

**2025 55th Annual IEEE/IFIP
International Conference on
Dependable Systems and
Networks - Supplemental Volume
(DSN-S 2025)**

**Naples, Italy
23-26 June 2025**



**IEEE Catalog Number: CFP25V03-POD
ISBN: 979-8-3315-1204-0**

**Copyright © 2025 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP25V03-POD
ISBN (Print-On-Demand):	979-8-3315-1204-0
ISBN (Online):	979-8-3315-1203-3
ISSN:	2833-2903

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S) **DSN-S 2025**

Table of Contents

Message from the General Chairs	xiii
Message from the Industry Chairs	xv
Message from the Tutorial Chairs	xvi
Message from the Disrupt'25 Chairs	xvii
Message from the Doctoral Forum Chairs	xviii
Message from the Poster Track Chairs	xix
Industry Committee	xx
Tutorial Committee	xxi
Disrupt'25 Committee	xxii
Doctoral Forum Committee	xxiii
Poster Committee	xxiv

Industry

LLMPrism: Black-Box Performance Diagnosis for Production LLM Training Platforms	1
<i>Zhihan Jiang (The Chinese University of Hong Kong, China), Rui Ren (Huawei Cloud Computing Technology Co., Ltd, China), Guangba Yu (The Chinese University of Hong Kong, China), Yulun Wu (The Chinese University of Hong Kong, China), Wenwei Gu (The Chinese University of Hong Kong, China), Yichen Li (The Chinese University of Hong Kong, China), Yujie Huang (The Chinese University of Hong Kong, China), Cong Feng (Huawei Cloud Computing Technology Co., Ltd, China), Zengyin Yang (Huawei Cloud Computing Technology Co., Ltd, China), Yongqiang Yang (Huawei Cloud Computing Technology Co., Ltd, China), and Michael R. Lyu (The Chinese University of Hong Kong, China)</i>	
Anomaly Detection in Energy Performance Certificates – From Oblivious to Enlightened	8
<i>Nawel Benarba (INSA Lyon – LIRIS, France), Mathieu Chevalier (INSA Lyon – LIRIS, France), Sara Bouchenak (INSA Lyon – LIRIS, France), Benjamin Bertin (INSA Lyon – LIRIS, France), and Olivier Jung (Kardino, France)</i>	
Beyond Component Failures: Safety Challenges in Complex Maritime Control Systems	15
<i>Odd Ivar Haugen (DNV, Norway), Aleks Karlsen (DNV, Norway), Steven Mearns Cargill (DNV, United Kingdom), and Jan van Tiggelen (DNV, Norway)</i>	

To Protect the LLM Agent Against the Prompt Injection Attack with Polymorphic Prompt	22
<i>Zhilong Wang (Bytedance, USA), Neha Nagaraja (Northern Arizona University, USA), Lan Zhang (Northern Arizona University, USA), Hayretidin Bahsi (Northern Arizona University, USA), Pawan Patil (Bytedance, USA), and Peng Liu (Pennsylvania State University, USA)</i>	
When Features Gets Exploited: Functional Abuse and the Future of Industrial Fraud Prevention	29
<i>Elisa Chiapponi (Amadeus IT Group, France), Umberto Fontana (Amadeus IT Group, France; Télécom SudParis, France), Elyssa Boulila (Amadeus IT Group, France; EURECOM, France), Claudio Costanza (Amadeus IT Group, France), Vincent Rigal (Amadeus IT Group, France), and Olivier Thonnard (Amadeus IT Group, France)</i>	
DDR5 DRAM Faults in the Field	36
<i>Majed Valad Beigi (Advanced Micro Devices, Inc, TX), Yi Cao (Google, CA), Grace Tsai (Google, Taiwan), Sudhanva Gurumurthi (Advanced Micro Devices, Inc, TX), and Vilas Sridharan (Advanced Micro Devices, Inc, MA)</i>	
Assessing the Transferability of Adversarial Patches in Real-World Systems: Implications for Adversarial Testing of Image Recognition Security	42
<i>Stephan Kleber (Mercedes-Benz Tech Innovation GmbH, Germany), Jeremias Eppler (Mercedes-Benz Tech Innovation GmbH, Germany), Tim Palm (Ulm University, Germany), Dennis Eisermann (Ulm University, Germany), and Frank Kargl (Ulm University, Germany)</i>	
Security-by-Design at the Telco Edge with OSS: Challenges and Lessons Learned	49
<i>Carmine Cesarano (Università degli Studi di Napoli Federico II, Italy), Alessio Foggia (Università degli Studi di Napoli Federico II, Italy), Gianluca Roscigno (System Management S.p.A, Italy), Luca Andreani (DigitalPlatforms S.p.A, Italy), and Roberto Natella (Università degli Studi di Napoli Federico II, Italy)</i>	
Expectations Versus Reality: Evaluating Intrusion Detection Systems in Practice	56
<i>Larry Huynh (University of Western Australia, Australia), Jake Hesford (University of Western Australia, Australia), Daniel Cheng (University of Western Australia, Australia), Alan Wan (University of Western Australia, Australia), Seungho Kim (Sungkyunkwan University, South Korea), Hyoungshick Kim (Sungkyunkwan University, South Korea), and Jin Hong (University of Western Australia, Australia)</i>	
Bridging the Safety Gap: A C-ITS Solution for Protecting Vulnerable Road Users	63
<i>Mario Fiorentino (South Engineering srl, Italy), Michele Caggiano (South Engineering srl, Italy), Alessandro Magliacane (South Engineering srl, Italy), Angelo Coppola (Federico II University of Naples, Italy), and Andrea Marchetta (Federico II University of Naples, Italy)</i>	
Observe and Regulate Memory Interference on MPSoC: A Practical Approach	70
<i>Andrea Bastoni (Technical University of Munich; Minerva Systems), Alexander Zuepke (Technical University of Munich; Minerva Systems), and Marco Solieri (Minerva Systems)</i>	

Cordial: Cross-Row Failure Prediction Method Based on Bank-Level Error Locality for HBMs	77
<i>Wenwei Gu (The Chinese University of Hong Kong, China), Jiazhen Gu (Huawei Hong Kong Research Center, China), Renyi Zhong (The Chinese University of Hong Kong, China), Wenyu Zhang (Huawei Hong Kong Research Center, China), Ming Li (Huawei Hong Kong Research Center, China), and Michael R. Lyu (The Chinese University of Hong Kong, China)</i>	
Energy-Efficient Anomaly Detection in Autonomous Vehicles using RSNNs	84
<i>Daeho Kim (Incheon National University, Korea), Eun-Kyu Lee (Incheon National University, Korea), and Ji-Woo Lee (Korea Automotive Technology Institute, Korea)</i>	
KubeChecker: Detecting Configuration Bugs in Container Orchestration	91
<i>Yilin Sun (Fudan University, China), Dian Lyu (Fudan University, China), Cheng Cui (Huawei Technologies Co., Ltd, China), and Hui Xu (Fudan University, China)</i>	
Quantitative Security Metrics: Assessment of Cyberattack Scenarios for Cyber-Physical Systems	98
<i>Mike Da Silva (De Vinci Higher Education, De Vinci Research Center, France) and Nga Nguyen (De Vinci Higher Education, De Vinci Research Center, France)</i>	
Regulating Prosumer Device Security: A Key Priority in Power Grid Protection	105
<i>Alfredo Petruolo (University of Naples 'Parthenope', Italy), Luigi Coppolino (University of Naples 'Parthenope', Italy), Roberto Nardone (University of Naples 'Parthenope', Italy), and Luigi Romano (University of Naples 'Parthenope', Italy)</i>	
Runtime Verification of Program Organization Units in Safe Programmable Logic Controller Systems	112
<i>Hisham Unniyankal (University of Genova, Italy; COBO SpA, Italy), Davide Ancona (University of Genova, Italy), Angelo Ferrando (University of Modena and Reggio Emilia, Italy), Fabio Parodi (Technoleader Srl, Italy), Alessandro Alessi (Technoleader Srl, Italy), and Federico Bottino (COBO SpA, Italy)</i>	
On the Feasibility of Exploiting the USB Power Line for Side-Channel Attacks against Samsung Smartphone Models	119
<i>Leonardo da Costa (Samsung Research and Development Institute Brazil), Witor Oliveira (Samsung Research and Development Institute Brazil), Caio Peres (Samsung Research and Development Institute Brazil), Rene de Mello (Samsung Research and Development Institute Brazil), Jonghun Song (Samsung Electronics, South Korea), Seokwon Jeong (Samsung Electronics, South Korea), and Hyungchul Jung (Samsung Electronics, South Korea)</i>	
IAM Role Diet: A Scalable Approach to Detecting RBAC Data Inefficiencies	126
<i>Roberto Moratore (ING Bank), Eduardo Barbaro (ING Bank & TU Delft), and Yury Zhauniarovich (TU Delft)</i>	
An Open-Source Implementation and Security Analysis of Triad's TEE Trusted Time Protocol	133
<i>Matthieu Bettinger (LIRIS-DRIM INSA Lyon, France), Sonia Ben Mokhtar (LIRIS-DRIM CNRS, France), and Anthony Simonet-Boulogne (iExec Blockchain Tech, France)</i>	

Large-Scale AI Infra Reliability: Challenges, Strategies, and Llama 3 Training Experience	140
<i>Xun Jiao (Meta Platforms, Inc, USA), Abhinav Pandey (Meta Platforms, Inc, USA), Karthik Pattabiraman (University of British Columbia (UBC), Canada), and Fred Lin (Meta Platforms, Inc, USA)</i>	
Hardware Telemetry at Scale: A Case Study on SSDs Endurance Monitoring in Datacenters	147
<i>Olusiji Medaiyese (Meta Platforms Inc.), Fred Lin (Meta Platforms Inc.), Harish Dixit (Meta Platforms Inc.), Richa Mishra (Meta Platforms Inc.), Andrea Baglioni (Meta Platforms Inc.), Leandro Silva (Meta Platforms Inc.), Mike Elkin (Meta Platforms Inc.), Andrei Ilyashenko (Meta Platforms Inc.), Gor Safaryan (Meta Platforms Inc.), Dhankaran Singh Ajravat (Meta Platforms Inc.), Xun Jiao (Meta Platforms Inc.), and Vineet Parekh (Meta Platforms Inc.)</i>	
Integrating Testing with Runtime Verification for Mission-Critical Distributed Control Systems	153
<i>Davide Ancona (University of Genova, Italy), Stefano Avola (University of Genova, Italy), Angelo Ferrando (University of Modena and Reggio Emilia, Italy), Pierpaolo Baglietto (University of Genova, Italy), Maurice H. ter Beek (CNR-ISTI, Italy), Andrea Parodi (M3S SrL, Italy), Giancarlo Camera (Hitachi Rail STS SpA, Italy), and Matteo Pinasco (Hitachi Rail STS SpA, Italy)</i>	
Be My Guest: Welcoming Interoperability into IBC-Incompatible Blockchains	160
<i>Michał Nazarewicz (No Affiliation), Dhruv D. Jain (Inclusive Layer), Miguel Matos (IST Lisbon & INESC-ID), and Blas Rodriguez (Inclusive Layer)</i>	
Towards Robust Autonomous Landing Systems: Iterative Solutions and Key Lessons Learned	167
<i>Sebastian Schroder (Macquarie University, Australia), Yao Deng (Macquarie University, Australia), Alice James (Macquarie University, Australia), Avishkar Seth (Macquarie University, Australia), Kye Morton (Skyy Network, Australia), Subhas Mukhopadhyay (Macquarie University, Australia), Richard Han (Macquarie University, Australia), and Xi Zheng (Macquarie University, Australia)</i>	

Tutorial

Generative AI in Cybersecurity: Generating Offensive Code from Natural Language	174
<i>Pietro Liguori (University of Naples Federico II, Italy), Roberto Natella (University of Naples Federico II, Italy), and Domenico Cotroneo (University of Naples Federico II, Italy)</i>	
Quantum Computing and Post-Quantum Cryptography: Preparing for the Next Era of Cybersecurity	176
<i>Hazel Murray (Munster Technological University, Ireland), George O'Mahony (Munster Technological University, Ireland), and Anila Mjeda (Munster Technological University, Ireland)</i>	
Benchmarking AI Agents for IT Automation Tasks with ITBench	178
<i>Jackson Clark (University of Illinois at Urbana-Champaign, USA), Rohan Arora (IBM Research, USA), and Saurabh Jha (IBM Research, USA)</i>	

Decentralized Federated Learning: Enhancing Reliability with Blockchain	180
<i>Antonella Del Pozzo (Université Paris-Saclay, France) and Maxence Perion (Université Paris-Saclay, France)</i>	
Evaluating Blockchain Fault Tolerance with STABL	182
<i>Vincent Gramoli (University of Sydney and Redbelly Network, Australia), Rachid Guerraoui (EPFL, Switzerland), Andrei Lebedev (University of Sydney, Australia), and Gauthier Voron (EPFL, Switzerland)</i>	
Model-Based Qualitative Dependability and Security Evaluation	184
<i>András Földvári (Budapest University of Technology and Economics, Hungary) and András Pataricza (Budapest University of Technology and Economics, Hungary)</i>	

Disrupt'25

Assessing the Validity of LLM-Driven Hazard Analysis: An Assessor's Perspective	186
<i>Michael Kevvay (MIREA - Russian Technical University, Russia), Vladislav Gryaznykh (MIREA - Russian Technical University, Russia), Oleg Kirovskii (Safety Consult LLC, Armenia), and Anton Korolev (MIREA - Russian Technical University, Russia)</i>	
Enhancing Accuracy in Approximate Byzantine Agreement with Bayesian Inference	191
<i>Roy Shadmon (UC Santa Cruz) and Owen Arden (UC Santa Cruz)</i>	
Replicating Human Immune System via Harmonic Radar: A Framework and Preliminary Results in Thwarting Cyber-Physical Attacks	196
<i>Nathanael Denis (King Abdullah University of Science and Technology, Saudi Arabia) and Roberto Di Pietro (King Abdullah University of Science and Technology, Saudi Arabia)</i>	
Digital Cluster Circuits for Reliable Datacenters	201
<i>Davide Rovelli (Università della Svizzera Italiana, Switzerland; SAP SE, Germany) and Patrick Eugster (Università della Svizzera Italiana, Switzerland)</i>	
Trusted Federated Learning: Towards a Partial Zero-Knowledge Proof Approach	206
<i>Yannis Formery (Univ. Gustave Eiffel, France), Leo Mendiboure (Univ. Gustave Eiffel, France), Jonathan Villain (Univ. Gustave Eiffel, France), Virginie Deniau (Univ. Gustave Eiffel, France), Christophe Gransart (Univ. Gustave Eiffel, France), and Stephane Delbruel (Univ. of Bordeaux, France)</i>	
UniPHY: Unified Physical Layer Security for LPWANs	211
<i>Stéphane Delbruel (Univ. Bordeaux, France), Leo Mendiboure (Univ. Gustave Eiffel, France), Yannis Formery (Univ. Gustave Eiffel, France), Joachim Bruneau-Queyreix (Univ. Bordeaux, France), and Laurent Réveillère (Univ. Bordeaux, France)</i>	
Rethinking BFT: Leveraging Diverse Software Components with LLMs	216
<i>João Imperadeiro (U. Minho and INESC TEC, Portugal), Ana Nunes Alonso (U. Minho and INESC TEC, Portugal), and José Pereira (U. Minho and INESC TEC, Portugal)</i>	

Doctoral Forum

Strategies to Describe and Timely Detect Attacks	221
<i>Tommaso Puccetti (University of Florence, Italy)</i>	
Effect of Human-Selected Hard Examples to Improve Accuracy of Semantic Segmentation	224
<i>Yuriko Ueda (Meiji University, Japan), Marin Wada (Meiji University, Japan), Miho Adachi (Meiji University, Japan), and Ryusuke Miyamoto (Meiji University, Japan)</i>	
Towards Provenance for Cybersecurity in Cloud-Native Production Infrastructure	227
<i>Paul R. B. Houshel (Télécom SudParis, France), Sylvie Laniece (Orange Innovation, France), and Olivier Levillain (Télécom SudParis, France)</i>	
Leaving No Blind Spots: Toward Automotive Cybersecurity	230
<i>Francesco Marchiori (University of Padova, Italy) and Mauro Conti (University of Padova, Italy)</i>	
Enhanced Cybersecurity Monitoring in Multi-Plant Flexible Manufacturing Environments	233
<i>Antonio Iannaccone (University of Naples "Parthenope", Italy) and Roberto Nardone (University of Naples "Parthenope", Italy)</i>	
On Predictive Modeling of Multi-Bit Upsets for Emulated Fault Injection	236
<i>Trishna Rajkumar (KTH Royal Institute of Technology, Sweden) and Johnny Öberg (KTH Royal Institute of Technology, Sweden)</i>	
AI Agent-Based Adaptive Task Offloading for Autonomous Drones in Dynamic Environments	239
<i>Qingyang Zhang (University of Tsukuba, Japan) and Fumio Machida (University of Tsukuba, Japan)</i>	
ScamDetect: Towards a Robust, Agnostic Framework to Uncover Threats in Smart Contracts	242
<i>Pasquale De Rosa (University of Neuchâtel, Switzerland), Pascal Felber (University of Neuchâtel, Switzerland), and Valerio Schiavoni (University of Neuchâtel, Switzerland)</i>	

Poster

DeepICS: Deep Causal Relationship Modeling for Multi-Source Log-Based Anomaly Detection in Industrial Control Systems	245
<i>Seong-Su Yoon (Chonnam National University, South Korea), Dong-Hyuk Shin (Chonnam National University, South Korea), and Ieck-Chae Euom (Chonnam National University, South Korea)</i>	
Poster: Designing Scalable, Secure Systems for Atomic-Scale Physical AI: Enabling Open Science and Collaborative Data Management and Analytics	247
<i>Lewis Tseng (UMass Lowell, USA) and Yu-Tsun Shao (USC, USA)</i>	
Poster: Agree to Disagree: Revisiting the Comparison of (Multi-)Paxos and Raft	249
<i>Lewis Tseng (UMass Lowell, USA)</i>	
Jailbreaking Generative AI: Empowering Novices to Conduct Phishing Attacks	251
<i>Rina Mishra (IIT Jammu, India), Gaurav Varshney (IIT Jammu, India), and Shreya Singh (IIT Jammu, India)</i>	
Adaptive Identity Management: Unified Personalization and Privacy Protection for Web Apps	253
<i>Min-Chieh Wu (National Yang Ming Chiao Tung University, Taiwan) and Yu-Sung Wu (National Yang Ming Chiao Tung University, Taiwan)</i>	

Intrusion Detection System with Domain-Incremental Continual Learning	255
<i>Hyejin Kim (Korea Institute of Energy Technology (KENTECH), Korea), Seunghyun Yoon (Korea Institute of Energy Technology (KENTECH), Korea), Dan Dongseong Kim (The University of Queensland, Australia), Jin-Hee Cho (Virginia Tech, USA), Terrence J. Moore (DEVCOM Army Research Lab., USA), Frederica F. Nelson (DEVCOM Army Research Lab., USA), and Hyuk Lim (Korea Institute of Energy Technology (KENTECH), Korea)</i>	
Detecting Scrapers on E-Commerce Websites using a Reduced Feature Set	257
<i>Umberto Fontana (Amadeus IT Group, France; Télécom SudParis, France), Elisa Chiapponi (Amadeus IT Group, France), Claudio Costanza (Amadeus IT Group, France), Vincent Rigal (Amadeus IT Group, France), Olivier Thonnard (Amadeus IT Group, France), Martynas Buozis (Amadeus IT Group, France), and Hervé Debar (Télécom SudParis, France)</i>	
Learnable Encryption with a Diffusion Property	259
<i>Ijaz Ahmad (Korea University, Korea), Joongheon Kim (Korea University, Korea), and Seokjoo Shin (Chosun university, Korea)</i>	
Security Vulnerability Risk Growth Model Based on CVSS 4.0	261
<i>Sora Okada (Takushoku University, Japan), Masaya Shimakawa (Takushoku University, Japan), and Takashi Minohara (Takushoku University, Japan)</i>	
TOsense: We Read, You Click	263
<i>Xinzhang Chen (The University of New South Wales, Australia), Hassan Ali (The University of New South Wales, Australia), Arash Shaghaghi (The University of New South Wales, Australia), Salil S. Kanhere (The University of New South Wales, Australia), and Sanjay Jha (The University of New South Wales, Australia)</i>	
PhishingHook: Catching Phishing Ethereum Smart Contracts Leveraging EVM Opcodes	265
<i>Pasquale De Rosa (University of Neuchâtel, Switzerland), Simon Queyruet (University of Neuchâtel, Switzerland), Yérom-David Bromberg (University of Rennes, France), Pascal Felber (University of Neuchâtel, Switzerland), and Valerio Schiavoni (University of Neuchâtel, Switzerland)</i>	
Study of Appropriate Information Combination in Image-Based Obfuscated Malware Detection ...	267
<i>Tetsuro Takahashi (Shizuoka University, Japan), Rikima Mitsuhashi (Shizuoka University, Japan), Masakatsu Nishigaki (Shizuoka University, Japan), and Tetsushi Ohki (Shizuoka University, Japan)</i>	
Looking for Anomalies in Cross-Chain Bridges	269
<i>André Augusto (Universidade de Lisboa, Portugal), Rafael Belchior (Universidade de Lisboa, Portugal; Blockdaemon, Ireland), Jonas Pfannschmidt (Blockdaemon, Ireland), André Vasconcelos (Universidade de Lisboa, Portugal), and Miguel Correia (Universidade de Lisboa, Portugal)</i>	
Real-Time GOOSE Attack Detection in IEC 61850 Substations using SDN-Based Traffic Inspection	271
<i>Seunghyun Yoon (Korea Institute of Energy Technology (KENTECH)), Ryansoo Kim (Electronics and Telecommunications Research Institute (ETRI)), Hark Yoo (Electronics and Telecommunications Research Institute (ETRI)), and Hyuk Lim (Korea Institute of Energy Technology (KENTECH))</i>	

Author Index 273