Toward an Intrusion-Tolerant Power Grid: Challenges and Opportunities

Amy Babay, John Schultz, Thomas Tantillo, Yair Amir
Johns Hopkins University — {babay, tantillo, yairamir}@cs.jhu.edu
Spread Concepts LLC — {jschultz, yairamir}@spreadconcepts.com

***Abstract*—While cyberattacks pose a relatively new challenge for power grid control systems, commercial cloud systems have needed to address similar threats for many years. However, technology and approaches developed for cloud systems do not necessarily transfer directly to the power grid, due to important differences between the two domains. We discuss our experience adapting intrusion-tolerant cloud technologies to the power domain and describe the challenges we have encountered and potential directions for overcoming those obstacles.**

I. Introduction

New threats facing the power grid pose a major challenge today. Power grid control systems were never designed to operate in hostile environments: they have traditionally used specialized networks that were "air-gapped" and inaccessible to attackers. As Supervisory Control and Data Acquisition (SCADA) systems for the power grid move to use IP networks to take advantage of their cost benefits and ubiquity, the "air-gap" assumption no longer holds, and these systems are becoming increasingly exposed to malicious attacks.

While cyberattacks pose a relatively new challenge for power grid control systems, commercial cloud systems have needed to address similar threats for many years. Systems running on the Internet today are constantly exposed to attacks and have developed security and resilience techniques that allow them to operate effectively in this open and often hostile environment. Therefore, there is an opportunity to leverage knowledge developed in the cloud domain to improve the security of power grid systems and make them resilient to sophisticated attacks and compromises.

However, our experience shows that technology and approaches developed for cloud systems do not necessarily transfer directly to the power grid, due to important differences between the two domains. Compared with cloud systems, SCADA systems for the power grid represent higher value targets and are more likely to be subjected to nation-state-level attacks. Cyberattacks on SCADA systems can severely damage physical grid infrastructure, disabling power generation or transmission and requiring extensive repairs. Therefore, SCADA systems have considerably higher resilience requirements than most commercial cloud systems. While cloud systems generally employ strong security and fault-tolerance, it is crucial for SCADA systems to remain operational even under sophisticated attacks that succeed in compromising part of the system (i.e. to be intrusion tolerant).

As we discuss in Section II-A, state-of-the-art research in building intrusion-tolerant systems can help SCADA systems reach the required level of resilience. However, deploying such technologies in practice presents another considerable challenge. SCADA systems have evolved over decades to meet the monitoring and control needs of power companies and are generally complex systems with many components, where control logic is distributed across many individual control units, each responsible for one part of the overall system. Due to the paramount importance of reliability in power grid control, introducing changes in these established and complex systems is difficult.

In Section II-B, we discuss directions for introducing new intrusion-tolerant capabilities into SCADA systems through open-source software and incremental deployment. However, a truly resilient power grid requires that every power utility deployment is secure and intrusion tolerant. The highly interconnected nature of the grid enables it to effectively mask failures by rerouting power, but it also allows a failure or attack in one segment of the grid to have cascading effects throughout the system. Therefore, the resilience of the grid is determined by the strength of its weakest links: an attacker who manages to compromise a few strategic utility deployments can cause grid-wide damage and blackouts.

To address this problem, we propose a service provider model, in which the expertise required to deploy and manage intrusion-tolerant monitoring and control systems and fend off nation-state attackers is offered by a few specialized providers that can serve many power utilities, rather than requiring each utility to develop and continuously maintain that expertise independently.

Compounding the above problems, power grid systems are much more dynamic than in the past, with new capabilities (e.g. smart grid) being developed that bring new attack vectors with them. Thus, the challenge is not only to make the existing systems secure and resilient but also to ensure that new additions to the systems do not degrade those qualities.

Making intrusion-tolerant SCADA a reality requires overcoming significant obstacles and bridging the wide gap that exists today between the knowledge required to run power-grid control systems and the knowledge required to run intrusion-tolerant systems that can withstand nation-state-level attackers. Therefore, we believe that this effort will require a partnership between government, industry associations, power companies, and the research community.

II. Challenges and Opportunities

We present four key challenges on the path to an intrusion-tolerant power grid and discuss opportunities for addressing these challenges.

A. Challenge 1: High-value systems require extreme resilience

Power grids are crucial to most aspects of modern life. Extended outages put lives at risk as water and sanitation systems, refrigeration and climate control, communications, healthcare, transport, trade, public safety, and more, all critically depend on a reliable supply of power. Because power is so fundamental to life today, these systems are high-value targets for attack. At the extreme, in warfare, disabling an enemy's power grid degrades their ability to respond and forces them to simultaneously handle a large scale civilian crisis. The opening salvos in future wars are likely to be cyberattacks on critical infrastructure such as the power grid. Nation-state actors with the motives, means, time, and expertise to execute such attacks are already probing and penetrating these systems. It is imperative that these systems be quickly hardened to be resilient to malicious attacks.

Attacks on the power grid can severely impact tens of millions to hundreds of millions of people. A single electric utility typically serves a sizable geographic area, often centered around a populous city, meaning that a successful attack on just one utility can affect millions of people. For example, Consolidated Edison in New York City serves the needs of nearly ten million people. This scale makes large utilities attractive targets for attackers. Worse, an attack on one utility can become a far larger, regional problem because utilities are interconnected through the power grid.

The power grid provides resilience to local failures as neighboring utilities will automatically and immediately raise their own generation and transmission to help meet any power shortfalls. However, this interdependence creates the possibility of large regional outages when failures cascade and utilities do not react strongly and quickly enough in concert. For example, the Northeast Blackout of 2003 originated locally in Ohio but cascaded to affect more than 50 million people throughout northeastern America [1]. The largest blackout in history occurred in 2012 in northern India when a cascade of failures cut off power for more than 600 million people [2]. Power grids likely have weak points that can be exploited by sophisticated attackers to cause a small set of failures to be magnified into destabilizing an entire power grid. Cambridge University recently analyzed a plausible scenario where a coordinated cyberattack on 50 generators in the northeastern United States could cause a cascade that would cut off power for nearly 100 million people for days to weeks with an economic impact ranging from $243B up to $1T [3]. To ensure that power grids are systemically protected, grid operations at every utility will need to become extremely resilient to attack – otherwise they risk becoming the weakest link in the chain that breaks.

More and more, power grid control systems, and Industrial Control Systems (ICS) in general, are becoming connected to the Internet. This opens them up to attack scenarios for which they were never designed. Most such systems were originally deployed on closed, private networks that were "air gapped" and had no control connections to exterior networks. Because of this assumption, most of these systems and the protocols they use have little internal security, as they were designed to run in a trusted, private environment. As the air gap disappears and IP networks make it possible to reach these systems from anywhere, the lack of internal security leaves these systems dangerously exposed to attack.

Today, most ICS security is devoted to perimeter defense to keep attackers out and ensure they cannot penetrate the internal, trusted network environment. Perimeter defense is necessary, but it is no longer sufficient. This fact has been demonstrated repeatedly in experiments and in several real-world attacks where ICS perimeter defenses have been penetrated. Stuxnet demonstrated that even a true air gap is not enough to keep out a malicious attack and that ICS internal security – even in a nation's nuclear development program – is weak [4]. The Dragonfly/Energetic Bear espionage attacks targeting the energy industry in North America and Turkey are estimated to have penetrated some 2,000 ICS sites and are surging again [5]. The Sandworm hacker team built the Black-energy toolkit variants that were specific to SCADA systems and their Human Machine Interface (HMI) components. This team successfully penetrated the Ukrainian power grid in late 2015 and shut down multiple substations, cutting off power to over 225,000 customers [6]. In late 2016, the Crashoverride attack again targeted the Ukrainian power grid and succeeded in shutting down a single substation [7]. It is believed that this attack was just a proof-of-concept that demonstrated even further developed tradecraft over previous attacks targeting the power grid.

Research-Based Intrusion-Tolerant Solutions. These real-world examples demonstrate that perimeter defense and IT best practices are not enough to protect power grid systems. Our recent work has shown, however, that a more comprehensive defense-in-depth approach employing strong network security practices and state-of-the-art intrusion tolerance techniques can considerably improve the resilience of SCADA systems.

To advance the goal of an intrusion-tolerant power grid, we have developed Spire, an intrusion-tolerant SCADA system [8]. Spire leverages intrusion-tolerant technologies originally developed to support monitoring and control of global clouds, including the Spines intrusion-tolerant network [9] and the Prime intrusion-tolerant replication engine [10]. Spire overcomes sucessful system-level compromises of SCADA control servers by replicating the SCADA master using Prime. At the network-level, Spire uses Spines to provide authenticated, encrypted, and resilient communication between the system components. A proxy connects the existing Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs), used for controlling physical equipment, to the system and limits their network attack surface. The typical, insecure industrial communication protocols used by PLCs, such as Modbus or DNP3, are used only on the direct connection between the PLC

and its proxy, which, ideally, can simply be an Ethernet cable. HMI communications are similarly terminated and protected behind a secure proxy. The rest of the communication in the system occurs over Spines.

In April 2017, Spire went through a red-team experiment at Pacific Northwest National Laboratory (PNNL), as part of a DoD Environmental Security Technology Certification Program (ESTCP) project led by Resurgo LLC. A hacker team from Sandia National Laboratories attacked both a commercial SCADA system and Spire. The results were surprising: the Sandia team obliterated the commercial system within a couple of hours, but was unable to affect Spire's operation over the allocated three days. On the third day of the experiment, the red team was given full control of one of Spire's SCADA master replicas (a situation the intrusion-tolerant replication protocol is designed to overcome) and access to the relevant source code, but they were still unable to disrupt the system.

While this does not mean that given more time, the Sandia experts would not have been able to cause damage in the Spire system, it demonstrates that there is a significant difference between current industry best practices and a research-based solution designed to withstand sophisticated system and network attacks. Critical infrastructure is currently vulnerable to attack, but our experience with Spire shows that there is an opportunity to improve the resilience of the power grid by applying research on secure and intrusion-tolerant systems.

B. Challenge 2: Established systems can be difficult to change

As part of an established industry, where systems can stay in service for decades and must meet strict reliability requirements, SCADA systems can be difficult to change. Intrusion-tolerant technology (like Spire) has the potential to significantly improve the resilience of power grid control systems, but the disruptive change it brings presents an obstacle for deployment.

Power companies today recognize the importance of securing their SCADA systems and are interested in solutions that will make them resilient to attacks and compromises, but the ability to receive support from established vendors is a major concern. Sacrificing current system stability to take advantage of potential improvements in attack resilience is not acceptable. Thus, if SCADA vendors do not support intrusion-tolerant SCADA systems, it will be difficult for power companies to deploy such solutions on their own.

Our past experience indicates that major SCADA providers are unlikely to introduce dramatic changes in their offerings without regulatory pressure. Working with a large commercial SCADA provider, an earlier version of the Prime intrusion-tolerant replication engine [11] was integrated into a commercial SCADA product to create a prototype intrusion-tolerant SCADA system for electricity transmission and distribution. While a description of the effort was published [12], the prototype was never made available: the company decided not to offer it commercially, and because it was proprietary, the source code could not be used for education or further research.

Open-Source Ecosystem. Open-source software provides an opportunity to educate the power industry, including power companies, SCADA vendors, industry associations and regulatory agencies, about the solutions that are possible and to prove that new technology is effective. Developing open-source SCADA solutions enables engagement with early adopters in the power industry who are willing to test innovative ideas, provide feedback, and ultimately consider them for deployment. Interacting with the power industry can in turn educate the research community about the specific requirements of power grid systems. Moreover, by demonstrating that secure and intrusion-tolerant SCADA systems can be made practical, we can spur regulators to strengthen their requirements for the resilience of commercial SCADA systems.

A robust open-source SCADA ecosystem is developing, making such an approach feasible. For example, pvbrowser [13], Proview [14], Tango Controls [15], and other open-source SCADA systems are maturing and have begun to be used in practice. OpenPLC [16] enables innovation in PLC software, and opens up the ability to test new ideas at all levels of the SCADA system in a lab setting with or without real PLC hardware. The Grid Solutions Framework [17] provides a collection of libraries for a variety of power utility applications.

Our contribution to the open-source SCADA ecosystem, Spire, provides an intrusion-tolerant SCADA system that includes a SCADA master implemented from the ground up with intrusion tolerance as a core design principle, a PLC/RTU proxy that isolates the PLC (and its insecure communication protocols, such as Modbus or DNP3) from the rest of the network, and pvbrowser-based HMI. Spire uses the open-source Spines intrusion-tolerant network [9] as its communication bus and the Prime intrusion-tolerant replication engine [10] to replicate the SCADA Master's state. We use OpenPLC for PLC emulation in development.

While complete open-source SCADA systems are useful tools in educating the power industry and regulators, widespread adoption of such solutions by power companies will take a lot of time and effort. As an intermediate step toward an intrusion-tolerant power grid, we propose exploring partial solutions that can improve security and resilience without replacing the entire control system.

Proxy-Based Approach. We envision a proxy-based approach, where the network between SCADA components can be made secure and intrusion-tolerant by connecting each component to a proxy. The proxies communicate through the Spines intrusion-tolerant network and sit directly next to the components they protect. We believe that such proxies can be supported by small-form computers such as the Nexx WT3020 [18] or Raspberry Pi [19]. While such a solution will not provide full intrusion tolerance (it will not overcome compromises of the system components), it will substantially enhance the overall resistance of the system to intrusions and can be practical for near-term deployment.

C. Challenge 3: Extreme resilience requires specialized expertise, exposing knowledge gap

As discussed in Section II-A, the interconnected nature of the grid means that the resilience of the grid as a whole may depend on the strength of its weakest links. Therefore, realizing an intrusion-tolerant power grid requires a systemic approach that ensures that all power installations throughout the grid are made resilient to intrusions.

Our experience with the red-team experiment described in Section II-A shows that effectively defending the grid requires expertise comparable to that of nation-state attackers. Today there is a serious knowledge gap: the specialized knowledge required to deploy power grid systems capable of fending off nation-state attackers is difficult to develop and maintain. In fact, as discussed in Section II-A, solutions are still in the realm of research. It is not feasible to expect all power installations (e.g. approximately 3200 installations across the United States) to independently develop this expertise and maintain it over time.

Taking inspiration from the cloud domain, a service-provider model offers the opportunity to develop specialized expertise and improve resilience for many power installations simultaneously by consolidating their management. In this model, power companies can outsource the management of their SCADA infrastructure to a specialized service provider and focus on their core expertise of running the grid itself. In turn, the service provider can invest significant resources to provide intrusion tolerance and resilient power grid management to many power installations. However, it is not straightforward for a service provider to completely take over SCADA system management, as each power installation is customized and fairly complex.

(Hybrid) Service-Provider Approach. This calls for a hybrid approach. We envision a service provider running an intrusion-tolerant state maintenance service that serves many power companies (each with their own instances), and individual power companies customizing their system endpoints (HMIs, PLCs, RTUs) and specifying their own state and message formats. The exact approach and division of responsibilities is an open question. At one extreme, the service provider offers only the core intrusion-tolerant SCADA software (which will be customized for each power installation) and provides consulting to help deploy it in the power companies. Alternatively, a service provider could be fully responsible for managing and running the SCADA infrastructure; this might include providing the state maintenance service, as well as remotely managing networks and SCADA components within power plants. This allows power companies to fully leverage the service provider's security and intrusion-tolerance expertise. In this case, the power company is responsible for the initial configuration and customization of the system for its specific environment and for operating the power system (using the SCADA system for monitoring and control). However, allowing remote management of system components that are not currently accessible from outside a power plant may introduce more risk, leading to an approach somewhere between these two extremes.

Cloud-Based SCADA. For wide-area SCADA systems responsible for monitoring and controlling multiple power substations, current research indicates that a cloud-based service provider approach can enable greater resilience to network attacks. Our work has shown that to withstand sophisticated network attacks that can isolate a targeted site from the rest of the network, the SCADA control servers should be replicated across multiple sites [20]. Using this approach, the system can be made to withstand the isolation of any single site (e.g. a control center) by using at least three total sites. However, constructing three control centers with full capabilities for controlling PLCs or RTUs in the field can be cost-prohibitive for power companies. By using commodity data centers to host some or even all of the replicas, this higher level of resilience can be made practical [21], [20].

However, allowing a service provider to manage SCADA infrastructure in data centers raises privacy concerns, as power companies may want to prevent sensitive information about the grid from reaching commodity data centers (e.g. due to concerns about unauthorized access in data centers serving many users). For example, one particularly sensitive type of information may be the locations and IP addresses of the PLCs and RTUs in the field (or of proxies that connect them to the monitoring and control network): keeping this information private makes it more difficult for an attacker to communicate with the field devices to potentially send them malicious commands.

To address these concerns, we propose abstracting the state exposed to the data centers. For example, to avoid revealing physical locations and IP addresses of field devices, we can assign each device a logical address, and the SCADA system can operate on these logical addresses [22].

In a mixed system where only some of the SCADA master replicas are hosted in data centers and the rest are hosted in control centers managed by the power companies, translation between physical and logical addresses can be done by the control-center replicas that need to communicate with the PLCs and RTUs.

A fully cloud-based architecture, in which all SCADA master replicas are hosted in data centers, is also possible. Such an architecture simplifies deployment and maintenance for the power company, as it does not need to manage any of the intrusion-tolerant replication infrastructure. In this model, power company control centers would not contain any SCADA master replicas but would host simple translation units that convert between physical and logical addresses when receiving updates from PLC/RTU proxies or sending them commands.

It may be useful for utility companies to abstract additional information, beyond physical addresses. To do this, the translation functions used by control-center SCADA masters or translation units can be made more sophisticated. Data-center SCADA masters would operate solely on abstract state and abstract operations (updates), using functions that take abstract operations as input and generate correct abstract responses,

without being able to understand the real meaning of those operations on the system. Such functions could be similar in nature to homomorphic encryption techniques that allow computation on encrypted data (e.g. [23], [24]).

These cloud-based SCADA architectures represent initial thoughts on how to effectively deploy intrusion-tolerant SCADA for a large number of distinct power installations. Based on the market size of the power industry, a "SCADA as a service" cloud-based approach will likely lead to a few competing providers, as in the cloud domain. Current SCADA manufacturers may be good candidates for providing such a service, but current cloud service providers or even new startups may fill this role as well. While the right architecture, organizational structure, and associated division of responsibilities for solving this problem is not yet clear, these ideas are meant to invite discussion and provide a starting point for further research and the development of new approaches.

D. Challenge 4: Evolving systems require dynamic defenses

In Sections II-A through II-C, we described challenges in securing today's power grid and discussed directions for making its control systems resilient to attacks and even intrusions. However, the power grid is undergoing a significant evolution, with new technologies fundamentally changing its control and communication structure.

In particular, smart grid technologies makes the power grid more intelligent by adding more communication and fine grained control, and decentralizing power production, distribution, and automatic decision making. For example, more customers are installing solar panels and energy storage systems and providing their excess power to the grid. Allowing these additional and new kinds of inputs and controls into the power grid opens up new kinds of security threats, creating a much larger attack surface.

As homes and businesses become nodes in a decentralized power network, with controllers capable of interacting and communicating with the grid, they also become potentially exploitable targets. Similar to computers on the Internet, these nodes can be manipulated or even taken control of by remote attackers through lack of appropriate security mechanisms or through exploitable bugs in their software.

Consider a computer worm spreading through the communications network of a smart grid creating a "botnet" of power customers. An attacker in control of such a botnet would be able to mount novel attacks on the system. For example, the attacker could turn off the consumption of all infected customers in a widespread denial-of-service attack. More subtly, they could target specific, high-value customers and disrupt their power service at sensitive times. To stress and potentially damage the system, the attacker could cycle the power consumption of a large number of customers in a tightly coordinated manner, causing huge spikes and troughs of demand. They might even be able to force decentralized power producers to produce power out-of-phase with the grid, possibly desynchronizing it, causing blackouts and even physical damage to equipment locally and remotely. The attacker could also lie and inject invalid information into the system, possibly causing incorrect and harmful decisions to be made. Many different kinds of attacks could be invented, but what makes these attacks novel is that the communications network that interconnects the controllers makes it possible for a very large group of them to be remotely manipulated and tightly coordinated.

Secure and Resilient Design. To address these new kinds of threats, security must be a paramount concern in the development and deployment of smart grids. Unlike existing SCADA systems, which were designed to operate in isolated trusted environments and are now facing a security crisis, new system components must be designed to operate in an open and hostile environment. The hardware and software of the controllers should be secured through mechanisms such as Trusted Platform Module (TPM) and Secure Boot, which try to ensure that only software digitally signed by a trusted authority is ever allowed to run. The controllers should be tightly locked down to only perform necessary functions to minimize their attack surface. The network communications within the smart grid must be strongly authenticated and protected through state-of-the-art, strong cryptographic protocols. Communications should potentially even be made resilient to the point of intrusion tolerance using an approach like the Spines intrusion-tolerant network protocols (see Section II-A). If security is left as a secondary feature or a later add-on, these systems are likely to be exploited.

Collaborative Ecosystem, Leveraging Lessons from the Cloud. Ensuring that smart grid architectures are designed with the necessary security and resilience measures in place requires collaboration between researchers, regulators, power companies, and vendors. Moreover, even if smart-grid controllers are designed and deployed with all of the necessary protections, over time, new bugs and holes will be found, new attacks will be developed, and patches and updates will need to be deployed. Maintaining the resilience of the power grid as new technologies are developed and new vulnerabilities are discovered requires a rich ecosystem supporting ongoing collaboration. The dynamic nature of emerging smart grid architectures and the threats they face suggest that models and lessons from the cloud domain may be valuable here as well.

For example, as discussed in Section II-B, open-source software can help create the necessary ecosystem of collaboration by providing a concrete starting point for discussions between the relevant parties, allowing them to learn about possible solutions, experiment and test their effectiveness, and discuss how they can be improved. As in the cloud domain, a mature open-source ecosystem can also enable faster innovation, drawing on community expertise to develop support for new technologies and protection against new threats.

Moreover, as discussed in Section II-C, taking inspiration from the cloud service-provider model to create dedicated service providers that manage systems for many individual utilities can help provide a more consistent and timely process for addressing new security threats. Rather than each utility needing to maintain the expertise to learn about new threats

and independently develop its own solutions, a few specialized providers can invest the resources necessary to create solutions that can immediately benefit many utilities simultaneously.

This kind of open ecosystem will require a major cultural change from the current power industry model of a few large vendors providing closed-source products. Some may argue that increased openness and the availability of open-source software will provide an advantage for attackers, by allowing them to learn about the systems in operation and discover vulnerabilities to exploit. However, in the current environment, systems are available in the commercial market, and although the source code is typically not provided, this does not pose a large barrier for a sophisticated attacker who can analyze the available executables. Moreover, security-by-obscurity does not provide strong protection over time. In fact, open-source software can become more secure than commercial software over time, as many people can analyze it to find and fix security flaws. Therefore, we contend that the advantages of an open environment considerably outweigh the disadvantages in the emerging dynamic environment.

III. Conclusion

We have presented several challenges on the path toward an intrusion-tolerant power grid and suggested opportunities for leveraging technologies and models from the cloud domain to improve the security and resilience of current and future power grid control systems. While cloud technologies cannot be directly applied to solve power grid problems in all cases, we have proposed intermediate or hybrid solutions and believe that an open collaborative ecosystem with a partnership between power companies, industry associations, vendors, government, and the research community can combine expertise from the power and cloud domains to facilitate the necessary innovations.

Acknowledgment

We thank Kevin Jordan for inspiring us to work on intrusion-tolerant SCADA systems for the power grid and for leading the DoD ESTCP project, together with Dianne Jordan, Eamon Jordan, Kevin Ruddell, and the rest of the Resurgo LLC team. We thank Trevor Aron, Samuel Beckley, and Marco Platania from the Johns Hopkins University Distributed Systems and Networks Lab for their work toward intrusion-tolerant open-source SCADA. We thank David Rolla, Brian Tepper, John Tica, Keith Webster, and the rest of the team at the Hawaiian Electric Company for teaching us about real power systems, providing feedback, and working with us to experiment with far-reaching ideas in actual power environments. We thank Jonathan Stanton from Spread Concepts LLC for providing guidance on state-of-the-art cloud networking setup in the wild. We thank Michal Miskin-Amir from Spread Concepts LLC for her key role in making the ESTCP project a successful collaboration.

This work was supported in part by DoD Environmental Security Technology Certification Program Project (ESTCP) EW-201607 to Resurgo LLC.

References

[1] U.S.-Canada Power System Outage Taskforce, "Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations," https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf, retrieved February 9, 2018.

[2] J. Yardley and G. Harris, "2nd day of power failures cripples wide swath of india," http://www.nytimes.com/2012/08/01/world/asia/power-outages-hit-600-million-in-india.html, retrieved February 9, 2018.

[3] Lloyd's of London, Cambridge Centre for Risk Studies, "Business blackout," https://www.lloyds.com/news-and-risk-insight/risk-reports/library/society-and-security/business-blackout, retrieved February 9, 2018.

[4] D. Kushner, "The real story of stuxnet," https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet, retrieved February 9, 2018.

[5] Symantec Inc., "Dragonfly: Western energy sector targeted by sophisticated attack group," https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks, retrieved February 9, 2018.

[6] Electricity Information Sharing and Analysis Center, "Analysis of the cyber attack on the ukrainian power grid," http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf, retrieved February 9, 2018.

[7] Dragos Inc., "Crashoverride analysis of the threat to electric grid operations," https://dragos.com/blog/crashoverride/CrashOverride-01.pdf, retrieved February 9, 2018.

[8] Johns Hopkins Distributed Systems and Networks Lab, "Spire: Intrusion-tolerant SCADA for the power grid," http://www.dsn.jhu.edu/spire, retrieved February 12, 2018.

[9] ——, "The Spines messaging system," http://www.spines.org, retrieved February 12, 2018.

[10] ——, "Prime: Byzantine replication under attack," http://www.dsn.jhu.edu/prime, retrieved February 12, 2018.

[11] Y. Amir, B. Coan, J. Kirsch, and J. Lane, "Prime: Byzantine replication under attack," *IEEE Trans. Dependable and Secure Computing*, vol. 8, no. 4, pp. 564–577, July 2011.

[12] J. Kirsch, S. Goose, Y. Amir, D. Wei, and P. Skare, "Survivable SCADA via intrusion-tolerant replication," *IEEE Trans. Smart Grid*, vol. 5, no. 1, pp. 60–70, Jan 2014.

[13] "pvbrowser. Simple process visualization," http://pvbrowser.de/pvbrowser/index.php, retrieved February 12, 2018.

[14] "Proview - open source process control," http://www.proview.se/v3/, retrieved February 12, 2018.

[15] "Tango controls," http://www.tango-controls.org/, retrieved February 12, 2018.

[16] T. Alves, "The OpenPLC project," http://www.openplcproject.com/, retrieved February 12, 2018.

[17] "Grid solutions framework," https://github.com/GridProtectionAlliance/gsf, retrieved February 12, 2018.

[18] "Nexx WT3020," OpenWRT Wiki https://wiki.openwrt.org/toh/nexx/wt3020, retrieved February 12, 2018.

[19] "Raspberry pi - teach, learn, and make with raspberry pi," https://www.raspberrypi.org/, retrieved April 16, 2018.

[20] A. Babay, T. Tantillo, T. Aron, M. Platania, and Y. Amir, "Network-attack-resilient intrusion-tolerant SCADA for the power grid," in *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, June 2018.

[21] Y. Amir, A. Babay, and T. Tantillo, "Network-attack-resilient intrusion-tolerant SCADA architecture," Patent PCT/US17/38 565, June, 2017.

[22] ——, "Systems and methods for cloud-based control and data acquisition with abstract state," Patent PCT/US18/15 451, January, 2018.

[23] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing*, ser. STOC '09. New York, NY, USA: ACM, 2009, pp. 169–178. [Online]. Available: http://doi.acm.org/10.1145/1536414.1536440

[24] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?" in *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop*, ser. CCSW '11. New York, NY, USA: ACM, 2011, pp. 113–124. [Online]. Available: http://doi.acm.org/10.1145/2046660.2046682