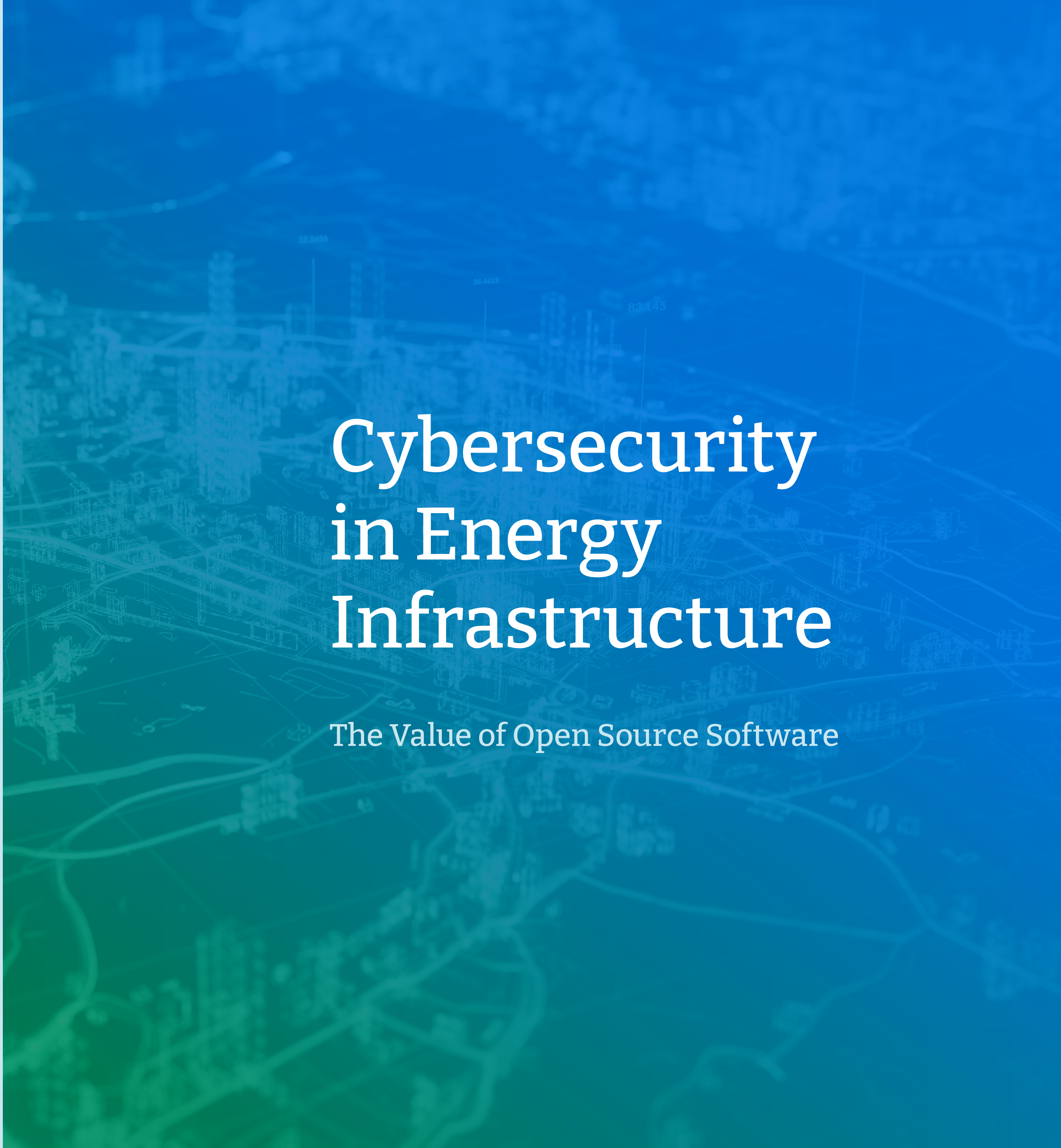
LF ENERGY

OpenSSF
OPEN SOURCE SECURITY FOUNDATION



Cybersecurity in Energy Infrastructure

The Value of Open Source Software

November 2023

Contents

Introduction

In an era where our dependence on digital systems is profound, the energy sector stands at a pivotal juncture. As the energy landscape undergoes a transformative shift driven by the urgency to address climate change, consumer demands, distributed energy resources, and the rise of energy electrification, the role of cybersecurity becomes paramount. This paper delves into how open source software is critical to the innovation and transformation of our energy infrastructure. Contrary to common misconceptions, OSS offers not just affordability and adaptability but also a robust shield against cyber threats.

Innovating together, the energy sector can meet the challenges of today for a bright future.

This transformation is reshaping how we produce, distribute, and consume energy. However, with digital advancements come challenges, including interoperability and cybersecurity. Open source's transparent nature, coupled with a vast community of developers, ensures rapid innovation, high software quality, and most importantly, robust security.

Since security starts with a solid foundation and processes, the paper covers best practices for open source development.

Innovating together, the energy sector can meet the challenges of today for a bright future.

This paper is jointly prepared by LF Energy and OpenSSF.

What is LF Energy?

LF Energy is an open source foundation that focuses on creating a technology ecosystem to support rapid decarbonization, which is advantageous for the environment, enables economic prosperity, and promotes social well-being for future generations. The Foundation provides a neutral, collaborative community to build shared digital investments that will transform the world's relationship with energy.

LF Energy, a vendor-neutral, non-profit organization, brings together various stakeholders, including energy producers, utilities, end users, academia, government, and the technology industry. They collaboratively develop technology solutions — including software solutions, standards, and specifications — for the energy sector to accelerate decarbonization and the general energy transition. They build communities to develop open technologies, frameworks, reference architectures, and research to alleviate pain points and identify the most urgent priorities to digitally transform the energy sector. This includes aspects such as cybersecurity, interoperability, control, automation, virtualization, flexibility, and digital orchestration for balancing supply and demand, challenges that cannot be solved by legacy, proprietary solutions.

By adopting an open source strategy that maximizes flexibility, agility, and interoperability, LF Energy aims to innovate faster and accelerate the energy transition. LF Energy projects provide a unified approach to developing non-differentiating code, enabling the world's power systems to rapidly transform to electrification. Members contribute resources and leadership to allow the community to innovate and advance decarbonization.

In essence, LF Energy is a trailblazer in using open source strategies to digitally transform the energy sector and accelerate decarbonization, bringing together diverse stakeholders to address the challenges and opportunities of the energy transition collectively.

What is the OpenSSF?

The Open Source Security Foundation (OpenSSF) is a cross-industry organization that brings together the most critical open source security initiatives and the individuals and companies that support them.

The OpenSSF's technical vision revolves around a future where participants in the open source ecosystem use and share high-quality software, with security handled proactively, by default, and as a matter of course. They provide tools, services, training, infrastructure, and resources to achieve this vision. They focus on mission-critical software, metrics, tooling, best practices, developer identity validation, vulnerability disclosures best practices, and more. It was established on the premise that security researchers need a mechanism to allow them to collaboratively address methods required to secure the open source security supply chain.

The OpenSSF is committed to collaboration and working upstream and with existing communities to advance open source security for all. The project's core values include public good, openness and transparency, maintainers first, diversity, inclusion, and representation, agility and delivery, credit where credit is due, neutrality, and empathy. These values guide their approach to improving the security of open source software, inviting and including people from various backgrounds, locations, identities, and perspectives, and promoting a culture of mutual respect and inclusiveness.

The Evolution of Energy Systems

The energy landscape is experiencing an unprecedented shift, primarily driven by the rise of distributed energy resources (DERs), a surge in energy electrification, and the pressing imperative to mitigate climate change. DERs, primarily encompassing wind turbines, solar panels, and energy storage systems, are pioneering a new energy production and consumption paradigm, ushering in a more distributed, dynamic, and unpredictable energy ecosystem. Concurrently, the urgency of addressing climate change has catalyzed the transition toward a sustainable, low-carbon energy ecosystem.[1] This evolution is further accelerated by electrification in sectors such as transportation and heating, thereby placing additional demands on energy infrastructure. The industry's stakeholders are now grappling with these changes, striving to navigate the energy system's growing complexity and propel the shift toward sustainability.

In this transformation, the efficacy of open source software (OSS) is becoming increasingly evident. Due to its affordability, adaptability, transparency, and interoperability, OSS is being embraced by more entities within the energy sector. Its low or non-existent procurement and distribution costs facilitate cost efficiencies and spur innovation. Furthermore, OSS empowers organizations to tailor software solutions to their specific requirements and operational parameters. The robust and expansive OSS user and developer communities enhance their value proposition through ongoing improvement and innovation, fostering an inclusive, collaborative software development ethos. This dynamic engenders rapid innovation, superior software quality, and robust security. Additionally, OSS offers a viable alternative to proprietary software, enabling businesses to evade vendor lock-in and maintain control over their IT infrastructure.

Digital Transformation

The digital transformation of the energy industry is helping the industry meet sustainability goals, integrate new generation systems, and improve internal and external processes. It affects all business functions.[2]

2023 ENERGY TRANSFORMATION READINESS STUDY

76% of energy stakeholders surveyed **have a clear strategic plan for digitalization** and have it already implemented.

The benefits are well-documented and extensive. Generally, digital systems are more intelligent, more efficient, and more reliable. For instance, an application of IoT in wind farms is predicted to save between 50M and 230M USD in operating expenses and improve the current 743 GW global wind power capacity to an amount that could supply 20% of the world's electricity by 2030.[3] Blockchain technology, such as Hyperledger Fabric, allows consumers with micro-generation power to purchase and sell excess electricity to other consumers rather than the local utility.[4] Artificial intelligence (AI) assists smart grids in self-healing and more accurately predicts future demand and trends.[5]

Energy companies know the need for digitalization and are implementing it. According to Linux Foundation Research, 76% of energy stakeholders have a clear strategic plan for digitalization and have already implemented it.[6]

Of course, there are challenges, as with any new technology: security,[7] privacy,[8] vendor lock-in, insufficient trained workforces, and more. The use of data and AI can create privacy implications if misused or not adequately protected. Similarly, blockchain technology has its own security and privacy concerns, such as data breaches, personal information exposure when stored on public ledgers, and the potential for abuse by malicious actors.

As technology is upgraded and new solutions considered, companies see the challenges with vendor lock-in and proprietary systems that require specially-trained employees.

The Role of Open Source in the Energy Transformation

Open Source is Time-Tested and Widely Adopted

New challenges and opportunities are ahead for energy companies, policymakers, and consumers alike as they work to manage the growing complexity of the energy system and undertake the transition to a more sustainable energy future.

With the inevitable digital transformation underway, the challenges are many. No one solution or concept will solve every challenge, but open source software is poised to tackle many of the difficulties and lift the entire industry through collaboration.

The world runs on open source software. From A Guide to Enterprise Open Source,[9] "Open source software (OSS) has

2023 ENERGY TRANSFORMATION READINESS STUDY

51% of energy stakeholders see IT and OT on the way to convergence in their organizations.

transformed our world and become the backbone of our digital economy and the foundation of our digital world. From the Internet and the mobile apps we use daily to the operating systems and programming languages we use to build the future, OSS has played a vital role. It is the lifeblood of the technology industry. Today, OSS powers the digital economy and enables scientific and technological breakthroughs that improve our lives. It's in our phones, our cars, our airplanes, our homes, our businesses, and our governments. But just over two decades ago, few people had heard of OSS, and its use was limited to a small group of dedicated enthusiasts."

A large, engaged community working on an open source project can often detect and patch security issues faster than a small, in-house team can.

While OSS dominates so much of our worldwide software stack, adoption of open source systems has been slower in the energy ecosystem. This is due, in many ways, to how the energy grid was built. However, digital transformation pushes information technology (IT) and operations technology (OT) to converge. 51% of energy stakeholders see IT and OT on the way to convergence in their organizations.[10] This drives the need for interoperable systems between providers. With the need to replace legacy systems with digital transformation, there is no better time.

Energy stakeholders see the need to adopt better solutions that offer flexibility, interoperability, and customization. Already, 64% of energy stakeholders report using more OSS than closed source.[11] Why? Because OSS reduces grid complexity by enabling integration and management of distributed energy resources (DERs) and easing application development.[12] Additionally, they see cost reduction and transition speedup as the most popular benefits and flexibility as the most promising features of OSS for energy stakeholders.

There are challenges, of course. Performance, support, and security are the main barriers to OSS adoption in the energy sector.[13] And security is top-of-mind for everyone these days.

Benefits of Open Source in the Energy Sector

Open source software offers several significant benefits for the energy sector. One of its main advantages is the principle of collective intelligence: through the open source model, programmers, engineers, and developers from all over the world contribute to building and improving the software. They collaborate around a common need for a particular software solution. This influx of diverse perspectives and skills enhances the robustness of the software and accelerates its development and refinement.

2023 ENERGY TRANSFORMATION READINESS STUDY

64% of energy stakeholders report that they use more open source software (OSS) than closed source.

While they work together to build and maintain the common tools, often hosting it in a vendor-neutral foundation such as the Linux Foundation, they all benefit from better foundational software and focus more of their time and resources on other innovations and products.

Security

From a security standpoint, open source software offers transparency.[14] The source code is openly available for inspection, which allows potential security vulnerabilities to be identified and addressed swiftly.[15]

But the benefits of transparency only occur if there is a robust community behind it. Open source software is the foundation of every application we rely on today.[16] Proactively addressing security concerns is vital to the future of nearly all industries in the modern economy,[17] and that requires a two-way street. It requires consumers to also contribute back to the community by incorporating the nature of OSS dependencies into standard cybersecurity and development practices and contributing back to the OSS communities that organizations rely on.[18]

A large, engaged community working on an open source project can often detect and patch security issues faster than a small, in-house team can. This proactive approach to security helps counter the increasingly sophisticated cyber threats the energy sector faces.

Customizability

Customizability is another benefit of open source software. It allows developers to adapt the source code to meet specific needs or integrate it with existing systems. This flexibility can be particularly beneficial in the diverse and complex infrastructure of the energy sector, where bespoke solutions are often needed. With OSS, you can customize a solution that is 90% there rather than either build a solution 100% from scratch or wait for a vendor to make the customizations you require.

Cost savings

Moreover, using open source software can lead to significant cost savings. Open source software is generally free to use, reducing initial investment costs. While there may be associated costs for implementation, ongoing maintenance, and community contribution, these are often lower than the licensing fees associated with proprietary software.

Finally, using and contributing to open source projects helps organizations build their reputation in the tech community. It demonstrates a commitment to collaboration, transparency, and improving industry standards. This can be an essential factor in attracting and retaining top talent in the industry. It also increases internal technical skills as developers go from specifying needs to off-the-shelf vendors to making the updates themselves. Internalizing knowledge and skills specific to your organization's business can lead to cost savings.

The Need for Open Source Specific to Digital Transformation

While several factors are driving digital transformation, underlying much of it is a need to address climate change. The time is yesterday, so solutions need to be developed and implemented sooner rather than later. Open source **offers the rapid innovation required.**

It also **offers the interoperability required.** Utilities will no longer have total control over energy systems when DERs replace centralized power generation. Because of the industry's fragmentation, not all power production, transmission, and distribution technologies are compatible, making interoperability crucial for integrating the extensive range of DERs that are going online. A single organization cannot create the necessary technologies alone — the outdated "black box" methods and closed source energy industry software cannot be used in this new era because they could result in different measurement standards and utility evaluation criteria. Open source prevents conflicting standards while ensuring the interoperability and compatibility of systems by providing vendor neutrality and collaborative development.[19]

It also **offers affordable, reliable, and adaptable solutions.** Organizations can use open source solutions that are already available and modify them to suit their unique requirements. Multiple open source solutions are in the early adoption phase at LF Energy. For instance, operators can create applications to perform dynamic power flow simulations and power security analyses on the network with an open source library, PowSyBl.[20] Organizations can also assist in the creation of OSS by joining open source communities and submitting code, instructions, and bug reports. Additionally, businesses can develop their own OSS and distribute it to the general public, encouraging creativity and accelerating the development of new solutions — recognizing the benefits of open source development for their own solutions. Finally, organizations can encourage the use of OSS in the energy industry by promoting its advantages and fostering stakeholder cooperation and knowledge sharing.

Highlights of Open Source Projects in Energy

LF Energy currently hosts nearly two dozen open source projects directly applicable to the energy ecosystem. Here are three highlights currently in production:

CoMPAS configures substations to enhance their automation, enabling efficient onboarding for renewables and greater device interoperability.

OpenSTEF provides more precise load forecasting to enable the onboarding of renewable energy from new sources while balancing greater consumer demand. **SEAPATH** is an open source platform for digital substations that enables more flexible, scalable, and innovative automation and protection. RTE and Savoir-faire Linux developed it under the LF Energy umbrella. SEAPATH has been developed using a test-driven approach to cybersecurity, with over 700 active tests in the continuous integration chain running in two distinct labs. Major players including GE are now active contributors to the project.

You might also be interested in reading more in-depth about how RTE and Alliander embraced open source to speed the modernization of the electrical grid in this report.

Check out all of the LF Energy projects and consider contributing to the projects as a developer, technical writer, marketer, or more. All skill sets are needed and appreciated.

Current State of Cybersecurity in Energy

The energy sector's cybersecurity presents a challenging landscape. It is a high-priority target for cyberattacks due to its strategic importance in maintaining national security and economic stability. In recent years, the energy infrastructure has seen an uptick in cyber threats, with attackers employing increasingly sophisticated methods. According to a report by the Kaspersky Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the energy sector was second only to building automation for the percentage of computers on which malicious objects are blocked.[21]

With the rapid digital transformation and decentralization of electricity generation and distribution, the cyberattack surface is significantly larger than previous, centralized power generation, and the need to work together to protect the system is non-negotiable. By working together on open source solutions and security best practices, we realize common benefits and individual cost savings.

What are recent cyberattacks on energy infrastructure?

Here is a sampling of cyberattacks on energy systems and other critical infrastructure over the past few years:

Ukrainian Power Grid Attack (2015)

This cyberattack targeted the Prykarpattyaoblenergo power facility, a critical infrastructure component in the Ivano-Frankivsk region of Ukraine. The systems were infected with malware, leaving nearly 700,000 people without power.[22, 23]

> *With the rapid digital transformation and decentralization of electricity generation and distribution, the cyberattack surface is significantly larger than previous, centralized power generation*

Cosmic Lynx Targets Electric Grids with Malware

CosmicEnergy is a new piece of malware that appears to be linked to Russia and targets industrial control systems (ICS), specifically to cause electric grid disruption. Once CosmicEnergy accesses a target's OT systems, it can initiate power disruptions by sending remote commands to powerline switches and circuit breakers. They also emphasized that it "illustrates that the barriers to entry for developing offensive OT capabilities are lowering as actors leverage knowledge from prior attacks to develop new malware."[24]

Chinese Espionage on U.S. Critical Infrastructure

Western intelligence agencies and Microsoft said in May 2023 that Volt Typhoon, a group they described as Chinese state-sponsored, had been spying on various U.S. critical infrastructure organizations, from telecommunications to transportation hubs. A U.S. official said they were using "built-in network tools to evade our defenses and leaving no trace behind." Such techniques are harder to detect as they use "capabilities already built into critical infrastructure environments."[25, 26]

SolarWinds

In 2020, a major software company providing system management tools, had its IT performance monitoring system, Orion, hacked by the Russian Foreign Intelligence Service. The authorized access actually occurred in September 2019, and the threat actors injected malicious code known as Sunburst into Orion in February 2020. The updated code was pushed to customers by SolarWinds in March and over 18,000 customers installed it. This allowed the criminals to access SolarWinds' customers' IT systems and install even more malware to spy on companies and organizations.[27, 28] The impact was massive, and is known to have compromised a number of energy systems.[29]

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued a critical alert concerning Russian state-sponsored and criminal cyber threats to critical infrastructure, including energy infrastructure (Alert AA22-110A). The advisory highlights the growing threat posed by Russian state-sponsored cyber activities. These actors have shown the capability and intent to target critical infrastructure sectors, including the energy industry. They employ various tactics, techniques, and procedures that can lead to data theft, service disruption, or even damage to physical assets.[30, 31] The threat actors leveraged the trust relationship between software vendors and customers, underscoring the need to further secure software supply chain security.[32]

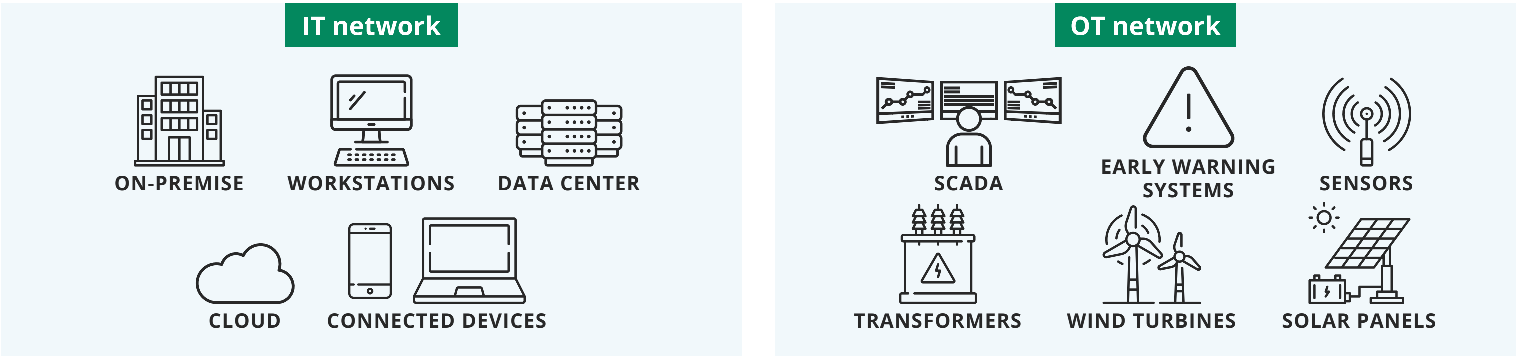
Colonial Pipeline

On May 7, 2021, the Colonial Pipeline, an oil pipeline in the U.S., was the victim of a ransomware attack. The attack forced them to shut down 5,500 miles of their oil pipeline, which supplies 45% of the oil for the U.S. East Coast. The hackers gained access to the system through an old company VPN that didn't require multi-factor authentication.[33, 34, 35]

Ransomware Attacks (2022)

Over one-third of ransomware attacks reported to the FBI last year impacted organizations in a critical infrastructure sector. Of the 2,385 ransomware attacks reported, 870 hit critical infrastructure organizations. 15 of those were in the energy sector.[36]

Potential Attack Surfaces



Challenges and Issues in Energy Sector Cybersecurity

The energy sector's growing dependence on digital technology and interconnected systems has led to increased cybersecurity challenges and has the potential to open doors to even more. Following is a synopsis of these challenges, focusing on technology, people, and processes. The industry can devise more effective strategies to protect vital energy infrastructure by recognizing and understanding these.

Technology Challenges

One of the main challenges is the complexity and diversity of the energy sector's infrastructure. It comprises a wide array of interconnected components, ranging from power generation facilities to transmission and distribution networks and consumer endpoints. While beneficial in operational efficiency, the digitalization of these systems expands the attack surface for potential cyber threats.

Another issue is the sector's widespread use of Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition

An undertrained, short staffed workforce creates additional vulnerabilities, from learning curves to experienced employees being too busy.

(SCADA) systems. While these technologies have revolutionized energy management, they were not designed with cybersecurity in mind. As such, they often lack the necessary security features to resist sophisticated cyber attacks.

This weakness is further exacerbated due to how industrial control systems (ICS) and operational technology (OT) are viewed. Too often, organizations view mutable systems as immutable. That is, the software that controls immutable systems, such as transmission lines, is also considered immutable. However, software running ICS is mutable and must be maintained and updated as any other software. Attackers understand they are mutable and are taking advantage of that fact.

People, Processes, and Organizational Culture

Addressing these challenges requires a comprehensive approach, which includes human resources, processes, and culture. Weak processes and controls, inadequate training, and staffing shortages open doors for attackers.

For instance, many organizations don't require security training, multi-factor authentication, strong passwords, robust user access control, blocking unauthorized hardware, etc. These can affect security more than the software running the systems.

Particular to industrial control systems, the OT often requires certification from a third party. When the software is viewed as immutable, any changes require recertification, a lengthy process which hinders the regular updating of the systems to address known vulnerabilities.

Finally, a skilled labor shortage and skill gaps in the sector create additional concerns. The energy infrastructure is complex and diverse and, as we note, fundamentally transforming. An undertrained, short staffed workforce creates additional vulnerabilities, from learning curves to experienced employees being too busy.

Best Practices in Open Source for Cybersecurity

One value of open source projects is that many minds from different backgrounds and organizations combine efforts, skills, and knowledge to make better projects. When people view something from various perspectives, they see different things that hamper groupthink and catch oversights.

The open source community comes together, through the OpenSSF, to collaborate and work both upstream and with existing communities to advance open source security for all. For instance, they hosted the Secure Open Source Software Summit 2023, where participants discussed the security challenges for the consumption of OSS in critical infrastructure sectors and beyond and highlighted the shared responsibility needed to ensure the resilience of OSS in critical infrastructure. During the summit, the OpenSSF released a SOSS Vision Brief detailing the community's work over the past year to further secure OSS and plan for the future. Learn more here and consider participating if you aren't already.

With the community, the OpenSSF also compiled and published concise guides for developing and evaluating open source software to help increase its resiliency against cyberattacks. Each guide is generally ranked by cost/benefit, recognizing that this will vary between organizations and projects. Below are some best practices and tools to develop, maintain, and use open source software.

OpenSSF Scorecard

OpenSSF Scorecard assesses open source projects for security risks through a series of automated checks. OSS developers created it to help improve the health of critical projects that the community depends on. However, anyone can use it to proactively assess and make informed decisions about accepting security risks within your codebase. You can also use the tool to evaluate other projects and dependencies and work with maintainers to improve codebases you might want to integrate.

Organizations need to train developers to develop secure software from the beginning of the process rather than relying on a security check and remediation later in the pipeline.

Scorecard helps enforce best practices that can guard against:

- Malicious maintainers
- Build system compromises
- Source code compromises
- Malicious packages

The OpenSSF runs a weekly scan of the 1 million most important open source projects judged by their direct dependencies and publishes the results in a BigQuery public dataset.

One of the criteria in Scorecard is earning an OpenSSF Best Practices badge. All LF Energy projects have to earn an OpenSSF Best Practices Badge at the passing level to graduate at the "incubation" stage.

Improve authorization and authentication policies

Stealing and using an authorized user's credentials is one of the most common entry points for malicious hackers. For example, the Colonial Pipeline ransomware attack came through a legacy corporate VPN that didn't require multi-factor authentication (MFA). At a minimum, users with any privileges on the system and all privileged developers should have MFA enabled on their accounts. In addition to MFA, use accounts that uniquely and verifiably identify individual users/actors and avoid hard-coded credentials, default passwords, and weak configurations.

Train developers to develop secure software

A core principle in building things is to build them right at each step. It is far easier than fixing mistakes later once you build upon them. The same holds for software. Organizations need to train developers to develop secure software from the beginning of the process rather than relying on a security check and remediation later in the pipeline. The free OpenSSF course or the hands-on Security Knowledge Framework course are excellent. SAFECode's Fundamental Practices for Secure Software Development provides a helpful summary. Linux Foundation Training & Certification, ISC2, and OpenSSF recently announced a new collaboration to empower the open source cybersecurity community through secure software development, knowledge sharing, education, certification and much more.

Evaluate software before using it as a dependency

Following the Concise Guide for Evaluating Open Source Software, evaluate ALL software before utilizing it. Only add it if needed, check its OpenSSF Scorecard score, double-check its name to counter typosquatting, and ensure it's from the correct repository.

You must also ensure you are using the most up-to-date version. According to Sonatype's 2022 State of the Software Supply Chain Report,[37] 95.5% of known-vulnerable downloads had a non-vulnerable option available. Taking the time to research and evaluate the software makes a difference.

Long response times, lack of processes and training, and alert fatigue, among other things, weaken an organization's security posture.

Use the Secure Supply Chain Consumption Framework (S2C2F)

To help guide your evaluation efforts, utilize S2C2F. It is a consumer-facing framework for evaluating open source software packages. The S2C2F guide outlines and defines how to securely consume OSS dependencies into the developer's workflow, and should be used by software developers at energy companies who are building software and applications to run energy infrastructure. Originally developed by Microsoft and donated to the OpenSSF in 2022, S2C2F is designed from the ground up to protect developers from accidentally consuming vulnerable packages (including malicious and compromised packages), helping to mitigate supply chain attacks by decreasing consumption-based attack surfaces.

Adopt Continuous Integration and Continuous Deployment (CI/CD)

Adopting CI/CD streamlines the software development process so that consumers can apply updates without the complexity of scheduling maintenance windows. This provides repeatable deployments, updates, and rollbacks and resilience to upgrades to address vulnerabilities in dependent software, including underlying operating systems

Process Improvements

When was the last time you heard a car alarm and thought, oh no, someone is breaking into a car? There are so many false alarms, we instinctively get annoyed and ignore them. This is an example of alert fatigue, a real issue in security. Long response times, lack of processes and training, and alert fatigue, among other things, weaken an organization's security posture.

Efficient and effective processes are critical. Look at optimizing system configurations, improving user access control, adopting secure coding practices, automating malware scanning protocols, and cloud infrastructure automation with API management. Human behavior will outwit cumbersome processes. While it likely isn't malicious, it can result in harmful actions. Making rules and processes easy to follow is one of the most impactful steps to improve your organization's resiliency.

Software Bills of Materials (SBOMs)

Since all modern software is built upon a foundation of other software, created by other organizations, software bill of materials (SBOMs) are an essential tool for understanding the components of open source software. They provide a detailed list of all the parts and pieces that make up a particular piece of software, including the version number, copyright information, vendor details, security vulnerabilities, and other pertinent details. This allows organizations to understand how their open source software is composed and address any potential security vulnerabilities.

SBOMs are also helpful for tracking compliance with regulations, determining licensing terms, and ensuring that users of open source software understand how to use it properly. Ultimately, SBOMs enable organizations to maximize the security and performance of their open source software or critical infrastructure while ensuring they remain compliant with applicable laws.

The U.S. government recently required that all software used in critical infrastructure in the U.S. have an SBOM[38]. The European Union is expected to follow suit soon.

SPDX is one standard available for communicating SBOM information, including provenance, license, security, and other related information. Because it is an ISO standard and open source, it is easily integrated into third-party OSS projects.

By incorporating provenance into software supply chain security, organizations can mitigate the risks associated with compromised software components

Know the Origin, Authenticity, and Integrity of Software Components

Establishing the origin, authenticity, and integrity of software components throughout the software supply chain (aka provenance) is critical. Use practices and technologies to ensure software and its components are trusted and free from malicious activities or vulnerabilities. This includes verifying the identity of software vendors, ensuring secure distribution, and monitoring for any unauthorized modifications. By incorporating provenance into software supply chain security, organizations can mitigate the risks associated with compromised software components and enhance the overall resilience of their systems.

SLSA (pronounced "salsa") stands for Supply-chain Levels for Software Artifacts and is a crucial security framework designed to protect the integrity of software supply chains. Recognizing the potential vulnerabilities any software can introduce into a supply chain, especially as systems become increasingly intricate, SLSA provides a structured checklist of standards and controls. These standards are crafted to prevent tampering, bolster integrity, and secure packages and infrastructure.

In-toto provides a framework to protect the integrity of the software supply chain. It does so by verifying that each task in the chain is carried out as planned, by authorized personnel only, and that the product is not tampered with in transit. It shows evidence: who, when, where, virus-free, etc.

Software Signing and Verification

Software signing is critical to ensure the integrity of updates, network communications, and binary distributions. It's essentially a digital seal of approval that guarantees the authenticity and trustworthiness of the software elements. It adds an extra layer of protection against unauthorized access and tampering. Plus, every signing event is recorded in an auditable and tamper-resistant log to verify the authenticity of software updates and patches easily.

Sigstore can be used to fortify the integrity and security of the open source software supply chain. It makes it easier and more automatic for developers releasing open source artifacts for public use to digitally sign what they make and for security experts to look up those artifacts in Sigstore's transparency log — a public, tamper-proof ledger of signatures.

Vulnerability Management

Vulnerability management is like the immune system of your digital infrastructure, identifying potential weaknesses and working to strengthen them. Effective vulnerability management helps identify these potential risks, ensuring that the software or system is continually updated and protected against emerging threats. It's a proactive approach, focusing on prevention rather than cure.

Of course, internal processes that automate continuous monitoring and reporting and utilizing SBOMs so you know what is in the stack are critical to effective vulnerability management.

The OpenSSF has a Vulnerability Disclosures Working Group that aims to improve open source security by developing and advocating well-managed vulnerability reporting and communication. They document and support best vulnerability disclosure and coordination practices and help share information on vulnerability information.

Conclusion

As the digital age propels the energy sector into uncharted territories, cooperation is key. Coming together on joint solutions is where open source shines, and its transparency strengthens its security posture and fosters adaptability to specific use cases. Let's harness the power of open source to ensure that our energy infrastructure remains resilient and ready to meet the challenges of tomorrow.

Like all things worthwhile, it takes an investment of time and resources. Contribute to projects, open up your own projects, and train employees in open source and security best practices. With a firm foundation, the entire ecosystem will be more stable.

Let's see what we can accomplish together.

Acknowledgments

First, we want to recognize all of the maintainers, contributors, and members of LF Energy and OpenSSF projects.

The following subject matter experts contributed to the background of this paper:

Eloi Bail, *Savoir-faire Linux*
Aeva Black, *Microsoft**
Florent Carli, *RTE France*
Frederic Didier, *RTE France*
Boris Dolley, *RTE France*
Dustin Ingram, *Google*
Anto Monti, *RWTH Aachen University*
Anne Tilloy, *RTE France*
Christophe Villemer, *Savoir-faire Linux*
David A. Wheeler, *The Linux Foundation*

* at time of contribution

Endnotes

[1] https://www.mdpi.com/1996-1073/14/23/7997

[2] Review and Categorization of Digital Applications in the Energy Sector, https://www.mdpi.com/2076-3417/9/24/5350#

[3] Optimization and digitization of wind farms using internet of things: A review, https://onlinelibrary.wiley.com/doi/abs/10.1002/er.6942

[4] Integrating big data and blockchain to manage energy smart grids—TOTEM framework, https://www.sciencedirect.com/science/article/pii/S2096720922000227

[5] https://orbit.dtu.dk/files/246750940/2020_09_16_PUBLICATION_GEEE_7.2020.INF.1_Digitalization_enabling_the_new_phase_of_EE_2_.pdf

[6] 2023 Energy Transformation Readiness Study

[7] https://www2.deloitte.com/us/en/pages/consulting/articles/cybersecurity-energy-sector.html

[8] https://orbit.dtu.dk/files/246750940/2020_09_16_PUBLICATION_GEEE_7.2020.INF.1_Digitalization_enabling_the_new_phase_of_EE_2_.pdf

[9] https://www.linuxfoundation.org/research/guide-to-enterprise-open-source

[10] 2023 Energy Transformation Readiness Study

[11] 2023 Energy Transformation Readiness Study

[12] 2023 Energy Transformation Readiness Study

[13] 2023 Energy Transformation Readiness Study

[14] https://www.ge.com/digital/blog/keep-open-mind-about-open-source-utility-environment

[15] https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/oss(10).pdf

[16] https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html

[17] https://www.linuxfoundation.org/research/census-ii-of-free-and-open-source-software-application-libraries

[18] https://www.linuxfoundation.org/research/addressing-cybersecurity-challenges-in-open-source-software

[19] https://www.cetril.org/interoperability/

[20] https://www.powsybl.org/

[21] https://ics-cert.kaspersky.com/publications/reports/2023/09/13/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2023/

[22] https://www.nec.com/en/global/techrep/journal/g17/n02/170204.html

[23] https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[24] https://www.scmagazine.com/news/cosmicenergy-malware-electric-grids

[25] https://www.reuters.com/technology/microsoft-says-china-backed-hacker-targeted-critical-us-infrastructure-2023-05-24/

[26] https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

[27] https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

[28] https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

[29] https://theintercept.com/2020/12/24/solarwinds-hack-power-infrastructure/

[30] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a

[31] https://www.finra.org/rules-guidance/guidance/cybersecurity-alert-050222

[32] https://www.csoonline.com/article/570191/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html

[33] https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

[34] https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

[35] https://www.nytimes.com/2021/06/08/business/colonial-pipeline-hack.html

[36] https://www.cybersecuritydive.com/news/ransomware-critical-infrastructure-2022/645068/

[37] https://www.sonatype.com/state-of-the-software-supply-chain/introduction

[38] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

www.lfenergy.org

www.openssf.org

To reference this work, please cite as follows: “Cybersecurity in Energy Infrastructure,” The Linux Foundation, November 2023