

2026 56th Annual IEEE International Conference on Dependable Systems and Networks Workshops (DSN-W 2026)

**Charlotte, North Carolina, USA
22-25 June 2026**

IEEE Catalog Number: CFP2641K-POD
ISBN: 979-8-3195-3245-9



Copyright © 2026, IEEE

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:	CFP2641K-POD
ISBN (Print-On-Demand):	979-8-3195-3245-9
ISBN (Online):	979-8-3195-3244-2
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

TABLE OF CONTENTS

Multi-Agent-based Failure Recovery Planning for a Connected Vehicle Platform	1
<i>Aoi Matsuda, Ippo Hiroi, Fumio Machida, Naohiro Ohtsu</i>	
Software-defined SEV for Confidential VMs Based on the Delegation Architecture in RISC-V	9
<i>Junpei Matsushita, Kenichi Kourai</i>	
From Agent Failure Paths to Quantified Residual Risk: A Compositional Framework for Resilient Agentic AI	17
<i>Hassan Karim, Sai Sitharaman, Deepti Gupta, Danda B. Rawat</i>	
Composable Trust in Agentic AI: Bridging Architectural Capability and System-Level Assurance	25
<i>Omar Al-Refai, Ibrahim Shahbaz, Eman Hammad</i>	
Agentic AI for Continuous Intelligence in Future Smart Connected Systems	29
<i>Likhitha Annapurna Kavuri, Deepti Gupta, Eman Hammad</i>	
NinjaShell: Skill-Aware Defense Against Malicious Agentic Skills	44
<i>Haddy Alchaer, Joseph Ghanem, Saurabh Bagchi</i>	
Consequence-Driven Dependability Models for Cyber-Physical Systems (CPS)	52
<i>Ronan Oostveen, Stefano Simonetto, Peter Bosch, Alessandro Chiumento, Maarten van Steen</i>	
Safety Beyond the Interface: Detecting Harm via Latent States in Large Language Models	56
<i>Alizishaan Khatri, Chiquita Prabhu, Omkar Neogi</i>	
From Threat Intelligence to Decision Theory: ATT&CK-Derived Utility Functions for Adversarial Risk Analysis in NIDS	61
<i>Mayank Raj, Nathaniel D. Bastian, Lance Fiondella, Gokhan Kul</i>	
PACT: Predictive Approximate Computing with Temporal Guarantees	67
<i>Gustavo Londono, Sibin Mohan, Sathish Gopalakrishnan, Radha Venkatagiri</i>	
Threat-Oriented Digital Twinning for Security Evaluation of Autonomous Platforms	72
<i>Thomas J. Neubert, Laxima Niure Kandel, Berker Peköz</i>	
Drivers of Secure and Correct Code: A Factorial Study of Size, Pre-Training, and Data Quality	78
<i>Pietro Liguori, Rrezarta Krasniqi, Domenico Cotroneo</i>	
Model Chunking in Decentralized Learning: From Privacy Defense to Privacy Leakage	85
<i>Halil Betmezoğlu, Bart Cox, Jérémie Decouchant</i>	
On the Reliability of Targeted Unlearning in 4-Bit Quantized LLMs	94
<i>Syed Ahsan Ali</i>	
Color Matters: Trigger Color Affects Success in Federated Backdoor Attacks	99
<i>Kavindu Herath, Joshua C. Zhao, Saurabh Bagchi</i>	
Establishing Zero-Shot LLM Performance at Network Tomography	106
<i>India-Jane Barry, Ilir Gashi, Kizito Salako, Pedro Marques, Pranava Madhyastha</i>	
Seeing in Shades of Gray: Real-time Federated Image-Based Malicious Traffic Detection	115
<i>Sapthak Mohajon Turjya, Moaz Usama, Mulham Fawakherji, Mahmoud Abouyoussef, Islam Obaidat</i>	

LLM-PEA: Leveraging Large Language Models Against Phishing Email Attacks	122
<i>Najmul Hasan, Prashanth BusiReddyGari, Haitao Zhao, Yihao Ren, Jinsheng Xu, Shaohu Zhang</i>	
Latent Space Probing for Adult Content Detection in Video Generative Models	129
<i>Alizishaan Khatri, Chiquita Prabhu</i>	
Trust Without Safeguards: A Red-Teaming Study of ProteinMPNN in Open Protein Design Pipelines	138
<i>Tia Pope, Ahmad Patooghy</i>	
On the Extreme Variance of Certified Local Robustness Across Model Seeds	145
<i>Minh Le, Phuong Cao</i>	
Resilience Assessment of AI Accelerators: A Driver-Level Fault Injection Methodology	152
<i>Marcello Cinque, Luigi De Simone, Nike Di Giacomo</i>	
AdROD: Adaptive Redundancy for Object Detection in Autonomous Driving	154
<i>Shunsuke Nagao, Fumio Machida</i>	
Controller Placement in Hybrid SDN Networks: Classical Heuristics vs Quantum-inspired Optimization	161
<i>Salman Khan, Deborsi Basu, Uttam Ghosh, Raja Datta</i>	
Quantum Generative Adversarial Networks for EEG-Based Sleep Stage Classification in Noiseless and Noisy Scenarios	169
<i>Sthefanie J. G. Passo, Ikram U. Khan, John J. Prevost</i>	
A Dependability Profile for Hybrid Quantum–Classical Systems	177
<i>Piyush A. Sonawane, Andrew Kelly, Naveed Mahmud</i>	
ThermalQuest: Gamifying Thermal Side-Channel Attack Education with Interactive Pipeline and Memory Visualization	184
<i>Jaswanth Chithu Sudharsan, Gökhan Kul</i>	
A Case for Unifying Trusted Execution Environments	188
<i>Thomas Prévost, Pierre-Louis Aublin, Hajime Tazaki, Kuniyasu Suzuki</i>	
Binding Application-Layer Provenance to CPU-rooted Attestation in Confidential VMs via a Kernel-resident Pseudo-CA	192
<i>Zen Ishikura, Sakae Chikara, Fumiaki Kudoh, Gen Takahashi, Hiroki Itoh, Kuniyasu Suzuki</i>	
Attestable Build Chain: Enabling Trust in Reproducible Builds	196
<i>Kenichiro Muto, Kuniyasu Suzuki</i>	
Automated Resilience Assessment for Autonomous Systems Using System-on-Chip Architectures	204
<i>Abigail Butka, Brian Butka</i>	
DisTrust: Adaptive Trust-Based Verification for Resilient Distributed Computation	212
<i>Fouad Afiouni, Saurabh Bagchi, Aravind Machiry</i>	