CHARIOT IMPACT

Evolution of platforms and contribution to scientific progress enabling novel, advanced semi-autonomous IoT applications through:

- Blockchain Privacy protection;
- Neural Networks, Firmware Security check;
- Safety Supervision Engine and Models.

Increased IoT usability and user acceptance, through strengthened security and user control:

- Enhanced trust and acceptance of IoT;
- Secure and safe IoT software development;
- Systemic modelling, Resilience enhancement for risk control in IoT systems;
- Predictive analytics for threats assessment;
- Models for Knowledge Management/Sharing;
- Advanced-intelligence dashboard.

Contribution to emerging or future standards and pre-normative activities:

- Standardised recommendations for securing IoT;
- Enhanced vision of safety control of the future;
- New safety certification guidelines

Promote the adoption of EU platforms in European and international context:

- Promotion of CHARIOT IoT cognitive computing platform as a premier for safety critical IoT;
- Population of CHARIOT's IoT topologies and domain models for Transport, Logistics and Smart Buildings sectors.

Support emergence of an open market of services and innovative businesses:

- Possibility for new/enhanced role of IoT in safety critical installations;
- Open environment for development of new cognitive IoT applications supporting PSS services and new collaborative business models.

PARTNERS

INLECOM SYSTEMS LTD

IBM

COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES

ATHENS INTERNATIONAL AIRPORT S.A.

EBOS TECHNOLOGIES LTD

VLTN GCV

TRENITALIA SPA

CLMS

ASPISEC SRL

TELCOSERV S.A.

INFORMATION SHARING COMPANY

PROJECT CONTACTS:

Project Coordinator:
Konstantinos Loupos
(konstantinos.loupos@inlecomsystems.com)

Dissemination Manager:
Antonio Martino
(a.martino@gruppoisc.com)

ONLINE LINKS:

Website:
http://chariotproject.eu/

LinkedIn

Twitter:
@CHARIOT_Project

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 780075.

COGNITIVE HETEROGENEOUS ARCHITECTURE

FOR INDUSTRIAL IOT

CHARIOT

Project Facts:

Project start: 1/1/18
Duration: 36 months
Budget: 4,928,562 euros
No. of partners: 11
Instrument: EC IoT, RIA

INDUSTRIAL CHALLENGES

Recently, Cloud Computing and Internet of Things (IoT) have been rapidly advancing as the two fundamental technologies of the "Future Internet" concept. Different IoT systems are designed and implemented according to the IoT domain requirements, typically not taking into consideration issues of openness, scalability, interoperability, and use case independence. This leads to a variety of new potential risks concerning information security and privacy, data protection and especially safety, all of which need to be considered in unison.

Clearly, the risk assessment model is influenced by the circumstances in which each IoT application and system is configured, deployed and used. Large scale connectivity of intelligent objects coupled with complex constraints inevitably leads to many security challenges, which are not included into the classical formulation of security problems and solutions.

Consequently, securing data, objects, networks, infrastructure, systems and people in IoT will have a prominent role in the research and standardization activities over the next several years.

THE CHARIOT CONCEPT

CHARIOT's main concept relies to the design develop and validate a holistic approach that addresses Privacy, Security and Safety of IoT operation in industrial settings that compromise safety critical elements by placing devices and hardware at the center of trust.

Objectives & Technological Approach

CHARIOT advances the state of the art by providing a **design method and cognitive computing platform towards Privacy, Security and Safety of IoT Systems,** placing devices and hardware at the root of trust, in turn contributing to high security and integrity of industrial IoT through the following:

- A **Privacy and Security Protection method** based on Public Key Infrastructure technologies and Blockchain affirming/approving transactions;
- A **Blockchain ledger categorising IoT physical, operational and functional changes;**
- A **fog-based decentralised infrastructure for Firmware and Operational Security integrity checking** leveraging a Blockchain ledger to enhance physical, operational and functional security of IoT systems;
- An **accompanying IoT Safety Supervision Engine providing a novel solution to the challenges of securing IoT data, devices and functionality** for new and existing industry-specific safety critical systems;
- A **Cognitive System and Method with accompanying supervision, analytics and prediction models** encapsulating these with the end goal of high fidelity security and integrity of Industrial 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.

Living Labs & System Validation

CHARIOT will apply the developed technologies into three actual industrial cases (Living Labs) to drive developments, involving significant industry representative tests, verifications and validations using generic representative Critical Infrastructures Designs while aid integrated system scalability testing and validation for all types of assets.

LL1: Active Predictive Maintenance of Railway Safety Critical Systems and Energy Efficiency Systems Monitoring (TRENITALIA):

Scope: To enhance the operation of railways' service including risk reduction for passengers and personnel, regulations compliance and create a safe and efficient operating environment in railways as well as facilitate timely recognition of sensors malfunction and maintenance prediction.

LL2: Smart Buildings – Cognitive Campus (IBM Ireland):

Scope: To enable the continued IoT evolution of automated/smart buildings into to a truly cognitive IoT environment providing safer and more efficiently managed working environments and drive advancements in Cognitive IoT globally.

LL3: Facilities Protection (Athens International Airport):

Scope: To address safety of airport Infrastructures and enhance protection of airports' facilities from physical and cyber threats by enhancing airports' capability on early detection/prediction of hazardous situations, in parallel with reduction in false positive alarms that could disrupt operations.