UNIVERSITATEA TEHNICĂ
„GHEORGHE ASACHI" DIN IAȘI
REGISTRATURA
-26-
Nr. 45632 / 02.11.2026

Tematică de concurs - poziția 1 (PRISM): Cercetător științific gradul III

1. Inteligență artificială și învățare automată pentru procesarea datelor radar

1. Metode de învățare automată și arhitecturi de rețele neuronale pentru detecția, clasificarea și recunoașterea obiectelor pe baza datelor radar.
2. Tehnici de extragere și selecție a caracteristicilor, clasificare și detectare a anomaliilor în date complexe.
3. Optimizarea și evaluarea modelelor AI/ML în funcție de acuratețe, robustețe și eficiență computațională.

2. Generarea datelor sintetice și tehnologii Digital Twin

1. Metode de simulare și generare a datelor radar sintetice pentru scenarii reale și virtuale.
2. Arhitecturi Digital Twin și mecanisme de sincronizare, corelare și aliniere a datelor reale și sintetice.
3. Utilizarea modelelor generative pentru augmentarea datelor și îmbunătățirea generalizării modelelor inteligente.

3. Securitatea și robustețea sistemelor inteligente

1. Identificarea anomaliilor și evaluarea comportamentului sistemelor radar prin metode AI/ML.
2. Analiza vulnerabilităților și evaluarea riscurilor de securitate în sisteme inteligente și medii virtualizate.
3. Metode de creștere a robusteții și fiabilității modelelor inteligente în condiții de funcționare variabile.

4. Validarea experimentală și coordonarea activităților de cercetare

1. Metodologii de testare și validare a modelelor AI/ML în medii de simulare și Digital Twin.
2. Evaluarea comparativă a rezultatelor experimentale și definirea indicatorilor de performanță.
3. Coordonarea activităților de cercetare, interpretarea rezultatelor și diseminarea contribuțiilor științifice.

Bibliografie – PRISM, Poziția 1

1. M. A. Richards, Fundamentals of Radar Signal Processing, 2nd Edition, McGraw-Hill, 2014. Available: https://www.mheducation.com/highered/mhp/product/fundamentals-radar-signal-processing-second-edition.html.

2. Y. Zhou et al., "Towards Deep Radar Perception for Autonomous Driving: Datasets, Methods, and Challenges," Sensors, vol. 22, no. 11, Art. 4208, 2022. Available: https://doi.org/10.3390/s22114208.
3. Z. Geng, H. Yan, J. Zhang, and D. Zhu, "Deep-Learning for Radar: A Survey," IEEE Access, vol. 9, pp. 141800–141818, 2021. Available: https://doi.org/10.1109/ACCESS.2021.3119561.
4. F. Tao, H. Zhang, A. Liu, and A. Y. C. Nee, "Digital Twin in Industry: State-of-the-Art," IEEE Transactions on Industrial Informatics, vol. 15, no. 4, pp. 2405–2415, 2019. Available: https://doi.org/10.1109/TII.2018.2873186.
5. F. Tao, Q. Qi, L. Wang, and A. Y. C. Nee, "Digital Twins and Cyber–Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison," Engineering, vol. 5, no. 4, pp. 653–661, 2019. Available: https://doi.org/10.1016/j.eng.2019.01.014.
6. H. Mun et al., "A Comprehensive Survey on Digital Twin: Focusing on Security Threats and Requirements," IEEE Access, 2025. Available: https://doi.org/10.1109/ACCESS.2025.3563621.
7. ISO, ISO 21448:2022 – Road Vehicles – Safety of the Intended Functionality (SOTIF), International Organization for Standardization, 2022. Available: https://www.iso.org/standard/77490.html.

Tematică de concurs - poziția 3 (PRISM): Asistent de cercetare științifică

1. Arhitecturi hardware și software pentru sisteme embedded

1. Principii de proiectare și organizare a sistemelor embedded și a sistemelor cibernetico-fizice.
2. Arhitecturi hardware și software pentru sisteme automotive și aerospace, microcontrolere și unități electronice de control (ECU).
3. Sisteme de operare în timp real, constrângeri temporale și cerințe de fiabilitate.

2. Rețele și protocoale de comunicație pentru sisteme automotive

1. Protocoale de comunicație specifice sistemelor embedded: CAN, CAN FD, LIN, FlexRay și Automotive Ethernet.
2. Arhitecturi de comunicație și integrarea senzorilor și subsistemelor electronice.
3. Standardul AUTOSAR și mecanisme de interoperabilitate între componentele sistemelor automotive.

3. Testarea și validarea sistemelor tehnice

1. Metodologii de testare și validare a sistemelor embedded hardware și software.
2. Tehnici de testare Model-in-the-Loop (MiL), Software-in-the-Loop (SiL) și Hardware-in-the-Loop (HiL).
3. Standarde de siguranță funcțională și procese de verificare și validare pentru sisteme automotive.

4. Integrarea și evaluarea sistemelor radar

1. Principii de funcționare și integrare a senzorilor radar în arhitecturile sistemelor automotive.
2. Analiza interfețelor hardware și software și verificarea comunicației dintre subsisteme.
3. Evaluarea experimentală a funcționalității, performanței și conformității soluțiilor integrate cu cerințele tehnice.

Bibliografie – PRISM, Poziția 3

1. E. A. Lee and S. A. Seshia, Introduction to Embedded Systems: A Cyber-Physical Systems Approach, 2nd Edition, MIT Press, 2017. Available: https://mitpress.mit.edu/9780262533812/introduction-to-embedded-systems/.
2. M. Wolf, Computers as Components: Principles of Embedded Computing System Design, 4th Edition, Morgan Kaufmann, 2016. Available: https://doi.org/10.1016/C2014-0-03242-5.
3. AUTOSAR, AUTOSAR Classic Platform – Specifications and Architecture. Available: https://www.autosar.org/standards/classic-platform.
4. ISO, ISO 26262:2018 – Road Vehicles – Functional Safety, International Organization for Standardization, 2018. Available: https://www.iso.org/publication/PUB200262.html.
5. ISO, ISO 21448:2022 – Road Vehicles – Safety of the Intended Functionality (SOTIF), International Organization for Standardization, 2022. Available: https://www.iso.org/standard/77490.html.
6. SAE International, ISO/SAE 21434:2021 – Road Vehicles – Cybersecurity Engineering, 2021. Available: https://saemobilus.sae.org/standards/isosae21434-road-vehicles-cybersecurity-engineering.
7. Robert Bosch GmbH, CAN Specification, Version 2.0, 1991.

Tematică de concurs - poziția 4,5 (PRISM): Asistent de cercetare științifică

1. Fundamentele securității cibernetice pentru sisteme embedded și automotive

1. Principii de securitate a sistemelor informatice și a sistemelor embedded: confidențialitate, integritate și disponibilitate.
2. Tipologii de vulnerabilități și amenințări asupra sistemelor automotive, senzorilor și protocoalelor de comunicație.
3. Metode de identificare a anomaliilor și evaluare a riscurilor de securitate.

2. Procesarea datelor radar și metode de inteligență artificială

1. Principii de achiziție, preprocesare și caracterizare a datelor radar reale și sintetice.
2. Algoritmi de învățare automată și rețele neuronale pentru clasificarea datelor și identificarea comportamentelor anormale.

3. Metode de antrenare, testare și evaluare a modelelor AI/ML utilizate în analiza datelor radar.

3. Securitatea sistemelor inteligente și tehnologiile Digital Twin

1. Arhitecturi Digital Twin și integrarea datelor provenite din sisteme fizice și medii de simulare.
2. Simularea scenariilor de atac și investigarea vulnerabilităților în sisteme cibernetico-fizice.
3. Utilizarea metodelor AI/ML pentru monitorizarea comportamentului sistemelor și detectarea anomaliilor și a potențialelor amenințări.

4. Testarea și evaluarea soluțiilor de securitate

1. Definirea scenariilor experimentale pentru evaluarea securității și robusteții sistemelor radar.
2. Aplicarea metodelor de testare și validare în medii virtuale și de simulare.
3. Analiza rezultatelor experimentale, documentarea vulnerabilităților identificate și evaluarea eficienței mecanismelor de detecție.

Bibliografie – PRISM, Poziția 4 și 5

1. Y. Zhou et al., "Towards Deep Radar Perception for Autonomous Driving: Datasets, Methods, and Challenges," Sensors, vol. 22, no. 11, Art. 4208, 2022. Available: https://doi.org/10.3390/s22114208.

2. A. Ouaknine, A. Newson, J. Rebut, F. Tupin, and P. Pérez, "CARRADA Dataset: Camera and Automotive Radar with Range-Angle-Doppler Annotations," in 2020 25th International Conference on Pattern Recognition (ICPR), 2021, pp. 5068–5075. Available: https://doi.org/10.1109/ICPR48806.2021.9413181.

3. S. Rajapaksha et al., "AI-Based Intrusion Detection Systems for In-Vehicle Networks: A Survey," ACM Computing Surveys, vol. 55, no. 11, Art. 237, 2023. Available: https://doi.org/10.1145/3570954.

4. ISO/SAE, ISO/SAE 21434:2021 – Road Vehicles – Cybersecurity Engineering, SAE International, 2021. Available: https://saemobilus.sae.org/standards/isosae21434-road-vehicles-cybersecurity-engineering.

5. H. Mun et al., "A Comprehensive Survey on Digital Twin: Focusing on Security Threats and Requirements," IEEE Access, 2025. Available: https://doi.org/10.1109/ACCESS.2025.3563621.

6. F. Tao, Q. Qi, L. Wang, and A. Y. C. Nee, "Digital Twins and Cyber–Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison," Engineering, vol. 5, no. 4, pp. 653–661, 2019. Available: https://doi.org/10.1016/j.eng.2019.01.014.

7. National Institute of Standards and Technology (NIST), Guide to Operational Technology (OT) Security, NIST Special Publication 800-82, Revision 3, 2023. Available: https://doi.org/10.6028/NIST.SP.800-82r3.

Tematică de concurs – poziția 6 (VulnHUNTER): Asistent cercetare științifică

1. Analiza Programelor și Identificarea Vulnerabilităților
    a. Analiza statică și dinamică a codului: Tehnici de *taint analysis*, execuție simbolică și *fuzzing*. Identificarea defectelor comune (CWE) precum *buffer overflows*, *integer overflows* și *use-after-free*.
    b. Vulnerabilități induse de procesul de compilare: Impactul optimizărilor de compilator asupra securității (ex. eliminarea verificărilor de tip dead code care curăță memoria sensibilă) și mecanisme de tip Undefined Behavior.
    c. Corelarea codului sursă cu fișierele binare: Tehnici de *binary lifting* și analiză comparativă (*diffing*) pentru identificarea vulnerabilităților în biblioteci compilate fără acces la sursă.
2. Tehnici de Exploatare și Analiza Vectorilor de Atac
    a. Mecanisme de control al fluxului de execuție: Exploatarea stivei (*stack smashing*), atacuri de tip *Return-Oriented Programming* (ROP) și *Jump-Oriented Programming* (JOP).
    b. Exploatarea heap-ului și a memoriei dinamice: Analiza vulnerabilităților în mecanismele de alocare dinamică a memoriei și manipularea structurilor de date interne.
    c. Analiza tehnicilor de evaziune: Modul în care atacatorii ocolesc protecțiile moderne (ex. *Information Leakage* pentru a învinge ASLR).
3. Metode de Corecție și Mitigare a Atacurilor
    a. Mecanisme de protecție la nivel de compilator și sistem de operare: Implementarea și limitările *Stack Canaries*, *Data Execution Prevention* (DEP/NX), *Address Space Layout Randomization* (ASLR) și *Control Flow Integrity* (CFI).
    b. Tehnici de *patching* și remediere: Strategii de aplicare a *patch*-urilor de securitate, utilizarea *wrapper*-elor de securitate și tehnici de *virtual patching*.
    c. *Hardening* și securitate prin design: Principiul privilegiului minim, izolarea proceselor (*sandboxing*) și utilizarea limbajelor de programare cu memorie sigură (*memory-safe languages*) ca metodă de mitigare pe termen lung.

Bibliografie – poziția 6

1. Y. Shoshitaishvili et al., "SOK: (State of) The Art of War: Offensive Techniques in Binary Analysis," 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 138-157, Available: https://doi.org/10.1109/SP.2016.17
2. V. J. M. Manès et al., "The Art, Science, and Engineering of Fuzzing: A Survey," in IEEE Transactions on Software Engineering, vol. 47, no. 11, pp. 2312-2331, 1 Nov. 2021, doi: 10.1109/TSE.2019.2946563, Available: https://ieeexplore.ieee.org/document/8863940
3. Irfan Ul Haq and Juan Caballero. 2021. "A Survey of Binary Code Similarity." ACM Comput. Surv. 54, 3, Article 51 (April 2022), 38 pages. Available: https://doi.org/10.1145/3446371

4. Yang et al., "Dead Store Elimination (Still) Considered Harmful", USENIX Security Symposium, 2017, Available: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-yang.pdf
5. J. Kang, Y. Sun, H. Xie, X. Zhu and Z. Ding, "Analysis System for Security Situation in Cyberspace Based on Knowledge Graph," 2021 7th International Conference on Big Data and Information Analytics (BigDIA), Chongqing, China, 2021, pp. 385-392, doi: 10.1109/BigDIA53151.2021.9619719. Available: https://ieeexplore.ieee.org/document/9619719
6. Xingqi Cheng, Xiaobing Sun, Lili Bo, and Ying Wei. 2022. "KVS: a tool for knowledge-driven vulnerability searching." In Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2022). Association for Computing Machinery, New York, NY, USA, 1731–1735. https://doi.org/10.1145/3540250.3558920

Tematică de concurs – pozițiile 7, 8 (VulnHUNTER): Asistent cercetare științifică

1. Securitatea memoriei și tehnici de codare sigură în limbajul C
    a. Tipologii de vulnerabilități specifice limbajului C (Buffer Overflow, Use-After-Free, Integer Overflow/Underflow, Format String Vulnerabilities, Memory Leaks).
    b. Cauze fundamentale la nivelul arhitecturii memoriei (Stack, Heap, BSS, Data segments).
    c. Standarde de codare sigură (Secure Coding Guidelines) și bune practici pentru mitigarea vulnerabilităților.
2. Tehnici avansate de compilare, linkeditare și protecții la nivel de binar
    a. Etapele procesului de compilare (lexicală, sintactică, semantică, optimizare, generare cod) și impactul lor asupra securității.
    b. Mecanisme defensive implementate la nivel de compilator și sistem de operare: ASLR (Address Space Layout Randomization), DEP/NX (Data Execution Prevention), Stack Canaries (SSP), PIE (Position Independent Executables).
    c. Tehnici moderne de mitigare: Control-Flow Integrity (CFI).
3. Validarea și mitigarea riscurilor de securitate
    a. Maparea vulnerabilităților pe standarde internaționale (ex: MITRE CWE - Common Weakness Enumeration).
    b. Proiectarea și implementarea de soluții de mitigare la nivel de cod sursă și arhitectură.
    c. Strategii defense-in-depth aplicate la nivelul dezvoltării de software (Secure Software Development Lifecycle).

Bibliografie – pozițiile 7, 8

1. Seacord, R. C. (2013). Secure Coding in C and C++ (2nd Edition). Addison-Wesley Professional.
2. Nielson, F., Nielson, H. R., & Hankin, C. (2015). Principles of Program Analysis. Springer.
3. Aho, A. V., Lam, M. S., Sethi, R., & Ullman, J. D. (2006). Compilers: Principles, Techniques, and Tools (2nd Edition). Pearson.
4. Howard, M., LeBlanc, D., & Viega, J. 24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them. McGraw-Hill. ISBN: 978-0-07-162676-7.
5. Software Engineering Institute (SEI) – Carnegie Mellon University. SEI CERT C Coding Standard: Rules for Developing Safe, Reliable, and Secure Systems.
6. MITRE Corporation. CWE (Common Weakness Enumeration) – Top 25 Most Dangerous Software Weaknesses (secțiunile relevante pentru C/C++, ex: CWE-119, CWE-416, CWE-190).
7. Abadi, M., Budiu, M., Erlingsson, Ú., & Ligatti, J. (2005). Control-Flow Integrity: Principles, Implementations, and Applications. ACM Transactions on Information and System Security (TISSEC).

Tematică concurs - poziția 2 (NeuroSafe): asistent de cercetare științifică

1. Analiza diverselor probleme în direcția fiabilității, dar și a vulnerabilităților sistemelor automotive
2. Proiectarea unor platforme din sfera securității cibernetice care să ajute la securizarea datelor provenite de la senzori din universul automotive, urmărind algoritmii criptografici potriviți
3. Analiza aplicațiilor bazate pe rețele neuronale adaptive cu impulsuri (spiking neural networks) în domeniul automotive
4. Analiza tipurilor de rețele SNN
5. Proiectarea/dezvoltarea unei platforme software care să evalueze diverse arhitecturi de rețele SNN

Bibliografie - poziția 2

1. D. Canino and G. Dini, "Cybersecurity of Automotive Wired Networking Systems: Evolution, Challenges, and Countermeasures," Electronics, vol. 14, no. 3, art. no. 471, Jan. 2025, doi: 10.3390/electronics14030471.
2. R. de Andrade, M. M. D. dos Santos, J. F. Justo Filho, L. R. Yoshioka, H. -J. Hof, and J. H. Kleinschmidt, "Security architecture for automotive communication networks with CAN FD," Computers & Security, vol. 129, art. no. 103203, Jun. 2023, doi: 10.1016/j.cose.2023.103203.
3. Loïc Cordone. Performance of spiking neural networks on event data for embedded automotive applications. Artificial Intelligence [cs.AI]. Université Côte d'Azur, 2022. English. ffNNT : 2022COAZ4097.
4. R. Khatoniar, D. Konar and V. Aggarwal, "Quantum-Enhanced Spiking Neural Networks", 2024 IEEE International Conference on Quantum Computing and Engineering (QCE), Montreal, QC, Canada, 2024, pp. 490-491, doi: 10.1109/QCE60285.2024.10370.
5. Ayasi, B.; Carmona, C.J.; Saleh, M.; García-Vico, A.M. A Practical Tutorial on Spiking Neural Networks: Comprehensive Review, Models, Experiments, Software Tools, and Implementation Guidelines. Eng 2025, 6, 304. https://doi.org/10.3390/eng6110304
6. AI in the automotive industry, IBM, https://www.ibm.com/think/topics/ai-in-automotive-industry.