CHARIOT 2ND PROJECT WORKSHOP:

(COORGANISED BY CHARIOT AND VESSEDIA PROJECTS)

"THE ROAD AHEAD FOR A COGNITIVE COMPUTING PLATFORM SUPPORTING A UNIFIED APPROACH TOWARDS PRIVACY, SECURITY AND SAFETY (PSS) OF IOT SYSTEMS"

DATE: 9 MAY 2019 - H. 09:00-17:00

VENUE: IBM TECHNOLOGY CAMPUS, BUILDING 9, HAMILTON AUDITORIUM

DAMASTOWN INDUSTRIAL PARK, MULHUDDART, DUBLIN 15, IRELAND. EIRCODE D15 HN66

As IOT is becoming more and more pervasive in everyday life, aspects connected with security, safety and privacy are elements that will become key in order to have a secure and wider diffusion of solutions based in this type of technology. Researchers, industries and final users are more and more interested in the integration of IOT solutions in innovative services but in order to be able to deliver them it is important that trust in users is built and compliance to data safety and privacy, is in place. In this area CHARIOT, the consortium is leading innovation actually driven by industrial needs.

This second workshop will be co-organized by CHARIOT and VESSEDIA EC projects and take place on the 9th May 2019, in Dublin Ireland, hosted by IBM. During the workshop the evolution of both projects will be presented, including the experience from the users and the first lessons learned on the different tasks. The actions of cooperation with the other IOT project under the H2020 program as well as the dissemination and standardization activities will be analyzed. A specific focus will be in the Living Lab driven from IBM Ireland

The **"Cognitive Heterogeneous Architecture for Industrial IoT" (CHARIOT)** three-year project, started its activities on the 1st of January 2018 with the objective to provide the overall design method and cognitive computing platform towards privacy, security and safety (PSS) over IoT Systems including elements of innovations like:

- A Privacy and security protection method building on state of the art Public Key Infrastructure (PKI) technologies to enable the coupling of a pre-programmed private key deployed to IoT devices with a corresponding private key on Blockchain system.
- A Blockchain ledger in which categories of IoT physical, operational and functional changes are both recorded and affirmed/approved by a combination of a cognitive engine and private key hashing between the cognitive engine and IoT devices to authorize change and, likewise, invalidating any and all other changes be they malicious or otherwise.
- A fog-based decentralized infrastructure for Firmware Security integrity checking that leverages a Blockchain ledger to enhance physical, operational and functional security of IoT systems, including actuation and deactivation.
- An accompanying IoT Safety Supervision Engine providing a novel solution to the challenges of securing IoT data, devices and functionality in new and existing industry-specific safety critical systems.

The projects CHARIOT & VESSEDIA have received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780075 & No 731453.

- A Cognitive System and Method with accompanying supervision, analytics and prediction models enabling high security and integrity of Industrials IoT.
- New methods and tools for static code analysis of IoT devices, resulting in more efficient secure and safer IoT software development and V&V.

The **"Verification Engineering of Safety and SEcurity critical Dynamic Industrial Applications" (VESSEDIA)** three-year project, started on the 1st of January 2017 with the objective to design and implement Safety and Security analysis technologies for IoT software, capable of improving dramatically the trustworthiness of such connected applications. For this aim, VESSEDIA enhances and scales up modern software analysis tools, in particular the open-source Frama-C analysis platform, to make them useful and accessible to a wider audience of developers of connected applications. VESSEDIA will tackle this challenge by

- Developing a methodology that makes it possible to adopt and use source code analysis tools as efficiently and with similar benefits as it is already possible in the case of highly-critical applications,
- Enhancing the Frama-C toolbox to enable efficient and fast implementation,
- Demonstrating the capabilities of the new toolbox on typical IoT applications, including an IoT Operating System (Contiki),
- Developing an ISO standard for classifying V&V tools and generalising the use of the toolbox,
- Contributing to the Common Criteria certification process, and
- Defining a "Verified in Europe" label for validating software products with European technologies.

The projects CHARIOT & VESSEDIA have received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780075 & No 731453.

2ND WORKSHOP PROGRAMME

Welcome reception		
09:00	09:15	**Registration and Coffee**
09:15	09:20	**Welcome and aim of workshop – Bora Caglayan** (IBM, IE), Konstantinos Loupos, CHARIOT Coordinator (INLECOM, GR), Armand Puccetti, VESSEDIA Technical Lead (CEA, FR)
Introduction and Opening Scene **Moderator:** *Konstantinos Loupos (INLECOM)*		
09:20	09:40	**Keynote: IoT, Security and Certification** (Franck Sadmi, Bureau Veritas, FR)
09:40	10:00	**The CHARIOT Project – overview** - Konstantinos Loupos, CHARIOT Coordinator (INLECOM, GR)
10:00	10:20	**The VESSEDIA Project – overview –** Armand Puccetti, VESSEDIA Technical Lead (CEA, FR)
10:20	10:40	**Coffee Break**
Session1: *IoT In Industrial Environments – challenges and opportunities* **Moderator:** *Bora Caglayan, IBM Ireland*		
10:40	11:00	**IoT Security Needs in Industrial Building Environments** (Bora Caglayan, IBM, IE)
11:00	11:20	**The Contiki Operating System** (Allan Blanchard, INRIA, FR)
11:20	11:40	**The 6LowPAN Network Management Platform** (Mounir Kelil, CEA, FR)
11:40	12:00	**Security needs of the Transport Sector:** TRENITALIA and Athens International Airport – (Vasos Hadjioannou, EBOS, CY)
12:00	13:10	**Lunch and Networking Break**
Session2: *Solutions for Industrial IoT with training examples* **Moderator:** *Armand Puccetti (CEA, FR)*		
13:10	13:30	**Industrial IoT and Platforms** (Bill Karakostas, VLTN, BE)
13:30	13:50	**Firmware security integrity checking** (Andrea Battaglia, ASPISEC, IT)
13:50	14:10	**Blockchain and Distributed Ledger Technologies** (Alexandros Papageorgiou, INLECOM Systems, UK)
14:10	14:30	**Static code analysis and Frama-C** (Franck Vedrine and Virgile Prevosto, CEA, FR)
14:30	14:50	**IBM IoT Cloud Ecosystem** (Bora Caglayan, IBM, IE)
14:50	15:10	**IoT Modelling Framework and Papyrus** (Shuai Li, CEA, FR)
15:10	15:30	**Monitoring and E-ACSL** (Julien Signoles, CEA, FR)
15:30	15:50	**Coffee Break**
Session3: *Standardization and Related Mechanisms with training examples* **Moderator:** *Mounir Kelil (CEA, FR)*		
15:50	16:10	**Overview of IoT cybersecurity standards and technologies** (Serena Sensini, ISC, IT)
16:10	16:30	**ISO Standard 23643 development on verification and validation tools** (Emmanuel Querrec, TUAS, FI)
Technical Panel Discussion: IoT Security – Systemic or Analytic approach		
16:30	17:00	*Discussion on the two project approaches, top-down (CHARIOT) and bottom-up (VESSEDIA), in tackling IoT security and safety challenges.* **Participants:** **Konstantinos Loupos** (CHARIOT Coordinator) **Armand Puccetti** (VESSEDIA Technical Lead) **Bora Caglayan** (IBM use case) **Allan Blanchard** (INRIA use-case)
17:00	17:10	**Wrap-up and Workshop Closing**

The projects CHARIOT & VESSEDIA have received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780075 & No 731453.