NEWSLETTER °1
NOVEMBER 2021

Welcome to the FOCETA project newsletter n°1!

In a context where applications are increasingly being developed based on complex autonomous systems driven by artificial intelligence, their safety, autonomy and trustworthiness are challenging, especially those of learning-enabled systems, not easily traced by continuous engineering.

The ultimate goal of the FOCETA project is to develop the foundations for continuous engineering of trustworthy learning-enabled autonomous systems. The underlying targeted scientific breakthrough of FOCETA lies in the convergence of model-driven and data-driven approaches. This convergence is further complicated by the need to apply verification and validation incrementally and avoid complete re-verification and re-validation efforts.

Our public newsletters will keep you up-to-date on the progress made within the project. You will discover how the consortium partners cooperate to achieve the project objectives. You will also know how and when we disseminate the FOCETA results.

THE FOCETA PROJECT IN A NUTSHELL

- **4 985 540 € EU funding**
- **656 Person-months**
- **An international consortium**
- **36 months project duration**
- **Started on 01/10/2020**
- **13 partners from 8 countries**

Read more about FOCETA on the project website

This project has received funding from European Union's Horizon 2020 research and innovation programme under grant agreement N°956123.

EDITORIAL BY THE PROJECT COORDINATOR

From the studies of Leibniz to the philosophy view, the human mind and/or brain has been perceived as an information-processing system and thinking as a form of computing. Over three centuries ago, two dreams have been mingled, the philosopher's and the engineer's: the philosopher's dream to have a sound method to reason correctly, the engineer's dream to have a machine to calculate efficiently and without error.

Any attempt to assimilate the human brain to a mechanical or computer machine necessarily leads to the negation of the autonomy of thought. The latter is not the result of chance or indeterminacy, but rather of a possibility of choice according to the reasoning based on rules and principles. By its organization, the human brain allows the emergence of the cognitive autonomy.

Of course, if we accept the idea of a level of existence proper to the cognitive processes, the philosophical dream becomes, more modestly, that of understanding the multiplicity of cognitive processes used by humans. The development of the general theory of automata and the formalisation of the construction of complex machines by Von Neumann allowed the pursuit of the engineer's dream. A major turning point took place around the 1960s, with the design of machines on the one hand, and progress in AI and cognitive science on the other hand. Significant successes have been achieved, for example, in the field of natural language processing.

Our world today is witnessing the genesis of a major shift in the way advanced technologies operate. Among this emerging wave of unrestricted automation, we are beginning to see increasingly independent and autonomous systems. The degree of interactions between these systems and any form of human controller is gradually being reduced and pushed further away.

In general, these autonomous systems are inherently sophisticated and operate in complex and unpredictable environments. Unfortunately, they still face deployment limitation in safety-critical applications (e.g., transportation, healthcare, etc.), due to lack of trust, behavioural uncertainty and technology compatibility with safe and secure system development methods. In particular, for ***Urban Autonomous Driving*** and ***Intelligent Medical Devices*** that are considered to be the hardest problem in autonomy, existing development of autonomous vehicles naturally includes the AI part (e.g., machine-learning for perception), as well as the CPS part (e.g., for vehicle control or decision making via infrastructure support). However, there are significant challenges in ensuring the quality of the overall system. We have developed the FOCETA project primarily to address these challenges by developing the foundations for continuous engineering of trustworthy learning-enabled autonomous systems.

Prof. Saddek Bensalem
UGA/Verimag
France

Figure 1: Prof. Saddek Bensalem, FOCETA Project Coordinator.

NEWS & EVENTS FROM FOCETA

Scientific papers published in open access within FOCETA project are available on the website >> Read

Watch the FOCETA project **video** >> Watch

Download the FOCETA project **leaflet** >> Download

Download the FOCETA project **poster** >> Download

Download the FOCETA **roll-up banner** >> Download

PROJECT CONTACT INFORMATION

Website: http://www.foceta-project.eu/

Project Coordinator: Saddek Bensalem (UGA)

Technical Coordinator: Dejan Nickovic (AIT)

PMO & Dissemination Manager: Sofia Santi (L-Up)

This project has received funding from European Union's Horizon 2020 research and innovation programme under grant agreement N°956123.

NEWS FROM FOCETA

THE FOCETA PROJECT METHODOLOGY

The vision of FOCETA is to introduce a mixed approach for engineering trustworthy learning-enabled autonomous systems based on combining the advantages of data-based and model-based techniques. This "mixed" approach integrates Learning Enabled Components (LECs) and classical components on the level of models. Moreover, it generates a new paradigm for implementing safety-aware LECs by fusing learning from examples and synthesis from specification. Finally, this novel mixed approach transfers verification technology for model-driven design to verification of LECs, and conversely, utilizes Machine Learning (ML) to improve testing of models.

Based on these key concepts, the FOCETA methodology is structured as follows. As a first step, several projects and key EU roadmaps in the fields of AI and cyber-physical systems (CPSs) are studied, which feed the first work package entitled "Industrial requirements and incremental safety-and-security cases". Focusing on the two FOCETA use cases (UC1: Safe and Secure Intelligent Automated Valet Parking (AVP): http://www.foceta-project.eu/automated-valet-parking/. UC2: Anaesthetic drug Target Control Infusion: http://www.foceta-project.eu/anaesthetic-drug-target-control-infusion/), the industrial needs and technical requirements are defined and refined in an iterative fashion by the FOCETA industrial partners. By doing do, this work package provides technical inputs for the three key scientific work packages for further development, as well as appropriate benchmarks for justifying the scalability of the developed scientific work. The key scientific work packages are: Modelling & Simulation; Verification & Validation; Agents for "Performance and Security beyond safety" via Runtime Monitoring and Enforcement (see Figure 2). These key scientific work packages cover the three main research strands on which the FOCETA project relies to tackle the challenges in autonomous systems.

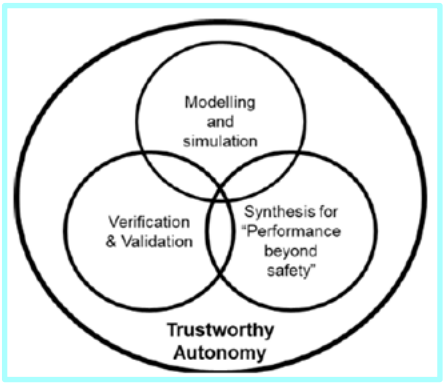

Figure 2: Technology strands in FOCETA which forms the key scientific work packages.

The first work package dedicated to industrial requirements also provide tool qualification requirements, as the developed tools will be integrated in the use case demonstrators in later project phases. This first work package also provides appropriate validation parameters for the use case demonstration, which is the core activity in the fifth and last scientific work package entitled "Methods and tools applied to industrial cases demonstrations".

As Modelling and Simulation are instrumental for integrating the data-driven and model-driven paradigms, the applied Verification and Synthesis techniques are tightly integrated in the modelling and simulation tools. Results from the three key scientific work packages, including the methodology and the research tools, will be used in the two use case demonstrators.

The technical knowledge about the FOCETA methodology and use cases is disseminated to the broader research community and the related industrial sectors to achieve the maximal impact. Figure 3 graphically depicts the workflow and the FOCETA project methodology.

In the next article, you will read about the main work performed and results achieved under the first work package "Industrial requirements and incremental safety-and-security cases".

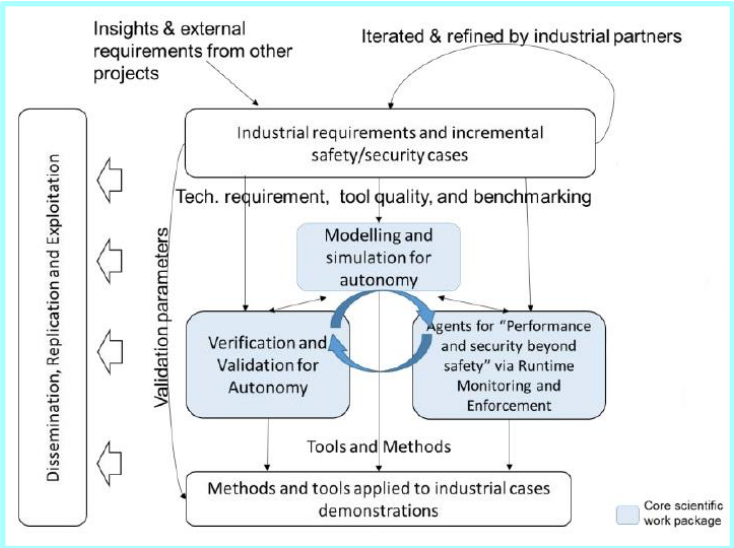

Figure 3: FOCETA project methodology.

Written by Sofia Santi (L-up) and Saddek Bensalem (UGA)

This project has received funding from European Union's Horizon 2020 research and innovation programme under grant agreement N°956123.

PROGRESS OF WORK SINCE OCTOBER 2020 WITHIN THE WORK PACKAGE "INDUSTRIAL REQUIREMENTS AND INCREMENTAL SAFETY-AND-SECURITY CASES", LED BY UGA

In this article we provide insights about the main work performed and results achieved since October 2020 within the work package "Industrial requirements and incremental safety-and-security cases", led by UGA.

As explained in the previous newsletter article regarding FOCETA methodology, the work package entitled "Industrial requirements and incremental safety-and-security cases" serves as the foundation of all the other research and technical activities performed within the FOCETA project.

Let's first recall the main goals of this work package. The aim of this work package is to generate requirements and their related validation strategies as inputs for the test and evaluation phase of the project, i.e., within the framework of the two FOCETA industrial demonstrators. Such requirements need to focus on trustworthiness and performance. Furthermore, the aim is to adopt a formalism that can describe systems with timing and cyber-physical components that are learning-enabled, or include components that involve neural networks (NN), trained using deep learning.

Within the first twelve months of the project, several activities have been achieved within this work package, thanks to the collaborative effort of partners UGA, Bar-Ilan University, Fortiss, Intel, Denso, Siemens and RGB. Specifically in this work package, but also more generally throughout the whole FOCETA project, a smooth coordination and cooperation between academic and industrial partners is key to achieve the expected results.

Under the task entitled "**Industrial Requirements and Incremental safety-and-security cases**", led by UGA, partners developed a requirements engineering methodology (Figure 4) for the FOCETA project and a tool that supports the requirements management.

Furthermore, partners defined the requirements with regard to the two FOCETA use cases, i.e., the automated valet parking system (AVP) with mixed traffic and the anaesthetic drug target control infusion.

In addition to the use-case-specific requirements that will serve as the main driving force for the technical developments in the project, partners also collected requirements for the methodologies, methods and tools that will be developed in the three core scientific work packages. Finally, partners defined the roadmap for using the collected requirements to develop measurable evaluation criteria for assessing the use cases and the engineering toolchain.

The activities in task "**Test Case and TRL Validation Scenario Definition**", led by UGA, focused on the validation of scenarios and parameters of the two FOCETA use cases. The work performed followed a scenario-driven approach, starting from the formulation of the vision towards which the project will develop. First of all, partners provided a detailed description of the two FOCETA use cases. For each use case, the academic partners defined detailed evaluation criteria. A validation target to be achieved by the end of the project was associated to each of the proposed technologies. Furthermore, partners identified the three groups of parameters to be considered to show how the technical development for the verification and validation (V&V) of autonomy will be demonstrated and evaluated in the other technical work packages. The first group of parameters is related to properties that we expect the autonomous systems to satisfy. The second group of parameters is a set of V&V techniques that deal with the properties in different ways. Finally, partners described how to evaluate the proposed techniques for monitoring and shielding on the FOCETA use cases.

In the task "**Formal Specification**", led by Bar-Ilan University, partners provided a new specification formalism based on abstracting away the internal structure of the neural network, including the internal values of the different neurons. This formalism will match the specification requirements for learning enabled autonomous systems. Partners tested the adequacy of this formalism against different requirements for the FOCETA use cases.

Written by Sofia Santi (L-up) and Saddek Bensalem (UGA)

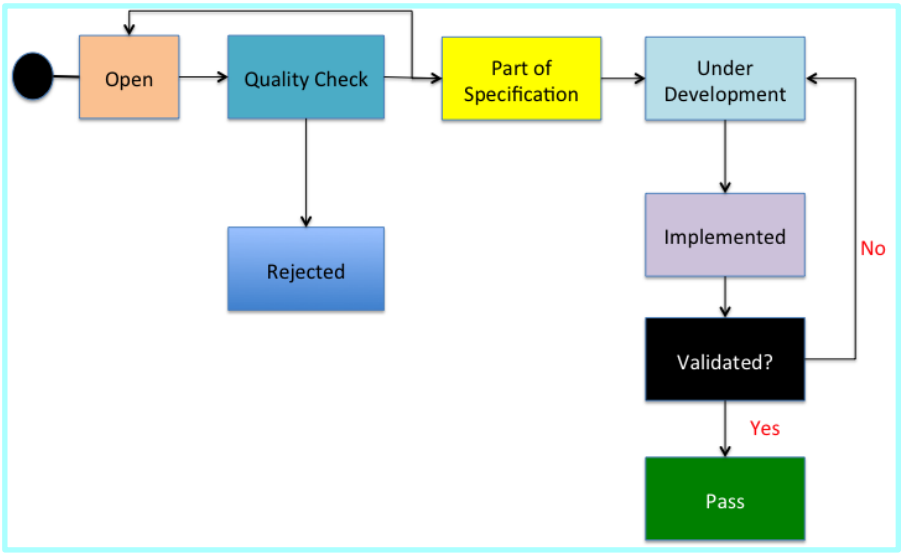

Figure 4: State diagram of the FOCETA requirement engineering process.

This project has received funding from European Union's Horizon 2020 research and innovation programme under grant agreement N°956123.

THE FIOOR TO THE PLAYERS: INTERVIEW WITH FOCETA PARTNERS

INTERVIEW WITH DR. XIAOWEI HUANG, ASSOCIATE PROFESSOR OF COMPUTER SCIENCE, UNIVERSITY OF LIVERPOOL

Dr. Xiaowei Huang is a Reader (Associate professor) of Computer Science at the University of Liverpool. Prior to Liverpool, he worked at University of Oxford, University of New South Wales, and Chinese Academy of Sciences. The research his group is currently conducting spans over machine learning, formal methods, and robotics. He has published over 40 papers, most of which appear in top conferences and journals. He has given invited talks and served as a panellist at several leading conferences, discussing topics related to the safety and security of applying machine learning algorithms to critical applications. Within FOCETA, Xiaowei is the leader of the work package "Verification and Validation for Autonomy". University of Liverpool is also involved in all other FOCETA project work packages.

Question 1 (Q1): Within the FOCETA project, the University of Liverpool is the leader of the work package entitled "Verification and Validation for Autonomy". What are the objectives of this work package?

Answer 1 (A1): This work package is to develop a comprehensive theoretical framework, together with software tools, for the verification and validation of learning-enabled systems, i.e., systems that consist of both model-based components and data-driven learning components. It addresses a set of cybersecurity risks such as robustness, fairness and unbiased decision making, transparency, poisoning attack, distributional shift, privacy (e.g., membership inference attack) etc. The goal is not only to enhance existing verification and validation techniques with promising machine learning techniques, but also to develop techniques to verify and validate these learning-enabled systems.

Q2: Could you explain in what extent the work package "Verification and Validation for Autonomy" plays a key role in view of the FOCETA project outcomes? What are the key assets of the University of Liverpool to lead these activities?

A2: FOCETA is to establish the principles for the future autonomous systems with learning-enabled components to guarantee safety while maximizing performance. As one of the scientific work packages, the "Verification and Validation for Autonomy" package is focused on two critical problems in autonomous systems, i.e., safety of machine learning components, and intelligent testing of the autonomous systems.

The University of Liverpool has a historical strength on artificial intelligence (AI) research, in particular the verification and reasoning of (symbolic) AI. In the past few years, we investigated the verification and validation of autonomous systems, taking into consideration the new development of machine learning which has been applied in e.g., self-driving cars, as the de facto techniques for the perception tasks and the promising techniques for the control tasks. In particular, we are leading the directions of the safety verification and the software testing of deep neural networks. In addition to methodological contributions, we also developed a number of relevant software tools, which are publicly available at GitHub (https://github.com/TrustAI).

Q3: Within the work package "Verification and Validation for Autonomy", the University of Liverpool is also the leader of the task "Systematic testing of learning components", which has just come to an end. What were the challenges of this task and how did you tackle them? Was the work achieved in line with the expectations?

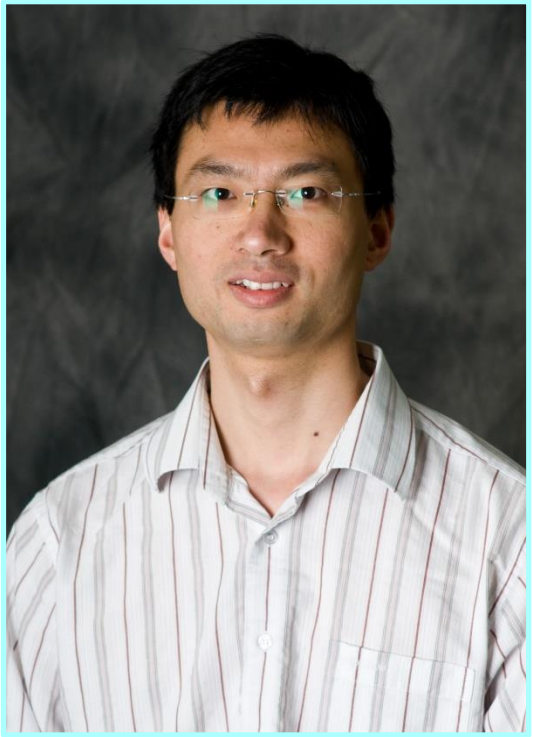

Figure 5: Dr. Xiaowei Huang.

A3: Testing frameworks can work efficiently in identifying the errors of a complex system with a set of test cases. While several testing frameworks have been proposed for neural networks, they cannot work well with real-world autonomous systems, due to (1) the lack of consideration to the coverage of real-world operational scenarios the autonomous system will be running, and (2) the lack of consideration to the potential, diverse errors.

These challenges were dealt with in the first year of FOCETA in the task "Systematic testing of learning components". For the first challenge, testing techniques for both test phase and operational phase were developed to consider how best to cover the real-world operational scenarios. For the test phase, this includes a testing framework for spatial-temporal input, a few sampling-based test case generation methods by considering a specifications formalism that can describe abstract scenarios, and a fault injection technique to consider the potential hardware environment. For the operational phase, this includes the application of an adaptable equivalence relation over real-world scenarios to the operational testing, and a reliability assessment model to quantitatively evaluate the risk of failures with operational

This project has received funding from European Union's Horizon 2020 research and innovation programme under grant agreement N°956123.

data. For the second challenge, we considered the evaluation of the effectiveness of adversarial training with respect to several perspectives of robustness, including distributional robustness, optimization robustness and geometric robustness.

Q4: What are the main next steps towards the achievement of the work package entitled "Verification and Validation for Autonomy"?

A4: There are two main next steps for this work package. One next step will be on utilising machine learning techniques to support the verification and validation of autonomous systems. Comprehensive validation of systems is often prohibitively time consuming, dictating the use of testing techniques. We are developing methods for automatically tuning the process of random testing as well as clustering the simulation data towards finding rare errors. The other next step will be on formal verification of learning components. While techniques for the verification of neural networks have recently been studied intensively, they still suffer from the scalability problem and can only work with small networks. We will develop methods to break the scalability barrier.

Q5: What is innovative about the activities that the University of Liverpool carries out within the FOCETA framework?

A5: The University of Liverpool's target is set to develop practically validated and theoretically grounded methods and tools to support the evaluation and improvement of learning-enabled autonomous systems with respect to the safety and performance properties, by considering the context set up by the use cases in the FOCETA project. Scientific results will be our main innovative contributions to FOCETA.

Q6: The FOCETA consortium gathers many different European and international partners, including leading research centers and academics, as well as prominent industrial partners. How do you evaluate the cooperation between all these oganisations?

A6: The collaboration is close and very healthy, with partners focusing on different aspects that are required by the two FOCETA use cases: autonomous driving and healthcare. Industrial partners are setting up simulation and physical environments, on which the techniques developed by the academic partners can be validated. On the other hand, the techniques developed by academic partners are based on the specification and requirement of the use cases provided by the industrial parnters.

FOCETA falls within my current research area on the verification and validation of deep learning. It contributes from a broader perspective – autonomous systems, where deep learning is currently a promising implementation technique to their components. […] I expect the outcome of FOCETA may shed some light on the future directions of my research area.

Q7: What is the impact of FOCETA project on your field of research?

A7: FOCETA falls within my current research area on the verification and validation of deep learning. It contributes from a broader perspective – autonomous systems, where deep learning is currently a promising implementation technique to their components. As FOCETA is rooted on practical use cases with significant inputs from our prominent industrial partners, I expect the outcome of FOCETA may shed some light on the future directions of my research area. In particular, most of the verification and validation tasks are computational expensive, but rather needed in practice, it is therefore needed to consider how to establish a trade-off. Any progress in this regard made by FOCETA can be a significant contribution.

Q8: Xiaowei, during your professional career, apart from several experiences in the UK, you worked as a researcher at the University of New South Wales at Sydney, Australia and Chinese Academy of Sciences. Would you say that these international experiences made you acquire specific intercultural skills? In what extent do they benefit the FOCETA project?

A8: My past experience of working in different countries has equipped me with awareness and skills in dealing with intercultural differences. FOCETA is a large consortium with both academic and industrial partners, from multiple countries. It is very likely that we might be speaking with different terminologies even for a same problem, and we might be dealing with an issue in different manners. Patience and skills in dealing with these will be needed to make sure the interaction is healthy and the project runs smoothly. I hope these skills can help buid trust between the University of Liverpool team and the other partners, and eventually help FOCETA achieve the best outcome.

DISCLAIMER - The information, statements and opinions in the above interview are personal views of the individuals involved in the FOCETA project and do not necessarily reflect the views of the FOCETA consortium as a whole, nor of the European Commission. None of them shall be liable for any use that may be made of the information contained herein.

This project has received funding from European Union's Horizon 2020 research and innovation programme under grant agreement N°956123.

GET TOGETHER

In this chapter you will find a selection of major conferences and other events which are of interest for the FOCETA community. We look forward to meeting you!

MEMOCODE '21 - 19TH ACM-IEEE INTERNATIONAL CONFERENCE ON FORMAL METHODS AND MODELS FOR SYSTEM DESIGN, 20-22TH NOVEMBER 2021, ONLINE

The focus of the MEMOCODE conference is on formal methods and models for developing computer systems and their components. MEMOCODE's objective is to emphasize the importance of models and methodologies in correct system design and development, and to bring together researchers and industry practitioners interested in all aspects of computer system development, to exchange ideas, research results and lessons learned. ***FOCETA partners UGA and AIT will give a presentation*** *based on their joint paper entitled "Sampling of Shape Expressions with ShapEx".*

Source: https://lcs.ios.ac.cn/memocode21/

FM '21 - 24TH INTERNATIONAL SYMPOSIUM ON FORMAL METHODS, 20-26TH NOVEMBER 2021, ONLINE

FM 2021 is the 24th international symposium in a series organized by Formal Methods Europe (FME). The topics covered include the development and application of formal methods in a wide range of domains including software, cyber-physical systems and integrated computer-based systems. ***FOCETA partner University of Liverpool will give a presentation*** *based on their paper entitled "Model-Free Reinforcement Learning for Lexicographic ω-Regular Objectives".*

Source: http://lcs.ios.ac.cn/fm2021/

SEFM '22 - 19TH INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING AND FORMAL METHODS, 6-10TH DECEMBER 2021, ONLINE

The conference aims to bring together researchers and practitioners from academia, industry and government, to advance the state of the art in formal methods, to facilitate their uptake in the software industry, and to encourage their integration within practical software engineering methods and tools. ***FOCETA partner AIT will give a presentation*** *based on their paper entitled "Mining Shape Expressions with ShapeIt".*

Source: https://sefm-conference.github.io/

AAAI-22 - 36TH AAAI CONFERENCE ON ARTIFICIAL INTELLIGENCE, 22ND FEBRUARY-1ST MARCH 2022, VANCOUVER, CANADA

The purpose of the AAAI conference is to promote research in artificial intelligence (AI) and scientific exchange among AI researchers, practitioners, scientists, and engineers in affiliated disciplines. AAAI-22 welcomes submissions on mainstream AI topics as well as novel crosscutting work in related areas. In case of acceptance of their paper, ***FOCETA partner AIT plans to give a presentation*** *at AAAI-22.*

Source: https://aaai.org/Conferences/AAAI-22/

ICSE 2022 - 44TH INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING, 21-29TH MAY 2022, PITTSBURGH, US

ICSE, the IEEE/ACM International Conference on Software Engineering, is the premier software engineering conference. Since 1975, ICSE provides a forum where researchers, practitioners, and educators gather together to present and discuss the most recent innovations, trends, experiences and issues in the field of software engineering. In case of acceptance of their papers, ***FOCETA partners University of Liverpool and AIT plan to give a presentation each*** *at ICSE 2022.*

Source: https://conf.researchr.org/home/icse-2022

ICRA22 - IEEE INTERNATIONAL CONFERENCE ON ROBOTICS AND AUTOMATION 2022, 23-27TH MAY 2022, PHILADELPHIA, US

As the flagship conference of the IEEE Robotics and Automation Society, ICRA brings together the world's top researchers and most important companies to share ideas and advances in the fields of robotics and automation. In case of acceptance of their paper, ***FOCETA partner University of Liverpool plans to give a presentation*** *at ICRA22.*

Source: https://www.icra2022.org/

This project has received funding from European Union's Horizon 2020 research and innovation programme under grant agreement N°956123.

ACC 2022 - AMERICAN CONTROL CONFERENCE 2022, 8-10TH JUNE 2022, ATLANTA, US

ACC is the annual conference of the American Automatic Control Council (AACC), the U.S. national member organization of the International Federation for Automatic Control (IFAC). The conference focuses on all areas of the theory and practice of automatic control. In case of acceptance of their papers, ***FOCETA partners Siemens and TUG plan to give a presentation each*** *at ACC 2022.*

Source: https://acc2022.a2c2.org/

CFS 2022 - 35TH IEEE COMPUTER SECURITY FOUNDATIONS SYMPOSIUM, 7-10TH AUGUST 2022, HAIFA, ISRAEL

The Computer Security Foundations Symposium (CSF) is an annual conference for researchers in computer security, to examine current theories of security, the formal models that provide a context for those theories, and techniques for verifying security. Topics of interest include access control, information flow, covert channels, cryptographic protocols, database security, language-based security, authorization and trust, verification techniques, integrity and availability models, and broad discussions concerning the role of formal methods in computer security and the nature of foundational research in this area. In case of acceptance of their paper, ***FOCETA partner AIT plans to give a presentation*** *at CSF 2022.*

Source: https://www.ieee-security.org/TC/CSF2022/

Follow the FOCETA project on LinkedIn

This project has received funding from European Union’s Horizon 2020 research and innovation programme under grant agreement N°956123.