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:	02.06.2016
Periodic report:	Publishable summary (as part of the 3rd periodic report according to EC regulations of the model contract)
Period covered:	01.06.2016 – 31.05.2017
Work packages contributing:	All
Due date:	May 2017 – M36
Actual submission date:	30.06.2016

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

Starting with a first SOTA analysis 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. This work was particularized by a gap analysis and concluded in a detailed requirements and scenario definition and the identification of sensors and components for monitoring and attack detection to be developed. Additionally, risk assessment methodologies we identified and analysed, carrying out a final selection of standards and methodologies most suitable for ECOSSIAN project. In addition, a SOC-design for all SOC level was introduced, including different participation levels for the CI operator.

Having analysed functional building blocks, information flows, data types and interfaces as well as understood the handling of incident reports inside the N-SOC, the system components for incident information collection, sharing, analysis, evaluation and visualization were developed and tested and necessary interfaces for the integration defined.

In addition to the development of a forensic toolset prototype, the secure data storage component was implemented. Realistic mitigation actions for national and European level were identified and discussed in External Stakeholder meetings.

A Business Impact Analysis was made for an example group of ECOSSIAN components to identify critical ECOSSIAN processes supporting activities regarding analysis of Business Continuity Planning (BCP) and Business Continuity Management Systems (BCMS) methodologies.

Every identified and developed components were first integrated into the ECOSSIAN integration network (EIN) to test the required interfaces between them. Demonstration scenarios were detailed enriched by support materials and demonstration speeches resulting in the definition of three national demonstrations and a Pan-European demonstration supported which were prepared and executed to show the capabilities of the integrated ECOSSIAN framework at operational, national and European levels.

The ECOSSIAN system was evaluated by analysing and testing the coverage of the defined functional and non-functional requirements, the questionnaires filled by external participants of each of the demonstrations and an evaluation including a selection of ethical, economical, legal, political, and societal (EELPS) criteria that are relevant when a complex system such as ECOSSIAN would be implemented in real operation. This evaluation concluded into several recommendations focussing on functional, technological and usability improvements.

Furthermore, legal and ethical requirements were identified, and protocols for public-private partnerships identified and analysed. Recommendations for the adoption of the Quality Criteria Catalogue are made and evaluated. In addition, special focus was set to ongoing legislative changes, such as the General Data Protection Regulation, the LE Directive and the draft NIS Directive.

The established robust IT infrastructure, support material such as web-pages, press releases, flyers, newsletters and presentations and social media presence (Twitter, LinkedIn) were established and maintained. Strategic and common exploitation plan as well as the standardization plans are developed on how to utilize research outputs coming from the ECOSSIAN project. Several internal and external (stakeholders) workshop along with numerous scientific publication attendances to conferences etc. strengthen the ECOSSIAN public/scientific perception.

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

Finally, all WPs produced altogether more than 50 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 was dedicated to the execution of full-scale demonstrations on national and European levels. The necessary preparations and the evaluation of demonstrations are 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**