MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susţinere
Şef departament:
FIODOROV Ion dr., conf.univ.

„___” _____ 2025

METODE DE IDENTIFICARE A VULNERABILITĂȚILOR SISTEMELOR SCADA

Proiect de master

Student: _____ **Rusu Constantin, SI-231M**

Coordonator: _____ **Putere Alexandru, lect.univ.**

Consultant: _____ **Cojocaru Svetlana, asist.univ.**

Chişinău, 2025

REZUMAT

Această lucrare examinează vulnerabilitățile sistemelor SCADA, esențiale pentru infrastructurile critice, și propune soluții pentru sporirea securității acestora. Studiul se axează pe vulnerabilitățile specifice acestor sisteme și pe tehnicile de evaluare a riscurilor, subliniind importanța unor măsuri avansate de protecție, cum ar fi autentificarea și monitorizarea continuă. Sunt analizate metodele de testare a securității și simulările utilizate pentru identificarea riscurilor, precum și recomandări pentru implementarea tehnologiilor moderne de securitate.

Lucrarea evidențiază strategii de protecție, incluzând măsuri de răspuns la incidente cibernetice și soluții pentru securizarea sistemelor SCADA, care sprijină protecția infrastructurilor critice. Rezultatele și recomandările pot fi aplicate de organizațiile interesate să îmbunătățească securitatea acestor sisteme și să contribuie la securitatea națională. Aceste soluții sunt esențiale pentru profesioniștii din domeniu și autoritățile responsabile de protecția infrastructurilor esențiale.

ABSTRACT

This master's thesis, is showing a detailed analysis that includes, vulnerabilities of SCADA systems, which are essential for critical infrastructures, and proposes solutions to enhance their security. The study focuses on the specific vulnerabilities of these systems and on risk assessment techniques, highlighting the importance of advanced protection measures such as authentication and continuous monitoring. It examines security testing methods and simulations used to identify risks, as well as recommendations for implementing modern security technologies.

This research paper, presents protection strategies, including measures for responding to cyber incidents and solutions for securing SCADA systems, which support the protection of critical infrastructures. The results and recommendations can be applied by organizations seeking to improve the security of these systems and contribute to national security. These solutions are essential for professionals in the field and authorities responsible for safeguarding critical infrastructures

CUPRINS

INTRODUCERE

În contextul digitalizării accelerate și al globalizării economice, infrastructurile critice au devenit pilonii de bază ai funcționării societăților moderne. Aceste infrastructuri, precum cele din domeniile energiei, apei, transporturilor și telecomunicațiilor, asigură servicii esențiale pentru viața de zi cu zi și pentru securitatea națională. Sistemele SCADA (Supervisory Control and Data Acquisition) sunt componente tehnologice indispensabile pentru monitorizarea și controlul acestor infrastructuri. Ele permit operatorilor să supravegheze și să gestioneze în timp real procesele industriale la scară largă, asigurând funcționarea eficientă și continuă a unor servicii fundamentale pentru populație și economie.

Cu toate acestea, dezvoltarea și integrarea SCADA în rețelele de infrastructuri critice aduce cu sine o serie de provocări majore în ceea ce privește securitatea cibernetică. Fiind inițial concepute pentru a funcționa în medii izolate, sistemele SCADA au fost ulterior integrate în rețele publice și în Internet, ceea ce le-a expus unor vulnerabilități cibernetice semnificative. Atacurile cibernetice împotriva infrastructurilor critice au devenit o amenințare reală, capabilă să destabilizeze servicii esențiale, să cauzeze pierderi economice substanțiale și, în cazuri extreme, să pună în pericol viața oamenilor.

Un exemplu notabil care evidențiază impactul devastator al atacurilor cibernetice asupra infrastructurilor critice este incidentul Stuxnet din 2010. Acest atac a vizat un sistem SCADA utilizat în cadrul programului nuclear iranian, distrugând echipamente esențiale fără a necesita o intervenție militară directă. Acest caz a atras atenția globală asupra vulnerabilităților sistemelor SCADA și a deschis calea pentru o mai mare conștientizare a riscurilor pe care aceste sisteme le implică, dacă nu sunt protejate corespunzător.

În ciuda acestor amenințări tot mai mari, multe dintre sistemele SCADA utilizate în infrastructurile critice sunt în continuare expuse riscurilor. Lipsa criptării, utilizarea unor protocoale de comunicație nesecurizate, precum și software-urile învechite, toate contribuie la vulnerabilitatea acestor sisteme. În plus, din cauza naturii complexe și a diversității infrastructurilor critice, vulnerabilitățile sunt adesea greu de identificat și de remediat în mod eficient. În acest context, protejarea sistemelor SCADA devine nu doar o prioritate pentru securitatea cibernetică, ci și o problemă de siguranță națională.

Scopul acestei cercetări este de a examina vulnerabilitățile specifice sistemelor SCADA utilizate în infrastructurile critice și de a evalua impactul acestora asupra securității naționale. Studiul va aborda natura vulnerabilităților cibernetice din aceste sisteme, metodele folosite de atacatori pentru a exploata aceste breșe și soluțiile disponibile pentru a le preveni și mitiga. De asemenea, cercetarea va sublinia măsurile de securitate necesare pentru protejarea infrastructurilor critice, având în vedere complexitatea amenințărilor și evoluția rapidă a tehnologiilor cibernetice.

Rezultatele cercetării vor contribui la o mai bună înțelegere a riscurilor asociate cu sistemele SCADA și vor oferi recomandări concrete pentru consolidarea securității acestor infrastructuri. Prin urmare, acest studiu va sprijini atât operatorii de infrastructuri critice, cât și factorii de decizie politică în dezvoltarea

unor strategii eficiente de apărare cibernetică. Astfel, protejarea sistemelor SCADA devine o măsură esențială nu doar pentru funcționarea infrastructurilor critice, dar și pentru menținerea securității și stabilității naționale într-un peisaj geopolitic tot mai volatil și complex.

Cercetarea vulnerabilităților sistemelor SCADA reprezintă un pas fundamental în asigurarea securității infrastructurilor critice, având un impact direct asupra protecției naționale și internaționale. Această lucrare își propune să contribuie la consolidarea securității cibernetice prin identificarea și remedierea vulnerabilităților critice din aceste sisteme complexe.

BIBLIOGRAFIE

[1] G. Yadav and K. Paul, “Architecture and Security of SCADA Systems: A Review,” Oct. 19, 2024, *arXiv*: arXiv:2001.02925. doi: 10.48550/arXiv.2001.02925.

[2] M. Smurthwaite and M. Bhattacharya, “Convergence of IT and SCADA: Associated Security Threats and Vulnerabilities,” *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 790, no. 1, p. 012041, Oct. 20, 2024, doi: 10.1088/1757-899X/790/1/012041.

[3] W. T. Shaw, *Cybersecurity for SCADA Systems*, 2nd ed., 1 online resource vols. PennWell Books, 2021.

[4] William.T.Shaw 1., *Cybersecurity for SCADA Systems*. 2021.

[5] “Ghid SCADA Ver. 2.0 | PDF,” Scribd. Accessed: Jan. 14, 2025. [Online]. Available: https://ro.scribd.com/document/539107882/Ghid-SCADA-ver-2-0

[6] Radvanovsky, R., & Brodsky, J. 9., *Handbook of SCADA/Control Systems Security. CRC Press*. 2013.

[7] Knapp, E. D., & Langill, J. T 8., *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Syngress*. 2014.

[8] “ÎS Moldelectrica. Starea sistemului energetic al RM.” Accessed: Jan. 14, 2025. [Online]. Available: https://www.moldelectrica.md/ro/activity/system_state

[9] “(PDF) IIS branch-and-cut for joint chance-constrained programs with random technology matrices,” ResearchGate. Accessed: Jan. 14, 2025. [Online]. Available: https://www.researchgate.net/publication/228847498_IIS_branch-and-cut_for_joint_chance-constrained_programs_with_random_technology_matrices

[10] “Prioritățile de dezvoltare a sectorului energetic, discutate de ministrul Victor Parlicov cu partenerii de dezvoltare,” Ministerul energiei. Accessed: Jan. 14, 2025. [Online]. Available: https://energie.gov.md/ro/content/prioritatile-de-dezvoltare-sectorului-energetic-discutate-de-ministrul-victor-parlicov-cu

[11] “Republica Moldova va beneficia de proiect-pilot al Băncii Mondiale dedicat ecurității cibernetice în sectorul energetic,” Ministerul energiei. Accessed: Jan. 14, 2025. [Online]. Available: https://energie.gov.md/ro/content/republica-moldova-va-beneficia-de-proiect-pilot-al-bancii-mondiale-dedicat-ecuritatii

[12] Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H., *SCADA Security in the Light of Cyber-Warfare. Computers & Security, 31(4), 418-436.* 2012.

[13] Igure, V. M., Laughter, S. A., & Williams, R. D., *Security Issues in SCADA Networks. Computers & Security, 25(7), 498-506.* 2006.

[14] “Sistemele de control industrial. Vulnerabilităţi şi scenarii,” Revista Intelligence. Accessed: Jan. 14, 2025. [Online]. Available: https://intelligence.sri.ro/sistemele-de-control-industrial-vulnerabilitati-si-scenarii/

[15] Karnouskos, S., *Stuxnet Worm Impact on Industrial Cyber-Physical System Security. In Proceedings of the 37th Annual Conference of the IEEE Industrial Electronics Society*. 2011.

[16] “Vulnerabilitățile sistemelor de control industrial cresc - Siguranta pe net.” Accessed: Jan. 14, 2025. [Online]. Available: https://www.sigurantapenet.ro/noutati/vulnerabilitatile-sistemelor-de-control-industrial-crec