should be persistently stored in a database.
- Asset availability: this is one of the most critical requirements. The processes or operations of the industrial plant must not be disturbed or interrupted by the tool. Since an active network scan always carries the risk of triggering disturbances, the execution of the asset detection requires a certain sensitivity as well as knowledge about the plant on the part of the executing employee. The operator should therefore be able to select from various intensity levels (profiles) for the detection.

- Usability: the tool should be easy to use and require little training.
- Extensibility: the tool should be easy to extend or adapt to new requirements and conditions.
- No need for expensive hardware scanners: the tool should also be able to work across the segmentation boundaries of the networks without having to install additional hardware.

5 IMPLEMENTATION OF THE OPEN-SOURCE OT ASSET MANAGEMENT TOOLS

The software was implemented as a web app. The asset discovery function was implemented via a Python "network discovery" script that uses the Netdiscover (Kali, 2023a), Nmap (Nmap.org, 2023a), and Crackmapexec (Kali, 2023b) scanning programs for different intensity profiles. This Python script can also be run without the web app and returns a CSV file that can then be read into the webapp or could potentially be further processed in other programs. By developing additional Python modules, the recognition of the program can thus be extended as desired.

5.1 Web App

The website provides the user interface for asset management. It currently consists of the following components: dashboard, table view and detail view. There is also a login and an admin portal, but these are not described further.

The dashboard provides an overview of the existing assets and the possibility to edit or delete them. In addition, the user can import or export data, or start a scan.

The table view provides an overview and management of the assets. All existing assets are displayed in a table. By means of a plug-in, functionalities are added to the table on client side. Automatically imported assets are colored differently from those added via CSV/Excel import. This allows for manual checks to confirm the correctness of the data. After verification the coloring can be removed.

For each object in the database (device, software, product, supplier) there is an editable detail view on all information about the objects.

5.2 Network Discovery Module

The module currently includes two functions that are used for asset detection via network: General Network Scan and Siemens S7 Scan. The module can be executed individually and can therefore be used independently of the web application. For example, one could just run the network discovery Python script on a mini computer in different network segments, and then add the resulting data to the asset management via CSV import.

5.2.1 General Network Scan

This function implements the main functionality of this module. It is divided into five different levels (profiles) that perform different scans. These levels are used to fulfill the requirement that the processes of the industrial plant must not be influenced. The user must assess for himself which level is appropriate for the device to be scanned. In addition to the IP range and the level, the user can also select a timeout, after which a scan should stop.

Level 0 - Very Cautious: This level is based on a passive ARP scan. If a network node searches for the MAC address of another node, it sends an ARP request via broadcast to the entire network. This request contains the IP and MAC address of the node as well as the IP address of the node being searched for. Since the message is sent to everyone, it is possible to receive it, for example with the command line program Netdiscover (Kali, 2023a), and thus obtain the information mentioned. Consequently, Netdiscover has now found a MAC address for each specified IP address, if available. This MAC address can be evaluated automatically. For this purpose, both Netdiscover and Nmap use tables which contain a mapping of the first part of the address to the respective manufacturer of the device. This type of scan is the safest of the methods implemented here, since it does neither generate nor affect any network data. It can therefore be used in fragile and highly available production environments. The disadvantage is that one must rely on ARP requests from the nodes and these also contain only little information. If a system does not send a request, it will not be detected. Note also, that the scan duration needs to be specified as the test has no natural end.

Level 1 – Cautious: To solve the problem of not being able to detect inactive devices, there is an option to perform an active ARP scan. This is the default setting of Netdiscover. The ARP scan automatically terminates as soon as it has queried all IP addresses in the specified range. Unlike level 0, Netdiscover now actively sends ARP requests to the specified IP address ranges. This guarantees that all nodes supporting ARP are discovered, but also brings risks. New frames are generated which could theoretically lead to failures. In reality, however, the active ARP scan is still mostly safe to use, since ARP as such works on the data link layer and therefore has little influence on applications located in higher layers. In addition, ARP request frames are comparatively small.

To ensure that no systems are overlooked, the active ARP scan is used as the basis in each of the following stages.

Level 2 – Medium: To find out more about the software and firmware used on the OT devices, an Nmap scan, more precisely a TCP SYN scan, is performed in level 2 in addition to the ARP scans. The scan is based on the SYN, ACK and RST protocol flags of the TCP handshake that is performed to establish a TCP connection. The server responds to a client's SYN request to a specific TCP port with the SYN and ACK flags being set if the port is open, and with the RST flag set if the port is closed. To the SYN/ACK response from the server, the client would normally respond with an ACK, and then begin TCP communication. However, Nmap sends an RST in response, so no connection is established. This means that this scan is relatively unobtrusive and harmless and can be performed quickly. It is also less likely to be blocked by firewalls compared to other scanning methods. However, if too many connection attempts are made in too short a time, the TCP SYN scan may be detected by a firewall or intrusion detection system, but this can be circumvented by configurable delays between scan packets. The result of the TCP SYN scan is a list of running hosts, and the ports open on them. Since standard ports are often used for certain services, Nmap offers a suggestion for a found service based on a database of open ports, but this suggestion may not always be correct. It should be noted that when implementing level 2, only the 100 most frequently used ports are scanned to keep the load low.

Level 3 – OS: To obtain even more information about the running services and the operating system of the devices, level 3 extends the TCP SYN scan to the 100 most frequent ports with the service and version detection (command option -sV) and the operating system detection of Nmap (option -O) being activated. Nmap sends packets to the services behind the ports found to draw conclusions about the type and version of the service based on the response. At this point at the latest, the availability of an industrial system is at risk, since direct addressing of ports can lead to jerks, dropouts or even the crash of the devices. Especially with older devices, port scans can trigger uncontrolled behavior, for example if the machine simply processes all incoming data without checking. Operating system detection works similarly and requires at least one open port to work and multiple open ports for a more accurate result. Testing in the experimental environment found that operating system detection worked poorly to not at all on Windows systems. Therefore, an additional Crackmapexec scan was implemented specifically for Windows systems. This scan is used by penetration testers to exploit Windows systems but is used in this context for the detection of Windows operating systems only (Kali, 2023b).

Level 4 - Full Port Scan: Since level 3 is not able to detect all services on a system (only the 100 most common ports are scanned), level 4 extends the scan to all 65,535 ports. Both OS and version detection are enabled via options, as well as time-wise aggressive scanning.

5.2.2 Siemens S7 Scan

The second function is based on the s7-info.nse script developed for Nmap (Nmap.org, 2023b). This script collects information about Siemens S7 controllers via a specified port. Siemens uses port 102 by default, so this is also used in the script. The function is intended to scan individual systems that are suspected to contain a PLC and should not be applied carelessly to the entire production environment. Therefore, a best practice should be to first identify potential S7 systems, e.g., by using a level 1 or 2 general network scan. After that the Siemens S7 scan can be used to collect detailed information on devices suspected to come from Siemens.

6 TEST OF THE OPEN-SOURCE OT ASSET MANAGEMENT TOOL

The OT asset management tool was tested at the case study enterprise as part of a proof of concept (PoC). It was compared directly with a solution from well-known manufacturers in industrial IT, which at the point of test was still under development. The purpose of testing the PoC was to find out whether - from enterprise perspective - a solution developed in-house based on open-source software could be an alternative to a paid asset management system.

6.1 Test Setup

A test environment consisting of various industrial devices was set up, including the following devices:

- Windows XP laptop
- Dell server
- Siemens SIMATIC S7-400 with a SIMATIC NET CP Industrial Ethernet Module
- Siemens SIMATIC S7-mEC
- Siemens SIMATIC S7-1500
- Siemens SIMATIC ET200SP
- Siemens SIMATIC HMI Touch
- WAGO 750-8206
- WAGO 750-375
- Commercial tool HW
- Own tool on mini PC
- Managed switch

The majority of devices can be seen in figure 2.

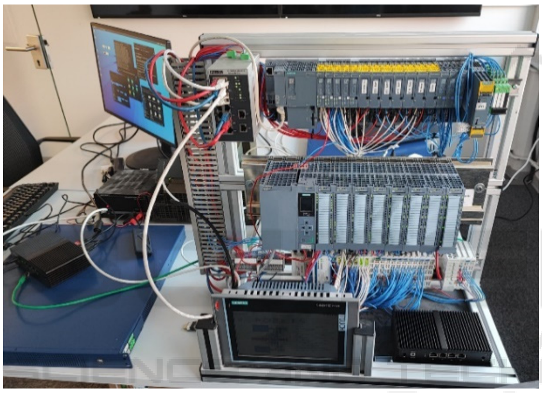

Figure 2: Subset of PoC setup at case study user site.

6.2 Test Execution and Results

6.2.1 ARP Scan

The test was started with the passive ARP scan (level 0). This worked in the test environment, but only delivered a few assets in the short test time (30 seconds), as expected.

The active ARP scan (level 1), on the other hand, was able to provide a complete overview of the devices that could be reached in the network. The mapping table provided information about the manufacturers of the devices. According to the company's contact persons, the ARP scan alone is helpful, as it provides information about which devices are available and which may still be missing from the data storage.

6.2.2 S7 Scan

The ARP scan and address mapping identified some of the systems as Siemens devices. Therefore, the tests continued with S7 scans for the respective devices.

The first scans were performed on the two older Siemens controllers (S7-400, S7-mEC). The SIMATIC S7-mEC had the port 102 closed. This port is normally open on all Siemens controllers and cannot be closed by the user. The S7-info.nse script could not find out any further information for this embedded device. On the S7-400 port 102 was open, but the S7 scan could not get any information about the PLC either. After consulting with the company's colleagues, this was most likely due to the fact that this PLC uses a non-native extension module for Ethernet, which leads to slight changes in communication compared to a normal Siemens PLC with an integrated Ethernet port. Adjustments to the s7-info.nse script might overcome this limitation, but this effort was not made, as both devices are more than 20 years old, and the company only has a small number of them left, which allows manual management, particularly, as those devices hardly receive any updates. Only the IP address, the MAC address and thus the manufacturer, as well as the open ports could be found out for the two tested devices. The comparison tool from the well-known manufacturer also could not find out anything else than the MAC and IP addresses for these two devices. Additionally, it provided the state of the devices (online or offline).

The two newer Siemens PLCs could be scanned successfully by means of the S7 scan as well as by the alternative tool. This provided information about the type of device, including serial number and firmware version. Via the serial numbers, all data about the hardware in use could also be obtained online.

7 CONCLUSIONS

The goal of the project was to improve OT security in industrial environments through simplified OT asset management. For this purpose, a case study with a real enterprise was performed, which led to a set of OT asset management requirements. As the search for suitable, free and open-source solution was unsuccessful, it was decided to implement a new asset management software due to dissatisfaction with existing commercial solutions. The tool was implemented as a proof of concept and then tested in a test environment of the company.

The test results were promising, also in comparison with a tool from a device manufacturer. All in all, the new tool could provide small companies with a cost-effective OT asset management solution. Also, large companies could benefit from the flexibility and extensibility of the solution.

REFERENCES

Asset Guardian (2023). *We protect the integrity of Industrial Automation and Control Systems software*, [Online], Available: https://www.assetguardian.com/, [24 Oct 2023].

Bluhm, P. (2020). IMAC/R/D – IT-Lifecycle-Management, [Online], Available: https://www.i-doit.com/en/blog/imac-r-d-it-lifecycle-management/, [24 Oct 2023].

BMJ (2021). *Neunte Verordnung zum Produktsicherheitsgesetz (Maschinenverordnung) (9. ProdSV) (Ninth Ordinance to the Product Safety Act (Machinery Ordinance)),* [Online], Available: https://www.gesetze-im-internet.de/gsgv_9/BJNR070410993.html, [24 Oct 2023].

BSI (2022). *Die Lage der IT-Sicherheit in Deutschland 2022 (The state of IT security in Germany 2022),* [Online], Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6 [24 Oct 2023].

BSI (2020). Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen (Specification of the requirements for the measures to be implemented in accordance with Section 8a (1) BSIG), [Online], Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Konkretisierung_Anforderungen_Massnahmen_KRITIS.pdf?__blob=publicationFile&v=3 /, [24 Oct 2023].

Claroty (2023). *Asset Management for Industrial Environments*, [Online], Available: https://claroty.com/industrial-cybersecurity/asset-management, [24 Oct 2023].

Crowdstrike (2023). *2023 Global Threat Report*, [Online], Available: https://www.crowdstrike.com/global-threat-report/ [24 Oct 2023].

Dragos (2023). *Visualize, Detect, & Respond to ICS/OT Cybersecurity Threats*, [Online], Available: https://www.dragos.com/platform/, [24 Oct 2023].

EU (2023). *EU Cyber Resilience Act,* [Online], Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act, [24 Oct 2023].

Gelle, E., Koch, T.E., Sager, P. (2005). *IT asset management of industrial automation systems*, in: 12th IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS'05).

Grokability (2023). *Snipe-IT Open Source IT Asset Management.* [Online], Available: https://snipeitapp.com/, [24 Oct 2023].

IBM (2021). What is Log4Shell?, [Online], Available: https://www.ibm.com/topics/log4shell, [24 Oct 2023].

IEC 62264-1:2013 (2013). *Enterprise-control system integration - Part 1: Models and terminology,* International Organization for Standardization (ISO).

Industrial Defender 82023). *OT Asset Management for Critical Infrastructure,* [Online], Available: https://www.industrialdefender.com/solutions/ot-asset-management, [24 Oct 2023].

Kali (2023a). *Netdiscover*, [Online], Available: https://www.kali.org/tools/netdiscover/, [24 Oct 2023].

Kali (2023b) Crackmapexec, [Online], Available: https://www.kali.org/tools/crackmapexec/, [24 Oct 2023].

Kassa, S.G. (2017*). IT Asset Valuation, Risk Assessment and Control Implementation Model,* [Online], Available: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/it-asset-valuation-risk-assessment-and-control-implementation-model/, [24 Oct 2023].

Khuntia, S.R., Rueda, J.L., Bouwman, S., Meijden, M. (2016). *A literature survey on asset management in electrical power [transmission and distribution] system*, in: International Transactions on Electrical Energy Systems 26(10).

Koch C.E. (2021). *Entwicklung eines Konzepts für das OT-Asset Management im Produktionsumfeld (Development of a concept for OT asset management in the production environment),* Bachelor Thesis at Duale Hochschule Baden-Württemberg Heidenheim, Germany.

Koskelo, M. (2021). OT-asset CMDB Solutions, Bachelor Thesis at Metropolia University of Applied Sciences, Metropolia, Finland.

Langner (2023). *OTbase - If you don't have OTbase, you don't have an OT asset inventory*, [Online], Available: https://www.langner.com/, [24 Oct 2023].

Microsoft (2023). *Microsoft Defender for IoT*, [Online], Available: https://www.microsoft.com/en-us/security/business/endpoint-security/microsoft-defender-iot, [24 Oct 2023].

NIST (2023), *Special Publication 800-82 Revision 3, Guide to Operational Technology (OT) Security,* [Online], Available: https://csrc.nist.gov/pubs/sp/800/82/r3/final, [24 Oct 2023].

Nmap.org (2023a). Nmap, [Online], Available: https://nmap.org/, [24 Oct 2023].

Nmap.org (2023b). s7-info NSE script - Nmap Scripting Engine documentation, [Online], Available: https://nmap.org/nsedoc/scripts/s7-info.html, [24 Oct 2023].

Nozomi Networks (2023). *Automate Your OT Asset Inventory Management*, [Online], Available: https://www.nozominetworks.com/solutions/iot-ot-asset-inventory-management, [24 Oct 2023].

PAS (2023). *OT Inventory & Configuration Management*, [Online], Available: https://pas.com/products-and-services/solutions/ot-inventory-configuration-management, [24 Oct 2023].

PI (2023). *PROFINET - the leading Industrial Ethernet Standard,* [Online], Available: https://www.profibus.com/technology/profinet/, [24 Oct 2023].

RFC 826 (1982). *An Ethernet Address Resolution Protocol*.

Sauer, F., Niedermaier, M., Kießling, S., Merli, D. (2019). *LICSTER - A Low-cost ICS Security Testbed for Education and Research*, 6th International Symposium for ICS & SCADA Cyber Security Research 2019 (ICS-CSR 2019).

Schneider Electric (2022). *What is Modbus and How does it work?,* [Online], Available: https://www.se.com/us/en/faqs/FA168406/, [24 Oct 2023].

Verve (2023). *Verve for OT/ICS Asset Inventory*, [Online], Available: https://verveindustrial.com/verve-security center/asset-inventory/, [24 Oct 2023].