

**2020 50th Annual IEEE/IFIP
International Conference on
Dependable Systems and
Networks Workshops
(DSN-W 2020)**

**Valencia, Spain
29 June - 2 July 2020**



**IEEE Catalog Number: CFP2041K-POD
ISBN: 978-1-7281-7264-4**

**Copyright © 2020 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:	CFP2041K-POD
ISBN (Print-On-Demand):	978-1-7281-7264-4
ISBN (Online):	978-1-7281-7263-7
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

2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN- W) DSN-W 2020

Table of Contents

Message from the Workshop Chairs	ix
Message from the Workshop on Dependable and Secure Machine Learning	x
Message from the Workshop on Data-centric Dependability and Security	xi
Message from the Workshop on High-Performance Computing Platforms for Dependable Autonomous Systems	xii
Message from the Workshop on Safety and Security of Intelligent Vehicles	xiii
Sponsors	xiv

DSML 2020: Dependable and Secure Machine Learning

Attacks

TAaMR: Targeted Adversarial Attack Against Multimedia Recommender Systems	1
<i>Tommaso Di Noia (Politecnico di Bari), Daniele Malitesta (Politecnico di Bari), and Felice Antonio Merra (Politecnico di Bari)</i>	
On the Generation of Unrestricted Adversarial Examples	9
<i>Mehrgan Khoshpasand (University of New Brunswick) and Ali Ghorbani (University of New Brunswick)</i>	
Blackbox Attacks on Reinforcement Learning Agents Using Approximated Temporal Information	16
<i>Yiren Zhao (University of Cambridge), Ilia Shumailov (University of Cambridge), Han Cui (University of Bristol), Xitong Gao (Shenzhen Institutes of Advanced Technology), Robert Mullins (University of Cambridge), and Ross Anderson (University of Cambridge)</i>	

Validation, Verification, and Defense

- PyTorchFI: A Runtime Perturbation Tool for DNNs .25.....
Abdulrahman Mahmoud (University of Illinois at Urbana-Champaign), Neeraj Aggarwal (University of Illinois at Urbana-Champaign), Alex Nobbe (University of Illinois at Urbana-Champaign), Jose Rodrigo Sanchez Vicarte (University of Illinois at Urbana-Champaign), Sarita V. Adve (University of Illinois at Urbana-Champaign), Christopher W. Fletcher (University of Illinois at Urbana-Champaign), Iuri Frosio (NVIDIA), and Siva Kumar Sastry Hari (NVIDIA)
- Online Verification through Model Checking of Medical Critical Intelligent Systems .32.....
João Martins (University of Coimbra, CISUC, DEI), Raul Barbosa (University of Coimbra, CISUC, DEI), Nuno Lourenço (University of Coimbra, CISUC, DEI), Jacques Robin (University of Paris 1 Pantheon-Sorbonne, CRI), and Henrique Madeira (University of Coimbra, CISUC, DEI)
- BlurNet: Defense by Filtering the Feature Maps .38.....
Ravi Raju (University of Wisconsin-Madison) and Mikko Lipasti (University of Wisconsin-Madison)

DCDS '20: DSN Workshop on Data-Centric Dependability and Security

- Association Rule Mining with Differential Privacy .47.....
Hao Zhen (National Taiwan University), Bo-Cheng Chiou (Feng Chia University), Yao-Tung Tsou (Feng Chia University), Sy-Yen Kuo (National Taiwan University), and Pang-Chieh Wang (Computational Intelligence Technology Center, Industrial Technology Research Institute)
- Pelican: A Deep Residual Network for Network Intrusion Detection .55.....
Peilun Wu (UNSW), Hui Guo (UNSW), and Nour Moustafa (UNSW)

Workshop on High-Performance Computing Platforms for Dependable Autonomous Systems

Hardware Platforms

- Open Source Hardware: An Opportunity for Critical Systems .63.....
Jimmy Le Rhun (Thales Research & Technology), Sylvain Girbal (Thales Research & Technology), and Daniel Gracia Pérez (Thales Research & Technology)
- Development of a NOEL-V RISC-V SoC Targeting Space Applications .66.....
Jan Andersson (Cobham Gaisler)

Software Platforms

Safe and Secure Software Updates on High-Performance Embedded Systems .68.....
Iruno Agirre (Ikerlan Technology Research Centre)

Certification Challenges

Approaching Certification of Complex Systems .70.....
Nicholas Mc Guire (Open Source Automation Development Lab) and Imanol Allende (Open Source Automation Development Lab)

AI Safety Landscape: From Short-Term Specific System Engineering to Long-Term Artificial General Intelligence .72.....
Jose Hernandez-Orallo (Universitat Politecnica de Valencia)

SSIV 2020: 6th International Workshop on Safety and Security of Intelligent Vehicles

AI and Adaptive Systems

AI and Reliability Trends in Safety-Critical Autonomous Systems on Ground and Air .74.....
Jyotika Athavale (Intel Corporation), Andrea Baldovin (Intel, Germany), Ralf Graefe (Intel, Germany), Michael Paulitsch (Intel Corporation), and Rafael Rosales (Intel, Germany)

Reward Tuning for Self-Adaptive Policy in MDP Based Distributed Decision-Making to Ensure a Safe Mission Planning .78.....
Mohand Hamadouche (Lab-STICC, CNRS), Catherine Dezan (Lab-STICC, CNRS), and Kalinka R. L. J. C. Branco (Universidade de Sao Paulo)

Dependability and Security Analysis

The Quantitative Risk Norm - A Proposed Tailoring of HARA for ADS .86.....
Fredrik Warg (RISE Research Institutes of Sweden), Rolf Johansson (Autonomous Intelligent Driving), Martin Skoglund (RISE Research Institutes of Sweden), Anders Thorsén (RISE Research Institutes of Sweden), Mattias Brännström (Zenuity AB), Magnus Gyllenhammar (Zenuity AB), and Martin Sanfridson (Volvo Technology AB)

Analysis of Cybersecurity Mechanisms with Respect to Dependability and Security Attributes.94
Behrooz Sangchoolie (RISE Research Institutes of Sweden), Peter Folkesson (RISE Research Institutes of Sweden), Pierre Kleberger (RISE Research Institutes of Sweden), and Jonny Vinter (RISE Research Institutes of Sweden)

Exploring Fault Parameter Space Using Reinforcement Learning-Based Fault Injection .102.....
Mehrdad Moradi (University of Antwerp), Bentley James Oakes (University of Antwerp), Mustafa Saraoglu (Technische Universität Dresden), Andrey Morozov (Technische Universität Dresden), Klaus Janschek (Technische Universität Dresden), and Joachim Denil (University of Antwerp)

Architecture and Deployment

Flexible Deployment and Enforcement of Flight and Privacy Restrictions for Drone Applications .110.....	
<i>Nasos Grigoropoulos (University of Thessaly) and Spyros Lalis (University of Thessaly)</i>	
Conceptual Design of Human-Drone Communication in Collaborative Environments .118.....	
<i>Hans Dermot Doran (Inst. of Embedded Systems / ZHAW, Winterthur, Switzerland), Monika Reif (Inst. of Applied Mathematics and Physics / ZHAW), Marco Oehler (Zurich University of Applied Sciences), Curdin Stöhr (Zurich University of Applied Sciences), and Pierluigi Capone (Centre for Aviation / ZHAW)</i>	
A Hierarchical Fault Tolerant Architecture for an Autonomous Robot .122.....	
<i>Anthony Favier (INPT ENSEEIHT, Université de Toulouse, France), Antonin Messioux (INPT ENSEEIHT, Université de Toulouse, France), Jérémie Guiochet (LAAS CNRS, Université de Toulouse, France), Jean-Charles Fabre (LAAS CNRS, INPT, Université de Toulouse, France), and Charles Lesire (ONERA/DTIS, Université de Toulouse, France)</i>	
Author Index .131	