INL/CON-23-70977-Revision-0

Software Bill of Materials in the Nuclear Industry

June 2023

Shannon Leigh Eggers, Baleigh Rae Morgan, Ethan S Bauer, Tori Brooke Simon, Drew Christensen

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/CON-23-70977-Revision-0

Software Bill of Materials in the Nuclear Industry

Shannon Leigh Eggers, Baleigh Rae Morgan, Ethan S Bauer, Tori Brooke Simon, Drew Christensen

June 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Software Bill of Materials in the Nuclear Industry

U.S.A

Shannon L. Eggers [a,1], Baleigh R. Morgan[a,2], Drew N. Christensen[b,3], Tori B. Simon[a,4], Ethan S. Bauer[a,5]

[a]Idaho National Laboratory, [b]Pacific Northwest National Laboratory

[1]Shannon.Eggers@inl.gov, [2]Baleigh.Morgan@inl.gov, [3]Drew@pnnl.gov, [4]Tori.Simon@inl.gov, [5]Ethan.Bauer@inl.gov

Abstract

Nuclear power plants (NPP) have thousands of digital assets throughout their facility. Typically, NPPs have asset and configuration management programs that capture the make, model, and version of a component. This information, however, usually only includes first- or second-tier components and does not capture the complete enumeration of software components and their dependencies within operational technology (OT) equipment. As seen with recent cyberattacks, this level of detail is insufficient for identifying if and where an exploitable vulnerability exists within a facility. A software bill of materials (SBOM) provides this detailed enumeration. Further, integrating SBOMs with vulnerability data sources and vulnerability attestation reports can provide improved awareness leading to better cyber risk management and incident response. Preferably, SBOMs are provided by the supplier; however, when an NPP already owns a device, it is less likely they will have a supplier provided-SBOM. Fortunately, SBOMs can be generated on installed digital assets. This paper provides an introduction to the U.S. Department of Energy Office of Nuclear Energy paper titled "Towards Software Bill of Materials in the Nuclear Industry," which describes the SBOM ecosystem and provides a suggested approach to methodically and seamlessly integrate an SBOM program in an NPP.

1. Introduction

Cyberattacks are a daily news occurrence. Ransomware attacks regularly impact business operations in every industry, including small business, medical, chemical, manufacturing, and energy. Supply chain cyberattacks on software and firmware are also increasing and becoming more sophisticated, not necessarily in the payload itself, but in the logistics required to successfully deploy an attack. For instance, the SolarWinds attack used five distinct pieces of malware through a complex series of actions to infiltrate and launch the final attack [1]. Furthermore, it is commonplace for software developers to integrate open-source software into their products. Without a proper inventory, or software bill of material (SBOM), the large number of software components in a single product may be unknown to both the end-user and the developer.

Large, industrial processes, such as a nuclear power plant (NPP), may use many digital systems for the operation of their plant. While the majority of NPPs maintain robust asset and configuration management systems, which may include a bill of materials (BOM), the information captured typically only includes first- or second-tier data on the make, model, and version (MMV) of the subcomponents. As the sophistication of cyberattacks continues, however, this high-level MMV information is insufficient. For instance, if an attack impacts a library, such as the Apache Log4j logging library, which is used in both proprietary and open-source Java-based software applications, end-users may remain unaware that they

have such a vulnerability at their facility. The vulnerability in Log4j enables adversaries to achieve remote code execution and take full control of a system [2].

The use of SBOMs at a facility can improve visibility into the complex network of components and dependencies within a digital asset or system. This detailed SBOM information can then be combined with other tools, such as vulnerability data sources and vendor attestation reports, to improve vulnerability management and reduce overall computer security risk. Many organizations are actively working to develop and improve the SBOM ecosystem, primarily by improving SBOM enumeration capabilities during software development such that complete SBOMs will be available for new products [3-5]. However, end-users at NPPs can also implement an SBOM program at their facility to enable SBOM generation on existing, installed digital assets. The remainder of this paper provides a brief introduction of the U.S. Department of Energy Office of Nuclear Energy Cybersecurity program report titled, "Towards Software Bill of Materials in the Nuclear Industry" [6].

2. SBOM Ecosystem

An SBOM is defined by U.S. Executive Order 14028 as a "formal record containing the details and supply chain relationships of various components used in building software" [7]. Thus, an SBOM is a listing of all software components, subcomponents, and their dependencies, regardless of the provenance or type (e.g., open-source, proprietary, custom). Components and subcomponents include source code, executables, libraries, and modules. Firmware is also typically included in an SBOM.

An SBOM by itself does not reduce cyber risk. An SBOM program's primary benefit is realized by integrating it with other tools and data sources within the SBOM ecosystem. For instance, a nuclear facility that has fully implemented an SBOM program integrated with vulnerability management and incident response programs can: (1) quickly determine if they are affected when a new software vulnerability is disclosed or a cyber incident occurs; (2) quickly identify where they are affected; and (3) rapidly respond to and/or remediate the vulnerability or incident. Integration of SBOMs with other tools and programs can also improve asset and configuration management efforts; improve cyber risk management decisions; enable improved integrity, authenticity, and assurance; and provide improved pedigree, provenance, and supply chain risk management information [6, 8].

When considering the possible loss of confidentiality (e.g., information theft) of an SBOM, an individual might think that an SBOM provides an adversary with too much intelligence and that implementing an SBOM program is too risky. However, it is commonly assumed that an adversary intent on targeting a facility already has more knowledge about an NPPs installed assets than the facility owner. SBOMs can 'level the playing field' between defender and attacker [6]. Even so, however, an SBOM program and any related information must be protected in accordance with the nuclear facility's security requirements. If the SBOM is vendor supplied, this information should also be protected throughout the supply chain.

Table 1 lists the baseline set of elements necessary to uniquely and unambiguously identify SBOM components and their relationships as defined by NTIA [9]. Additional details on each of these SBOM elements is provided in [6].

Several standards exist for SBOM formats, including CycloneDX [10], Software Package Data Exchange (SPDX) [11], and Software Identification (SWID) [12]. All three standards capture similar information and can be used for SBOM generation, ingestion, and use. Using a standard machine-readable format enables better integration capabilities and improved likelihood towards automation. The use of automated or semi-automated tools

Table 1. Baseline SBOM elements.

Data fields	(required) author name, timestamp, component name, component version, supplier name, unique identifiers, relationship (recommended) component hash, license information
Automation/semi-automation	automatic generation, machine readability, standard data formats
Practices	frequency, depth, known unknowns, completeness, distribution and delivery, access control, and accommodation of mistakes

improves efficiency and completeness in SBOM generation, especially considering the potential for large and complex content in an NPP. Of course, it is more likely that full automation will occur during product development as opposed to SBOM generation on installed digital assets. Humans-in-the-loop will likely be required for SBOM enumeration within an NPP. SBOMs generated from compiled or object code will generally be less complete than SBOMs generated from source code.

Tools developed for the SBOM ecosystem are available from both open-source and commercial developers. These tools are categorized based on function by NTIA, as follows [13]:

1. Produce an SBOM (e.g., automatically as part of the software build process, manually, or as an audit tool)
2. Consume an SBOM (e.g., enable viewing or human readability, provide difference comparisons, analyze and/or ingest/import into other software or tools)
3. Transform an SBOM (e.g., translate to another file type, merge data, integrate into tools such as APIs or libraries).

3. Vulnerability Management Use Case

Figure 1 illustrates proposed process steps for integrated SBOM vulnerability management analysis as described in [6]. In step 1, components and subcomponents are determined through SBOM enumeration. In step 2, known vulnerability data, such as vendor notifications, third-party notifications, and data repositories (e.g., Common Vulnerabilities and Exposures [CVE] and the National Vulnerability Database [NVD]) are gathered. In step 3, vendor attestation reports are acquired from suppliers. In step 4, this vulnerability data is correlated with SBOM data to identify vulnerabilities on installed components within the facility. Finally, in step 5, this correlated information is used within the facility's cyber risk management plan to identify, prioritize, and treat cyber risks.

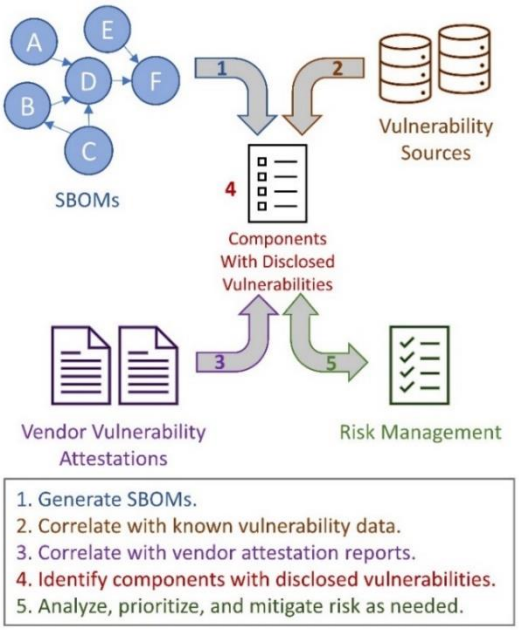

Figure 1. Process steps for integrated SBOM vulnerability management analysis [6].

4. An SBOM Program Implementation Approach (Adapted from [6])

Implementing an SBOM program at an existing NPP will be a lengthy process. The long duration is primarily due to the number of installed digital assets at an NPP and the limited times available to take

them out-of-service for SBOM enumeration. Many digital assets in an NPP can only be accessed while they are offline during maintenance or an outage. The steps provided in [6] are to be used as a guide to tailor a project specifically for a facility, as each nation-state and NPP owner may have different requirements. It is intended to integrate an SBOM program into an NPP using existing resources with limited additional funding and personnel—the likelihood for embarking on the project is higher if it can be accomplished within existing operation and maintenance (O&M) budgets. Long term, it is anticipated that successful implementation will simplify cyber risk and vulnerability management, thereby reducing future O&M costs while improving overall security posture.

The functional objectives for the project are to [6]:

- use existing personnel
- simplify current plant processes
- integrate into existing programs and workflows (e.g., cybersecurity, asset and configuration management, engineering change, digital engineering, supply chain)
- establish semi-automated and periodic (or continuous) vulnerability management
- reduce overall cyber risk to improve the security posture of the NPP.

While implementing an SBOM project at an NPP is a lengthy undertaking and SBOM ecosystem tools and integration concepts are still evolving, the most important step is to start the project. As the project continues, facility owners will benefit from enhanced software transparency, improved response time to new threats and vulnerabilities, and reduced cyber risk.

Suggested activities for each stage of the SBOM project are listed in Table 1. 'Crawl' activities are foundational activities that lay the groundwork for the program. 'Walk' activities are foundational activities that result in establishment of tools and repositories to enable SBOM enumeration. During this phase, integration with vulnerability data and correlation tools will start to provide actionable risk management information. 'Run' activities are enhancing activities that establish automation (or semi-automation) tools for enhanced monitoring of vulnerabilities and seamless integration with other NPP programs.

Each phase and activity are further described in [6]. The selection and order of activities in each phase are recommendations; an NPP may choose to skip an activity or move an activity up or down depending on their overall project timeline and resource availability.

Table 2. Recommended SBOM project activities for each "crawl, walk, run" phase [6].

Phase	Step	Activity
CRAWL (foundational)	1	Develop a project plan and change management plan
	2	Determine project roles and responsibilities
	3	Identify existing programs and workflow changes
	4	Determine SBOM format and minimum requirements
	5	Identify repository and security requirements
	6	Identify tooling requirements
	7	Create SBOM documentation
	8	Update procurement procedures
	9	Identify other policy and procedure changes
	10	Prioritize digital assets and develop SBOM generation schedule
	11	Acquire available SBOMs and vulnerability information
	12	Run a pilot test
WALK (sustaining)	1	Establish/acquire SBOM tooling
	2	Establish or enhance SBOM repository
	3	Generate and maintain SBOMs
	4	Establish or enhance vulnerability tracking
	5	Establish vulnerability incident response process
RUN (enhancing)	1	Integrate into existing NPP programs and processes
	2	Develop capabilities to dynamically monitor SBOM vulnerabilities
	3	Establish/enhance a secured, central repository for all data
	4	Complete SBOM generation for all installed digital assets
	5	Maintain awareness of ongoing industry advancements

5. New Reactor Build

The SBOM implementation recommendations apply to both existing and new nuclear facilities. If the implementing organization is an NPP owner, they should require the reactor vendor to supply SBOMs for all provided digital assets. Alternatively, if the implementing organization is the reactor vendor, they should use similar guidance to require SBOMs from their suppliers for all digital assets in their reactor build such that they can then provide complete SBOM information to their customers. It is more efficient and complete to generate SBOMs during software development and it is easier to develop a complete listing of all software components during initial stages of the systems engineering lifecycle. Regardless of whether the entity is the NPP owner or reactor vendor, SBOMs should be required with every procurement and contract agreement. Additionally, any in-house developed assets should require SBOM generation as part of the development process. SBOMs should also be updated throughout the systems engineering lifecycle as modifications occur.

Conclusion and Future Work

Implementing and integrating an SBOM program into an NPP can provide improved awareness into a facility's cyber risk management and supply chain management programs. Additionally, integration of SBOMs with other plant programs and workflows will improve the capability and efficiency of plant operations. Capturing lower tier components and dependencies and then integrating this information with vulnerability sources and vendor attestation reports will provide the capability to rapidly identify if and where a newly discovered vulnerability is located. This information can then be used by personnel to prioritize risks and enable much faster response and mitigation times. Integrating SBOMs with cyber supply chain risk management will enable the NPP to better identify compromises in the supply chain through evaluation of pedigree, provenance, and integrity of SBOM characteristics. This SBOM process may also be adopted for use in other nuclear facilities.

A primary objective for implementing the program in a "crawl, walk, run" method is to minimize implementation costs by using existing NPP resources while incrementally improving the cybersecurity posture of the facility. However, this stepwise approach can be tailored as necessary to implement the program based upon the requirements of the facility, as slowly or quickly as desired.

Planned future work includes (1) performing a case study of this methodology at a nuclear reactor to identify benefits and gaps and (2) investigating the use of new tooling within the SBOM ecosystem. We also aim to extend collaborations with industry and government groups to enable adoption of SBOM programs in nuclear facilities. It is also recognized that fully complete digital BOMs (DBOM) will include the hardware BOM (HBOM). Future work will maintain awareness of ongoing developments on HBOMs in order to integrate those findings into a more holistic NPP DBOM.

Acknowledgments

This work was supported by the U.S. DOE Office of Nuclear Energy Cybersecurity Crosscutting Technology Development Program and the U.S. DOE National Nuclear Security Administration Office of International Nuclear Security under the DOE Idaho Operations Office, Contract DE-AC07-05ID14517.

References

[1] Eckels, S., J. Smith, and W. Ballenthin. *SUNBURST Additional Technical Details*. Mandiant, Accessed on: January 20, 2023. Available: https://www.mandiant.com/resources/blog/sunburst-additional-technical-details

[2] CISA. *Apache Log4j Vulnerability Guidance*. Cybersecurity and Infrastructure Security Agency (CISA), Accessed on: June 2022. Available: https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

[3] CISA. *Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force*. Cybersecurity and Infrastructure Security Agency, Accessed on: June 2022. Available: https://www.cisa.gov/ict-scrm-task-force

[4] *Software Bill of Materials*. CISA, Accessed on: September 2022. Available: https://www.cisa.gov/sbom

[5] INL. *Idaho National Laboratory Software Bill of Materials: Exploring a proof of concept for the energy community*. Accessed on: June 2022. Available: https://inl.gov/sbom-poc/

[6] Eggers, S., "Towards Software Bill of Materials in the Nuclear Industry," Idaho National Laboratory, Idaho Falls, ID, 2022.

[7] Executive Office of the President, "Executive Order 14028 on Improving the Nation's Cybersecurity," 2021, Available: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

[8] NTIA, "Roles and benefits for SBOM across the supply chain," NTIA Multistakeholder Process on Software Component Transparency, 2019, Available: https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf.

[9] U.S. Department of Commerce, "The minimum elements for a Software Bill of Materials (SBOM) pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity," 2021, Available: https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf.

[10] *CycloneDX Specification Overview*. CycloneDX Core Working Group, Accessed on: June 2022. Available: https://cyclonedx.org/specification/overview/

[11] *SPDX Specifications*. Linux Foundation, Accessed on: June 2022. Available: https://spdx.dev/specifications/

[12] *Software Identification (SWID) Tools*. NIST, Accessed on: September 2022. Available: https://pages.nist.gov/swid-tools/

[13] NTIA, "How-to guide for SBOM generation," NTIA Software Transparency Healthcare POC, Available: https://www.ntia.gov/files/ntia/publications/howto_guide_for_sbom_generation_v1.pdf.