2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W 2023)

Porto, Portugal
27 – 30 June 2023

IEEE Catalog Number: CFP2341K-POD
ISBN: 979-8-3503-2544-7

Copyright © 2023 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:	CFP2341K-POD
ISBN (Print-On-Demand):	979-8-3503-2544-7
ISBN (Online):	979-8-3503-2543-0
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

2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)

DSN-W 2023

Table of Contents

Welcome Message from the DSN 2023 General Chairs ..... **xiii**
Message from the Workshop Chairs of DSN 2023 ..... **xv**
Message from the SSIV 2023 Organizers ..... **xvii**
Message from the DCDS 2023 Organizers ..... **xix**
Message from the DSML 2023 Organizers ..... **xxi**
Message from VERDI 2023 Organizers ..... **xxiii**
Message from the AxC 2023 Organizers ..... **xxiv**
SSIV 2023 Committee ..... **xxv**
DCDS 2023 Committee ..... **xxvi**
DSML 2023 Committee ..... **xxvii**
VERDI 2023 Committee ..... **xxviii**
AxC 2023 Committee ..... **xxix**
SSIV 2023 Keynote ..... **xxx**
DCDS 2023 Keynotes ..... **xxxi**
DSML 2023 Keynotes ..... **xxxiii**
VERDI 2023 Keynotes ..... **xxxv**
AxC 2023 Keynote ..... **xxxvii**

DCDS '23: DSN Workshop on Data-Centric Dependability and Security

Research Session 1: Diagnosis and Analysis of System Failures

Diagnosing Applications' I/O Behavior through System Call Observability 1
Tânia Esteves (INESC TEC & U. Minho), Ricardo Macedo (INESC TEC & U. Minho), Rui Oliveira (INESC TEC & U. Minho), and João Paulo (INESC TEC & U. Minho)

Predicting Cloud Applications Failures from Infrastructure Level Data 9
Jomar Domingos (University of Coimbra), Frederico Cerveira (University of Coimbra), Raul Barbosa (University of Coimbra), and Henrique Madeira (University of Coimbra)

Underestimation-Aware Failure Statistical Model Creation for Large Scale Critical Systems 17
Szilárd Bozóki (Budapest University of Technology and Economics, Hungary), Imre Kocsis (Budapest University of Technology and Economics, Hungary), and András Pataricza (Budapest University of Technology and Economics, Hungary)

Research Session 2: Vulnerabilities and Malicious Websites

IVSign: Interpretable Vulnerability Signature Via Code Embedding and Static Analysis 25
Ao Ding (Shanghai Jiao Tong University;Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, China), Gaolei Li (Shanghai Jiao Tong University;Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, China), Xiaoyu Yi (Shanghai Jiao Tong University;Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, China), and Yuchen Liu (North Carolina State University, USA)

Security Risk Growth Models for Software Vulnerability Assessment 32
Takashi Minohara (Takushoku University, Japan) and Masaya Shimakawa (Takushoku University, Japan)

JABBERWOCK: A Tool for WebAssembly Dataset Generation towards Malicious Website Detection ... 36
Chika Komiya (Osaka University, Japan), Naoto Yanai (Osaka University, Japan), Kyosuke Yamashita (Osaka University, Japan), and Shingo Okamura (National Institute of Technology, Nara College, Japan)

SSIV'2023: 9th International Workshop on Safety and Security of Intelligent Vehicles

Session 1: Planning and Optimization

EMER-GO: Real-Time Grip Enhanced Speed Advisory for Emergency Intelligent Transportation Systems 40
Vincenzo M. Arricale (Megaride S.r.l., Italy), Michele Caggiano (South Engineering S.r.l., Italy), Marcello Cinque (Federico II University of Naples, Italy), Angelo Coppola (Federico II University of Naples, Italy), Flavio Farroni (Federico II University of Naples, Italy), Mario Fiorentino (South Engineering S.r.l., Italy), Andrea Garofalo (South Engineering S.r.l., Italy), Andrea Marchetta (Federico II University of Naples, Italy), Antimo Perfetto (Federico II University of Naples, Italy), and Aleksandr Sakhnevych (Federico II University of Naples, Italy)

Multi-objective Optimization for an Online Re-Planning of Autonomous Vehicles 48
Kilian Le Gall (Lab-STICC/UBO, France), Laurent Lemarchand (Lab-STICC/UBO, France), and Catherine Dezan (Lab-STICC/UBO, France)

Session 2: Safety Assessment and Evaluation

An ETSI ITS-Enabled Robotic Scale Testbed for Network-Aided Safety-Critical Scenarios 52
José M. Pinheiro (Faculdade de Engenharia – Universidade do Porto, Portugal), Ênio V. Filho (Instituto Superior de Engenharia do Porto – Instituto Politécnico do Porto;CISTER Research Center in Real-Time & Embedded Computing Systems, Portugal), Pedro M. Santos (Instituto Superior de Engenharia do Porto – Instituto Politécnico do Porto;CISTER Research Center in Real-Time & Embedded Computing Systems, Portugal), and L. Almeida (Faculdade de Engenharia – Universidade do Porto;CISTER Research Center in Real-Time & Embedded Computing Systems, Portugal)

PSP Framework: A Novel Risk Assessment Method in Compliance with ISO/SAE-21434 60
Franco Oberti (Politecnico di Torino;PUNCH Softrontix, Italy), Ernesto Sanchez (Politecnico di Torino, Italy), Alessandro Savino (Politecnico di Torino, Italy), Filippo Parisi (PUNCH Softrontix, Italy), and Stefano Di Carlo (Politecnico di Torino, Italy)

Edge-Aided V2X Collision Avoidance with Platoons: Towards a Hybrid Evaluation Toolset 68
João Pereira (Instituto Superior de Engenharia do Porto (ISEP)), Harrison Kurunathan (Instituto Superior de Engenharia do Porto (ISEP);CISTER Research Center), Enio Filho (Instituto Superior de Engenharia do Porto (ISEP);CISTER Research Center), and Pedro M. Santos (Instituto Superior de Engenharia do Porto (ISEP);CISTER Research Center)

Integration of U-Space Safety Assessment Methodologies with Experimentation 72
Omid Asghari (University of Coimbra, Portugal), Naghmeh Ivaki (University of the Coimbra, Portugal), and Henrique Madeira (University of Coimbra, Portugal)

Session 3: Security Assessment and Algorithms

Susceptibility of Autonomous Driving Agents to Learning-Based Action-Space Attacks 76
Yuting Wu (Nanyang Technological University), Xin Lou (Illinois at Singapore), Pengfei Zhou (University of Pittsburgh), Rui Tan (Nanyang Technological University), Zbigniew T. Kalbarczyk (University of Illinois at Urbana-Champaign), and Ravishankar K. Iyer (University of Illinois at Urbana-Champaign)

An Automotive Cybersecurity Maturity Level Assessment Programme 84
Patrick Grümer (University of Porto, Portugal) and Pedro Brandão (University of Porto, Portugal)

CarFASE: A Carla-based Tool for Evaluating the Effects of Faults and Attacks on Autonomous Driving Stacks 92
Mehdi Maleki (RISE Research Institutes of Sweden, Sweden), Ashfaq Farooqui (RISE Research Institutes of Sweden, Sweden), and Behrooz Sangchoolie (RISE Research Institutes of Sweden, Sweden)

BEAT-Traffic: A Blockchain-Enabled Infrastructure for Anonymous-Yet-Traceable Traffic Reporting 100
Marina Dehez-Clementi (Université de Toulouse, France), Jean-Christophe Deneuville (Université de Toulouse, France), Emmanuel Lochin (Université de Toulouse, France), and Jérôme Lacan (Université de Toulouse, France)

Safeguarding Cooperative Maneuver Information with Practical Byzantine Fault Tolerance 108
Emanuel Vieira (Universidade de Aveiro, Portugal), João Almeida (Universidade de Aveiro, Portugal), Joaquim Ferreira (Universidade de Aveiro;Campus Universitário de Santiago, Portugal), and Paulo C. Bartolomeu (Universidade de Aveiro, Portugal)

Session 4: Safe Collaborative Manoeuvres

Minimal Risk Manoeuvre Strategies for Cooperative and Collaborative Automated Vehicles 116
Victoria Vu (Semcon Sweden AB, Sweden), Fredrik Warg (RISE Research Institutes of Sweden, Sweden), Anders Thorsén (RISE Research Institutes of Sweden, Sweden), Stig Ursing (Semcon Sweden AB, Sweden), Fredrik Sunnerstam (Agreat AB, Sweden), Jimmy Holler (Epiroc Rock Drills AB, Sweden), Carl Bergenhem (Qamcom Research and Technology AB, Sweden), and Irina Cosmin (Agreat AB, Sweden)

DSML 2023: Dependable and Secure Machine Learning

Session 1: Keynote Talk

Session 2: Dependable and Secure Image Classification

Adversarial Patch Detection and Mitigation by Detecting High Entropy Regions 124
Niklas Bunzel (Fraunhofer SIT / Athene, Germany), Ashim Siwakoti (Fraunhofer SIT / Athene, Germany), and Gerrit Klause (Fraunhofer SIT / Athene, Germany)

IB-RAR: Information Bottleneck as Regularizer for Adversarial Robustness 129
Xiaoyun Xu (Radboud University, The Netherlands), Guilherme Perin (Leiden University, The Netherlands), and Stjepan Picek (Radboud University, The Netherlands)

A Concise Analysis of Pasting Attacks and Their Impact on Image Classification 136
Niklas Bunzel (Fraunhofer SIT / Athene, Germany) and Lukas Graner (Fraunhofer SIT / Athene, Germany)

Session 3: Keynote Talk

Session 4: Other Dependable and Secure ML Systems

FADO: A Federated Learning Attack and Defense Orchestrator 141
Filipe Rodrigues (Universidade de Lisboa, Portugal), Rodrigo Simões (Universidade de Lisboa, Portugal), and Nuno Neves (Universidade de Lisboa, Portugal)

Enhancing the Reliability of Perception Systems using N-Version Programming and Rejuvenation 149
Júlio Mendonça (University of Luxembourg, Luxembourg), Fumio Machida (University of Tsukuba, Japan), and Marcus Völp (University of Luxembourg, Luxembourg)

Revenue Maximization of a Slice Broker in the Presence of Byzantine Faults 157
Muhidul Islam Khan (University of Stavanger, Norway) and Gianfranco Nencioni (University of Stavanger, Norway)

AxC23: 8th Workshop on Approximate Computing

Regular Session #1 - Cross-Layer and AI-based Approximation

Cross-Layer Approximations for System-Level Optimizations: Challenges and Opportunities 163
Jorge Castro-Godínez (Instituto Tecnológico de Costa Rica (TEC), Costa Rica), Muhammad Abdullah Hanif (New York University Abu Dhabi (NYUAD), UAE), and Muhammad Shafique (New York University Abu Dhabi (NYUAD), UAE)

Design Space Exploration of Approximate Computing Techniques with a Reinforcement Learning Approach 167
Sepide Saeedi (Politecnico di Torino, Italy), Alessandro Savino (Politecnico di Torino, Italy), and Stefano di Carlo (Politecnico di Torino, Italy)

Regular Session #2 - Circuit Level Approximation

Generic Accuracy Configurable Matrix Multiplication-Addition Accelerator using HLS 171
Luis G. León-Vega (Università degli Studi di Trieste, Italy) and Jorge Castro-Godínez (Instituto Tecnológico de Costa Rica, Costa Rica)

A Parametrizable Template for Approximate Logic Synthesis 175
Morteza Rezaalipour (USI Università della Svizzera italiana, Switzerland), Marco Biasion (USI Università della Svizzera italiana, Switzerland), Ilaria Scarabottolo (USI Università della Svizzera italiana, Switzerland), George A. Constantinides (Imperial College London, United Kingdom), and Laura Pozzi (USI Università della Svizzera italiana, Switzerland)

Input-Aware Accuracy Characterization for Approximate Circuits 179
Ali Piri (Univ Lyon, ECL, INSA Lyon, CNRS, UCBL, CPE Lyon, INL, France), Salvatore Pappalardo (Univ Lyon, ECL, INSA Lyon, CNRS, UCBL, CPE Lyon, INL, France), Salvatore Barone (University of Naples Federico II, Italy), Mario Barbareschi (University of Naples Federico II, Italy), Bastien Deveautour (Univ Lyon, ECL, INSA Lyon, CNRS, UCBL, CPE Lyon, INL, France), Marcello Traiola (University of Rennes, France), Ian O'Connor (Univ Lyon, ECL, INSA Lyon, CNRS, UCBL, CPE Lyon, INL, France), and Alberto Bosio (Univ Lyon, ECL, INSA Lyon, CNRS, UCBL, CPE Lyon, INL, France)

AxASRE: A Novel Approach to Approximate Adder Synthesis Results Estimation. 183
Pedro T. L. Pereira (Graduate Program on Microelectronics (PGMicro) - Federal University of Rio Grande do Sul (UFRGS), Brazil), Guilherme Paim (Graduate Program on Microelectronics (PGMicro) - Federal University of Rio Grande do Sul (UFRGS), Brazil), Paulo Flores (Instituto Superior Técnico, Portugal), Eduardo Costa (Graduate Program on Electronic Engineering and Computing - Catholic University of Pelotas (UCPel), Brazil), and Sergio Bampi (Graduate Program on Microelectronics (PGMicro) - Federal University of Rio Grande do Sul (UFRGS), Brazil)

Regular Session #3 - Approximation in the Field

Exploit Approximation to Support Fault Resiliency in MPI-based Applications 187
Roberto Rocco (Informazione e Bioingegneria (DEIB) of Politecnico di Milano, Italy) and Gianluca Palermo (Informazione e Bioingegneria (DEIB) of Politecnico di Milano, Italy)

Stochastic Computing as a Defence Against Adversarial Attacks 191
Florian Neugebauer (University of Stuttgart, Germany), Vivek Vekariya (fortiss GmbH, Germany), Ilia Polian (University of Stuttgart, Germany), and John P. Hayes (University of Michigan, USA)

Guardband Optimization for the Preconditioned Conjugate Gradient Algorithm 195
Natalia Lylina (University of Stuttgart, Germany), Stefan Holst (Department of Creative Informatics at Kyushu Institute of Technology, Japan), Hanieh Jafarzadeh (University of Stuttgart, Germany), Alexandra Kourfali (University of Stuttgart, Germany), and Hans-Joachim Wunderlich (University of Stuttgart, Germany)

Multi-metric SMT-Based Evaluation of Worst-Case-Error for Approximate Circuits 199
Morteza Rezaalipour (USI Università della Svizzera italiana, Switzerland), Lorenzo Ferretti (Micron Technology, United States), Ilaria Scarabottolo (USI Università della Svizzera italiana, Switzerland), George A. Constantinides (Imperial College London, United Kingdom), and Laura Pozzi (USI Università della Svizzera italiana, Switzerland)

Low Power Streaming of Sensor Data Using Gray Code-Based Approximate Communication 203
Somayeh Sadeghi-Kohan (Paderborn University, Germany), Sybille Hellebrand (Paderborn University, Germany), and Hans-Joachim Wunderlich (University of Stuttgart, Germany)

VERDI 2023: 1st International Workshop on Verification & Validation of Dependable Cyber-Physical Systems

Session #1

NetLoiter: A Tool for Automated Testing of Network Applications using Fault-Injection 207
Michal Rozsíval (Brno University of Technology) and Aleš Smrčka (Brno University of Technology)

RISC-V Timing-Instructions for Open Time-Triggered Architectures 211
Nithin Ravani Nanjundaswamy (German Aerospace Center, Germany), Gregor Nitsche (German Aerospace Center, Germany), Frank Poppen (German Aerospace Center;NXP Semiconductors Germany GmbH, Germany), and Kim Grüttner (German Aerospace Center, Germany)

Session #2

Evaluating the Safety Impact of Network Disturbances for Remote Driving with Simulation-Based Human-in-The-Loop Testing 215
Shrishti Trivedi (KTH Royal Institute of Technology, Sweden) and Fredrik Warg (RISE Research Institutes of Sweden, Sweden)

Using AI to Inject Vulnerabilities in Python Code 223
Frédéric C. G. Bogaerts (University of Coimbra, Portugal), Naghmeh Ivaki (University of Coimbra, Portugal), and José Fonseca (Polytechnic Institute of Guarda, Portugal)

Timeseries-aware Uncertainty Wrappers for Uncertainty Quantification of Information-Fusion-Enhanced AI Models based on Machine Learning 231
Janek Groß (Fraunhofer IESE, Germany), Michael Kläs (Fraunhofer IESE, Germany), Lisa Jöckel (Fraunhofer IESE, Germany), and Pascal Gerber (Fraunhofer IESE, Germany)

Modelling V&V Workflows to Improve Development Processes of Software-Intensive Systems 239
Thomas Bauer (Fraunhofer IESE, Germany), Wolfgang Herzner (Austrian Institute of Technology (AIT), Austria), Bob Hruska (LieberLieber Software GmbH, Austria), Katia Di Blasio (Intecs Solutions S.p.A., Italy), and Zain Shahwar (Pumacy Technologies AG, Germany)

Session #3

SMT-Based Stability Verification of an Industrial Switched PI Control Systems 243
Stylianos Basagiannis (Collins), Ludovico Battista (FBK), Anna Becchi (FBK), Alessandro Cimatti (FBK), Georgios Giantamidis (Collins), Sergio Mover (Ecole Polytechnique), Alberto Tacchella (FBK), Stefano Tonetta (FBK), and Vassilios Tsachouridis (Collins)

llhsc: A Devicetree Syntax and Semantic Checker 251
Vítor Rodrigues (VORTEX Colab, Portugal) and André Matos Pedro (VORTEX-CoLab, Portugal)

Translating Natural Language Requirements to Formal Specifications: A Study on GPT and Symbolic NLP 259
Iat Tou Leong (University of Coimbra) and Raul Barbosa (University of Coimbra)

Session #4

Simplifying Requirements Formalization for Resource-Constrained Mission-Critical Software 263
Carlos Mão de Ferro (Universidade de Lisboa), Anastasia Mavridou (KBR Inc.;NASA Ames Research Center), Michael Dille (KBR Inc.;NASA Ames Research Center), and Francisco Martins (Universidade dos Açores)

Preliminary Risk and Mitigation Assessment in Cyber-Physical Systems 267
András Földvári (Budapest University of Technology and Economics), Francesco Brancati (ResilTech S.r.l.), and András Pataricza (Budapest University of Technology and Economics)

Formal Verification for Safe AI-based Flight Planning for UAVs 275
R. Bouchekir (fortiss GmbH, Germany), M. Guzman (fortiss GmbH, Germany), A. Cook (Third party, Germany), J. Haindli (Third party, Germany), and R. Woolnough (Third party, Germany)

Formalizing Model Inference of MicroPython 283
Carlos Mão de Ferro (Universidade de Lisboa, Portugal), Tiago Cogumbreiro (University of Massachusetts Boston, USA), and Francisco Martins (Universidade dos Açores, Portugal)

SIMoT: A Low-Fidelity Orchestrator Simulator for Task Allocation in IoT Devices 290
Tiago Fragoso (University of Porto, Portugal), David Silva (University of Porto, Portugal), João Pedro Dias (University of Porto, Portugal), André Restivo (University of Porto, Portugal), and Hugo Sereno Ferreira (University of Porto, Portugal)

Author Index **297**