ASSURE

Future Proofing of ICT Trust Chains: Sustainable Operational Assurance for SoS Security and Privacy

Discover ASSURED

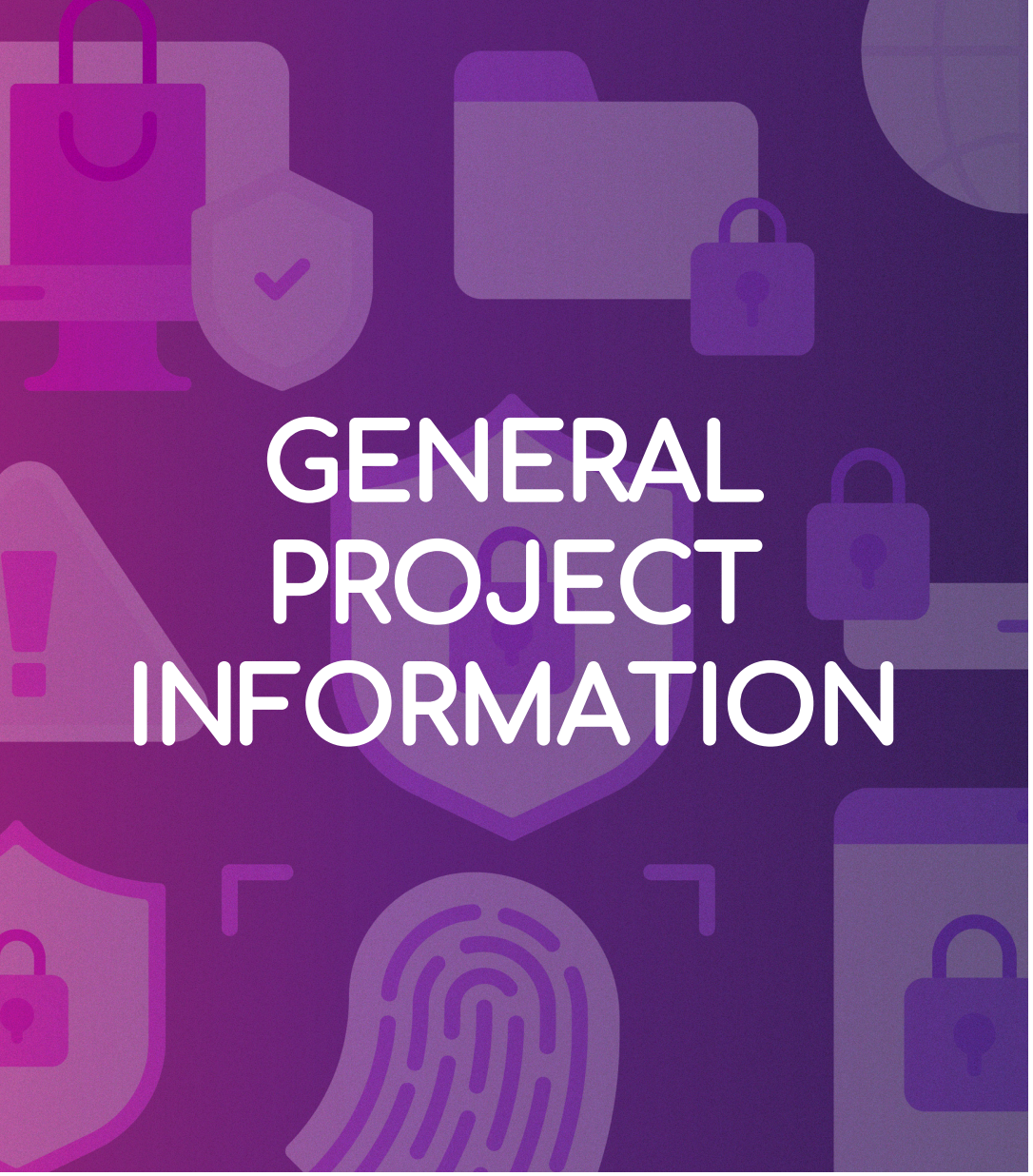
Thanassis Giannetsos

Head of Digital Security & Trusted Computing Group
Ubitech Ltd

Future Proofing Supply Chains

Online, 13/12/201

www.project-assured.eu



GENERAL PROJECT INFORMATION

- **PROJECT REFERENCE:** 952697
- **PROJECT START:** SEPTEMBER 1st, 2021
- **DURATION:** 3 YEARS
- **TOTAL COST/EC CONTRIBUTION:** 5M EUROS
- **14 PARTNERS** FROM **10 DIFFERENT EU COUNTRIES**
- **WEBSITE:** https://www.project-assured.eu/

FUTURE PROOFING OF ICT TRUST CHAINS

SUSTAINABLE OPERATIONAL ASSURANCE AND VERIFICATION REMOTE GUARDS FOR SYSTEMS-OF-SYSTEMS SECURITY AND PRIVACY.

The vision of ASSURED is to design and implement a novel *policy-driven, formally verified, runtime assurance framework in the complex domain of Cyber-Physical System (CPS).*

Motivation & Challenges

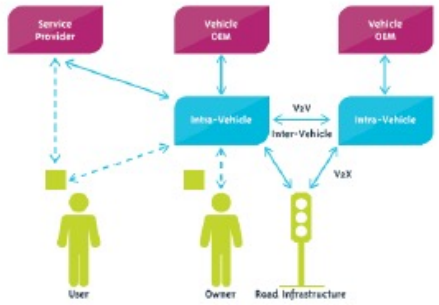
- As the demand for increasingly autonomous CPSs grows, so does the need for **certification mechanisms to ensure their safety**. Current methods towards software and system validation requires exhaustive offline testing of every possible state scenario PRIOR to fielding the system.
- Novel assurance services are needed to ensure that the control output of such controllers does not put the system or people interacting with it in danger
- Especially in safety-critical applications

- **What is needed:**
  - ✓ *Convergence of **security/trust** and **safety***
  - ✓ ***Verification techniques** to allow intelligent controllers to perform within a predetermined envelope of acceptable behavior*
  - ✓ ***Trusted Supply Chains** - Decentralized Roots of Trust*
  - ✓ *Efficient ways for **certifying the correct execution** of heterogeneous devices*
  - ✓ ***Collective Threat Intelligence***
  - ✓ ***Enhanced Data Sharing***

ASSURED

BACKGROUND AND RATIONALE

Securing Supply Chains – Digital Trust



Smart Cities....Autonomous Cars...Intelligent Transportation Systems - Software as core enabler

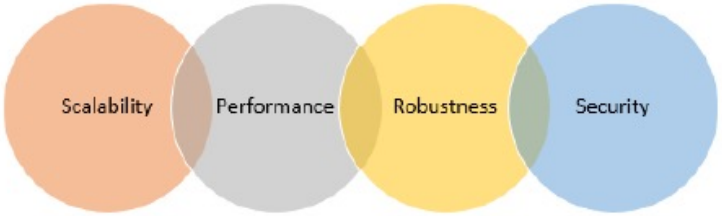
- Security & Operational Assurance in all phases of SDLC life-cycle
  - ✓ **Establishing and maintaining trust** - *from secure production, through distribution in the supply chain, and ending with secure disposal*
- **Device and Data Integrity & Operational Correctness for:**
  - ⇒ Ensuring the trusted execution of connected components
  - ⇒ Safeguarding code updates against tampering
  - ⇒ Ensuring that firmware and software code comply with internal policies
  - ⇒ Protecting against unauthorized and erroneous production runs
- BUT codebase is too large!!

Software eats the world...and what's left is data

- **Impractical to provide secure execution guarantees for the entire codebase**
  - ⇒ No complete & correct definitions for all adversarial behaviors
  - ⇒ No option to control the global attack surface - Current security measures provide targeted defense
  - ⇒ But do we need it? *Partially correct execution even in compromised environments*
- Functional safety (ISO 26262) specifies the need for integrity and trustworthiness of input/output data to/from safety-critical functionalities
  - ✓ Understanding what is reasonable (safety-critical) for an ECU of a certain type to be doing offers most promise in defending in a quantifiable way automotive systems
  - ✓ Identify **safety-critical functions** and **data** as properties and verify their correct execution and/or configuration (during **run-time**)

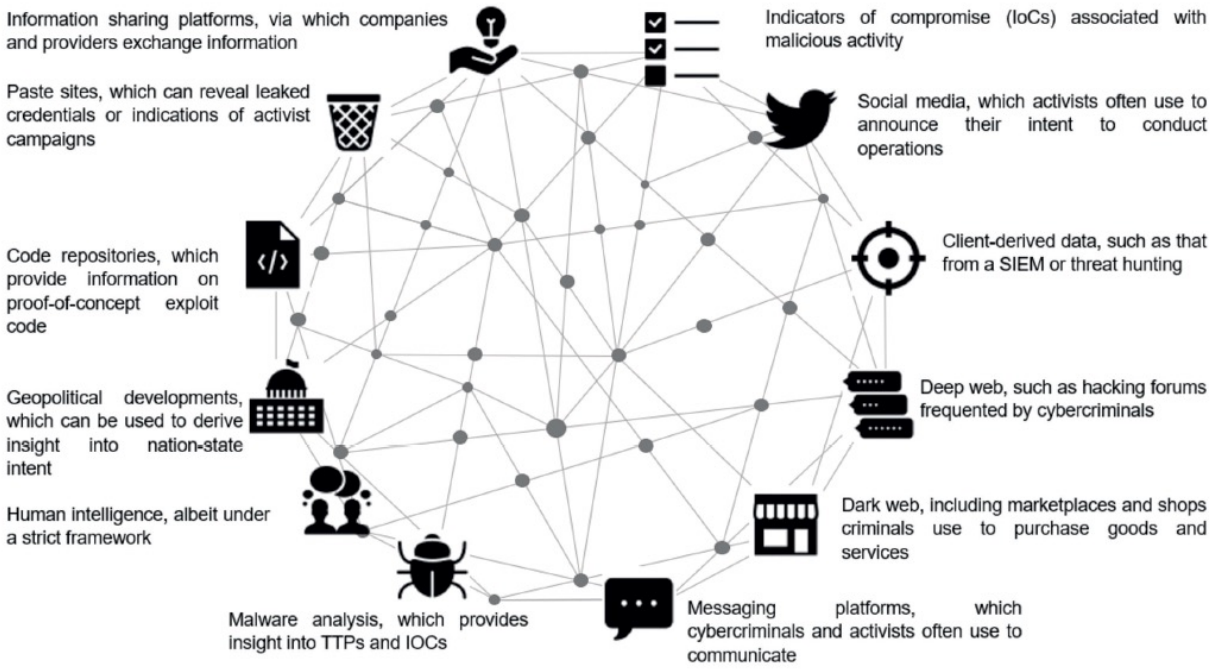
Remote Attestation

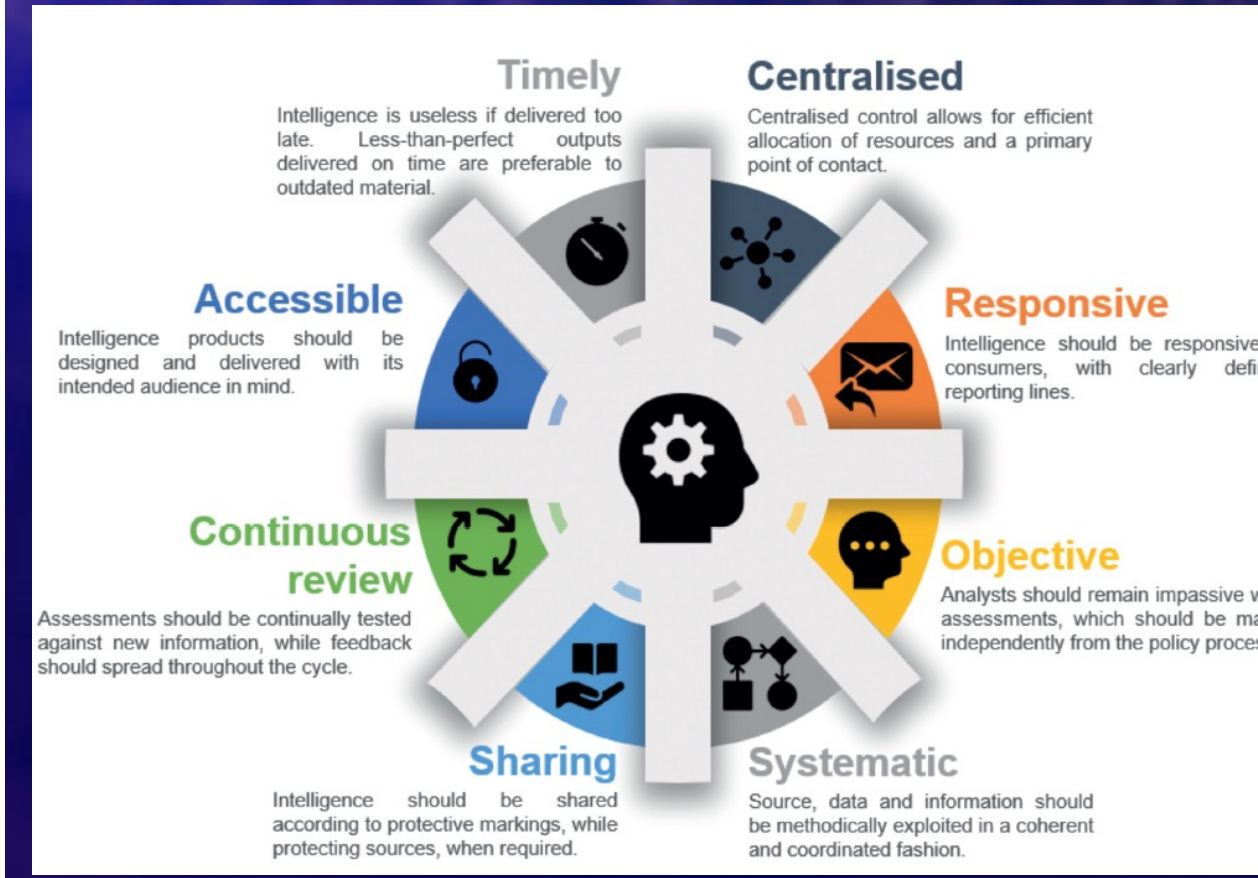
- Remote attestation has been researched for many years
  - ✓ TPM Attestation (2001), Property-based Attestation (2004), Software-based Attestation (2004), Dynamic RoT (2005), PUF-based Attestation (2011), SWARM Attestation (2015), Control-Flow Attestation (2016)
- **Challenges:**
  - ⇒ Not all of them address run-time attacks
  - ⇒ Performance issues when trying to attest the entire control-flow
  - ⇒ Hard assumptions on isolation of software modules and the OS
  - ⇒ Disruptive during the tracing of the control-flow paths
- **Hybrid solution**
  - ✓ Control-Flow Property-based Attestation



Furthermore…Threat Intelligence Sharing

- Different levels of threat intelligence
- Information Sharing
- Use of Blockchain-based Market





ASSURED Vision

ASSURED aims to deliver a novel policy-driven, formally verified, runtime assurance framework in the complex domain of heterogeneous CPSoS. The core idea is to leverage and enhance runtime property-based attestation and verification techniques so as to allow intelligent (unverified) controllers to perform within a predetermined envelope of acceptable behavior, and a risk management approach to extend this to a larger SoS. of protocols and software processes, software attestation, blockchain technology for distributed verification of transactions between system elements and control-flow attestation techniques for enhancing the operational correctness of such devices.

FOR WHO? ASSURED will enable a new mode of certification and verification for mixed-criticality services running at various levels in the overall application stack

WHY? Turn the supply chain into a real-time verified ecosystem governed by attestation policies (through smart contracts) to safeguard the correct state of all assets during the entire lifecycle of operation.

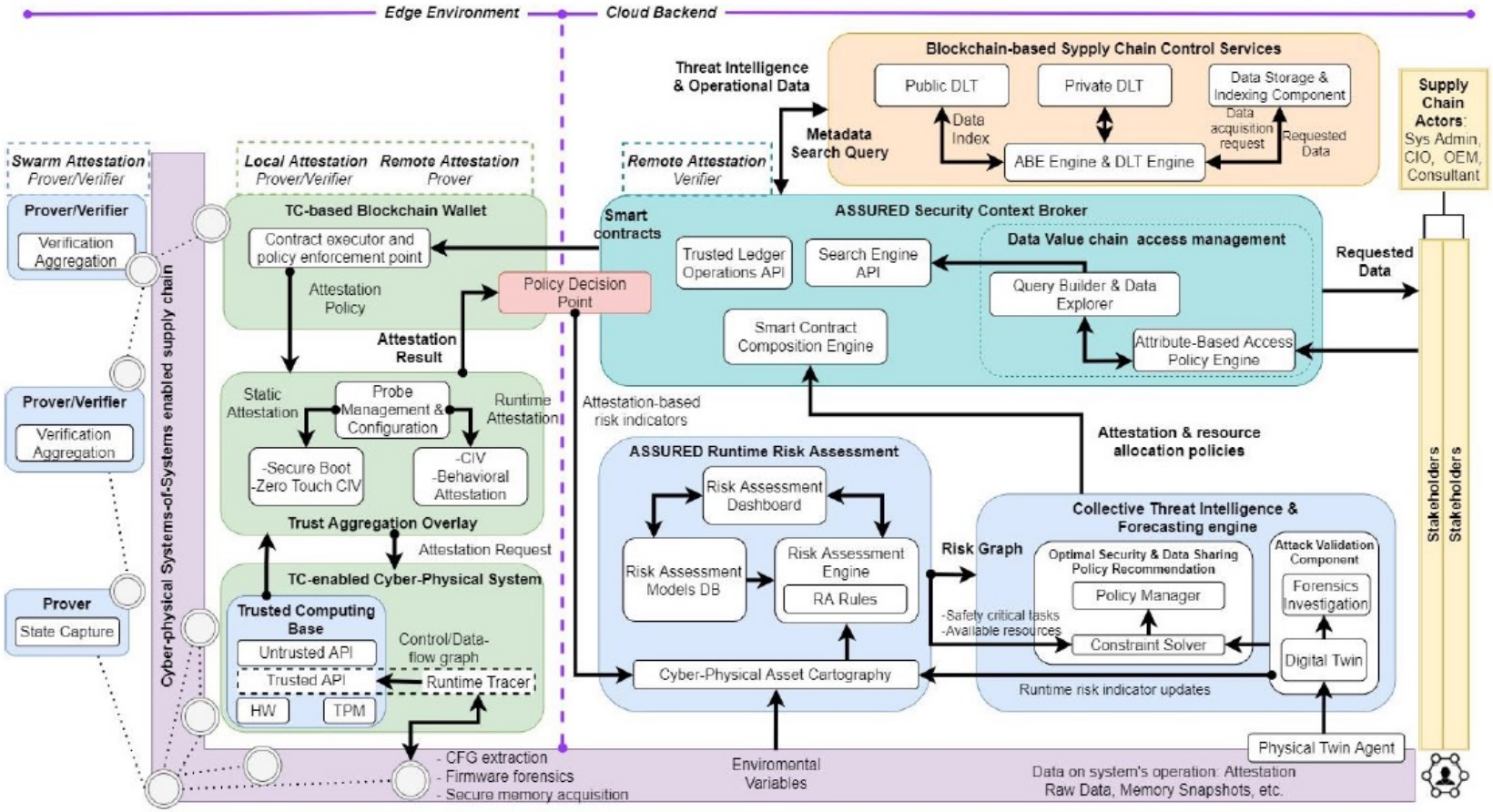
Safeguard also attestation/verification & threat intelligence data sharing.

Key Technological Aspects

- **Main innovations**
  - ✓ Converge security and safety for mixed-criticality services
  - ✓ Risk Assessment & Collective Threat Intelligence
  - ✓ New bundle of novel attestation services
  - ✓ Device Data & Execution Stream Processing and Monitoring
  - ✓ DLTs for certification activities & threat intelligence sharing
  - ✓ Novel Trusted Ledger-based Operations
    - Trusted Authentication, Trust over crypto operations, ABE, SE, PRE
  - ✓ Smart contracts for (ON-CHAIN) policy deployment & (OFF-Chain) enforcement

Reference Architecture

- **Main innovations**
  - ✓ Converge security and safety for mixed-criticality services
  - ✓ New bundle of novel attestation services
  - ✓ Device Data & Execution Stream Processing and Monitoring
  - ✓ DLTs for certification activities & threat intelligence sharing
  - ✓ Novel Trusted Ledger-based Operations
    - Trusted Authentication, Trust over crypto operations, ABE, SE, PRE
  - ✓ Smart contracts for (ON-CHAIN) policy deployment & (OFF-Chain) enforcement



Enhanced operational assurance for supply-chains comprising heterogeneous devices

- Secure Configuration, Deployment, Operation, Management & Maintenance
- New breed of attestation schemes including Control-flow Attestation, Configuration Integrity Verification, Direct Anonymous Attestation (DAA), Jury-based Attestation, Swarm Attestation
- Development of novel **software-based tracing mechanism** for monitoring the state of a remote device
- Managament of attestation policies & results through the use of Blockchain
- Converge **security and safety** for mixed-criticality services

Provision of Run-time Risk Assessment and Vulnerability Analysis Methodologies

- ASSURED will design **risk analysis methods** that target all the phases of a system's development lifecycle, from design time to near real-time quantification of newly identified attacks
- Lead to **optimized set of security (attestation) policies** to be deployed/enforced
  - *Constraint-based Network Learning*
- Through **Blockchain and smart contract** technologies
- **Validation and Verification using formal security analysis**

Threat Intelligence Information Sharing through use of a Blockchain-based Market

- ASSURED will leverage **DLTs for certification activities & threat intelligence sharing**
- Novel trusted ledger operations
  - *Trusted Authentication, Trust over Crypto Operations, Attributed-based Encryption, Searchable Encryption*
  - **TC-based Blockchain Wallet** running at the device
- To be aligned with current trends in SSI standards

PROJECT GOAL #4

Implementation and evaluation of all attestation and tracing schemes

- Demonstrate the applicability of the designed attestation schemes to a wide range of IoT ecosystems
- Implementation and rigorous evaluation of all designed algorithms
  - *Distinct devices and OSes*
  - *Virtualized environments*
  - *Equipped with various Trusted Computing Bases*

Standardization within TCG, ISO/IEC, and ETSI

- Development of standardisation proposals that push the state of the art in the areas of attestation, certification, Blockchain and secure on- and off-chain data management
- Involve the technical committees of the relevant standards bodies, notably **ISO, IEC, ETSI** and the **TCG**

ASSURE

USE CASES

SMART MANUFACTURING

SAFE HUMAN-ROBOT COLLABORATION IN AUTOMATED ASSEMBLY LINES.

ASSURED Framework will be able to perform a quantitative and qualitative analysis of the CPS attacks as well as to provide the essential security mechanisms in order to provide enhanced data integrity and trustworthiness and recognize a manipulation of used CPS components which shall lead to appropriate mitigation steps through the combined use of RA, attestation and trust management.

Focus On Detecting Comrpomised Devices That May Lead To Fatal Accidents On The Manufacturing Floor.

SMART CITIES

SECURE, CROSS-VERTICAL COLLABORATION OF "PLATFORM-OF-PLATFORMS" FOR ENHANCED PUBLIC SAFETY.

ASSURED Framework will use all the runtime risk assessment and auditable security policy enforcement mechanisms (via the use of smart contracts) to allow fast prototyping and enable protection at a device level, and collaboratively prove its nominal functionality to the belonging network.

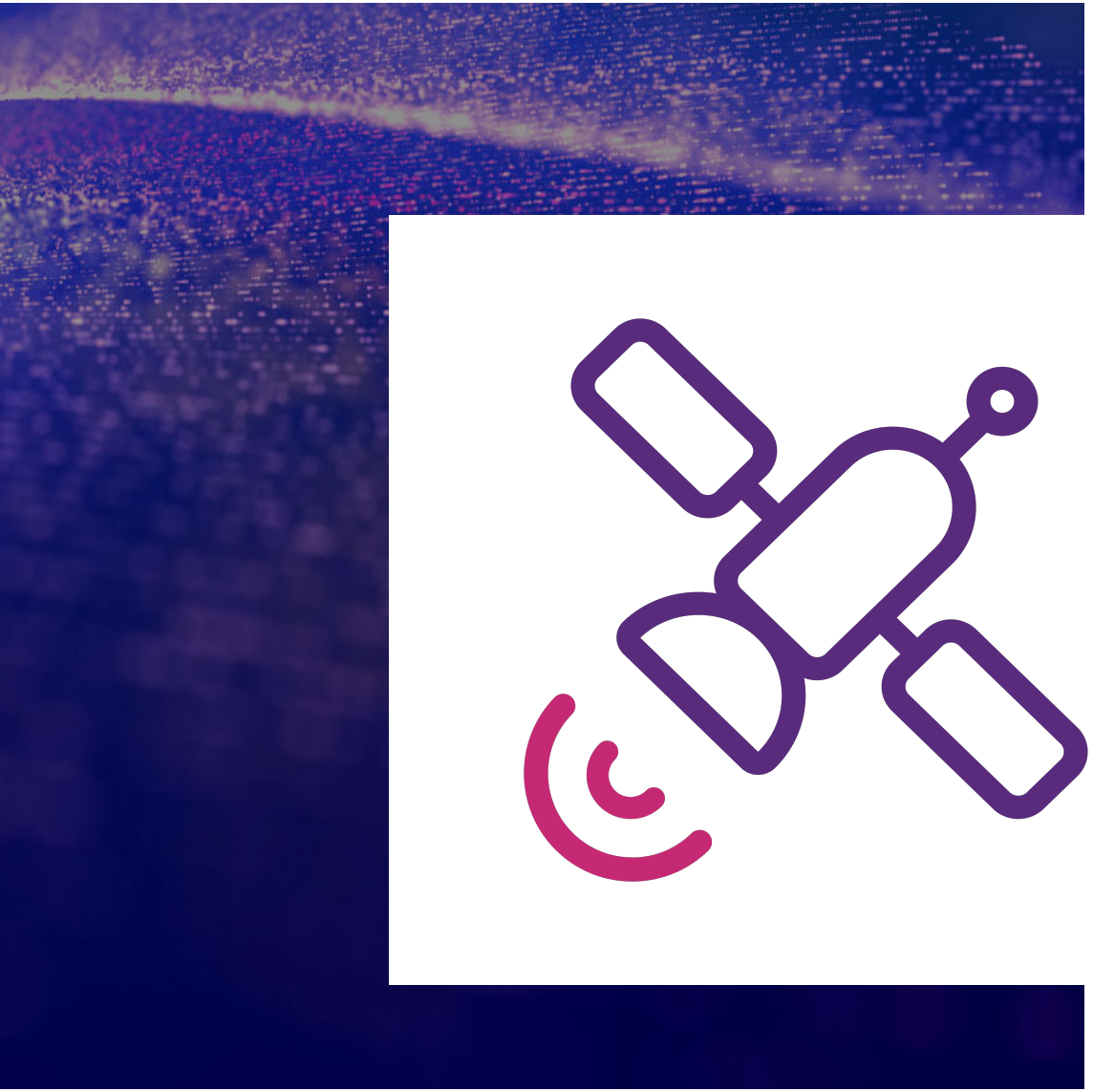
Focus on Secure And Privacy-preserving Data Sharing.

SMART AEROSPACE

AIRCRAFT DEVICE USE-CASE.

ASSURED platform will be used to perform runtime security attestation of (selected) aircraft embedded device (constituent or holistic firmware update, ultra-secure operation mode, new data exchange schemes, new key distribution).

Focus on Operational Assurance Of All Devices Comprising The «Brain» Of An Aircraft



SMART SATELLITE COMMUNICATIONS

DIGITAL SECURITY OF SMART SATELLITE COMMUNICATIONS.

ASSURED will be used to perform runtime attestation of a key distribution application at the level of constellation.

Key distribution is highly crucial for several applications (e.g. surveillance, communication, etc.) utilize application-level and transport-level encryption techniques fortify the confidentiality, integrity and availability of the processed data.

- ASSURED will provide a new generation of **trust assessment and operational assurance mechanisms** for protecting the entire lifecycle of a supply chains
- ASSURED fills the gaps that currently threatens the long-term security properties of CPSoS
- Will enable ASSURED systems to act as **decentralized roots of trust** that can:
  - Securely interact with cloud services and other devices
  - Access corporate services
  - Perform safety-critical operations with verifiable evidence on their correctness
  - Along with a wide range of other services
- Adoption guidelines of such hardware-solutions can benefit not only the industries of interest but also other domains such as **Intelligent Transportation Systems**, **eHealth**, **Industry 4.0**, **Digital Media and Content Protection**, etc.

Where we are now...

ASSURED

I Analyzing the Landscape of Security, Privacy, Trust in SoS Value Chains

WP1

- State-of-play analysis
- Security, Privacy, Trust Consideration
  - Requirements
  - Operational Assurance
- Use case scenarios and requirements consolidation
- Security & Information Process Modelling
  - Attestation Properties
- Security & Threat Intelligence Data Sharing

II Developing the ASSURED Components

WP2 – WP3 – WP4

- Architectural Design
- Development of ASSURED Core Security Services Bundle
  - Runtime Attestation Enablers
  - TC-based Blockchain Control Services
- ASSURED Risk Assessment
  - Collective Threat Intelligence
- ASSURED DLTs
  - Smart Contracts

III Verifying, Validating and Demonstrating the ASSURED Framework

WP5 - WP6

- Verification & Validation framework elaboration
- Integration of the ASSURED Framework
- Technical Verification and Validation
- Demonstrators SetUp
- Demonstrators Implementation
- Impact Assessment & Lessons learnt

IV Warranting Sustainability and Preparing Market Entry

WP7

- Market analysis
- Detailed exploitation strategy
- Impact Assessment
- Business Plan
- Dissemination
- Communication
- Standardization

THE CONSORTIUM

ASSURED

UBITECH ubiquitous solutions

MARTEL innovate

Suite5 We Deliver Intelligence

INTRASOFT INTERNATIONAL

SPACE

United Technologies Research Center

uni systems

BIBA Bremer Institut für Produktion und Logistik

CITY OF ATHENS DAEM

TECHNISCHE UNIVERSITÄT DARMSTADT

TU Delft

DTU

UNIVERSITY OF SURREY

NVIDIA

THANKS

PROJECT-ASSURED.EU

@Project_Assured

ASSURED project is funded by the EU's Horizon2020 programme under Grant Agreement number 952697