

Newsletter

March 2015 - Issue 2



Mission Statement

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

ECOSSIAN on the web - www.ecossian.eu

Apart from general **ECOSSIAN** project information, related news, like upcoming meetings and conferences, as well as ECOSSIAN scientific publications and other dissemination material can be found on our **project website**. In addition to that, all public deliverables will be uploaded and made accessible on our project website after official approval by the European Commission.

In this Issue

- Mission Statement
- ECOSSIAN on the web
- Motivation behind ECOSSIAN
- Past and upcoming Meetings & Events
- Work in progress
- Scientific Publications
- Upcoming & Submitted Public Deliverables
- Outlook

Motivation behind the ECOSSIAN Project

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 that really integrates functionalities across all these levels. Cooperation of privately operated CIs and public bodies (governments and EU) is difficult but mandatory. ECOSSIAN is a European attempt to develop a holistic system addressing these challenges. One goal is a prototype facilitating preventive functions like threat monitoring, early indicator and real threat detection, alerting, support of threat mitigation and disaster management. The system will be tested, demonstrated and evaluated in realistic use cases that are defined on a high level. An international rail network use case, a cyber-terrorism use case, a gas-network use case, and an ICT use case are existing examples and are being used as a starting point. End users, such as Rede Ferroviaria Nacional (REFER), Bord Gais Eireann (GAIS) and Poste Italiane (PI), contribute to the use case definition according to their experiences. Demonstrations, based on scenarios defined, will be performed and show the capabilities of the integrated system deployed in realistic operational contexts.

Technical Meeting Rome/ITALY

From 12th–14th November 2014, the ECOSSIAN Consortium met for a technical meeting in Rome, hosted by partner Poste Italiane (PI). Main topics of this face-2-face meeting were the discussion of the technical status of the project, especially the progress of WP1. As three technical work packages started in Mo6, the meeting was a great opportunity to kick-off WP2, WP3 and WP4. Furthermore, it was ensured that all partners have a common understanding of the overarching project goal and strong commitment for the “guiding European use cases”. Besides the technical discussions, also management related issues were handled during the meeting.

Upcoming Meetings & Events:

- **COBIT Conference**
14th - 15th March, Orlando/USA
- **ICIT 2015 - IEEE International Conference on Industrial Technology**
17th - 19th March, Sevilla/SPAIN
- **ICMIE 2015 - 4th International Conference on Manufacturing and Industrial Engineering**
21st - 23rd March, Singapore/ASIA
- **Technical Meeting**
26th - 27th March, Lisbon, PORTUGAL
- **Workshop & Technical Meeting**
19th - 21st May, Ottobrunn, GERMANY

Key Data:

Start Date:	1 June 2014
End Date:	31 May 2017
Duration:	36 months
Project Reference:	607577
Project Costs:	€ 13.196.720,61
Project Funding:	€ 9.224.459,00

Consortium:

Project Coordinator:

Technical Leader:

Project Website:

19 partners (9 countries)

Dr. Klaus-Michael Koch
coordination@ecossian.eu

Mag. Helmut Kaufmann, MSc
helmut.kaufmann@airbus.com

www.ecossian.eu



FOLLOW US ON **Twitter**

https://twitter.com/FP7_ECROSSIAN

Work progress in ECOSSIAN

The ECOSSIAN project has started successfully and the ongoing work is well on track. Collaboration among partners has harmonized and is functioning well, supported by a well-established IT and communication infrastructure. A project website and information platform was set up and dissemination materials, such as project leaflets, a poster and a roll-up have been created. In **WP1 "Stock-taking, Requirements & Specification, Architecture Design"** the state of the art of CI security provision has been reviewed in order to provide a global understanding of the current means available to detect and manage security problems. Further, partners are drafting the use cases and demonstration scenarios and are about finalizing the development of requirements. Simultaneously, work on the design of the overall architecture as well as the gap analysis of security technologies is carried out. **WP2 "Threat Detection Module"** was kicked-off during the technical meeting in Rome and initial work on real time monitoring and incident & attack detection has already started. In **WP3 "Analysis, Aggregation, Correlation and Visualization"** partners have started with the evaluation and extension of data collection mechanisms. A face-2-face meeting is scheduled in February, where partners will discuss single building blocks, their interconnections, and the integration in the overall ECOSSIAN theme. Part of **WP4 "Threat Mitigation and Incident Management"** is the design and implementation of facilities to produce and store unforgeable evidence of security breaches. Work towards measures for prevention of CI incidents is about to start. **WP7 "Legal, Ethical and Social Foundations"** is focused on the analysis of the applicable legal framework as well as on legal requirements. At the moment a thorough analysis on the sector business, procedural and entrepreneurial legal frameworks is being conducted in order to identify opportunities, obstacles and possible models for inter-sectorial cooperation.

Scientific Publications

Semi-Synthetic Data Set Generation for Security Software Evaluation

F. Skopik, G. Settanni, R. Fiedler, I. Friedberg, in proceedings of the International Conference on Privacy, Security and Trust, IEEE, 2014

Combating Advanced Persistent Threats: From Network Event Correlation to Incident Detection

I. Friedberg, F. Skopik, G. Settanni, R. Fiedler, in Elsevier Computer and Security, Elsevier, 2014

Outlook

The ECOSSIAN team is confident that the successful project start as well as the satisfactory work progress will continue to exist also in the upcoming project periods. One of the main objectives in the following months will be the finalization of the requirements definition. The design of new functionalities, including legal requirements, technological and technical aspects and organizational needs will be finished and the use cases and demonstration scenarios will be defined. Another focus during the upcoming months will be on the gap analysis of security technologies and procedures, as well as on the development of an overarching architectural framework.

During the next technical meeting in March, hosted by partner Policia Judiciaria (PJ) in Lisbon, **WP 5 "Integration, Preparation of Demonstration and Evaluation"** will be kicked-off. This WP is about integrating the components developed within the project and validating the ECOSSIAN approach. Moreover, the system will be deployed within realistic environments and prepared for the demonstration activities.

Public Deliverables submitted

- D1.2 "Requirements Report"
- D7.1 "Analysis of the applicable legal framework"
- D7.2 "Legal Requirements"
- MS1 "Requirements identified"

Upcoming Public Deliverables

- D7.3 "Information sharing policies in disaster situations—Version 1"

Upcoming Public Milestones

- MS2 "Use cases defined"
- MS3 "Workshop 1 successfully took place"

Key Data:

Start Date:	1 June 2014
End Date:	31 May 2017
Duration:	36 months
Project Reference:	607577
Project Costs:	€ 13.196.720,61
Project Funding:	€ 9.224.459,00

Consortium:

Project Coordinator:

Technical Leader:

Project Website:

19 partners (9 countries)
Dr. Klaus-Michael Koch
coordination@ecossian.eu
Mag. Helmut Kaufmann, MSc
helmut.kaufmann@airbus.com
www.ecossian.eu