SANCUS - Towards Unifying the Analysis and Control of Security, Privacy and Service Reliability

Charilaos Zarakovitis
NCSR ”DEMOKRITOS”
c.zarakovitis@iit.demokritos.gr

Nikolaos Pitropakis
Eight Bells LTD
nikolaos.pitropakis@8bellsresearch.com

Dimitrios Klonidis
UBITECH Ltd
dklonidis@ubitech.eu

Hicham Khalife
Thales Com. & Security
hicham.khalife@thalesgroup.com

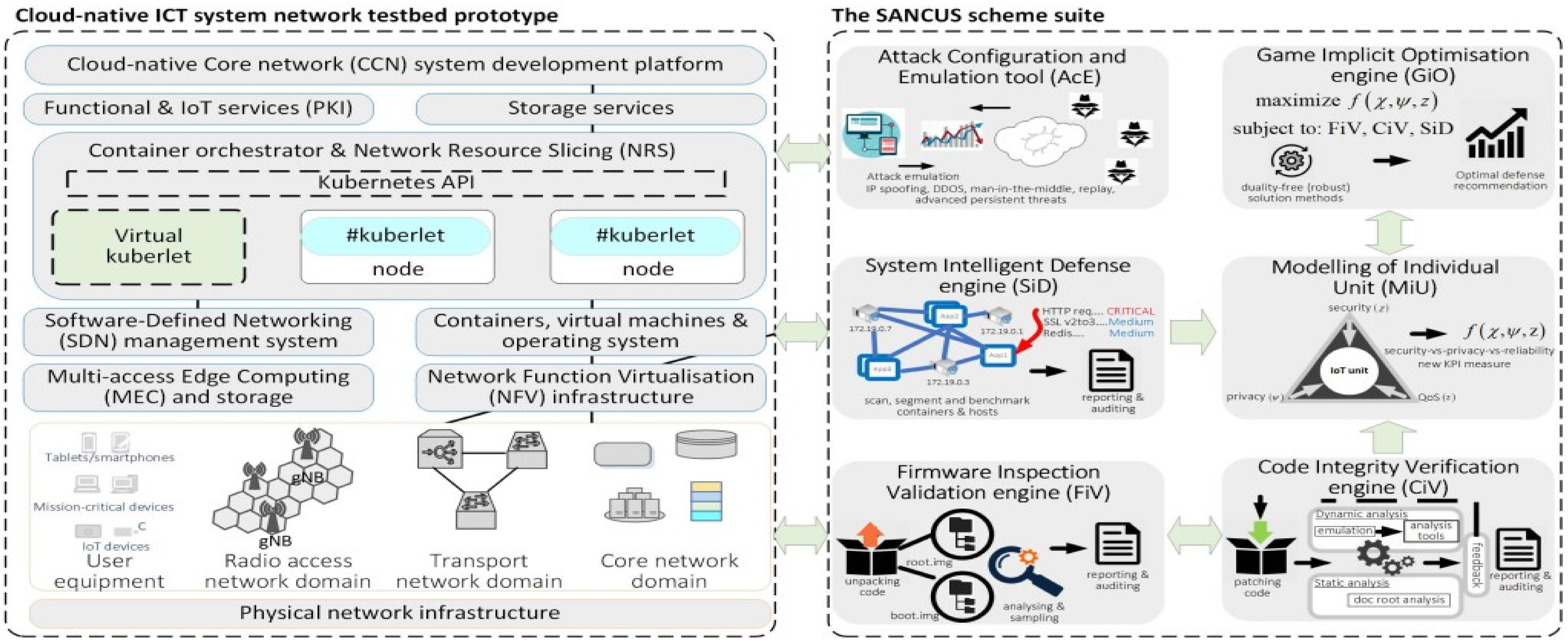
Rationale

Advance new technologies such as 5G and edge processing, require intelligent cybersecurity solutions to cope with complex system attacks in the most efficient manner and without compromising the Quality-of-Service (QoS) reliability. It is noted though that security and privacy are holistic attributes that are highly influential to the overall aspects of QoS reliability at both communication and application levels.

Key idea

SANCUS relies on expressing the notions of cyber security and digital privacy by means of final formulas and fuse these formulas into optimisation strategies to acquire the truly optimal defense recommendation in dynamic manner.

The aim is to obtain inclusive solutions in the form of unified **security-vs-privacy-vs-reliability** trade-offs, for manipulating the system network cybersecurity, privacy and quality of service performance jointly, explicitly and automatically.



Cloud-native ICT system network testbed prototype

The SANCUS scheme suite

Cloud-native Core network (CCN) system development platform
Functional & IoT services (PKI)
Storage services
Container orchestrator & Network Resource Slicing (NRS)
Kubernetes API
Virtual kuberlet
#kuberlet
node
#kuberlet
node
Software-Defined Networking (SDN) management system
Containers, virtual machines & operating system
Multi-access Edge Computing (MEC) and storage
Network Function Virtualisation (NFV) infrastructure
Tablets/smartphones
Mission-critical devices
IoT devices
User equipment
gNB
gNB
Radio access network domain
Transport network domain
Core network domain
Physical network infrastructure
Attack Configuration and Emulation tool (AcE)
Attack emulation
IP spoofing, DDOS, man-in-the-middle, replay, advanced persistent threats
Game Implicit Optimisation engine (GiO)
maximize $f(\chi,\psi,z)$
subject to: FiV, CiV, SiD
duality-free (robust) solution methods
Optimal defense recommendation
System Intelligent Defense engine (SiD)
172.19.0.7
172.19.0.1
172.19.0.3
App2
App1
App3
HTTP req.... CRITICAL
SSL v2to3....Medium
Redis.... Medium
scan, segment and benchmark containers & hosts
reporting & auditing
Modelling of Individual Unit (MiU)
security (z)
privacy (ψ)
QoS (z)
IoT unit
$f(\chi,\psi,z)$
security-vs-privacy-vs-reliability new KPI measure
Firmware Inspection Validation engine (FiV)
unpacking code
root.img
boot.img
analysing & sampling
reporting & auditing
Code Integrity Verification engine (CiV)
patching code
Dynamic analysis
emulation
analysis tools
Static analysis
doc root analysis
feedback
reporting & auditing

Implementation remarks

Platform implementation considers 6 main engines related to a reference 5G system testbed prototype as shown in figure above:

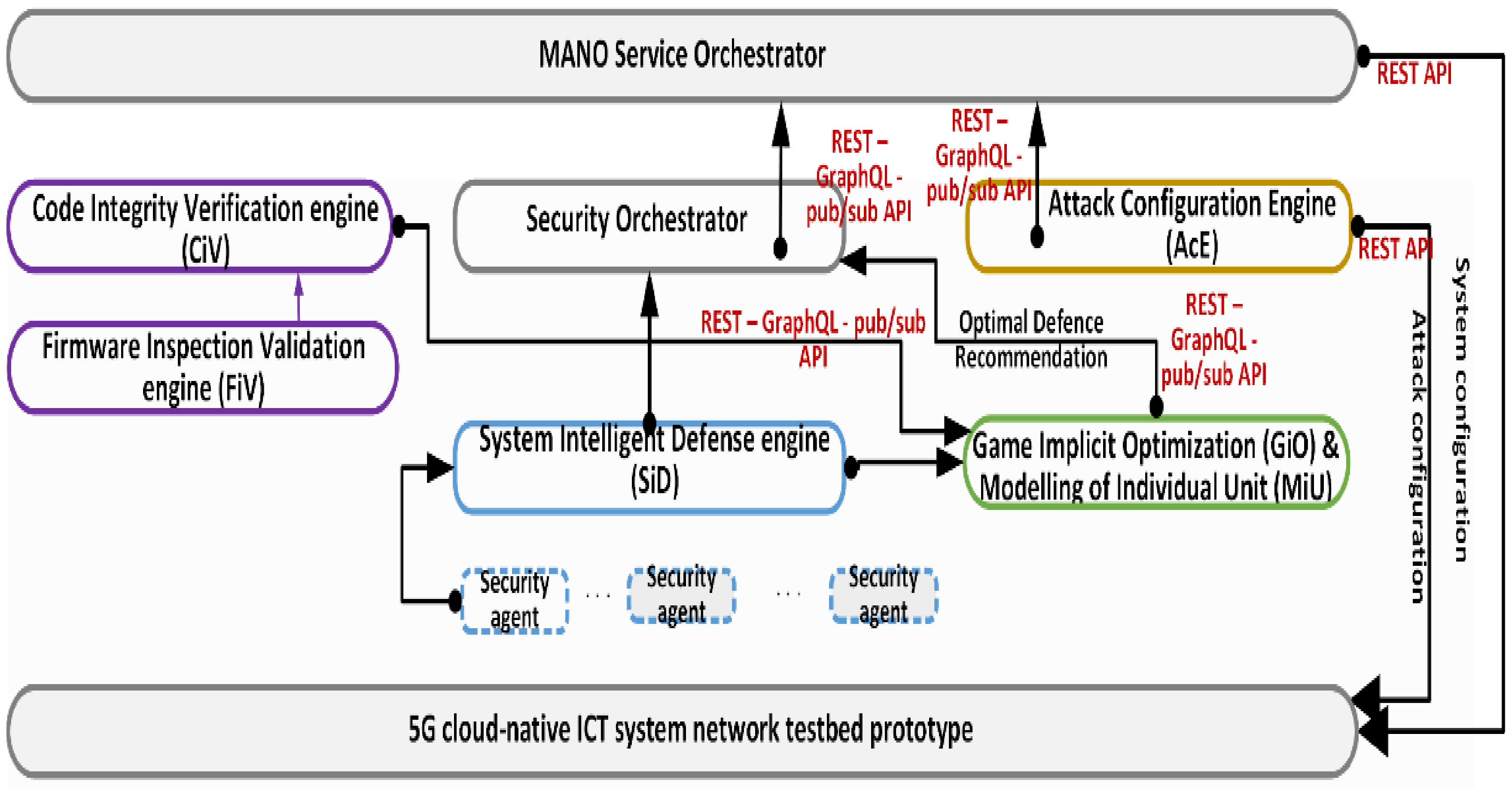
- FiV – Firmware unpacking of OEM IoT devices incl. analysis and sampling
- CiV – Firmware code inspection combining static (symbolic) and dynamic analysers for maximising the surface of vulnerability discovery
- SiD – Runtime risk analysis of system components by multiple monitoring agents with reduced complexity targeting high quality delivery in real-time
- AcE – Attack emulation module for configuring various testing scenarios
- MiU – Modelling of the IoT unit for expressing the trade-off between cyber security, digital privacy and QoS reliability. Extraction of a combined KPI
- GiO – Game implicit optimization of cybersecurity performance by maximising the security-vs-privacy-vs-reliability efficiency

Ground braking platform features envisioned within SANCUS:

- Novel intelligent cybersecurity performance optimization scheme design allowing the joint security, privacy and reliability performance optimization
- Automated cybersecurity firmware validation and verification using new analysis methods
- Automated cybersecurity risk assessment for open-source software
- Revolutionary multi-dimensional modelling approach of IoT unit
- Automated cybersecurity performance optimisation using intelligent game implicit approach
- Robust computational algorithms for KPI trade-offs' calculations
- Integrateability in standardized 5G systems including testing and demonstration

The SANCUS platform architecture

FiV unpacks a given set of IoT firmware images and performs pre-processing sanitisation, and classification. The outcome is fused into the CiV engine that performs static and dynamic analysis for code vulnerabilities. In parallel, the SiD engine performs continuous risk assessment of the software runtime deployment environment. The outcomes of FiV, CiV and SiD are processed by the MiU engine, so as, to be expressed by means of optimisation criteria. The Analytic Hierarchy Process concept together with probabilistic weighting are used to implement the groupings of data risks related to each network device. Next, the GiO engine optimises security, subject to the updated security modelling and by capturing the heterogeneity among all the created expected utility fitness functions of the network devices. The output of GiO is fused into the Security Orchestrator, which creates new Security Policy Templates, or upgrades existing templates. These are provided to the MANO Orchestrator instructing the move of VNF for protecting the system.



MANO Service Orchestrator
REST API
REST – GraphQL - pub/sub API
REST – GraphQL - pub/sub API
Code Integrity Verification engine (CiV)
Security Orchestrator
Attack Configuration Engine (AcE)
REST API
Firmware Inspection Validation engine (FiV)
REST – GraphQL - pub/sub API
Optimal Defence Recommendation
REST – GraphQL - pub/sub API
System Intelligent Defense engine (SiD)
Game Implicit Optimization (GiO) & Modelling of Individual Unit (MiU)
Security agent
Security agent
Security agent
Attack configuration
System configuration
5G cloud-native ICT system network testbed prototype

Conclusion

– SANCUS offers a novel cybersecurity scheme that automates in-depth inspection and analysis of OEM firmware, continuous software risk assessment, adaptive modelling of the network unit and dynamic security-vs-privacy-vs-reliability efficiency optimization. A testbed prototype is developed for the system implementation and validation of complex use cases. SANCUS constitutes a paradigm shift in the design of next-generation cybersecurity solutions with much potential to improve trust and confidence in our global digital ecosystem.

Visit
https://www.sancus-project.eu/

Contact
info@sancus-project.eu

Follow SANCUS in

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 952672