Advanced Engineering Days

aed.mersin.edu.tr

Analysis of security challenges in SCADA systems, a technical review on automated real-time systems

Fatmir Basholli*[1], Besjana Mema[2], Dolantina Hyka [2], Albina Basholli[3], Adisa Daberdini[4]

[1]Albanian University, Department of Engineering, Tirana, Albania, fatmir.basholli@albanianuniversity.edu.al
[2]Mediterranean University of Albania, Department of Information Technology, Albania, dolantina.hyka@umsh.edu.al; besjana.mema@umsh.edu.al
3Polytechnic University of Tirana, Fakulty of Mathematics Engineering and Physics Engineering, Tirana, Albania, e-mail: a.basholli@fimif.edu.al
4Aleksander Xhuvani University, Informatics Department, Elbasan, adisa.daberdini@uniel.edu.al

Cite this study: Basholli, F., Mema, B., Hyka, D., Basholli, A., & Daberdini, A. (2023). Analysis of security challenges in SCADA systems, a technical review on automated real-time systems. Advanced Engineering Days, 8, 18-22

Keywords
Cloud security
Critical infrastructure
Honeynet
Industrial control systems
SCADA

Abstract

Cybersecurity is a rapidly growing concern in many technological areas of the industrial economy. Supervisory Control and Data Acquisition (SCADA) systems are particularly vulnerable to cyber-attacks and must be equipped with the appropriate tools and techniques to detect attacks, accurately distinguish them from normal traffic, overcome cyberattacks when they are present and to prevent them from disrupting these systems. The three main goals of IT cybersecurity are confidentiality, integrity, and availability (CIA), but these three goals have different levels of importance in the technology industry operational (OT), where availability comes before confidentiality and integrity. Cloud cyberattacks are increasing rapidly, posing a major challenge to such systems. One of the layers of security in both IT and OT are honeypots. Honeypots are used as a security layer to mitigate attacks, known attacker techniques, and network and system vulnerabilities that attackers can exploit. In this paper, we recommend the use of SCADA honeypots for the early detection of possible malicious intrusions within a network of SCADA devices, where an analysis of SCADA honeypots gives us the opportunity to know which protocols are attacked most often, as well as the behaviors, locations and attackers' intentions. We use an ICS/SCADA honeypot called Conpot, which simulates real ICS/SCADA systems with several ICS protocols and ICS/SCADA PLCs.

Introduction

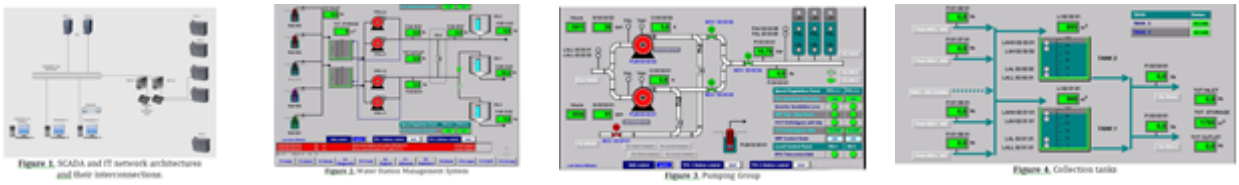
Hydroelectric plants, thermal plants, and water treatment plants are examples of traditional industrial systems that are designed to operate in highly controlled and segregated environments. However, the recent exposure of industrial control systems (ICS) to the Internet has made access and technological adaptation easier, which has led to the exploitation of security holes by attackers to launch attacks against ICS. These attacks can significantly affect the economy and national security of countries [1-3]. SCADA systems are considered a type of industrial control systems that allow users to monitor and control industrial processes locally or remotely through sensors and actuators. SCADA systems allow industrial organizations to operate critical infrastructure by controlling and monitoring real-time data and processes of various sectors, such as power generation systems, oil, gas, and manufacturing plants. SCADA systems have evolved from independent platform and infrastructure with proprietary communication mechanisms and protocols to Internet-based SCADA, with full integration into corporate information technology (IT) networks and the adoption of various Internet protocols such as Broadcast Control Protocol/Internet Protocol (TCP/IP) [4-6]. As complex industrial operations require efficient advanced environments, the idea of moving SCADA systems to the cloud has been proposed.

The paper highlights the potential impact of OT cyberattacks on national security and the economy and provides valuable insights into the various components of OT networks, including PLCs, RTUs, and HMIs.

Additionally, the study explores the use of honeypot technology as a security layer, and highlights the importance of investing in new security technologies. The paper concludes by discussing some of the most notable OT incidents and highlights the need for organizations to prioritize OT cybersecurity and take steps to prevent these attacks [7-10].

Material and Method

The common misconception of SCADA systems is that they are considered isolated and 'secure', with a lower chance of cyber-attack. Risk analysis and management methodologies are disproportionately focused on outdated SCADA systems, in which basic protocols are developed without regard to modern security requirements. SCADA systems are directly or indirectly connected to the Internet with corporate networks, user terminals and infrastructure as a result of its driving forces for integration with effective organizational platforms, work scheduling and intelligent power configurations [11-12].



SCADA systems are becoming more vulnerable to network vulnerabilities and Internet security threats as a result of rapid technical advances, changing operating frameworks and evolving business cultures. These changes and perspectives require an appropriate risk management strategy that includes Industrial Control Mechanisms, IT, Communications, access control, distribution networks and operations, as well as SCADA systems connected to the enterprise, network operators and Internet channels. Organizations should promote a safety culture for the SCADA system, procedures and regulations [13-15].

A SCADA network typically includes a central control server, a communications module, and one or more remote locations with field devices. Location-based SCADA sensor nodes continuously monitor various aspects of the electromagnetic apparatus, sending data to field monitoring systems such as Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs). Field control systems will provide digital information to a command post, where software will evaluate essential data and set allowable variable limits. This information is then sent to equipment in the field, where actions are taken to reduce various risks or improve system performance. The information is stored in the data history and displayed on the Human Machine Interface (HMI), which centrally monitors the data [16-20].

Ethernet/IP, Modbus, DNP3, Profinet, and other SCADA protocols are commonly used over large geographic areas. More than a wide area network (WAN), protocols communicate over satellites, wireless or electromagnetic systems, wireless carriers, traditional telecommunications, and/or outsourced telecommunications mediums. Due to the expansion of network connectivity and online access of assets in the SCADA system, there is a risk of multiple vulnerabilities and cyber attacks. To increase the security of SCADA networks, it is vital to implement appropriate security measures [21-23].

This study addresses and examines the following aspects of automated SCADA systems:

• What is the SCADA system, what is it for and the benefits of using this system.; • A review of relevant technologies based on the latest research and studies by designing a risk assessment framework without disturbing the environment in their future works.; • Potential risk areas of SCADA systems and risk assessments for reducing or eliminating specific risks in the system.; • Threat analysis and various cybersecurity challenges of cloud-based SCADA systems.

Results and Discussion

The application of the SCADA system and its impact on the management of Ujesjelles Kanalizime companies

What is SCADA?, Real-time process control system used for central monitoring and remote control of pumping station and urban wastewater treatment plant. SCADA is not just a hardware, nor a software. It is a concept, it is a system as a proper combination of hardware, software and protocol.

Why is SCADA needed?, The possibility to remotely collect different data in different places; The possibility to control the process remotely; The ability to create reports on the current and past state of the system; The ability to send the necessary information to engineers and operators in real time. Benefits of SCADA – s:

- *Allows an operator at the main facility to monitor and control the process that is distributed across different locations.*
- *Eliminates the need for service personnel to go to each location for inspection.*
- *Data collection.*

- *Real-time monitoring, system modification, problems, increasing equipment life, automatic report generation.*
- *Reduction of operating cost.*
- *Provides instant system performance information.*
- *Improves system efficiency and performance.*
- *Reduces the number of worker hours (labor cost) needed for defects or services.*
- *Compliance of facilities with regulatory agencies through automatic report generation.*

Practical implementation of SCADA at a Pump Station

The Station Control System, the local SCADA is composed of two identical workstations (ws01 & ws02) with additional software that allows the completion of the operating station. The architecture of the SCADA System is client / server. The server is responsible for managing and maintaining the underlying data where the process data is kept. Customer access process data through service calls. SCADA at the ADM building has workstation ws03 which exchanges data with TPS_PLC through level 2 Ethernet LAN, the protocol it connects to is TCP / IP.

Telecontrol

The telecontrol system is composed of appropriate software and electronic equipment in order to ensure the safe and reliable transfer of data for commands, measurements, statuses and alarm signals between the control center and individual units.

SCADA - Wastewater Treatment Plant (application project)

PLC1 is located in the Operations Building and is responsible for:
Cooling and Heating System; UPS.
PLC2 is located at the Inlet Pump Station and is responsible for:
Inlet Pumps 1, 2; Fine Shutters 1,2; Spiral Pump; MCC fan
PLC3 is located in the Operations Building and is responsible for:
The first phase of aeration of the Baths; the second phase of aeration of the Baths; Water Service System; Flow Circulation Measurement. The Control System with automation at the highest level ensures that plant operators receive all the relevant information and have a reflection of the current state of all plant processes in the control room.

Grills. The cleaning of the grills takes place in 2 ways, where the first way is the control through the minimum and maximum level of water that starts the cleaning cycle of the grills; while the second mode is the automatic mode where time control is a priority since the cleaning cycle starts automatically. Aeration of the treatment tanks, the Operator will have the possibility to choose a pre-set aeration program for different cases of the current load of dirty water (50%, 75% and 100%) by means of the SCADA system [24-26].

Figure 5. Position of instruments for control and monitoring

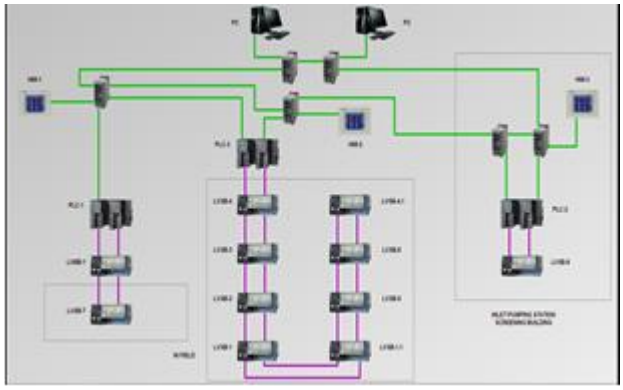


Figure 6. Computer network of SCADA - s

Conclusion

SCADA is a computer-based system for industrial process control, which collects real-time data from remote locations. Connecting SCADA equipment to the Internet presents security vulnerabilities where various cyber attacks target the system's network. This research proposed a study and an analysis of vulnerabilities and cyber attacks affecting the security of SCADA systems, moving the traditional system to the cloud environment, because

SCADA systems depend on real-time industrial operations. Organizations can use honeypots, which are decoy systems designed to lure attackers away from real assets, to gather information about the types of attacks being launched against their systems.

References

1. Cai, N., Wang, J., & Yu, X. (2008, July). SCADA system security: Complexity, history and new developments. In 2008 6th IEEE International Conference on Industrial Informatics, 569-574. https://doi.org/10.1109/INDIN.2008.4618165
2. Mema, B., & Basholli, F. (2023). Internet of things in the development of future businesses in Albania. Advanced Engineering Science, 3, 196-205.
3. Kelly, C., Pitropakis, N., Mylonas, A., McKeown, S., & Buchanan, W. J. (2021). A comparative analysis of honeypots on different cloud platforms. Sensors, 21(7), 2433. https://doi.org/10.3390/s21072433
4. Basholli, F., Daberdinİ, A., & Basholli, A. (2023). Detection and prevention of intrusions into computer systems. Advanced Engineering Days (AED), 6, 138-141.
5. Zeng, P., & Zhou, P. (2018). Intrusion detection in SCADA system: A survey. In Intelligent Computing and Internet of Things: First International Conference on Intelligent Manufacturing and Internet of Things and 5th International Conference on Computing for Sustainable Energy and Environment, IMIOT and ICSEE 2018, Chongqing, China, September 21-23, 2018, Proceedings, Part II 5 (pp. 342-351). Springer Singapore.
6. Basholli, F., Mezini, R., & Basholli, A. (2023). Security in the components of information systems. Advanced Engineering Days (AED), 7, 185-187.
7. Nazir, S., Patel, S., & Patel, D. (2020). Cloud-based autonomic computing framework for securing SCADA systems. In Innovations, algorithms, and applications in cognitive informatics and natural intelligence, 276-297. https://doi.org/10.4018/978-1-7998-3038-2.ch013
8. Demertzis, K., & Iliadis, L. (2018). A computational intelligence system identifying cyber-attacks on smart energy grids. Modern discrete mathematics and analysis: with applications in cryptography, information systems and modeling, 97-116. https://doi.org/10.1007/978-3-319-74325-7_5
9. Tariq, N., Asim, M., & Khan, F. A. (2019). Securing SCADA-based critical infrastructures: Challenges and open issues. Procedia computer science, 155, 612-617. https://doi.org/10.1016/j.procs.2019.08.086
10. Rubio, J. E., Alcaraz, C., Roman, R., & Lopez, J. (2019). Current cyber-defense trends in industrial control systems. Computers & Security, 87, 101561. https://doi.org/10.1016/j.cose.2019.06.015
11. Mema, B., Basholli, F., Xhafaj, D., Basholli, A., & Hyka, D. (2023). Internet of things in the development of future businesses in Albania. Advanced Engineering Days, 7, 139-141
12. Molle, M., Raithel, U., Kraemer, D., Graß, N., Söllner, M., & Aßmuth, A. (2019). Security of cloud services with low-performance devices in critical infrastructures. CLOUD COMPUTING 2019, 98.
13. Zhang, S., Luo, X., & Litvinov, E. (2021). Serverless computing for cloud-based power grid emergency generation dispatch. International Journal of Electrical Power & Energy Systems, 124, 106366. https://doi.org/10.1016/j.ijepes.2020.106366
14. Shen, J., Xu, J., Cai, K., & Ji, Y. (2021). Retracted: Access Point Authentication Scheme of SCADA System Based on Cloud Computing Technology. In Journal of Physics: Conference Series, 1748(2), 022010. https://doi.org/10.1088/1742-6596/1748/2/022010
15. Basholli, F., Hyka, D., Basholli, A., Daberdini, A., & Mema, B. (2023). Analysis of cyber-attacks through simulation. Advanced Engineering Days (AED), 7, 120-122.
16. Yang, X., Yuan, J., Yang, H., Kong, Y., Zhang, H., & Zhao, J. (2023). A Highly Interactive Honeypot-Based Approach to Network Threat Management. Future Internet, 15(4), 127. https://doi.org/10.3390/fi15040127
17. Hyka, D., & Basholli, F. (2023). Health care cyber security: Albania case study. Advanced Engineering Days (AED), 6, 121-123.
18. Mellado, J., & Núñez, F. (2022). Design of an IoT-PLC: A containerized programmable logical controller for the industry 4.0. Journal of Industrial Information Integration, 25, 100250. https://doi.org/10.1016/j.jii.2021.100250
19. Yang, Y. S., Lee, S. H., Chen, W. C., Yang, C. S., Huang, Y. M., & Hou, T. W. (2022). Securing SCADA Energy Management System under DDos attacks using token verification approach. Applied Sciences, 12(1), 530. https://doi.org/10.3390/app12010530
20. Harizaj, M., Bisha, I., & Basholli, F. (2023). IOT integration of electric vehicle charging infrastructure. Advanced Engineering Days (AED), 6, 152-155.
21. Kumar, A., Bhushan, B., Malik, A., & Kumar, R. (2022). Protocols, solutions, and testbeds for cyber-attack prevention in industrial SCADA systems. Internet of Things and Analytics for Agriculture, Volume 3, 355-380. https://doi.org/10.1007/978-981-16-6210-2_17
22. Daberdini, A., Basholli, F., Metaj, N., & Skenderaj, E. (2022). Cyber security in mail with Fortiweb and Fortinet for companies and institutions. Advanced Engineering Days (AED), 5, 81-83.

23. Polat, H., Türkoğlu, M., Polat, O., & Şengür, A. (2022). A novel approach for accurate detection of the DDoS attacks in SDN-based SCADA systems based on deep recurrent neural networks. Expert Systems with Applications, 197, 116748. https://doi.org/10.1016/j.eswa.2022.116748
24. Hyka, D., Hyra, A., Basholli, F., Mema, B., & Basholli, A. (2023). Data security in public and private administration: Challenges, trends, and effective protection in the era of digitalization. Advanced Engineering Days (AED), 7, 125-127.
25. Franco, J., Aris, A., Canberk, B., & Uluagac, A. S. (2021). A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems. IEEE Communications Surveys & Tutorials, 23(4), 2351-2383. https://doi.org/10.1109/COMST.2021.3106669
26. Basholli, A., Mema, B., Basholli, F., Hyka, D., & Salillari, D. (2023). The role of education in cyber hygiene. Advanced Engineering Days (AED), 7, 178-181.