***Kód tématu:*** 404-BTSM-CZ

# Metodika kybernetické bezpečnosti robotických systémů v prostředí Průmyslu 4.0/5.0

***Školitel:*** doc. Ing.  Milan Navrátil, Ph.D.

***Konzultant:*** Ing. Lukáš Králík, Ph.D.

***Ústav fakulty***: Ústav elektroniky a měření

***Studijní program:*** Bezpečnostní technologie, systémy a management

***Anotace:***

Práce se zaměřuje na návrh a experimentální ověření metodiky kybernetické bezpečnosti robotických systémů v prostředí Průmyslu 4.0/5.0, kde dochází ke konvergenci IT/OT a k růstu napadené plochy výrobních systémů. Jádrem výzkumu bude systematická analýza hrozeb a zranitelností robotických systémů se zvláštním důrazem na komunikační řetězec PLC–robot–HMI–senzory, typické útoky na řídicí systémy a specifika kolaborativních robotů (dopady na bezpečnost osob i provoz). Na základě vytvořeného threat modelu bude navržena bezpečnostní architektura pro OT (segmentace, řízení identit, princip nejmenších oprávnění, monitorování a detekce incidentů) s využitím principů Zero Trust a doporučení relevantních standardů pro průmyslové automatizační a řídicí systémy. Součástí výstupů bude metodika zabezpečení (postupy, kontrolní body, doporučené technické a organizační kontroly) a sada experimentů na robotické lince, které ověří účinnost navržených opatření vůči vybraným scénářům útoků i provozním omezením OT.

***Literatura:***

[1] Sumit Kumar a Harsh Vardhan. Cyber security of OT networks: A tutorial and overview. arXiv [online]. 2025. Dostupné z: https://doi.org/10.48550/arXiv.2502.14017

[2] Manar Alanazi; Abdun Mahmood; Mohammad Jabed Morshed Chowdhury. SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. Computers & Security. 2023, 125, 103028. Dostupné z: https://doi.org/10.1016/j.cose.2022.103028

[3] Rajiv Raich; Anagha Raich; Nandkishor Kinhekar. Securing the Convergence of IT and OT Networks in Cyber Physical System: Policy, Architecture and Implementation Challenges. ITM Web of Conferences [online]. 2025, 79, 01005. Dostupné z: https://doi.org/10.1051/itmconf/20257901005

[4] Marianna Lezzi; Mariangela Lazoi; Angelo Corallo. Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry. 2018, 103, 97–110. Dostupné z: https://doi.org/10.1016/j.compind.2018.09.004

[5] Azfar Khalid; Pierre T. Kirisci; Zeashan Hameed Khan; Zied Ghrairi; K.-D. Thoben; Jürgen Pannek. Security framework for industrial collaborative robotic cyber-physical systems. Computers in Industry. 2018, 97, 132–145. Dostupné z: https://doi.org/10.1016/j.compind.2018.02.009

[6] Keith Stouffer; Michael Pease; CheeYee Tang; Timothy Zimmerman; Victoria Pillitteri; Suzanne Lightman; Adam Hahn; Stephanie Saravia; Aslam Sherule; Michael Thompson. Guide to Operational Technology (OT) Security (NIST SP 800-82r3). Gaithersburg: National Institute of Standards and Technology, 2023 [online]. Dostupné z: https://doi.org/10.6028/NIST.SP.800-82r3

[7] International Society of Automation. ISA/IEC 62443 Series of Standards [online]. Dostupné z: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[8] Janusz Pochmara a Aleksandra Świetlicka. Cybersecurity of Industrial Systems—A 2023 Report. Electronics [online]. 2024, 13(7), 1191. Dostupné z: https://doi.org/10.3390/electronics13071191