From NIST to Next-Gen: Advancing Smart Grid Cybersecurity for a Sustainable Future

Audheya Mannepalli | PUBP 6727 | 11/21/2024

Acknowledgment

I would like to thank the professors and TAs of the Cybersecurity Practicum course for their ongoing feedback and support throughout the class. The positive and constructive feedback that I received was very valuable and has helped me craft a detailed, more nuanced, and more organized paper. Additionally, I would like to thank my group mates for their invaluable contributions during peer feedback sessions. Their insightful suggestions, helpful resources and contacts, and constructive criticism were instrumental in refining my arguments and strengthening the overall quality of my paper.

Table of Contents

Introduction

The smart grid represents a transformative shift in the energy sector, analogous to the evolution from rotary phones to smartphones. It's a leap from traditional, mechanical infrastructure to interconnected digital technologies, enhancing efficiency reliability, and sustainability. Central to this transformation is the replacement of mechanical meters with "smart meters". These digital meters, equipped with software and communication capabilities, can transmit energy consumption data back to the utility company. It's akin to having a constant, two-way conversation between your home and the power company, enabling remote meter reading, outage detection, and even demand response programs [1].

This modernization also involves a complex integration of diverse elements, including renewable energy sources (like solar and wind power plants), smart homes and commercial buildings, smart transport systems, and various types of power plants. This interconnectedness allows for two-way communication between energy providers and consumers, enabling the grid to dynamically adjust to supply and demand, much like a conversation. It leverages data-driven insights, gathered from grid components to optimize energy usage, reduce waste, and make informed decisions [3], [8], [9].

What is the Problem?

However, this increased connectivity also introduces significant cybersecurity risks. Like connecting your laptop to public Wi-Fi at a coffee shop, the smart grid's reliance on interconnected devices, communication networks, and data exchange creates vulnerabilities that malicious actors can exploit. This expansion of the attack surface and the increasing sophistication of cyberattacks raises concerns about data breaches, grid disruptions, and even physical damage to critical infrastructure. The potential consequences are far-reaching, and they include:

1) Disruptions: Cyberattacks can cause widespread power outages, impacting critical infrastructure and public safety [2].
2) Data Breaches: Sensitive customer information, operational data, and trade secrets can be exposed [3].
3) Financial Losses: Energy theft, billing fraud, and ransomware attacks can lead to significant financial losses for both utilities and customers

4) Physical Damage: The compromise of critical grid components can lead to catastrophic equipment failures and safety hazards, potentially endangering lives and causing environmental damage [4].

Further complicating the cybersecurity landscape is the rapid integration of emerging technologies:

1. The Internet of Things (IoT): The proliferation of IoT devices within the grid, from smart meters to household appliances, expands the attack surface exponentially. Even seemingly innocuous devices like smart refrigerators and thermostats can become entry points for malicious actors if not adequately secured.
2. Advanced Metering Infrastructure (AMI), Advanced Distribution Management Systems (ADMS), and Distributed Energy Resources (DER): These technologies, while crucial for grid modernization, add layers of complexity and require even more robust cybersecurity measures to ensure their secure integration and operation [1].
3. Cloud Computing: The adoption of cloud-based systems for data storage and processing offers advantages such as scalability and cost-effectiveness. However, it also harbors risks of misconfigurations, data breaches, and service interruptions that can compromise grid reliability and data integrity [1].

Many different stakeholders and works of literature express concerns about these regulatory framework gaps, in addition to the everchanging cybersecurity landscape and the necessity to constantly "keep up" with cyber threats. For example, technology vendors like Siemens and General Electric desire clear and well-defined security requirements to facilitate seamless integration into smart grid environments. [5]. Larger utility companies like Duke Energy have expressed concerns about adapting to rapid technological changes and keeping up with the evolving threat landscape and would like more specific and practical guidance that is customized to their complex environments. [1].

To tackle these challenges head-on, the industry is actively taking steps to enhance smart grid cybersecurity. Utilities are partnering with specialized vendors and implementing secure communication protocols and tokenization systems to enhance protection at the meter level. The ongoing shift to cloud-based systems, with projects undertaken by consulting firms like Accenture, highlights the commitment to enhance security and resilience, [1]. The focus on limiting access and privilege, coupled with the ongoing integration of emerging technologies, emphasizes the dynamic nature of the smart grid and the continuous need for adapting security strategies.

Despite these efforts, there are still gaps that remain within existing cybersecurity frameworks. The core problem that this document will cover, lies in the limitations of the NIST Smart Grid Cybersecurity Framework, which is officially titled, the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0. For conciseness, this will be referred to as the 'NIST Framework' in this document. While this framework provides a very valuable foundation, it presently does not fully address the unique and ever-evolving challenges posed by the smart grid. These gaps include inadequate guidance on securing IoT devices, ensuring data privacy, managing supply chain risks, and mitigating advanced persistent threats (APTs). The rising costs of cybercrime globally further highlight the importance of more robust cybersecurity measures to be implemented within the smart grid context [1].

What is the Solution?

To address these critical gaps, this project proposes a three-part solution:

1. **Deliverable 1:** Conduct a robust gap analysis of the NIST Framework to identify the specific discrepancies between the framework and the unique challenges the smart grid faces today, zoning into specific emerging technology threats, such as the Internet of Things.
2. **Deliverable 2:** Craft additions to the NIST Framework that integrate advanced technologies to mitigate the identified risks. This will be in the tabular format in the current NIST Framework, with an added 'solution' column that delves into implementable solutions.
3. **Deliverable 3:** Develop a 'Smart Grid Cybersecurity Playbook', which is a set of actionable recommendations, in the format of a checklist. This includes best practice mitigation strategies and a practical guide for stakeholders which promotes the implementation of proactive defense strategies to enhance the resilience and security of the smart grid.

Gap Analysis

The gap analysis will use a combined-method approach to analyze and enhance smart grid cybersecurity. It begins with a literature review to establish a foundational understanding of current challenges and best practices in cybersecurity. Then, it will involve a thorough review of the framework, an in-depth assessment of existing and emerging threats as well as an identification of discrepancies between the current framework's recommendations and the threat landscape. The identified gaps are then documented and expanded upon. Stakeholder

engagement involves thorough interviews to gather in-depth perspectives on cybersecurity needs and priorities, specifically with an expert who works in the energy industry and has had hands-on experience with smart grid cybersecurity. Further, based on these findings, additions to the framework and a smart grid cybersecurity playbook will be crafted (deliverable 2 and deliverable 3, respectively).

Gap 1: New Technologies Come with New Risks

- The current NIST Framework does an excellent job with general cybersecurity advice, and briefly touches on some protocols for emerging technologies. But presently, there is still not enough detail on some of the new threats that are present in the current smart grid threat landscape. For example, the NIST framework can be enhanced if further instructions on IoT threats are incorporated. Clearer instructions on how to lock down IoT devices and ensuring that data is safe in the cloud are paramount for securing the smart grid. Specifically, the gaps regarding the instructions on IoT devices are [7].:
    - Secure Firmware & Software Updates: IoT devices often lack robust mechanisms for secure firmware and software updates, and this makes them easier to hack. The NIST Framework needs to incorporate the importance of updating these mechanisms, such as code signing, secure boot processes, and integrity checks
    - Real-Time Threat Detection & Response: The ever-changing nature of the smart grid requires real-time threat detection and response capabilities to address potential attacks on IoT sensors and communication networks. The framework needs to have instructions/recommendations on how to implement advanced threat detection and response solutions that are specific to IoT devices in the smart grid.

Gap 2: Privacy Matters

- The NIST Framework currently talks about keeping data safe/hidden/inaccessible from bad actors, but it can be perceived as a bit vague. The privacy considerations are broad and may not completely capture the nuances of smart grid data, which typically includes highly granular, time-series information about energy consumption patterns. Smart grids collect an ample amount of personal and operational data, thus, smart grid cybersecurity frameworks need clearer guidelines on how exactly to keep that information anonymous, and 'who gets to see what'. And because there is

'privacy-enhancing tech' out there, enhanced framework recommendations can point us towards those solutions. Specifically, the gaps regarding privacy matters are:

- Data Anonymization: The framework presently mentions the potential for high-frequency energy usage data to inadvertently reveal private information. However, there is no clear guidance on how to effectively anonymize and de-identify this data while maintaining its utility for grid management purposes. The framework needs to incorporate specific techniques for data anonymization and de-identification.
- Third-Party Access and Data Sharing: The framework could benefit from more explicit guidelines on data sharing and access controls in the smart grid ecosystem. The framework needs to address the importance of clear data-sharing agreements, robust access controls, and transparency mechanisms.

Gap 3: Supply Chain Issues

- Although the NIST Framework briefly mentions supply chain risks, it could benefit from delving more into how to deal with them. It could be beneficial to have specific strategies for ensuring that the equipment and software used in the smart grid are trustworthy and haven't been tampered with. The current framework, as highlighted by the control family ID.SC primarily focuses on establishing risk management processes, assessing suppliers, and incorporating security requirements into agreements. Specifically, the gaps regarding supply chain issues are:
  - Limited Scope of Supplier Assessments: The NIST Framework highlights assessing suppliers and third-party partners but could benefit from clear guidance on evaluating the security practices of sub-suppliers within the supply something extremely important in the multi-layered smart grid.
  - Proactive vs Reactive Supply Chain Risk Management: The NIST Framework presently focuses on establishing and managing SCRM processes, which is very valuable, but it could be bolstered by emphasizing proactive risk identification and mitigation strategies, such as threat intelligence and incident response techniques.

Gap 4: The Growing Threat of Advanced Persistent Threats (APTs) [6].

- The NIST Framework presently does not have specific guidance/protocols on addressing the unique challenges posed by APTs targeting smart grids. Nation-state actors or well-resourced cybercriminal groups often orchestrate these highly sophisticated and persistent attacks, which can have tragic consequences for critical infrastructure.
- To understand what APTs (Advanced Persistent Threats) are and encompass, they are characterized by their prolonged nature, frequently employing advanced techniques to infiltrate networks and evade detection to achieve their objectives. They do this through means such as data exfiltration, sabotage, or disruption of operations (Sciencedirect.com, 2019). And while the concept of APTs has been around for some time, their methods and the technologies that they exploit are constantly evolving. APT groups are increasingly leveraging new technologies like AI and machine learning to enhance their attacks, making them a continuously emerging threat. Specifically, the gaps regarding APTs are:
    - Lack of APT-Specific Threat Intelligence Guidance: The framework doesn't explicitly address the need for specialized threat intelligence focused on APT actors targeting smart grids and their specific motivations.
    - Absence of APT-Focused Incident Response Recommendations: There is currently no guidance on developing incident response plans customized to the unique characteristics of APT attacks against smart grids. Such a gap can lead to delayed and/or ineffective responses, magnifying an APT attack's impact.
    - Limited Guidance on Long-Term APT Mitigation: The NIST Framework presently does not explicitly address the need for long-term mitigation strategies to address the persistent nature of APTs.

Additions to the NIST Framework

The following table presents proposed additions to the NIST Framework, specifically designed to address the unique cybersecurity challenges of the modern smart grid. These additions build upon the existing framework's structure, retaining its six core columns while incorporating a new 'Solution' column. This added column provides concrete, implementable strategies for mitigating identified risks, delving into specific contexts and steps within a clear, tabular format.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Signage	Solution
Functional	Enterprise Risk	Concerns about establishing and maintaining trusted identities for IoT devices throughout their lifecycle in the smart grid	The increase of IoT devices in the smart grid increases the attack surface and requires robust identity manageme nt.	1) IoT devices often have long lifecycles, and their security posture can change over time due to factors like software updates, configuration changes, and physical tampering 2) Need to ensure that only authorized and trusted IoT devices can connect to the grid and access sensitive data and systems	1) Increased reliance on distributed intelligence: As the grid becomes more decentralized, with intelligence embedded in edge devices, ensuring the trustworthines s of those devices is paramount 2) Scalability Challenges: Securely provisioning and managing a large number of diverse IoT devices can be complex, requiring automated and scalable solutions	1) Implement least privilege access control: Granting devices only the minimum necessary permissions to perform their functions 2) Continuous security monitoring: Implement real-time monitoring of device behavior and security posture to detect anomalies and potential threats

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Signage	Solution
Data Management	Regulatory Compliance	Ensuring compliance with relevant data privacy regulations (e.g. GDPR, CCPA) in the context of smart grid data	Smart meters and other IoT devices collect sensitive data about energy consumption patterns, raising privacy concerns	Need to comply with data protection regulations and implement appropriate safeguards to protect consumer data and ensure ethical data handling	1) Data anonymization and pseudonymization techniques 2) Data minimization and data retention policies: consent management	1) Transparency and control: Provide consumers with clear information about data collection practices and give them control over their data 2) Data Minimization: Collect only the data necessary for grid operations 3) Data Security: Employ encryption, secure storage, and data integrity checks to protect data confidentiality and integrity

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Signage	Solution
Trustworthiness	Security (Advanced Persistent Threats)	Addressing the growing threat of APTs targeting smart grid infrastructure and data	The increasing connectivity and complexity of smart grids make them attractive targets for sophisticated and persistent cyberattacks	1) APTs are often state-sponsored or highly organized groups with significant resources, employing secretive tactics to infiltrate networks, remain undetected for extended periods, and exfiltrate data or disrupt operations. 2) These attacks can target critical smart grid components, potentially causing widespread outages or manipulating energy markets	1) Require security controls to be embedded at all layers of smart grid architecture, from edge devices to the control center. 2) This includes secure communication protocols, intrusion detection and prevention systems, and comprehensive access controls.	1) Advanced Threat Detection: Deploy advanced security tools like intrusion detection systems (IDS), and security information and event management (SIEM) systems to detect APT activity 2) Regular Security Assessments: Conduct regular security assessments and penetration testing to pinpoint vulnerabilities and improve defenses 3) Security Monitoring and Incident Response: Establish 24/7 security monitoring and incident response functionalities to rapidly detect, respond to, and recover

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Signage	Solution
Trustworthiness	Supply Chain Risk Management	Ensure equipment and software used in the smart grid are trustworthy and have not been tampered with	Increased reliance on third-party vendors increases the potential for vulnerabilities	Complex supply chains make it challenging to trace the origin and security posture of components	1) Require security controls to be embedded at all layers of the supply chain, from the initial design and manufacturing to deployment and maintenance 2) This includes secure development practices, code reviews, vulnerability assessments, and penetration testing	1) Enhanced Supply Chain Visibility: Gain deeper visibility into the entire supply chain, including sub-suppliers 2) Proactive Risk Mitigation: Utilize threat intelligence and vulnerability scanning to identify and address risks

Smart Grid Cybersecurity Playbook

Now that we have identified key cybersecurity concerns and proposed enhancements to the NIST Framework, it's important to provide clear and actionable mitigation strategies for stakeholders across all industries. This guidance will act as a practical playbook, enabling a proactive approach to cybersecurity rather than simply reacting to incidents.

And keep in mind, that robust cybersecurity is not merely about preventing operational disruptions; it's also about safeguarding against legal repercussions and reputational damage. We've witnessed how cyberattacks, like the ransomware attacks that cripple a hospital's power

supply, can have severe consequences, potentially jeopardizing patient safety and disrupting critical services.

While the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) standards provide a valuable foundation for securing critical infrastructure within the energy sector, this playbook delves deeper and broader. It offers specific guidance customized to the smart grid, going beyond the bulk electric system focus of the NERC-CIP to cover the wider network of interconnected devices and systems. [10].

The following checklist provides seven actionable best practice mitigation strategies that smart grid stakeholders can implement to strengthen their defenses and ensure the reliable delivery of energy.

1. Implement Robust Anomaly Detection
    a. Train machine learning models on historical data to detect unusual fluctuations in grid frequency or voltage that might indicate an attack on grid stability
    b. Consider the unique communication protocols used in smart grids when analyzing network traffic for anomalies. These would include those related to distributed energy resources (DERs) like solar panels and wind turbines.
2. Enforce the Principle of Least Privilege
    a. Engineers accessing control systems remotely should only have the necessary permissions to perform their specific tasks, such as monitoring equipment status or adjusting voltage settings. They should not have access to unrelated systems, like customer billing databases or network configurations
    b. Segment the network to isolate critical systems from less sensitive parts of the grid. This limits the potential damage an attacker could cause even if they gain access to a user account with limited privileges
3. Protect against Insider Threats
    a. Implement access controls that prevent a user from making unauthorized changes to critical grid settings without a second authorization from a supervisor, which helps prevent accidental or malicious actions by a single individual
    b. Routinely monitor user activity for suspicious behavior, such as attempts to access or modify configurations of critical equipment, which can help detect unauthorized activities even by users with legitimate access
4. Securely Manage Supply Chain Risks

    a. Conduct thorough due diligence before onboarding any vendor by evaluating their security practices, certifications, and incident response capabilities. Ensure that this vetting process is extended to sub-suppliers and other third parties involved in the supply chain to gain better visibility into potential risks
    b. Implement ongoing monitoring of suppliers' security posture through routine vulnerability assessments, penetration testing, and security audits. Routinely review and update security requirements in contracts with suppliers to ensure that they are in alignment with emerging threats
5. Ensure Secure Software Development
    a. When developing firmware for smart meters, ensure that rigorous code reviews and penetration testing happen to identify and address vulnerabilities that could allow attackers to disrupt communications with the utility
    b. Adhere to secure coding standards specific to industrial control systems
6. Regularly Update and Patch Systems
    a. Prioritize patching vulnerabilities in critical grid components to prevent disruptions to grid stability and reliability
    b. Develop patch management procedures that take into account the operational constraints of the smart grid, like the need to avoid downtime during peak demand periods

Evaluation

To assess the overall cohesiveness, clarity, and flow of this project, a qualitative interview was conducted with Ned Boyd, an industry expert in the smart grid whom I've consulted with throughout this project. During the evaluation interview, Ned evaluated the project based on several key metrics on a scale of 1-5, including feasibility, clarity, detail, organization, and usefulness. His feedback provides valuable insights into the strengths and areas for potential improvement of the project. Here is a breakdown of his comments:

Feasibility (3 out of 5): Ned believes that my proposed solutions are implementable, but cautioned that the implementation process within a utility company could be lengthy. He explained that these companies often have complex decision-making procedures. These processes typically involve heavy vendor research, approvals from different stakeholders, signoffs, and adjustments to the policy. From his experience, fully implementing the type of recommendations that I am proposing could take over a year. Because the project covers a

myriad of heavy technical and policy changes/updates, he thinks it may not be the most feasible or practical, in terms of timeline.

Clarity (5 out of 5): Ned found my explanations clear and easy to understand, and believes that even for someone who does not have a strong technical background, they would be able to easily understand and follow the content. He appreciated the use of layman's terms and visual aids (like the charts used for the additions to the NIST Framework), combined with more in-depth explanations.

Detail (5 out of 5): Ned was impressed with the level of detail that I provided, particularly in my coverage of 'blue team' defense strategies (SIEM, IDS, etc.). He felt that I adequately explained the importance of security monitoring and provided sufficient information without being too vague or confusing.

Organization (4 out of 5): Ned noted that I had a clear flow of information, from pinpointing the need for cybersecurity in the smart grid to outlining solutions. He did suggest that I could include more clear transition sentences and paragraphs to ensure that the transition from one solution to the next was more clear.

Organization (4 out of 5): Ned noted that I had a clear flow of information, from pinpointing the need for cybersecurity in the smart grid to outlining solutions. He did suggest that I could include more clear transition sentences and paragraphs to ensure that the transition from one solution to the next was more clear.

Usefulness (5 out of 5): Ned expressed that he believed that the project would be very useful, highlighting its relevance to grid security and its clear identification of necessary solutions. He believes that the project overall effectively conveys the importance of protecting the smart grid and offers concrete recommendations to do so.

In addition to the more structured scoring, Ned also provided valuable feedback on how the project addresses key aspects of smart grid security, including supply chain risks, real-time monitoring, data management, and public perception.

Supply Chain Security: Ned strongly commended the project's focus on supply chain security, agreeing that evaluating sub-suppliers' cybersecurity practices is crucial. He supported the call for thorough due diligence, including using third-party risk assessments and demanding evidence of strong security practices. He particularly appreciated the project's emphasis on the risks of outdated software and firmware.

Real-Time Monitoring and Data Management: Ned praised the project's recognition of the growing importance of real-time monitoring and its highlighting of solutions offered by companies like Schneider Electric. He also affirmed the project's focus on responsible data management and minimizing data collection.

Security Operations Center (SOCs): Ned was pleased to see the project acknowledge the role of managed security services and their potential to provide utilities with access to advanced security tools and expertise.

Public Perception: Ned commended the project for addressing the critical issue of public perception and emphasizing the need for clear communication and transparency to build trust. He specifically highlighted the importance of addressing public anxieties and past negative experiences, such as those that arose during the 2021 Texas winter storm, where power outages and coinciding smart meter installations led to conspiracy theories and mistrust.

Limitations

Scope and Technical Depth: To maintain accessibility for a wider audience, the project provides a high-level overview of smart grid cybersecurity concepts without delving into intricate technical details. For instance, the discussion on data anonymization does not include specific software solutions or step-by-step procedures. Similarly, areas like co-reviews and patching lack detailed technical groundwork.

Real-World Validation: The project's insights are primarily based on theoretical analysis and existing literature. It lacks real-world validation through pilot projects, data analysis, and surveys that could provide more concrete evidence of the recommendations' effectiveness.

Resource Constraints: Implementing the project's recommendations would require significant financial investments and human resources. The project does not include a detailed analysis of these economic and logistical constraints, which could pose challenges to real-world implementation.

Future Work

To enhance the project's impact and move towards practical implementation, the following future work and next steps can be done:

Step-by-Step Guides: In my project, I did not detail the specifics of how to perform some of the more technical processes, such as data anonymization. In the future, it would be helpful to create a detailed guide that lays out the exact steps involved, offers specific software and tool suggestions, and provides best practices for ensuring that the data is protected while still being useful.

Expand Technical Guidance: Similarly, for things like code reviews and patching, I could provide much more detailed instructions and background information. This would help people put these security measures in place. It would be helpful to create checklists, flowcharts, or other visual aids to make it easier to understand.

Conduct Pilot Projects: The majority of the project is based on theory and leveraging previous smart grid cybersecurity frameworks. To test the validity and efficacy of the proposed recommendations, it would be important to test them in real-world pilot projects. This would entail implementing the security measures in a controlled setting and collecting data to see how well they work.

Gather Empirical Data: Finally, to make this project even stronger, it would be beneficial to surpass simply reviewing the existing literature and gathering some real-world data. This can be done through surveys, interviews, and focus groups.

Address Resource Constraints: The proposed recommendations in this project will inevitably cost money and require a workforce. It is important to carefully assess the financial and human resource needs to actually carry out these recommendations and address any challenges that may arise in the process of doing so.

Develop Sample Implementation Timeline: To better help stakeholders understand how to put these recommendations into practice, it would be useful to create sample timelines for implementation. These timelines would show when it makes the most sense to implement different security measures, giving stakeholders a clearer idea of how to prioritize and schedule their efforts.

Conclusion

In conclusion, this project examined the cybersecurity risks inherent in the increasingly interconnected smart grid, emphasizing the need to address vulnerabilities arising from emerging technologies like IoT and AMI. It highlighted the limitations of the NIST Framework in fully addressing these evolving threats.

To enhance grid security, the project proposed a three-part solution: a gap analysis of the NIST Framework, additions incorporating advanced technologies and solutions, and a practical 'Smart Grid Cybersecurity Playbook' with actionable recommendations for stakeholders. Industry expert Ned Boyd commended this robust approach, particularly expressing enthusiasm for the focus on real monitoring, responsible data management, and the role of managed security services in providing advanced security capabilities.

The project acknowledges limitations in its scope and lack of real-world validation but underscores the need for a holistic approach to cybersecurity. This includes fostering a culture of awareness across all personnel, and recognizing that even a single phone call exploiting social engineering tactics can compromise security. Ned also emphasized the importance of addressing public perception and building trust through clear communication, especially in light of past incidents like the 2021 Texas winter storm that fueled anxieties. Future efforts should prioritize continuous training and collaboration to ensure a resilient and secure smart grid.

From a learning perspective, crafting this project helped me understand how seemingly unrelated topics like cybersecurity, energy infrastructure, and sustainability are deeply intertwined. It highlighted the increasing complexity of cybersecurity and its critical role in protecting our evolving technological landscape. It was an interesting and insightful experience, and I appreciate the support throughout the semester. Thank you for reading my paper!

Works Cited

1. Ned Boyd, personal communication, September 26, 2024
2. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0

   Greer, C., Wollman, D. A., Prochaska, D., Boynton, P. A., Mazer, J. A., Nguyen, C., FitzPatrick, G., Nelson, T. L., Koepke, G. H., Jr., A. R. H., Pillitteri, V. Y., Brewer, T. L., Golmie, N. T., Su, D. H., Eustis, A. C., Holmberg, D., & Bushby, S. T. (2021, October 14). *NIST framework and Roadmap for Smart Grid Interoperability Standards, release 3.0*. NIST. https://www.nist.gov/publications/nist-framework-and-roadmap-smart-grid-interoperability-standards-release-30

3. Inside Privacy. (2021, July 14). *ENISA publishes new guidelines for Smart Grid Cyber Security*. https://www.insideprivacy.com/data-security/enisa-publishes-new-guidelines-for-smart-grid-cyber-security/
4. 2010 Smart Grid System Report. (n.d.). https://www.energy.gov/sites/prod/files/2010 Smart Grid System Report.pdf
5. *Cybersecurity – Siemens AG*. siemens.com Global Website. (n.d.). https://www.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/grid-security.html#DownloadWhitePaper
6. Colak, I., Wang, W., Otuoze, A. O., Mrabet, Z. E., Leszczyna, R., Razak, M. F. A., MaoG., Jokar, P., Bekara, C., LiuX., WangB., ChaiB., FangX., … Goel, S. (2019, September 16). *Security aspects of internet of things aided Smart Grids: A bibliometric survey*. Internet of Things. https://www.sciencedirect.com/science/article/abs/pii/S2542660519302148?via%3Dihub
7. *The internet of things and increasing threats to the electric grid*. ASIS Homepage. (n.d.). https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2024/february/Internet-of-Things-Increasing-Threats-Electric-Grid/#:~:text=As%20IoT%20devices%20become%20more,and%20damage%20the%20grid%20infrastructure.
8. Digital Grids | E.ON. (n.d.-b). https://www.eon.com/en/energy-grids/digital-grids.html
9. Iea. (n.d.). *Smart grids*. IEA. https://www.iea.org/energy-system/electricity/smart-grids
10. Awati, R., & Cole, B. (2022, March 2). *What is NERC CIP (Critical Infrastructure Protection) and how does it work?*. Search Security. https://www.techtarget.com/searchsecurity/definition/North-American-Electric-Reliability-Corporation-Critical-Infrastructure-Protection-NERC-CIP