Ecossian

European Control System Security Incident Analysis Network

ECOSSIAN – Irish demonstration

Cork, March 1st 2017

Gas Networks Ireland

ECOSSIAN FP7 PROJECT:

Protection of Critical Gas Infrastructures against Cyber-attacks

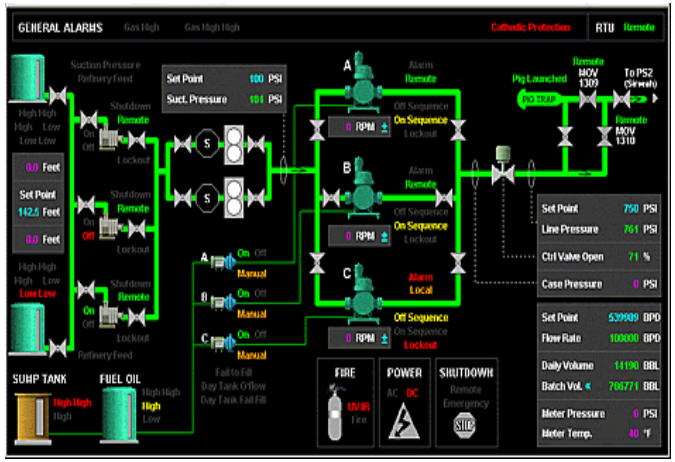
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

Cork, March 1st 2017

European Control System Security Incident Analysis Network

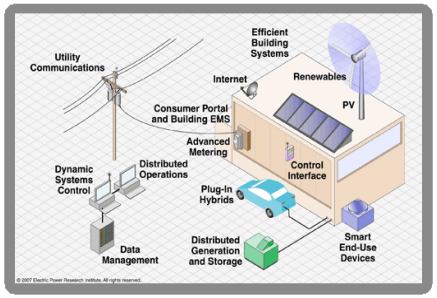
Background

- Modern Society **strongly relies** on reliable and continuous availability of **critical infrastructures** and their services
  - A **serious disruption** of such services could lead to risk for safety of life and economic welfare
  - Critical infrastructures are more and more **in focus of attacks** out of the cyber-space
    - Terrorists
    - Governments
    - Competitor/industrial espionage
    - Cyber criminals and …



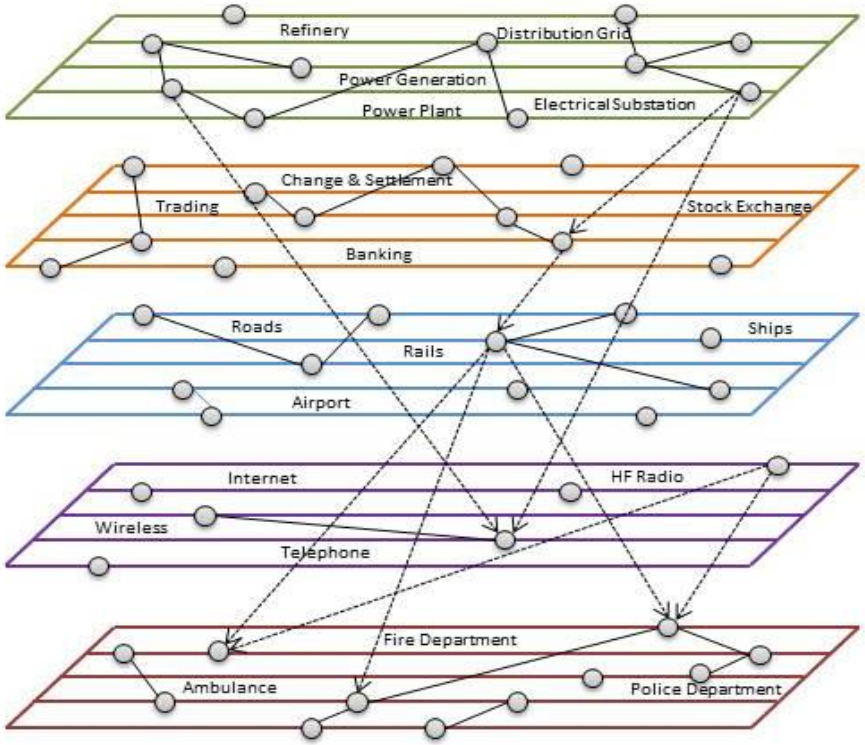
Motivation

- Attack surface to critical infrastructures is continuously growing because:
  - **Deployment of COTS-products**
  - Change from proprietary protocols and products to common technologies coming from the pure IT world“
  - Losing the „Air-Gaps“ through convergence
  - **More and more use of mobile devices and services**
  - **Very long Life-Cycle of plants (10-25 years)**
  - **Security capabilities of used technologies is 5 to 10 years behind enterprise IT**
  - Common cyber-security approach is only very limited applicable in systems with these special needs e.g. real time response



Motivation

- Interdependencies between critical infrastructure (CI)



Energy, Oil & Gas

Finance

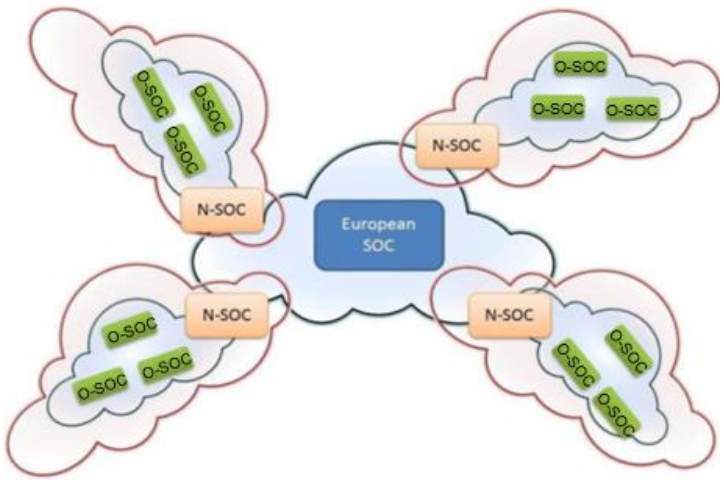
Transportation

Information & Telecom

Emergency Services

Project goals

- Development of a cross-border European early warning system for critical infrastructures
- Three tiers of collaborative, interconnected Secure Operation Centres (SOCs)
  - **Local/sub-state SOC (O-SOC)** early detection and data collection with aggregation
  - **National SOC (N-SOC)** Situational Awareness using aggregated and correlated data



  - **Transnational SOC with command and control capabilities with inclusion of member state SOCs (E-SOC)** Transnational Situational Awareness and coordinated and consistent crisis management

Project goals summary

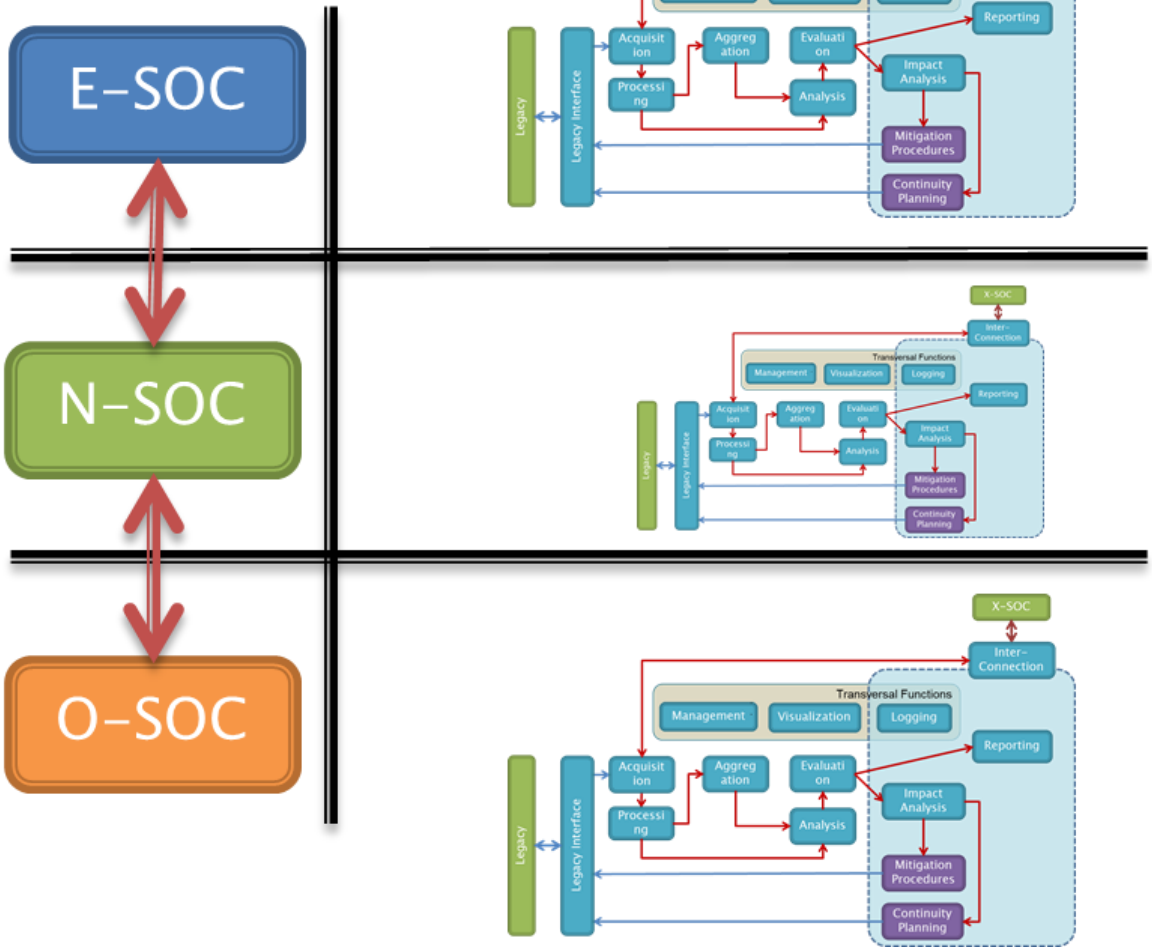
A layered system architecture for a pan-European

cooperative threat management, early-warning and situational awareness:

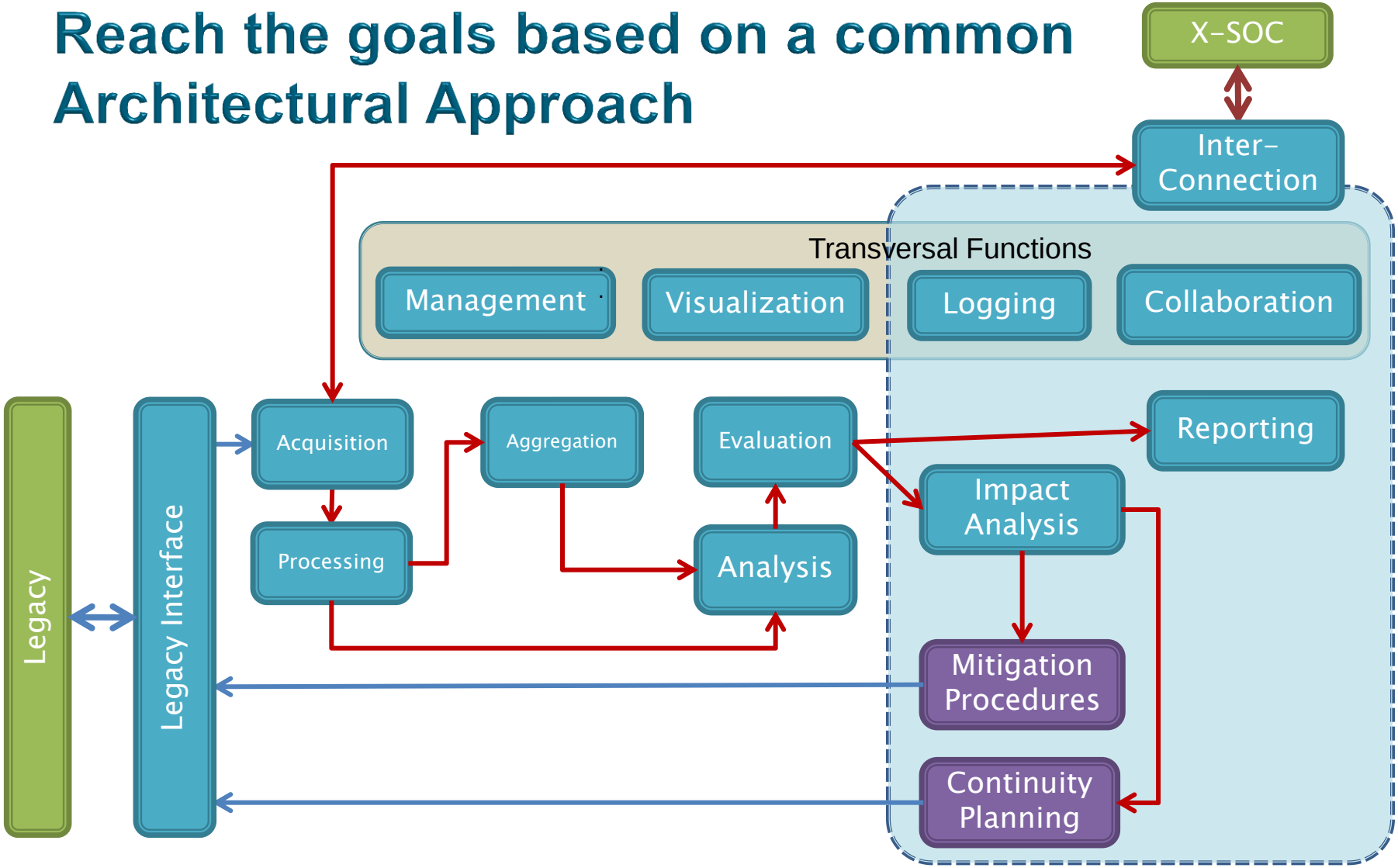
- Cross-country and cross-sectorial collaboration
- Anonymity and privacy (confidentiality) preserving for all joining members
- Secure information sharing and collaboration platform compliant to legal and other regulatory requirements
- Near-real-time detection of attacks
- Technologies and processes for monitoring and threat/incident detection
- Data analysis, aggregation, correlation and visualization
- Threat mitigation, impact analysis, interdependencies and incident management
- Evaluation of the regulatory, social and economic boundary conditions
- **Full-scale demonstration** of the integrated ECOSSIAN system on all levels (O-SOC, N-SOC, E-SOC)

Architectural Approach

- Same architecture at each SOC level, but
- Detailed implementations and technologies may differ

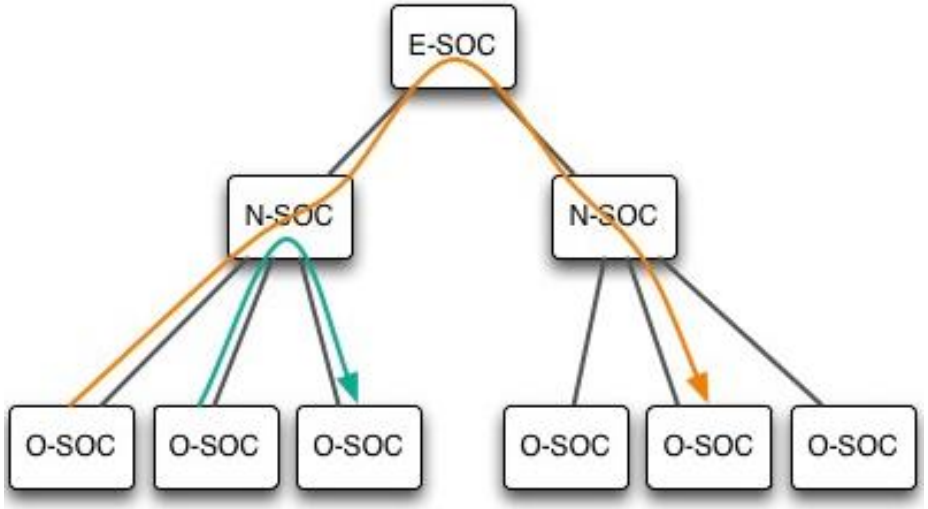


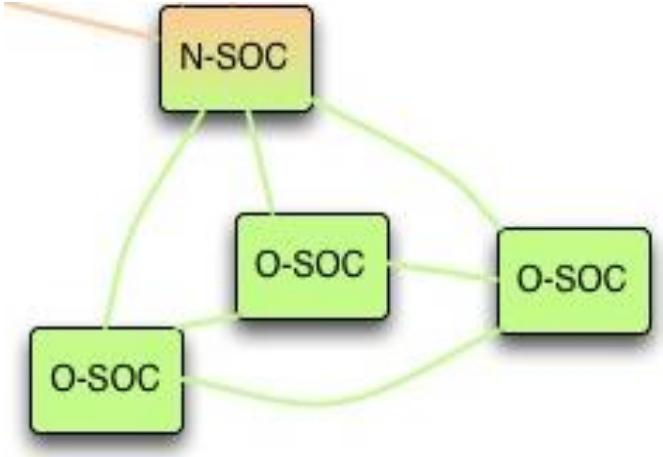
Reach the goals based on a common Architectural Approach



Information sharing

- Definition of a tailored **hybrid <u>voluntary</u> sharing model**, combining hierarchical and P2P sharing models
  - O-SOC ←→N-SOCs ←→ E-SOC: **Hub-and-Spokes**
  - O-SOC ←→ O-SOC: **Peer to peer**





Consortium Overview

Germany
•Airbus Defence and Space GmbH
•Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung E.V.
•Institut für Automation und Kommunikation E.V. Magdeburg
•Cassidian Cybersecurity GmbH
•CESS GmbH Centre for European Security Strategies

France
•Cassidian Cybersecurity SAS
•Bertin IT

Austria
•Technikon Forschungs- und Planungsgesellschaft mbH
•AIT Austrian Institute of Technology GmbH

Belgium
•Katholieke Universiteit Leuven

Italy
•Poste Italiane SPA
•Alma Mater Studiorum University of Bologna

Ireland
•Gas Networks Ireland
•Espion Limited

United Kingdom
•Airbus Group Ltd.

Finland
•Teknologian Tutkimuskeskus VTT

Portugal
•Inov Inesc Inovacao – Instituto de novas tecnologias
•Infraestruturas de Portugal S.A
•Polícia Judiciária (PJ)

Overall scenario presentation:

Protection of Critical Gas Infrastructures against Cyber-attacks

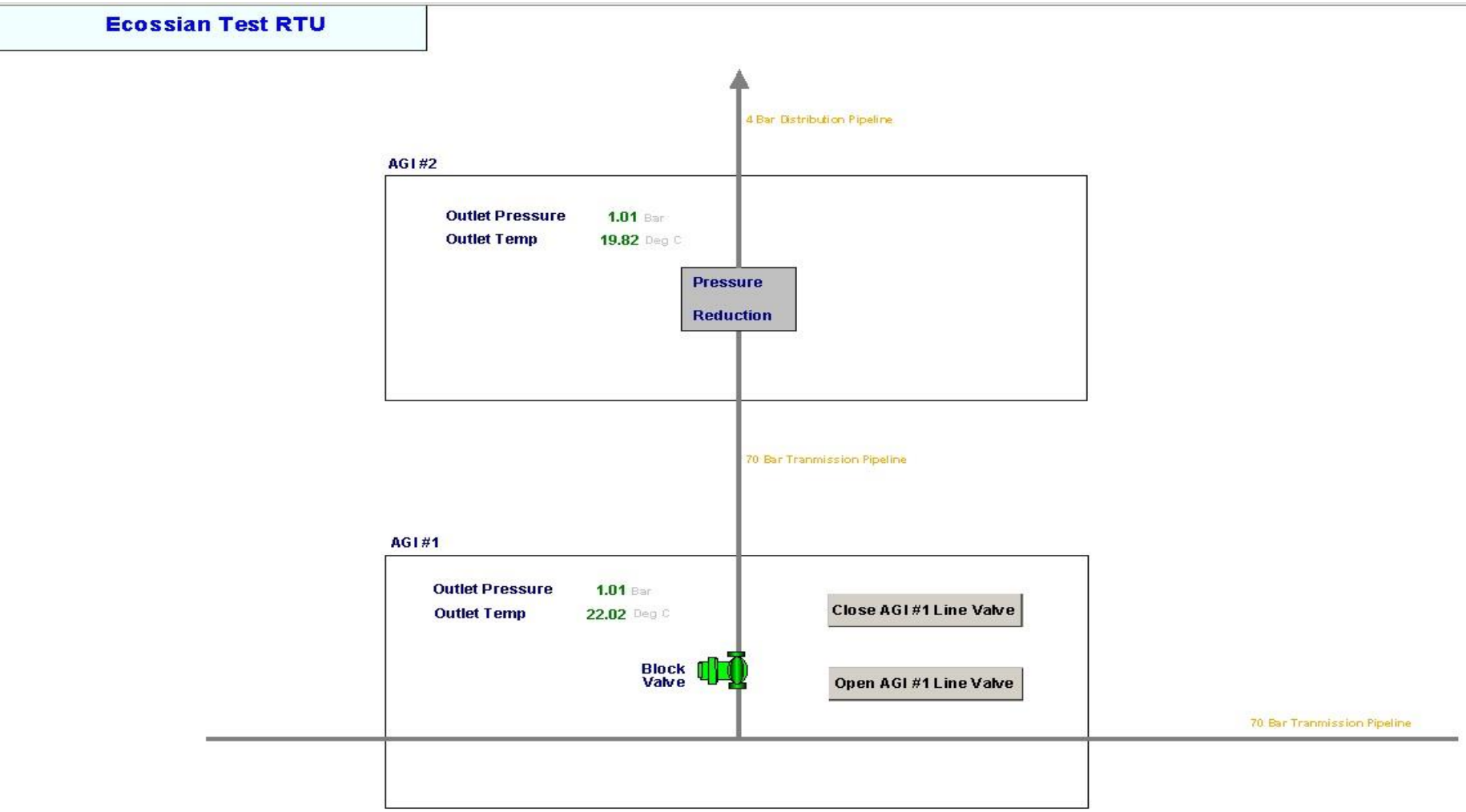
Cork, March 1st 2017

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

Gas Networks Ireland

European Control System Security Incident Analysis Network

SCADA Screenshot



Objectives and demonstration flow

- **Objective:**
  - **Detection of a cyber-attack on a gas provider infrastructure.**

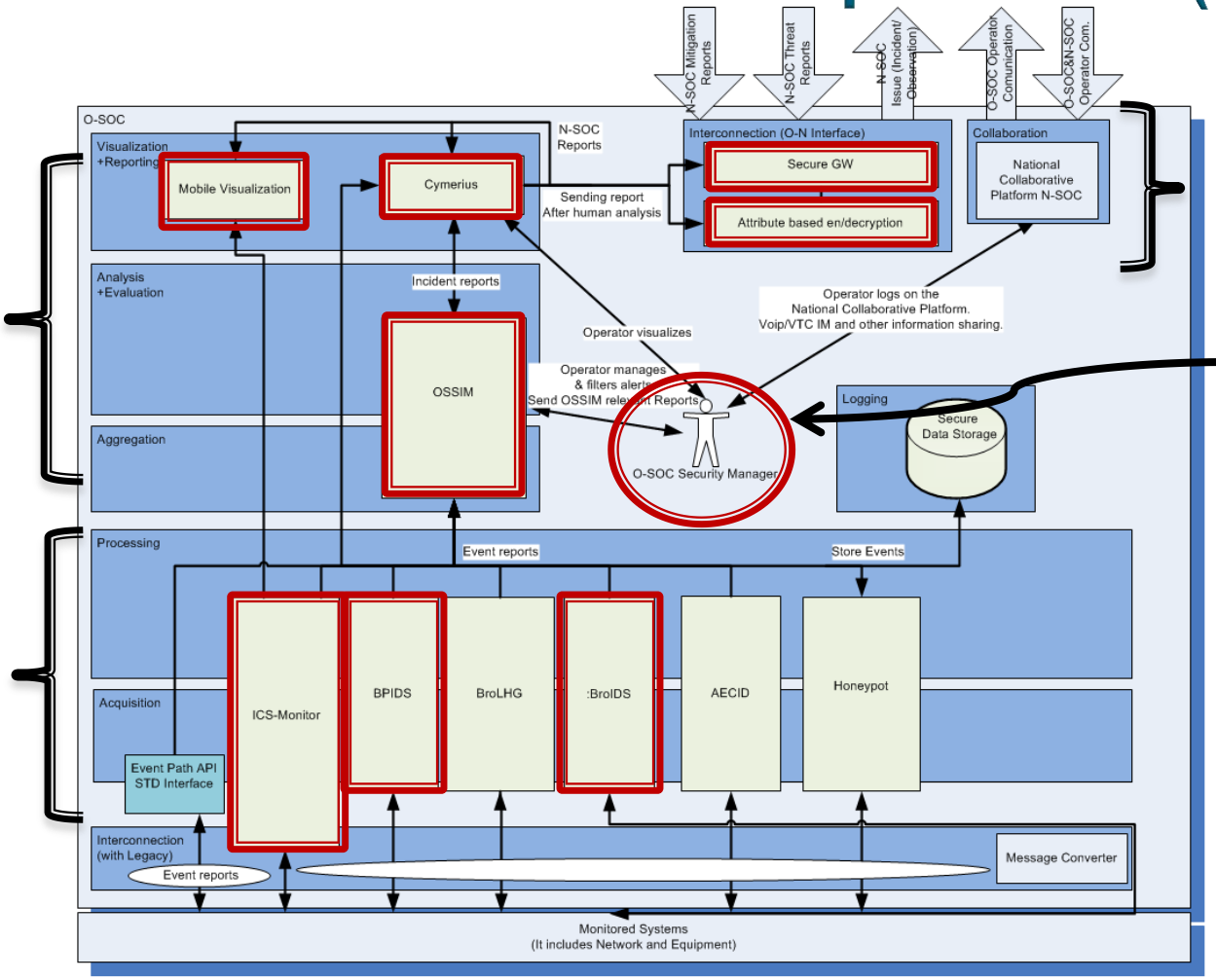
- Demonstration flow:
  - Phase 1: Attack
  - Phase 2: Detection
  - Phase 3: Incident response & Mitigation

- Relevance
  - Address incidents and events that match current threats that pose a real danger to industrial networks

Demonstrated ECOSSIAN capabilities (O-SOC)

O-SOC supervision:
- OSSIM
- Cymerius
- Mobile Visualization

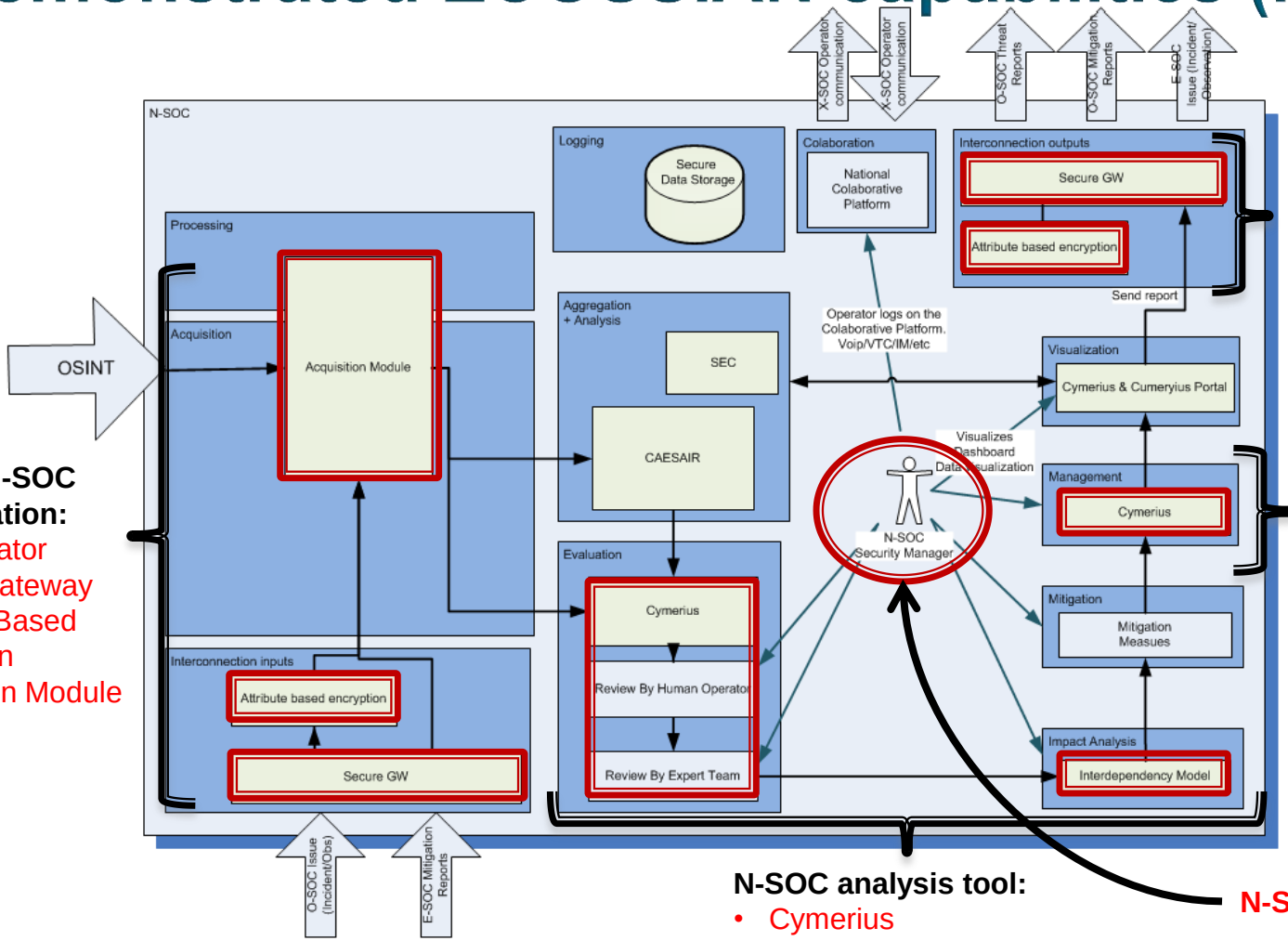
Sensors:
- BPIDS
- ICS-Monitor
- BroIDS



O-SOC / N-SOC communication:
- Encapsulator
- Secure Gateway
- Attribute Based Encryption

O-SOC operator

Demonstrated ECOSSIAN capabilities (N-SOC)



N-SOC to O-SOC communication:
- Encapsulator
- Secure Gateway
- Attribute Based Encryption

O-SOC to N-SOC communication:
- Encapsulator
- Secure Gateway
- Attribute Based Encryption
- Acquisition Module

N-SOC supervision:
- Cymerius

N-SOC analysis tool:
- Cymerius
- Interdependency Model

N-SOC operator

Ecossian

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

Gas Networks Ireland

Operational demonstration

Phase 1: Attack

European Control System Security Incident Analysis Network

Introduction

- **The aim of the attacker is to induce the Grid Operator on the belief that there is a massive gas leak on the pipe.**

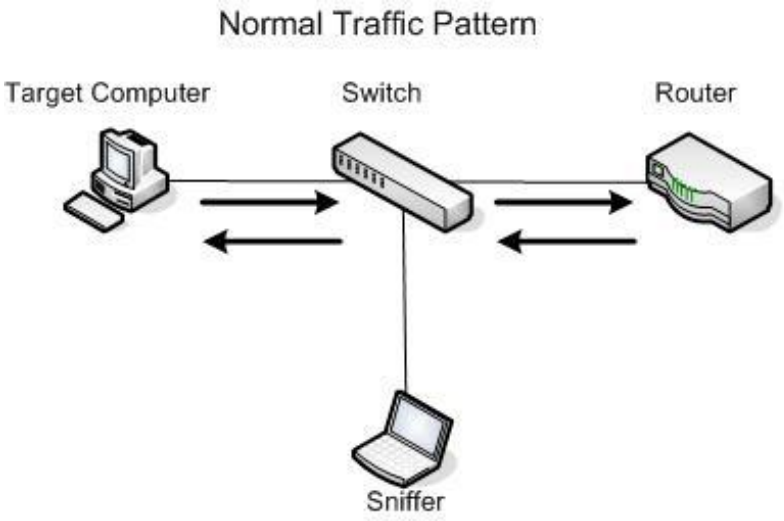
- **The Grid Operator would then close the block valves, thereby isolating the town and electricity power station from the gas network.**

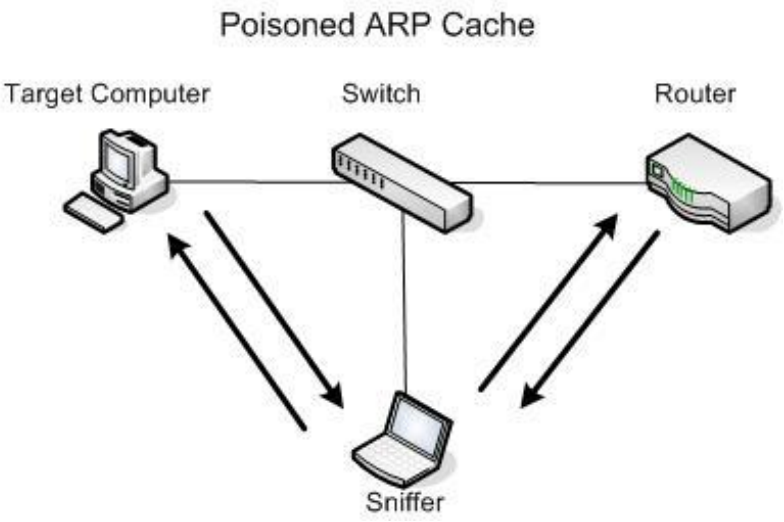
- Attacker

- **Network intrusion**:
  - **Penetration**
  - **Information gathering** (infrastructure, systems, operational routine…)
  - **Persistent connection** to several equipment of the network
    - **Obtain a Man in The Middle position**

- **Attack 1: Suppression of the sensors readouts**:
  - **Traffic diverted** from the Pressure Reduction equipment to the SCADA servers
  - **Suppression some of the readouts** of the sensors in order to create the false impression that some of the sensors are malfunctioning.
- **Attack 2: False telemetry readings**:
  - **False values of the pressure and temperature readouts** are sent to the Grid Operator.
- **Attack 3: disturb communication to a PROFINET device**
  - **Changing IP address** of a PROFINET device **remotely** by sending a special crafted packet
  - **PROFINET device** will be **unreachable** due to missing security measures of the PROFINET protocol itself

- **Normal communication:**
  - **Sending an IP packet over an Ethernet:**
    - **Source send a broadcast ARP (Address Resolution Protocol) packet asking:**
      - **Who has the MAC (Media Access Control) address for the target IP X.W.Y.Z.**
    - **Target replying to a ARP request:**
      - **Target IP X.W.Y.Z. is at MAC XX:XX:XX:XX:XX**
    - **Then the Source will send all the packets for that IP address to the corresponding MAC address.**
- **ARP poisoning Attack:**
  - **The attacker injects fake ARP reply packets in the network informing one or both ends of the communication that his MAC address is the correct address for the other end's IP.**
  - **This will result in all the traffic being routed through the attacker workstation allowing traffic modification or supression.**





Ecossian

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

Operational demonstration

Phase 2: Detection

Gas Networks Ireland

European Control System Security Incident Analysis Network

Introduction

- **Detection of the attack by three sensors of the ECOSSIAN system: BPIDS, ICS-Monitor and BroIDS.**
  - The network is monitored by ECOSSIAN sensors that **detect isolated and uncorrelated "evidences"** related to the running attack.
  - These evidences **reveal traces left behind by sophisticated techniques** adopted by the attacker.

- Attacker

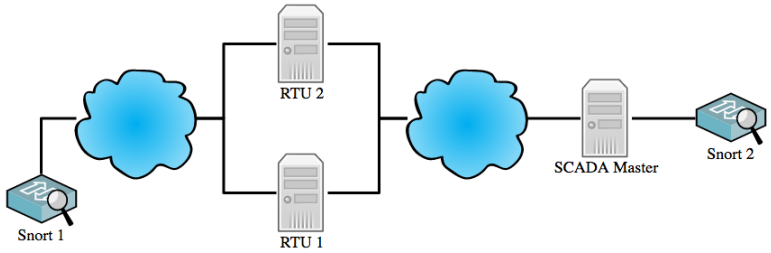
- O-SOC Operator
  - **Supervision** of the security issues of the company's IT.
  - **Real-time view** on the cyber security state of the controlled network and processes.

Mobile Visualization

BPIDS

Business process specification-based intrusion detection system :

- Detects deviations from specification of monitored critical processes:
  - Input: Real time raw data captured directly from passive network sensors or logs. The events are mapped into process activities.
  - Output: Detected deviations providing:
    - Contextual information regarding the business process where the deviation was detected (Systems involved, previous process history, expected process activities, etc.)



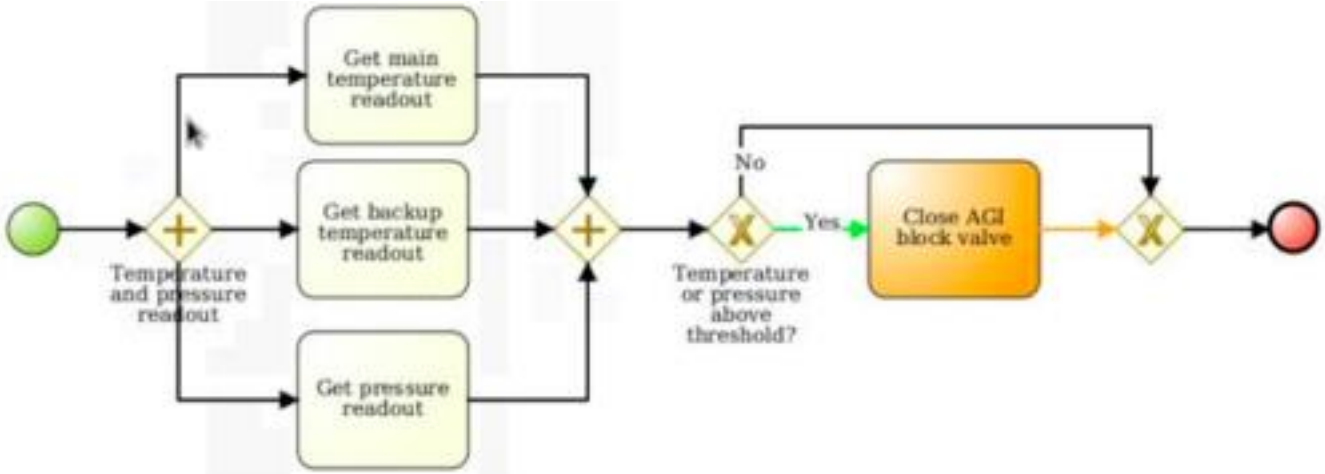
Sensor #1: ICS-Monitor & Mobile Visualization

Event detected
•Network topology change.

ICS-Monitor
•*Detects the change on the network topology*
•*Shows that the communication between the RTU and the SCADA servers is compromised.*
•*Evaluates the overall industrial communication to learned and typical behaviour found in the ICS-plant.*

Mobile Visualization
•*Display*
•*Short time of communication silence in the graphic visualization of the process values*
•*Evaluation of the process values showing that a possible incident happened.*

Sensor #2: BPIDS



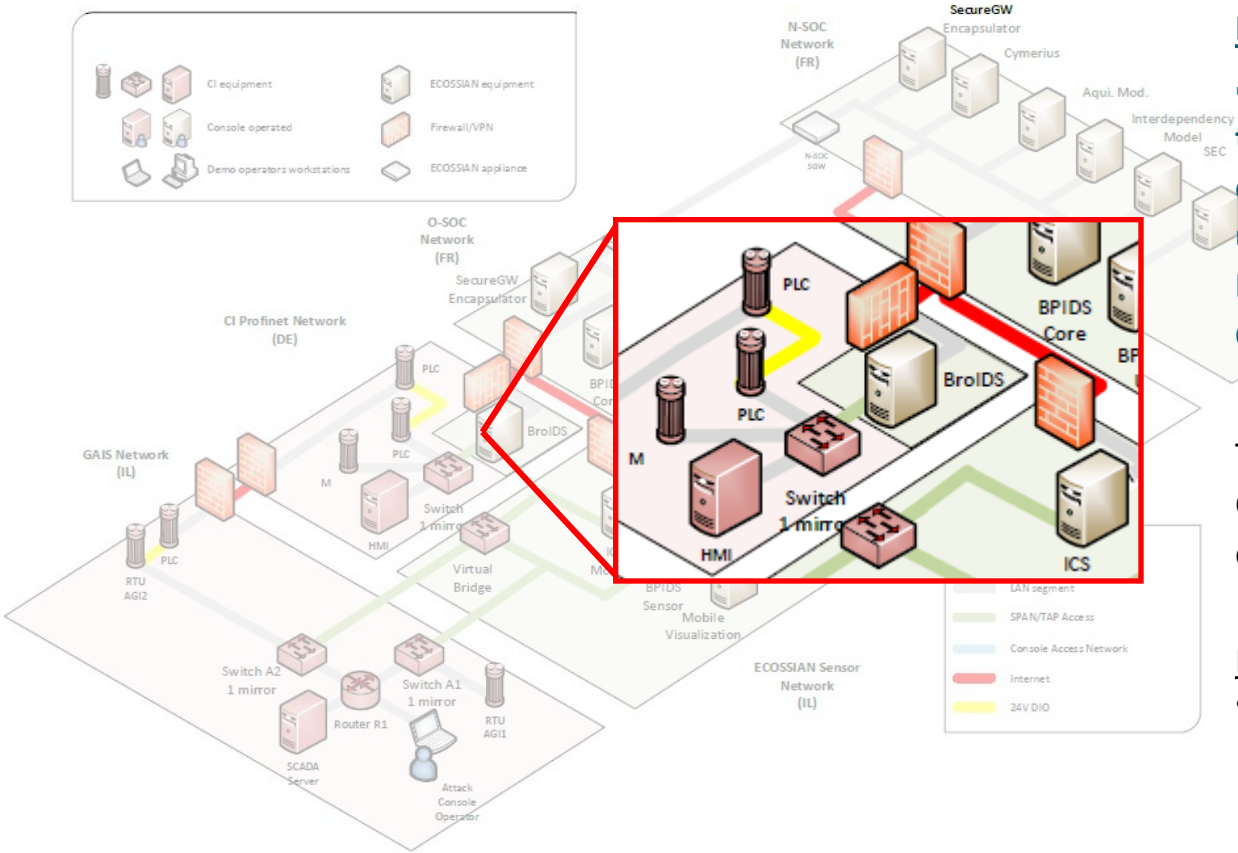
Attacks detected

1.Suppression of the sensors' readouts – messages from the RTU to the SCADA server are being supressed

2.Detects that the set of messages produced by the RTU and the ones received at the SCADA server do not match

- ***Concludes that the sensors readouts at the SCADA server are incorrect***

Sensor #3: BroIDS-ICS



ECOSSIAN capabilities

▪The BroIDS-ICS sensor, analysing the PROFINET protocol, will detect changes in topology because of unexpected IP requests by using the PROFINET Discovery and basic Configuration Protocol (DCP).

The combination of BroICS-ICS and Cymerius helps to **alert** the O-SOC operator **about a possible intrusion**

Event detected

- Network topology change

Ecossian

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

Gas Networks Ireland

Operational demonstration

Phase 3: Incident response and mitigation

European Control System Security Incident Analysis Network

Introduction

- **Investigation, incident response and mitigation:**
  1. Incident supervision and analysis (O-SOC level)
  2. National collaboration and support for solving the incident (O-SOC to N-SOC incident forwarding)

- O-SOC operator

- N-SOC Operator
  - High-level information from O-SOCs
  - **Situational awareness** and view on the **nation's critical infrastructures**
  - **Nation-wide forensics analysis**

O-SOC level: supervision

SIEM (OSSIM or others)

- Open source Security Information and Event Management System
- **Aggregation** and **Correlation** of **Sensor Events**

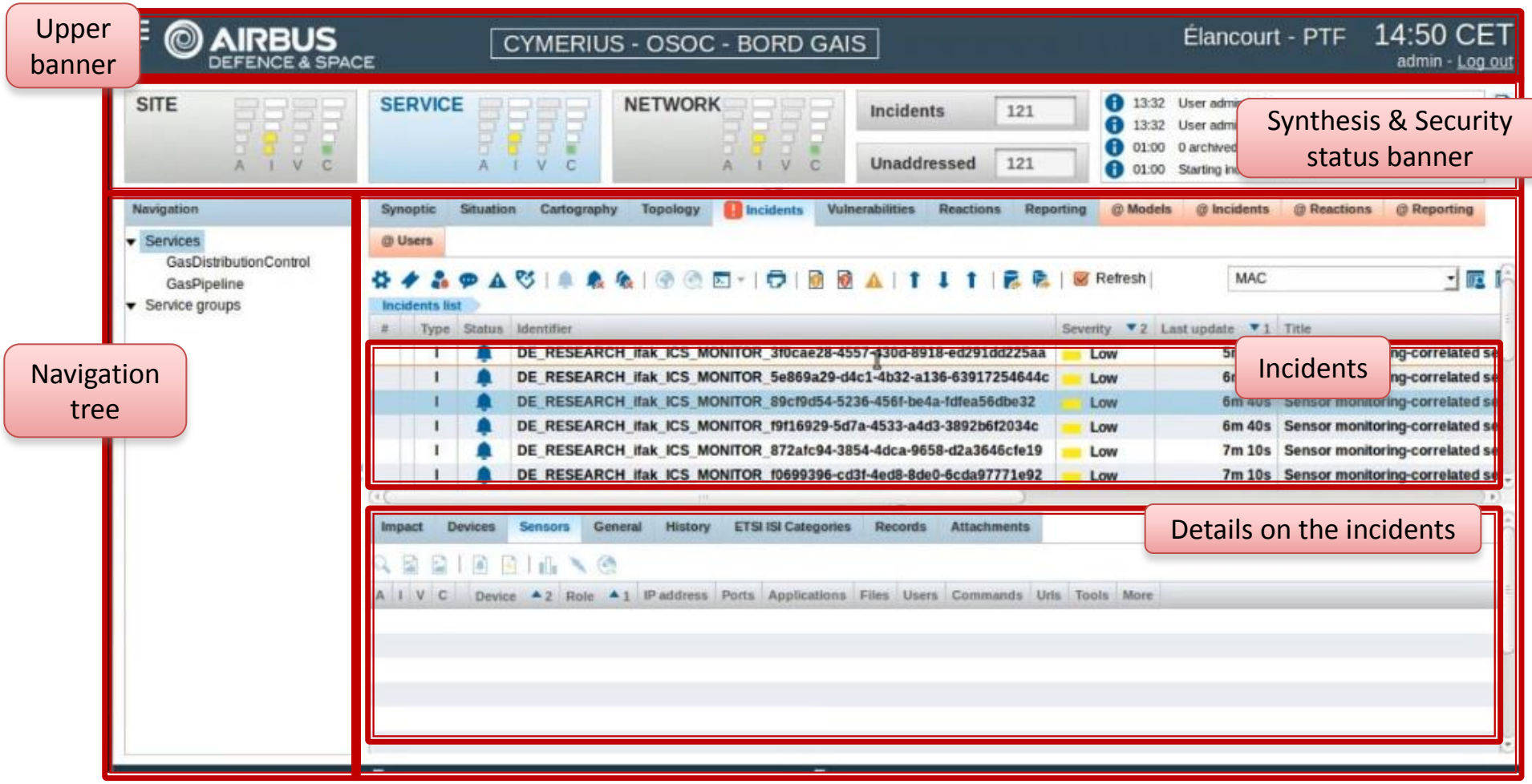
O-SOC Cymerius

- **Situational awareness** solution used within a SOC
- Incident view linked with a **business impact evaluation**
- Situation overview along with **mitigation actions** specifically adapted to cyber incidents

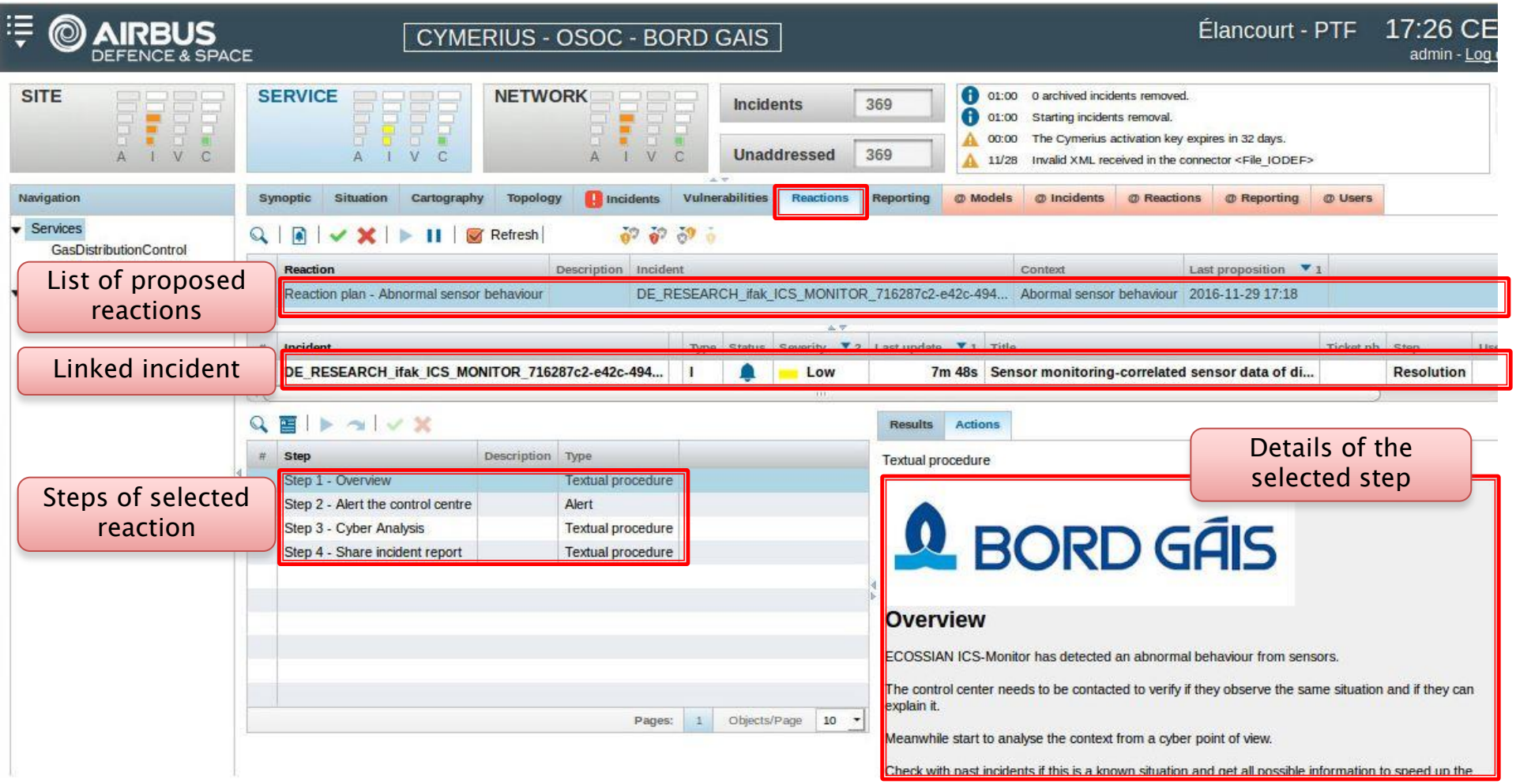
ECOSSIAN capabilities

- **Supervision** of the cyber-security state of the **monitored infrastructure**.
- Capacity to supervise incidents in a centralized and user-friendly way.
- **Inter-operability with many different SIEM** solutions (like OSSIM in this case).

Cymerius – Incident supervision



Cymerius – Reaction plan



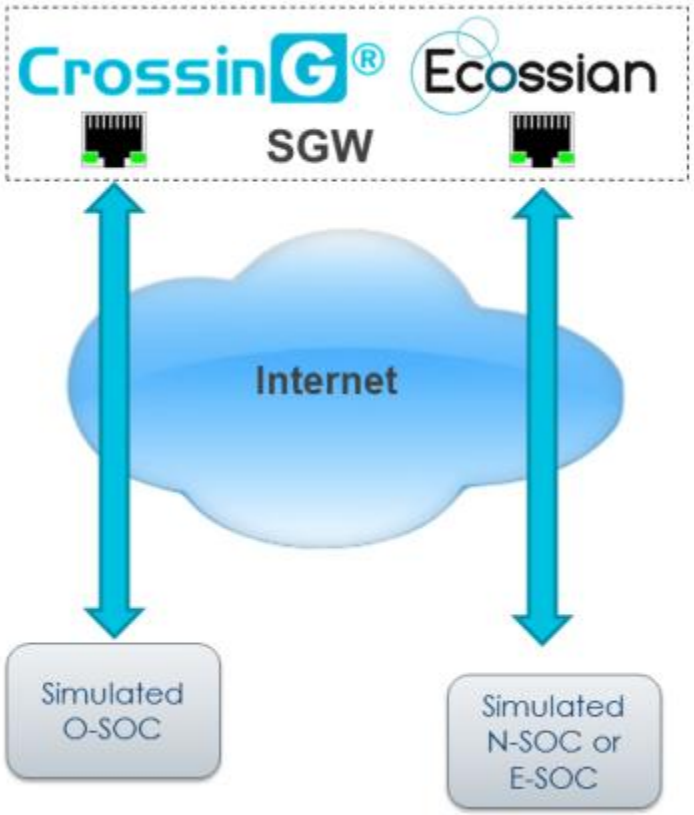
List of proposed reactions

Linked incident

Steps of selected reaction

Details of the selected step

O-SOC to N-SOC: incident forwarding



Secure Gateway

- Encapsulator interface
- Unidirectional information channel
- Virus and malware verification
- Security label verification
- Security event logging
- Anonymization by the Encapsulator module
- Every message going out of the SOC shall be **approved by a SOC Manager**.

Information sharing

- **Cryptographic Access Control**: design of mechanisms for providing **confidentiality** of shared information

Attribute-Based-Encryption

Attributes Definition

Attribute Type	Possible Values
SOC-Level	OSOC, NSOC, ESOC
Country	AT, DE, ES, FR, GB, IE, NL, PT, …
SOC Sector	Chemical, Dams, Defense, Emergency_Services, Financial_Services, Government_Facilities, Healthcare_and_Public Health, Information_Technology, Nuclear, Transportation_Systems, Water_and_Wastewater_Systems, etc.
TLP	TLP-Red, TLP-Amber, TLP-Green

Access Policies Formulation

Policy: ((“OSOC” AND “GB” AND “Health”) OR (“TLP-Red”))

Partial Message Encryption

TTP	
ID	example:ttp-7d9fe1f7-429d-077e-db51-92c70b8da45a
Title	Victim Targeting: Electricity Sector and Industrial Control System Sector
Victim Targeting	
Identity	CIQIdentity3.0InstanceType
Specification	
Organisation Info	
Industry Type	Electricity, Industrial Control Systems

Policy: E-SOC, Electricity, ICS

Acquisition Module

Collects data reported by the O-SOCs, and acquired from public external sources, temporarily stores it, and makes it available to the analysis components.

Compliant with the most widely adopted data formats and protocols for cyber incident and threat information description and exchange.

N-SOC level: analysis

N-SOC Cymerius

- Update incident with Impact Analysis (from Interdependency Model) and recommendations (from N-SOC operator)

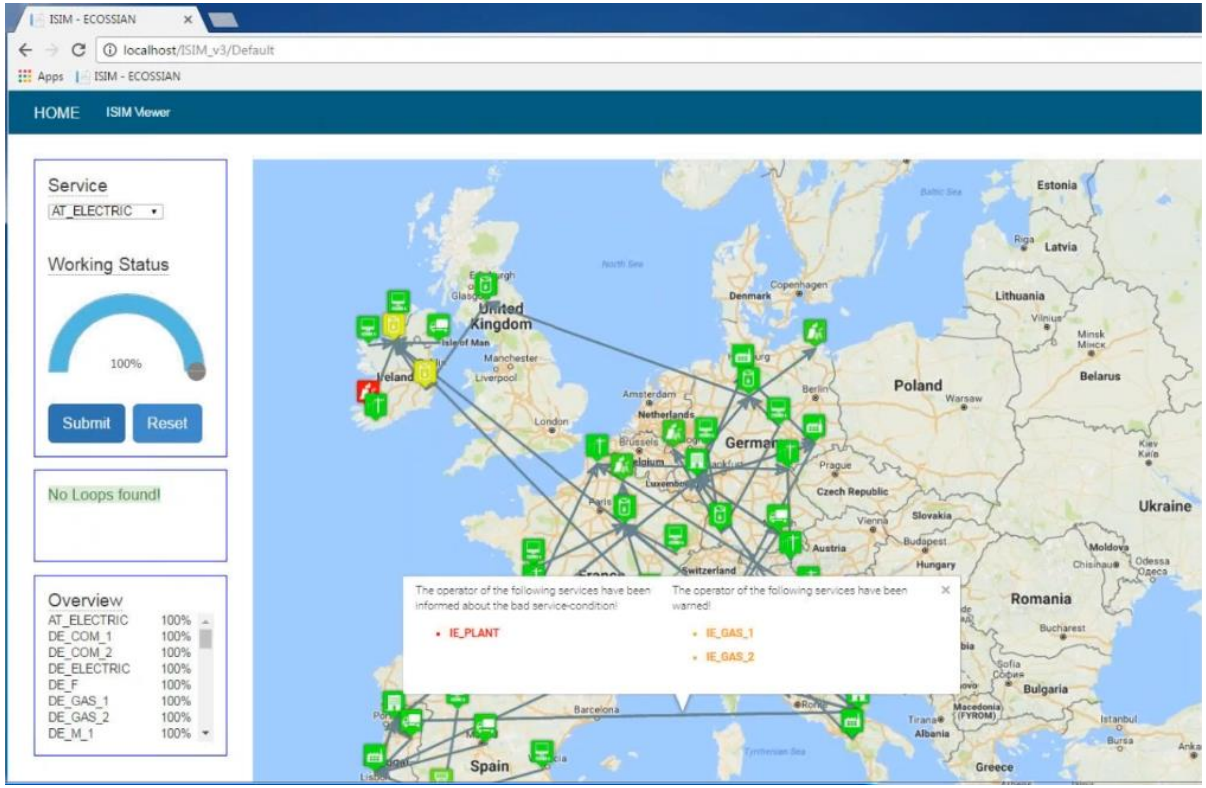
ECOSSIAN capabilities

- **National support :** Collaboration and support at national level to help the SOC at Operator level solving the incidents they are facing.
- **Analysis tools:** Interdependency Model
  - **Centralised database:** Centralise useful information (such as **situation awareness** and **impact analysis**).

Interdependency Model

- Support situational awareness and find out interdependencies
- CIs dependant of the service of the disturbed CI
- System-of-systems approach

Interdependency Model



ECOSSIAN capabilities

- **The Interdependency Model presents all CIs and there location in Europe. After the attack the model highlights all affected CIs and shows a list of immediately affected CIs and their availability.**

The information are send to Cymerius and **integrated in the incident report** for a **comprehensive evaluation of the criticality of the incident**.

Mitigation & feedback sharing (lesson learned)

Mitigation

- The O-SOC operator **updates the incident report with complementary information** on how the incident was open, analysed and closed.

Detection and mitigation feedback sharing

- **Sharing of feedback information on detection and mitigation procedures at national and European levels**.

ECOSSIAN capabilities

- **National support:** Collaboration and support at national level to help the SOC at Operator level solving the incidents they are facing.
- **Preparedness of Critical Infrastructures and SOC Operators in Ireland and in Europe.**

N-SOC warnings: national awareness

ECOSSIAN capabilities

▪Situational awareness at National & European levels

- **Warnings sharing:** warnings issued by the O-SOC are forwarded to the SOCs at national and European levels
- **Threat information sharing:** broadcast by the N-SOC to the **other critical infrastructures** that could suffer from the same kind of attack.
- **Secure communication (Secure Gateway)**
- **Encryption capabilities (Attribute-Based Encryption)**

Conclusions (1/2)

A layered system architecture for a pan-European cooperative threat management, early-warning and situational awareness:

- Cross-country and cross-sectorial collaboration – providing a secure information sharing enviroment;
- Anonymity and privacy (confidentiality) preserving for all joining members – usage of attribute based encryption and anonymization techniques at the Secure Gateway;
- Secure information sharing and collaboration platform compliant to legal and other regulatory requirements – cryptography and privacy protecting mechanisms;
- Technologies and processes for monitoring and threat/incident detection and near-real-time detection of attacks – set of advanced sensors for detecting threats in ICS;

Conclusions (2/2)

- Data analysis, aggregation, correlation and visualization – tools at O and N level;
- Threat mitigation, impact analysis, interdependencies and incident management – recommendations on good practices;
- Evaluation of the regulatory, social and economic boundary conditions
- **Full-scale demonstration** of the integrated ECOSSIAN system on all levels (O-SOC, N-SOC, E-SOC):
  - 3 National demonstrations (O and N level)
    - **Ireland**
    - **Italy**
    - **Portugal**
  - **1 European wide demonstration in France (O, N and E level);**
- **Project ends on May 2017.**