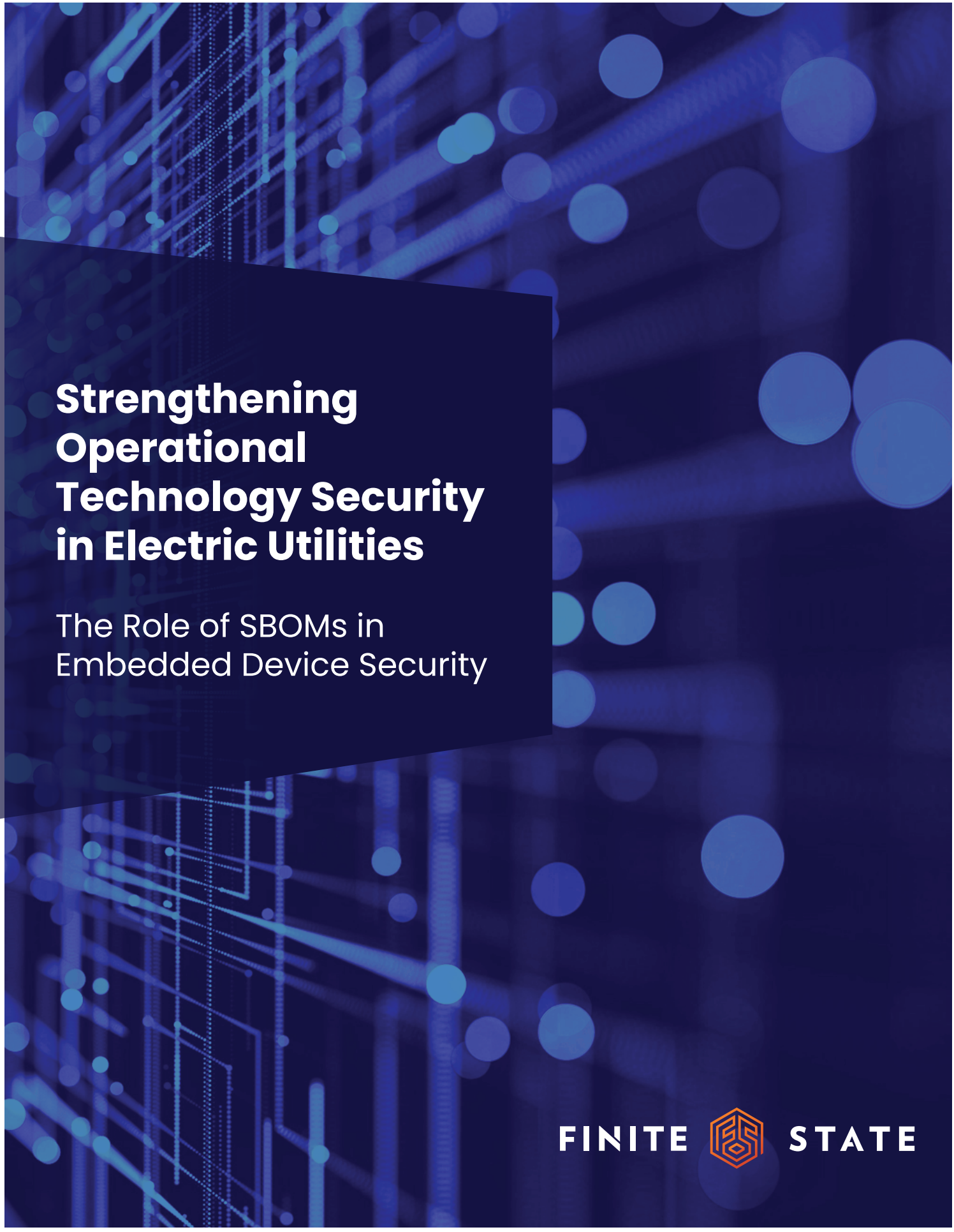
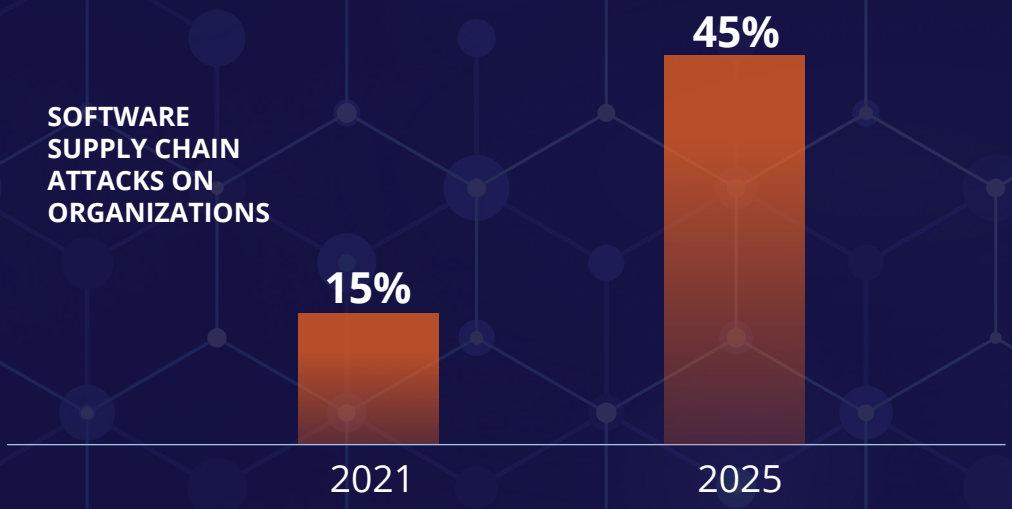

Strengthening Operational Technology Security in Electric Utilities
The Role of SBOMs in Embedded Device Security
FINITE STATE

FINITE STATE

As operational technology (OT) equipment becomes increasingly interconnected and electric utilities embrace digital transformation, the need for robust software supply chain security is crucial for ensuring the stability and reliability of the power grid.

The threat to public safety and national security is real. According to Gartner, "by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021."



Two of every three executives name cybercrime as their top threat this year, and nearly 30% of large organizations expect an increase in OT attacks that could stop production and generate impacts rippling throughout supply chains, according to 2023 PwC research.

Embedded devices, which are integral to the functioning of software supply chains, and the nation's power grid, require a comprehensive approach to security that includes an understanding of the software components they rely on. One key element in such an approach is the Software Bill of Materials (SBOM). This article will discuss the role of SBOMs in enhancing software supply chain security for OT equipment in electric utilities and highlight the limitations of SBOMs in addressing all security challenges.

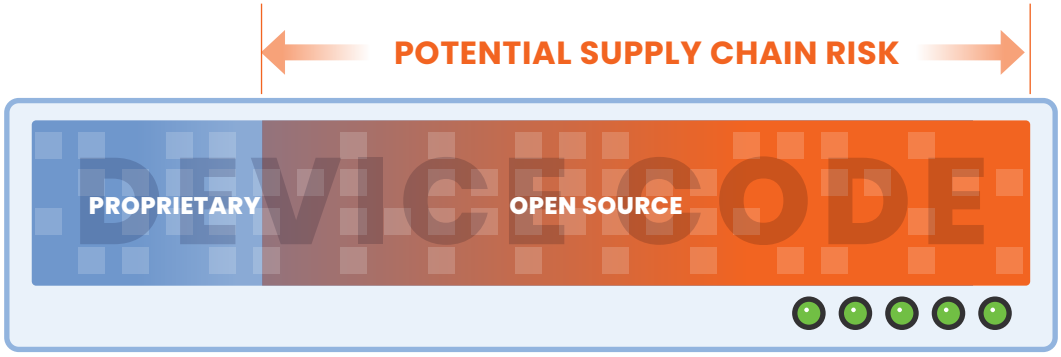
[1] "Emerging Tech: A Software Bill of Materials Is Critical to Software Supply Chain Management," Gartner, Driver, Mark, September 6, 2022.

[2] 'A C-suite united on cyber-ready futures – Findings from the 2023 Global Digital Trust Insights,' PwC, Joyce, Sean, 2023.

Understanding SBOMs in the Context of OT Equipment

A Software Bill of Materials (SBOM) is a document that enumerates all the components within a software product, including open-source libraries, proprietary code, and third-party dependencies. In the context of OT equipment, an SBOM provides transparency into the software composition of critical embedded devices that the power grid depends on, making it easier for utilities to identify potential vulnerabilities, manage updates, and ensure compliance with licensing requirements.

But why is an SBOM critical, and in some cases, mandated? Any device connected to an OT network likely features 15–20% of code that's proprietary to the manufacturer. The rest of the code across the device is compiled open source code spanning the components, binaries and chip sets — and that is where supply chain risk emerges. Now, multiply how many of those devices might reside at any given substation, and you have a level of exposure that's significant.



SBOMs and Software Supply Chain Security in Electric Utilities

The integration of SBOMs into a comprehensive software supply chain security program for electric utilities offers several advantages:

Improved Vulnerability Management

By providing a clear view of the software components within embedded devices, an SBOM allows utilities to quickly identify known vulnerabilities in third-party dependencies. Security teams can then prioritize remediation efforts based on the potential impact on the power grid and the risk associated with each vulnerability.

Better Risk Assessment

An SBOM enables electric utilities to better understand the risks associated with their software supply chain by giving them insights into the origin of each component in their embedded devices. This knowledge can be used to assess the security posture of suppliers and prioritize security efforts based on the risk profile of individual components.

Enhanced License Compliance

Open-source components in embedded devices often come with specific licensing requirements. An SBOM allows utilities to track and manage licenses, ensuring compliance and avoiding potential legal issues.

Streamlined Incident Response

In the event of a security incident affecting OT equipment, an SBOM can expedite the response process by helping security teams quickly identify affected components in embedded devices and develop a targeted remediation plan.

Facilitated Software Patching

Keeping software up to date with the latest security patches is crucial for maintaining a secure supply chain for embedded devices in electric utilities. An SBOM can help utilities identify outdated components and streamline the patching process, reducing the window of opportunity for attackers.

Limitations of SBOMs in Software Supply Chain Security for Electric Utilities

While SBOMs are a valuable tool in a comprehensive software supply chain security program for electric utilities, they have certain limitations:

Unidentified Vulnerabilities

SBOMs can help utilities identify known vulnerabilities in their embedded devices' software components. However, they are ineffective at detecting previously unknown or undisclosed vulnerabilities. To mitigate this risk, utilities should employ additional security measures, such as static and dynamic code analysis, penetration testing, and runtime application self-protection.

Insider Threats

SBOMs provide transparency into the software composition of embedded devices but do not address risks associated with malicious insiders or compromised developers. Utilities should implement robust access controls, secure development practices, and continuous monitoring to protect against insider threats.

Tampering and Counterfeiting

An SBOM does not guarantee the integrity of the software components it enumerates. Attackers could tamper with or counterfeit components in the supply chain, introducing malicious code or vulnerabilities. To counter this risk, utilities should establish a secure development lifecycle (SDLC) that includes processes for validating the integrity of third-party components, such as cryptographic signing and code reviews.

Continuous Monitoring

While SBOMs can facilitate the identification and remediation of vulnerabilities, they do not provide real-time monitoring of software components in embedded devices. Electric utilities should implement continuous monitoring solutions that track changes to the software supply chain, detect anomalies, and raise alerts for potential security incidents.

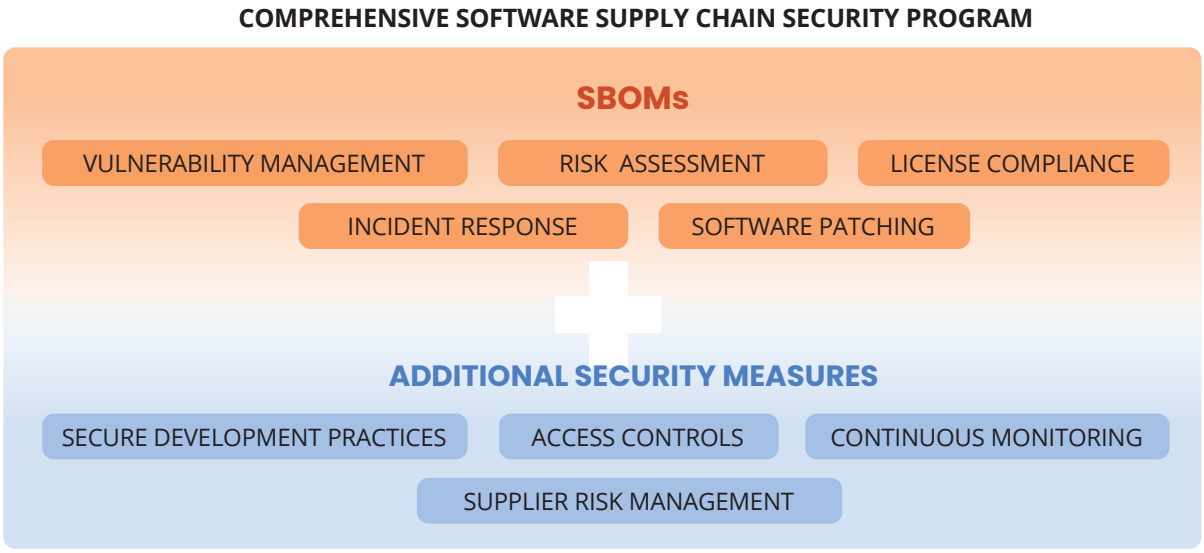
Supplier Security

Although SBOMs provide insights into the origin of oftware components in embedded devices, they do not ensure the security posture of suppliers. Utilities must assess the security practices of their suppliers and establish ongoing communication channels to receive updates about potential vulnerabilities or incidents. Implementing a robust supplier risk management program and conducting regular audits can help maintain a secure software supply chain for OT equipment.

Next Steps: Drawing Conclusions about SBOMs

Software Bills of Materials (SBOMs) play a crucial role in enhancing software supply chain security for operational technology equipment in electric utilities by providing transparency into the composition of critical embedded devices, facilitating vulnerability management, risk assessment, license compliance, incident response, and software patching. However, SBOMs alone cannot address all aspects of software supply chain security for electric utilities.

Utilities should recognize the limitations of SBOMs and implement a comprehensive software supply chain security program that incorporates additional security measures, such as secure development practices, access controls, continuous monitoring, and supplier risk management. By adopting a holistic approach to software supply chain security for OT equipment, electric utilities can better protect their critical infrastructure and mitigate the risks associated with software vulnerabilities and supply chain attacks.



While they are a critical component of any software supply chain program, SBOMs, by themselves, do not represent a comprehensive and complete approach to securing electric utilities from the totality of threats that lurk in the software supply chains of our nation's critical infrastructure. Simply put, software supply chain security and SBOM are not one and the same.

While SBOMs, by definition, cannot protect against threats such as unreported vulnerabilities, insider threats, and tampering and counterfeiting, they do represent an indispensable tool in the fight for software supply chain security in today's electrical utilities through informing vulnerability management, enabling better risk assessment, and streamlining incident response efforts.

How to Get Started with SBOMs: Trust, But Verify

When utilities receive an SBOM from a supplier, there's an element of trust that comes as part of that exchange of information. While building trust relationships with suppliers is critical when receiving SBOMs, or any information, from them, verification is better.

Experience tells us that trust relationships, inevitably, break down. Thankfully, SBOMs can be verified, and should be subject to verification when they're used in critical industries such as electric utilities. When the stakes rise high, electric utilities should be equipped to do their own testing and generation of SBOMs, and be prepared to ask suppliers what tools they use and trust to generate the SBOMs they provide.

It's no secret that the SBOM industry, and the connected device ecosystem, is new and rapidly evolving. If you need help navigating the software and binaries you receive from suppliers, ask for help. While the SBOM Challenge at the S4x23 ICS industry event showed that SBOMs, in form and function, differ widely among providers, Finite State's Next Generation Platform emerged as the only platform that could complete all facets of the challenge and surfaced five times more vulnerabilities than any other competitor.

Finite State was also named the 2023 winner of the "Industrial IoT Product of the Year" award, "Security Automation Solution of the Year" award by CyberSecurity Breakthrough, and the 2022 "IoT Evolution Security Excellence" and "IoT Platforms Leadership" awards from IoT Evolution World.

Ready to See Finite State in Action? Schedule a Demo

Finite State brings visibility and control to the supply chains of the connected devices and embedded systems of today's electric utilities. The Finite State Next Generation Platform unpacks and analyzes every file, configuration, and setting in a firmware build and creates a comprehensive SBOM.

Finite State's SBOM identifies known and zero-day vulnerabilities, assigns a score that reflects your risk level, and delivers insights you can act on now to secure your software before it's too late.

Let's look at your software and its supply chain, using our intuitive platform. We'll help you secure your critical infrastructure faster and help mitigate the risks that threaten the safety and functioning of the power grid.

Schedule a demo today

FINITE STATE

finitestate.io