Special Interest Group on Design Automation
ACM/SIGDA E-NEWSLETTER, Vol. 55, No. 12

SIGDA - The Resource for EDA Professionals

This newsletter is a free service for current SIGDA members and is added automatically with a new SIGDA membership.

Online archive: https://www.sigda.org/publications/newsletter

SIGDA News

1. **Europe Issues Recommendations for the Next European Chips Act**
SEMI Europe has released its SEMI Europe Chips Act Report, a wide-ranging assessment of how the European Chips Act is taking shape and where it still falls short. Approved by the SEMI European Advisory Board, the report consolidates industry feedback and outlines policy recommendations ahead of the next phase of legislation.

2. **OpenAI and Foxconn Team Up to Target Next-Gen AI Hardware Manufacturing**
OpenAI and Hon Hai Technology Group (Foxconn) have formed a new collaboration aimed at accelerating US-based manufacturing of next-generation AI infrastructure hardware. According to a recent announcement, the OpenAI-Foxconn collaboration focuses on co-designing advanced data center systems and strengthening domestic supply chains to support rapidly growing AI compute demands.

3. **AMD Maps Out Strategy for Leadership in Future Compute and AI**
AMD used its 2025 Financial Analyst Day in New York to outline its long-term strategy for future compute and AI, detailing new product roadmaps and multi-year financial targets. The company highlighted strong momentum across CPUs, GPUs, and adaptive computing platforms as it positions itself for the next phase of growth.

4. **NVLink Fusion Joins Arm Neoverse for the Next-Gen AI Data Centers**
Arm and NVIDIA are extending their long-running collaboration with the integration of NVIDIA NVLink Fusion into the Arm Neoverse platform. The announcement underscores the accelerating shift toward energy-efficient AI data center architectures. As hyperscalers race to boost AI throughput without escalating power budgets, the companies aim to deliver a unified, coherent infrastructure capable of scaling to next-generation workloads.

Message from the EiC

Dear Readers,

In this edition, we bring you the latest news and activities in our community, upcoming conferences, paper deadlines, an insightful article on What Are AI-Generated Attacks in Industrial Control Systems, and job openings worldwide.

Please do not hesitate to write to us if you want to contribute articles and announcements or share your thoughts and feedback.

Sandeep Chandran,
Editor-in-Chief,
SIGDA e-Newsletter

5. **Nokia and NestAI Advance Physical AI with €100M Partnership**
Arm and NVIDIA are extending their long-running collaboration with the integration of NVIDIA NVLink Fusion into the Arm Neoverse platform. The announcement underscores the accelerating shift toward energy-efficient AI data center architectures. As hyperscalers race to boost AI throughput without escalating power budgets, the companies aim to deliver a unified, coherent infrastructure capable of scaling to next-generation workloads.

6. **Pasqal and LG Electronics Partner to Accelerate Quantum Computing for Industry**
Pasqal, a neutral atom quantum computing company, has announced a strategic partnership with LG Electronics aimed at advancing quantum technologies for real-world industrial applications. The company announced that the partnership includes an equity investment from LG in Pasqal, signaling the consumer electronics giant's serious commitment to exploring next-generation computing.

7. **3D DRAM Breakthrough Promises Major AI Inference Performance Gains**
d-Matrix and Alchip have announced a joint effort to develop what they call the world's first 3D DRAM-based datacenter inference accelerator. The technology is aimed at eliminating the performance, cost, and scalability limits constraining today's AI infrastructure. The companies say the collaboration leverages the strengths of both teams: Alchip's ASIC design experience and d-Matrix's digital in-memory compute platform.

8. **Arduino Unveils Nesso N1 Pocket IoT Kit with Multi-Protocol Connectivity**
Arduino has introduced the Nesso N1, a compact IoT development kit created in collaboration with M5Stack. According to Arduino, the device brings the flexibility of the Arduino ecosystem into a rugged, handheld form factor designed for rapid prototyping and connected-device deployment.

What Are AI-Generated Attacks in Industrial Control Systems?

Contributing author: Mujeeb Ahmed <Mujeeb.Ahmed@newcastle.ac.uk>
Senior Lecturer in Computing, School of Computer Science, Newcastle University, UK

AE: Alberto Marchisio <alberto.marchisio@nyu.edu>

Industrial Control Systems (ICS) are foundational to critical infrastructure such as water treatment plants, power grids, and manufacturing facilities. These systems rely on sensors, actuators, and programmable logic controllers (PLCs) to monitor and control physical processes. As ICS become increasingly digitized and interconnected,

SIGDA E-News Editorial Board

they also become more vulnerable to cyber threats. Among the emerging threats is a new class of adversarial behavior: **AI-generated attacks**.

Why AI-Generated Attacks Matter

Traditional attack scenarios in ICS are often crafted manually by domain experts. These attacks are based on known vulnerabilities and require deep knowledge of the system's design and operational constraints. However, manual attack generation is time-consuming, expensive, and inherently limited in scope. For example, in the SWaT (Secure Water Treatment) testbed, human experts were able to generate only 36 attack scenarios over several days of continuous operation [1].

AI-generated attacks offer a scalable alternative. By leveraging machine learning and large language models (LLMs), researchers can automatically generate thousands of attack patterns—many of which are novel and previously unseen. These attacks can be used to stress-test anomaly detection systems, uncover hidden vulnerabilities, and improve the robustness of ICS defenses.

Rule-Based Attack Generation: Association Rule Mining

A technique based on Association Rule Mining (ARM) is proposed in [1]. Using historical attack data from the SWaT testbed, the system learns patterns of sensor and actuator states that lead to unsafe conditions.

To make this concept accessible, consider the following general rule:
If certain components (e.g., pumps or valves) are in specific states, then another component is likely to be in a risky state.

For example:
If Pump P203 is ON and Flow Sensor FIT101 reads high, then Valve MV201 is OPEN.

Such rules are automatically extracted from data and represent potential attack patterns. In the SWaT case study, over 110,000 such patterns were generated—far exceeding the manually crafted scenarios.

LLM-Based Attack Generation: AttackLLM

Building on the limitations of rule-based methods, [2] introduces **AttackLLM**, a multi-agent framework powered by large language models like GPT-4 and DeepSeek-V3. These agents analyze both process data and system design documentation to infer control invariants and generate attack patterns.

AttackLLM operates in two workflows:

- **Invariant Extraction**: LLM agents derive control logic from sensor-actuator relationships and validate them against operational data.
- **Attack Generation**: Using validated invariants, the system generates attack patterns that exploit vulnerabilities in the control logic.

For example, one attack involves spoofing the water level sensor (LIT101) to falsely indicate a low level, causing the inlet valve (MV101) to remain open and leading to tank overflow. Another stealthy attack gradually alters sensor readings by 1mm per minute—evading detection while causing cumulative damage.

Implications and Future Directions

AI-generated attacks represent a paradigm shift in ICS security. They enable: **Scalable attack simulation, Improved detector training, Discovery of hidden**

Paper Deadlines

HOST'26 – IEEE Int'l Symposium on Hardware-Oriented Security and Trust
Washington DC, USA
Abstracts due: Dec. 1, 2025
Deadline (winter): Dec. 8, 2025
May 4-7, 2026
http://www.hostsymposium.org

MDTS'26 – IEEE Microelectronics Design & Test Symposium
Albany, New York, USA
Deadline: Dec. 15, 2025
May 18-20, 2026
http://natw.ieee.org

FCCM' 26 - IEEE International Symposium On Field-Programmable Custom Computing Machines
Atlanta, Georgia, USA
Abstracts due: Jan. 10, 2026
Deadline: Jan. 17, 2026
May 13-16, 2026
https://www.fccm.org/

DAC'26 – Design Automation Conference
Long Beach, California, USA
Engineering Track Deadline: Jan. 12, 2026
July 26-29, 2026
http://www.dac.com/

vulnerabilities. However, they also raise concerns: **Adversarial use by malicious actors, Model robustness and adaptability, Ethical and safety considerations.**

Conclusion

AI-generated attacks are not just a research novelty—they are a necessary evolution in the defense of industrial control systems. By automating the discovery of attack patterns, researchers can better understand system vulnerabilities, improve anomaly detection, and build more resilient infrastructure.

References:

[1] Muhammad Azmi Umer, Chuadhry Mujeeb Ahmed, Muhammad Taha Jilani, and Aditya P. Mathur. Attack Rules: An Adversarial Approach to Generate Attacks for Industrial Control Systems using Machine Learning. CPSIoTSec '21, ACM, 2021.
[2] Chuadhry Mujeeb Ahmed. AttackLLM: LLM-based Attack Pattern Generation for an Industrial Control System. FMSys '25, ACM, 2025.
[3] Chuadhry Mujeeb Ahmed, Gauthama Raman M R, and Aditya P. Mathur. Challenges in Machine Learning based approaches for Real-Time Anomaly Detection in Industrial Control Systems. CPSS '20, ACM, 2020.

SIGDA Partner Journal

ACM Transactions on Design Automation of Electronic Systems (TODAES) features groundbreaking research and development in the specification, design, analysis, simulation, testing, and evaluation of electronic systems, with a focus on computer science and engineering. The journal's impact factor increased to 2.2 in 2023, more than doubling its value from 2020. Additionally, each issue highlights a notable contribution as the Editor's Pick for special recognition.

TODAES also recognizes papers and outstanding junior researchers through the best paper and rookie of the year awards. Authors can send their paper submissions to the manuscript portal.

TODAES welcomes special issue proposals from leading researchers and practitioners. Such proposals should be emailed to Prabhat Mishra, Senior Associate Editor, at prabhat@ufl.edu

TODAES Special Issue Call for Papers

Special Issue on Co-Design and Design Automation for Optical/Photonic Computing Systems

This special issue seeks original submissions on pioneering research aimed at advancing co-design and EDA methodologies to support the modeling, simulation, design optimization, and physical implementation toward hybrid integration of optical computing/interconnect and electronic systems with high reliability, scalability, and efficiency. All these topics, as well as further potential topics mentioned below, are of interest to this special issue.

Important Dates

- Submissions deadline EXTENDED: Dec 15, 2025
- First-round review decisions EXTENDED: February 15, 2026

Upcoming Conferences

FPT'25 - Int'l Conference on Field-Programmable Technology
Shanghai, China
Dec. 2-5, 2025
http://icfpt.org

ISED'25 – Int'l Conference on Intelligent Systems and Embedded Design
Chhattisgarh, India
Dec. 17-19, 2025
http://isedconf.org

iSES'25 – IEEE Int'l Symposium on Smart Electronic Systems
Hyderabad, India
Dec. 17-20, 2025
http://www.ieee-ises.org

HiPC'25 – IEEE Int'l Conference on High Performance Computing, Data, And Analytics
Hyderabad, India
Dec. 17-20, 2025
http://www.hipc.org

VLSID'26 – International Conference on VLSI Design & International Conference on Embedded Systems
Pune, Maharashtra, India
Jan. 3 - 7, 2026
https://vlsid.org/

ASP-DAC'26 - Asia and South Pacific Design Automation Conference
Hong Kong, China
Jan. 19-22, 2026
http://www.aspdac.com

HiPEAC'26: Int'l Conference on High Performance Embedded Architectures & Compilers
Krakow, Poland
Jan. 26-28, 2026
https://www.hipeac.net/2026/krakow/

- Deadline for revision submissions EXTENDED: March 15, 2026
- Notification of final decisions EXTENDED: April 15, 2026
- Tentative publication EXTENDED: Spring 2026

Submissions should be made through the ACM TODAES submission site (http://mc.manuscriptcentral.com/todaes)

For questions and further information, please contact guest editors at:

- Jiaqi Gu, Arizona State University, jiaqigu@asu.edu
- Cunxi Yu, University of Maryland, cunxiyu@umd.edu
- Sudeep Pasricha, Colorado State University, sudeep@colostate.edu
- Xu Wang, Cadence Design Systems, xubc@cadence.com

More information can be found in this call for papers.

ACM TECS Editor-In-Chief Call for Nominations

The term of the current Editor-in-Chief (EiC) of the ACM Transactions on Embedded Computing Systems (TECS) is coming to an end, and the ACM Publications Board has set up a nominating committee to assist the Board in selecting the next EiC. TECS forms an archival source for publishing high-quality research and developmental results referring to analysis, design, behavior, and experience with embedded computing systems.

The subjects of emphasis are embedded perspectives on: system-level modeling, specification, and synthesis; hardware/software codesign; real-time systems; validation verification; fault tolerance, robustness, reliability and dependability; security and privacy. The scope of TECS also includes emerging technologies, embedded devices and networks for Internet of Things and edge computing, e.g., edge AI and embedded system architectures for TinyML.

Nominations, including self-nominations, are invited for a three-year term as TECS EiC, beginning on April 1, 2026. The EiC appointment may be renewed at most one time. This is a voluntary position, but ACM will provide appropriate administrative support.

Appointed by the ACM Publications Board, Editors-in-Chief (EiCs) of ACM journals are delegated full responsibility for the journal's editorial management consistent with the journal's charter and general ACM policies. The Board relies on EiCs to ensure that the journal's content is of high quality and that the editorial review process is both timely and fair. They have the final say on the acceptance of papers, the Editorial Board size, and Associate Editors' appointment. The ACM Volunteer Editors Position Description contains a complete list of responsibilities. Self-nominations are encouraged and should include a CV and a statement of the candidate's vision for the future development of TECS.

The deadline for submitting nominations is January 15, 2026, although nominations will continue to be accepted until the position is filled. Please send all nominations to the search committee chair. The search committee members are:

- Krishnendu Chakrabarty (Arizona State University), Chair
- Partha Pratim Pande (Washington State University)
- Preeti Ranjan Panda (Indian Institute of Technology, Delhi)
- Wei Zhang (Hong Kong University of Science and Technology)
- Sebastian Steinhorst (Technical University of Munich)

The ACM Publications Board Liaison is: Sartaj Sahni (University of Florida)

ISSCC'26 – IEEE Int'l Solid-State Circuits Conference
San Francisco, California, USA
Feb. 16-20, 2026
http://isscc.org

FPGA'26 – ACM/SIGDA Int'l Symposium on Field-Programmable Gate Arrays
Seaside, California, USA
Feb. 22-24, 2026
http://www.isfpga.org

ISPD'26 – ACM Int'l Symposium on Physical Design
Bonn, Germany
Mar 15-18, 2026
http://www.ispd.cc/

ISQED'26 - Int'l Symposium on Quality Electronic Design
San Francisco, California, USA
Apr. 8-10, 2026
http://www.isqed.org

DATE'26 - Design Automation and Test in Europe
Verona, Italy
April 20-22, 2026
http://www.date-conference.com

RTAS'26 - IEEE Real-Time and Embedded Technology and Applications Symposium
Saint Malo, France
May 12-14, 2026
http://2026.rtas.org

ISCAS'26 – IEEE Int'l Symposium on Circuits and Systems
Shanghai, China
May 24-27, 2026
https://2026.ieee-iscas.org/

Technical Activities

1. **NXP BMS Chipset Helps Improves Battery Health Monitoring**
NXP's EIS battery management chipset enhances safety, longevity, and performance in EVs and energy storage systems…

2. **Sub-Millimeter Heat Pipe Targets Chip Cooling**
A new closed-loop fluid arrangement may ease the never-ending challenge of chip cooling…

3. **Could NTT's Low-Power Chip Be a Game Changer for Drones?**
NTT Research chip's standout feature is its ability to perform real-time object detection on full-resolution 4K video streams at under 20W—a very attractive proposition for battery-powered aerial platforms…

4. **Crypto Mining ASIC Goes Deep Sub-Threshold On 3 nm**
Japanese crypto-mining ASIC company Triple-1 is about to tape out its third-generation Bitcoin-mining chip, Kamikaze III, built on TSMC 3-nm process technology. Kamikaze III will offer power efficiency of 10.45 J/TH, thanks to proprietary techniques that enable sub-threshold operation, and the company plans to use the same technology in a forthcoming AI accelerator chip…

Job Positions

Purdue University, US

Job Title: Assistant/Associate Professor of Computer Sciences

Description: The School of Applied and Creative Computing at Purdue University invites applications for a full-time, non-tenure track Assistant or Associate Professor of Practice position on the West Lafayette, Indiana campus, starting in Fall 2026. We are seeking an accomplished professional with experience in Cybersecurity or Cloud Computing. This position is a key part of our strategic effort to bridge industry practice with academic excellence, with a primary focus on teaching to ensure our students are prepared to meet the critical challenges of defending against modern cyber threats, architecting resilient cloud environments, and managing scalable cyber infrastructure in an increasingly intelligent and connected world. The successful candidate will be expected to: Translate industry expertise into impactful educational experiences; Develop and teach undergraduate and graduate courses, especially in applied areas; Ensure curriculum remains aligned with cutting-edge industry practices; Mentor students for successful careers; Leverage professional networks to build industry and government partnerships; Contribute to the school's collaborative and interdisciplinary culture; Engage in service within the school, university, and profession. For more information, please refer to https://facultyvacancies.com/assistantassociate-professor-of-computer-sciences,i43959.html.

University of Zurich, Switzerland

Job Title: Doctoral Candidate in AI and Optimization

Description: Start of employment 1st of March 2026 or by agreement. The Department of Mathematical Modeling and Machine Learning (DM3L) at University of Zurich is seeking applications for a Doctoral Candidate in AI and Optimization. We offer an exciting and stimulating environment to study and work in. The successful candidate will work on a project in the AI and Optimization Lab with Prof. Anastasia Koloskova. The emphasis of the doctoral project is on the intersection of theory and practice in areas such as distributed optimization, federated learning, machine learning, privacy, or unlearning. For more information, please refer to https://facultyvacancies.com/doctoral-candidate-in-ai-and-optimization,i43964.html.

VinUniversity, Vietnam

Job Title: Faculty of Computer Science

Description: The College of Engineering and Computer Science (CECS) at VinUniversity provides a rigorous academic foundation and extensive opportunities for interdisciplinary, application-oriented research and learning. In collaboration with seven research centers, CECS combines an international-standard curriculum with state-of-the-art facilities and strategic industry partnerships, particularly within the Vingroup ecosystem, to cultivate an academic environment that catalyzes technological and scientific breakthroughs. Faculty members of Electrical Engineering is a fulltime research focused position at College of Engineering and Computer Science and will have the opportunity to collaborate with Environmental Intelligence Research Cluster on: AI-Guided Discovery of Advanced Materials; Recyclable and Rare-Earth-Free Functional Materials; Functional Nanomaterials for Biomedical and Environmental Applications; Two-Dimensional and Quantum Materials for Next-Generation Devices; AI-Driven Smart Sensor Technologies. For more information, please refer to https://vinuni.talent.vn/job/faculty-of-computer-science-9802.

Notice to authors