OUR USE CASES

Smart Manufacturing:
Safe human-robot-collaboration in automated assembly lines.

Smart Cities
Secure, cross vertical collaboration of “platforms-of-platforms” for enhanced public safety.

Smart Aerospace
To increase the trustworthiness of all internal aircraft components.

Smart Satellites
To secure the communication between all involved entities; protect keys on satellites and ground stations

More details on our use cases are available on www.project-assured.eu

ASSURED is a holistic security solution for providing high Levels of Assurance (LoA) on the correct operation of heterogeneous supply chains, comprising multiple embedded systems of different profiles and resource capabilities, thus, safeguarding the entire lifecycle of various safety-critical application domains.

✉ INFO@PROJECT-ASSURED.EU

@PROJECT_ASSURED

in @ASSURED-PROJECT

SCAN ME WITH YOUR PHONE

FOLLOW US!

ASSURED project is funded by the EU's Horizon 2020 programme under Grant Agreement number 952697.

ASSURED

FUTURE PROOFING OF ICT TRUST CHAINS

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

PROJECT-ASSURED.EU

As the demand for increasingly autonomous **Cyber-Physical Systems (CPSoS)** grows, so does the need for advanced certification mechanisms that can enhance their security posture without compromising their safety.

In ASSURED, we introduce an innovative, formally verified runtime assurance framework for implementing the transition to Zero Trust concept with the principle "***Never Trust, Always Verify***" for assuring vertical trust for all deployed devices of a service graph chain so that:

- **Devices** can provide verifiable evidence on their correct configuration and behavioral profiles prior to establishing trustworthy and secure communication channels between them;
- **Businesses** can achieve security and safety convergence across the entire Edge-Cloud continuum;
- **Service Providers** can benefit from the customizable Trusted Computing Base of ASSURED that can convert their devices into "hardened" security tokens that may also remain secure long-term against an enhanced threat landscape in such decentralized deployments.

WHAT ASSURED SAFEGUARD OFFERS:

- **Enhanced Operational Assurance** for increasing trust to a device output through the implementation **of novel attestation and verification methods as a means of assurance and trusted interoperability** between a wide range of CPSoS. This not only includes integrity of system hardware and software but also includes correctness and integrity of mission critical and/or sensitive data.
- **Dynamic/Runtime Risk Assessment** for identifying those risk dependencies in the overall service graph chains that can affect the most the safety of the system. This, in turn, enables the suggestion of an optimized set of security policies to be enforced.
- **Threat Intelligence Information Sharing** for the secure and auditable sharing of threat intelligence data only to authorized and authenticated devices and users for creating a "threat hygiene marketplace" as well as for advanced certification of the devices' operational profile to be up-to-dated with the latest security patches.
- **Secure Data Sharing** through the implementation of efficient and lightweight crypto primitives that enable the confidentiality and integrity of all exchanged data. This also includes the management of even encrypted data with a high-level of granularity so that only authorized users can have access to such encrypted data; i.e., through ASSURED's Attribute-based Encryption functionalities.
- **Decentralized Identity Management** for ensuring the correctness of each claimed identity of all actors in a supply chain environment as well as the verification of their claimed attributes. ASSURED is aligned with the Self-Sovereign Identity (SSI) concept to ensure secure identification and authentication to access a multitude of services (even offered under different Service providers) under the eIDAS regulation.
- **Safety Zones Detection** in a deployed supply chain for enabling the optimized recommendation of the best of security policies. No consideration of the obsolete "*one policy captures them all*" concept.
- **Open Source Software, Open APIs and Open Data Models** following an open-source implementation road-map for enabling the integration of ASSURED building blocks in a multitude of diverse supply chain ecosystems.