ECOSSIAN FP7 PROJECT:

Project overview

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

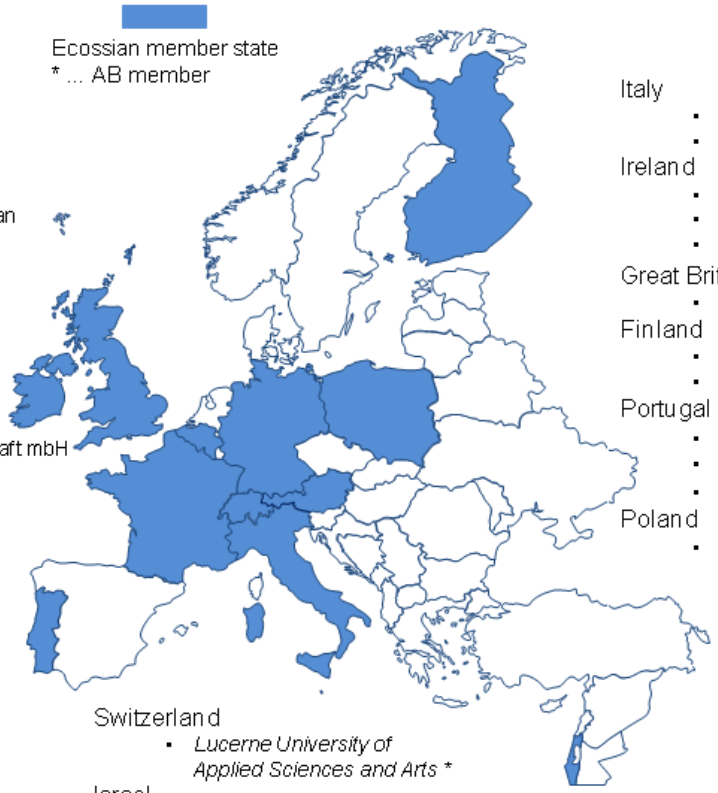
Presented by:
Klaus-Michael KOCH
TECHNIKON Forschungsgesellschaft mbH

DRS-workshop
2016.02.22 @ Vienna

Ecossian

European Control System Security Incident Analysis Network

ECOSSIAN Consortium Overview



Germany
- EADS Deutschland GmbH
- Fraunhofer AISEC
- ifak Institut für Automation und Kommunikation e.V.
- CESS GmbH Centre for European Security Strategies
- Cassidian Cybersecurity GmbH
- *BSI Federal Office for information security **

France
- Cassidian Cybersecurity France
- Bertin Technology

Austria
- Technikon Forschungsgesellschaft mbH
- Austria Institute of Technology
- *Austrian Ministry of Interior **
- *Austrian Federal Ministry of Defence and Sports **
- *OMV Refining**

Belgium
- ICRI KU Leuven

Italy
- Poste Italiane SPA
- University of Bologna

Ireland
- Bord Gais
- Espion Group
- *UCD Dublin**

Great Britain
- *EADS UK (subcontractor)*

Finland
- VTT
- *Finish Interior Ministry **

Portugal
- INOV Inesc Inovação
- REFER
- Ministerio da Justiça

Poland
- Police Academy in Szczytno

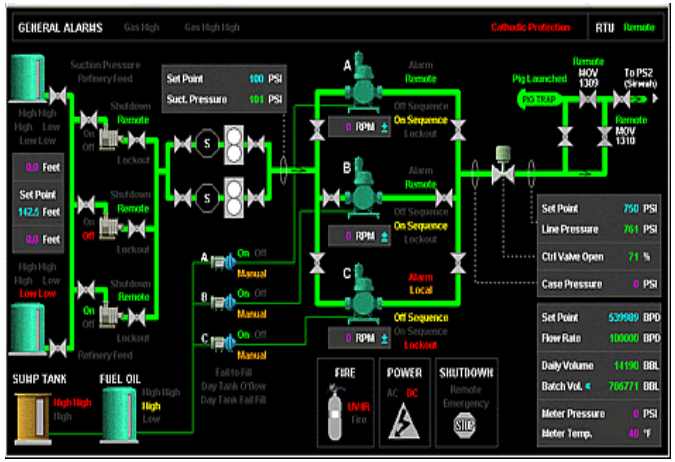
Switzerland
- *Lucerne University of Applied Sciences and Arts **

Israel
- *White Cyber Knight WCK **

Global
- *Europol **
- *University of California/ICSI **

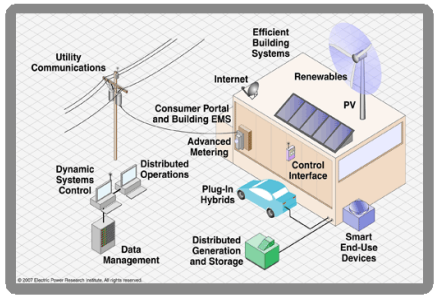
Background

- 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 …
    - … growing convergence by “script kiddies”



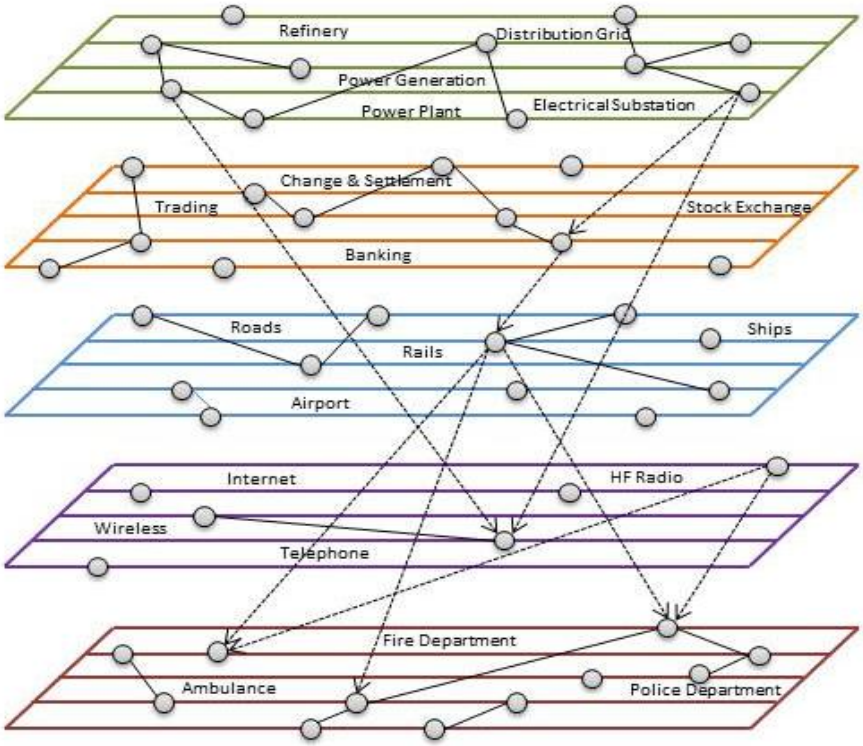
Motivation

- Attack surface to critical infrastructures is continuously growing because:
  - Deployment of Commercial off-the-shelf (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 industrial 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



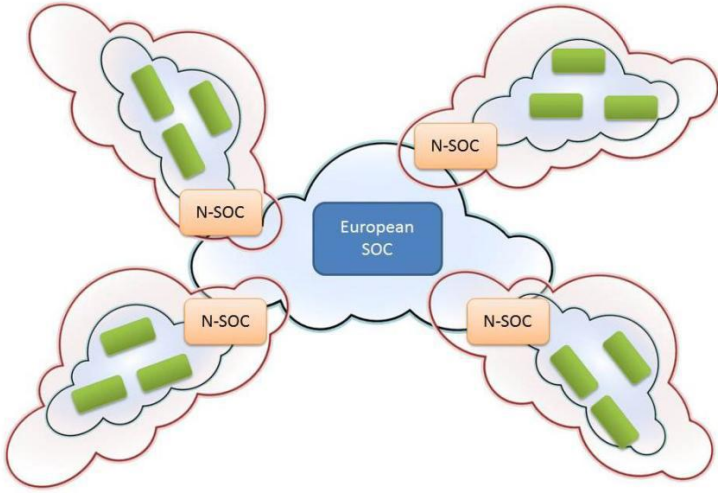
Motivation

- Interdependencies between critical infrastructure (CI)



Project goals (1)

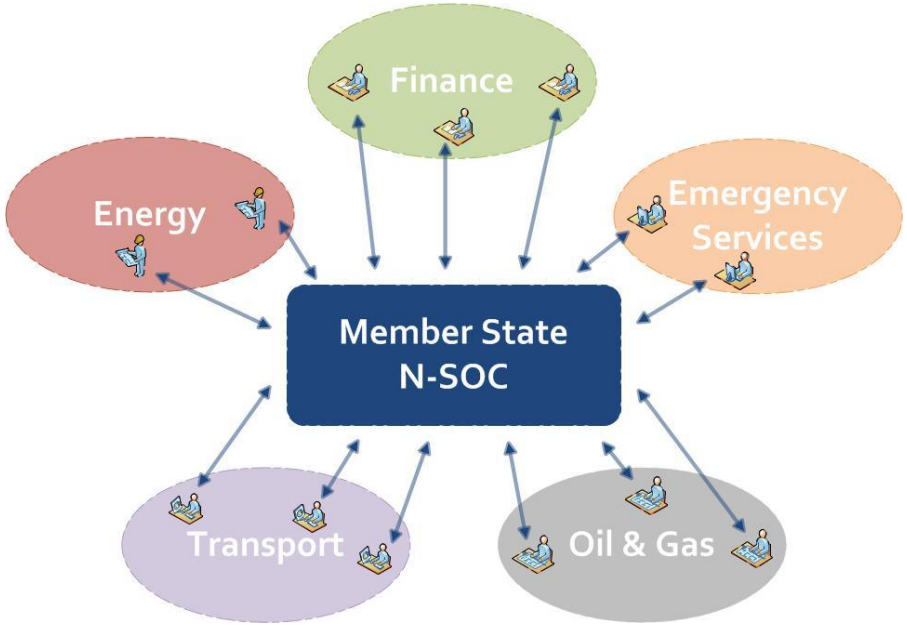
- Development of a cross boarder European early warning system for critical infrastructures
- Three tiers of collaborative, interconnected Secure Operation Centres (SOCs)
  - **Local/sub-state SOC (O-SOC)** early detection and data collection with aggregation
  - **National SOC (N-SOC)** Situational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

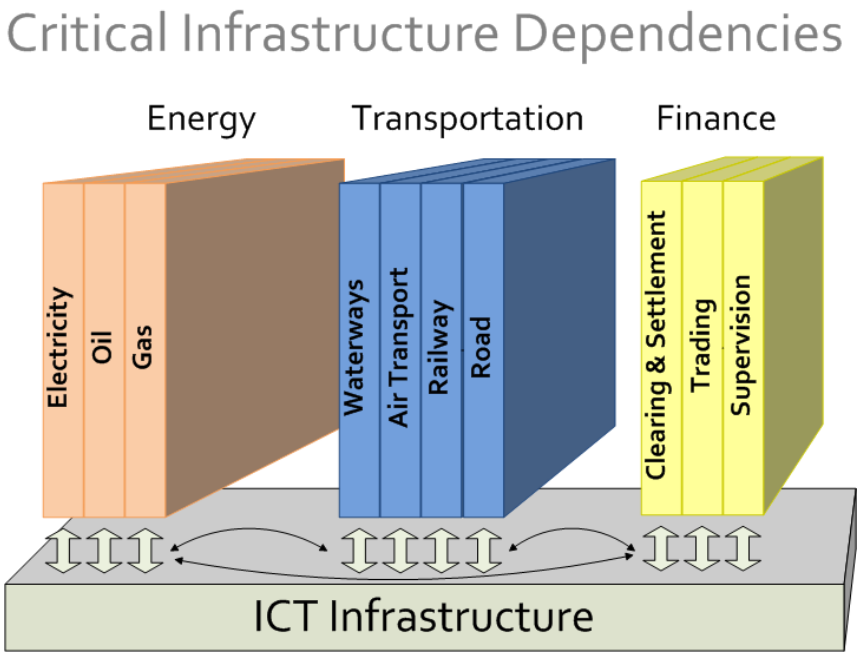


  - **Transnational SOC with command and control capabilities with inclusion of member state SOCs (E-SOC)** Transnational Situational Awareness and coordinated and consistent crisis management

Project goals (2)

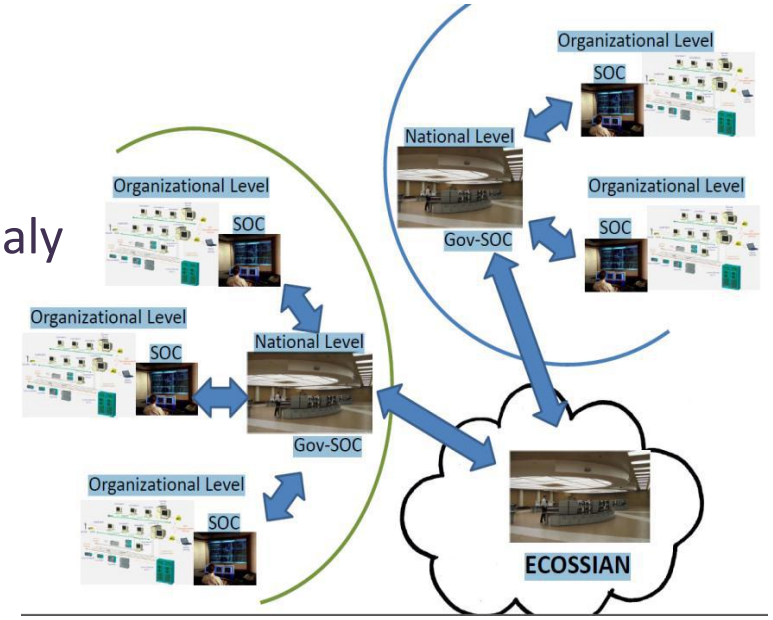
- Development of a cross boarder European early warning system for critical infrastructures



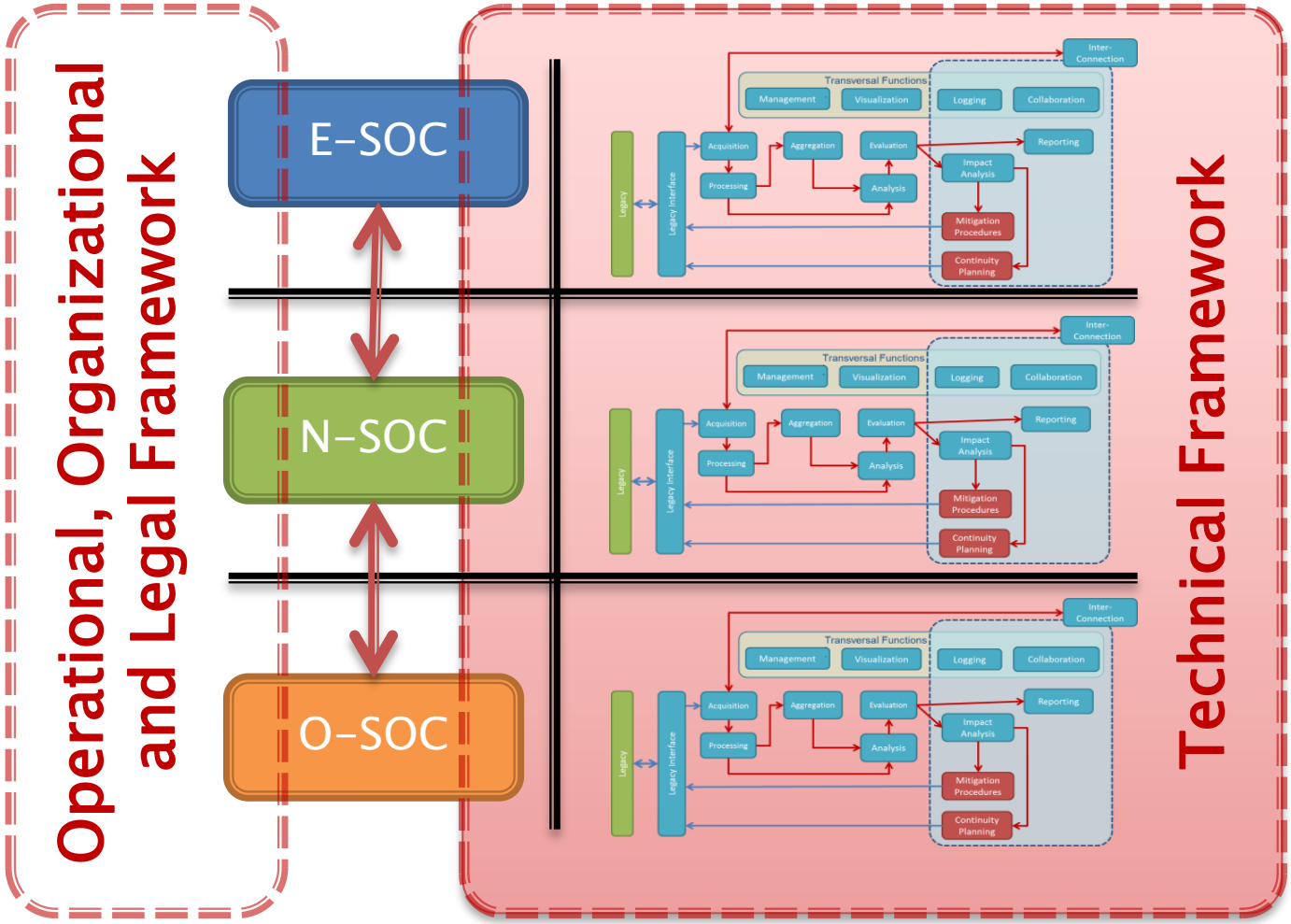


Project goals (3)

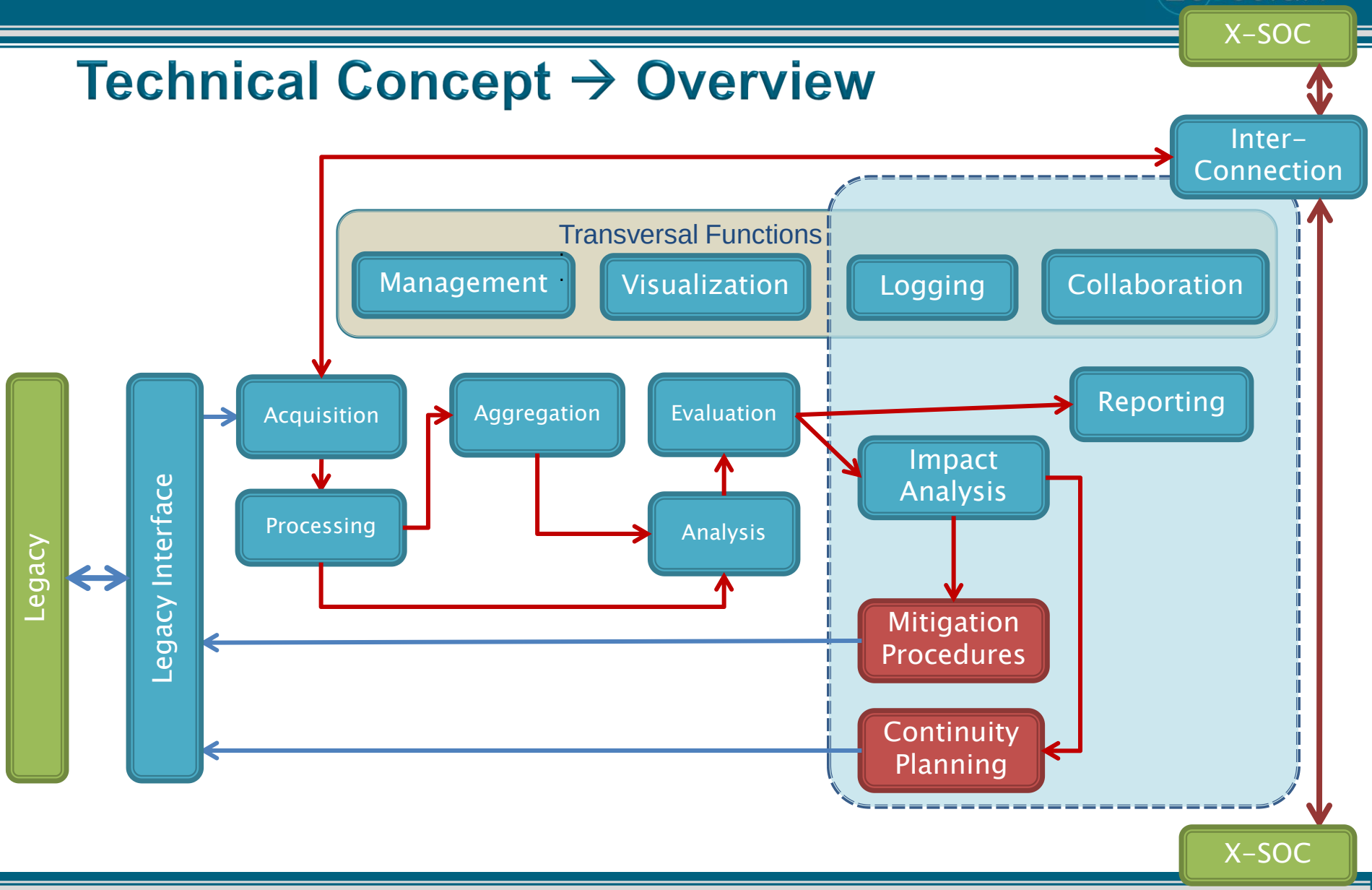
- Technological as well as organisational solution development under consideration of data protection and legal aspects
- Ensuring secure and trusted information exchange
- Anonymity and privacy (confidentiality) preserving for all joining members
- Near real time detection of attack artefacts and indicators of compromise through anomaly detection on all levels
- Early warning framework for pro-active protection and timely, coordinated mitigation and defence measures



Technical Concept → Overview



Technical Concept → Overview

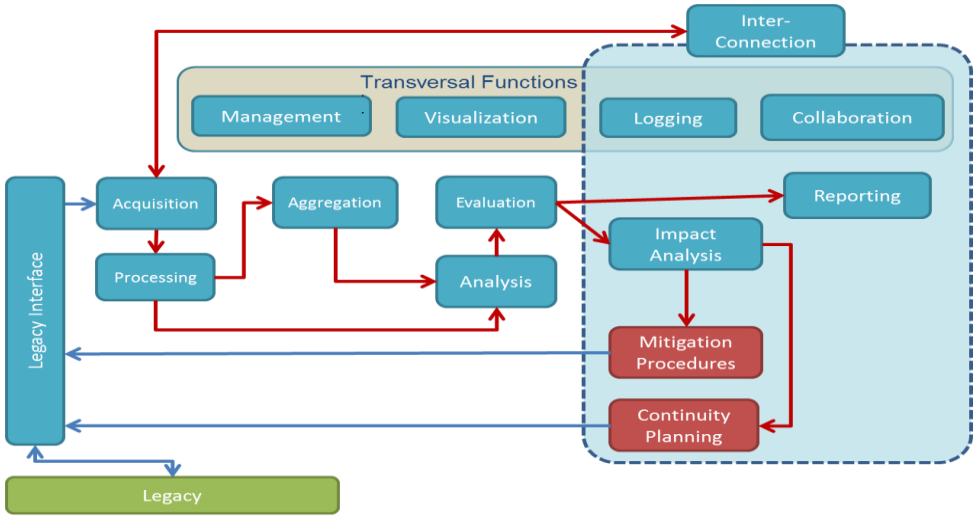


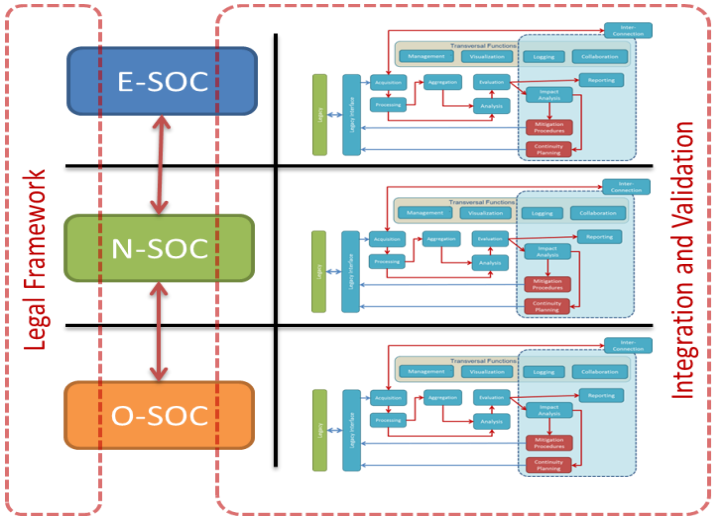
Some of the tools used/extended

- Threat detection:
  - Business Process specification based IDS –BPIDS (INOV)
  - Network analysis framework BRO(EADS) + Honyed (EADS)+ BROLhg(VTT)
  - Industrial Control Systems (ICS) Monitor (IFAK)
  - Automated Event Correlation for Incident Detection – AECID (AIT)
- Aggregation:
  - ICS Monitor, BPIDS, AECID (AIT)
- Analysis:
  - OSSIM - Open Source Security Information Management,
  - Qradar® – Security Platform for integrating security information and event management
  - Collaborative Analysis Engine for Situational Awareness & Incident Response – CAESAIR (AIT)
- Visualization:
  - Cymerius® - Surveillance tool to detect, centralise and evaluate security incident (CAS-FR)
- Communications:
  - CrossinG (BRT) with IODEF, STIX and Attribute Based Encryption

Technical Concept → Overview

- This general architecture applies to each SOC
- Concept of specializations applies to each SOC → implementations may be different, specifically at different level
- SOCs may collaborate on a single level or accross levels exploiting ECOSSIAN Inter-connection FB
- Operations and communication must comply to applicable legal conditions





Timeline

- Started: June 2014
- Uses Cases, Requirements and Architecture: Finished
- Stakeholders feedback on the solution: Ongoing
  - Workshops in: Portugal, Italy, Finland, Germany and Austria
- First public demonstrations: 4Q of 2016
  - Regional demos: Portugal, Ireland, Italy, France
  - Possible lab demos: Germany, Austria
  - European demo (France): 1Q 2017
- Finished: May 2017

ECOSSIAN Grant Agreement No. 607577

"The **ECOSSIAN** project has received funding from the European Union's Seventh Framework Programme ([FP7/2007-2013]) under grant agreement number SEC-607577."

If you need further information, please contact the coordinator:
TECHNIKON Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55 Fax: +43 4242 233 55 77
E-Mail: coordination@ecossian.eu