Publishable Summary

Project number:	607577
Project acronym:	ECOSSIAN
Project title:	ECOSSIAN: European Control System Security Incident Analysis Network
Start date of the project:	1st June, 2014
Duration:	36 months
Programme:	FP7/2007-2013

Date of the reference Annex I:	27.03.2014
Periodic report:	Publishable summary (as part of the 1st periodic report according to EC regulations of the model contract)
Period covered:	01.06.2014 – 31.05.2015
Work packages contributing:	All
Due date:	May 2015 – M12
Actual submission date:	20.08.2015 (V2)

Project Coordinator:	Dr. Klaus-Michael Koch Technikon Forschungs- und Planungsgesellschaft mbH (TEC)
Tel:	+43 4242 233 55 00
Fax:	+43 4242 233 55 77
E-Mail:	coordination@ecossian.eu
Project website:	www.ecossian.eu

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement n° 607577.

Chapter 1 Publishable Summary

Project name: ECOSSIAN
Grant Agreement: 607577
Project website: http://www.ecossian.eu/
Contact: coordination@ecossian.eu

Start date: 1st June 2014
Duration: 36 months

1.1 Project context and main objectives

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

The ECOSSIAN Project aims to:

- Implement an Operator Security Operation Centre (O-SOC) in order to enhance a security-state awareness to support operators of CI.
- 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.
- Connect Member States N-SOC to a European Security Operation Centre (E-SOC); enable collaborative cross-border and cross-sectorial incident management for CI.
- Improve the effectiveness of decision-making and incident response capabilities in Member States.
- Connect Member States N-SOC to a European Security Operation Centre (E-SOC).
- Accomplish a full-scale demonstration of the implemented ECOSSIAN framework and system.
- 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.
- Create an entry point for EU-US collaborative in cyber defense.

Motivation:

The protection of CI increasingly demands solutions which support incident detection and management at the levels of individual CI, among dependent CL, and across borders. The required approach ought to integrate functionalities across all these levels. Collaboration of privately operated CLs and public bodies, such as governments and EU is difficult but mandatory.

In the wake of 10 years of analysis and research on partial effects in CI Protection (CIP) and for individual infrastructure sectors, ECOSSIAN was created to develop this holistic area. One of the key developments is a prototype, facilitating preventive functions like threat monitoring, early indicator and real treat detection, alerting, support of threat mitigation and disaster management. The concept of the project contains analysis, assessment and consideration of societal perception and appreciation, the existing and required legal framework, questions of information security and implications on privacy.

Objectives & Technical Approach:

ECOSSIAN aims to improve the safety of the cyber security via implementation a pan-European early warning and situational conversance framework with command and entity management. In order to achieve its overall goal, the project has a number of important objectives. The tree main objectives are:

- European Programme for Critical Infrastructure Protection (EPCIP).
- Strategy and Action Plan developed by the European Commission.
- Worldwide Initiatives on Cyber Security of Industrial Control Systems and Smart Grids followed by ENISA and Member States.

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

1.2 Work performed and main results achieved

A review/assessment of the CI SOTA, with respect to the EU legislative framework, stakeholders, technologies and procedures related to SOCs and CERTs, organisational aspects, secure technologies, best practices for secure information sharing built the basis for the project. Based on the information provided by operators of CIs, scenarios have been defined within the energy, finance and transportation sectors. Activities led to the identification of architecture requirements, organisational needs and main functionalities. A gap analysis was carried out, aiming to identify requirements that are already fulfilled by current technologies, shortages in SOTA solutions as well as areas where major effort is needed. Further the architecture general framework and main components were outlined. This result will pave the way for the architecture further development. A preliminary identification of risk assessment methodologies was achieved to be exploited for ECOSSIAN risk analysis.

Required needs and the expectations from a technical perspective were identified in order to cover most of the requirements and use cases/scenarios.

A detailed understanding of how to handle incident reports in an N-SOC, delivered by single organizational O-SOCs, has been established. A better understanding about the functional building blocks, information flows, information and data types, as well as interfaces between them, was developed. Further steps included the creation of a preliminary architectural sketch and mapping of the functional blocks of the architecture were performed.

It was started to develop a forensics toolset prototype by collecting tools that can be utilised in forensics investigations and a proposed design for the prototype tool. The partners worked on a continuity plan for the ECOSSIAN system, especially from the business continuity perspective. The continuity deliverable and the deliverable concerning mitigation procedures of both the ECOSSIAN system and CIs in general, has been started by creating common visions of the topics. Analyses the impacts of incidents for CIs in different sectors has started and some applicable models and frameworks for interdependency modelling have been defined.

To integrate the specified and developed components, it was started to analyse the current status of the architecture. Information regarding all technical components that will require integration were collected. The data collected regarding available components, information regarding technologies and interfaces was documented to setup the integration plan and environment. Demonstration scenarios definition has started to detail the use cases. A storyboard expert group was set up to discuss the refined attack scenarios.

Furthermore, the legal and ethical requirements were identified. In addition, ground work and data gathering has been focused. Analysis of existing protocols for public-private partnerships started. The initial analysis was provided and recommendations for the adoption of the Quality Criteria Catalogue from the ValueSec project were made. This involved the verification of the possibility of its use in the project and its adaptability.

A robust IT infrastructure (e.g. www.ecossian.eu, SVN repository, mailing lists) has been established and maintained. ECOSSIAN has been advertised by e.g. web pages, press releases, flyers, newsletters and is also visible on Twitter and LinkedIn. All dissemination activities are announced via http://www.ecossian.eu/news.

The overall project management covers all management components on contractual, financial, legal, technical, administrative and ethical topics. Some main tasks are organising meetings and conf calls, monitoring the work plan/progress and acting as help desk for partners in everyday issues.

Finally the planning of the tasks/deliverables is well on track. All currently started WPs produced altogether 16 Deliverables.

1.3 Expected final results and their potential impact

ECOSSIAN will differ to previously and currently running projects by building up on the results and approaches of these projects by developing a holistic, integrated and user friendly early warning system for all stakeholders on operator, Member State and European side while complying to legal and regulatory requirements. The exchange of data and the sharing of information are commonly understood to improve the attack mitigation or resistance by combining forces. This is a prerequisite for situational awareness cross borders. The ECOSSIAN system explicitly includes a pan-European layer in the E-SOC that connects the national SOCs at the European level; by providing a common situational awareness this will enable the collaboration of all relevant stakeholders in Member States and Associated Countries. The layered approach in the ECOSSIAN architecture improves reaction speed by enabling a first (preliminary) response already on O-SOC level, thus avoiding delays due to more complex decision making on N-SOC or E-SOC level, nevertheless also providing capabilities for consistent and integral response. The basic incident detection technologies developed in the project as well as the analysis, aggregation and correlation methods will enable an improved and more accurate threat detection considering the information shared by all collaborating parties. This provides the capability for an adequate early-warning system. Legal, social and economic aspects will inherently be considered in the ECOSSIAN architecture, the development of threat detection methods, information sharing and exploitation capabilities as well as the design of threat mitigation and incident management components. A full-scale demonstration of the platform is dedicated to the execution of full-scale demonstrations on national and European levels. The necessary preparations and the evaluation of demonstrations will be performed as well.
We can summarize the expected impacts areas as follows:

- Facilitate the **emergence of common European solutions in CIP**
- Develop a **secure cyber environment in CI sectors** other than ICT in Europe
- Facilitate the **emergence of new cyber security interoperability standards**