ATLANTIS

Improved resilience of CIs against large scale transnational and systemic risks

The project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. **101073909**

ATLANTIS IDENTITY CARD

WHO: **37 PARTNERS** FROM **10 COUNTRIES (+ 8 INDIRECTLY ASSOCIATED)**

WHAT: EC HE GRANT UNDER THE CALL CL3-2021-INFRA-01

WHEN: 1 OCTOBER 2022 → 30 SEPTEMBER 2025 (36 MONTHS)

WHY: IN RESPONSE TO TOPIC: CL3-2021-INFRA-01-01 *"EUROPEAN INFRASTRUCTURES AND THEIR AUTONOMY SAFEGUARDED AGAINST SYSTEMIC RISKS"*

MISSION: IMPROVE THE RESILIENCE AND THE PROTECTION CAPABILITIES OF INTERCONNECTED ECI EXPOSED TO **EVOLVING SYSTEMIC RISKS DUE TO EXISTING AND EMERGING LARGE-SCALE, COMBINED, CYBER-PHYSICAL THREATS AND HAZARDS**, GUARANTEE THE CONTINUITY OF OPERATIONS, WHILE MINIMIZING CASCADING EFFECTS BY ADOPTING SUSTAINABLE SECURITY SOLUTIONS.

HOW: HORIZON INNOVATION ACTION (BUDGET: **€ 12,728,564.50**, FUNDING: **€ 9,998,535**)

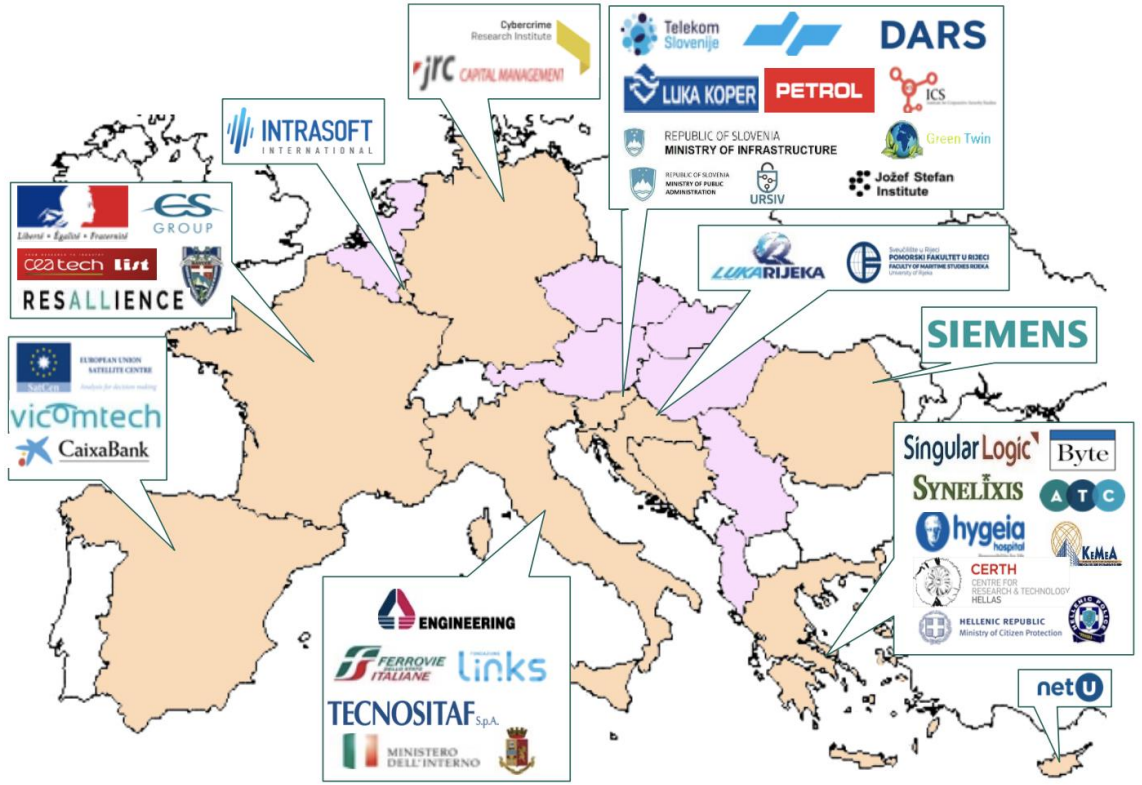
ATLANTIS

The project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. **101073909**

ATLANTIS COVERAGE #1

GEOGRAPHICAL COVERAGE

- **CENTRAL**: ITALY, FRANCE, BELGIUM, GERMANY, LUXEMBURG, AUSTRIA, NETHERLANDS
- **SOUTHERN-EAST**: GREECE, CYPRUS, ROMANIA, SLOVENIA, CROATIA, ALBANIA, SLOVAKIA, HUNGARY,
- **SOUTHERN-WEST**: SPAIN



ATLANTIS

The project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. **101073909**

ATLANTIS COVERAGE #2

VALUE-CHAIN COVERAGE

- **CI OPERATORS AND CI END-USERS** IN VARIOUS SECTORS (**12**): LUK (**PORT**), LUR (**PORT**), DARS (**HIGHWAY**), SITAF (**HIGHWAY**), SZ (**RAILWAY**), FST (**RAILWAY**), TS (**TELCO**), PET (**ENERGY**), HYG (**HEALTHCARE**), CXB (**FINANCE**), JRC (**FINANCE SERVICE**), SDIS73 (**FIRE SERVICE**)
- **CIP/CIR SOLUTION/TECHNOLOGY PROVIDERS** (**6**)**:** ENG, CS GROUP, INTRA, SLG, SIEM, RES
- **RESEARCH INSTITUTES** (**9**)**:** KEMEA, ICS, SAT, JSI, PRFI, CEA, CERTH, LINKS, VICOM
- **INNOVATIVE HIGH-TECH SME** WITH SECURITY EXPERTISE (**6**): SYN, NETU, BYTE, ATC, CRI, SNEP.
- **SECURITY GOVERNMENT ENTITIES** (**4**)**:** MZI (**SLOVENIAN MINISTRY FOR INFRASTRUCTURE**), UIV (**SLOVENIAN MINISTRY OF INFORMATION SECURITY**), MDI (**ROAD, RAIL AND COMMUNICATIONS SECURITY**), HPL (**HELLENIC POLICE**)

The project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. **101073909**

ATLANTIS LANDSCAPE #1

- EU Security Union Strategy for the period 2020-2025 identifies the protection of CI as one of the main priorities for the EU and its Member States.
- Digital and interconnected CIs are based on novel and sophisticated technologies which generate potential **new vulnerabilities**, either accidental or intentional.
- Networked CIs might cause **long-lasting cascading effects** in other **multi-sector and cross-border** CIs
- CIs increasingly appear as potential **new targets** for **new threats and attacks**, especially the hybrid ones (e.g. cyber-physical), operating in a **rapidly evolving societal, technological and business environment**
- Limited research on **large scale, transnational and cross-domain coordinated attacks**, especially at a **systemic level**

ATLANTIS

The project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. **101073909**

ATLANTIS LANDSCAPE #2

- ATTACK SURFACE AND THE IMPACT OF ATTACKS CAN ESCALATE RAPIDLY AND NEGATIVELY AFFECT OTHER CIS AND WIDER PARTS OF VITAL SOCIETAL FUNCTIONS
  - **CYBER-PHYSICAL** AND **COORDINATED** (AMONG DIFFERENT ACTORS, EVEN IN DIFFERENT COUNTRIES), **MIXED** (USING DIFFERENT TACTICS), **DISRUPTIVE** (LEADING TO THE COLLAPSE OF ENTIRE SYSTEMS, SECTORS OR REGIONS), **UNEXPECTED**, **SUBVERSIVE**, AND **DIFFICULT TO IDENTIFY** EARLY
  - MAJOR **NATURAL HAZARDS** (E.G. FLOODS, WILDFIRES, OFTEN UNEXPECTED AND UNPREDICTABLE) ARE ALSO BIG CONCERNS THAT CAN CREATE DISRUPTION TO ECI, THUS AFFECTING WIDER FUNCTIONS OF OUR SOCIETY.
- UNDERSTAND THE SYSTEM AS A **COMPLEX NETWORK OF INDIVIDUAL AND INSTITUTIONAL ACTORS** WITH DIFFERENT AND OFTEN CONFLICTING INTERESTS

ATLANTIS

The project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. **101073909**

ATLANTIS STRATEGIC CHALLENGE AND MISSION

ATLANTIS AIMS AT **ENHANCING RESILIENCE AND CYBER-PHYSICAL-HUMAN (CPH) SECURITY OF THE KEY ECI**, GOING BEYOND THE SCOPE OF DISTINCT ASSETS, SYSTEMS, AND SINGLE CI, **BY ADDRESSING RESILIENCE AT THE SYSTEMIC LEVEL** AGAINST MAJOR NATURAL HAZARDS AND COMPLEX ATTACKS THAT COULD POTENTIALLY DISRUPT VITAL FUNCTIONS OF THE SOCIETY.

THE MISSION OF ATLANTIS IS TO **IMPROVE THE RESILIENCE** AND THE PROTECTION CAPABILITIES OF **INTERCONNECTED ECI EXPOSED TO EVOLVING SYSTEMIC RISKS** DUE TO EXISTING AND EMERGING LARGE-SCALE, COMBINED, CYBER-PHYSICAL THREATS AND HAZARDS, **GUARANTEE THE CONTINUITY OF OPERATIONS, WHILE MINIMIZING CASCADING EFFECTS** IN THE INFRASTRUCTURE ITSELF, THE ENVIRONMENT, OTHER CIS, AND THE INVOLVED POPULATION, ENABLING PUBLIC AND PRIVATE ACTORS TO MEET CURRENT AND EMERGING CHALLENGES BY ADOPTING SUSTAINABLE SECURITY SOLUTIONS.

The project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. **101073909**

ATLANTIS SECURITY STRATEGIC GOALS

1. **AWARENESS.** **IMPROVE KNOWLEDGE ON LARGE-SCALE**, VULNERABILITY ASSESSMENT AND LONG-TERM SYSTEMIC RISKS

2. **CAPABILITY.** **IMPROVE THE SYSTEMIC RESILIENCE OF ECI**, THROUGH NOVEL, ADAPTIVE, FLEXIBLE, AND CUSTOMIZABLE SECURITY MEASURES ("BY DESIGN") AND TOOLS ("BY INNOVATION")

3. **COOPERATION.** **EFFECTIVE COOPERATION** AMONG CI OPERATORS AND GOVERNMENT SECURITY STAKEHOLDERS, WHILE PRESERVING CI AUTONOMY AND SOVEREIGNTY

4. **TECHNOLOGY.** **DELIVER AN OPEN TECHNOLOGICAL FRAMEWORK** THAT WILL PROVIDE THE ECIS WITH AI-BASED SOLUTIONS FOR INCREASED **AWARENESS**, **CAPABILITY**, AND **COOPERATION** IN MANAGING SYSTEMIC THREATS

ATLANTIS

The project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. **101073909**

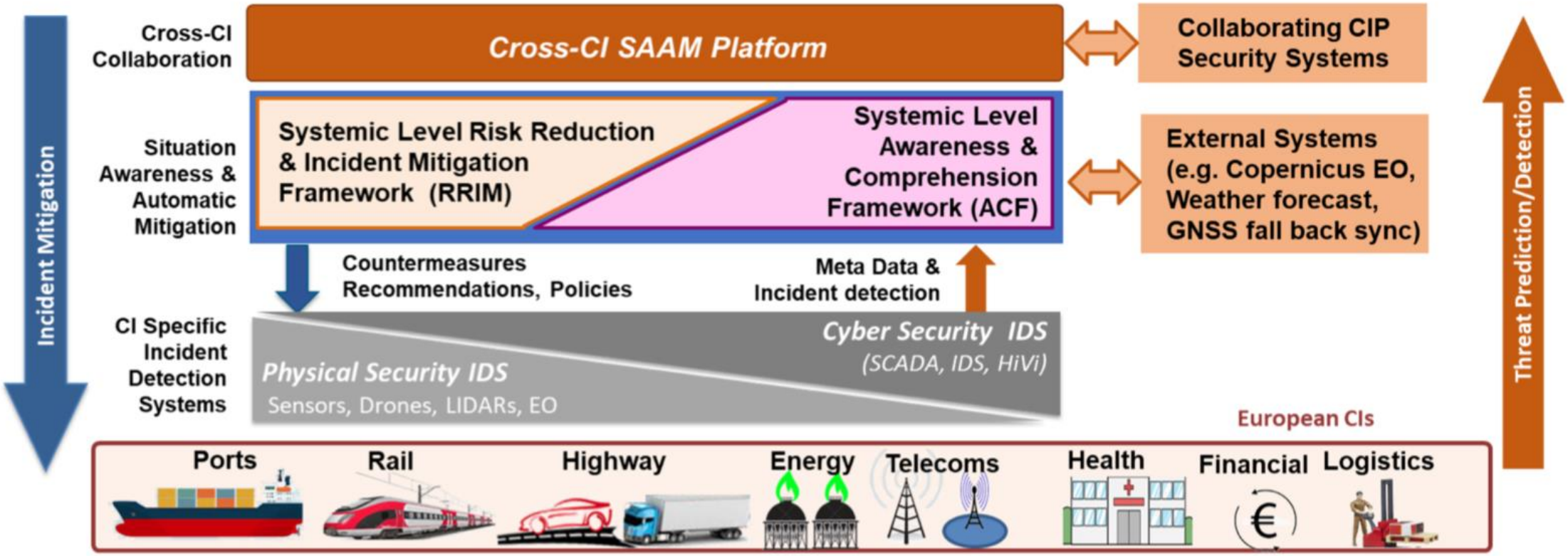
ATLANTIS OBJECTIVES

1. CONTINUOUS AND COLLABORATIVE **LARGE-SCALE HYBRID VULNERABILITY ASSESSMENT** SUPPORT
2. **LONG-TERM INTRA-DOMAIN, CROSS-DOMAIN, AND CROSS-BORDER** SYSTEMIC RISK ANALYSIS
3. CONFIDENTIALITY PRESERVING **FEDERATED MACHINE LEARNING** (FML) AND **EXPLAINABLE AI** (XAI)
4. TRUSTED COLLABORATIVE **CROSS-DOMAIN/CROSS-BORDER KNOWLEDGE SHARING** AND MITIGATION
5. **5G AND MULTI-CONSTELLATION SATELLITE SYSTEMS** TO COMPLEMENT GNSS IN PNT SERVICES
6. IMPROVED USE OF **THREAT INTELLIGENCE** FOR THE ANTICIPATION OF SYSTEMIC RISKS
7. SYSTEMIC, LARGE-SCALE, **CPH** SITUATION AWARENESS FOR RESILIENT ECI
8. **REAL-TIME COOPERATIVE CYBER/PHYSICAL SECURITY MONITORING** AND MITIGATION FACILITY
9. **REAL-WORLD DEMONSTRATION** OF ATLANTIS METHODOLOGY AND FRAMEWORK
10. **SKILLS IMPROVEMENT AND CAPABILITY MATURITY**
11. **COOPERATION SUPPORT AND ETHICAL, LEGAL, AND SOCIETAL ACCEPTANCE** OF THE ATLANTIS SOLUTIONS

ATLANTIS

The project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. **101073909**

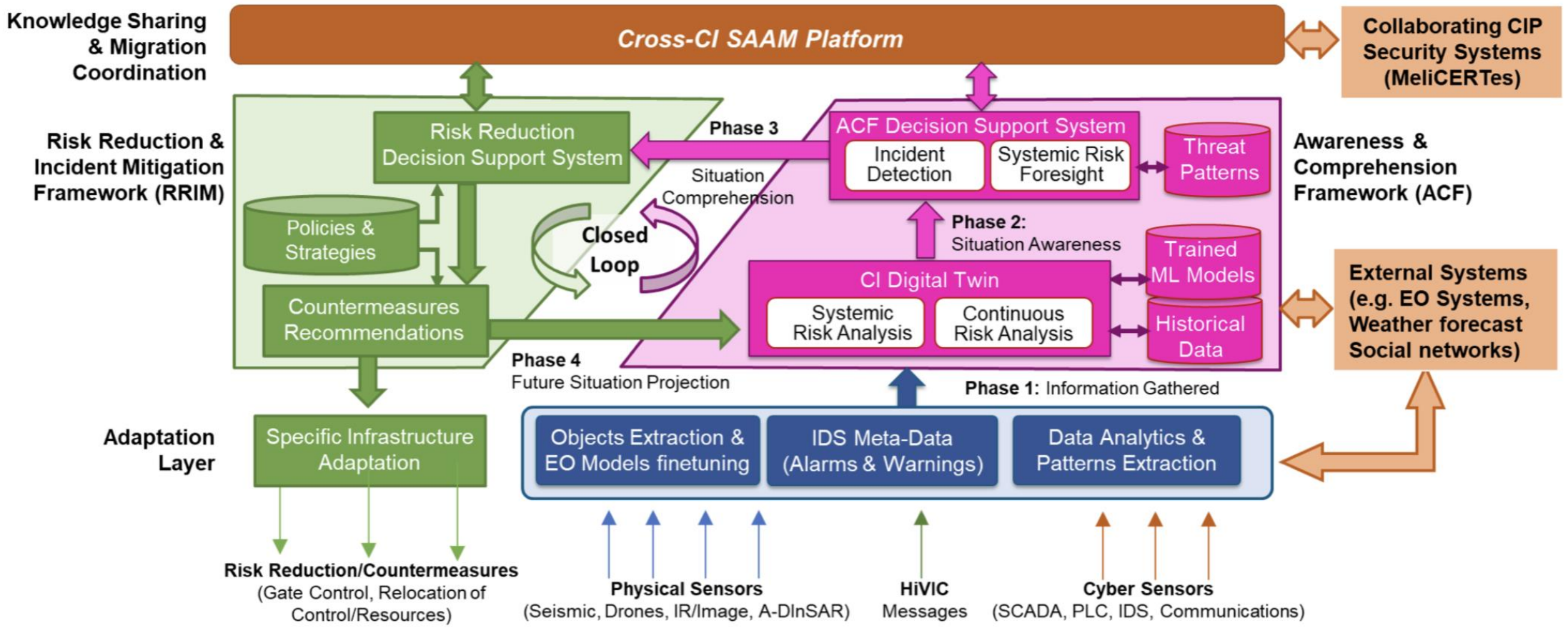
ATLANTIS 3-LAYER HIGH-LEVEL ARCHITECTURE



ATLANTIS

The project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. **101073909**

ATLANTIS COLLABORATING FRAMEWORKS



ATLANTIS

The project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. **101073909**

VALIDATION IN LARGE SCALE PILOTS – LSP #1

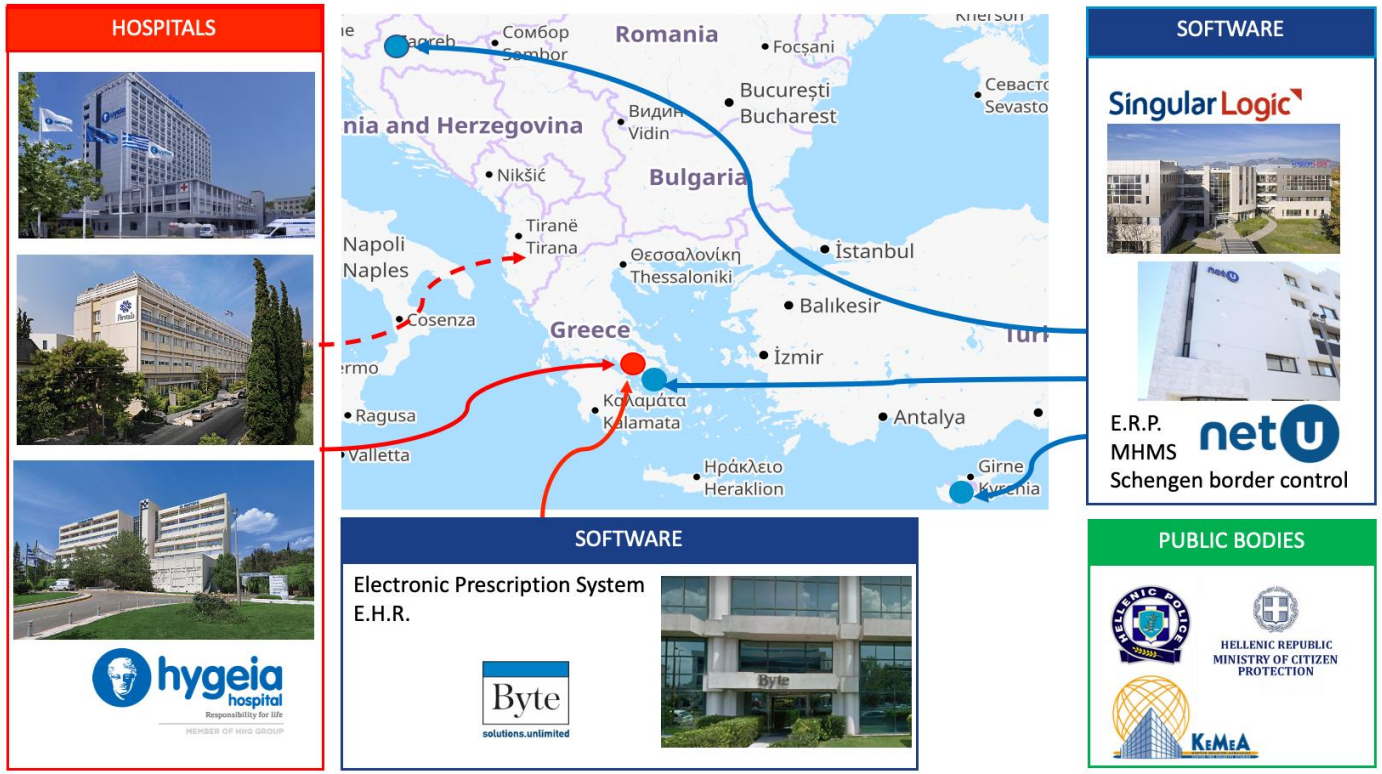
Cross-Border/Cross Domain Large Scale Pilot in Transport, Energy and Telecoms
(Slovenia, Croatia, Italy and France)

ATLANTIS

The project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. **101073909**

VALIDATION IN LARGE SCALE PILOTS – LSP #2

Cross Domain Large Scale Pilot in Health, Logistics/Supply Chain and Border control
(Greece, Cyprus, Croatia, Albania)

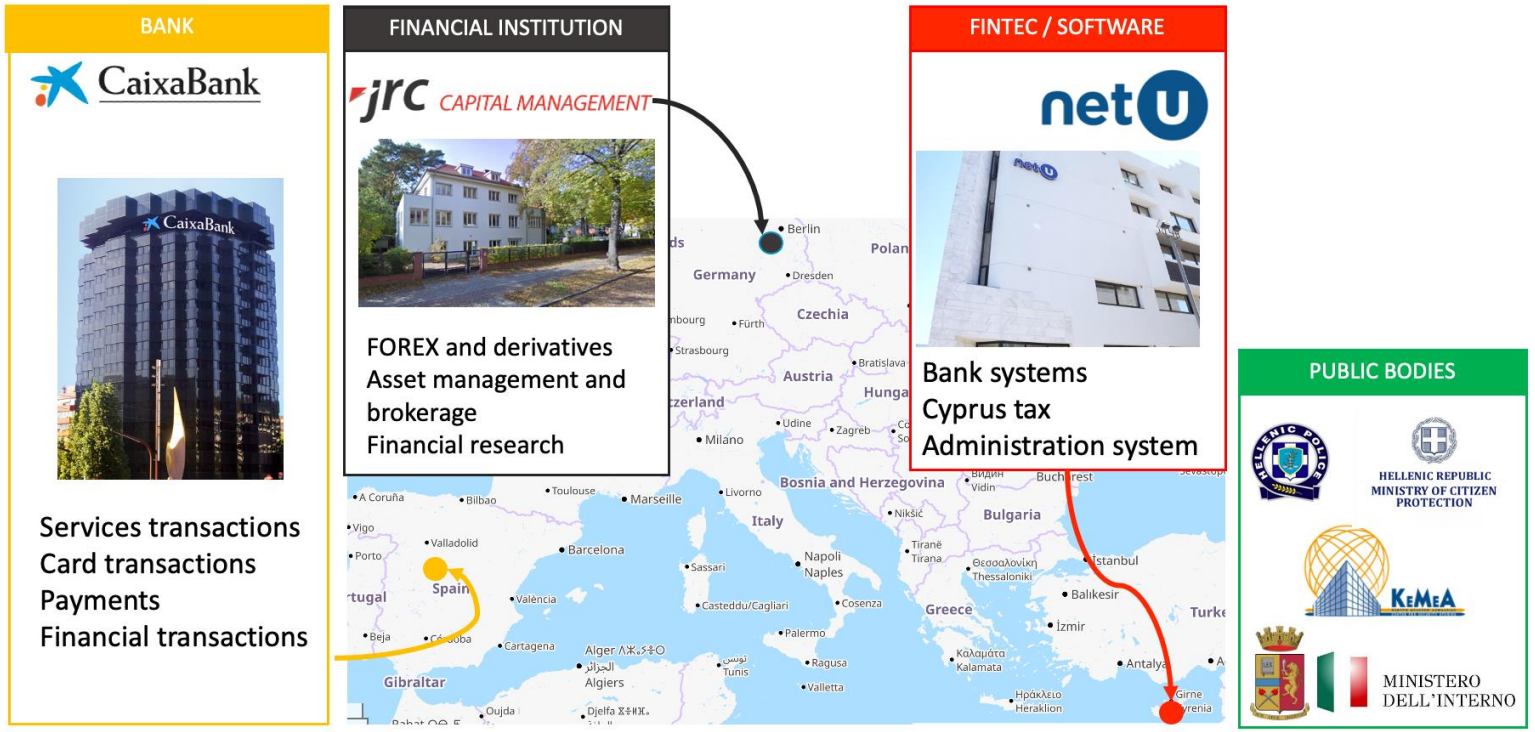


ATLANTIS

The project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. **101073909**

VALIDATION IN LARGE SCALE PILOTS – LSP #3

Cross Domain Large Scale Pilot in Health, Logistics/Supply Chain and Border control
(Spain, Germany and Cyprus)



ATLANTIS

The project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. **101073909**

VALIDATION IN LARGE SCALE PILOTS – OVERVIEW

	Countries		Security						Threats							
	Directly Involved	Indirectly Involved	Sectors\ Domains	Physical	Cyber	Human	Tactical	Strategic	Climate Change	Natural Hazards	Aging/ Natural	Human Attack	Human Mistake	Hybrid	Dis- information	Systemic
LSP1	4	0	3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LSP2	2	2	3	✓	✓	✓	✓	✓	-	-	-	✓	✓	✓	✓	✓
LSP3	3	10	1	-	✓	✓	-	✓	-	-	-	✓	✓	✓	✓	✓

ATLANTIS

The project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. **101073909**

ACKNOWLEDGEMENT

The project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. **101073909**

The project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. **101073909**

Find more

www.atlantis-horizon.eu/

ATLANTIS

The project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. **101073909**