IFIP WG 10.4 Agenda for workshop (Jan 20, 2022 - Jan 22, 2022)

Each talk gets 30 mins + 10 mins for Q&A. Each session is 1 hour 20 mins long.

All times below are in **CET (Central European Time)**

Workshop Title: ***"AI and Dependability: And the twain shall meet"***

Jan 20th (Day 1): Total time: 3 hours

Introduction to the workshop (10 mins) - 2:00 PM

Session 1: Software Engineering and Testing (2:10 PM to 3:30 PM)

Session Chair: Yair Amir, Johns Hopkins Univ.
Rapporteur: Andrea Cecccarelli, Univ. of Florence

Presenters:

1. Michael Lyu, CUHK, *Software Dependability Modeling with A Data-Driven AI Paradigm*

2. Lionel Briand, Univ. of Ottawa, *Trustworthy Machine Learning-Enabled Systems*

10 minute break

Session 2: Self-Driving Cars and Safety (3:40 PM to 5:00 PM)

Session Chair: Cristina Nita-Rotaru, Northeastern Univ.
Rapporteur: Domenico Cotroneo, Univ. of Naples

Presenters:

1. Paolo Rech, University of Trento, *Can we Rely on Self-Driving Cars? Evaluation and Mitigation of Neutron-Induced Errors in Convolutional Neural Networks for Autonomous Vehicles*

2. Daniel Schneider, Fraunhofer IESE, *Safety-critical systems with Machine Learning components: Challenges and Solutions*

Jan 21st (Day 2): Total time: 3 hours

Session 1: Safety and other considerations (2:00 PM to 3:20 PM)

Session Chair: Lorenzo Strigini, City University, London
Rapporteur: António Casimiro, Univ. of Lisboa

Presenters:

1. Andre Lourenco, CardioID*, Integrating Physiological Monitoring in the Industry*

2. Timothy Tsai, Nvidia, *What Safety Challenges for Autonomous Systems Would Benefit from Research?*

   10 minute break

Session 2: Summary and free form discussion (3:30 PM to 4:50 PM)

1. Summary from the rapporteurs of the different sessions (15-20 mins)

2. Free form discussion (1 hour)

   Closing (10 mins)

Jan 22nd (Day 3 - Members only): Total time: TBD

1. Business meeting (90 mins)

10 minute break

2. Research reports (TBD)

   a. Jay Lala, Raytheon (20 minutes) - *Autonomous Vehicles: Safety Measures and Benchmarks for Perception & Cognition Functions*

Talk Titles, Abstracts and Bios (in order of appearance in the schedule)

1. Michael Lyu, CUHK

Title: Software Dependability Modeling with A Data-Driven AI Paradigm

Abstract: Traditional software dependability modeling is mainly performed by treating the software under operation as a black box and by predicting its future behavior based on the observed number of failures in the past. Analytical models assuming various statistical distributions have been devel-oped to fit the failure data. This approach becomes inadequate when it comes to modern software systems, especially cloud service systems, which are complex, huge, highly interactive, and wide-ly distributed.

In this talk, I will introduce a new paradigm for software dependability modeling with data-driven AI techniques, in which four perspectives of dependability modeling for modern software systems will be discussed: 1) from black-box to white-box, (2) from model-centric to data-centric, (3) from macro-level to micro-level, and (4) from static analysis to dynamic analysis. In (1), going beyond a single failure number, we open the box of software to characterize the dependability more comprehensively. In (2), instead of comparing the goodness of different analytical models, we reveal software dependability details from the heterogeneous data. In (3), by delving into the internal software operations, we investigate dependability issues in a fine-grained way. In (4), facing the ever-changing nature of today's software, we demonstrate how the data-driven paradigm facilitates the dynamic aspect of dependability modeling. We conclude that in the evolu-tion of dependability modeling, the paradigm shift to a data-driven AI approach is an inevitable modeling effort to combat the massive complexity of modern software systems.

Bio: Michael Rung-Tsong Lyu is a Choh-Ming Li Professor of Computer Science & Engineering at the Chinese University of Hong Kong. He received a B.S. in Electrical Engineering from the National Taiwan University, an M.S. in Electrical and Computer Engineering from University of California, Santa Barbara, and a Ph.D. in Computer Science from University of California, Los Angeles. His research interests include software reliability engineering, dependable computing, machine learning, artificial intelligence, and distributed systems. He published a widely cited McGraw-Hill Hand-book of Software Reliability Engineering, and a Wiley book on Software Fault Tolerance. He is a Fellow of the IEEE, a Fellow of ACM, a Fellow of AAAS, and an IEEE Reliability Society Engineer of the Year. He received China Computer Federation (CCF) Overseas Outstanding Contributions Award in 2018, and the 13th Guanghua Engineering Science and Technology Award in 2021.

2. Lionel Briand, Univ. of Ottawa

Title: Trustworthy Machine Learning-Enabled Systems

Abstract: This talk will provide a personal perspective on the state of art regarding the automated testing and analysis of software systems enabled by machine learning. Such systems typically contain components relying on machine learning, whose behavior is not specified or coded but driven by training data, but which interact with other components in the system and play a critical role. Typical examples include cyber-physical systems that rely on machine learning in their perception (e.g., analyzing camera images) and control (e.g., sending commands to actuators) layers. In my reflections, I will rely both on my analysis of the state of the art and personal experience in research projects carried out with industrial partners in the automotive and satellite domains.

Bio: Lionel C. Briand is professor of software engineering and has shared appointments between (1) School of Electrical Engineering and Computer Science, University of Ottawa, Canada and (2) The SnT centre for Security, Reliability, and Trust, University of Luxembourg. He is the head of the SVV department at the SnT Centre and a Canada Research Chair in Intelligent Software Dependability and Compliance (Tier 1). He holds an ERC Advanced Grant, the most prestigious European individual research award, and has conducted applied research in collaboration with industry for more than 25 years, including projects in the automotive, aerospace, manufacturing, financial, and energy domains. He is a fellow of the IEEE and ACM. He was also granted the IEEE Computer Society Harlan Mills award (2012) and the IEEE Reliability Society Engineer-of-the-year award (2013) for his work on model-based verification and testing.

3. Paolo Rech, University of Trento

Title: Can we Rely on Self-Driving Cars? Evaluation and Mitigation of Neutron-Induced Errors in Convolutional Neural Networks for Autonomous Vehicles

Abstract: Driverless cars are the new trend in the automotive market and, to burst deep space exploration, NASA and ESA are willing to add self-driving capabilities to their rovers. Ingenuity, landed in Mars in 2021, is the first autonomous vehicle to move outside of the Earth. To be implemented, a self-driving system needs to analyze a huge amount of images and signals in real time. This is achieved thanks to Convolutional Neural Networks (CNNs) executed on Graphics Processing Units (GPUs) or dedicated accelerators, such as the Google's Tensor Processing Unit (TPU). In the talk, after a brief description of radiation effects at physical level, we will investigate the reliability of GPUs and TPUs, show if and why a neutron-induced corruption can modify the autonomous vehicles behaviors, and discuss the implications of these corruptions for the adoption in large scale of self-driving vehicles.

The presented evaluation, to be accurate and precise, is based on the combination of beam experiments and fault injection at different levels of abstractions (RTL, microarchitectural, and software). This combination allows us to have a realistic evaluation of the error rate, distinguish between tolerable errors and critical errors, and to design efficient and effective hardening solutions for CNNs. By hardening only critical error sources, by modifying some of the key layers in a CNNs, by taking advantage of GPUs novel architectural solutions, or by applying algorithm protection, we are able to significantly increase the reliability of the application (up to 85% error detection) without unnecessary overhead (overhead as low as 0.1%).

Bio: Paolo Rech received his master and Ph.D. degrees from Padova University, Padova, Italy, in 2006 and 2009, respectively. He was then a Post Doc at LIRMM in Montpellier, France. Since 2022, Paolo will be an associate professor at Università di Trento, in Italy and since 2012 he is an associate professor at UFRGS in Brazil. He is the 2019 Rosen Scholar Fellow at the Los Alamos National Laboratory, he received the 2020 impact in society award from the Rutherford Appleton Laboratory, UK. In 2020 Paolo was awarded the Marie Curie Fellowship at Politecnico di Torino, in Italy. His main research interests include the evaluation and mitigation of radiation-induced effects in autonomous vehicles for automotive applications and space exploration, in large-scale HPC centers, and quantum computers.

4. **Daniel Schneider, Fraunhofer IESE**

Title: Safety-critical systems with Machine Learning components: Challenges and Solutions

Abstract: Machine learning is presently a hot topic because numerous very promising application scenarios for this technology emerged in a broad range of application domains. One particular application scenario is using ML in the context of highly automated and autonomous systems. Perception, reasoning, decision making, all being aspects of cognition, are key for such systems, but often difficult to realize by traditional means. ML is showing great promise here and could thus be an important enabler for highly automated and autonomous systems. However, there is a pretty solid blocking point in terms of assuring important properties of ML components. Safety is obviously particularly critical and, if not assured, will lead to delaying or even preventing market introduction of otherwise very promising and innovative systems. This talk will: i) give a short motivation and intro to ML in critical systems, ii) highlight the key challenges from a safety perspective, iii) give a brief overview on solution approaches that are presently pursued, and, iv) detail some of the work going on at IESE, namely in what regards dealing with uncertainties and dynamic risk management.

Bio: Daniel Schneider received his Dipl.Inf. degree (M.Sc.) from TU Kaiserslautern in 2004. Afterwards he became an employee of the Fraunhofer Institute of Experimental Software Engineering (IESE) in Kaiserslautern. During his time at IESE, he assumed different roles (research scientist, project manager, senior engineer, program manager) and received his Dr.-Ing. degree (Ph.D.) from TU Kaiserslautern. Since 2014, he has been the head of the "Safety Engineering" department. Daniel Schneider was and is member and manager of numerous publicly as well as industry funded research projects. He is author and co-author of over 70 conference, journal and magazine publications, most of which focusing on engineering safety critical cooperative automated systems.

5. **André Lourenço, CardioID**

Title: Integrating Physiological Monitoring in the Industry

Abstract: The monitorization of physiological signals is attracting a lot of attention in several applications. From everyday life monitoring of heart rate using wearables, to more sophisticated systems that enable the acquisition of Electrocardiogram (ECG) in a non intrusive way using for example a steering wheel. In this talk we will show how CardioID is developing these ideas and integrating years of research on signal processing and machine learning in industry projects.

Bio: André Lourenço holds a Licenciatura (2001), a MSc (2002), and a PhD in Electrotechnical and Computers Engineering (2014), all from Instituto Superior Técnico (IST), Universidade de Lisboa. After a brief period in the industry, working on IT projects at WeDo Consulting (2001) and on instrumentation and testing at Lusospace (2003-2005), Lourenço has developed his work on academia, and on the scientific transfer of academic research to industry. Since 2005, he lectures at Instituto Superior de Engenharia de Lisboa (ISEL) and collaborates as a researcher at Instituto de Telecomunicações (IT), focused on signal processing and programming. André's speciality is pattern recognition, beginning with clustering algorithms and after that several other machine learning methods applied to biosignal and human-factors analysis. Currently, he is CEO and one of the founders of CardioID Technologies, a Portuguese company that works with sensors, electronics, signal processing, and machine learning for biometrics and health monitoring applications, mainly using physiological signals acquired in unobtrusive and seamless ways in challenging settings (such as vehicles).

6. **Timothy Tsai, Nvidia**

Title: What Safety Challenges for Autonomous Systems Would Benefit from Research?

Abstract: Autonomous systems, including cars, drones, and robots, offer the potential of significantly changing the lives of consumers and the operation of businesses. In addition to the primary need for correct functionality, the safe operation of these systems in an environment with humans, other systems, and other valuable objects is vital. Some safety issues can currently be adequately addressed with sufficient engineering resources. However, other safety issues either require an inordinate amount of resources or have no apparent solutions. This talk will discuss the landscape of autonomous system safety and suggest key areas that would benefit from further research.

Bio: Timothy Tsai is currently a senior research scientist at NVIDIA. He has been investigating resilience as a researcher for several decades in six different corporate research labs in the telecommunications, semiconductor, systems, and storage industries. His current areas of focus include resilience for high-performance computing, autonomous vehicles, and artificial intelligence. He received Ph.D. and M.S. degrees from the University of Illinois at Urbana-Champaign and a B.S. degree from Brigham Young University.