Ecossian

European Control System Security Incident Analysis Network

MISSION

The mission of ECOSSIAN is to **improve** the **detection** and management of highly sophisticated **cyber security incidents** and attacks against critical infrastructures by implementing a pan-European **early warning** and situational awareness framework with command and **control facilities**.

MOTIVATION

The **protection** of **Critical Infrastructure** (CI) increasingly demands solutions which support incident detection and management at the levels of individual CI, across CIs which are depending on each other, and **across borders**. An approach is required which really integrates functionalities across all these levels. Cooperation of privately operated CIs and public bodies (governments and EU) is difficult but mandatory.

After more than 10 years of analysis and research on partial effects in CI Protection (CIP) and for individual infrastructure sectors, ECOSSIAN is a European attempt to develop this holistic system.

One goal is a **prototype** which facilitates preventive functions like **threat monitoring**, early indicator and real threat **detection**, **alerting**, support of threat **mitigation** and disaster management. The factors of societal perception and appreciation, the existing and required legal framework, questions of information security and implications on privacy will be analyzed, assessed and regarded in the concept.

OBJECTIVES

The European economy and the welfare of its citizens require that the **European Critical Infrastructures function properly**. To address this issue the ECOSSIAN project contributes to the

- European Programme for Critical Infrastructure Protection (EPCIP)
- Strategy and Action Plan development by the European Commission
- Worldwide Initiatives on Cyber Security of Industrial Control System and Smart Grids followed by ENISA and member states.

ECOSSIAN will establish a working and exchange relation to the Security and Defence Agenda, who has already produced useful guidelines on how to **improve Europe‘s CIP**.

THE ECOSSIAN PROJECT AIMS TO:

- **Establish** and enhance a **security-state awareness** to support operators of CI by implementing an Operator Security Operation Centre (O-SOC);
- Combine O-SOCs of Member States’ identified and designated CI in a National Security Operation Centre (N-SOC);
- **Improve** the effectiveness of **decision-making** and incident response capabilities in Member States through real-time situational awareness, information sharing and command & control opportunities;
- Support a pan-European **early-warning** entity through the connection of Member States N-SOC to a European Security Operation Centre (E-SOC), including the required interoperability standards;
- Enable consistent and collaborative **cross-border** and cross-sectorial **incident management** for CI by utilizing E-SOC capabilities;
- Build **trusted relationships** and engage the CI operators at the EU level;
- Ensure trustworthiness, **anonymity, privacy** and **legality** of action for all stakeholders and end users as necessary;
- Perform a full-scale **demonstration** of the implemented ECOSSIAN framework and system;
- Build an entry point for EU-US collaborative information sharing efforts in cyber defence to create readiness to react on a global basis.

TECHNICAL APPROACH

WP1 “Stock-taking, Requirements & Specification, Architecture Design” reviews the state-of-the-art of CI security provisions, defines suitable use case scenarios and evaluates the main gaps not adequately addressed by currently available SOC technologies. Further goals are the drawing of the ECOSSIAN platform and monitoring of basic security methodological aspects.

WP2 “Threat Detection Module” deals with research and development in extending current state-of-the-art techniques and methodologies. The focus is on identifying indicators and artefacts of cyber-attacks in real-time to be able to trigger alarms in a timely manner.

WP3 “Analysis, Aggregation, Correlation and Visualisation” focuses on the analysis of collected data and their aggregation and correlation in order to generate a higher level view on systems and services of CI providers. A further objective is the proper visualization of gathered information suitable for decision makers.

WP4 “Threat Mitigation and Incident Management” deals with research and development of novel approaches for better handling of threats and realized risks to CI. Also, a forensic tool is planned and implemented in the WP.

WP5 “Integration, Preparation of Demonstration and Evaluation” targets the integration of all the components developed in the project, including testing and validation of the ECOSSIAN approach. Final objective for this WP is to prepare the system for the demonstration activities.

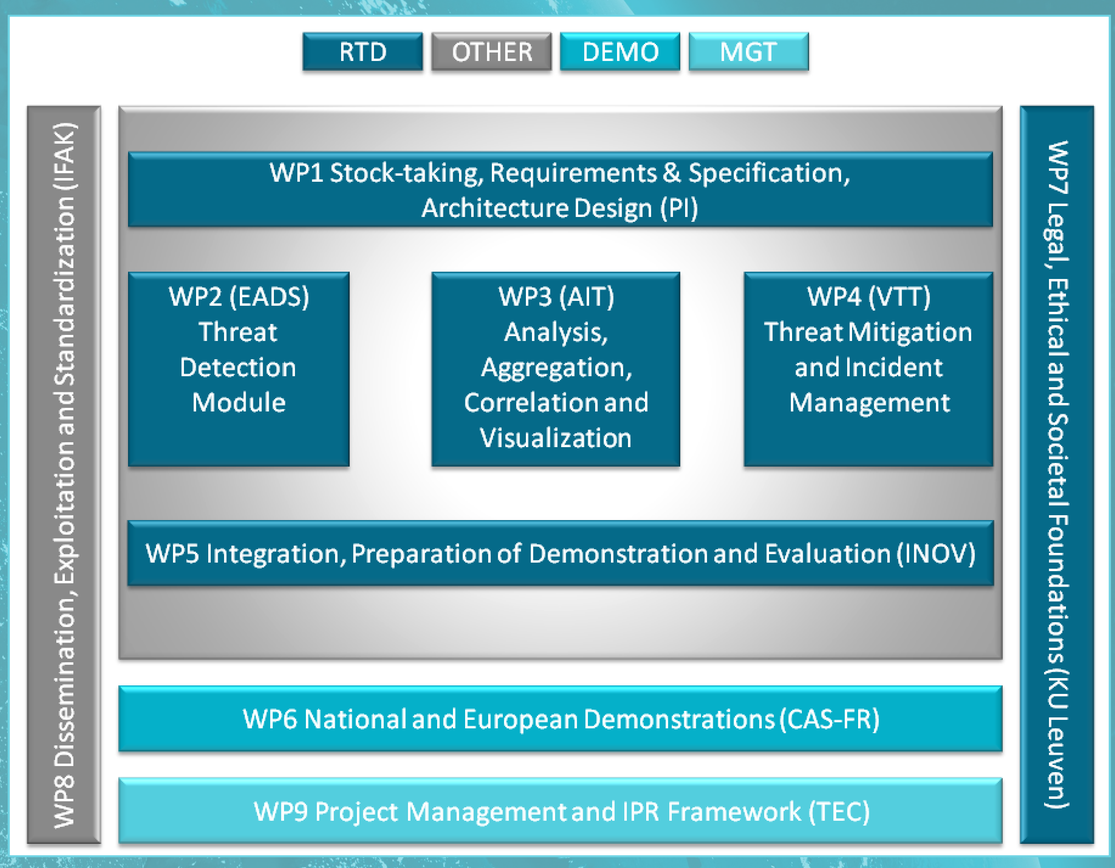
WP6 “National and European Demonstration” proves how the ECOSSIAN system can be used and how information will be shared between CIs and governmental stakeholders.

WP7 “Legal, Ethical and Social Foundations” focuses on legal and business aspects of the crisis prevention and management. Its goal is to ensure that the developed system is compliant with the legal framework in the areas of privacy, data protection and information sharing

WP8 “Dissemination, Exploitation and Standardisation” focuses on the transfer of knowledge developed in ECOSSIAN to industrial communities, academia and the general public as well as on the exploitation of results and on identifying project outcomes to be passed to standardisation working groups.

WP9 “Project Management an IPR Framework” deals with the overall legal, ethical, financial and administrative management as well as the maintenance of the consortium agreement and IPR protection.

In order to maximise the efficiency of such a complex project, the work performed in the framework of ECOSSIAN is organised in **nine different work packages** with significant dependencies and expected synergies among them.



Coordinator:

Dr. Klaus-Michael Koch
Technikon Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a
A-9500 Villach
Tel.: +43 4242 233 55 - 71
Fax: +43 4242 233 55 - 77
E-Mail: coordination@ecossian.eu
Web: www.ecossian.eu

Project Partners:

Project number: 607577
Project start: 1st June, 2014
Project duration: 3 years
Total costs: EUR 13.196.720,61
EC contribution: EUR 9.224.459,00

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no [607577].