

Leveraging Hardware Reverse Engineering to Improve the Cyber Security and Resilience of the Smart Grid

Arne Roar Nygård^a, and Sokratis Katsikas^b

*Department of Information Security and Communication Technology, Norwegian University of Science and Technology,
Gjøvik, Norway
{arne.nygard, sokratis.katsikas}@ntnu.no*


Keywords: Digital Supply Chain Attack, Smart Grid, Cyber Resilience, Hardware Reverse Engineering


Abstract: Cyber-attacks on digital supply chains are rising, and Critical Infrastructures (CIs) such as the Smart Grid are prime targets. There is increasing evidence that vendors, service providers, and outsourced IT -providers are at equal risk of being used by malicious actors to gain a foothold in the power grid - delivering exploits that can disrupt electric power delivery and severely damage our economy. Long digital supply chains with components from different manufacturers require a new approach and methods to ensure the needed security in Critical Infrastructures. Hardware Reverse Engineering (HRE), commonly used for verifying the security of an embedded system, includes disassembling to analyse, test, and document the functionality and vulnerability of the target system. This paper proposes leveraging HRE for improving both the security and the resilience of the power infrastructure against cyber-attacks enabled through the digital supply chain, by organising HRE activities, and how this can be organized within the equipment procurement process in a Distribution System Operator (DSO).

1 INTRODUCTION

Many rely on suppliers to deliver products, systems, and services. It's how we do business. However, supply chains are often large and complex, with equipment from different vendors. In addition, in recent years, there's been a significant increase in cyberattacks resulting from vulnerabilities within the supply chain. These attacks can result in devastating, expensive, long-term ramifications for affected organisations, their supply chains, and their customers. Likewise, cyberattacks on digital supply chains are officially rising, and the power grid is a prime target. It is no longer just the software and hardware suppliers that are being used as doorways to the power grid. There is increasing evidence that service providers such as accountancy firms, legal firms, cloud providers, outsourced Information Technology (IT) providers, and security and Security Operation Centers (SOC) providers, among others, are at equal risk of being used by malicious actors to gain a foothold into the power grid and deliver exploits that can result in outages and inflict severe damage to our economy. Cybersecurity focuses on harden-

ing the system to prevent such degradation; the focus is on the degree of degradation. In contrast, cyber resilience focuses on recovery. The fundamental notion of cyber resilience is the acceptance of cyber compromise as a likely event, and that the target systems suffer as a result of the compromise; the focus is on the system's ability to recover and adapt, not just resist. Cyber resilience characterises what happens after an adverse event and requires preparedness for known and unknown threats (Kott, A. and Linkov, I. (eds.), 2019). This paper focuses on Hardware Reverse Engineering (HRE) as a security tool. Hardware Reverse Engineering (HRE), commonly used for verifying the security of an embedded system, includes disassembling to analyse, test, and document the functionality and vulnerability of the target system. We propose leveraging HRE for improving both the security and the resilience of the power infrastructure against cyber-attacks enabled through the digital supply chain, by organising HRE activities, and how this can be organized within the equipment procurement process in a DSO. The remaining of the paper is structured as follows: In Section II the necessary background and the related work are presented. In Section III we present our proposal and in Section IV we summarize our conclusions and outline directions

^a  <https://orcid.org/0000-0001-5368-0917>

^b  <https://orcid.org/0000-0003-2966-9683>

for future work.

2 BACKGROUND AND RELATED WORK

The main research question addressed in the paper is: "How to improve cyber security and cyber resilience in Operational Technology (OT) Cyber Physical Systems (CPS) in the smart grid by leveraging Hardware Reverse Engineering?" Findings from a systematic literature review performed in (Nygård and Katsikas, 2022) and research on how the management of the digital supply chain is organised within organizations involved in the operation of the smart grid are used in addressing this. A DSO is used as a case study to showcase how the proposed approach can be integrated into relevant processes.

2.1 The Smart Grid as a Critical Infrastructure

Infrastructures are categorised as critical when their disruption impacts the well-being of the society. Society increasingly depends on a secure electricity supply to maintain functionality and cover basic needs. Consequently, a secure and safe electricity supply is critical for the community, and the electric power system is thus one of society's critical infrastructures and is expected to be continuously available (Zio, 2016). Accordingly, critical infrastructures must fulfil dependability requirements that impose rigorous techniques during procurement, development, commissioning and training/preparedness, as well as in regulatory audits of the operational systems (Assenza, G. et al, 2019).

The IoT-based Smart Grid is the empowered form of conventional power lines with IoT technologies. As information and communication technologies (ICT) are developed and applied in traditional power systems, the use of Smart Grid Cyber-Physical Systems (CPS) in Industrial Control Systems (ICS) increases too. However, as ICSs for critical infrastructures are becoming increasingly interconnected, cyber threats against critical infrastructure are becoming more sophisticated and challenging to defend against (Sperstad et al., 2020), and the IoT-based Smart Grid systems are no exception. Indeed, the electric grid faces significant cybersecurity risks from various actors, including criminals, terrorists, "hacktivists," and foreign governments. The grid is vulnerable to cyberattacks that could cause catastrophic, widespread, and lengthy blackouts (Sperstad et al., 2020), (Gun-

duz and Das, 2020), (United States Senate Republican Policy Committee, 2016).

2.2 Cyber-Physical and embedded systems

Cyber-Physical Systems (CPSs) integrate computation, communication, and control capabilities of Information and Communication Technology (ICT), with traditional infrastructures. This integration facilitates the monitoring and controlling of objects in the physical world as one of the essential requirements of different CIs (Rath and Tomar, 2021). These cyber-physical systems range from minuscule (e.g., pacemakers) to large-scale (e.g., a national power grid). The Internet of Things (IoT) and embedded systems are interdependent - one cannot function without the other. Embedded systems are microcontrollers equipped with specialized software enabling multiple devices to connect to the internet. Embedded computers that run secure embedded software are all around us. A large portion of the information ecosystem consists of embedded connected computers that participate in the physical control and the measurement of CIs and utilities, such as smart grid, automotive and industrial controls. In addition, they are pervasive near people, such as in cell phones, activity trackers, medical devices, or biometric tokens (Yuce et al., 2018). Indeed, deploying Internet-enabled embedded devices distributed over major critical domains may create indirect and nonobvious interconnections with the underlying CIs (Alcaraz et al., 2019). Embedded systems have a symbiotic relationship tying hardware to software, and it is that relationship that operates the device, and that "entire thing" is called firmware collectively (Brash, 2020). Firmware is crucial to system operation, providing instructions and guidance for the device to communicate with other devices or perform basic tasks and functions as the software intended. Because it connects hardware to software, firmware is necessary for a wide range of electronics such as smart grids, traffic lights, digital watches, printers, remote controls, mobile phones, network routers and switches, and servers (U.S. Department of Commerce and U.S. Department of Homeland Security,).

2.3 Securing Embedded Systems

In OT or ICS environments it is possible to identify embedded systems, their models, known vulnerabilities, potential network-born risks on several legacy insecure network protocols, weak authentication schemes, and even to determine their location. Finding a vulnerability does not require a trained eye.

Still, it does require a certain amount of knowledge about how systems work, how they are put together, how software is designed, and even a certain amount of detective skills. Systems engineering, programming / computer science, and cyber security can accelerate vulnerability discovery (Brash, 2020). Hardware components form the basis of trust in virtually any computing system. Thus, security failures in hardware pose a devastating threat to our daily lives. Accordingly, detecting vulnerabilities in hardware is paramount to ensure the security of embedded systems. As a result, security engineers commonly employ hardware reverse engineering to identify security vulnerabilities, detect intellectual property violations, or conduct large-scale integration (VLSI) failure analysis. Hardware Reverse Engineering is usually the tool of choice to detect fabrication faults, copyright infringements, counterfeit products, or malicious manipulations. It should be noted, however, that while hardware reverse engineering is a highly complex and universal tool for legitimate purposes, it can also be employed with illegitimate intentions, undermining the integrity of Integrated Circuits via piracy, subsequent weakening of security functions, or insertion of Hardware Trojans (Nygård. et al., 2022).

2.4 Digital supply chain

The term "supply chain" denotes the ecosystem of processes, people, organisations, and distributors involved in creating and delivering a final solution or product. In the ICT domain, the supply chain involves a wide range of resources (hardware and software), storage (cloud or local), distribution mechanisms (web applications, online stores), and management software. A supply chain attack is a powerful cyberattack that can breach even the most sophisticated security defences through legitimate third-party vendors. In the ICT domain, ensuring the integrity of the supply chain is becoming an essential concern, as components are often manufactured, owned, and operated by different entities across the globe; thus, the cascading effects from a single attack may have a widely propagated impact. This is even more so when components are used in ICSs operating in CIs. It is, therefore, essential to understand such attacks and attack vectors, the security challenges thereof, and measures to mitigate these (Nygård and Katsikas, 2022). For example, electric power grids have heavily adopted IT to perform real-time control, monitoring, and maintenance tasks (Sperstad et al., 2020). Digital Supply Chain risks may include the insertion of counterfeits, unauthorised production, tampering, theft, insertion of malicious software and hardware, and poor

manufacturing and development practices in the digital supply chain (Boyens et al., 2022). When assessing vendor security practices, the UK National Cyber Security Centre (NCSC) (National Cyber Security Centre (NCSC),) recommends that operators rely on something other than vendor documentation to determine vendor security. Instead, security assessments should be based on the vendor's implemented security behavior. A robust method to do this is Reverse Engineering, which retrieves information from anything artificial to understand its inner structures and workings (Fyrbiak et al., 2017).

3 HRE FOR CYBERSECURITY AND CYBER RESILIENCE

Cyber risk cannot be completely eliminated but needs to and can be managed, i.e., identified, assessed, and treated (Nygård and Katsikas, 2022). Nevertheless, even after treatment, a residual risk always remains. This implies that the probability of a cyber-attack to succeed is larger than zero. This, in turn, implies that the cyber risk owner should have in place processes and procedures for responding to and recovering from a successful cyber-attack. The current understanding in the cyber security community is that the system itself should be built in a way as to facilitate the response and recovery processes.

3.1 Resilience and cyber resilience

Resilience is the ability to recover from or easily adjust to shocks and stresses. Resilience refers to a system's ability to recover or regenerate its performance after an unexpected impact produces a degradation (Kott, A. and Linkov, I. (eds.), 2019). Resilience needs to be distinguished from the more established term "robustness." While both concepts share the objective of resisting stress, shock, disturbance, or disruption, the resilience concept is more dedicated to doing this in a manner of being "prepared to be surprised" rather than "preparing not to be surprised" (Mottahedi et al., 2021). Resilience is "the ability to withstand and reduce the magnitude and duration of disruptive events, which includes the capability to anticipate, absorb, adapt to, and rapidly recover from such an event." Importantly, we regard this "ability" as technical, organisational, and human properties and resources. A resilient digital infrastructure is necessary to support the platforms of a digital economy and society. The digital infrastructure is the physical hardware and related software that enables end-to-end information and communications systems

to operate. At the same time, critical infrastructures are becoming digitalised and made "smart" through the rollout of the smart grid, smart city, and intelligent transportation system projects, which further increase our reliance on resilient digital infrastructure. At the organizational level, organizations need to invest sufficiently in cybersecurity, plan for cybersecurity, build a security culture among employees, and adopt security-by-design and privacy-by-design principles (Dig,). The resilience of a CI can be distinguished into Soft Resilience and Hard Resilience. Hard Resilience represents the behavior of the technical part of the CI, and Soft Resilience means the people and the organisation running the CI before, during, and after the disruption (Mottahedi et al., 2021).

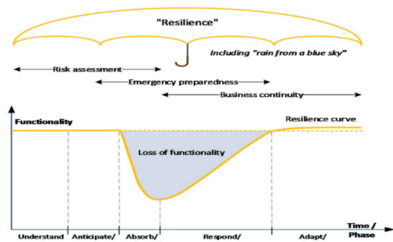


Figure 1: The Concept of Resilience (Kott, A. and Linkov, I. (eds.), 2019)

Cyber Resilience is the ability of an organization to protect itself from, detect, respond to and recover from cyber-attacks. By being resilient, organisations can reduce the impact of an attack and ensure that they can continue to operate effectively (IT Governance, 2023). Cyber resilience is the ability of an actor to resist, respond and recover from cyber incidents to ensure the actor's operational continuity (Kott, A. and Linkov, I. (eds.), 2019). Cyber resilience has emerged as a priority complementary to the management of cyber risk, that seeks to ensure that digital systems can maintain basic performance levels, even while capabilities are degraded by a cyber-attack (Jacobs et al., 2018). A resilience approach reduces downtime, enables response, and achieves a holistic approach to cyberattacks. CI needs a resilience framework for suppliers to manage supply chain risks as no such frameworks are available today. This framework should be flexible and applicable to each supplier in the supply chain for CI (Aarland and Gjørseter, 2022). Hardware device manufacturers rely on a complex chain of component suppliers, which may present organizational risks. Device vulnerabilities stemming from the supply chain make firmware an attractive target. Vulnerabilities buried in device components are almost invisible to most users, and enterprises may be unaware of or incapable of identifying these vulnerabilities. In

such specialised industries, only a few manufacturers may produce most of these parts (U.S. Department of Commerce and U.S. Department of Homeland Security,).

3.2 Reverse engineering (RE)

“The security of hardware is of the utmost importance, just like the foundation of your house: if it's bad, then your house may catastrophically collapse at some point. For an attacker, the hardware interface offers more avenues than a software interface. Yes, there may be all sorts of vulnerabilities in software with different impacts. But if an attacker breaks the security of a hardware interface, everything is at risk. Software attacks are often focused on exploiting a specific application. Weaknesses in hardware often lead to exploitation at the operating system level. And once we're in the operating system, every application is at risk, not just one. The attack surface is much bigger” (Witteman and Goncharov, 2023). To increase security and resilience at the hardware level, one must know how the target devices are vulnerable and identify relevant attack vectors. A robust method to do this is reverse engineering, which retrieves information from anything artificial to understand its inner structures and workings (Fyrbiak et al., 2017). Thus, RE can be very supportive in securing digital supply chains and increasing cyber resilience. In the software world, RE boils down to taking an existing program for which source code or proper documentation is unavailable and attempting to recover details regarding its design, security functions, and implementation (Nygård. et al., 2022). On the hardware side, a lack of focus on the early detection and mitigation of hardware vulnerabilities can have devastating consequences that are far more costly and time-consuming to remediate than software incidents (Cycuity Team, 2022). Over the past few years, hackers have increasingly targeted firmware to launch devastating attacks and that hardware security technologies can help protect against these risks (U.S. Department of Commerce and U.S. Department of Homeland Security,). These include the highly reliable hardware roots of trust technologies, which can be used to verify, protect or restore the system, data or code integrity and attest identity for components in a hardware system. Traditionally, Hardware RE (HRE) has been about taking shrink-wrapped products and physically dissecting them to uncover their design secrets. Such secrets were then typically used to make similar or better products. In many industries, HRE involves examining the product under a microscope or taking it apart and figuring out what each piece does (Kott, A.

and Linkov, I. (eds.), 2019). Additionally, HRE may be employed to understand a product's physical and functional details to replicate or redesign the original (Fyrbiak et al., 2017) or to improve one's product and analyze a competitor's product. In contrast, HRE is in this paper illuminated as a tool for revealing vulnerabilities and malicious manipulations. In the context of resilience, HRE has evolved to enable the understanding of increasingly complex systems.

While formal hardware security practices have existed for decades, the connected era is rewriting the rulebook for how semiconductor companies and product manufacturers need to approach hardware security. As a result, more and more cyber risk and security management frameworks are adopting the concept of cyber Resilience (e.g., the Department of Homeland Security's Cyber Resilience Review (CRR) or the National Institute of Standards and Technology (NIST) Special Publication 800-160 Volume 2). A first-ever E.U.-wide legislation of its kind: the Cyber Resilience Act introduces mandatory cybersecurity requirements for hardware and software products throughout their lifecycle. E.U. standards based on the Cyber Resilience Act will facilitate its implementation and will be an asset for the E.U. cybersecurity industry in global markets. The new Cyber Resilience Act will complement the E.U. cybersecurity framework: the Directive on the security of Network and Information Systems (NIS Directive), the Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), which the European Parliament and the Council recently agreed, and the E.U. Cybersecurity Act (European Commission, 2022).

3.3 The use case

Distribution System Operators (DSO), are the entities responsible for distributing and managing energy from the generation sources to the final consumers. DSOs are in the process of employing Digital Substations to substitute traditional substations. The Digital Substation is a term applied to electrical substations where operation is managed between distributed intelligent electronic devices (IEDs) interconnected by communications networks. In the electric power industry, an intelligent electronic device (IED) is an integrated microprocessor-based controller of power system equipment, such as circuit breakers, transformers and capacitor banks. IEDs receive data from sensors and power equipment and can issue control commands, such as tripping circuit breakers if they sense voltage, current, or frequency anomalies, or raise/lower tap positions in order to maintain the de-

sired voltage level. Some recent IEDs are designed to support the IEC61850 standard for substation automation, which provides interoperability and advanced communications capabilities. IEDs are used as a more modern alternative to, or a complement of, setup with traditional remote terminal units (RTUs). Unlike the RTUs, IEDs are integrated with the devices they control and offer a standardized set of measuring and control points that is easier to configure and require less wiring. Most IEDs have a communication port and built-in support for standard communication protocols (DNP3, IEC104 or IEC61850), so they can communicate directly with the SCADA system or a substation programmable logic controller. Alternatively, they can be connected to a substation RTU that acts as a gateway towards the SCADA server (McDonald, 2007). A phasor measurement unit (PMU) is a device used to estimate the magnitude and phase angle of an electrical phasor quantity (such as voltage or current) in the electricity grid using a common time source for synchronization. Securing the IEDs and PMUs in a digital substation is paramount for the overall cybersecurity and resilience of the smart grid. The use case focuses on mitigating the risk of intrusion into the physical site of a digital substation: Intelligent electronic devices (IEDs) are deployed in power systems to facilitate advanced automation and control of critical equipment. The hardware of these devices is considered root-of-trust. An engineer, technical staff, or an outsider with malicious purposes intrudes into the Digital Substation-fenced area and connects to the digital components. An attacker may gain access to an IED or PMU device by obtaining login credentials. Once it is compromised, an attacker can seize control of the physical entities in substations and may interrupt the normal functioning of switch devices, sabotage primary equipment and manipulate measurements to impact the stability of the power supply. If so, the attacker may reprogram the device, access data on the device, and/or stop/change device functionalities. The use case aims to enhance cyber resilience by developing new knowledge, research competence and innovating methods to investigate the potential hardware security vulnerabilities in Intelligent Electronic Devices (IEDs and PMUs) used in the "real world" smart grid. DSOs acquire equipment, including IEDs and PMUs, by following an approach consistent with that described in the ISO 27001 for handling third parties. With an eye towards improving cybersecurity and resilience in the context of the use case, this approach can be modified by introducing a "reverse engineering" subprocess, as shown in Figure 2.



Figure 2: Proposed inclusion of a Reverse Engineering subprocess into the equipment procurement process at a DSO

4 CONCLUSION

Several approaches have been proposed for securing the digital supply chain. Certification has been advocated as one of the most effective ways to ensure security in components from different vendors. Hardware Reverse Engineering (HRE) for uncovering vulnerabilities introduced through the digital supply chain in OT components in CI is proposed as an additional, complementary approach. The complexity of the digital supply chain ecosystem and the identified challenges create a need to address the issue of securing the infrastructure from a resilience rather than strictly a cybersecurity standpoint. Thus, cyber resilience has emerged as a complementary priority that seeks to ensure that digital systems can maintain essential performance levels, even while a cyber attack degrades capabilities. The inclusion of a reverse engineering subprocess within the equipment procurement process followed by a DSO is possible, and is expected to result in measurable improvement of bot cybersecurity and cyber resilience of digital substations in the power industry. Future research includes the pilot implementation of our proposed approach in a DSO on one hand, the execution of laboratory experiments for assessing the cybersecurity of IEDs and PMUs by means of HRE, and the preparation of training material for DSO technical staff on HRE.

ACKNOWLEDGEMENTS

This work has been funded by the Research Council of Norway in part by Project no. 320932 “Reverse Engineering som metodikk for verifikasjon av sikkerhet i digitale verdikjeder i en kritisk infrastruktur” and in part by Project no. 310105 “Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS)”.

REFERENCES

Aarland, M. and Gjørseter, T. (2022). Digital supply chain vulnerabilities in critical infrastructure: A systematic literature review on cybersecurity in the energy sector. In *Proceedings of the 8th International Conference on Information Systems Security and Privacy - Volume 1: ICISSP*, pages 326–333. INSTICC, SciTePress.

- Alcaraz, C., Burmester, M., Cuellar, J., Huang, X., Kotzanikolaou, P., and Psarakis, M. (2019). Guest editorial special issue on secure embedded iot devices for resilient critical infrastructures. *IEEE Internet of Things Journal*, 6(5):7988–7991.
- Assenza, G. et al (2019). White paper on industry experiences in critical information infrastructure security: A special session at critis. In *Nadjm-Tehrani, S. (eds) Critical Information Infrastructures Security. CRITIS 2019. Lecture Notes in Computer Science, vol 11777*. Springer, Cham.
- Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., and Fallon, M. (2022). Assessment of the Critical Supply Chains Supporting the U.S. ICT Industry.
- Brash, R. (2020). Protecting Embedded Systems in OT Cyber Security. <https://verveindustrial.com/resources/blog/protecting-embedded-systems-in-ot-cyber-security/>.
- Cycuity Team (2022). Detect and prevent security vulnerabilities in your hardware root of trust. https://cycuity.com/type/white_paper/detect-and-prevent-security-vulnerabilities-in-your-hardware-root-of-trust/.
- European Commission (2022). Proposal for a regulation of the european parliament and of the council on horizontal cybersecurity requirements for products with digital elements and amending regulation (eu) 2019/1020. <https://ec.europa.eu/newsroom/dae/redirection/document/89543>.
- Fyrbiak, M., Strauß, S., Kison, C., Wallat, S., Elson, M., Rummel, N., and Paar, C. (2017). Hardware reverse engineering: Overview and open challenges. In *2017 IEEE 2nd International Verification and Security Workshop (IVSW)*, pages 88–94.
- Gunduz, M. Z. and Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, 169:107094.
- IT Governance (2023). IT Governance’s Cyber Resilience Framework. <https://www.itgovernance.co.uk/cyber-resilience-framework>.
- Jacobs, N., Hossain-McKenzie, S., and Vugrin, E. (2018). Measurement and analysis of cyber resilience for control systems: An illustrative example. In *2018 Resilience Week (RWS)*, pages 38–46.
- Kott, A. and Linkov, I. (eds.) (2019). *Cyber Resilience of Systems and Networks*. Springer.
- McDonald, J. (2007). Substation automation basics - the next generation. <https://electricenergyonline.com/energy/magazine/321/article/Substation-Automation-Basics-The-Next-Generation.htm>.
- Mottahedi, A., Sereshki, F., Ataei, M., Qarahasanlou, A. N., and Barabadi, A. (2021). Resilience estimation of critical infrastructure systems: Application of expert judgment. *Reliability Engineering System Safety*, 215:107849.
- National Cyber Security Centre (NCSC). Vendor security assessment: Assessing the security of network equipment.
- Nygård, A. R. and Katsikas, S. (2022). Sok: Combating threats in the digital supply chain. In *Proceedings*

- of the 17th International Conference on Availability, Reliability and Security, ARES '22, New York, NY, USA. Association for Computing Machinery.
- Nygård, A. R., Sharma, A., and Katsikas, S. (2022). Reverse engineering for thwarting digital supply chain attacks in critical infrastructures: Ethical considerations. In *Proceedings of the 19th International Conference on Security and Cryptography - SECRYPT*, pages 461–468. INSTICC, SciTePress.
- Rath, M. and Tomar, A. (2021). Chapter 7 - smart grid modernization using internet of things technology. In Tomar, A. and Kandari, R., editors, *Advances in Smart Grid Power System*, pages 191–212. Academic Press.
- Sperstad, I. B., Kjølle, G. H., and Gjerde, O. (2020). A comprehensive framework for vulnerability analysis of extraordinary events in power systems. *Reliability Engineering System Safety*, 196:106788.
- United States Senate Republican Policy Committee (2016). Infrastructure Cybersecurity: The U.S. Electric Grid. <https://www.rpc.senate.gov/policy-papers/infrastructure-cybersecurity-the-us-electric-grid>.
- U.S. Department of Commerce and U.S. Department of Homeland Security. Assessment of the critical supply chains supporting the u.s. ict industry.
- Witteman, M. and Goncharov, K. (2023). Marc witteman on the roots of riscure, device security, and pre-silicon. <https://www.riscure.com/security-highlight-marc-witteman-on-the-roots-of-riscure-device-security-and-pre-silicon/>.
- Yuce, B., Schaumont, P., and Witteman, M. (2018). Fault attacks on secure embedded software: Threats, design, and evaluation. *Journal of Hardware and Systems Security*, 2(2):111–130.
- Zio, E. (2016). Critical infrastructures vulnerability and risk analysis. *European Journal of Security Research*, 1:97–114.