Securing the City: Essential Practices for SCADA System Management

Tim Olsen
Gonzaga University

Hsin-Yun Chen
Gonzaga University

Sarah Gehman
Gonzaga University

Ty-Hunter Hosack
Gonzaga University

William Smith
Gonzaga University

ABSTRACT

Supervisory Control and Data Acquisition (SCADA) systems are critical for managing essential city services like water treatment, waste management, and electricity generation. However, implementing and maintaining these systems presents significant challenges for IT leaders. This study, conducted in collaboration with the City of Spokane's Public Works IT Team, examines the application and maintenance of SCADA systems within the city. Through interviews with the IT Team, the study identifies seven key lessons for IT leaders seeking to enhance SCADA system efficiency. These lessons address common issues, including the importance of understanding system requirements and costs, regulating updates, establishing a non-production practice environment, implementing a change management process, prioritizing safety, fostering open communication channels, and investing in staff training. The study also outlines four prevalent SCADA-related problems with recommended solutions, aimed at optimizing organizational performance and system reliability. This research offers valuable insights for IT leaders working with SCADA systems in mid-sized cities and beyond, contributing to the growing body of knowledge on effective SCADA management practices.

Subject Areas: Information Systems, Public Administration
Article Type: Peer-Reviewed Journal Article

Introduction

Our modern lives depend on a complex web of public utilities that we often take for granted. From the clean water that flows from our taps to the electricity that powers our homes, these essential services are managed by sophisticated IT systems known as Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems allow for remote and on-site process control, data gathering and processing, and interaction with actuators and sensors, ensuring the efficient and reliable operation of critical infrastructure (Sean et al., 2020).

The importance of effectively managing these IT systems cannot be overstated. A failure in a SCADA system can have devastating consequences, leading to disruptions in essential services, environmental damage, and even loss of life. For example, a failure in a water treatment plant could result in contaminating the river.

The history of SCADA systems is punctuated by incidents of malicious attacks. In 1982, the Siberian pipeline explosion, believed to be the first cyber incident involving a SCADA system, involved a Trojan horse that modified valve and pump operations, leading to an explosion (Ismail et al., 2014). The Salt River Project in Arizona in 1994 was infiltrated through a dial-up modem, allowing attackers to steal and modify customer information and system logs (Do et al., 2017). These early attacks illustrate the vulnerability of SCADA systems and the need for robust security measures (Alanazi et al., 2023).

More recent attacks, such as the Stuxnet worm in 2010, which targeted the Iranian nuclear program, and the 2015 Russian power grid hack that caused a widespread outage, highlight the increasing sophistication of cyber threats against critical infrastructure (Falliere et al., 2011; Mesbah & Azer, 2019). These attacks demonstrate the potential for significant disruption and damage when SCADA systems are compromised. Given the critical role of SCADA systems in maintaining essential services and the escalating threat of cyberattacks, it is imperative for organizations to prioritize the security and efficiency of their SCADA systems (Sims, 2024).

SCADA systems are clearly essential to the functioning of society, however due to their secluded and isolated nature they are not a popular topic for managerial research. While the security and cybersecurity of SCADA systems, and network communication protocols are popular topics of research, managerial best practices for ongoing operations are lacking in the literature. Accordingly, we address the following question requestion: “What are the managerial best practices for SCADA systems in a mid-sized city?”

This paper examines the application and maintenance of SCADA systems within the City of Spokane in Washington, USA. The following section reviews the fundamental components of SCADA systems, the literature on managing SCADA systems, and a case description of SCADA systems in the city of Spokane. The methods section outlines the research design and data collection process, which involved interviews with the City’s Public Works IT team. Key findings are presented as seven managerial lessons learned, along with specific actions IT leaders can implement. Each lesson is explored in depth, outlining the challenge, and the solution implemented by the City of Spokane. Finally, the paper concludes by discussing the implications of these lessons for SCADA management, as well as opportunities for future research to enhance system security and efficiency.

Background and Literature Review

SCADA systems offer both monitoring and control capabilities, providing a comprehensive approach to managing critical infrastructure. Sensors strategically placed throughout the system collect data on key variables like temperature, pressure, water levels, and other relevant metrics (Gaushell & Darlington, 1987). This information is transmitted to SCADA displays, providing operators with real-time insights into the system's performance.

Remote control of actuators and other devices in response to monitored data are essential for SCADA systems. When a variable exceeds a predefined threshold, the system can automatically trigger actions like opening valves or adjusting pump speeds to prevent potential problems (Sayed & Gabbar, 2017). For example, if a water tank experiences high pressure, a sensor might detect this condition and trigger the system to open a valve, releasing pressure and preventing damage.

Isolated physical connections (Ethernet and dedicated ports) between Programmable Logic Controllers (PLCs) and Human Machine Interfaces (HMIs) are key component for SCADA systems. This physical isolation from the internet helps to enhance security, as it significantly reduces the risk of external attacks via wireless networks (Nankya et al., 2023). This robust security is crucial for protecting essential services like electricity and water supply. Security of SCADA networks continues to a major research focus (Ayaburi & Sobrevinas, 2015; Hernández Jiménez et al., 2017; Hudgens et al., 2019; Ismail et al., 2014; Slay & Miller, 2006).

Real-time and historical data, allowing for immediate analysis of system performance and identification of trends are key components of SCADA systems. This data can be used for troubleshooting, optimizing processes, and predicting potential issues (Poosapati et al., 2019). The automation capabilities of SCADA systems streamline processes, reduce human error, and improve efficiency (Sartor et al., 2024). The systems are designed to communicate across different vendors, ensuring compatibility and seamless integration between various components (Pau et al., 2022). Communication between and monitoring network nodes continues is a major research focus (Kbean & Sadkhan, 2020; Rohmingtluanga et al., 2023; Upadhyay et al., 2022).

Case Description

The City of Spokane utilizes SCADA systems to manage and control a range of critical infrastructure, ensuring the continuous operation of essential services for its residents. These systems play a vital role in the following systems:

Solid Waste Management: The city's Waste to Energy Facility is the only one in the state of Washington and one of about 75 in the nation. It relies on SCADA for monitoring and controlling processes, ensuring the safe and efficient disposal of solid waste.

Waste Water Treatment: The City of Spokane operates one of the most advanced wastewater treatment facilities in the region (see Figure 1) that treats an average of 34 million gallons a day of wastewater. SCADA systems play a crucial role in monitoring and controlling various aspects of the water treatment process, protecting the quality and safety of the water supply.

*Figure 1. Spokane's Riverside Park Water Treatment Plant (*Water Management*, 2024)*

Combined Sewer Overflow (CSO) Tanks: These tanks are designed to collect stormwater and provide additional wastewater storage, minimizing the risk of sewer overflows during heavy rainfall (Wastewater Combined Sewer Overflow (CSO), 2024). The city is currently implementing a SCADA system for these tanks, initially focusing on monitoring capabilities. The future implementation of control capabilities will allow for remote responses to issues, reducing the need for on-site interventions.

Hydro-Electric Power Generation: The city's hydroelectric dam on the Spokane River (see Figure 2) generates over 70 million kilowatts of electricity annually, powering homes and businesses within the community (*Upriver Dam*, 2024). SCADA systems are used to monitor and control the dam's operations, ensuring optimal power generation and efficient water management.

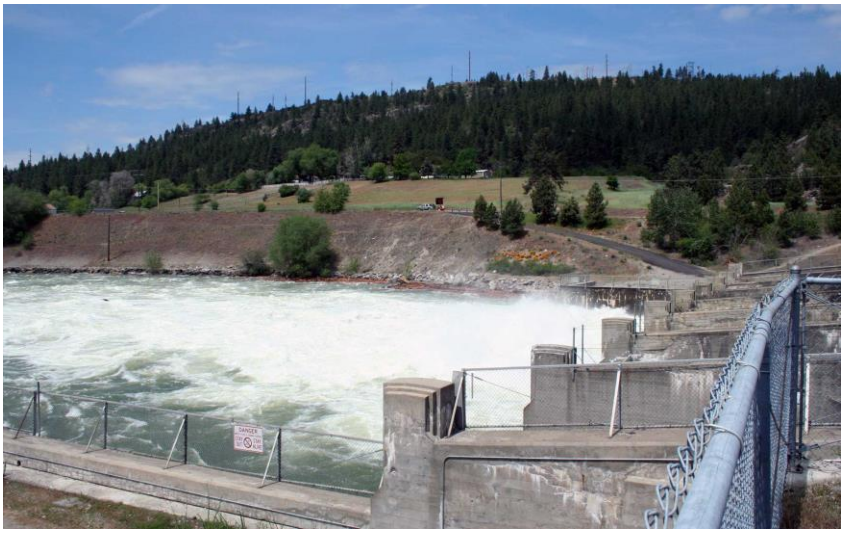

*Figure 2. The city owned Upriver Dam (*Protecting Upriver Dam for the Future*, 2016)*

Water Department: the city's water department delivers up to 180 million gallons a day of clean drinking water.

The City of Spokane's comprehensive use of SCADA systems across its essential infrastructure highlights the critical role of these systems in ensuring the smooth and reliable operation of vital services. The city's experience with SCADA management provides valuable insights into the challenges and best practices associated with maintaining these complex IT systems.

Method

This study employed a single-site case study design (Yin, 2003), drawing upon Clinical IS Research principles (Baskerville et al., 2023; Myers, 2023) to uncover practical managerial lessons regarding SCADA systems. The research focused on the experiences of the Public Works IT Team of the City of Spokane, a team with many years of experience in the field.

Data collection centered around a 100-minute group interview conducted by four researchers with the Public Works IT Team. The interview employed a semi-structured format, utilizing open-ended questions. The interview questions were framed around three key areas, inspired by Reunamäki & Fey's (2023) framework of problems, solutions, and pitfalls to avoid (see Table 1).

Problems	Tell us about your journey with SCADA, what challenges have you faced?	This aimed to uncover challenges and issues encountered
Solutions	How have you dealt with these challenges?	This sought practical solutions and strategies developed
Pitfalls and Remedies	What pitfalls should others watch out for, and how can they avoid them?	This aimed to identify common pitfalls others could avoid and their remedies

Table 1. Interview Guide based on Reunamäki & Fey's (2023) framework

To mitigate potential bias and groupthink, each researcher independently took notes during the interview, subsequently sharing and comparing their observations. Multiple interviewers has shown to enhance creditability in qualitative research (Patton, 2014).

Data analysis involved an inductive approach (Baskerville & Lee, 1999; Winter, 2014), initially categorizing findings into broad themes like "change management issues" and "technology issues." This process ultimately led to the identification of seven distinct problems and their corresponding solutions. These findings were then validated by employees representing relevant teams and organizational leadership. This practice is known as a "member check" or "respondent validation" and is a technique shown to improve the validity of qualitative studies (McKim, 2023). The following sections will present and discuss these seven problem-solution pairs in detail.

Findings

Key Lessons Learned in SCADA Usage

In this section we present seven lessons that emerged, with key actions to be taken by management. Table 2 summarizes the seven lessons, and key actions for managers.

Lesson	Description	Key Actions
1. Understand Systems & Costs	Before implementation, thoroughly assess organizational needs, including processes, systems, goals, and required software/hardware expertise. Consider feasibility and cost-effectiveness, factoring in installation, maintenance, testing, and training expenses.	Analyze organizational needs, utilize models like the Purdue Model, hire experienced personnel, and plan for ongoing maintenance and support.
2. Regulate System Updates	Prioritize timely software and hardware updates to maintain security and optimal functionality. Stay informed about vulnerabilities and implement patches proactively.	Subscribe to release notes, establish update schedules (ad hoc, cyclical, planned, emergency), document changes meticulously.
3. Implement Non-Production Practices	Establish a controlled environment to test PLC logic, updates, and patches before live deployment. This minimizes risks and allows for identifying and mitigating potential issues beforehand.	Invest in dedicated testing equipment, replicate real-world scenarios, and thoroughly troubleshoot before deployment.
4. Establish a Change Management Process	Develop and implement a clear change management process to ensure smooth and controlled implementation of updates and patches. Define roles, responsibilities, communication channels, and approval processes.	Define approval hierarchy, establish communication protocols (e.g., automated notifications), maintain detailed documentation of all changes, and create rollback plans for unforeseen issues.
5. Prioritize Safety Measures	Emphasize safety in all aspects, including personnel safety protocols (PPE, established procedures) and technological safeguards. Conduct regular equipment maintenance, control access to critical areas, and replace aging equipment proactively.	Implement regular equipment checks and maintenance, enforce strict access control measures (physical and digital)
6. Foster Open Communication	Encourage clear, consistent communication within the IT team and across departments. Provide clear direction, actively listen to team members, and foster a culture of open dialogue.	Establish clear goals and expectations, encourage active listening, and feedback, and ensure team members understand the rationale behind decisions.
7. Invest in Staff Development	Prioritize continuous learning and development opportunities for IT staff. Provide training programs, encourage specialization, and nurture existing talent to stay ahead of technological advancements and maintain a highly skilled workforce.	Offer training programs, support professional development, and create a culture of continuous learning and growth.

Table 2. Seven Key Lessons for Effective SCADA Management

Lesson 1: Know the Systems and Associated Costs

Make sure to understand the organization's specific needs and requirements before implementing a SCADA system. This includes the processes and systems the SCADA system will be monitoring and controlling, as well as the goals and objectives of the organization. It is critical to ensure that the people in the organization who will be working with the system have the necessary knowledge of software and hardware to use the systems effectively.

One tool the City of Spokane uses in their SCADA implementation is the Purdue Model (found in the appendix below). This model is used to identify different layers of protection and detect any airgaps that need to be filled. The city is implementing a new system to support functionality of the CSO tanks at the water treatment plant. The new system will monitor the

level of a few dozen tanks that have accumulated rain and sewer water to prevent unclean water from entering the Spokane River. To support this effort, the city hired an engineer already familiar with the Purdue Model at the water treatment facility. After a year of working alongside the CSO tanks and installing SCADA, they are hiring a new engineer to transfer the knowledge over and maintain standards to follow from precedent.

There are many constraints involved in general implementation and maintenance, so you must understand the full implications before moving forward. The reality is that it will not be feasible or cost effective for many organizations, even with the increased benefits it would provide. The cost of implementing a SCADA system can include expenses such as installation, maintenance, testing, and training. Ongoing maintenance and support, which ensures their continued operation, can include costs such as software updates, hardware maintenance and replacement, and technical support. Additionally, costs of hardware and software required for SCADA systems can vary significantly depending on the complexity and scope of the systems. This is a practical lesson, often overlooked in by researchers who often focus on security and network communication, ignoring practical concerns like cost.

Lesson 2: Regulate Updates of the System as Needed

It is important to keep the software and hardware systems up to date to remain secure and function optimally. In doing so, IT managers can be responsive and protect their organization from vulnerabilities. Outdated technology can pose security risks and cause performance issues, leading to a negative impact on the organization's operations and reputation. Any outdated web application, either internal or external, can be exploited and expose the plant to a data breach.

In addition to managing updates as needed, patches can be used to implement new features or functions, fix an existing bug, or protect from an identified vulnerability. It is common to not receive just one patch, but a series of patches all at once through a patch release. Vendors are constantly providing additional patches, that if implemented, should allow the software to continue to perform as intended. This information is oftentimes relayed through release notes. Subscriptions to manufacturers' release notes ensure that an organization is on top of their system updates and aware of any vulnerabilities on any appliance.

Patches and updates help ensure that the organization can continue to achieve its goals and objectives while providing a safe and efficient environment for its users and technicians. These updates can be performed on an ad hoc, cyclical, planned, or emergency basis. Ideally, planning for these updates on the front-end helps deter problematic or emergency implementation after the fact. While security and updates are an important part of research,

This finding compels managers to develop their own update or patching process, which is the practical side of the result of much research on security for SCADA systems. Research shows that often managers need to rank order patches based on how critical they are (Yadav & Paul, 2019).

Lesson 3: Create a Non-Production Practice

When it comes to implementing innovative technologies and systems, there is always a risk of encountering unforeseen issues that could negatively impact the system's functionality. To minimize this risk, IT managers should consider establishing a non-production practice that allows them to test the ladder language before implementing any new update or patches. Ladder logic is a programming language widely used in industrial control systems, particularly with Programmable Logic Controllers (PLCs). It uses a graphical representation resembling a ladder,

with rungs and rails, to visually depict the logical flow and execution of control instructions for automation tasks.

A non-production practice is one where the software is tested offline to replicate its impact or usage and identify any potential issues and bugs before going live. It is common to experience troubleshooting problems with outdated data systems, customized processes, or any new and unfamiliar system. Problems identified can then be mitigated safely by making any necessary adjustments and fixes before the language is rolled out, minimizing the risk of unexpected problems or security threats.

Having a couple of extra PLC's and HMI's that are dedicated to testing the ladder language before it is implemented is the best way to create a non-production practice. While it does require an additional cost, the ability to view the new ladder language in practice before its implementation into the actual system can highlight potential vulnerabilities or glitches. Since SCADA systems are used for essential functions within the city, making sure the new code will have the desired impact can ensure the plants will continue to function properly. This finding appears to be a novel finding not discussed in the literature previously. Future research can address best practices for non-production practices.

Lesson 4: Have Your Change Management Process In-Place

When problems or bottlenecks arise in IT, quick responses can be critical to keeping the technology running and secure. As such, it is helpful to have your change management process in-place prior to these unforeseen problems arising. There will always be pushbacks, but being clear on any rationale behind implemented or proposed changes is a great first step to minimizing this potential barrier. Change management is not often discussed in literature related to SCADA, however (Deák, 2024) and (Tungkagi et al., 2021) both see study it as a requisite for success in changes to SCADA systems.

For example, when a patch is needed for a system, a notification is sent with the reason behind the patch with more information found in the release notes which all stakeholders need to be aware and knowledgeable of. A change request can then be sent in. Automatic notifications come through to key stakeholders whenever a change request is received with information on when it will be applied, the rollback of that change, and the benefit of implementing the patch. From here, they must track the change, keep the team notified, and await approval. Oftentimes, the team members who submit change requests lack the authority to apply it. Knowing who is the main decision maker for these actions, whether a chairperson or head of the change control board, is critical for ownership and creating a rollback plan as needed. Following approval, application takes place. Throughout this process, you must document the changes made to the system for future reference and tracking.

Lesson 5: Do Not Forget Safety Measures

Safety is such an expansive term here, including the safety of the plant's technology and the individuals involved. Wearing personal protective equipment and following protocols are critical across the organization. Safety can also be connected to maintaining the technology and patch implementation. In terms of general maintenance, having a set cadence to check every piece of equipment, per the manufacturer, is important. This includes things as simple but crucial as disassembling a pump to re-oil the bearings. But this can be for items that are nearing the end of their life that need to be replaced. From the moment a piece of equipment is used, the

depreciation clock begins. Replacement helps avoid accidents that can be detrimental to the safety of the staff and overall function of their systems.

Safety also includes controlling access across the organization, internally and externally. For example, it should be pre-determined which personnel are allowed in what areas of the plant. This protects both the equipment and staff. Recent literature has developed the importance of safety both in the system design (Fonseca, 2023), as well as the environment in which the systems are placed (Fares, 2021; Khatib & Zaher, 2024).

Lesson 6: Open Communication Channels

As an IT manager, providing clear direction and goals to the team is crucial for achieving success. Each team member needs to understand what is expected of them to reduce the likelihood of misunderstandings and confusion. As diversity continues to take root in the communities we live and work in, there are countless factors that interrupt our daily communication efforts. Clear communication reduces the likelihood of confusion, time-wasting, team ineffectiveness, and lost productivity.

The IT Director at the city shared, "One of the things that is most important is you are going to provide direction to a team of people. Make sure that direction is clear.... And in doing so, [open] the possibility of dialogue." The IT world is no different than any other management team. Communicating clearly and effectively, paying attention to what others are saying, and asking questions if something is unclear is essential for managers. It saves time and increases productivity by having the full team on the same page and aware of one another's viewpoints. Additionally, team members can prioritize their duties and concentrate on the most important activities by having a clear sense of direction. As a result, IT managers and leaders must ensure their team fully articulates the organization's goals and priorities, providing them with a clear path to success.

To be effective as leaders, IT managers need to be willing to listen and learn from their employees and specialists and encourage a culture that celebrates speaking up. Not only will this make them more effective as a leader, but it will also support and inform difficult decision making when necessary. However, managers must also always be prepared to make decisions that align with the organization's objectives, even if that may be a challenging or unpopular approach. Managers can develop a culture of accountability and achieve long-term success for their team and company by balancing these skills. There is much literature on team dynamics and performance improvement (Bull Schaefer & Copeland, 2024) and we expect this applies to the context of SCADA systems.

Lesson 7: Invest, Nurture, and Train Staff

In today's fast-paced and ever-changing world, organizations need to have highly skilled and adaptable employees who can keep up with the latest industry trends and technologies. To achieve this, IT leaders must create learning opportunities and provide training and development programs. This can help employees improve their skills and obtain up-to-date knowledge and information. At the same time, this can lead to better outcomes for the organization, such as increased efficiency and higher profitability. Therefore, it is essential for IT managers to provide opportunities for growth, nurture their talents, and offer continuous training and development.

And as technology continues to evolve, specialization has become critical within each information technology team. Investing in these key staff members is essential to keeping your

systems running smoothly and being strategic on growth and maintenance plans. It costs far more to recruit and train a new employee than nurture and maintain the ones you already have, making it the ideal economic and strategic business strategy. This lesson aligns well with research on the high cost of employee turnover (Li et al., 2022).

Conclusion

This study aimed to identify and understand practical managerial lessons regarding the implementation and maintenance of SCADA systems in essential city services. Through a single-site case study design, utilizing a semi-structured group interview with the Public Works IT Team of the City of Spokane, seven key lessons for effective SCADA management emerged. These lessons emphasized the importance of understanding system requirements and costs, regulating updates, establishing non-production testing environments, implementing robust change management processes, prioritizing safety measures, fostering open communication, and investing in staff training and development.

Perhaps the most interesting on novel findings that have not been addressed in prior literature are the importance of having a non-production practice and understanding of system costs. While software development has production and development environments (Haakman et al., 2021), the physical nature of SCADA systems underlies the importance of having complete systems that have not been placed in production. Because the total cost of ownership of physical systems can be difficult to fully understand at adoption (McKeen & Smith, 2010), the importance of understanding costs mirrors what we see in software development and discussions of technical debt (Rinta-Kahila et al., 2023).

The findings highlight the critical role of proactive planning, continuous learning, and open dialogue in ensuring the secure and efficient operation of SCADA systems. By adhering to these lessons, IT leaders can mitigate risks, enhance system reliability, and ensure the uninterrupted delivery of critical city services. While much of the literature on SCADA systems deals with technical subjects (network and security), these findings contribute to the literature on managerial best practices for SCADA systems.

However, it is important to acknowledge the study's limitations. As a single-site case study, the findings may not be directly generalizable to all organizations. Future research could address this limitation by conducting comparative case studies across multiple cities or industries to explore variations in SCADA management practices and challenges. Additionally, future studies could go deeper into the economic aspects of SCADA implementation and maintenance, providing more concrete guidance on cost-benefit analysis for IT leaders.

Despite these limitations, this research contributes valuable insights for IT leaders tasked with managing SCADA systems, particularly in the context of mid-sized cities. By highlighting both the challenges and best practices associated with SCADA systems, this study offers practical guidance for improving the efficiency, security, and ultimately, the resilience of these critical infrastructure systems.

References

Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2023). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Computers & Security*, *125*, 103028. https://doi.org/10.1016/j.cose.2022.103028

Ayaburi, E., & Sobrevinas, L. (2015). Securing Supervisory Control and Data Acquisition Systems: Factors and Research Direction. *AMCIS 2015 Proceedings*. https://aisel.aisnet.org/amcis2015/ISSecurity/GeneralPresentations/9

Baskerville, R., & Lee, A. S. (1999). Distinctions among Different Types of Generalizing in Information Systems Research. In O. Ngwenyama, L. D. Introna, M. D. Myers, & J. I. DeGross (Eds.), *New Information Technologies in Organizational Processes: Field Studies and Theoretical Reflections on the Future of Work* (pp. 49–65). Springer US. https://doi.org/10.1007/978-0-387-35566-5_5

Bull Schaefer, R. A., & Copeland, L. K. (2024). Performance reviews as an active method to improve feedback and performance. *Active Learning in Higher Education*, *25*(1), 41–52. https://doi.org/10.1177/14697874221091898

Deák, T. (2024). *Resistance to change: Distribution system operators reaction to the introduction of a new SCADA system*. https://hdl.handle.net/2437/373824

Do, V. L., Fillatre, L., Nikiforov, I., & Willett, P. (2017). Security of SCADA systems against cyber–physical attacks. *IEEE Aerospace and Electronic Systems Magazine*, *32*(5), 28–45. IEEE Aerospace and Electronic Systems Magazine. https://doi.org/10.1109/MAES.2017.160047

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. Stuxnet dossier. *White Paper, Symantec Corp., Security Response*, *5*(6), 29.

Fares, B. (2021). *An integrated risk analysis framework for safety and cybersecurity of industrial SCADA system* [Master thesis, uis]. https://uis.brage.unit.no/uis-xmlui/handle/11250/2788245

Fonseca, C. A. A. (2023). SCADA System of Pipelines. In ABCM - Brazilian Society of Mechanical Sciences and Engineering, J. L. de França Freire, M. R. Rennó Gomes, & M. Guedes Gomes (Eds.), *Handbook of Pipeline Engineering* (pp. 1–28). Springer International Publishing. https://doi.org/10.1007/978-3-031-05735-9_18-1

Gaushell, D. J., & Darlington, H. T. (1987). Supervisory control and data acquisition. *Proceedings of the IEEE*, *75*(12), 1645–1658. Proceedings of the IEEE. https://doi.org/10.1109/PROC.1987.13932

Haakman, M., Cruz, L., Huijgens, H., & van Deursen, A. (2021). AI lifecycle models need to be revised. *Empirical Software Engineering*, *26*(5), 95. https://doi.org/10.1007/s10664-021-09993-1

Hernández Jiménez, J., Chen, Q., Nichols, J., Calhoun, C., & Sykes, S. (2017). Towards a Cyber Defense Framework for SCADA Systems Based on Power Consumption Monitoring. *Hawaii International Conference on System Sciences 2017 (HICSS-50)*. https://aisel.aisnet.org/hicss-50/eg/supply_chain_security/5

Hudgens, B., Hartner, C., Adams, B., & Regnier, E. (2019). Investing in Cyber Defense: A Value-Focused Analysis of Investment Decisions for Microgrids. *Hawaii International Conference on System Sciences 2019 (HICSS-52)*. https://aisel.aisnet.org/hicss-52/dg/cybersecurity_and_government/2

Ismail, S., Sitnikova, E., & Slay, J. (2014). Towards Developing SCADA Systems Security Measures for Critical Infrastructures against Cyber-Terrorist Attacks. In N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, & T. Sans (Eds.), *ICT Systems Security and Privacy Protection* (pp. 242–249). Springer. https://doi.org/10.1007/978-3-642-55415-5_20

Kbean, N. A. W., & Sadkhan, S. B. (2020). A Survey on Key management for SCADA. *2020 6th International Engineering Conference "Sustainable Technology and Development" (IEC)*, 97–102. https://doi.org/10.1109/IEC49899.2020.9122853

Khatib, H. A., & Zaher, A. A. (2024). IIoT-based SCADA System for Cargo Ships. *2024 15th Annual Undergraduate Research Conference on Applied Computing (URC)*, 1–6. https://doi.org/10.1109/URC62276.2024.10604525

Li, Q., Lourie, B., Nekrasov, A., & Shevlin, T. (2022). Employee Turnover and Firm Performance: Large-Sample Archival Evidence. *Management Science*, *68*(8), 5667–5683. https://doi.org/10.1287/mnsc.2021.4199

McKeen, J. D., & Smith, H. (2010). Developments in Practice XXXVII: Total Cost of Ownership. *Communications of the Association for Information Systems*, *27*(1). https://doi.org/10.17705/1CAIS.02732

McKim, C. (2023). Meaningful Member-Checking: A Structured Approach to Member-Checking. *American Journal of Qualitative Research*, *7*(2), 41–52.

Mesbah, M., & Azer, M. (2019). Cyber threats and policies for industrial control systems. *2019 International Conference on Smart Applications, Communications and Networking (SmartNets)*, 1–6. https://ieeexplore.ieee.org/abstract/document/9069761/

Nankya, M., Chataut, R., & Akl, R. (2023). Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies. *Sensors*, *23*(21), Article 21. https://doi.org/10.3390/s23218840

Patton, M. Q. (2014). *Qualitative Research & Evaluation Methods: Integrating Theory and Practice*. SAGE Publications.

Pau, M., Mirz, M., Dinkelbach, J., Mckeever, P., Ponci, F., & Monti, A. (2022). A Service Oriented Architecture for the Digitalization and Automation of Distribution Grids. *IEEE Access*, *10*, 37050–37063. IEEE Access. https://doi.org/10.1109/ACCESS.2022.3164393

Poosapati, V., Katneni, V., Manda, V. K., & Ramesh, T. L. V. (2019). Enabling Cognitive Predictive Maintenance Using Machine Learning: Approaches and Design Methodologies. In J. Wang, G. R. M. Reddy, V. K. Prasad, & V. S. Reddy (Eds.), *Soft Computing and Signal Processing* (pp. 37–45). Springer. https://doi.org/10.1007/978-981-13-3393-4_5

Protecting Upriver Dam for the Future. (2016, June 1). https://my.spokanecity.org/news/stories/2016/06/01/protecting-upriver-dam-for-the-future/

Reunamäki, R., & Fey, C. F. (2023). Remote agile: Problems, solutions, and pitfalls to avoid. *Business Horizons*, *66*(4), 505–516. https://doi.org/10.1016/j.bushor.2022.10.003

Rinta-Kahila, T., Penttinen, E., & Lyytinen, K. (2023). Getting Trapped in Technical Debt: Sociotechnical Analysis of a Legacy System's Replacement. *Management Information Systems Quarterly*, *47*(1), 1–32.

Rohmingtluanga, C., Datta, S., Sinha, N., & Ustun, T. S. (2023). SCADA based intake monitoring for improving energy management plan: Case study. *Energy Reports*, *9*, 402–410. https://doi.org/10.1016/j.egyr.2022.11.037

Sartor, M., Souza, L., Júnior, A., Rebelo, H., Cotta, K., Vianna, L., Pereira, R., & Morais, M. (2024). Assets Performance Management systems for hydroelectric power plants—A survey. *Electric Power Systems Research*, *228*, 110080. https://doi.org/10.1016/j.epsr.2023.110080

Sayed, K., & Gabbar, H. A. (2017). Chapter 18—SCADA and smart energy grid control automation. In H. A. Gabbar (Ed.), *Smart Energy Grid Engineering* (pp. 481–514). Academic Press. https://doi.org/10.1016/B978-0-12-805343-0.00018-8

Sean, W.-Y., Chu, Y.-Y., Mallu, L. L., Chen, J.-G., & Liu, H.-Y. (2020). Energy consumption analysis in wastewater treatment plants using simulation and SCADA system: Case study in northern Taiwan. *Journal of Cleaner Production*, *276*, 124248. https://doi.org/10.1016/j.jclepro.2020.124248

Sims, R. (2024). Implementing a Zero Trust Architecture For ICS/SCADA Systems. *Masters Theses & Doctoral Dissertations*. https://scholar.dsu.edu/theses/445

Slay, J., & Miller, M. (2006). A Security Architecture for SCADA Networks. *ACIS 2006 Proceedings*. https://aisel.aisnet.org/acis2006/12

Tungkagi, H., Saragih, J. D., Lubis, R. D. P., & Syamil, A. (2021). A Feasibility Study of SCADA Implementation at an Indonesian Oil Company. *Jurnal Ilmiah Mandala Education*, *7*(2), Article 2. https://doi.org/10.58258/jime.v7i2.2046

Upadhyay, D., Zaman, M., Joshi, R., & Sampalli, S. (2022). An Efficient Key Management and Multi-Layered Security Framework for SCADA Systems. *IEEE Transactions on Network and Service Management*, *19*(1), 642–660. IEEE Transactions on Network and Service Management. https://doi.org/10.1109/TNSM.2021.3104531

Upriver Dam. (2024, July 3). https://my.spokanecity.org/publicworks/water/upriver-dam/

Water Management. (2024, June 24). https://my.spokanecity.org/publicworks/water/

What Is the Purdue Model for ICS Security? (2024, May 17). https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security

Winter, R. (2014). Towards a Framework for Evidence-Based and Inductive Design in Information Systems Research. In M. Helfert, B. Donnellan, & J. Kenneally (Eds.), *Design Science: Perspectives from Europe* (pp. 1–20). Springer International Publishing. https://doi.org/10.1007/978-3-319-13936-4_1

Yadav, G., & Paul, K. (2019). PatchRank: Ordering updates for SCADA systems. *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 110–117. https://doi.org/10.1109/ETFA.2019.8869110

Appendix

Figure 1: The Purdue Model (*What Is the Purdue Model for ICS Security?*, 2024)