BUXORO DAVLAT TEXNIKA UNIVERSITETI (BUXORO TABIIY RESURSLARNI BOSHQARISH INSTITUTI) (O‘ZBEKISTON),

BIRLASHGAN MILLATLAR TASHKILOTINING “QISHLOQ XO‘JALIGI VA OZIQ OVQAT” TASHKILOTI (FAO),

GUMBOLT NOMIDAGI BERLIN UNIVERSITETI (GERMANIYA),

PRESOV UNIVERSITETI (SLOVAKIYA),

VALENSIYA POLITEXNIKA UNIVERSITETI (ISPANIYA),

ZALF AGROTEXNOLOGIYALAR ILMIY TADQIQOT MARKAZI (GERMANIYA),

INTI XALQARO UNIVERSITETI (MALAYZIYA),

HERRIOT WATT UNIVERSITETI (MALAYZIYA)

“YASHIL ENERGETIKA VA UNING QISHLOQ VA SUV XO’JALIGIDAGI O’RNI” MAVZUSIDAGI XALQARO ILMIY VA ILMIY-TEXNIKAVIY ANJUMANI

MATERIALLAR TO‘PLAMI

29-30-aprel, 2025-yil

ISSN: 978-9910-10-082-6
UO‘K 556.182:551.5(08)
BBK 26.222+26.236
«DURDONA» Nashriyoti

“Yashil energetika va uning qishloq va suv xo’jaligidagi o’rni” mavzusidagi xalqaro ilmiy va ilmiy-texnikaviy anjumani materiallar to‘plami (2025-yil 29-30-aprel) -B.: Buxoro davlat texnika universiteti (Buxoro tabiiy resurslarni boshqarish instituti), 2025.

To‘plamga kiritilgan tezislardagi ma’lumotlarning haqqoniyligi va iqtiboslarning tog‘riligiga mualliflar mas’uldir.

Elektron pochta manzili: buxtimi@mail.ru

7. Pirus D. // Proceedings of the 4th International Topical Meeting NPIC&IMIT 2004. Colombus, September, 19–22, 2004. P. 1165–1172.

8. “Suv ta’minoti va oqava suvlari tizimlarini avtomatlashtirish” Ubaydullayeva D.R., Xayitov A.N., Abdullayev H.H., Sharifov H.Sh. Darslik-2020

9. "Pump Handbook" by Igor J. Karassik, Joseph P. Messina, and Paul Cooper

UDK: 004.7:004.42(045)

CYBERSECURITY FOR SCADA SYSTEMS

Zarina Khaydarova Ruzimurodovna
assistant, Department of Automation and Management of Production Processes, Bukhara Institute of Natural Resources Management of the NRU “TIIAME”
E-mail: zarinakh317@gmail.com

Annotation: *This article highlights the increasing need for cyber security in SCADA systems due to the growing threats and interconnectedness of industrial systems. It also provides an overview of best practices and regulatory frameworks to guide organizations in strengthening the security of their critical infrastructure.*

Keywords: *SCADA, industrial operations, real-time data, remote monitoring, IT integration*

Introduction. Supervisory Control and Data Acquisition (SCADA) systems are crucial in controlling industrial processes such as electricity generation, water treatment, and manufacturing. These systems have evolved over time, integrating IT networks and communication protocols for enhanced efficiency and monitoring. However, as these systems are increasingly connected to broader networks, they have become attractive targets for cyber attacks. This article discusses the significance of cybersecurity in SCADA systems, potential threats, and best practices for securing these critical infrastructures.

In the 1960s, when the first computer-based supervisory control and data acquisition systems (SCADA) were being developed, there was no cultural concept of needing to provide any particular protective measures to keep such systems safe from intentional attacks.

SCADA systems monitor and control various industrial operations. These systems provide operators with real-time data, enabling remote monitoring and control of processes that are geographically dispersed. The integration of SCADA with corporate IT systems allows for enhanced data analytics and system management, but it also opens the door for cybersecurity vulnerabilities.

Supervisory control and data acquisition (SCADA) systems are used to monitor and remotely control critical industrial processes, such as gas pipelines, electric power transmission, and potable water distribution/delivery. As such, SCADA systems are important to our daily lives, even though most people never see them or even know of their existence.

To properly understand what SCADA systems are, how they came to be, and why they are designed the way they are, one needs a basic understanding of the history of SCADA system development. It is also helpful to know why things have evolved and what factors have pushed this evolution. Computer-based supervisory control systems were introduced in the 1960s, and the first such systems were based on the mainframe computer technology available at the time.

These systems were not yet called SCADA systems, as that particular acronym did not come into general use until the 1980s. SCADA systems were developed to replace older technologies (e.g., tone telemetry) and to provide features and functions that required computational and logical capabilities. The incorporation of a computer into telemetry systems provided a means for manipulating, processing, storing, and presenting data that could not be provided with previous technologies.

Best Practices for Securing SCADA Systems

To improve SCADA system security, organizations should follow several best practices:

Use of Firewalls: Firewalls should be implemented between SCADA networks and external networks to prevent unauthorized access.

Encryption: Encrypting communication channels within SCADA systems ensures data confidentiality and integrity.

User Authentication: Multi-factor authentication (MFA) should be used to ensure that only authorized users can access SCADA systems.

Vendor Security: Organizations must vet and ensure that third-party vendors follow proper security practices when providing SCADA system components.

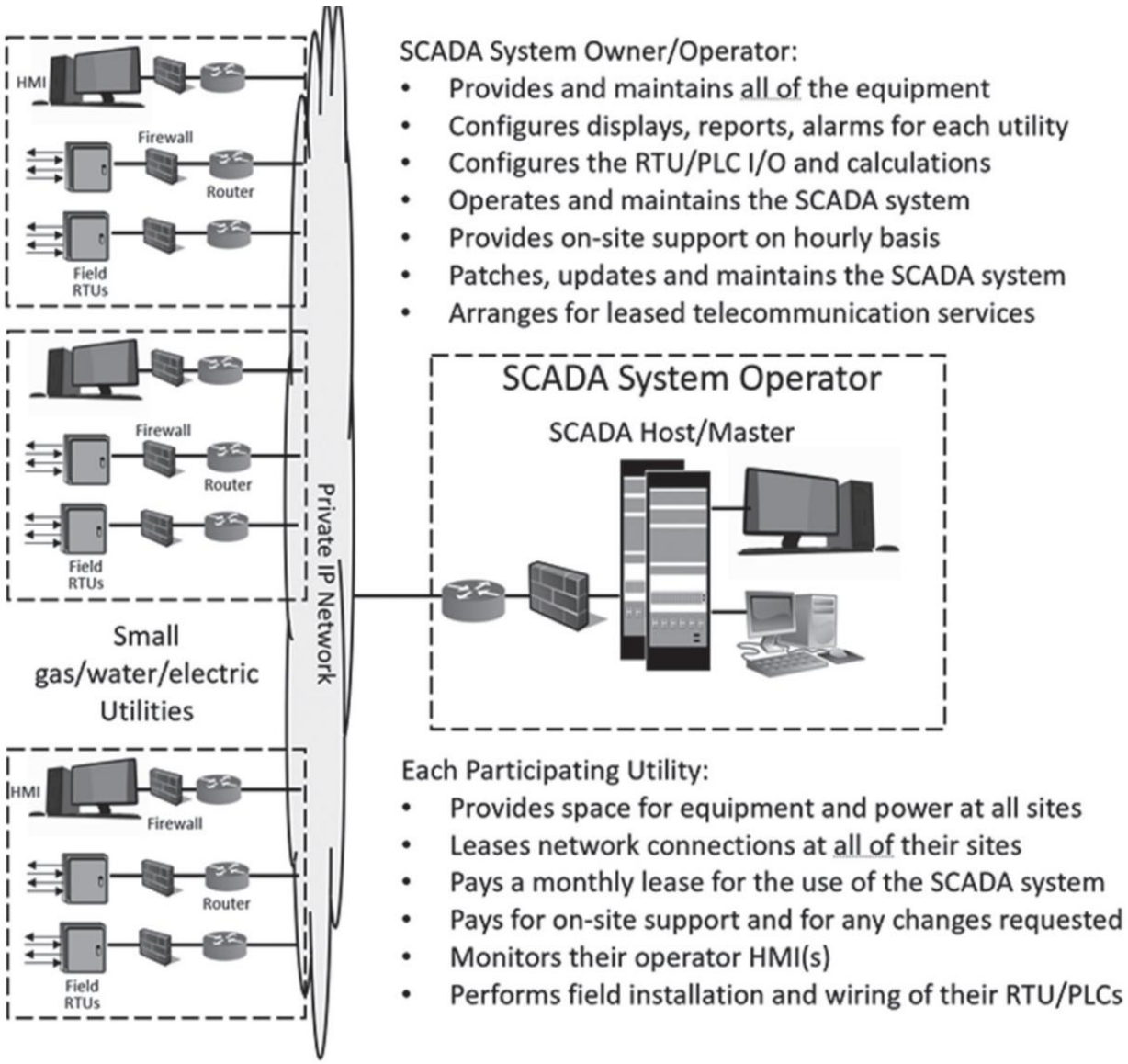

Fig. 1 SCADA as a service

As SCADA systems evolve, new threats are emerging, particularly with the rise of **Industrial Internet of Things (IoT)** and **5G networks**. The connectivity of devices and sensors opens new attack vectors for cybercriminals. Additionally, the rise of artificial intelligence (AI) and machine learning (ML) could be used by attackers to conduct more sophisticated and adaptive attacks on SCADA systems. To counter these emerging threats, it is critical for organizations to stay informed about the latest security trends and continually adapt their cybersecurity practices.

Conclusion.Securing SCADA systems is paramount to the safe operation of critical infrastructure. As threats continue to evolve, organizations must adopt comprehensive cybersecurity measures tailored to the unique needs of SCADA systems. By leveraging the right technologies, frameworks, and best practices, industries can enhance the resilience of SCADA systems and reduce the risk of potentially catastrophic cyber attacks.

References

1. **National Institute of Standards and Technology (NIST)**. (2015). *NIST SP 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security*. National Institute of Standards and Technology.

2. **International Electrotechnical Commission (IEC)**. (2018). *IEC 62443-3-3: Industrial Communication Networks-Network and System Security*. IEC.

3. **ISO/IEC 27001**. (2013). *Information Technology-Security Techniques-Information Security Management Systems-Requirements*. International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

4. Хайдарова, З.Р., Убайдуллаева, Ш.Р., & Шарифов, Х.Ш. (2020). К вопросу автоматизированного управления горячим водоснабжением в фермерском хозяйстве с использованием возобновляемых источников энергии. *The Way of Science International scientific journal*, 2(72), 39-42.

5. Juraev, F., Khamroyev, G., Khaydarova, Z., Khamroyev, I., & Ibodov, I. (2021). The usage of a combined machine in the process of preparing the land for planting. *E3S Web of Conferences*, 264, 04092. https://doi.org/10.1051/e3sconf/202126404092

6. Салиева, О. К., & Хайдарова, З. Р. (2017). К вопросу анализа структурных функциональных методов проектирования информационной системы. *Материалы конференции «Современные материалы, техника и технология»*, 335-337.

7. Файзиев, Ш. И., Едгорова, О. О., & Хайдарова, З. Р. (2016). Синтез помехоустойчивых алгоритмов адаптивного управления динамическими объектами. *Материалы конференции «Будущее науки-2016»*, 78-80.

8. Файзиев, Ш. И., Ахмедов, А. А., & Хайдарова, З. Р. (2016). Алгоритмы оценивания состояния динамических систем. *Материалы конференции «Будущее науки-2016»*, 76-78.

УДК 004.891

SCADA-СИСТЕМЫ В АВТОМАТИЗАЦИИ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

Интанкина Екатерина
стажёр кафедры «Управление и,автоматизация процессов производства»,Бухарского института управления природными ресурсами
E-mail:intankinakatya@gmail.com

Аннотация: *В данной статье выполнен обзор SCADA - систем, используемых в современных автоматизированных системах управления технологическими процессами. В настоящее время тематика искусственного интеллекта охватывает огромный перечень научных направлений, начиная с таких задач общего характера, как обучение и восприятие (программы решения интеллектуальных задач и системы, основанные на знаниях), заканчивая специальными задачами (нейроподобные структуры, интеллектуальное программирование и интеллектуальные системы) .*

Ключевые слова: *SCADA-система, автоматизированное управление, АСУТП.*

При решении современных задач управления сложными многопараметрическими и сильносвязанными системами, объектами, производственными и технологическими процессами приходится сталкиваться с решением неформализуемых либо трудноформализуемых задач, поэтому всем новейшим информационно-управляющим системам должно быть присуще свойство интеллектуальности.

В настоящее время одним из направлений и весьма эффективной технологией автоматизированного управления динамическими системами во многих отраслях промышленности являются системы класса SCADA (Supervisory Control And Data Acquisition, диспетчерское управление и сбор данных) [2, 3].