2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W 2025)

Naples, Italy
23-26 June 2025

IEEE

IEEE Catalog Number: CFP2541K-POD
ISBN: 979-8-3315-1206-4

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:	CFP2541K-POD
ISBN (Print-On-Demand):	979-8-3315-1206-4
ISBN (Online):	979-8-3315-1205-7
ISSN:	2325-6648

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 Workshops (DSN-W)

DSN-W 2025

Table of Contents

Message from the General Chairs ..... **xiii**
Message from the Workshop Chairs ..... **xv**
Message from the WDMD Workshop Chairs ..... **xvi**
Message from the VERDI Workshop Chairs ..... **xvii**
Message from the S2AIM Workshop Chairs ..... **xviii**
Message from the AxC Workshop Chairs ..... **xx**
Message from the DT4DRS Workshop Chairs ..... **xxi**
Message from the FORCE Workshop Chairs ..... **xxii**
Message from the EnvSys Workshop Chairs ..... **xxiii**
Message from the DSML Workshop Chairs ..... **xxiv**
WDMD Organization ..... **xxv**
VERDI Organization ..... **xxvi**
S2AIM Organization ..... **xxvii**
AxC Organization ..... **xxviii**
DT4DRS Organization ..... **xxix**
FORCE Organization ..... **xxx**
EnvSys Organization ..... **xxxi**
DSML Organization ..... **xxxii**
WDMD Keynotes ..... **xxxiii**
VERDI Keynote ..... **xxxviii**
S2AIM Keynote ..... **xxxix**
AxC Keynote ..... **xl**
DT4DRS Keynote ..... **xli**
FORCE Keynotes ..... **xliii**
EnvSys Keynote ..... **xlv**
DSML Keynotes ..... **xlviii**

4th International Workshop on Dependability Modeling and Digitalization (WDMD)

Characterizing Modern GPU Resilience and Impact in HPC Systems: A Case Study of A100 GPUs 1
Shengkun Cui (University of Illinois Urbana-Champaign, USA), Archit Patke (University of Illinois Urbana-Champaign, USA), Ziheng Chen (University of Illinois Urbana-Champaign, USA), Aditya Ranjan (University of Illinois Urbana-Champaign, USA), Hung Nguyen (University of Illinois Urbana-Champaign, USA), Phuong Cao (University of Illinois Urbana-Champaign, USA), Brett Bode (University of Illinois Urbana-Champaign, USA), Gregory Bauer (University of Illinois Urbana-Champaign, USA), Saurabh Jha (IBM Research, USA), Chandra Narayanaswami (IBM Research, USA), Daby Sow (IBM Research, USA), Catello Di Martino (Nokia Bell Labs, Brazil), Zbigniew T. Kalbarczyk (University of Illinois Urbana-Champaign, USA), and Ravishankar K. Iyer (University of Illinois Urbana-Champaign, USA)

3rd International Workshop on Verification & Validation of Dependable Cyber-Physical Systems (VERDI)

A Hybrid Cybersecurity Assessment Framework for Unmanned Aircraft Vehicles Based on IMECA and Penetration Testing 7
Artem Abakumov (National Aerospace University KhAI, Ukraine), Vyacheslav Kharchenko (National Aerospace University KhAI, Ukraine), and Peter Popov (University of London, United Kingdom)

Refining Environmental Requirements for Autonomous Driving Systems: Leveraging the FRAV Framework 15
Mahwish Kundi (Maynooth University, Ireland), Faraz Ahmad (Abdul Wali Khan University Mardan, Pakistan), and Rosemary Monahan (Maynooth University, Ireland)

Safety-Centric Architecture for AI-Enabled Autonomous Driving Systems 23
Jatin Arora (VORTEX CoLab, Portugal; ISEP, Portugal), Alexandre Esper (ISEP, Portugal; Capgemini Engineering, Portugal), and Vasco Santos (VORTEX CoLab, Portugal)

Model-Driven, Logic-Supported Exploratory Dependability Analysis 27
András Földvári (Budapest University of Technology and Economics, Hungary) and András Pataricza (Budapest University of Technology and Economics, Hungary)

Enhancing Cyber-Physical System Dependability via Synthesis: Challenges and Future Directions 35
Max Taylor (Idaho National Laboratory, United States) and Arthur Amorim (The University of Central Florida, United States)

Reasoning with Happens-Before Relations about Concurrent Programs in the Theta Framework 43
Csanád Telbisz (Budapest University of Technology and Economics, Hungary), Levente Bajczi (Budapest University of Technology and Economics, Hungary), Dániel Szekeres (Budapest University of Technology and Economics, Hungary), András Vörös (Budapest University of Technology and Economics, Hungary), and István Majzik (Budapest University of Technology and Economics, Hungary)

Dependability Assurance with Symbolic Reasoning in LLM-Enabled Systems 47
András Gergely Deé-Lukács (Budapest University of Technology and Economics) and András Földvári (Budapest University of Technology and Economics)

Program Verification for Rigorous Analysis of Decision Tree Ensembles against Specifications 55
Iat Tou Leong (University of Coimbra), Aleksandar Avdalovic (Louisiana State University), and Raul Barbosa (University of Coimbra)

DURA-CPS: A Multi-Role Orchestrator for Dependability Assurance in LLM-Enabled Cyber-Physical Systems 63
Trisanth Srinivasan (Cyrion Labs, USA), Santosh Patapati (Cyrion Labs, USA), Himani Musku (Carnegie Mellon University, USA), Idhant Gode (Cornell University, USA), Aditya Arora (University of California San Diego, USA), Samvit Bhattacharya (Cyrion Labs, USA), Abubakr Nazriev (University of Montana, USA), Sanika Hirave (Oakland University, USA), Zaryab Kanjiani (Cornell University, USA), and Srinjoy Ghose (University of North Texas, USA)

1st International Workshop on Safe and Sustainable AI-Aided Manufacturing (S2AIM)

Leveraging Time-Frequency Features for Contact Classification and Regression with a Piezoelectric Tactile Skin for Robotic Fingertips 71
Nicole Alati (University of Bologna, Italy), Davide Bargellini (University of Bologna, Italy), Alex Pasquali (University of Bologna, Italy), Yahya Abbass (University of Genoa, Italy), Maurizio Valle (University of Genoa, Italy), Gianluca Palli (University of Bologna, Italy), and Roberto Meattini (University of Bologna, Italy)

Ransomware Threats in Manufacturing Industry: Patterns Based on Dark Web Tor Groups 79
Luis de-Marcos (Universidad de Alcalá, Spain), Adrián Domínguez-Díaz (Universidad de Alcalá, Spain), Carlos Cilleruelo (Universidad de Alcalá, Spain), and Daniel Rodríguez (Universidad de Alcalá, Spain)

Human-AI Interaction Implementation in Consolidate Digital Environments through a Collaborative and Multidisciplinary Design Approach 83
Michele Zannoni (University of Bologna, Italy) and Virginia Vignali (University of Bologna, Italy)

Orchestration of Sustainable Mixed-Criticality Systems over Heterogenous Edge Nodes 88
Francesco Boccola (University of Naples Federico II Via Claudio 21, Italy), Marcello Cinque (University of Naples Federico II Via Claudio 21, Italy), Luigi De Simone (University of Naples Federico II Via Claudio 21, Italy), Davide De Vita (University of Naples Federico II Via Claudio 21, Italy), and Nike Di Giacomo (University of Naples Federico II Via Claudio 21, Italy)

Robot Situation and Task Awareness using Large Language Models and Ontologies 96
Victor Molina (Universitat Politècnica de Catalunya, Spain), Oriol Ruiz-Celada (Universitat Politècnica de Catalunya, Spain), Raul Suarez (Universitat Politècnica de Catalunya, Spain), Jan Rosell (Universitat Politècnica de Catalunya, Spain), and Isiah Zaplana (Universitat Politècnica de Catalunya, Spain)

Experimental Evaluation of a User-Centered Unilateral Telemanipulation System for Training and Control in Robotic Industrial Scenarios 104
Mattia Tafuri (University of Bologna, Italy), Davide Chiaravalli (University of Bologna, Italy), Mona Saber Gharamaleki (University of Bologna, Italy), Claudio Melchiorri (University of Bologna, Italy), Gianluca Palli (University of Bologna, Italy), and Roberto Meattini (University of Bologna, Italy)

10th Workshop on Approximate Computing (AxC)

XMULT: An Energy-Efficient Design of Approximate Multiplier 111
Ahsan Rafiq (Tallinn University of Technology, Estonia) and Maksim Jenihhin (Tallinn University of Technology, Estonia)

Deep&Wide: Achieving Area Efficiency in Scalable Approximate Accelerators 115
Farjana Jalil (Bielefeld University of Applied Sciences and Arts, Germany), Muhammad Awais (Paderborn University, Germany), Qazi Arbab Ahmed (Bielefeld University of Applied Sciences and Arts, Germany), Hassan Ghasemzadeh Mohammadi (Reneo Group GmbH, Germany), Thorsten Jungeblut (Bielefeld University of Applied Sciences and Arts, Germany), and Marco Platzner (Paderborn University, Germany)

On the Resilience of INT8 Quantized Neural Networks on Low-Power RISC-V Devices 119
Antonio Porsia (Politecnico di Torino, Italy), Giacomo Perlo (Politecnico di Torino, Italy), Annachiara Ruospo (Politecnico di Torino, Italy), and Ernesto Sanchez (Politecnico di Torino, Italy)

A Margin Based Early-Stopping Approach for Random Forest Classifiers 123
Mario Barbareschi (University of Naples Federico II, Italy) and Antonio Emmanuele (University of Naples Federico II, Italy)

1st International Workshop on Digital Twins for Dependability, Resilience and Security (DT4DRS)

An Architectural Framework for Urban Digital Twin Design: A Case Study on Hydrogeological Risk Management 127
Angelo Martella (University of Salento, Italy), Antonella Longo (University of Salento, Italy), Cristian Martella (University of Salento, Italy), Marco Zappatore (University of Salento, Italy), and Francesca Miccoli (University of Salento, Italy)

An Integrated Digital Twin Architecture for Real-Time Urban Air Quality Management 135
Manoj Herath (Institut Polytechnique de Paris, France), Hrishikesh Dutta (Institut Polytechnique de Paris, France), Roberto Minerva (Institut Polytechnique de Paris, France), Noel Crespi (Institut Polytechnique de Paris, France), Maira Alvi (Institut Polytechnique de Paris, France), and Syed Mohsan Raza (Institut Polytechnique de Paris, France)

A Digital Twin Approach to Autonomous Emergency Braking: HiL Testing with Raspberry Pi and Standardized Scenarios 139
Roland Nagy (Budapest University of Technology and Economics, Hungary) and Árpád Török (Budapest University of Technology and Economics, Hungary)

Network and Vehicle Digital Twins for Hardware in the Loop Simulation of C-ITS Applications 146
Andrea Marchetta (University Federico II of Naples, Italy), Tamás Márton Kazár (Budapest University of Technology and Economics, Hungary), Marcello Cinque (University Federico II of Naples, Italy), Angelo Coppola (University Federico II of Naples, Italy), Zsombor Pethő (Budapest University of Technology and Economics, Hungary), Zsolt Szalay (Budapest University of Technology and Economics, Hungary), and Árpád Török (Budapest University of Technology and Economics, Hungary)

A Digital Twin Network for Proactive Security: The Smart Grid Use-Case 152
Biagio Boi (University of Salerno, Italy) and Christian Esposito (University of Salerno, Italy)

A Model-Based Approach for Cybersecurity Assessment of Off-Road and Defense Vehicles 160
Umberto Bellini (Università di Trento, Italy; IVECO Group, Italy), Marzieh Kordi (Università degli Studi di Firenze, Italy; IMT School for Advanced Studies, Italy), Bruno Crispo (Università di Trento, Italy), Paolo Lollini (Università degli Studi di Firenze, Italy), Andrea Bondavalli (Università degli Studi di Firenze, Italy), and Davide Compar (IVECO Group, Italy)

Using Digital Twins as an Upgrade Path for Critical Infrastructure Control Systems 168
Huzaifah Nadeem (University of Pittsburgh, USA) and Amy Babay (University of Pittsburgh, USA)

Toward Predictive Diagnostics: Real-Time Digital Twin for Electric Vehicle Power Systems 176
Emil Nagy (Budapest University of Technology and Economics, Hungary), József Pázmány (Jaguar Land Rover Hungary, Hungary), Dávid Tollner (Budapest University of Technology and Economics, Hungary), and Árpád Török (Budapest University of Technology and Economics, Hungary)

Foundations Of Reliable Classical-quantum Engineering (FORCE)

Assessing the Elephant in the Room in Scheduling for Current Hybrid HPC-QC Clusters 184
Paolo Viviani (LINKS Foundation, Italy), Roberto Rocco (E4 Computer Engineering, Italy), Matteo Barbieri (E4 Computer Engineering, Italy), Gabriella Bettonte (E4 Computer Engineering, Italy), Elisabetta Boella (E4 Computer Engineering, Italy), Marco Cipollini (Politecnico di Torino, Italy), Jonathan Frassineti (CINECA, Italy), Fulvio Ganz (E4 Computer Engineering, Italy), Sara Marzella (CINECA, Italy), Daniele Ottaviani (CINECA, Italy), Simone Rizzo (E4 Computer Engineering, Italy), Alberto Scionti (LINKS Foundation, Italy), Chiara Vercellino (LINKS Foundation, Italy), Giacomo Vitali (LINKS Foundation, Italy), Olivier Terzo (LINKS Foundation, Italy), Bartolomeo Montrucchio (Politecnico di Torino, Italy), and Daniele Gregori (E4 Computer Engineering, Italy)

A Typology of Quantum-Classical Faults 188
Edoardo Giusto (University of Naples Federico II, Italy), Santiago Núñez-Corrales (UIUC, USA), Alessandro Cilardo (University of Naples Federico II, Italy), Nicola Mazzocca (University of Naples Federico II, Italy), and Travis Humble (Oak Ridge National Laboratory, US)

Near-Term Application Engineering Challenges in Emerging Superconducting Qudit Processors .. 196
Davide Venturelli (USRA, USA), Erik Gustafson (USRA, USA), Doga Kurkcuoglu (Fermilab, USA), and Silvia Zorzetti (Fermilab, USA)

ATTAQ: Adversarial Robustness of Quantum Machine Learning 200
Francesco Marchiori (University of Padova, Italy) and Mauro Conti (University of Padova, Italy)

Supply Chain Malware Detection via Classical and Quantum Kernel Methods in Embedded Systems 208
Sthefanie J. G. Passo (University of Texas at San Antonio, United States), Vishal H. Kothavade (University of Texas at San Antonio, United States), and John J. Prevost (University of Texas at San Antonio, United States)

AI-Augmented Parameter Initialization for QAOA 216
Jai Nana (Case Western Reserve University, USA), Xinpeng Li (Case Western Reserve University, USA), Ning Xie (Florida International University, USA), Shusen Pu (University of West Florida, USA), Yifan Yu (University of Washington, USA), Qiang Guan (Kent State University, USA), Xiaotian Han (Case Western Reserve University, USA), Shuai Xu (Case Western Reserve University, USA), and Vipin Chaudhary (Case Western Reserve University, USA)

Quantum Circuit Optimization for Protein Structure Prediction 220
Xinpeng Li (Case Western Reserve University, US), Vinooth Rao Kulkarni (Case Western Reserve University, US), Jai Nana (Case Western Reserve University, US), Shusen Pu (University of West Florida, US), Ning Xie (Florida International University, US), Qiang Guan (Kent State University, US), Ruihao Li (Cleveland Clinic, US), Shulei Zhang (Case Western Reserve University, US), Shuai Xu (Case Western Reserve University, US), Daniel Blankenberg (Cleveland Clinic, US), and Vipin Chaudhary (Case Western Reserve University, US)

Workshop on Environment-System Symbiosis (EnvSys)

Weather Impact Analysis for UAV-Based Deforestation Monitoring Systems 224
Tasfia Nuzhat (University of Tsukuba, Japan), Fumio Machida (University of Tsukuba, Japan), and Ermeson Andrade (Federal Rural University of Pernambuco, Brazil)

Federated Learning-Based Approach for Landslide Prediction – The Case Study in Taiwan 231
Po-Wu Cheng (National Cheng Kung University, Taiwan) and Wen-Ping Tsai (National Cheng Kung University, Taiwan)

Beyond Control: Embracing Emergent Behavior in Symbiotic Digital Twin and CPS Ecosystems ... 235
Andrea Garbugli (University of Bologna, Italy), Armir Bujari (University of Bologna, Italy), and Paolo Bellavista (University of Bologna, Italy)

Integrating Groundwater Level Forecasting Models into Climate Risk Assessment for Adaptive Water Resource Management: A Case Study of Tainan, Taiwan 236
Pei-Ju Tsang (National Cheng Kung University, Taiwan) and Wen-Ping Tasi (National Cheng Kung University, Taiwan)

Experience: Evaluating Real-Time Drone OS under Extreme and Adversarial Environment 240
Vina Dang (UMAss Lowell, USA), Layann Shaban (UMAss Lowell, USA), and Lewis Tseng (UMAss Lowell, USA)

The Eighth Workshop on Dependable and Secure Machine Learning (DSML)

Revisiting Adversarial Perception Attacks and Defense Methods on Autonomous Driving Systems 242
Cheng Chen (Louisiana State University, LA), Yuhong Wang (Louisiana State University, LA), Nafis S Munir (Louisiana State University, LA), Xiangwei Zhou (Louisiana State University, LA), and Xugui Zhou (Louisiana State University, LA)

On the Transferability of Adversarial Attacks from Convolutional Neural Networks to Variants of ChatGPT4 250
Niklas Bunzel (TU Darmstadt, Germany)

Learning from the Good Ones: Risk Profiling-Based Defenses Against Evasion Attacks on DNNs... 256
Mohammed Elnawawy (University of British Columbia, Canada), Gargi Mitra (University of British Columbia, Canada), Shahrear Iqbal (National Research Council Canada, Canada), and Karthik Pattabiraman (University of British Columbia, Canada)

Audio Jailbreak Attacks: Exposing Vulnerabilities in SpeechGPT in a White-Box Framework 259
Binhao Ma (University of Missouri-Kansas City, United States), Hanqing Guo (University of Hawai'i at Mānoa, United States), Zhengping Jay Luo (Rider University, United States), and Rui Duan (University of Missouri-Kansas city, United States)

FHE ML Tuxedo: A Tailored Wrapper Architecture for Homomorphic Encryption in Machine Learning 266
Martin Nocker (MCI - The Entrepreneurial School, Austria), Linus Henke (MCI - The Entrepreneurial School, Austria), and Pascal Schöttle (MCI - The Entrepreneurial School, Austria)

Hallucination Detection in LLMs via Beam Search Sampling and Semantic Consistency Analysis... 274
Radouane Bouchekir (An-Institut Technische Universität München, Germany), Fathiyeh Faghih (An-Institut Technische Universität München, Germany), and Tewodros A. Beyene (An-Institut Technische Universität München, Germany)

Securing AI Code Generation Through Automated Pattern-Based Patching 282
Francesco Altiero (University of Naples Federico II, Italy), Domenico Cotroneo (University of Naples Federico II, Italy), Roberta De Luca (University of Naples Federico II, Italy), and Pietro Liguori (University of Naples Federico II, Italy)

Decoding Neighborhood Environments with Large Language Models 290
Andrew Cart (UNC Pembroke, USA), Shaohu Zhang (UNC Pembroke, USA), Melanie Escue (UNC Pembroke, USA), Xugui Zhou (Louisiana State University, USA), Haitao Zhao (UNC Pembroke, USA), Prashanth BusiReddyGari (UNC Pembroke, USA), Beiyu Lin (University of Oklahoma, USA), and Shuang Li (NC A&T State University, USA)

A Lightweight Reputation-Based Mechanism for Incentivizing Cooperation in Decentralized Federated Learning 298
Kavindu Herath (Purdue University, USA), Suraj Mahangade (Purdue University, USA), and Saurabh Bagchi (Purdue University, USA)

Author Index **305**