16-20|9
Heraklion
Crete|Greece

ENISA-FORTH
SUMMER SCHOOL 2019
on Network &
Information Security

nis-summer-school.enisa.europa.eu

enisa

FORTH

ENISA-FORTH
SUMMER
SCHOOL
on Network &
Information Security
2019

It is our pleasure to welcome you to the 6th Network and Information Security **(NIS'19)** Summer School, taking place in Crete, Greece, 16 September - 20 September 2019. This event, having a different "special theme" every year, is jointly organised by the European Union Agency for Cybersecurity **(ENISA)** and the Foundation for Research and Technology - Hellas **(FORTH).**

The theme for this year is **"Security Challenges of Emerging Technologies"**.

The Security Challenges of Emerging Technologies refer to the security challenges and opportunities posed by new technologies. Examples hereto are Artificial Intelligence, Modern Network Infrastructures (i.e. 5G), IoT applications, Machine Learning, etc.

ENISA and FORTH bring together to this Summer School a distinguished faculty from around the world with the purpose to identify current trends, threats and opportunities against the background of recent advances on NIS measures and policies.

Recognizing the multi-dimensional facets and intricacies causing changes in the information risks landscape, an array of lectures will cover a variety of key aspects on policy, economic, legal and research matters. By going through a natural evolution cycle, but also by adopting current trends in networking and exchange of knowledge, this year's Summer School aims at increasing interaction among participants via targeted breakout sessions which will enhance dialogue and exchange of ideas.

The audience includes policy makers from EU Member States and EU Institutions, decision makers from industry and members of the academic community.

We would like to thank our keynote speakers, facilitators, faculty and sponsors for their significant contribution to the success of this event.

You can find in this leaflet information with regards projects that are sponsoring NIS'19. More details are available in NIS'19 site.

The program of the Event is available on-line

CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

- 56 partners (46 + 10 from June 2019)
- 19 countries (16 EU member states 3 associated countries)

- 27 partners from academia 28 partners from industry and organisations
- 16.000.000 € EC funding 7.000.000 € additional funding (national authorities and industry)

CONCORDIA's Social Media

Website: https://www.concordia-h2020.eu
Email: contact@concordia-h2020.eu
Twitter: @concordiah2020
LinkedIn: https://www.linkedin.com/in/concordia-h2020
Facebook: https://www.facebook.com/concordia.eu

CONCORDIA's Objectives

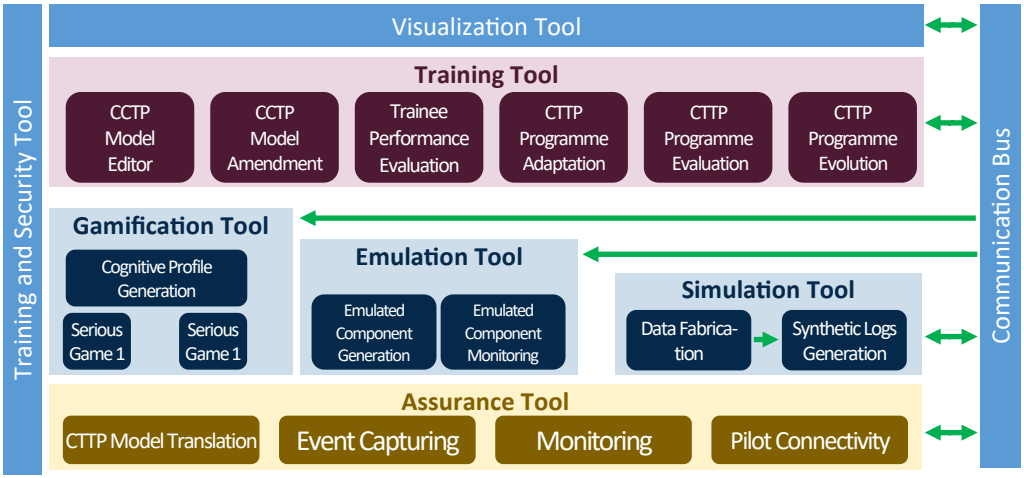
1. Position the CONCORDIA ecosystem.
2. Using an open, agile and adaptive governance model and processes.
3. Devise a cybersecurity roadmap to identify powerful research paradigms,
4. Develop next-generation cybersecurity solutions.
5. Scale up existing research and innovation with CONCORDIA's virtual lab and services.
6. Identify marketable solutions and grow pioneering techniques
7. Develop sector-specific (vertical) and cross-sector (horizontal) industrial pilots with building incubators.
8. Launch Open Calls to allow entrepreneurs and individuals to stress their solutions with the development.
9. Set up an Advisory Board, comprised by leaders of industry, standardization, policy and politics
10. Mediate between multiple communities:
11. Establish an European Education Ecosystem for Cybersecurity.
12. Provide expertise to European policy makers and industry.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 830927.

Cyber Security Threats and Threat Actors Training - Assurance Driven Multi-Layer, end-to-end Simulation and Training

https://www.threat-arrest.eu/

THREAT-ARREST aims to develop an **advanced training platform** incorporating **emulation**, **simulation**, **serious gaming** and **visualization** capabilities to adequately prepare stakeholders with different types of responsibility and levels of expertise in defending high-risk cyber systems and organizations to **counter advanced, known** and **new cyber-attacks**.



OBJECTIVES

- Develop the means for specifying cyber security threat training and preparation models and programs
- Develop emulation capabilities enabling hands-on experience against these cyber-attacks
- Develop multi-layer simulation capabilities enabling the realistic simulation of cyber systems
- Develop cyber-security training based on serious games
- Develop key capabilities for the effective delivery of CTTP programs,
- Align training and simulation with the continuous security assurance of real operational cyber systems
- Demonstrate the use of the THREAT-ARREST framework for effective training
- Ensure the uptake, commercialization, and the delivery of innovation of project outcomes by developing an ecosystem around the THREAT-ARREST framework.

Start Date: 2018-09-01
Duration: 36 months
Project Cost: €6,431,125
Project Coordinator: FORTH

Supported by the EU Horizon 2020 Programme under grant number 786890

RESilient transport InfraSTructure to extreme events

RESIST

PILOTS - Validation of RESIST Solutions

RESIST project

RESIST is a European project (September 2018 – August 2021) aiming to increase the resilience of seamless transport operation to natural and man-made extreme events, protect the users of the European transport infrastructure and provide optimal information to the operators and users of the transport infrastructure.

RESIST objectives

Despite the relatively good safety record of the transport sector, sudden failures of infrastructure assets are not uncommon. Extreme weather events, such as heavy rain and flooding, can result in bridge collapses and earthworks failures, which are safety critical issues. Furthermore, transport infrastructure operators are tasked with ongoing maintenance activities regarding infrastructure assets, whereby decisions regarding where to prioritise investments are often tricky due to the complex nature of transport networks and the vast quantity of infrastructure assets.

RESIST will use risk analyses and further develop recent exploitable research results in robotics, driving under panic, sensing and communications, to dramatically improve the speed and effectiveness, while reducing the cost, of structural vulnerability assessment, situation awareness, response operations and increased users' protection under extreme events towards a high level of resilience of the transport infrastructure.

PILOT 1

Egnatia Motorways Bridge T9 Peristeri area GREECE

PILOT 2

a) Millaures Viaduct at A32 Motorway ITALY

b) St. Petronilla Tunnel of the A32 Highway ITALY

EGNATIA ODOS SA · TECNOSITAF SpA · FEHRL · CATEC · National Research Council of Italy · FORTH · UNIVERSITAT POLITÈCNICA DE VALÈNCIA · TU Graz Graz University of Technology · RISA · ERRA · Sphynx Technology Solutions · NETIVEI ISRAEL · Roadaz

www.resistproject.eu

CERTCOOP

Trans-European and Greek CERTs collaboration project

https://www.certcoop.eu/

Objectives

To increase cyber security in Greece, the consortium will offer to public sector and critical infrastructures the following:

1. Penetration tests: during the action penetration tests will be performed in public institutions and the critical infrastructure of the country
2. The organization of workshops and seminars to increase awareness on cyber security, and inform about cyber-attacks as one of the major risks they may face
3. The access provision to a web portal which will provide information on current cybersecurity issues and an easy to use interface to report cyber-security incidents

Partners

Foundation for Research and Technology - Hellas	Greek Research and Technology Network	National Authority Against Electronic Attacks-National CERT	The Cyber Defense Directorate

Start date: 1st October 2017
Duration: 24 Months
EC Contribution: 748.733€

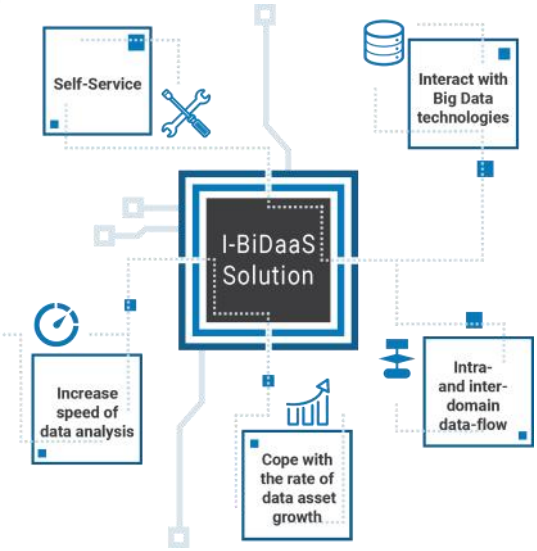
Coordinator: FORTH
Contact: Dr. Sotiris Ioannidis
sotiris@ics.forth.gr

Co-financed by the Connecting Europe Facility of the European Union

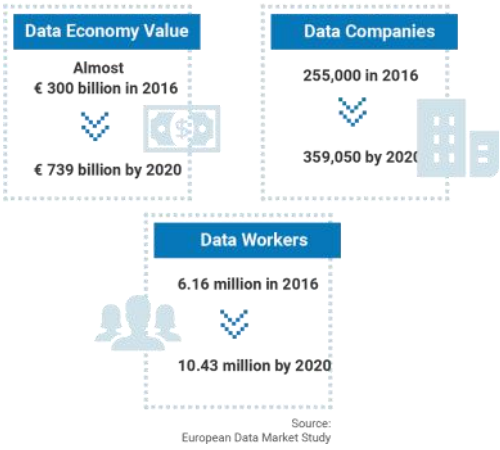
Industrial Driven Big Data
As a Self-Service Solution

I-BiDaaS aims to empower users to easily utilize and interact with big data technologies, by designing, building, and demonstrating, a unified solution that: significantly increases the speed of data analysis while coping with the rate of data asset growth, and facilitates cross-domain data-flow towards a thriving data-driven EU economy.

The Data Economy is considered an essential factor for growth competitiveness innovation, job creation, and societal progress in general.



The European Data Market



Benefits of using the I-BiDaaS Solution

Experimental protocol for validating the I-BiDaaS solution

www.ibidaas.eu

@Ibidaas

www.linkedin.com/in/i-bidaas

This project has received funding from the European Union's Horizon 2020 Research and Innovation program under grant agreement No 780787.

CYBERSECURITY FOR SMALL AND MEDIUM-SIZED ENTERPRISES

SMESEC

a lightweight cybersecurity framework for thorough protection

68% of SMEs have no systematic approach for ensuring cybersecurity

60% of all cyber attacks or breaches in 2016 were aimed at SMEs

60% of SMEs who were victims of cyber attacks did not recover and shut down within 6 months

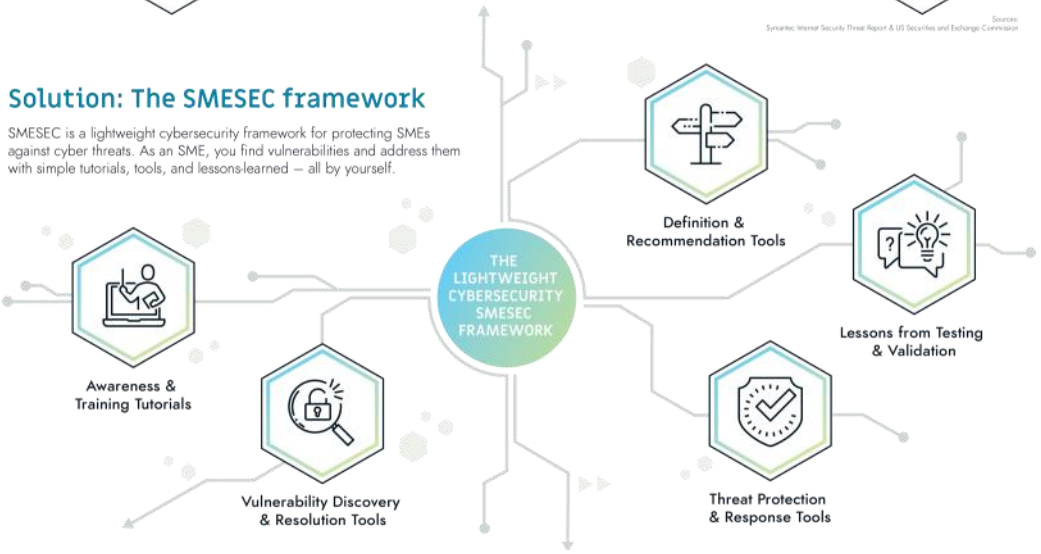
Cyber threats to SMEs

Small and medium-sized enterprises (SME) are the new big target for cyber attacks. SMEs see themselves confronted with a large variety of cyber threats.

Sources:
Symantec Internet Security Threat Report & US Securities and Exchange Commission

Solution: The SMESEC framework

SMESEC is a lightweight cybersecurity framework for protecting SMEs against cyber threats. As an SME, you find vulnerabilities and address them with simple tutorials, tools, and lessons-learned – all by yourself.



Benefits of using the SMESEC framework for your enterprise

Do it yourself
Step-by-step guidance for meeting customer requirements and standards

Keep the investment small
Cost-effective tutorials and tools suitable for a busy environment

Keep it simple
Practices adapted to your company instead of complicated formal policies and procedures

SMESEC Consortium Members

Contact project leader: Jose Francisco Ruiz, Atos Spain SA, jose.ruizr.external@atos.net

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740787 (SMESEC). This work is supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 17.00067. The opinions expressed and arguments employed herein do not necessarily reflect the official views of these funding bodies.

smesec.eu

CyberSure

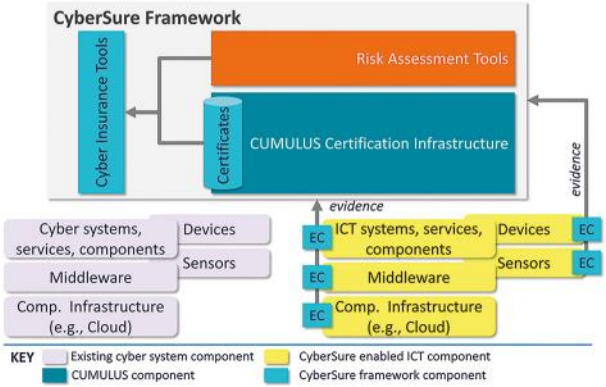
CYBER Security InSURancE
A Framework for Liability Based Trust

CyberSure aims to develop a framework for creating and managing cyber insurance policy in order to enhance the trustworthiness of cyber systems and provide a sound basis for liability in cases of security and privacy breaches in them. The framework will be supported by a platform of tools enabling an integrated risk cyber system security risk analysis, certification and cyber insurance. **CyberSure** will develop its cyber insurance platform at TRL-7.

cybersure.eu

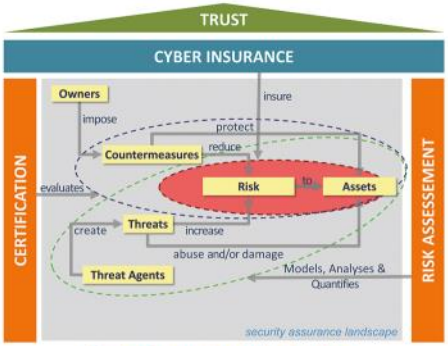
CyberSure Framework: CyberSure platform incorporates three basic components:

- a certification infrastructure
- a risk management tool
- insurance management tools



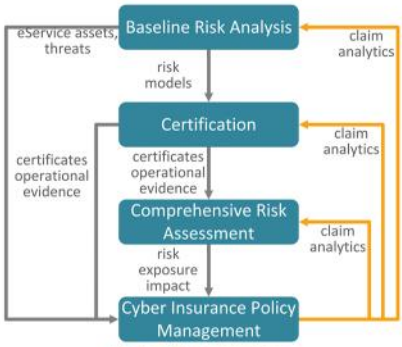
Objectives

- ✓ Establish a framework for automating the creation and management of cyber insurance policies
- ✓ Develop a TRL-7 platform supporting creation, monitoring and adaptation of cyber insurance policies
- ✓ Demonstrate the use of the CyberSure framework in real world trials
- ✓ Create conditions for improving cyber insurance practice and the trustworthiness of cyber systems and commercialising the use of the CyberSure platform and framework



CyberSure conceptual pillars

Insurance policies insure cyber system assets against specific risks.



CyberSure process

Integration of cyber insurance, certification and risk assessment will be realised through four steps

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No

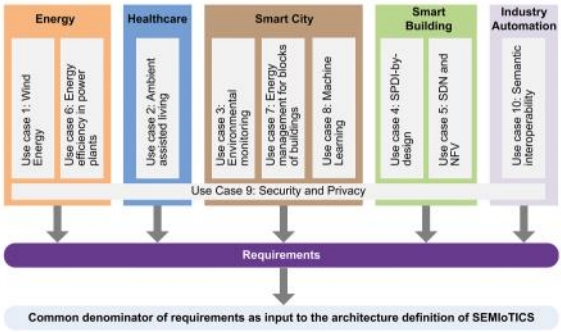
Duration: 01/01/17 to 31/12/20
Budget: 1,647,000€
Topic: MSCA-RISE-2016 - Research and Innovation Staff Exchange
Coordinator: Foundation for Research and Technology - Hellas (FORTH)

SEMIoTICS

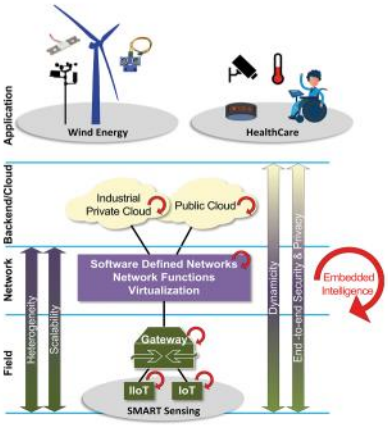
Smart End-to-end Massive IoT Interoperability, Connectivity and Security

Develop a pattern-driven framework, built upon existing IoT platforms, to enable and guarantee secure and dependable actuation and semi-autonomic behaviour in IoT/IIoT applications.

https://www.semiotics-project.eu/



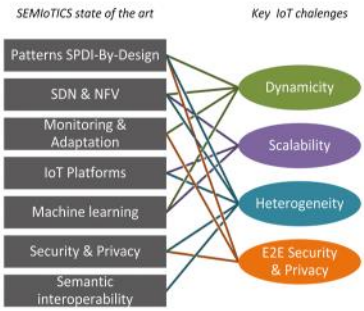
Domains affecting SEMIoTICS architecture definition



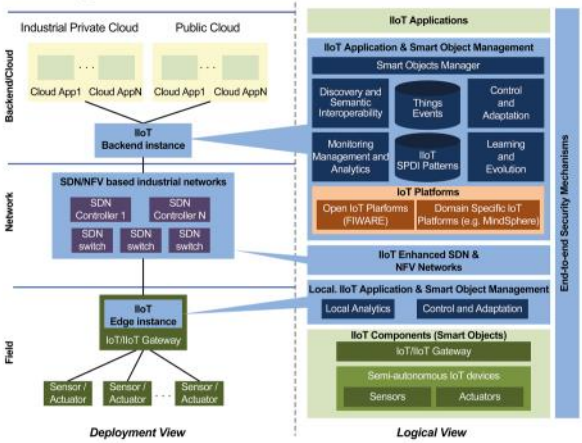
Key IoT challenges driving SEMIoTICS

SEMIoTICS demonstrates following 3 use cases:

- **Wind Energy:** Local smart behaviour at IIoT devices in wind turbines.
- **Healthcare:** Socially assistive robotic solution for ambient assisted living.
- **Smart Sensing:** Intelligent heterogeneous embedded sensing.



SEMIoTICS beyond the state of the art targeting



Envisioned architecture and deployment of SEMIoTICS framework

This project has received funding from the European Union's Horizon 2020 research and innovation programme

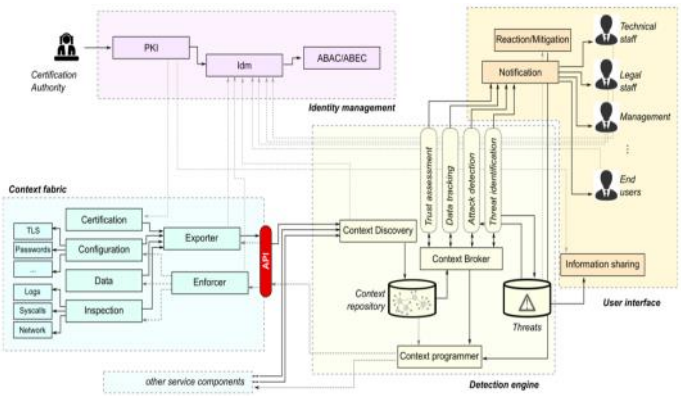
G.A. Number: 780315 **StarTting date:** 01/01/2018
Budget: €4,995,915 **Duration:** 36 months

GUARD

A CYBERSECURITY FRAMEWORK TO GUARANTEE RELIABILITY AND TRUST FOR DIGITAL SERVICE CHAINS

guard-project.eu

CONCEPTUAL FRAMEWORK



The GUARD framework will be made of four main macro-blocks:

- context fabric, concerning the definition of embedded security functions;
- detection engine, including the context repository and processing algorithms;
- identity management, to manage certifications, authentication, authorization, and access control in a multi-domain environment;
- user interface, interfacing the GUARD technologies with users and other domains.

IMPACT

- enhanced protection against novel advanced threats
- Advanced technologies and services to manage complex cyber-attacks and to reduce the impact of breaches
- Contribute to the development of the CSIRT Network across the EU
- Addressing mayor trends in the evolution of technologies utilised in future ICT infrastructures

OBJECTIVES

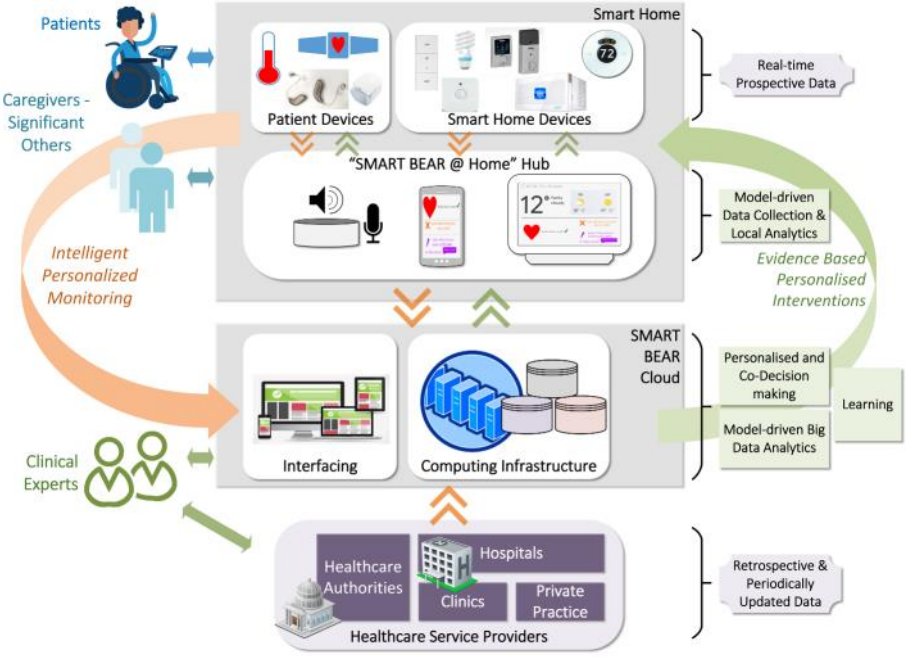
- Design a holistic framework for advanced end-to-end assurance and protection of business service chains
- Improve the detection of attacks and identification of new threats, by applying real time and/or offline machine learning
- leverage “programmability” to shape the granularity of context information to the actual needs.
- developing user tools for visualisation, notification, configuration, investigation, mitigation.
- Develop new business models for commercial exploitation
- Identify business opportunities and initiate tangible actions for successful commercial exploitation

This project has received funding from the European Union ‘s Horizon 2020 research and innovation program under grant agreement No 833456 .

Smart Big Data Platform to Offer Evidence-based Personalised Support for Healthy and Independent Living at Home

Digital tools hold promise for many health benefits that can enhance the independent living and well-being of the elderly. Yet, their use is often perceived to have technological and privacy risks. SMART BEAR will deliver a solution offering:

- Continuous and objective monitoring and interventions for 21st century precise and personalised medicine towards optimising disease and associated risks' management
- Measurable improvements to the Quality of Life of the elderly and their ability to live independently



This project has received funding from the European Union Horizon 2020 innovation Action under grant agreement No 823951

Budget: € 22,379,512.49
Duration: Sep 19 - Aug 23

SPIDER 5G CYBER RANGE

A cyberSecurity Platform for vIrtualiseD 5G cybEr Range services

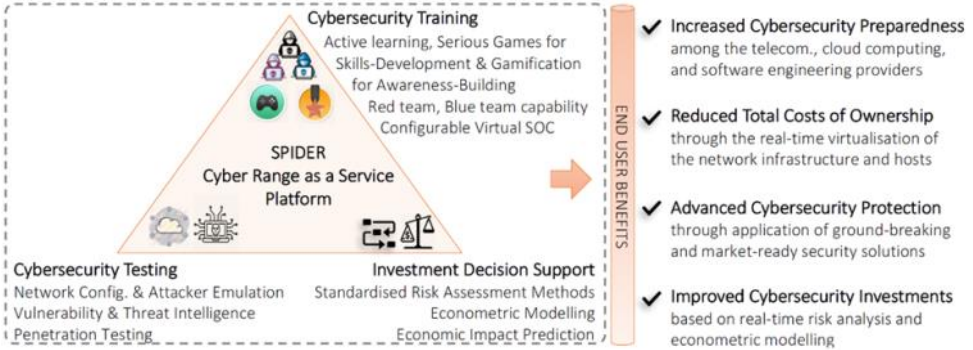
VISION

The vision of SPIDER is to deliver a next-generation, extensive, and replicable cyber range platform for the telecommunications domain and its fifth generation (5G), offering cybersecurity emulation, training and investment decision support. Towards this vision, it features integrated tools for cyber testing including advanced emulation tools, novel training methods based on active learning as well as econometric models based on real-time emulation of modern cyber-attacks

SPIDER PLATFORM

SPIDER will deliver an innovative Cyber Range as a Service (CRaaS) platform that extends and combines the capabilities of existing telecommunication testbeds and cyberranges with the most recent advances in telecommunications management and emulation, gamification and serious games training as well as economics of cybersecurity. The SPIDER cyber range platform rests on three major pillars:

1. cybersecurity testing and assessment, with emphasis on new security technologies
2. cybersecurity training in defending against advanced cyber-attacks
3. cybersecurity investment decision support



OBJECTIVES

- Design the architecture of a CRaaS platform for the telecommunications domain.
- Provide the telecommunications infrastructure that can support a cyber range with the latest 5G virtualisation, infrastructure management and orchestration technologies
- Design state-of-the-art AI/Machine Learning-based technologies capable of assessing the security of critical virtualised communication infrastructures.
- Design a digital gamified and serious game-based learning environment for training experts and non-experts
- Devise and integrate improved risk analysis and econometric models that can support organisations in making optimal investment decisions
- Design and implement a monitoring and reporting layer that can track the progress and outcomes of the end users while testing and training with the SPIDER CRaaS platform.
- Demonstrate and validate the integrated SPIDER CRaaS platform across four pilots.

ERICSSON cnit Telefónica THALES Atos UBITECH POLITÉCNICA

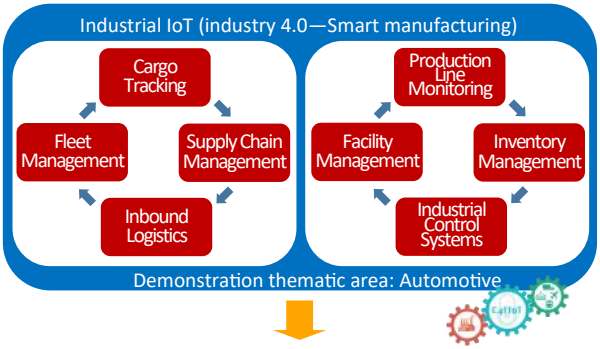
Singular Logic UNIVERSITY OF PIRAEUS RESEARCH CE FORTH SERIOUS GAMES INTERACTIVE UNIVERSITY OF PIRAEUS RESEARCH CENTER CITY UNIVERSITY LONDON Cyberlens

This project has received funding from the EU H 2020 Research & Innovation program under Grant Agreement No 833685.

infalia InfoCom Sphynx Technology Solutions

Cybersecurity 4.0: Protecting the Industrial Internet of Things

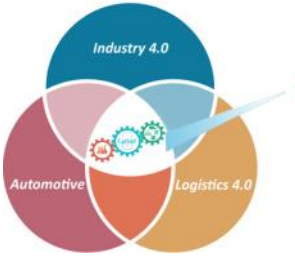
C4IIOT will design, build and demonstrate a novel framework that implements an innovative IoT architecture paradigm to provide an end-to-end holistic and disruptive security-enabling solution for minimizing the attack surfaces in Industrial IoT systems.



one big idea.

Cybersecurity challenges:

- Detect in almost real time vulnerabilities and incidents in a large scale IoT system
- Achieve visibility and control across the distributed industrial value chain - extensive monitoring
- End-user education need to extend across the complete industrial value chain
- Lack of security in protocols and gateways
- Lack of analytics related to security
- All parts of the industrial value chain follow standards and IoT security regulations



- Hardware-enabled security assurance
- Context-aware intelligence for detecting anomalous or malicious behavior
- Security assurance by horizontal device-to-device communication architectures

2 demonstration scenarios

https://www.c4iiot.eu/

FORTH · CRF Centro Ricerche Fiat · Infineon · Thales · Hewlett Packard Enterprise · cea · IBM · AEGIS IT Research · Pantheon Sorbonne · ITML · Sphynx Technology Solutions · University of Greenwich · vip

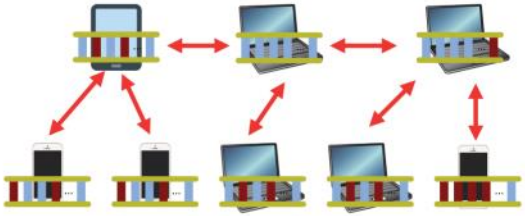
Start Date: 1st June 2019 **EU Contribution**: 4,993,533 **Duration:** 36 Months **Project Coordinator:** Forth
This project has received funding from the EU H2020 RIA program under Grant Agreement No 833828.

BIO-PHOENIX

BIOLOGICALLY INSPIRED COMPLEX SOFTWARE SYSTEM RECONSTRUCTION AT NEAR EXTINCTION STATES

https://www.bio-phoenix.eu/

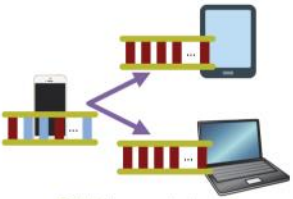
BIO-PHOENIX approach is to develop a solution for extensive system reconstruction based on the concept of computational DNA (co-DNA). Similarly, to DNA, the co-DNA will model and encapsulate the basic functional units of a software system that are required to fully reconstruct it.



Software System: a network fo co-DNA enabled system cells

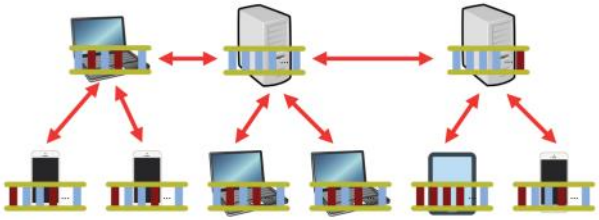
The overall aim of BIO-PHOENIX is to create a fundamentally different paradigm of designing and implementing software systems with a bio-inspired, co-DNA based capability for self-organisation and self-reconstruction, resilient to extensive damage.

System in near extinction



co-DNA transmission for system recosntruction

co-DNAt acceptance, rejection and further retransmission



Reconstructed System: a potentioal altered set of system cells and communiaction networks

This project has received funding from the European Union's Horizon 2020 research and innovation staff exchange programme (RISE) under the Marie Skłodowska-Curie grant agreement No 823951

Budget: €1,324,800, **Duration:** 1 July 2019 - 30 June 2023

A Framework for Pairing Circular Economy and IoT: IoT as an enabler of the Circular Economy & circularity-by-design as an enabler for IoT

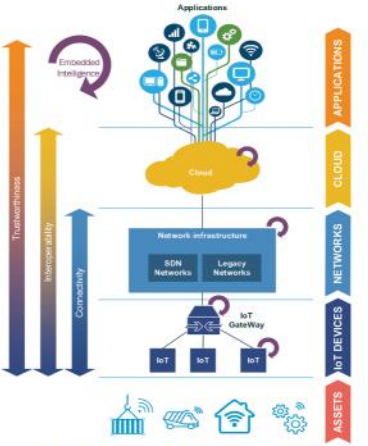
https://www.ce-iot.eu/

AIM

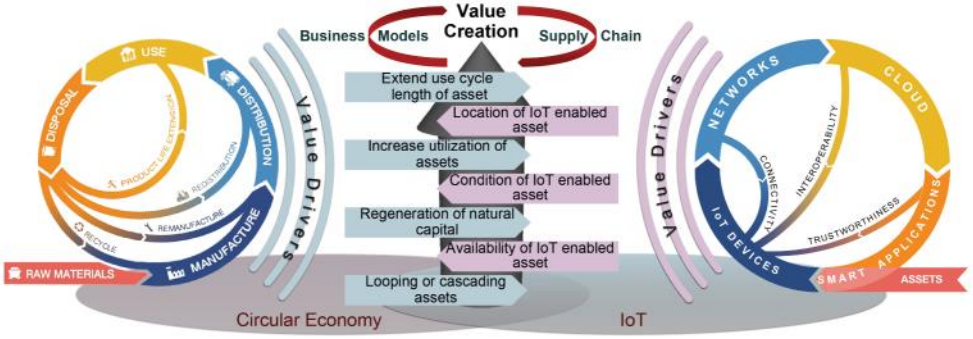
To develop an innovative framework of interplay between Circular Economy and IoT, to explore novel ways in which this interaction can drastically change the nature of products, services, business models and ecosystems.

The CE-IoT framework will be bi-dimensional and bi-directional in terms of circularity aiming to develop:

- Novel circular economy business models and service supply chains to unlock CE-IoT synergies
- An Open circular-by-design IoT architecture, where "smart" IoT objects are integrated in the IoT ecosystem through patterns



Key Technical challenges: Trustworthiness, Interoperability, Connectivity



CE-IoT vision blends the paradigm of Circular Economy and Internet of Things to explore novel ways in which this interaction can drastically change the nature of products, services, business models and ecosystems. This way Circular Economy and IoT provide value drivers that merge to new value creation.

École des Ponts business school · University of Cambridge Judge Business School · FORTH · cablenet · BLUESOFT EFFICIENT SOLUTIONS · Deloitte.

This project has received funding from the European Union's Horizon 2020 Research and Innovation Staff Exchange programme (RISE) under the Marie Skłodowska-Curie grant agreement No 777855 **Budget:** €1,692,000.00, **Duration:** 1 July 2018 - 30 June 2022

https://www.ideal-cities.eu

Ideal Cities

Intelligence **D**riven Urban IoT **E**cosystems for Circular S**A**fe and Inc**L**usive Smart **C**ities

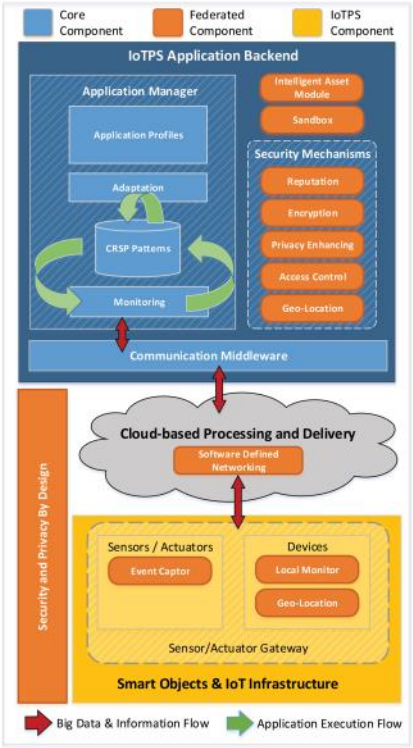
Ideal Cites aims to provide a novel, open and extensible platform to enable the secure and resilient acquisition and sharing of information that is collected by individual citizens and/or authorities, through IoT and participatory data.

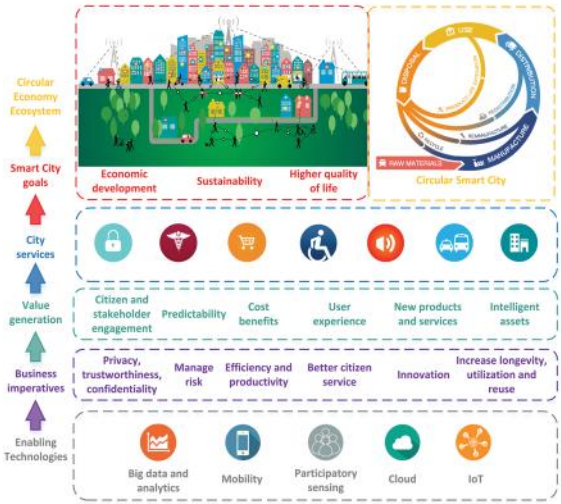
The IoT and Participatory Sensing (IoTPS) envisioned architecture:

Communication Middleware: for connecting applications with IoT devices and/or smart devices for participatory sensing.

Security Mechanisms: basic device and/or user identification, authentication, access control, privacy enhancing, confidentiality maintaining, integrity and encryption functions.

Application Manager: the application back-end, which serves as the runtime environment for the various IoTPS application profiles.



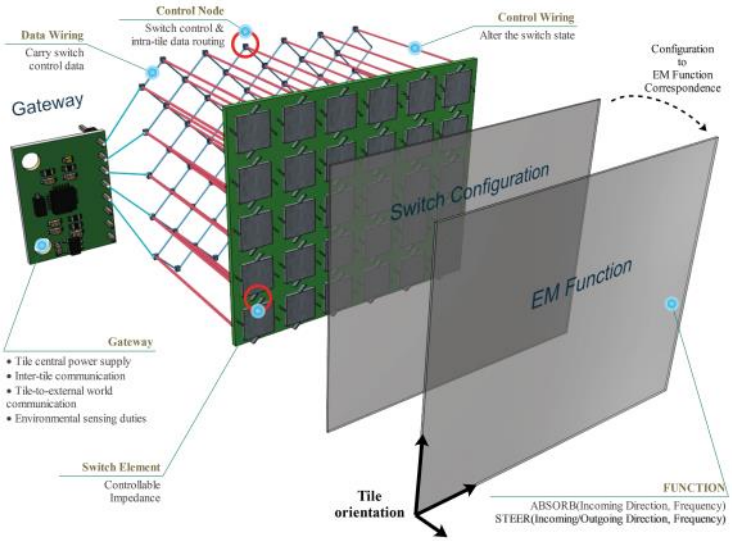


Ideal Cities will form an exploitation plan, assessing the potential availability and a strategic conclusion for each of the business imperatives of the Smart City value chain. Market driving forces for Smart Cities will be considered along with their positive or negative influence on potential products.

This project has received funding from the European Union's Horizon 2020 research and innovation staff exchange programme (RISE) under the Marie Skłodowska-Curie grant agreement No 778229 **Budget:** €1,692,000.00, **Duration:** July 18 - June 22

METASURFACE HYPERVISOR

VisorSurf — A Hardware Platform for Software-Driven Functional Metasurfaces



"To control electro-magnetic interaction via software"

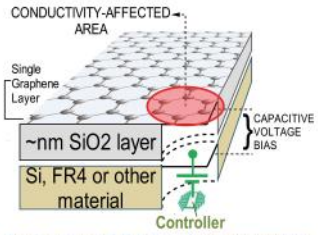
Objectives

VisorSurf's main objective is the development of a hardware platform, the HyperSurface, whose electromagnetic behavior can be defined programmatically. The key-enablers are the metasurfaces, artificial materials whose electromagnetic properties depend on their internal structure. HyperSurfaces merge metamaterials with a network of miniaturized, custom electronic controllers, the nanonetwork. The nanonetwork receives external programmatic commands and alters the metasurface structure, yielding a desired electromagnetic behavior for the HyperSurface.

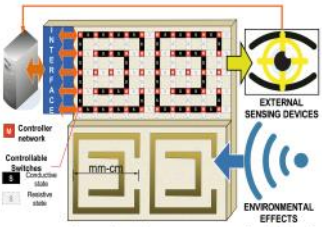
Implementation

Two experimental prototypes will be implemented:

- a switch-based fabric array as the control medium;
- a Graphene based, making use of its exquisite properties to provide finer control.



Exploration of the Graphene properties



Incorporating the Electromagnetic behavior of mater into smart control loops

Embedded Systems
Electromagnetism
Metasurfaces
Nano-networks
Softwarization

Horizon 2020
FETOPEN – RIA
Project ID: 736876

Duration:
2017 – 2020

Total cost:
EUR 5.748.000

Coordinated by
FORTH

Get more info
www.visorsurf.eu

Stay Tuned
VisorSurf
@VisorSurf

FORTH
University of Cyprus
Fraunhofer Gesellschaft
SignalGenerix
UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH
Aalto University

This project has received funding from the European Union's Horizon 2020 research and innovation programme-Future Emerging Topics (FETOPEN) under grant agreement No 736876

UNICORN

A DevOps-as-a-Service Framework

An open DevOps platform to design, deploy and manage secure and elastic by design multi-cloud microservices

Horizon 2020
European Union funding
for Research & Innovation

...making CLOUD COMPUTING easier for SMEs and STARTUPS!

unicorn-project.eu @Unicorn_H2020 unicorn@cincubator.com

Features

Unified DevOps Tool

Offer a single tool for application **development**, **deployment**, and **management** during the whole application lifecycle

Monitoring & Resource Adaptation

Unicorn **elasticity library** supports apps to elastically **(de-)allocate resources** and provides **real-time monitoring** and **analytics**

True Multi-Cloud Deployments

Unicorn supports **transparent** and **automated multi-cloud deployments** for services to span across cloud zones and geographical regions

Privacy & Security Adoption

Unicorn **security** and **privacy design libraries** prevent **data breaches** and **ensure** customer **privacy**

Unicorn Ecosystem & technologies

UNICORN Contest

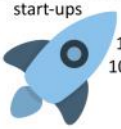
CLOUD INCUBATOR HUB

redikod

Steinbeis

3 hubs

Participate in a **contest** for SMEs and start-ups



12 selected, 10.000 € each

Extend your product using UNICORN framework or develop a **prototype**

Participate on innovation **workshops**

Test elasticity, security, privacy features

This work is supported by the European Commission in terms of Unicorn 731846 H2020 project (H2020-ICT-2016-1)


CITRIX


Sphynx
Technology
Solutions


Blue
car rental


CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion


AR
THREAT
ST


RESIST


CERTCOOP


I-BiDaaS
Industrial-Driven Big Data as a Self-Service Solution


SMESEC


Cyber
Sure


SEMIOTICS


GUARD


Smart
Bear


SPIDER
5G CYBER RANGE


C4IIoT


BIO
PHOENIX


CELOT


Ideal
Cities


Visor
SURF


UNICORN