OPEN INDUSTRY 4.0 ALLIANCE

White Paper

Vulnerability Management for Software-Driven Machinery

IMPRINT

Publisher

Open Industry 4.0 Alliance

Christoph Merian-Ring 12, 4153 Reinach, Switzerland

https://openindustry4.com

info@openindustry4.com

Status

File: Vulnerability Management for Software-Driven Machinery

October 9th, 2024 – Version 1.0

Editors

Lucas Wolf (Open Industry 4.0 Alliance)

Authors

Martin Flöer (Weidmueller)

Sebastian Fischer (conplement AG)

Vitaliy Volevach (Siemens)

Dr. Florian Probst (Software AG)

Lucas Wolf (Open Industry 4.0 Alliance)

Abstract

This white paper outlines the mitigation of vulnerability risks for software-driven industrial machinery. To address this, the concept of Software Bill of Materials (SBoM), an approach to automatically identify vulnerabilities in individual industrial assets, is presented.

The underlying hypothesis is that security on the shopfloor does not emerge from striving for fully disconnected and isolated systems (Stuxnet as an extreme example). Instead, it's about using IoT connectivity and interoperability to quickly and flexibly respond to new vulnerability threats.

Primarily, we want to focus on manufacturers of software-driven machinery and second, the operators of the machinery on the shopfloor since both groups have considerable pressure to get vulnerability threats under control.

In the current landscape, there is no standardized method for automated security tracking of software and hardware in IT and OT environments. As a result, both groups need to develop proactive strategies to mitigate these risks. By leveraging SBoM as a standardized submodel for digital twins, manufacturers and operators can achieve a more systematic and automated approach to vulnerability management. In this regard, the white paper outlines the advantages of SBoM in collaborative value chains and presents key insights and analyses on the current state and future trends in managing software vulnerabilities in industrial settings.

Context

Emerging vulnerability threat: The number of software-driven assets across all industries is constantly increasing. The generic rational behind this is that optimization potential moves from optimizing the hardware as such to software and data-driven process optimization. To support this trend, manufacturers of industrial equipment and machinery improve their products with software. What drives innovation on one side, opens vulnerability threats on the other. Today, the software operated on industrial machinery often reaches a hard to handle complexity. The ability to ensure that all used software components are safe to use lags behind. To address this issue, regulatory bodies are introducing rules addressing the security demand e.g. “Cyber Resilience” from the European Commission or mandatory Software Bill of Material regulations from German BSI. Those regulations will become mandatory in the next years.

Now, what is the SBoM? The Software Bill of Materials is a detailed inventory that lists all the non-physical components, such as firmware, software, open-source libraries, programming language packages, third-party tools and similar. The SBoM is also provided with a standardized submodel for a digital twin. According to the IDTA (Industrial Digital Twin Association e.V.) it is defined the following:

“The submodel „Software Bills of Material“ represents a formal, machine-readable inventory of software components and their dependencies, as well as information about these components and their hierarchical relationships. The mandatory features of the submodel enable unambiguous identification of the individual software components. Optional features are defined to support extended use cases. The current standardized formats for interoperable exchange of the Software Bill of Material are taken into account in the development of the submodel. The submodel is based on the results of the IDTA submodel „Hierarchical Structures enabling Bills of Material“. The submodel offers numerous advantages for the use cases in the collaborative value chains, e.g. in software development, supply chain management, vulnerability management, asset management, procurement, etc.”.

[source: https://industrialdigitaltwin.org/content-hub/teilmodelle]

The mandatory introduction of SBoMs presents challenges for SMEs due to limited resources and expertise. However, SBoMs enhance transparency and security by offering manufacturers clear visibility into software components, aiding in vulnerability management, and providing end users with the necessary information to assess and protect against security risks.

The Intersection of IT and OT: Bridging the Gap

As the industrial sector embraces digital transformation, the convergence of Information Technology (IT) and Operational Technology (OT) has become an essential aspect of efficient vulnerability management. Traditionally, IT and OT have operated in silos, with IT focusing on data management, software applications, and network security, while OT has dealt with the control and monitoring of physical processes on the shop floor. However, this separation is increasingly unsustainable as software-driven machinery grows more complex, and the need for secure, seamless integration between these domains becomes paramount.

IT environments are typically characterized by established protocols, robust cybersecurity frameworks, and regular patching cycles. In contrast, OT environments are less standardized and have been designed for reliability and continuity, often with systems that have lifespans of 10-20 years or more. These legacy systems may run outdated software, making them vulnerable to security threats, especially when connected to more modern, internet-facing IT networks.

The differences in priorities also pose challenges. While IT prioritizes data integrity and confidentiality, OT emphasizes system availability and safety. For example, shutting down a factory's OT system to apply a security update could halt production and incur significant financial losses. This disparity makes it difficult to implement standardized vulnerability management practices across both IT and OT.

The increasing connectivity of industrial equipment, driven by the Industrial Internet of Things (IIoT) and Industry 4.0 initiatives, necessitates the integration of IT and OT systems. This convergence allows manufacturers and operators to benefit from enhanced data analytics, predictive maintenance, and improved decision-making. However, it also expands the attack surface, exposing OT environments to cyber threats that have traditionally targeted IT systems.

Achieving secure convergence requires the adoption of interoperable technologies and protocols that can facilitate seamless data exchange between IT and OT devices. This is where standardized models, such as the Asset Administration Shell (AAS) and the Software Bill of Materials (SBoM), play a crucial role. By providing a common language for representing software and hardware components, these models enable centralized monitoring, vulnerability tracking, and proactive response across both domains.

Current Challenges in OT Device Management

Today, inventory management of installed devices and software versions is predominantly handled using Microsoft Excel. OT administrators typically discover devices manually and log them in spreadsheets. In some cases, the data is transferred to a Microsoft Access database with custom views and reports before being integrated into SAP systems.

The task of managing and resolving issues with OT devices relies on a mix of proprietary tools, which vary based on device type (such as PLCs or network infrastructure devices). These solutions, provided by automation equipment vendors, are often Windows desktop applications designed to handle equipment health, device state management, and firmware updates, but they operate independently. Examples include the “Totally Integrated Automation Portal” (Siemens) and “IndraWorks” (Bosch Rexroth). Due to the lack of open interfaces, these tools typically do not connect to broader management systems like ERP or IT asset management. Moreover, they are often restricted to specific notebook computers and operating system versions, limiting their flexibility.

This fragmented approach introduces complications with managing different passwords, credentials, usability issues, and the need for training on multiple tools, which burdens service crews.

Most industrial equipment today, such as drive systems, lack secure remote connectivity. As a result, personnel must travel on-site, armed with the appropriate software tools on their laptops, to perform updates or configurations. Establishing a direct connection to each device is both time-consuming and inefficient. Additionally, administrators face challenges in identifying vulnerabilities and determining the appropriate fixes, often relying on services from VDE (Verband der Elektrotechnik Elektronik Informationstechnik e.V.) or CISA (Cybersecurity & Infrastructure Security Agency). Monitoring vulnerabilities remains a mostly manual task, with each equipment vendor publishing security advisories and updates on their own websites, such as Siemens Industry Online Support (SIOS). With multiple vendors, the effort required to stay updated becomes increasingly cumbersome.

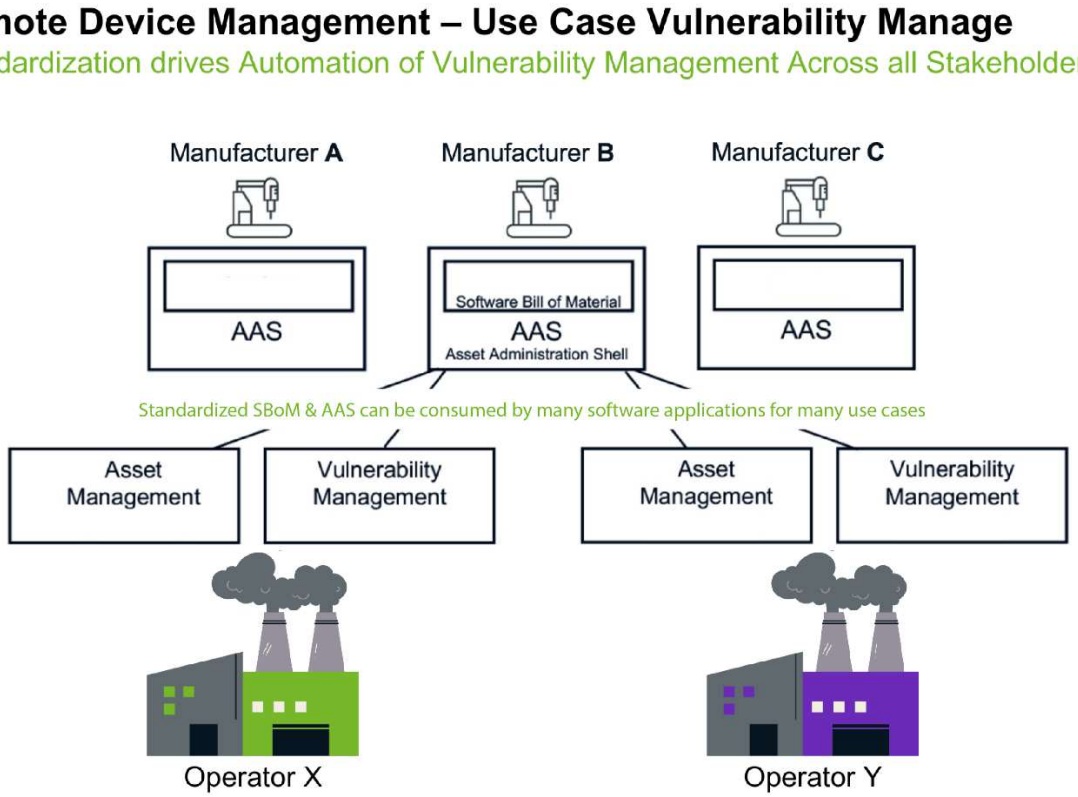
When it comes to integrating IT and OT systems, current solutions fall short. Most available device management systems are tailored for IT equipment and fail to address the unique requirements of OT environments. Even when OT devices are included, support is typically limited to specific device classes and is vendor-specific. For OT device management to evolve, it needs to shift from these manual, isolated practices to a centralized, automated. Only through integrating OT devices into a network can effective remote maintenance and control be achieved. An Asset Administration Shell (AAS) alone offers limited benefits if the devices are not connected to the network. By providing open interfaces, centralized asset management can be established, forming a foundation for standardized processes, streamlining workflows, and enabling efficient digital vulnerability management.

Applications & Use Cases

The Open Industry 4.0 Alliance is addressing this challenge by aiming to create a comprehensive guide and best practices for overcoming the hurdles of interoperable IT and OT integration across different manufacturers. The SBoM use case demonstrates a practical implementation of cross-vendor vulnerability management through the exchange of SBoMs based on the IDTA Software Bill of Material sub-model.

In addition to vulnerability management, SBoM offers several other valuable use cases and benefits. For instance, SBoM enables enhanced license compliance by providing a clear view of all software components, ensuring that companies adhere to licensing requirements. It also facilitates smoother incident response processes, as organizations can quickly identify which devices or systems are affected by a specific vulnerability and take appropriate action. Furthermore, SBoM supports efficient software lifecycle management, helping manufacturers keep track of software updates, dependencies, and compatibility across their devices.

Using the IDTA submodel, the SBoM is provided in a standardized, machine-readable format that is independent of the manufacturer. This allows management systems to analyze the SBoM and compare it against a list of known security vulnerabilities. Each time new software vulnerabilities are published or when software changes occur in production, such as after an update, a new comparison can be conducted automatically, ensuring that potential threats are detected promptly.



The SBoM significantly contributes to achieving a higher level of security by offering complete transparency into the software components running on each device. By having detailed knowledge of all software elements, organizations can proactively identify and address vulnerabilities before they are exploited. This transparency also helps build trust, as it demonstrates a commitment to security and allows stakeholders to verify the integrity and safety of devices in their operational environments.

Through this standardization, the connection between vulnerability databases and actual device information is managed in a vendor-neutral manner. It is crucial to develop open solutions that guarantee interoperability, not only for the SBoMs of devices from different manufacturers but also for the various software tools used in device and vulnerability management. This approach ensures that organizations can maintain a high level of security across diverse ecosystems, reducing the risk of breaches and minimizing the impact of potential vulnerabilities.

Conclusion

The growing number of software packages and vulnerabilities within industrial machinery makes it unrealistic to manage these threats manually. The only practical way forward is to automate how we handle and track software vulnerabilities, using standardized tools and methods to create a more organized approach.

We don't have to start from scratch. The IT sector has been dealing with these challenges for years, and we can take their tried-and-tested practices to help manage vulnerabilities in industrial settings. By combining this knowledge with cross-vendor standards, we can create solutions that work across different industries and types of equipment.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has suggested three main steps for vulnerability management that are just as useful in the industrial world:

- First: Asset Discovery & Vulnerability Identification
- Second: Implementing Security Controls
- Third: Patch Management

In this paper, we've focused mainly on the first step - getting a clear inventory of the software in use and identifying vulnerabilities. We've shown how using a SBoM makes it easier to track software components and spot potential security issues.

To deal with other challenges like patch management or continuous monitoring, it will be essential to work together and use common industry standards. This is where we, the Open Industry 4.0 Alliance (OI4), come into play. As a group of companies dedicated to promoting open standards and improving connectivity across different industrial systems, we aim to tackle some of the biggest challenges in managing vulnerabilities.

We are committed to promoting cross-vendor standards to ensure that SBoMs and other security practices can function effectively across various manufacturers and systems. Additionally, we provide best practices and practical guides through working groups (WG) such as the Remote Device Management WG.

Furthermore, we foster a collaborative environment by encouraging companies to share their experiences and learn from one another, helping to strengthen the overall approach to vulnerability management. Lastly, we actively support key technologies like the Asset Administration Shell (AAS), which plays a crucial role in organizing and managing SBoMs across different brands and types of equipment, ensuring a seamless and efficient handling of vulnerabilities in software-driven machinery.