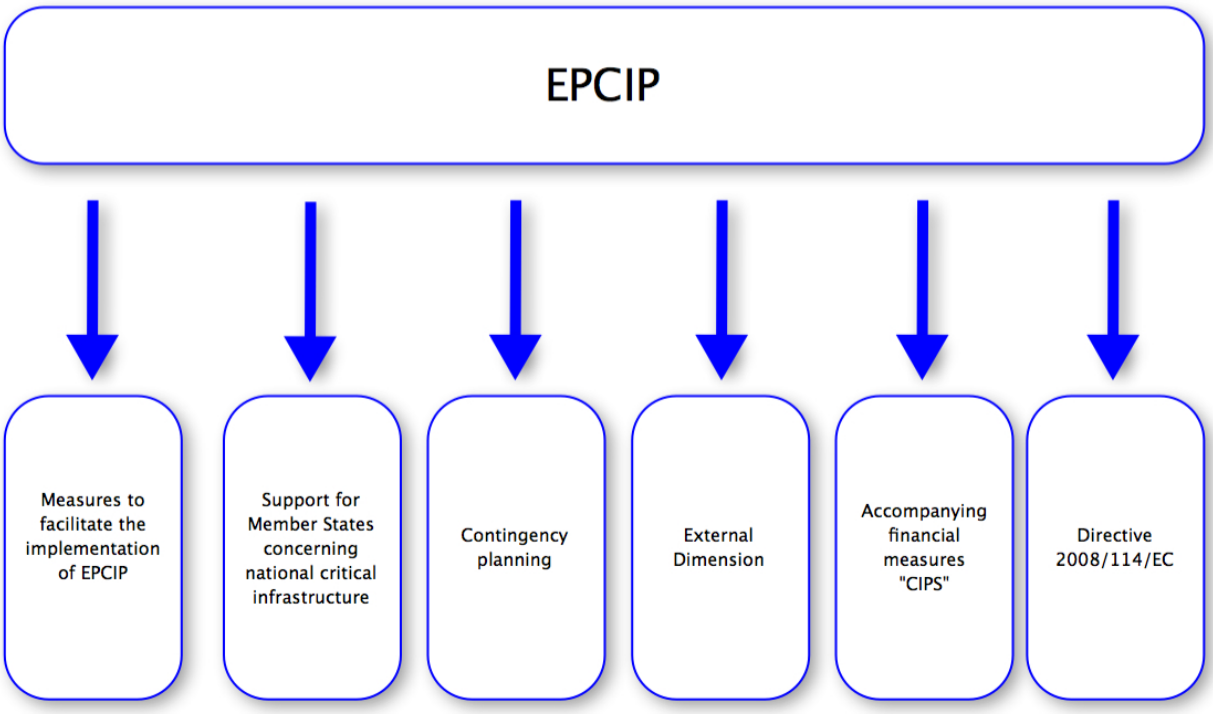
CIPS III workshop on research projects financed by DG HOME CIPS specific programme

Workshop Proceedings
12 November 2013
Brussels, Belgium

Athina Mitsiara
Georgios Giannopoulos

2014



EUR 26537 EN

Joint Research Centre

European Commission
Joint Research Centre
Institute for Protection and Security of the Citizen

Contact information
Georgios Giannopoulos
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 210, 21027 Ispra (VA), Italy
E-mail: georgios.giannopoulos@jrc.ec.europa.eu
Tel.: +39 0332 78 6211
Fax: +39 0332 78 5469

http://stanet.jrc.it/
http://www.jrc.ec.europa.eu/

JRC 87634 EN

EUR 26537 EN
ISBN 978-92-79-35583-7
ISSN 1831-9424

Doi: 10.2788/12429

Luxembourg: Publications Office of the European Union, 2014

Printed in Italy

Contents

Introduction and scope of the CIPS III workshop

DG HOME has financed a series of research projects in the period 2007-2013 under the specific programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks". This funding scheme is designed to protect citizens and critical infrastructures from terrorist attacks and other security related risks. Within the framework of the support activities of JRC to DG HOME, three CIPS workshops have been organised until now. The first CIPS workshop was organised in Rome in 2011, the second in Ispra in 2012 and the third one in Brussels in 2013. All CIPS workshops are co-organised by DG HOME and DG JRC. CIPS I and CIPS II were mainly focused on technical issues and presentation of projects. In both workshops the aim was to provide the latest research results of selected projects.

However, the objective for CIPS III was somehow different. Apart from the value for the CIPS research community, CIPS III aimed at disseminating information on the future of the CIPS research both at content as well as at operational level. The 2013 CIPS call was the last one of the current funding scheme. The next funding scheme for the period 2014-2020 will be articulated in a different way. The participants of the workshop were researchers, Member States representatives and stakeholders. This composition facilitated the exchange of views which is of vital importance.

The projects were selected on the basis of their maturity, the results provided up to now,

on their relevance with EPCIP policy objectives as well as on their relevance with emerging security issues. Further to this, it was important to demonstrate the impact of CIPS projects at different scales, European, national and regional and finally it was important to demonstrate how capacity building in previous CIPS calls opens new opportunities for integrating knowledge and efforts for improving the protection of critical infrastructures. The workshop started with an introduction from Mr Olivier Luyckx, Head of Unit of A.1 Unit "Crisis Management and Fight against terrorism" explaining the objectives and the scope of this workshop.

Presentation on CIPS scheme and technical achievements during the period 2007-2013

Mr. Torben Fell, DG HOME

Mr. Fell provided an overview of the achievements of CIPS funded projects. He explained where CIPS fits in the context of the European Program for the Critical Infrastructure Protection (EPCIP), with a reference to the revised EPCIP that focuses more on the interdependencies and on cross-sectorial issues. Data gathered from the mid-term evaluation of the program covering the years 2007-2010 were presented, as well as data for the period 2011-12. Finally, Mr. Fell presented some statistics of the whole period of the program (2007-2012) and some of the achievements of the program were outlined.
A question about measuring the efficiency of the budget allocated to the CIPS raised a discussion on how the outcome of the CIPS projects can contribute to the future policy developments at EU level. HOME focuses on four blocks; the critical interdependencies, the risk assessment policies, the preparedness for future mitigation action and the collaboration with the European Response Centre (ERC) in terms of response and consequence management. Thus research activities should provide input to support these activities.

CIPS Scheme: Results Obtained and Technical Achievements 2007-2013

Torben Fell
DG HOME

12.11.2013

Overview

- CIPS in context of EPCIP
- Data: CIPS mid-term evaluation (2007-2010)
- Data: CIPS 2011 & 2012
- Trends, achievements

The European Programme for Critical Infrastructure Protection (EPCIP)

Measures designed to facilitate the implementation of EPCIP

- **CIWIN**
- **CIP expert groups**
- **CIP information sharing**
- **identification and analysis of interdependencies**
- **ERN-CIP**

Support for Member States concerning National Critical Infrastructure

Contingency planning

External dimension

Accompanying financial measures

EU programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013

Directive 2008/114/ EC 8 December 2008

A procedure for the identification and designation of European Critical Infrastructures (ECI)

CIPS

- **Objective: to fund CIP-related measures and projects**
- **EUR 140 million for the period 2007-13 allocated for operational cooperation and coordination actions**
- **Mid-term evaluation conducted in the framework of the programme "Security and Safeguarding Liberties" (COM(2011)318)**
- **Since 2007 over 100 projects funded, including:**
  - Methodologies for risk analysis
  - Analyses of dependencies and interdependencies
  - Exercises
  - Studies

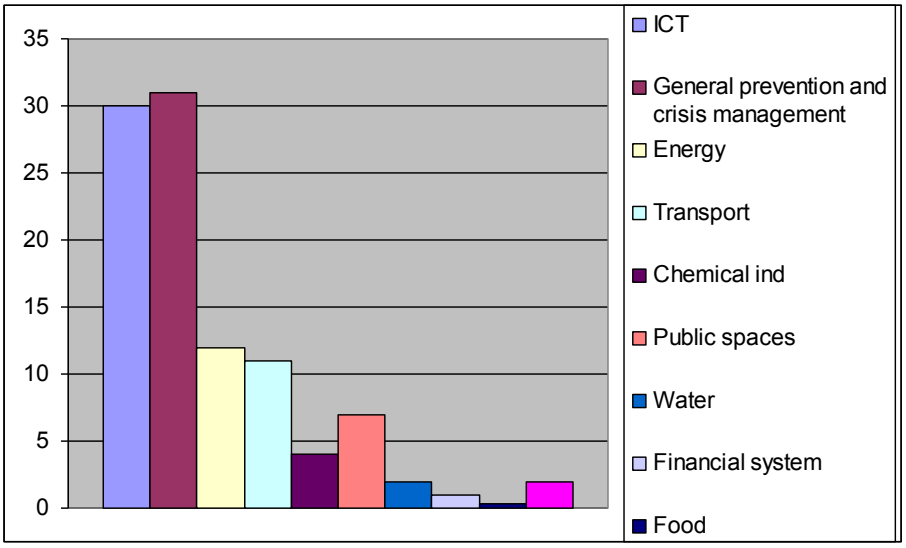
Funded projects 2007-2010

±100 projects

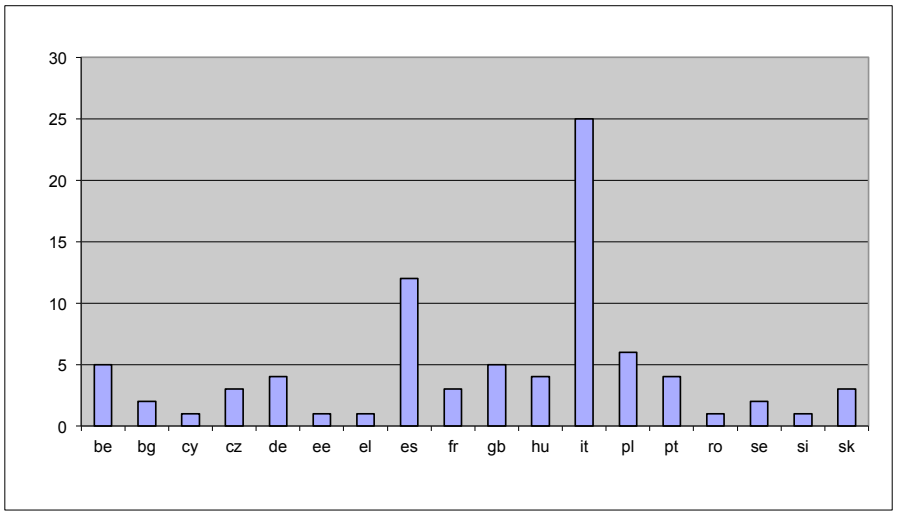
Total awarded amount:± 37 Mio/€

Average grant: ± 400.000 €

Main areas of intervention (2007-2010)



Geographical distribution (2007-2010)

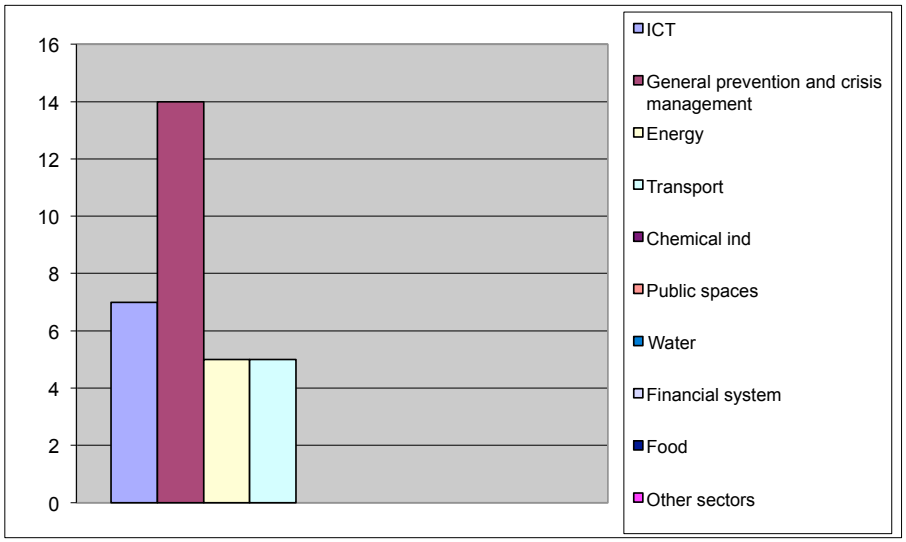


Funded projects 2011-2012

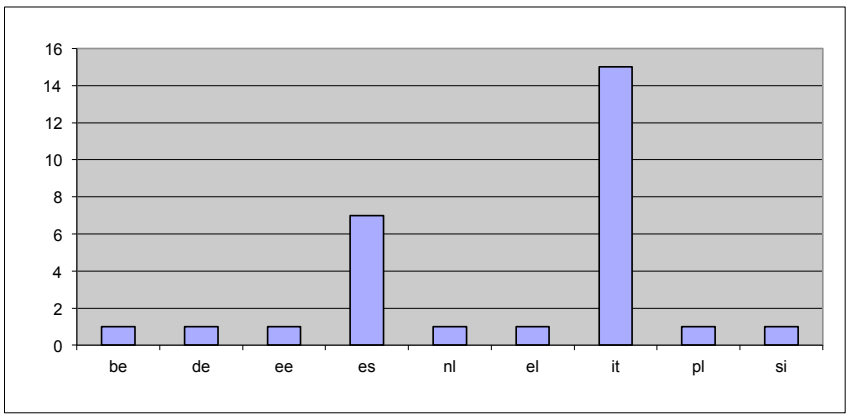
Number of projects: 29

CIPS 2011: 6.165.794,48€
CIPS 2012: 6.565.220,49€

Main areas of intervention (2011-2012)



Geographical distribution (2011-12)

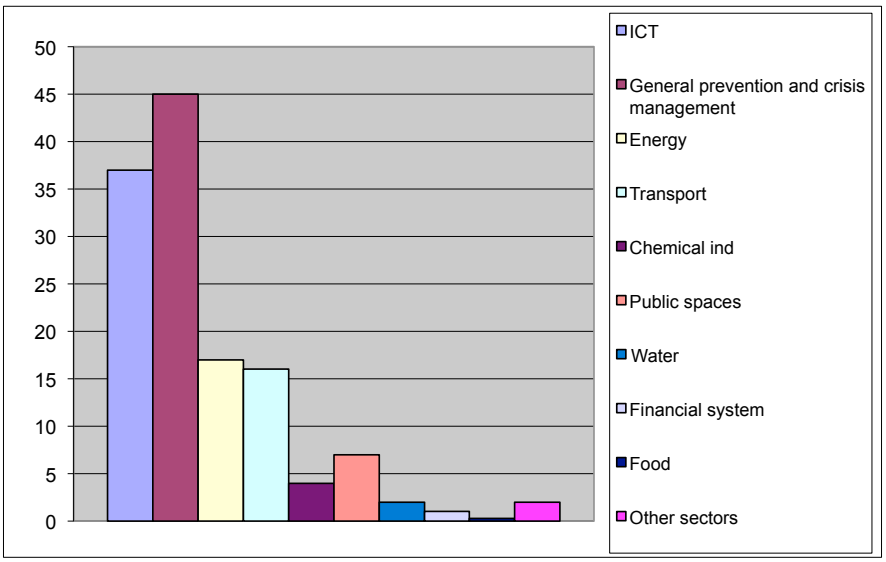


Funded projects 2007-2012

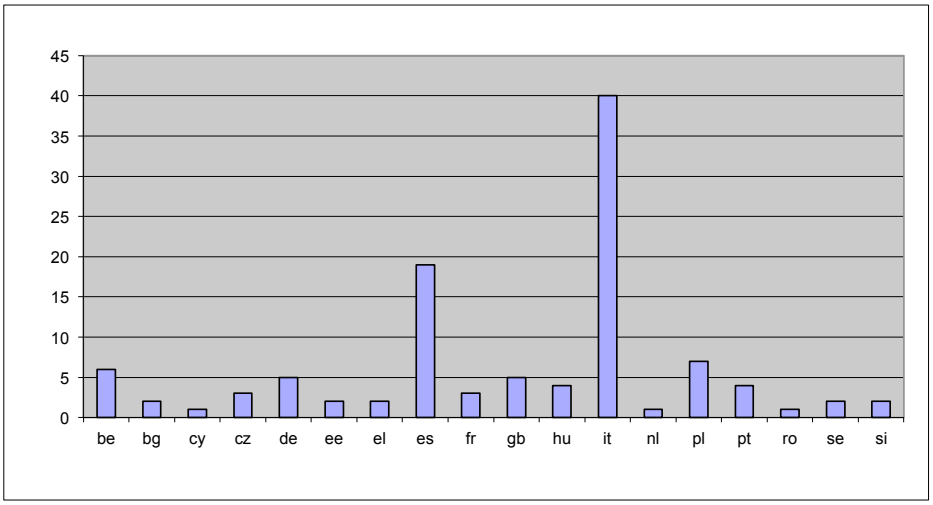
No of projects ±130

Total awarded amount:± 50 Mio/€

Main areas of intervention 2007-2012



Geographical distribution (2007-2012)



CIPS Research activities (Public Procurement)

Main elements	A **large number** of projects covering a wide range of **CI security topics**
	Mostly **national consortia** with extensive experience on security research
	Relatively **small** and **focused** projects

2008	• Terrorism related • Transport sector (inspired by 9/11, Madrid, London)
2009	• Cybersecurity, Internet • Exercises, Interdependencies
2010	• High level approaches – towards integration • Risk assessment, risk management, business continuity
2011	• ICT sector becomes more important • First elements of standardization
2012	• Smart-grids, cyber-physical convergence • Regional dimension

CIPS projects: Achievements

Main findings	Establishment of a CI research community with a mixture of policy makers, national authorities and researchers
	Tight links with national CI research – Transfer of knowledge
	Development of methodologies for specific topics
	Development of tools to be used by operators/ infrastructure owners
	No fundamental research – This is an FP7 (Horizon 2020) priority.

Collaborative Cyber/Physical Security Management System

Professor Nineta Polemi, University of Pireaus, Greece

Professor Polemi presented the issues related to the security of the commercial ports, including some basic concepts, the protection of the commercial ports, the security management w.r.t. the existing methodologies and their weaknesses when applied to the port infrastructures. Finally, she presented some initial results from the CYSM project.

University of Piraeus
Research Center, Greece

Collaborative Cyber/Physical Port Security Management

Associate Professor N. Polemi
University of Piraeus (Greece)–Dept. of Informatics
dpolemi@gmail.com
http://athina.cs.unipi.gr/security-lab/

Topics

- Basic Concepts
- Protecting Ports' CIIs
- Security Management
- CYSM initial results
- Conclusions

Basic Concepts

PIT System

Users/ Procedures
(internal, external, cargo, vessels)

Information/data
(marine, coastal, trade,..)

e/m-Services
(vessel, cargo, inland logistics, ..)

IT equipment / Software
(servers, navigation, RFIDs, cameras, ERPs, …)

Telecom
(networks, routers, optical fibers, ..)

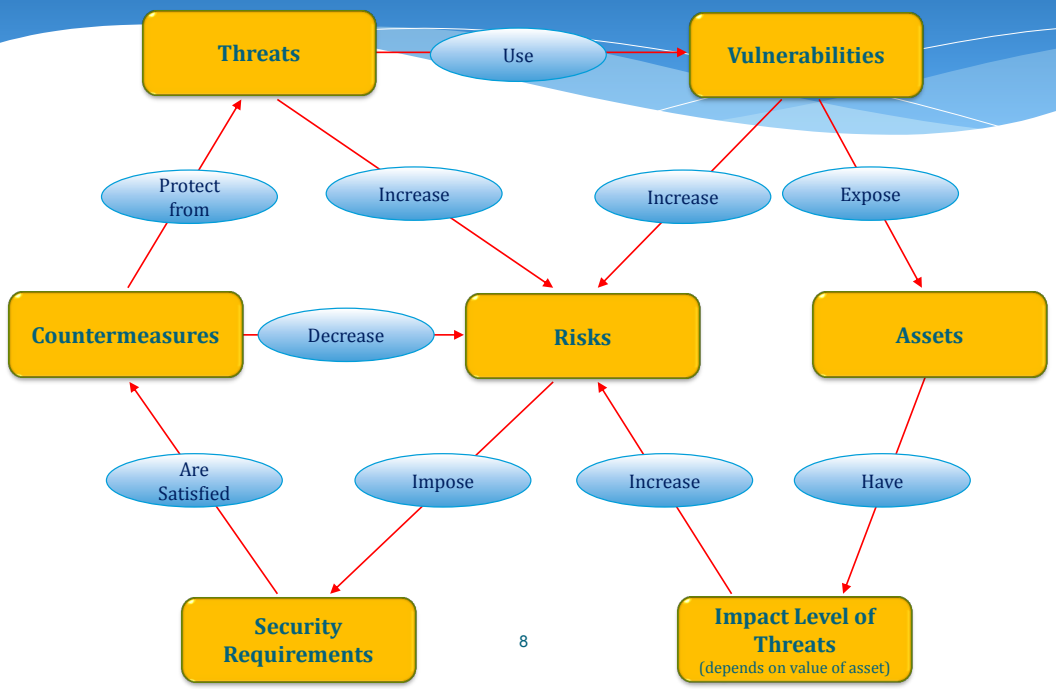
Infrastructure
(buildings, terminals, gates, data centers)

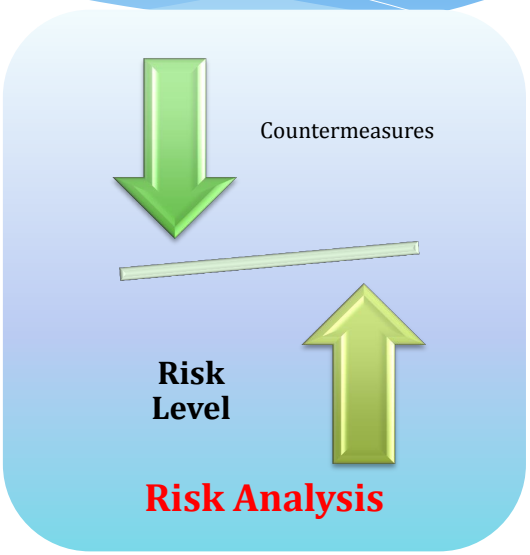
- **Security:** (cyber security): Ensure the Confidentiality, Integrity, Access Control, Availability of all assets in all layers of the IT system.
- **Safety (physical security):** Ensure the access control and availability of the assets in the two layers (1st, 6th).

Asset	Anything that has value to the organization
Threat **Threat level** **Impact level**	Potential cause of an unwanted incident, which may result in harm to the ICT system or the organization Frequency of occurrence Consequences of threat (if occurs)
Countermeasure/ Control	The action(s) (software, procedure, technique) to protect an asset from a threat
Vulnerability **Vulnerability level**	A weakness of an asset that can be exploited by the threat How much exposed is the asset(s) to the threat
Risk level	Combination of threat level, impact level and vulnerability level

Threats and attacks

- **Loss of Availability**
  - Denial of Service , wiretapping, key stealth, insertion, session hijacking, network routing, hidden channel
- **Loss of Integrity**
  - Key guessing, cryptanalytic attacks
- **Loss of Authenticity**
  - Unauthorized access, site impersonation
  - Client-System intrusion (viral infection, backdoor installation, infor-mation stealing, forged/unvoluntary user actions, command execution)
- **Loss of Confidentiality**
  - Espionage Personal, Corporate, National and Military
  - Data & Information Breach
- **Loss of Non-repudiation**
  - Key guessing, cryptanalytic attacks



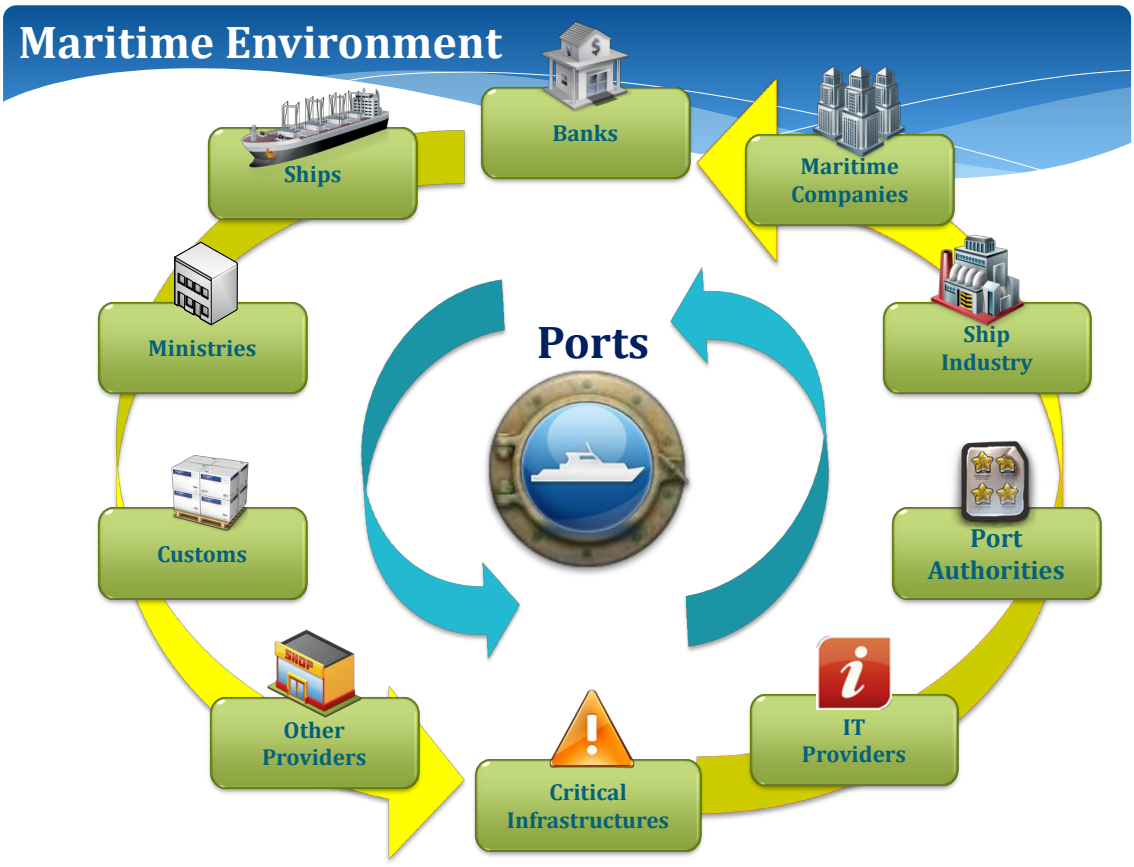


Protecting Ports' CII


Port of Valencia -Spain

The importance of Port Security

- **3.5 billion tonnes** of freight is loaded and unloaded in EU ports every year
- **400 million ferry** passengers are transported every year.
- **Port security breaches** cause serious economic damage to operators, and users throughout the supply chain. Supply chain related attacks has increased steadily over the past decade, reaching 3299 attacks in 2010 (PWC2013 report).
- In 2013 on the port of Antwerp allowed hackers to access secure data giving them the location and security details of containers causing the theft cargo.



Critical Information Infrastructure Protection (CIIP) :

Commercial ports are large-scale infrastructures hosting information systems that their degradation/interruption/impairment has serious consequences on national security, economy, health, safety or welfare of citizens.

-Commercial Ports are **transportation critical infrastructures** [Dept. of Homeland Security, USA, 2007]

-31 March 2011 on CIIP – "Achievements and next steps: towards global cyber-security" - COM(2011) 163

Examples of Cyber threats

Assets	Threats	Vulnerabilities	Impacts
e-reservation service	Loss of integrity	No PKI enable service	Disruption of reservations, economic +cascading effects
Navigation system	Unauthorised Data Access	Lack of logical access control and audit	Alteration of itineries
ERP	Malicious Code	Irregular update of Antivirus	Economic loses
RFIDs	Eavesdropping on RFID readers	The server does not share a private key with each tag	Commercial espionage

Examples of Countermeasures

Assets	Risk (Threats , Assets) >3	Countermeasures
e-reservation service	Loss of integrity	Strong authentication mechanism Digital Signatures
Navigation system	Unauthorised Data Access	Strong authentication and audit mechanisms
ERP	Malicious Code	Regular updates of Antivirus Create strong policy for opening email attachments
RFIDs	Eavesdropping on RFID readers	Cryptography for each RFID tag

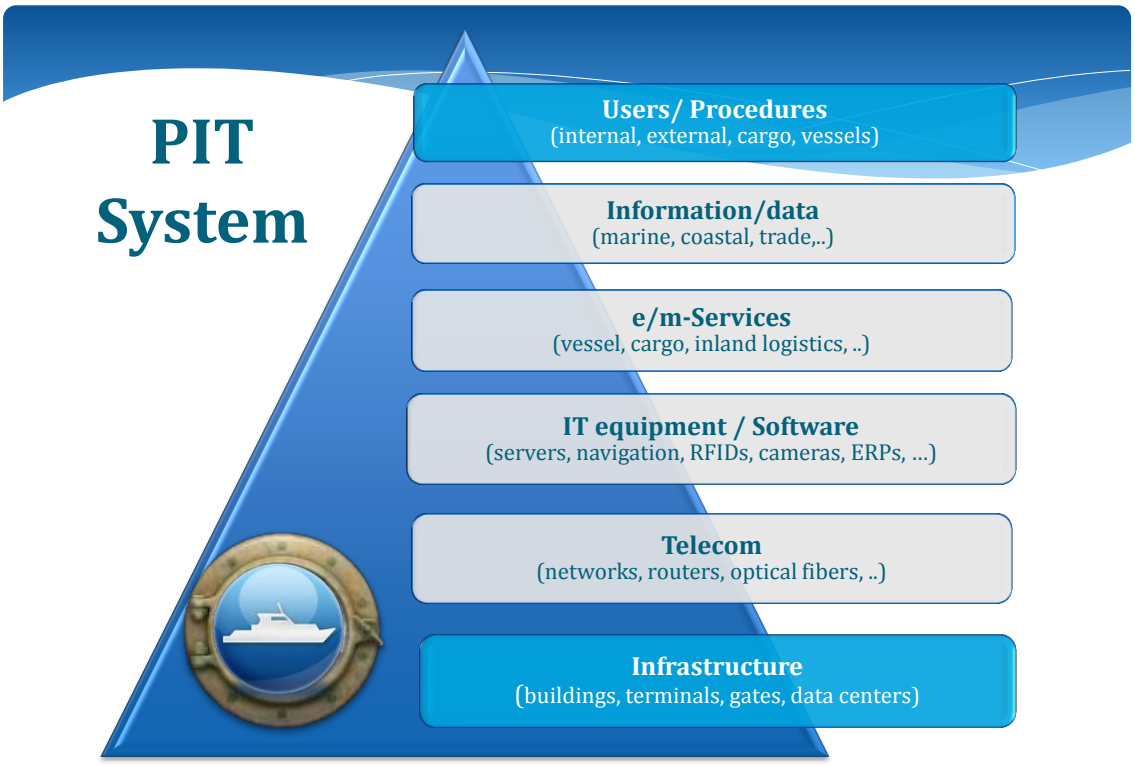
Existing Maritime Legislation

International Maritime Organization (IMO) published:

- **MARPOL** (e.g. MEPC.: 189(60), 190(60), Annex VI) for the **sea protection**
- **SOLAS** (e.g. MSc.: 286(86), 256(84), 46(66), 291(87), 216(82), 282(86), 291(87), 290(87)) for the **safety** of the ships, passengers and cargo and the **ISPS** addressing:
  - audit
  - secure access/handling of cargo
  - availability of telecommunication infrastructure
  - incident reporting
  - creation of security team
  - training

Existing Maritime Methodologies & Tools

- **MSRAM** and its extended version MSRAM-PLUS/FORETELL address only physical security and they are compatible with the ISPS
- **MARISA** concentrate on the safe navigation of ships during their presence in the port
- **CMA** detects abnormal behavior of ships and identifies respecting threats
- **National methodologies** (Estonia, Jordan , Russia) also concentrate only on the safety of ports



- Maritime Safety Approaches
  - cover only physical infrastructure
  - consider only physical threats and calculate physical related risk
  - they do not consider physical & cyber threats rising from their interdependency with the other maritime entities
  - the implementation of the ISPS code is left at national level i.e. there is not a standard providing the exact procedures and measures that need to be undertaken (e.g. like the ISO27002) in order for a port to become ISPS compatible.
  - are not user centric

Security Management Standards

•ISO/IEC 27001:2005 – Information technology – security techniques – information security management systems – requirements13

•ISO/IEC 27035:2011 (revising ISO/IEC TR 18044:2004) Information technology –security techniques – information security incident management Standards of individual Member States (for instance BSI)

•NIST SP 800-61 Computer security incident handling guide recommendations of the US Department of Commerce, National Institute of Standards and Technology

• CMU/SEI-2004-TR-015 Report on defining incident management processes forcomputer security incident response teams (CSIRTs).

- ICT Security Management Approaches
  - most of them are not supported by software tools.
  - rely on a plethora of questionnaires
  - they fail to capture the complexity of infrastructure interconnections, cross-sector impacts, dependencies with other systems or infrastructures and cascading effects within a sector or across sectors.
  - They are very generic, failing to provide targeted technical solutions that address specific sectoral (e.g. maritime) problems and threats e.g. interdependent threats rising from associated entities, sector-specific threats (e.g. weather conditions, strikes) and sector-specific legislation (e.g. ISPS in maritime environment).
  - limited collaborative abilities
  - primitive methods for evaluation, determination and mitigation of corporate risks.
  - ineffective procedures for the elaboration of the diverse knowledge that exists on large entities.

CIIP methodologies

- Agent-based simulation model of the U.S. economy(COMM-ASPEN)
- Electricity market complex adaptive system (EMCAS)
- Hazardous operations (HAZOP)
- Multi-network interdependent CI for analysis of lifelines (MUNICIPAL)
- National agent-based laboratory for economics (N-ABLE)
- Transportation routing analysis geographic IT system (TRAGIS)
- Urban infrastructure suite (UIS)
- Virtual Interacting Network Community (VINCI)

They cover energy, economy, transport (airports, railways NOT ports)

CYSM PROJECT

CYSM

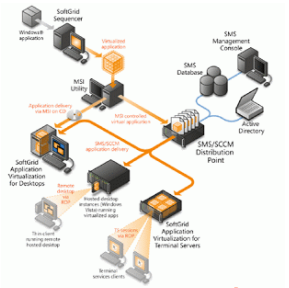
Consortium

Partner		Role
PORT INSTITUTE FOUNDATION OF STUDIES AND COOPERATION OF THE VALENCIA REGION (FEPORTS)		Project Coordinator
UNIVERSITY OF PIRAEUS RESEARCH CENTRE (UPRC)		Technical Manager
SINGULARLOGIC ANONYMOS ETAIRIA PLIROFORIAKON SYSTIMATON & EFARMOGON PLIROFORIKIS (SiLo)		Technical Partner
Università degli Studi di Genova (DITEN)		Technical Partner
Piraeus Port Authority S.A. (PPA)		Pilot
Valenciaport Foundation for Research, Promotion and Commercial Studies of the Valencian region (VPF)		Pilot
Port-of-Mykonos (POM) (subcontractor of SiLo)		Pilot

Security & Safety Management Approaches

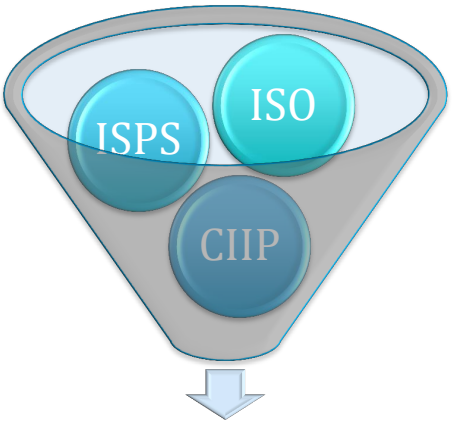
Critical Infrastructures Security Management Approaches

Maritime Safety Approaches



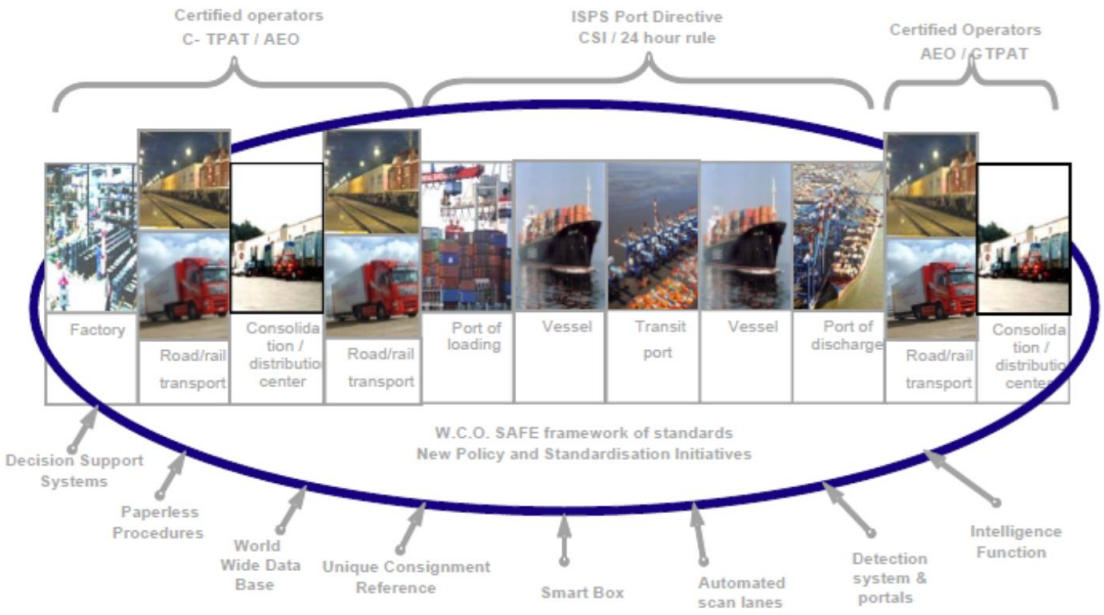
ICT Security Management Approaches

PORT SECURITY MANAGEMENT



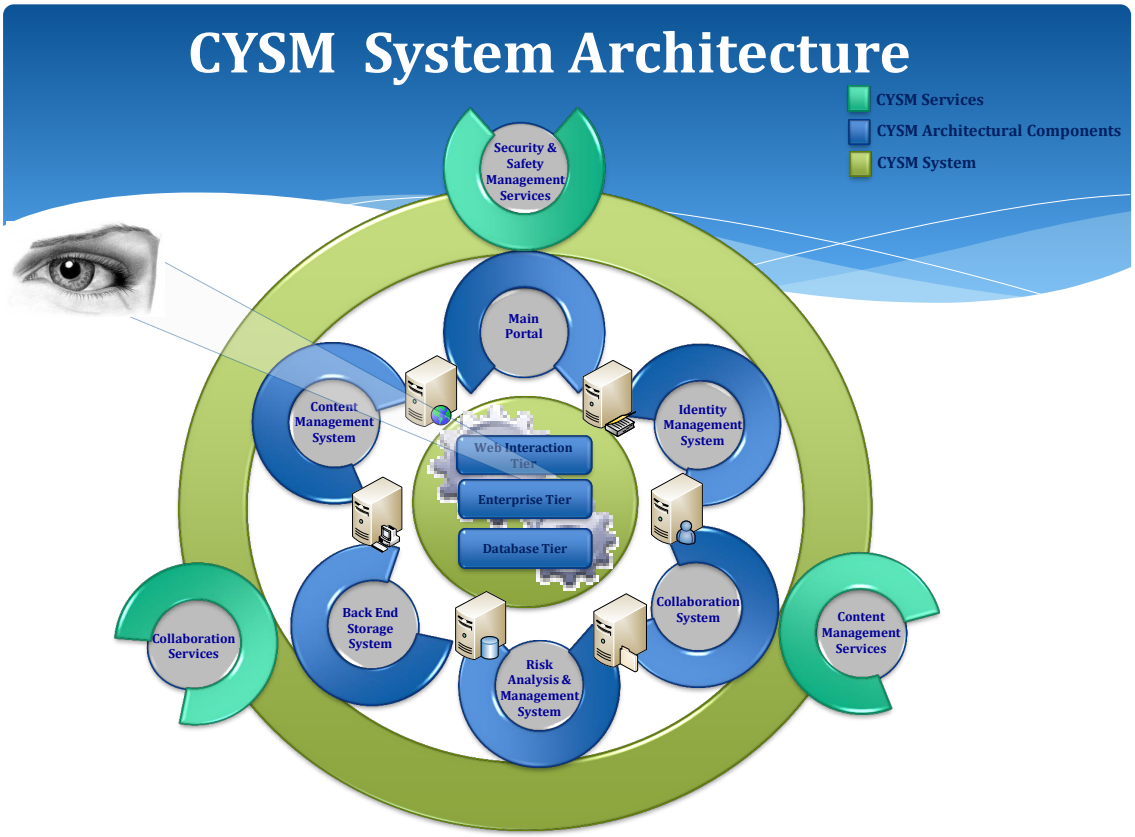
CYSM methodology

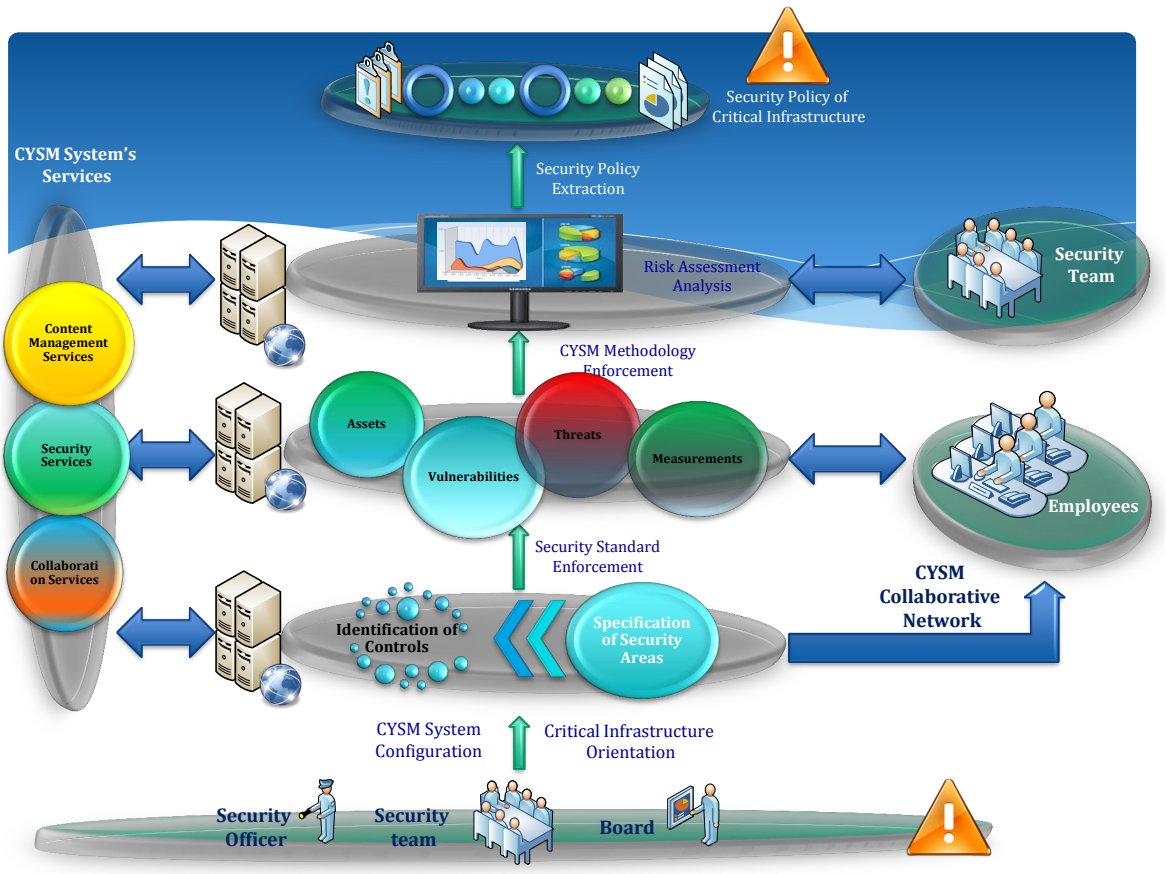
Well protected ports have an advantage in Global Supply Chains



CYSM Security Management methodology

- *Compatible with standards* (e.g. ISO27001, and ISPS code)
- *Multi-scope analytic*: Be able to perform risk analysis using different scopes
- *Collaborative:* Ensures collaboration among all ICT port users
- *Broad analytic:* Analyses sectoral, interconnected and interdependent threats
- *Time and resource economical:* Avoids the plethora of questionnaires and frustrating interviews with all participants
- *Accurate:* Derives accurate results
- *Good Functional requirements:* Needs to be clear for all actors involved, precise, and measurable
- *Easy to implement:* Easy to implement even for inexperienced users
- *Well documented:* All steps of the methodology can be documented in clear format with clear outcomes for each step
- *Responsibility centric:* Methodology has to be oriented to users' role


CYSM System Architecture
CYSM Services
CYSM Architectural Components
CYSM System
Security & Safety Management Services
Main Portal
Content Management System
Identity Management System
Web Interaction Tier
Enterprise Tier
Database Tier
Back End Storage System
Collaboration System
Collaboration Services
Content Management Services
Risk Analysis & Management System


Security Policy of Critical Infrastructure
CYSM System's Services
Security Policy Extraction
Risk Assessment Analysis
Security Team
Content Management Services
CYSM Methodology Enforcement
Assets
Threats
Vulnerabilities
Measurements
Security Services
Employees
Collaboration Services
Security Standard Enforcement
CYSM Collaborative Network
Identification of Controls
Specification of Security Areas
CYSM System Configuration
Critical Infrastructure Orientation
Security Officer
Security team
Board

Conclusions

Port of Carrara-IT

- **(Sector-specific) Risk assessment methodologies** and tools addressing the complexity/distribution of ICT systems are needed;
- Ports are major service providers however they do not adopt “Good ICT-security and privacy practices” (ENISA 2011, 2012);
- **Harmonised security management practices** requires collaboration (e.g. United Nations, IMO, EMSA, IALA, SMDG, ITIGG, PROTECT, DG-MOVE);
- Not new standards are needed, we only need **targeted SM methodologies** compliant with: ISPS code, ISO and CIIP standards;
- **CYSM results** will contribute towards a holistic approach to port security.

Special Session

"Secure and Sustainable maritime digital environment"

within The Fifth International Conference on
Information, Intelligence, Systems and Applications (IISA 2014)
(http://iisa2014.unipi.gr/)

July 07th 2014
Chania Crete, Greece

SHORT HISTORY The maritime sector is critical in terms of economic activities and commercial impact especially under the current economic turmoil. An enhanced, sustainable maritime digital environment has to rely on well protected and advanced facilities, secure ICT infrastructure and innovative technologies as well as trustworthy e/m-maritime services.

Session Chair

-Associate Professor Nineta Polemi, University of Piraeus, Department of Informatics

Program Session Committee

-Dr David Incertis
The Port Institute for Studies and Co-Operation in the Valencian Region – FEPORTS

- DI Dr. Markus Clabian
AIT Austrian Institute of Technology GmbH

SCOPE: The workshop aims to bring together all maritime scientists, developers, operators and stakeholders in order to address challenges and propose solutions which will lead to a secure, sustainable and competitive maritime digital market leading to its trustworthiness, internationalization and growth.

The *main topics* that this special session will cover are:

- ✓ Port Security
- ✓ Innovative, secure e/m-port services
- ✓ Privacy aware e/m-maritime services
- ✓ Automated Board Control Systems (ABCs)and biometric passports
- ✓ Secure Port Community Systems
- ✓ Green Ports
- ✓ Trustworthy maritime logistics

Thank you

Security Liaison Officer

Mr. Alessandro Lega, Universita Campus Bio-Medico di Roma, Italy

Mr. Lega gave an overview on the SLO project, which aims to develop a full job description for the Security Liaison Officer, the person responsible to facilitate the connection between the designated European Critical Infrastructures and the National authorities. The presentation included the project summary in terms of the deliverables and the methodology that has been established for their realization, the progress of the project, some preliminary results and the future actions.

The question that followed the presentation was what the added value of this project would be, since there are ISO standards which define in detail the duties and responsibilities of the Security Manager. The reply of Mr. Lega was the role of the Corporate Security Officer is indeed defined within companies. However the Liaison Officer should be a person who will link the organizations with the public authorities, in order to avoid any conflict of interest. Finally, he mentioned that the above mentioned standards for the security management are currently under revision.

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Home Affairs

Establishing a common profile for the SLO position

www.slo-project.eu
info@slo-project.eu

JRC CIPS 3rd Workshop
Brussels, 12 November, 2013

SLO project

Main issue of the project:

WHO SHOULD BE THE SECURITY LIAISON OFFICER?

Why is the SLO project necessary?

According to the EU Directive 114/2008/EC:

"Security Liaison Officers (SLO) should be identified for all designated ECIs in order to facilitate cooperation and communication with relevant national critical infrastructure protection authorities. With a view to avoiding unnecessary work and duplication, each Member State should first assess whether the owners/operators of designated ECIs already possess a Security Liaison Officer or equivalent. Where such a Security Liaison Officer does not exist, each Member State should take the necessary steps to make sure that appropriate measures are put in place. It is up to each Member State to decide on the most appropriate form of action with regard to the designation of Security Liaison Officers."

**** Although the Directive outlines the need for such a critical position, it does not define the parameters surrounding the SLO or "equivalent" position.***

SLO project

Partners:

UCBM
University
Campus Bio-Medico
of Rome (Italy)

ARPIC
Romanian Association for
Critical Infrastructures and
Services Protection
(Romania)

Associate partners:

AIIC
Italian Association of
Critical Infrastructure
Experts (IT)

BCManager
Italian Association of
Business Continuity
Manager (IT)

ASIS International
Italian Chapter (IT)

Transelectrica
Romanian TSO (RO)

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
www.unicampus.it

Why is the SLO project necessary?

Within Critical Infrastructure organizations in the EU community, the role of the SLO remains an extremely fluid concept.

Through identification of the static standards amongst Security Managers who operate within European Critical Infrastructures

And subsequently performing gap analysis,

This research aims to identify a framework for the Security Liaison Officer (SLO) position as mandated by Article 6 of the EU Directive 2008/114/EC.

How to define the SLO position

CURRENT ROLE OF THE SECURITY

- Open Source Documents
- Questionnaires
- Interviews

OPTIMUM ROLE OF THE SLO

CAFÉ WORKSHOPS (BUCHAREST, ROME, BRUSSELS)

FRAMEWORK TO SHAPE THE SLO POSITION

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
www.unicampus.it

Project Summary: Analysis of SLO and SCM profiles

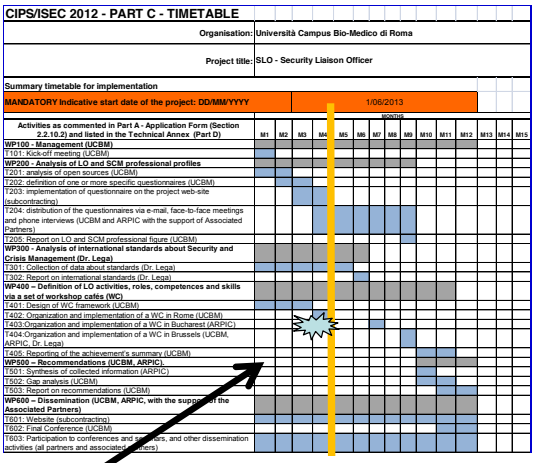
OUTPUT:
Deliverable 1: Analysis of SLO and Security and Crisis Manager (SCM) professional profiles

Analysis of open sources	To analyse the profile of SLO and SCM in the literature, to better understand how to proceed to the other activities of the WP and of the whole project	Month1-2	State of the role of SLO and SCM
Creation of four specific questionnaires	To define questionnaires (Public Authorities, Head of Security Depts., CSO or equivalent and Academia) to obtain more data than in literature and to facilitate the discussion during the workshops and the final results of the project	Month2-3	Template of the questionnaire with compilation guideline
Implementation of questionnaire on the project web-site (subcontracting)	Implementation of the questionnaire (and of the compilation guideline) on the project web-site and definition of how to insert and retry data	Month3-4	A web-based platform to fill in questionnaires and to manage the elicit knowledge
Distribution of the questionnaires via e-mail, face-to-face meetings and phone interviews	To collect data about the actual professional figure of SLO and SCM	Month4-12	A set of filled questionnaires able to support the characterisation of SLO and SCM
Report on SLO and SCM professional figure	Summarize the results of the performed analysis	Month9	Report on collected data

Project Scheduling

Start date: June 2013
Duration: 12 months

- ✓ Defined (4) questionnaires
- ✓ Started distribution of the questionnaires (just collected 10 questionnaires)
- ✓ Set-up the project website
- ✓ Started collection (and analysis) of public documents
- ✓ Performed the first cafe workshop
- ✓ Set-up an advisory board (AB)
- ✓ Performed the first meeting of the AB
- ✓Started dissemination activities


CIPS/ISEC 2012 - PART C - TIMETABLE

Organisation: Università Campus Bio-Medico di Roma

Project title: SLO - Security Liaison Officer

Summary timetable for implementation

MANDATORY Indicative start date of the project: DD/MM/YYYY 1/06/2013

months

Activities as commented in Part A - Application Form (Section 2.2.10.2) and listed in the Technical Annex (Part D)	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15
WP100 - Management (UCBM)															
T101: Kick-off meeting (UCBM)															
WP200 - Analysis of LO and SCM professional profiles															
T201: analysis of open sources (UCBM)															
T202: definition of one or more specific questionnaires (UCBM)															
T203: implementation of questionnaire on the project web-site (subcontracting)															
T204: distribution of the questionnaires via e-mail, face-to-face meetings and phone interviews (UCBM and ARPIC with the support of Associated Partners)															
T205: Report on LO and SCM professional figure (UCBM)															
WP300 - Analysis of international standards about Security and Crisis Management (Dr. Lega)															
T301: Collection of data about standards (Dr. Lega)															
T302: Report on international standards (Dr. Lega)															
WP400 – Definition of LO activities, roles, competences and skills via a set of workshop cafés (WC)															
T401: Design of WC framework (UCBM)															
T402: Organization and implementation of a WC in Rome (UCBM)															
T403:Organization and implementation of a WC in Bucharest (ARPIC)															
T404:Organization and implementation of a WC in Brussels (UCBM, ARPIC, Dr. Lega)															
T405: Reporting of the achievement's summary (UCBM)															
WP500 – Recommendations (UCBM, ARPIC).															
T501: Synthesis of collected information (ARPIC)															
T502: Gap analysis (UCBM)															
T503: Report on recommendations (UCBM)															
WP600 – Dissemination (UCBM, ARPIC, with the support of the Associated Partners)															
T601: Website (subcontracting)															
T602: Final Conference (UCBM)															
T603: Participation to conferences and workshops, and other dissemination activities (all partners and associated partners)															

We are at the end of the 4th month

Bucharest , 11 October 2013

Advisory Board

An Advisory Board (AB) has been set-up to support the project team in the definition of the questionnaires and to operate as a “door-opener” within specific communities

Contributes in dissemination activities and for specific tasks

Performed the first AB meeting in Rome on June 5th 2013

AB is composed by representatives of Associated Partners

- Adrian Vâlciu (Transelectrica, Romania)
- Sandro Bologna (AIIC, Italy)
- Francesco Lambiase (BCManager, Italy)

And by external experts representative of different CI sectors

- Marko Sukilovic (ASIS International)
- Francesco Di Maio (ENAV, Italy)
- Umberto Saccone (ENI, Italy)
- Laura Barettini (Odgers Berndtson)
- Maria Giovannone (ANMIL, Italy)
- Fabrizio Sechi (Fastweb, Italy)

Project Summary: Analysis of International standards about Security and Crisis Manager

OUTPUT:
Deliverable 2: Survey on international standard about the professional figure of Security and Crisis Manager (SCM)

Collection of data about standards	To collect the different standard existing about the professional figure of SCM	Month 1-5	Identification and classification of the different standards related with SCM
Report on international standards	To critically summarize the International standards related with SCM	Month 6	Survey of the most relevant international standards about SCM

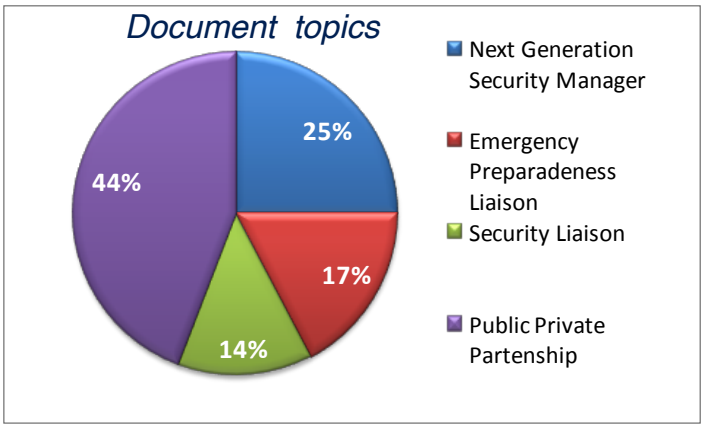
Project Summary: Definition of SLO activities, roles, competences and skills via a set of workshop cafés

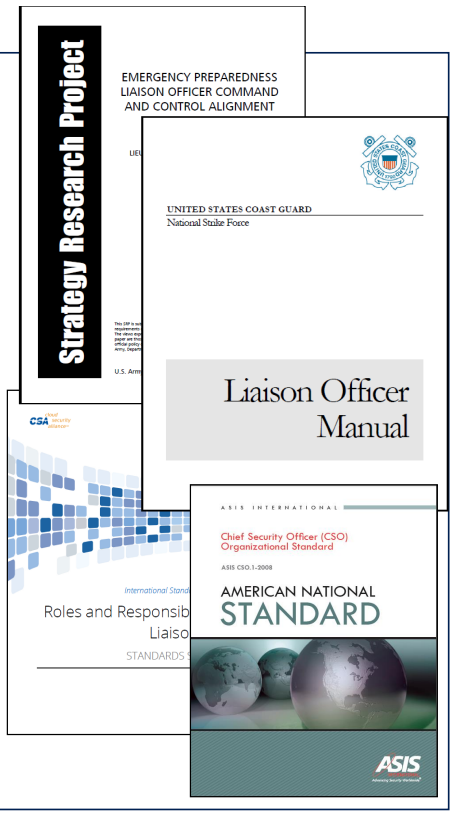
OUTPUT:
Deliverable 3: Report on SLO desideratum profile

Design of Café Workshop (CW) framework	To design the CW in terms of methodologies, questions, material, and logistic aspects	Month 1-3	guideline on CW
Organization and implementation of a CW in Bucharest	Perform a CW	Month 4	summary of the CW
Organization and implementation of a CW in Rome	Perform a CW	Month 7	summary of the CW
Organization and implementation of a CW in Brussels	Perform a CW	Month 9	summary of the CW
Reporting of the achievement's summary	To synthetize the results of the 3 CW's	Month 11-12	Report on information collected via the CW's

Open document analysis

Analyzed about 100 documents about SLO and related aspects



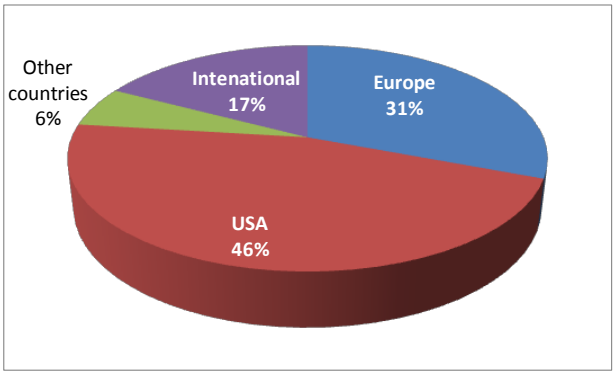


Open document analysis

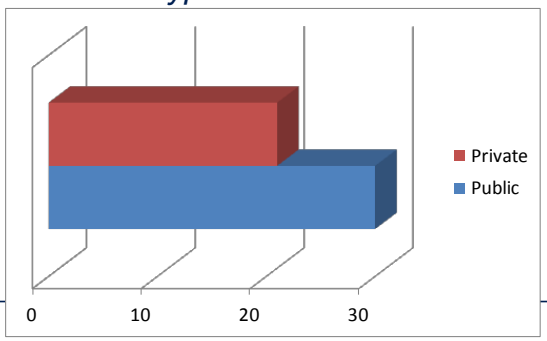
To implement effective CIP strategies

- Private-Partnership cooperation is assumed as one of the key elements
- Information sharing is an important aspect both between public and private, but also among private operators (no-sector limited)
- Information sharing (technological) platforms are useful for early alerting (pre-event), and lessons learned (post-event)
- a central aspect is the **notation of trust** and specifically face-to-face knowledge & trust

Source geographical distribution

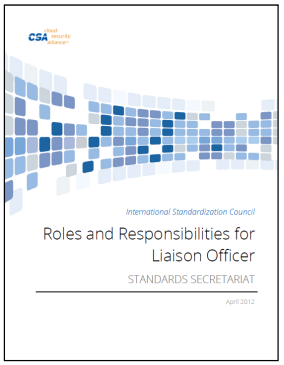


Type of document



Open document analysis

- There are some attempts to standardize the Liaison Officer figure
- Large part of material from US (and military field)
- In US the National Infrastructure Advisory Council (NIAC) is comprised of 30 members selected among Chief Executive Officers



A liaison officer is a person that liaises between two organizations to communicate and coordinate their activities by serving as an official go-between for senior officials of both organizations

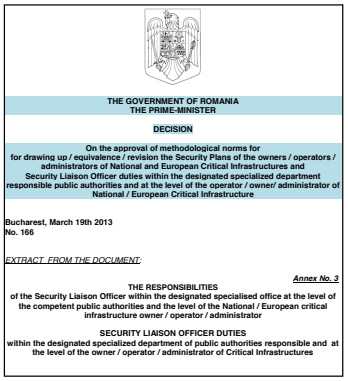
Today in Europe there is no legislative or regulatory document to specify the figure of SLO

Open document analysis

Romania has setup a Government Decision regarding SLO
(n. 166 March 18th 2013 – Annex 3)

The Security Liaison Officer (SLO) is the head of the specialised compartment (comprising at least a three man team) designated at the level of the competent public authorities or the level of the National / European critical infrastructure owner / operator / administrator, and is under the direct authority of the leader of the competent public authorities, respectively that of the National / European critical infrastructure owner / operator / administrator. He is also:

The person responsible for activities in the field of Critical Infrastructure Protection /head of compartment, at the level of the competent governing body;
The head of compartment, specialising in National / European Critical Infrastructure Protection, at the level of the National / European critical infrastructure owner / operator / administrator.



THE GOVERNMENT OF ROMANIA
THE PRIME-MINISTER

DECISION

On the approval of methodological norms for
for drawing up / equivalence / revision the Security Plans of the owners / operators / administrators of National and European Critical Infrastructures and
Security Liaison Officer duties within the designated specialized department responsible public authorities and at the level of the operator / owner/ administrator of National / European Critical Infrastructure

Bucharest, March 19th 2013
No. 166

EXTRACT FROM THE DOCUMENT:

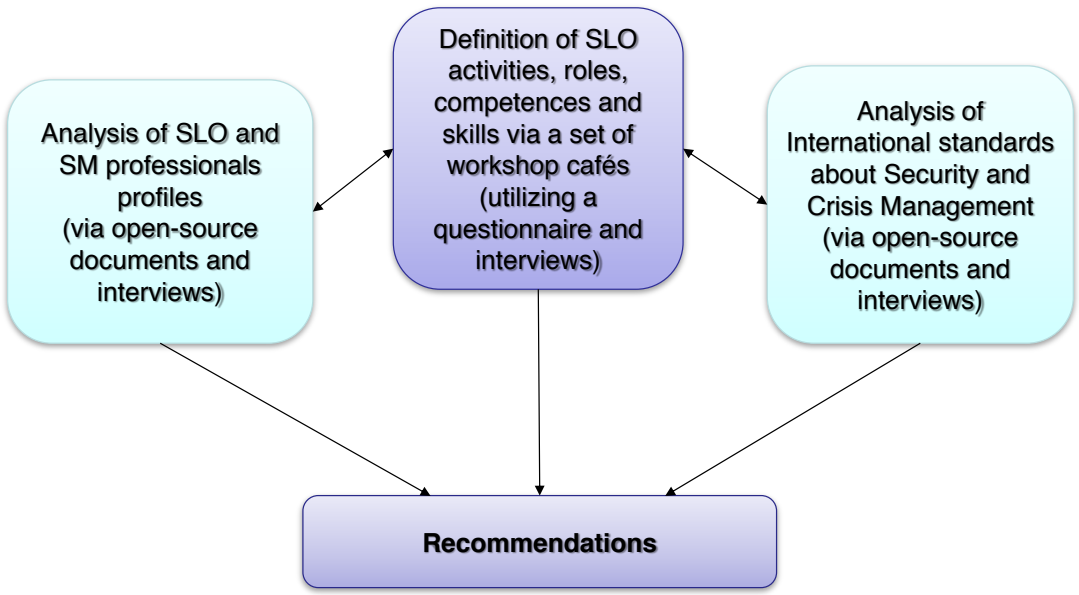
Annex No. 3

THE RESPONSIBILITIES
of the Security Liaison Officer within the designated specialised office at the level of the competent public authorities and the level of the National / European critical infrastructure owner / operator / administrator

SECURITY LIAISON OFFICER DUTIES
within the designated specialized department of public authorities responsible and at the level of the owner / operator / administrator of Critical Infrastructures

It specifies the SLO competences, separately, those of Public Authorities SLO from those of SLO operating in private National or European Critical Infrastructures

Project chart



Questions to be Answered

Who is the SLO? Which are his/her competencies, rules, background?

Which should be his/her position inside the organization?

What roles and responsibilities should the SLO position entail (before, during and after crisis scenarios)?

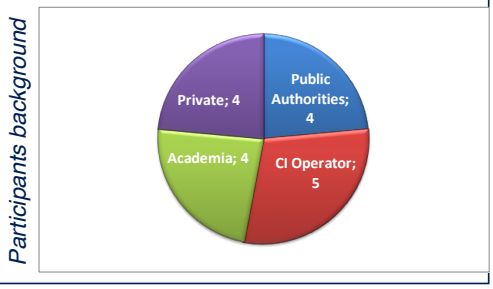
Café Workshop

First Café Workshop, Bucharest
11th October 2013

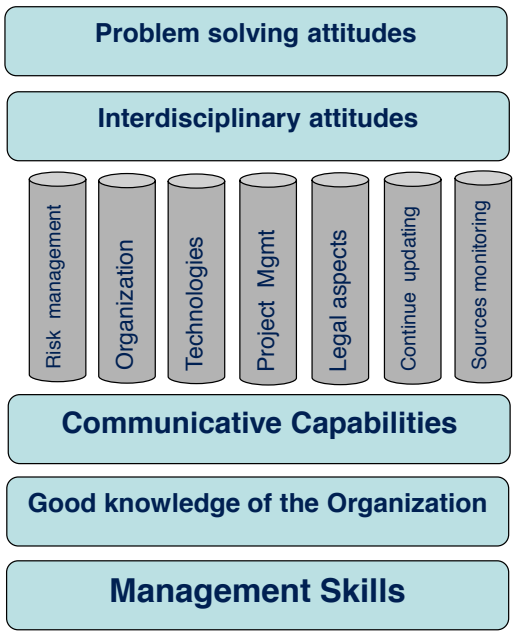
The 18 participants were divided into 3 groups with each group assigned a specific topic:
- SLO background
- SLO operational role
- SLO tasks

After 2 hours of constructive discussion, each group shifted to a new room with a new topic (with the aim that no one discussed the same topic twice).

The SLO project team operated as facilitators for each group.



Preliminarily Results



SLO should have clearly articulated skills and experience

SLO should primarily be a coordinator/facilitator able to effectively communicate inside and outside the organization

SLO should have a strong competence on his own organization and his sector; along with knowledge regarding other sectors, technologies and legislations

SLO should have experience in management (former experience in law-enforcement or military field might be useful, but not mandatory)

A mandatory continuing training process should be aligned with context changes

A very strong relationship with PA and other equivalent (international) professionals is crucial

Preliminarily Results

SLO should have visibility on ALL security aspects

✓ SLO should directly report to CEO

✓ When located inside the Security Dept., the SLO should fall under an independent inside office

✓ The SLO should serve as a P.O.C. for sharing information between Critical Infrastructures

✓ The SLO should have strong autonomy with a bottom-up and top-down information sharing system

Open Questions ?

Which is the role of the SLO during a crisis ?

Active management – POC of emergency

Not involved (no operational role)

This has emerged as a crucial point.

This choice depends on his collocation inside the organization, his operational role, and more importantly, his dependencies with PA, starting from the identification process.

How should the SLO be nominated from?

- ✓ Autonomously by ICE
- ✓ Autonomously by ICE (compliant with SLO professional prescriptions)
- ✓ Indicated by ICE and nominated by PA
- ✓ Nominated directly by PA

Project Timeline Structure

- June 2013 • "Kick-Off" meeting – Rome, Italy
- Oct 2013 • Café Workshop I - Bucharest, Romania
- Jan 2014 • Café Workshop II – Rome, Italy
- March 2014 • Café Workshop III – Brussels, Belgium
- April 2014 • ASIS Conference presentation in the Hague
- June 2014 • Final Conference – Rome, Italy

Preliminarily Results

"Kick-off" Meeting – Rome, IT (June 2013)

- The Questionnaire to be utilized for the project (constructed from open source documents and operational expertise) was disseminated and analyzed by the group.
- Some of the main aspects discussed: Bureaucracy, utilizing a 'whole person concept', focusing on peculiarities of security standards to analyze their potential added value, Public- Private understandings of the SLO profile, and differentiating between SLO and Security Manager.

Café Workshop I – Bucharest, RO (October 2013)

- The meeting focused on three separate elements of the SLO profile: Skills, Operational Role and Tasks. These elements were analyzed and resulted in numerous innovative ideas and future elements for consideration. Further, the group discussed novel vulnerabilities stemming from the implementation of dramatically differing policies. The Questionnaire was also critiqued by participating members in order to improve results and increase efficiency.

SLO project website

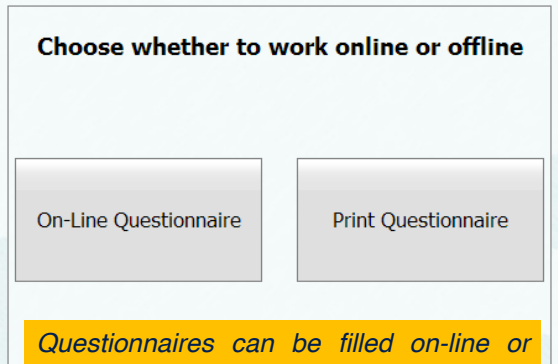
http://www.slo-project.eu/

There are **4** different questionnaires based on the role of the responder:

- Public Authority
- Head of Security Department
- Security Officer
- Academia/Expert

Questionnaires at:

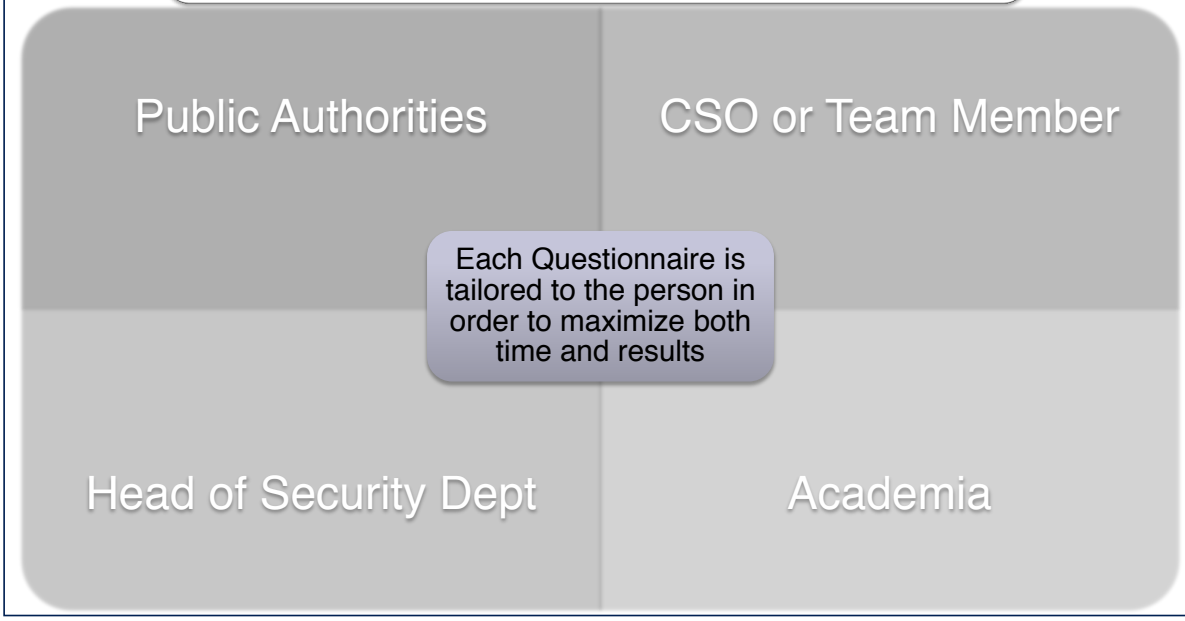
http://survey.slo-project.eu/



Questionnaires can be filled on-line or printed and filled out by hand (and returned via mail). Time required is an estimated 20 minutes.

Questionnaire Setup

There are 4 distinctly different Questionnaires – Prior to beginning the questionnaire, the user selects which category they fall under and are directed accordingly



Project Progress

- The Questionnaire has been completed by roughly two dozen select participants in an effort to garner feedback
- The web designer is continuing to tweak the design of the questionnaire to increase flow and efficiency
- The final product should be available by mid-November
- We expect to form substantive findings by the end of March 2014 (however, we will be accepting the submission of questionnaires until the end of May)

Whats Next?

- The hope of the project is to provide the EU with a practical framework that can be unanimously applied
- Understanding the differing needs and perspectives of each EU country, the framework provided should be rigid yet pliable in its application to each country (also taking into consideration Public-Private Partnership)
- We do not foresee the results of the SLO project providing a new standard for EU countries to adhere to; this project is aiming to sharpen an existing standard through novel recommendations via multiple disciplines (both theoretical and operational sides are exploited for this research project)

SLO Project: Dissemination- July 2014

The consortium will largely disseminate the results of the project to the scientific community, public authorities and to public and private operators and institutions, exploiting also the support of ARPIC, AIIC, ASIS Italy, BCManager, and Transelectrica.

Website (sub-contracting)	To disseminate project activities and results, to create an online form for questionnaires, to allow file sharing in a private area to project partners	Month 1-12	A website containing information on the project and online questionnaire forms and a private area for project partners
Final Conference	To illustrate to MS, CI, media and scientific community the results of the project	Month 11	
Participation to conferences and seminars, and other dissemination activities	To advertise SLO project and to illustrate preliminary and final results of the project	Month 1-12	Scientific and popular papers, lectures, etc.

http://www.slo-project.eu/

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
www.unicampus.it

Threat-Vulnerability Path Identification for Critical Infrastructures Compilation of a comprehensive all hazards catalogue for critical infrastructure

Professor Paolo Trucco, Politecnico di Milano, Italy

Professor Trucco gave a presentation on the THREVI project, which is defined as the Threat - Vulnerability Path Identification for Critical Infrastructures - Compilation of a comprehensive and dynamic all-hazards catalogue for critical infrastructure. The presentation included the aims and the results of the project, the objectives of the Consortium, information on hazards and threat modeling, interdependencies modeling and future actions. The discussion that followed included some technical points (whether the tool has a regional dimension). Responding to where this program fits with respect to DG HOME priorities, it was clarified that it fits to "Prevention" pylon of CIPS.

THREVI² Project

Compilation of a comprehensive and dynamic all-hazards catalogue for critical infrastructure

Prof. Paolo Trucco
Department of Management, Economics
and Industrial Engineering
Politecnico di Milano

III CIPS Workshop - Brussels, 12 November 2012

EUROPEAN COMMISSION
DIRECTORATE-GENERAL HOME AFFAIRS
Directorate A : Internal Security

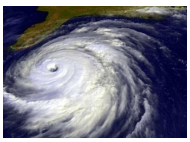
Agenda

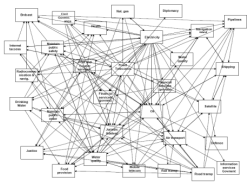
Threat - Vulnerability Path Identification for Critical Infrastructures

- Aim and Results
- Objectives and Consortium
- Hazards and Threat Modelling
- CI System and Interdependency Modelling
- SW Tool
- Next steps

THREVI² aim and scope

Threat - Vulnerability Path Identification for Critical Infrastructures



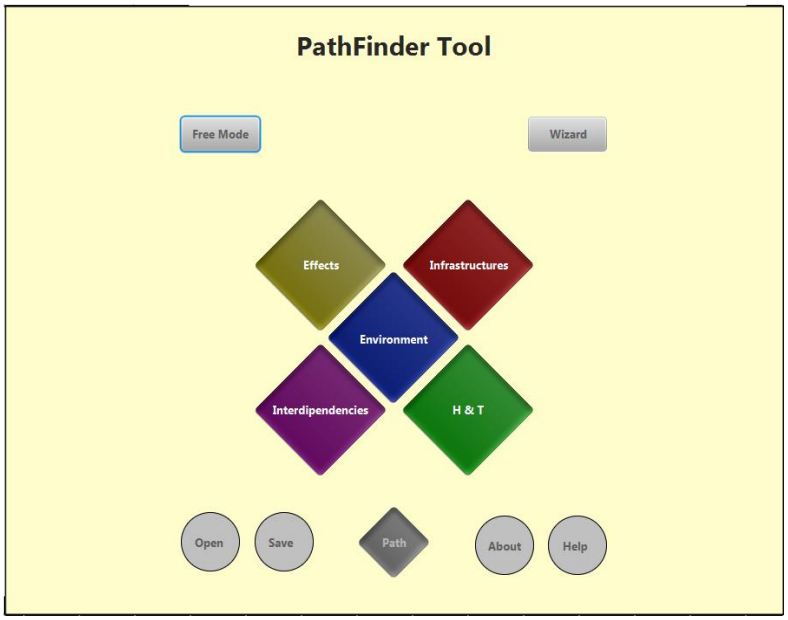


Key issues and needs in CI Risk Assessment:

- How to practically apply an all hazards approach to large CI systems ?
- How to account for and characterise main vulnerabilities of CI systems as well as cascading effects between interdependent CI?
- How to identify types of potential impacts and consequences with regard to a wide spectrum of targets?

THREVI² main result

Threat - Vulnerability Path Identification for Critical Infrastructures



- **Topologies of different CI systems**
- **Internal and external CI interdependencies**
- **Specification and modelling of hazards and threats**
- **Environmental conditions**
- **Multiple targets and Effects**

CASCADING MECHANISMS (Paths)

Intended beneficiaries and applications

THREVI²
Threat - Vulnerability Path Identification for Critical Infrastructures

	Public Authorities	CI Operators	Other Businesses
CIP Governance and PPP implementation	▪ CI specification ▪ CI impact assessment ▪ Information sharing	▪ Vital node analysis ▪ Vulnerability and Interdependency analysis	▪ Vulnerability analysis
Land use planning	▪ CI impact assessment ▪ Societal risk assessment		
CI systems design and operations	▪ Design review ▪ Certification ▪ Auditing	▪ Resilience engineering	▪ Resilience engineering
Emergency Planning	▪ Design and audit of Emergency Plans ▪ Training and exercise	▪ Training and exercise ▪ Business continuity planning	▪ Business continuity planning

THREVI² objectives

THREVI²
Threat - Vulnerability Path Identification for Critical Infrastructures

- Developing a **comprehensive and multi-dimensional all-hazards catalogue** for critical infrastructures by:
  - a (sub-)ontology for Hazards and Threats;
  - a (sub-)ontology for physical and functional topologies of Critical Infrastructures and their interdependencies;
  - merging them through vulnerability models

- Developing a software tool (**PATHFINDER**) to support the analyst in generating a **set of relevant disruption scenarios**.

THREVI² consortium

Threat - Vulnerability Path Identification for Critical Infrastructures

NIER Ingegneria S.p.A (NIER) – *Coordinator*

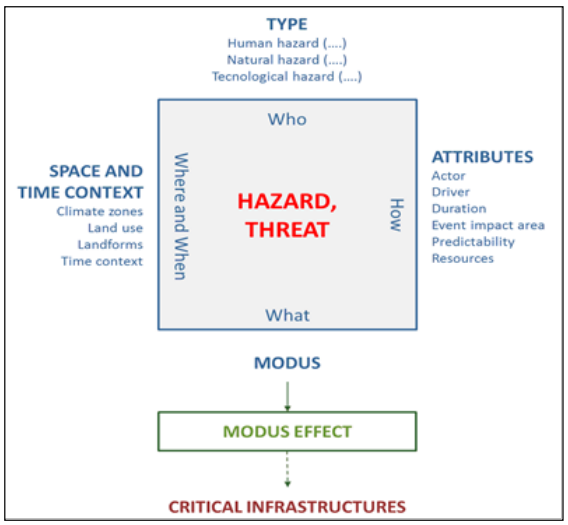
RGS S.r.l., Risk Governance Solutions (RGS)

Politecnico di Milano, Department of Management, Economics and Industrial Engineering (POLIMI)

Università Campus Bio-Medico di Roma - Faculty of Engineering (UCBM)

Hazard & Threat Ontology

Threat - Vulnerability Path Identification for Critical Infrastructures



Who?
Events Type sub-ontology; the first level identifies three main super-classes: natural, human and technological hazards.

How the hazard can occur?
Hazard attributes sub-ontology.

What action are triggered by the hazard?
"Modus" and "Modus effect" concepts are introduced to describe the impact mechanism.

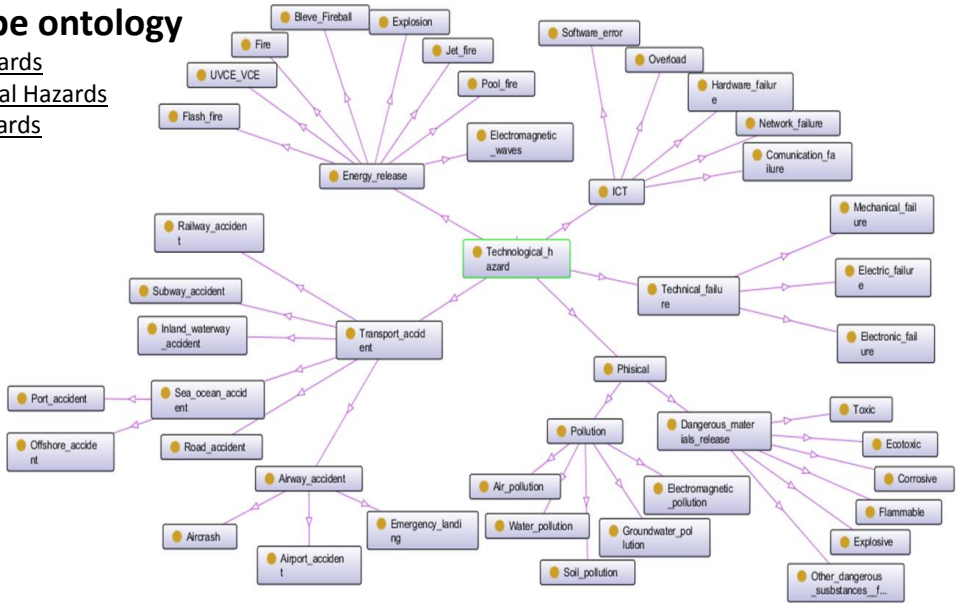
Where and when the hazard can occur?
Spatial and temporal attributes sub-ontology.

Hazard & Threat Ontology

THREVI²
Threat - Vulnerability Path Identification for Critical Infrastructures

Event Type ontology

☑ Natural Hazards
☑ Technological Hazards
☑ Human Hazards

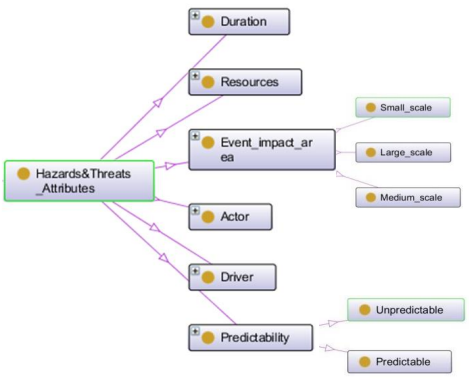


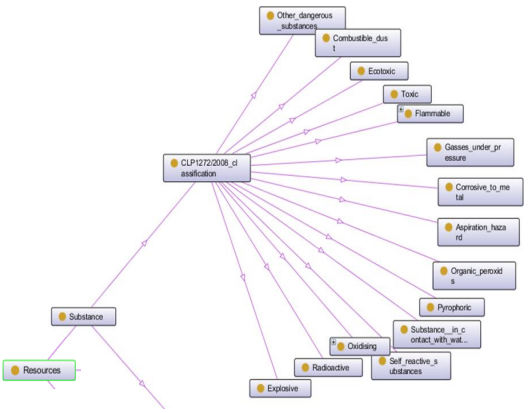
Hazard & Threat Ontology

THREVI²
Threat - Vulnerability Path Identification for Critical Infrastructures

Hazard attributes sub-ontology

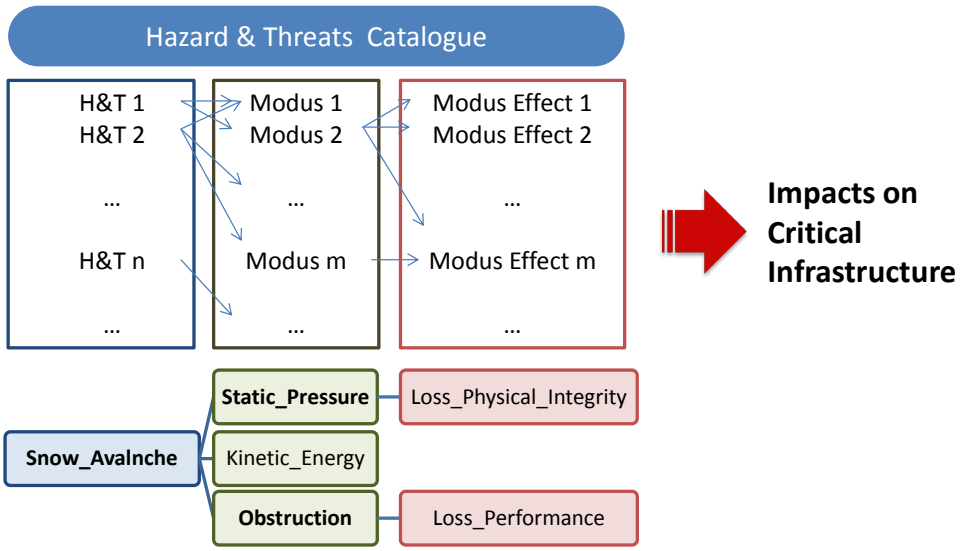
☑ Duration
☑ Resource
☑ Event_impact_area
☑ Actor and driver
☑ Predictability





Hazard & Threat Ontology

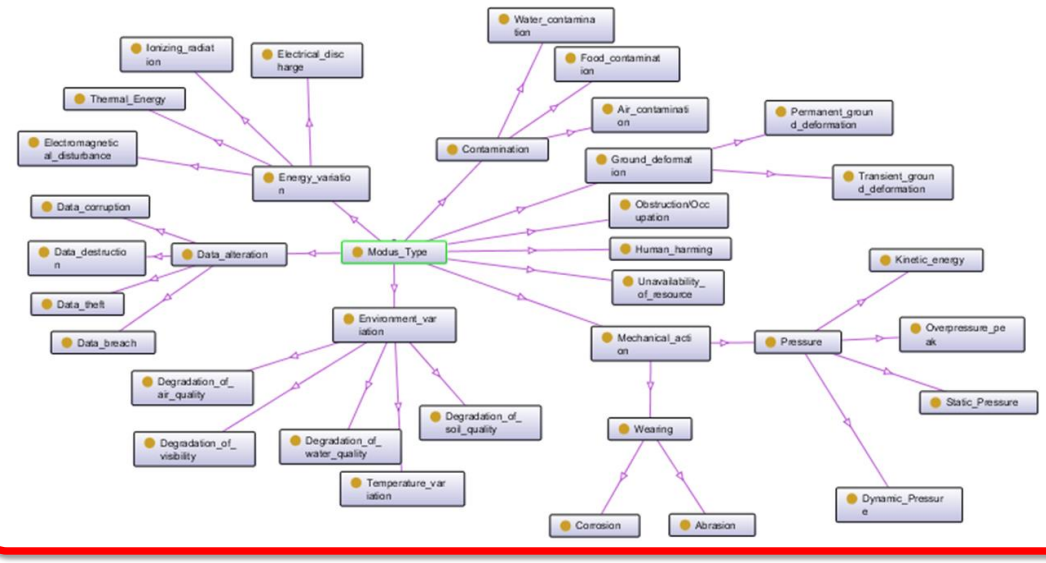
Impact modelling and taxonomy



Hazard & Threat Ontology

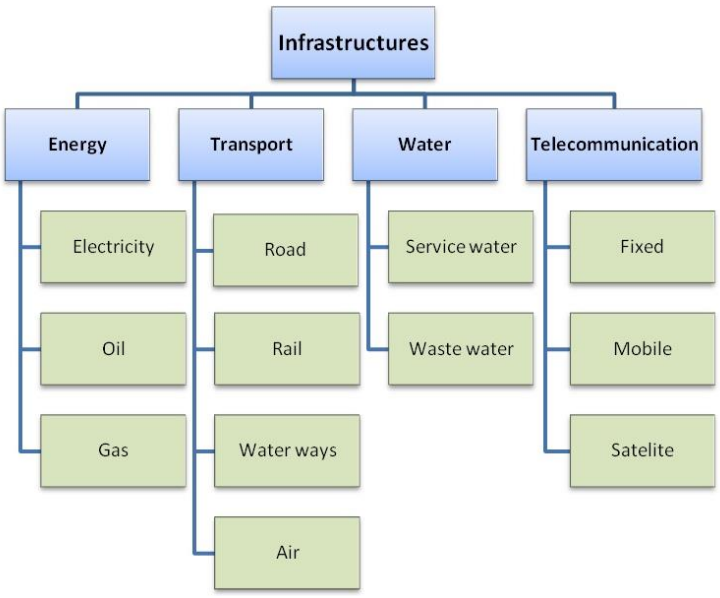
THREVI²
Threat - Vulnerability Path Identification for Critical Infrastructures

Modus and Modus Effects



Infrastructure Topology and Asset Taxonomy (ITAT)

THREVI²
Threat - Vulnerability Path Identification for Critical Infrastructures



More than **100** references have been reviewed:

- Scientific publications
- Technical reports, standards and databases
- Regulatory documents

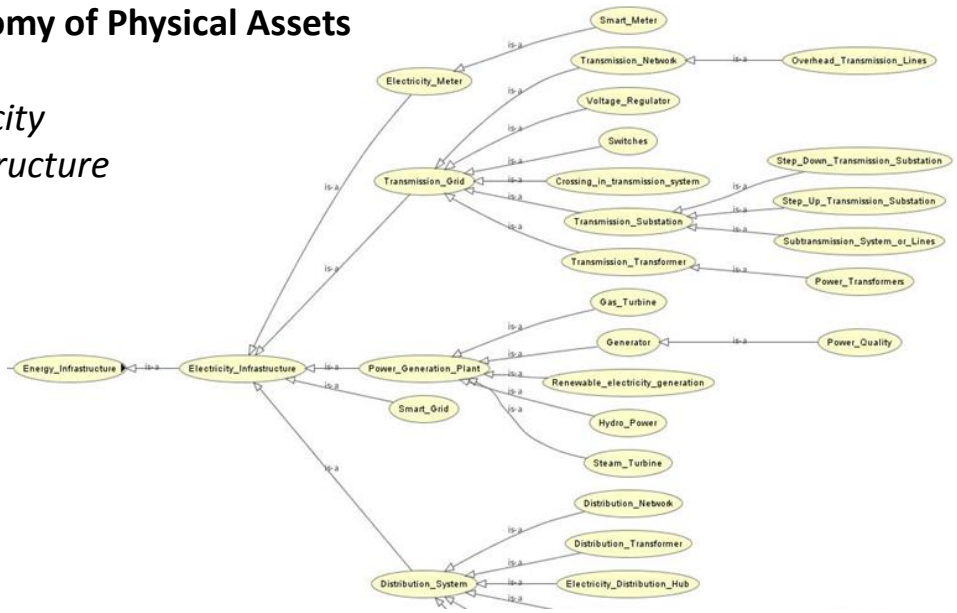
64 used to develop **24** coordinated sub-ontologies

Infrastructure Topology and Asset Taxonomy (ITAT)

THREVI²
Threat - Vulnerability Path Identification for Critical Infrastructures

Taxonomy of Physical Assets

Electricity Infrastructure

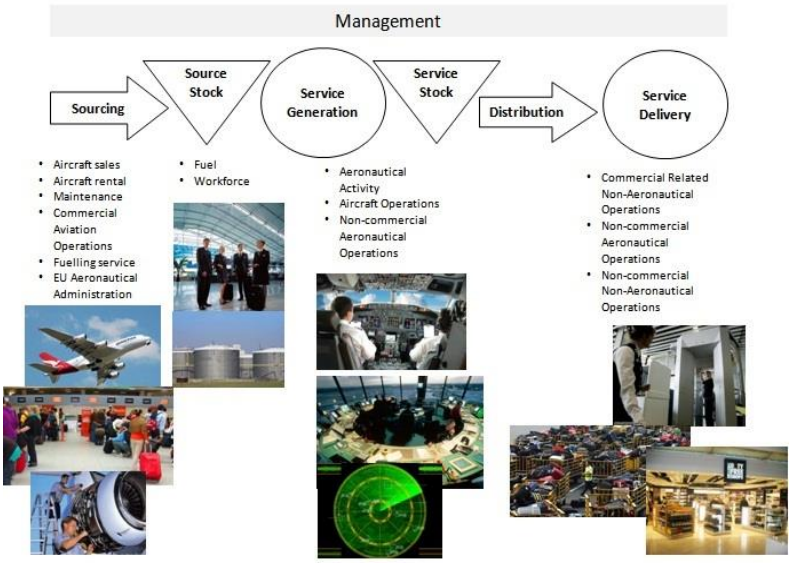


Infrastructure Topology and Asset Taxonomy (ITAT)

THREVI²
Threat - Vulnerability Path Identification for Critical Infrastructures

Ontology of functions

Air Transport Infrastructure



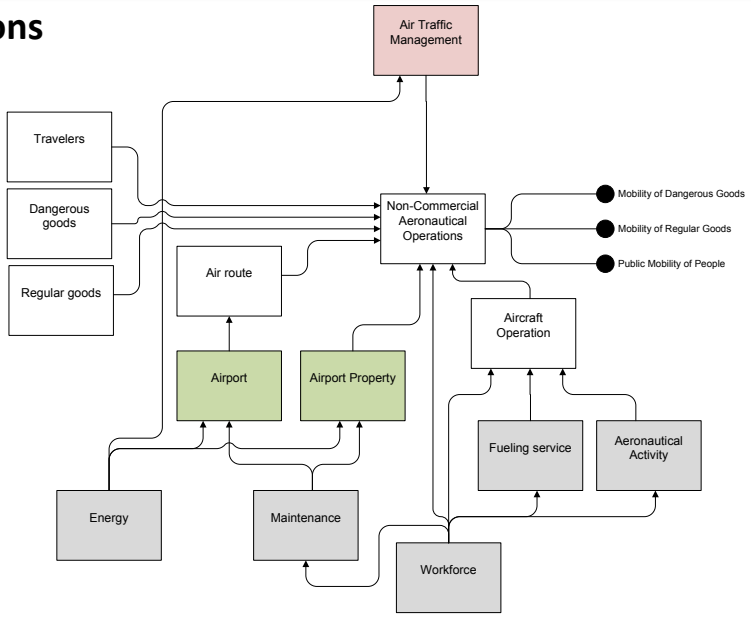
Infrastructure Topology and Asset Taxonomy (ITAT)

THREVI²
Threat - Vulnerability Path Identification for Critical Infrastructures

Ontology of functions

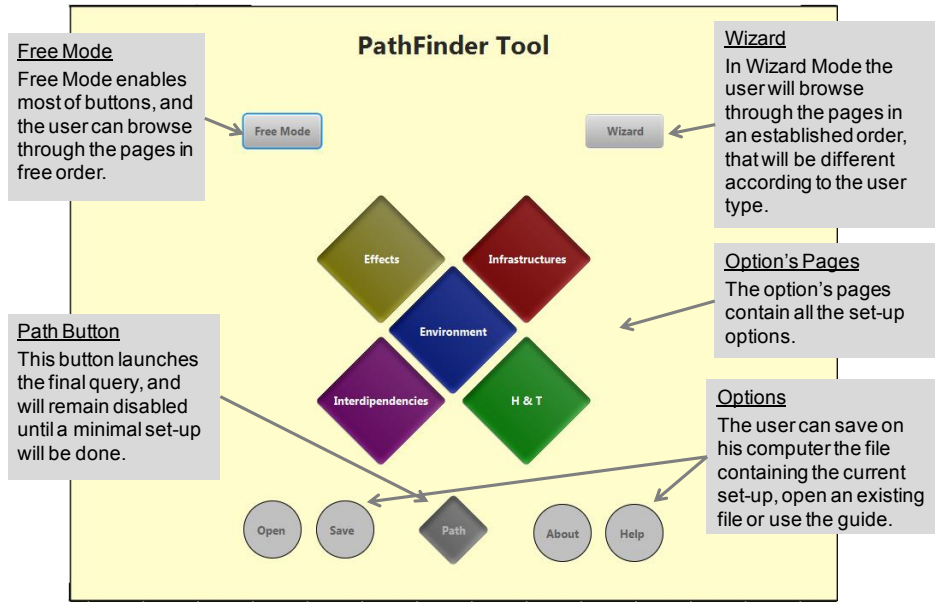
Air Transport Operations

Service Gen Phase



THREVI PathFinder Tool

Threat - Vulnerability Path Identification for Critical Infrastructures



Free Mode
Free Mode enables most of buttons, and the user can browse through the pages in free order.

Wizard
In Wizard Mode the user will browse through the pages in an established order, that will be different according to the user type.

Option's Pages
The option's pages contain all the set-up options.

Path Button
This button launches the final query, and will remain disabled until a minimal set-up will be done.

Options
The user can save on his computer the file containing the current set-up, open an existing file or use the guide.

Call for contributions and collaborations

Threat - Vulnerability Path Identification for Critical Infrastructures

- THREVI^2 validation
  - **Validation of Ontologies**
    - Experts will be provided with the draft version of the ontologies and a review template
    - About 3**0** international CI experts from private operators and public agencies have been already involved.
  - **Validation of the Software Tool**
    - Development of pilot applications in collaboration with Member States and/or CI operators
    - Experts will be provided with the PATHFINDER tool and specific technical support

Conclusions

THREVI² Threat - Vulnerability Path Identification for Critical Infrastructures

- THREVI² has harmonised and integrated all the relevant knowledge for the characterisation of threats, vulnerabilities and interdependencies of CIs systems
- The Interdependency Ontology and the final integration of THREVI² Ontology will be finalised by December 2014
- The PATHFINDER Tool will be developed and tested in two pilot applications by July 2014
- THREVI² will implement a consistent validation process involving European public bodies and operators

THREVI² Threat - Vulnerability Path Identification for Critical Infrastructures

Thank you!

www.threvi2.eu

Prof. Paolo Trucco
Dept. Management, Economics and Industrial Engineering
Via Lambruschini 4/b - building 26/B - 20156 Milan (Italy)

office: +39 02 2399 4053
fax: +39 02 2399 4067
e-mail: paolo.trucco@polimi.it
website: www.ssrm.polimi.it

EUROPEAN COMMISSION
DIRECTORATE-GENERAL HOME AFFAIRS
Directorate A : Internal Security

NIER INGEGNERIA RGS RISK GOVERNANCE SOLUTIONS

EUMASS - European Mass Transit System Security Risk Assessment and Audit Methodology

Mr. Fabio Bagnoli, D'Appolonia, Italy

Mr. Bagnoli presented the EUMASS project, the European Mass-Transit System Security Risk Assessment and Audit Methodology. This is a project that was financed by the CIPS 2008 and its duration was two years (2009-2011). The presentation was divided into the following parts; the consortium, the project's objectives, the approach and the methodologies that were used, the supporting software tools, a use case validation and the follow up.

The discussion that followed included the clarification of some technical details. The first point was on the availability of tool for the operators for audit purposes, as the tool provides the structure for performing audits. The second point was whether the risk assessment methodology was based on the experience of the operators. Finally, to the question if the operators have tried to change the security measures based on this tool, the response was that the operators use the tool as a guide to proceed with the updating of the existing security measures and the creation of new ones.

European Mass Transit System Security
Risk Assessment and Audit Methodology

D'APPOLONIA Isdefe ATM POLITECNICO DI MILANO

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

D'Appolonia S.p.A.

D'Appolonia is a major Italy-based engineering company that provides multidisciplinary engineering consulting and design services to a great variety of public and private clients

The Company has been established by Dr. Elio D'Appolonia in 1956 in Pittsburgh (Pennsylvania), and is present in Italy since 1981

In 1983 the Italian office, headquartered in Genoa, became the independent company D'Appolonia S.p.A.

The company since December 2011 is part of the RINA Group

Engineering Services

D'Appolonia provides engineering and management services during the whole project life cycle:

- Feasibility studies and research
- Conceptual design and project specifications
- Preliminary and detailed design
- Physical and virtual validation
- Management of suppliers and system integration
- Construction management and supervision
- Commissioning and support to homologation and certification
- Maintenance and operation

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Engineering Divisions

D'Appolonia is organized in seven Divisions:

Environment and Energy

Health and Safety

Engineering Design

Siting

Electronic Systems

Innovation Consulting

Transport Engineering

Background

EUMASS Project addresses the specific topic of the Transport related objectives (2008 call):

"Development of a risk assessment and audit methodology capable of assessing the vulnerabilities of a mass-transit system (i.e. subways and railways) from a potential terrorist attack."

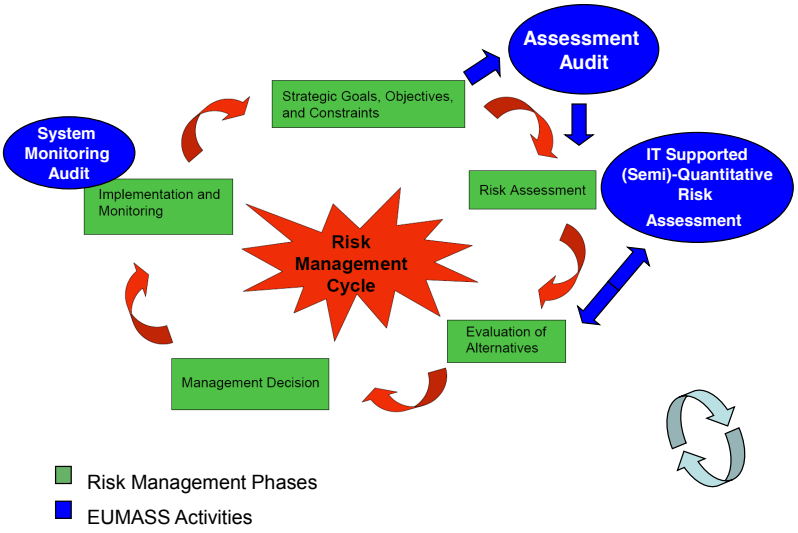
"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

EUMASS Objectives

- ✓ The EUMASS objective was the delivery of a unified and flexible solution for **risk assessment methodology** to be applied by all European Mass Transit operators.
- ✓ Main goal was to achieve an integrated process composed by the audit and risk assessment methodologies supported by a software tool.
- ✓ An **audit method** was prepared to translate empirical evaluations into objective inputs for the risk analysis models and to monitor them during the system lifecycle.
- ✓ A semi-quantitative risk assessment methodology was developed to continuously evaluate the risks associated to a system and to evaluate the effectiveness of the implemented countermeasures.
- ✓ A software tool was developed to support the user along the whole process.

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

EUMASS Approach



"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

European Mass Transit System Security
Risk Assessment and Audit Methodology

AUDIT METHODOLOGY

Two phases, why?

- Data Gathering: in order **to gather information about the system and the operation in a structured way**, to be used as input for the risk assessment methodology

- System Monitoring: **a periodic review**
  - **to check if the conditions verified at the beginning of the analysis** are still applicable or should be modified
  - **to check the implementation of the measures** foreseen with the risk assessment

The data gathering and the system monitoring have the same structure.

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Data Gathering

- Definition and recording of objectives
  - Security
  - Operational
  - Performance
- Identification of Areas involved in the risk assessment process
- Identification of existing countermeasures in place
- Identification of Vulnerabilities
- Hints from field operators

D'APPOLONIA Isdefe ATM POLITECNICO DI MILANO

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Monitoring

- Review of system composition
- Verification of conditions
  - Vulnerabilities
  - Countermeasures effectiveness
  - Incidents / Accidents
- Verification of Policies
- Verification of Personnel Training
- Countermeasure effectiveness evaluation (KPI based)
- Hints from field operators

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Supporting tools

- Checklists
  - To carry out the initial survey for data gathering
  - To carry out the periodic monitoring on the system
- Inventory management for checklists

- Monitoring checklists will be automatically generated by the risk assessment supporting tool based on system composition, identified scenarios and on past experience gathered from past analysis

D'APPOLONIA Isdefe ATM POLITECNICO DI MILANO

Checklist Example

EUMASS Audit Checklist

Please fill in the present table according to the following instructions:
- For each countermeasure listed choose it is implemented in your system
- If it is implemented choose the type of countermeasure implemented
- If it is implemented fill list the assets which the countermeasure is applicable to

ID	Countermeasure Category	Countermeasure	Implemented		If implemented, type of Implementation and implementation level (%)								Assets which is applicable to	Note
1	Access Control	Access control on employee only areas	Yes	No	Ad-Hoc design		Hardening		Strict Monitoring		Removal			
2	Access Control	Fare gates or "fare only" areas	Yes	No	Ad-Hoc design		Hardening		Strict Monitoring		Removal			
3	Access Control	Access prohibition on gates in case of overcrowding	Yes	No	Ad-Hoc design		Hardening		Strict Monitoring		Removal			
4	Access Control	Flux separation	Yes	No	Ad-Hoc design		Hardening		Strict Monitoring		Removal			
5	Access Control	RFID driver identification system for tracking and route plans	Yes	No	Ad-Hoc design		Hardening		Strict Monitoring		Removal			
6	Access Control	Automatic vehicle identification for access control on gates on parking lots and garages	Yes	No	Ad-Hoc design		Hardening		Strict Monitoring		Removal			
7	Access Control	Car plate registration for access control on gates on parking lots and garages	Yes	No	Ad-Hoc design		Hardening		Strict Monitoring		Removal			
8	Access Control	Position tracker for access control on gates on parking lots and garages	Yes	No	Ad-Hoc design		Hardening		Strict Monitoring		Removal			
9	Access Control	Badge systems on employee only areas	Yes	No	Ad-Hoc design		Hardening		Strict Monitoring		Removal			
10	Access Control	Biometrical systems on employee only areas	Yes	No	Ad-Hoc design		Hardening		Strict Monitoring		Removal			

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

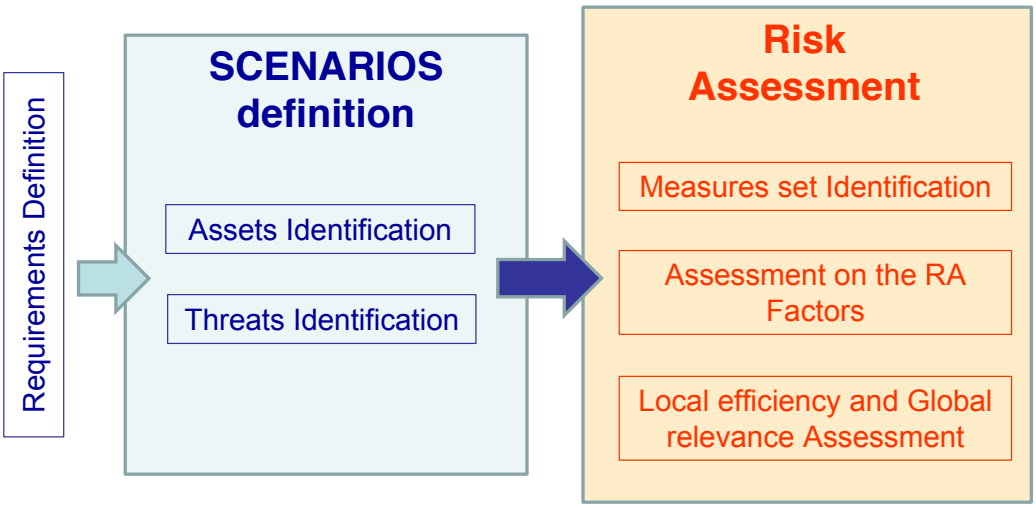
Audit Main Issues

- Objectivity of results
- Not ambiguous questions
- Uniquely identify the person to be interviewed for each question
- Questions grouped by theme
- Respect of applicable security restrictions
- Recordable
- Repeatable

RISK ASSESSMENT METHODOLOGY

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Risk Assessment Flow Chart



Risk Analysis Principles

- **Semi-quantitative** methodology
- **Applicability to all the assets** included in a Mass Transit System
- **Flexibility** in order to let it **to be applied at different levels** (system, sub-system, elements)

Risk = Probability * Impact
= [Threat * (Attractiveness * Vulnerability)] * Impact

Target attractiveness allows the evaluation of the level of interest that a particular asset would have in the eyes of the adversary (type of effect). It is dependant from:

- Target relevance in relation with adversary aims
- Capability of the adversary

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Assets identification

Metro is supposed to be located in a major capital city. Sensitive assets are:

- Station Building
- Platform
- Track Sections
- Service Accesses
- Vehicle
- Technological systems - Control Centre
- Technological systems - Ventilation System
- Technological systems - Communication System
- Technological systems - Signalling System
- Technological systems - Power Supply System
- Depot

D'APPOLONIA Isdefe ATM POLITECNICO DI MILANO

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Threat identification

Metro is exposed to a number of threats, such as:

- Explosives attack of large scale
- Hijacking of a train / service vehicle
- Sabotage of tracks / equipments
- Illegal acts (smuggling)
- Intrusion in the information system
- Dispersion of chemical, biological or radiological agent
- Use of a train as a weapon
- Criminality and Vandalism
- Suspicious Behavior
- Terrorism alert
- Arson

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Assessment Step by Step

Validation of the measures set (y/n)

Effectivenes of the measures on the RA components (y/n)

Evaluation of the Local efficiency and Global relevance on the RA components for each measure (%)

Risk Assessment Methodology Application aiming at the **definition** of the necessary factors (**Attractiveness, Vulnerability** and **Impact**) for evaluating the Risk

R

Risk Analysis Output

The final output is a percentage based Risk value related to the selected scenario.

The Risk Assessment provides the influence of the countermeasures, which are or could be implemented, on the risk level for each scenario.

This allows an effective comparison of the improvements that can be achieved by adding a new countermeasure or improving the existing ones against different threats on the same asset.

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

SUPPORTING SOFTWARE TOOLS

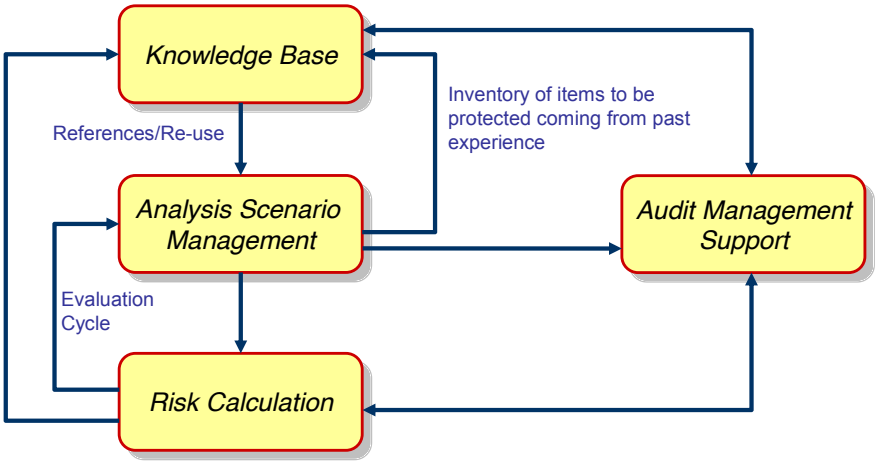
Support Tool structure

A tool supporting the entire process by providing the following main functionalities:

- Knowledge Base Management which provides the facilities to collect in a library all the information necessary to carry out Risk Analysis and to share experiences and knowledge
- Risk Analysis Scenario Management which provides support in the composition, versioning and duplication of scenario, object of the risk analysis
- Risk Analysis Calculation and Evaluation which provides instruments and algorithms to calculate, quantify, evaluate and mitigate risk
- Auditing Support Management which provides facilities to generate, record and maintain the checklist templates as well as audit reports and the filled checklists

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

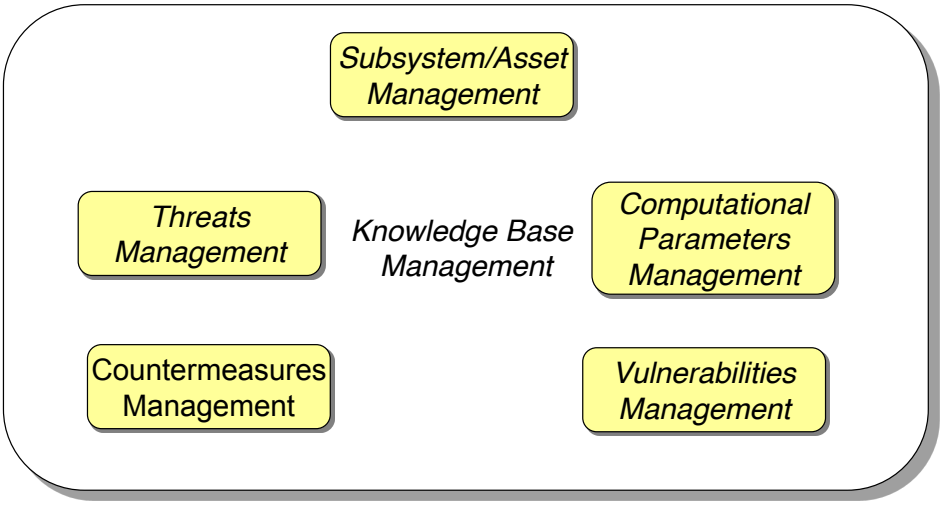
Key Concepts



D'APPOLONIA Isdefe ATM POLITECNICO DI MILANO

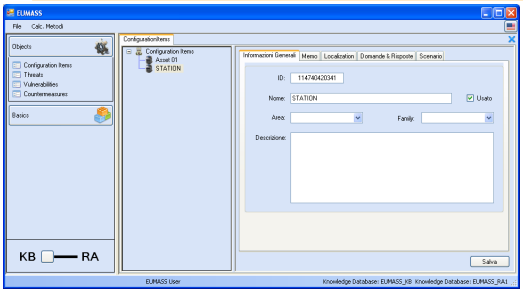
"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

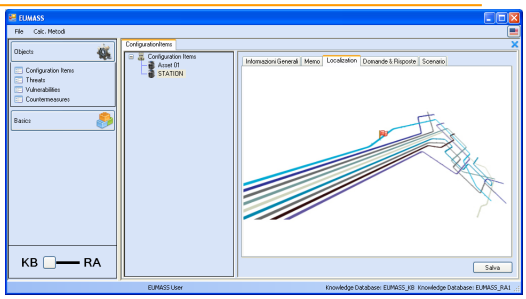
Knowledge Base Management

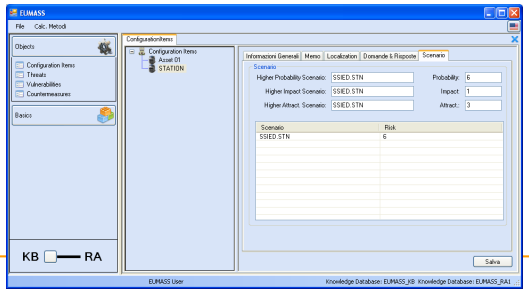


"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

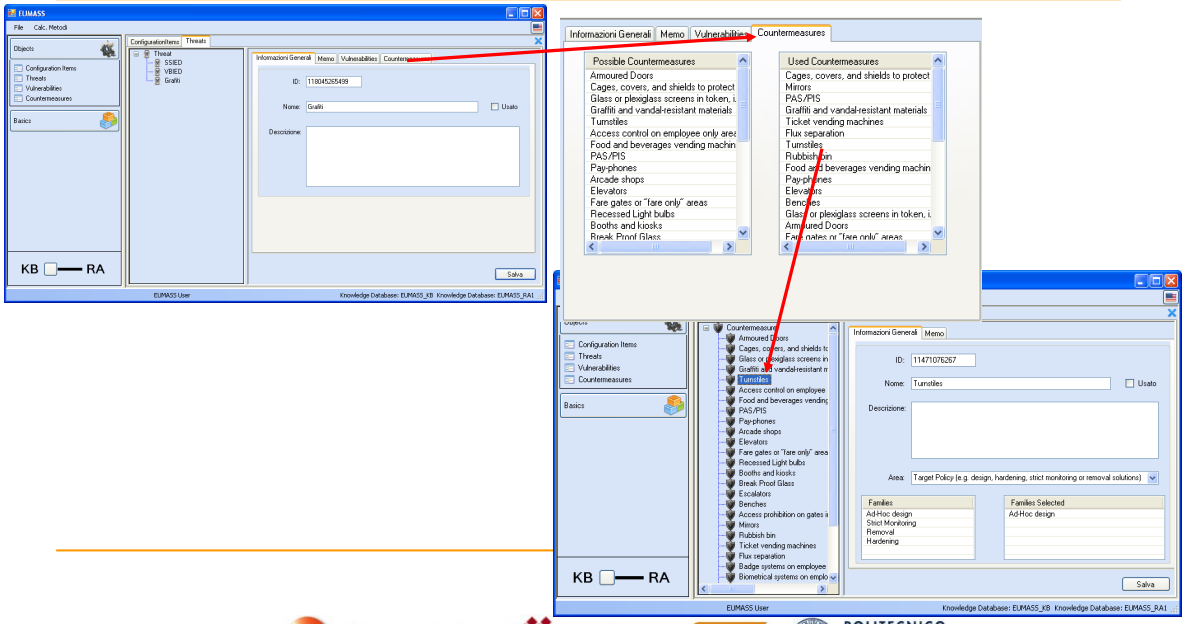
Sub-System/Asset Management





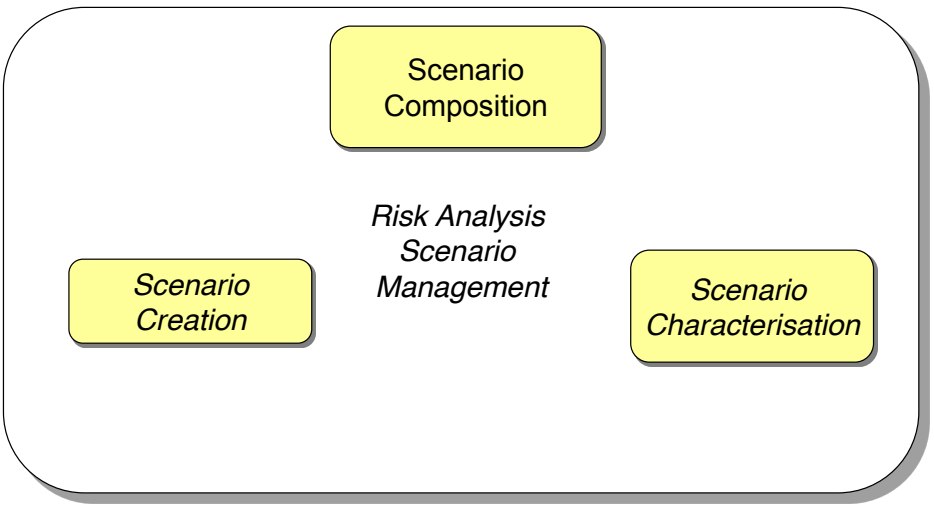


Threats / Countermeasures / Vulnerabilities Mgt



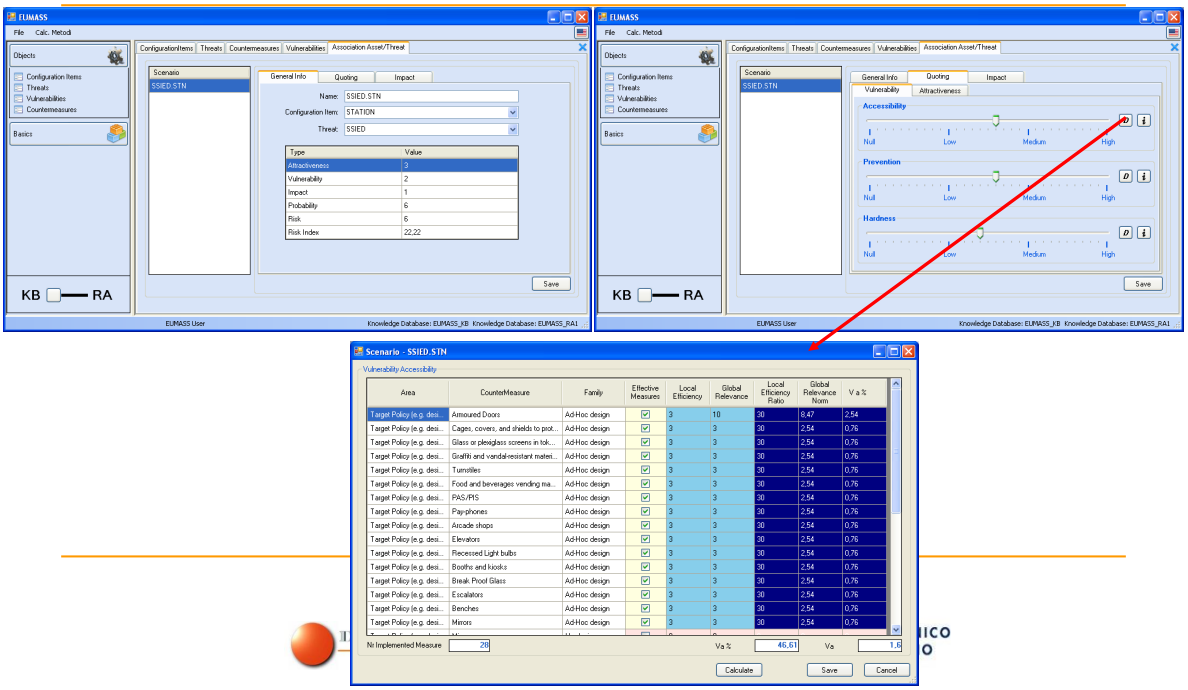
"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Analysis Scenario Management



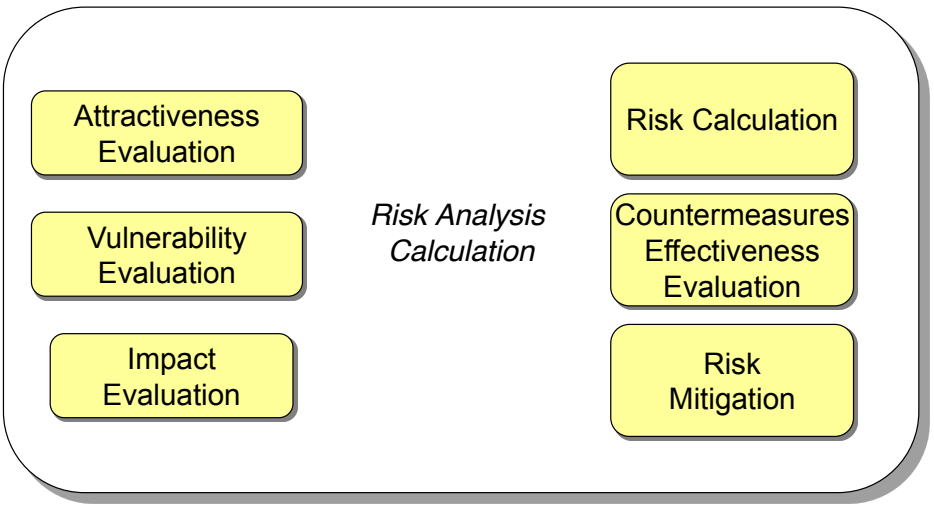
"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Scenario Composition and Characterisation



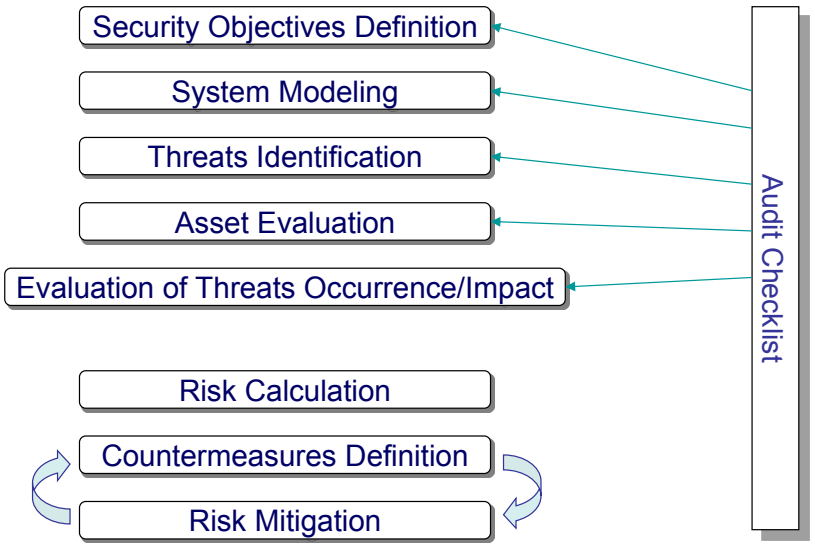
"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Risk Calculation



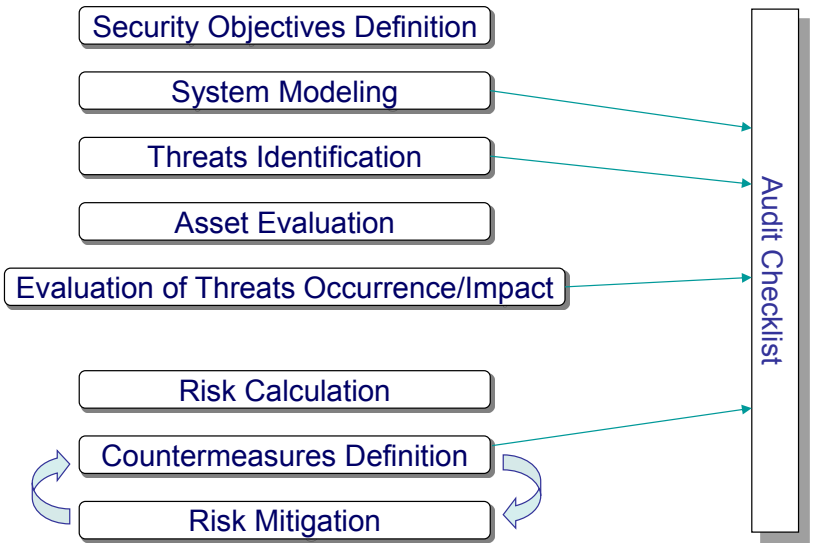
"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Inputs – Checklist data



"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Outputs – Monitoring Checklist



USE CASE VALIDATION

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Definition of a use case based on a true world scenario

- Number of passengers using the station
- Role within the PT network taking into account the number of interchanges with other lines or modes
- Response efforts be particularly difficult as the station is very deep, elevated or underneath a major structure
- Symbolic importance of the station or symbols existing in the neighbourhood / Postcard view
- Official events being organised nearby that can temporarily raise the risk level
- History of events
- Attack or attempted attacks in the past

D'APPOLONIA Isdefe ATM POLITECNICO DI MILANO

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Test Bed Station Facts

Characteristic of the PT Hub:

- 70.000 transit passengers between 7.00 a.m. to 9.00 a.m., in every working day

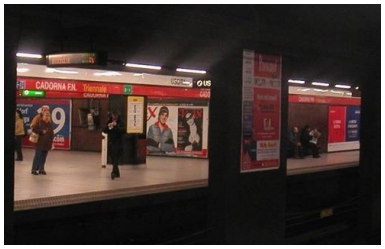
- 2 metro lines crossing (Line A and Line B)
- 1 train terminal station on surface with a high level traffic flow
- 7 Bus / Tram ATM lines in correspondence
- 1 Taxi parking
- Terminal of 6 suburban bus lines

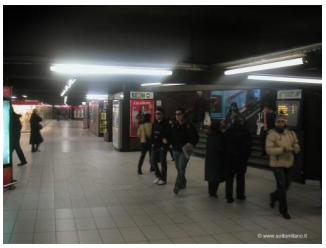
D'APPOLONIA Isdefe ATM POLITECNICO DI MILANO

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Use Case Scenarios

- Explosive attack on central platform between metropolitan lines A and B of the studied Station: aim of the attack is to generate victims
- Explosive attack in the technological room: the target of this attack is to damage the infrastructure and interrupt the service continuity





D'APPOLONIA Isdefe ATM POLITECNICO DI MILANO

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

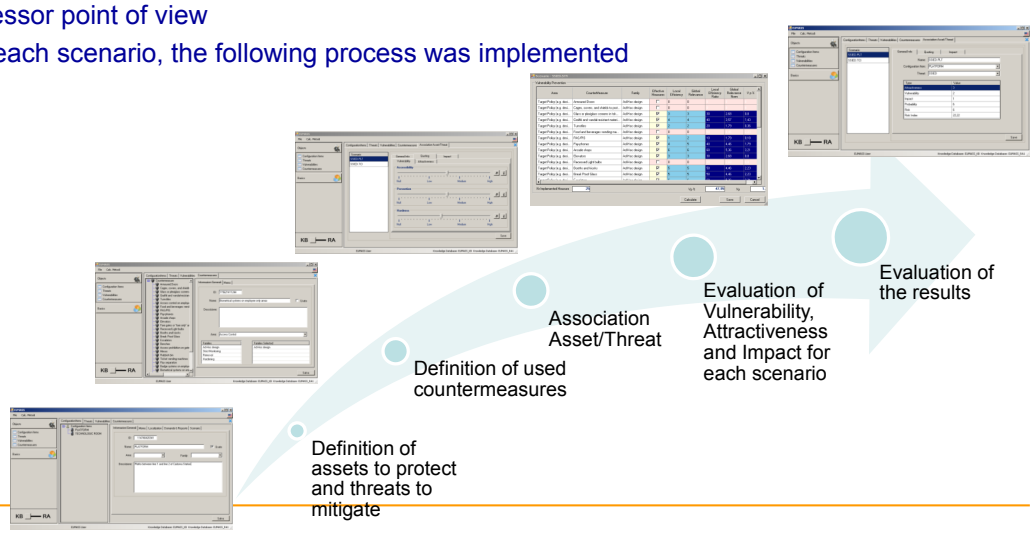
Application of the methodology

Factor	Sub factor	Expected value scenario 1	Expected value scenario 2
Vulnerability	Va (Accessibility)	3	2
	Vp (Prevention)	2.5	2.5
	Vh (Hardness)	3	3
Attractiveness	Apv (Perceived Vulnerability)	3	2
	Aph (Perceived Hardness)	2	3
Impact	Ip (impact on people)	2,5	1
	Ii (impact on infrastructure)	2.5	3
	Is (Impact on service continuity)	3	3

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Validation

- Use of the EUMASS tool and evaluation of the results
- Assessor point of view
- For each scenario, the following process was implemented



Review and analysis of the results

SCENARIO 1			
Factors	**Subfactors**	**Expected values (assessor perception)**	**Obtained values (with Tool Support)**
Vulnerability	Accessibility	3	2,7
	Prevention	2,5	2,9
	Hardness	3	3
Attractiveness	Perceived Vulnerability	2,5	2,7
	Perceived Hardness	3	3
Impact	People	2,5	2,9
	Infrastructure	2,5	2,9
	Service continuity	3	2,9
RISK LEVEL		20,8	23,7
RISK LEVEL %		76,9%	87,8%

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Review and analysis of the results

SCENARIO 2			
Factors	**Subfactors**	**Expected values**	**Obtained values**
Vulnerability	Accessibility	2,0	2,9
	Prevention	2,5	2,9
	Hardness	3,0	3,0
Attractiveness	Perceived Vulnerability	2,5	2,9
	Perceived Hardness	3,0	3,0
Impact	People	1,0	3,0
	Infrastructure	3,0	3,0
	Service continuity	3,0	2,9
RISK LEVEL		13,8	25,6
RISK LEVEL %		50,9%	94,9%

D'APPOLONIA Isdefe ATM POLITECNICO DI MILANO

Conclusions

- After the analysis performed the EUMASS methodology is considered by ATM, as operator, to be valid, detailed and very solid
- Existing and already accepted methodologies provide results comparable with the ones obtained by the EUMASS methodology
- Results obtained by an assessor using the EUMASS methodology (on paper and subjective process based on expert knowledge) are similar to the ones obtained with the EUMASS Tool (more detailed and objective)
- Carrying out a risk assessment on paper with the EUMASS Methodology will take less time than carrying out the same assessment for the first time on the tool, but the tool will provide with more detailed and precise results
- However the tool will speed up the process of analysing new systems similar to the ones already assessed and/or modify existing ones and to re-evaluate them

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

FOLLOW UP

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

Extension towards cost benefit (COBALT Project)

- Main aim of the COBALT is to provide CI operators and owners with an instrument which will help in defining the risk their infrastructures are subject to.
- COBALT aims at providing end-users with an instrument that will help them evaluating which countermeasures are the most effective to reduce the risks a CI is subject to, from an implementation and maintenance costs point of view.
- Finally COBALT aims at developing and instrument to evaluate the CI security generating a report showing the evaluated risks and the countermeasures implemented.

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

European Mass Transit System Security
Risk Assessment and Audit Methodology

OUR VISION

Our vision

- Close cooperation with end users, public bodies and other operators of Critical Infrastructures
- Strong synergies with industries providing technologies
- Definition and validation of new comprehensive methodologies for all the analyses to be undertaken to assess threats, vulnerabilities and risks, that could be offered to Critical Infrastructures operators and other end users
- Combination with deep competences in the involved domains
- Involvement in projects in different domains
- Cross fertilization among the different involved areas and their relevant approaches
- Development of new harmonised methodologies and implementation of supporting tools to propose to our customers

"With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Justice, Freedom and Security"

European Mass Transit System Security Risk Assessment and Audit Methodology

THANK YOU

fabio.bagnoli@dappolonia.it

Secure Baltic Sea region

Mr. Przemyslaw Komorowski, Prometheus Foundation, Poland

Mr. Komorowski presented a summary of a project with a regional dimension under the title "The Prevention and Management of Consequences of Terrorism in the LNG Terminal in Swinoujscie as an Element of Baltic Sea Region Security". The presentation included the project's objectives, activities, progress, evaluation and some implementation problems.

Project The Prevention and Management of Consequences of Terrorism in the LNG Terminal in Swinoujscie as an element of Baltic Sea Region Security

Reference number: HOME/2011/CIPS/AG/4000002100

CIPS III Workshop, 12th November 2013

"The Prevention and Management of Consequences of Terrorism in the LNG Terminal in Swinoujscie as an Element of Baltic Sea Region Security"

Provincial Police Headquarters in Szczecin and Regional Development Foundation „PROMETHEUS"

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Home Affairs

Project The Prevention and Management of Consequences of Terrorism in the LNG Terminal in Swinoujscie as an element of Baltic Sea Region Security

Reference number: HOME/2011/CIPS/AG/4000002100

General information

- **Project start:** 1st Setpemeber 2012
- **Project duration**: 16 months
- **Total project budget:** EUR 140 726, 89
- **Project participants:**
  - public institutions: the Provincial Police Headquarters in Szczecin, Town Office in Szczecin and in Koszalin, the Maritime Office in Szczecin, the Fire Brigade Service, Provincial Office, Central Statistical Office, Government Security Center, Bureau of International Police Cooperation KGP, Regional Inspectorate environmental protection, Maritime Border Guard Department
  - private institutions: Polish Energy Group SA, TP SA, Polish Cellular Digital Telephony, NBP, Chemical Plants Police SA

Training – app. 220 people; Simulation exercises: 137 people; international conference 101 persons.

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Home Affairs

Project The Prevention and Management of Consequences of Terrorism in the LNG Terminal in Swinoujscie as an element of Baltic Sea Region Security

Reference number: HOME/2011/CIPS/AG/4000002100

Objectives of the project

- **Main goal**: ensuring safety of persons, public places and critical infrastructure in case of a terrorist threat

- supporting coordinated and organizational operations aimed at increasing efficiency of protection of objects with characteristics of a critical infrastructure in case of sudden and violent events such as terrorist attack

- conducting common exercises based on realistic scenarios in order to enhance coordination and cooperation between services responsible for crisis management

- identification of critical infrastructure and developing common standards of safety in emergency measures of critical infrastructure to exchange know-how and experience in protection of people and objects

- improving management skills in an emergency situations in critical infrastructure

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Home Affairs

Project The Prevention and Management of Consequences of Terrorism in the LNG Terminal in Swinoujscie as an element of Baltic Sea Region Security

Reference number: HOME/2011/CIPS/AG/4000002100

Project activities

1) Organisation of an international conference with workshops

2) Simulation of operational activities in the area of Port Szczecin – Swinoujscie

3) A series of trainings in order to develop common standards of behaviour during the terrorist threat among employees of critical infrastructure

4) Project Management

5) Communication and dissemination: a conference, promotional materials, website, ads in newspapers.

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Home Affairs

Project progress

1) Organisation of an international conference with workshops - DONE
2) Simulation of operational services - DONE
3) A series of trainings - DONE
4) Project Management – IN PROGRESS
5) Communication and dissemination: IN PROGRESS
   - Closing conference
   - Study visit in Spain

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Home Affairs

Project The Prevention and Management of Consequences of Terrorism in the LNG Terminal in Swinoujscie as an element of Baltic Sea Region Security

Reference number: HOME/2011/CIPS/AG/4000002100

Evaluation

1) international conference with workshops

- For the vast majority of the participants the conference content was attractive

- MULTIDISCIPLINARITY The assurance of security LNG Terminal knowledge from various spheres of science

- COORDINATION Competences related to public safety are divided between various entities. There is no possibility to assure safety without harmonious system

- ANTICIPATION The terrorist threat has a dynamic character, therefore there is a need of constant work which would enable to foresee actions of terrorist organizations

- INCORPORATION OF EXPERIENCES The LNG Terminal is first investment of the kind in Poland
- PRECISION AND COHERENCE OF LEGISLATION In the area of public security the present legislation not always suits needs of effective actions.

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Home Affairs

Evaluation

2) Simulation command post-exercise "Organization and Conducting of Police Activities in Cooperation with non-police Entities in the Event of Terrorist Threat to LNG Terminal in Swinoujscie"

- Majority of the observers adopted a moderately positive view of the quality level of security in LNG Terminal in relation to the simulation

- The participants found the simulation to be useful: majority of them stated that their expectations were met (91,7%)

- The simulation had a positive impact on the knowledge and skills of the majority of participants (87,5%)

- The most positive impact was observed with respect to the ability of doing ones tasks properly, working with the prepared equipment and understanding the process of real crisis situation

- Anti-terrorist actions were the element that won special acclaim

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Home Affairs

Project The Prevention and Management of Consequences of Terrorism in the LNG Terminal in Swinoujscie as an element of Baltic Sea Region Security

Reference number: HOME/2011/CIPS/AG/4000002100

Implementation problems

- out-dated values in the budget constructed in 2011, in relation to the current market prices;

- national legislation of the public entities which doesn't allow for moving savings between budget's paragraphs;

- grant's transfer procedures - Awarded grant is transferred to the Polish Ministry of Finance and an Applicant have to request for the payment of tranches. This is the long-term process, resulting often in a lack of funds for the implementation of tasks in line with planned deadlines;

- exchange rate - settlement with the European Commission is based on the exchange rate of the ECB, while the settlement with the State budget is based on the exchange rate of the Polish National Bank;

- lack of response to invitations sent to international experts - Invitations had been sent independently and via the Ministry of Internal Affairs;

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Home Affairs

Project The Prevention and Management of Consequences of Terrorism in the LNG Terminal in Swinoujscie as an element of Baltic Sea Region Security

Reference number: HOME/2011/CIPS/AG/4000002100

Implementation problems

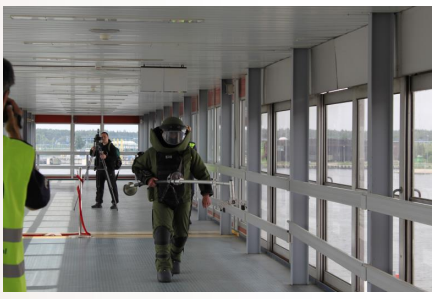
- refusal to participate in the simulation exercises because of the high cost of participation. Anti-Terrorist Operations Bureau (BOA), The Internal Security Agency (ABW) refused to invitation because PPH was not able to cover costs of their participation, especially to cover costs of transportation of specialized equipment necessary to conduct exercises.

- GROM Military Unit wasn't able to participate in simulation exercises, despite the earlier interest in participating, because were ordered to go to Afghanistan mission.

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Home Affairs

Project The Prevention and Management of Consequences of Terrorism in the LNG Terminal in Swinoujscie as an element of Baltic Sea Region Security

Reference number: HOME/2011/CIPS/AG/4000002100



With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Home Affairs

Project The Prevention and Management of Consequences of Terrorism in the LNG Terminal in Swinoujscie as an element of Baltic Sea Region Security

Reference number: HOME/2011/CIPS/AG/4000002100

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Home Affairs

Project The Prevention and Management of Consequences of Terrorism in the LNG Terminal in Swinoujscie as an element of Baltic Sea Region Security

Reference number: HOME/2011/CIPS/AG/4000002100

Thank you for your attention!

Contact persons:

Ms. Wioletta Wisniewska, Provincial Police Headquarters in Szczecin
wwisniewska@szczecin.policja.gov.pl

Ms. Mariola Stanczyk-Chlebiej, RDF „Prometheus”
mstanczyk@faberconsulting.com

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Home Affairs

Business Continuity Planning for Critical Infrastructures

Mr. Daniel Mosquera Benitez, ISDEFE, Spain

Mr. Mosquera presented the BUCOPCI project, which stands for Business Continuity Planning for Critical Infrastructures. The presentation was about the objectives of the project, the role of the stakeholder group, the project's results and conclusions. In the discussion that followed, it was highlighted that the project's outcome is a set of guidelines or recommendations which can be partially adopted to facilitate the activities of the transport sector. An interesting point of this project was the active participation of the stakeholders (technical steering) during all stages of the project.

Isdefe

Your best ally

3rd CIPS Conference

Results of the CIPS co-funded project, BUCOPCI.

Prepared and presented by: Daniel MOSQUERA-BENITEZ

Brussels, 12th of November 2013

Contents of the presentation

- **BUCOPCI –** What is it about? – [5 min]
- **Stakeholder Group –** The role of the end-users? – [5 min]
- **Project Results –** What do we get at the end of the project? – [10 min]
- **Project Conclusions –** [5 min]

BUSINESS CONTINUITY PLANNING

Bucopci

FOR CRITICAL INFRASTRUCTURES

July 2011 – July 2013

"With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme"

European Commission - Directorate-General Home Affairs

BUCOPCI

- Definition and Objectives,
- BUCOPCI as part of the CIPS programme

Isdefe

Definition and Objectives.

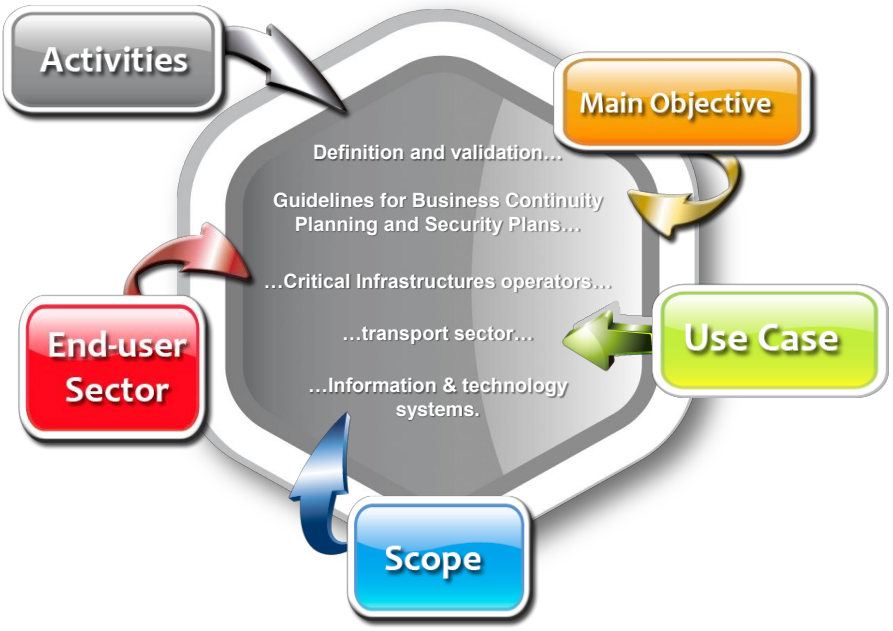
BUCOPCI stands for:

Business Continuity Planning for Critical Infrastructures, but…

What is it about?

3rd CIPS Conference. Results of the CIPS co-funded project, BUCOPCI.

Definition and Objectives.



Definition and Objectives.

*Identify best practices on **Business***

***Continuity** and **Security Planning**.*

Definition and Objectives.

*Develop a **set of guidelines** on Business Continuity and Security Planning **for Critical Infrastructure Operators**.*

Definition and Objectives.

***Increase awareness on Security and Business Continuity Planning** among Critical Infrastructure Operators from the transport sector.*

BUCOPCI as part of the CIPS programme

Objective 1 - Prevention and preparedness of risks.

- Stimulating, promoting and supporting the **development of methodologies** for the protection of Critical Infrastructures (CI), in particular risk assessment methodologies.

Objective 2 – Consequence management:

- Stimulating, promoting and supporting **exchange of knowledge** and experience, in order to establish best practices.

Stakeholders Group

- The added value of the stakeholders group.
- Stakeholders group members

The added value of the stakeholders group.

- **Expertise** in BCP/OSP is critical
- **Best practices** should be identified
- **Expectations** from guidelines should be covered
- **Realistic** scenarios must be defined
- Validation should be **done by experts**
- Guidelines should go **beyond theory**

Stakeholders group members

- Per sector:
  - Air Transport and Air Traffic Management
  - Road, Rail and Multimodal Transport
  - Critical Infrastructure Authority
  - Industry
- Per organization:
  - Cork Airport / Dublin Airport Authority (Ireland)
  - AENA – Spanish Airports and Air Navigation (Spain)
  - EUROCONTROL HQ (Brussels)
  - CASSIDIAN (France)
  - RENFE (Spain)
  - DHL Supply Chain (Spain)
  - CNPIC (Spain)

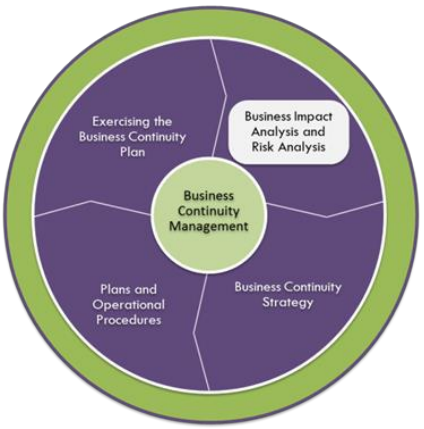
Project Results

- Guidelines for Business Continuity Planning
- Guidelines for CI Operator Security Planning
- Secondary results

Isdefe

Guidelines for Business Continuity Planning

- Built following the Business Continuity Management Cycle and presented in 4 chapters:
  - Understanding the organization,
  - Determining Continuity Strategy,
  - Development and implementation of BCM,
  - Practices, Maintenance and Review.
- Theoretical and Practical Sections. Step-by-step guide explaining the methodology implementation
- Extended information with specific information on implementation.

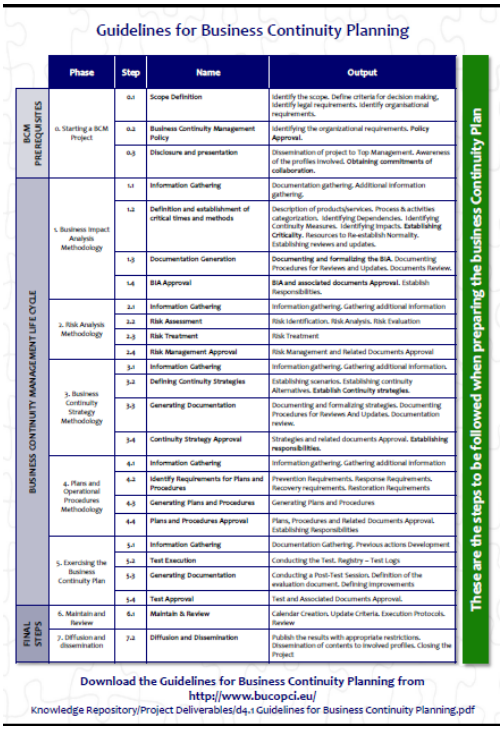


3rd CIPS Conference. Results of the CIPS co-funded project, BUCOPCI.

Guidelines for Business Continuity Planning

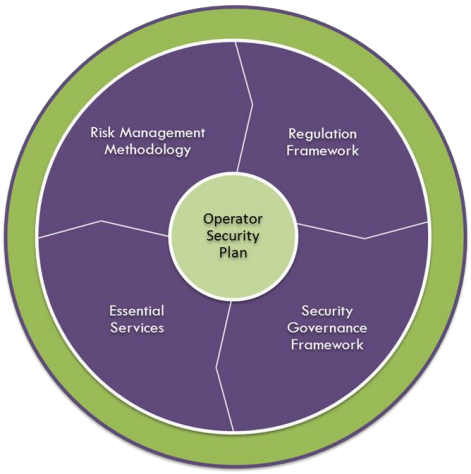
8 Steps Approach:

- Step 0. Starting a BCM Project
- Step 1. Business Impact Analysis Methodology
- Step 2. Risk Management Methodology
- Step 3. Business Continuity Strategy Methodology
- Step 4. Plans and Operational Procedures Methodology
- Step 5. Exercising the Business Continuity Plan
- Step 6. Maintain and Review
- Step 7. Diffusion and disseminationTercer nivel



Guidelines for CI Operator Security Planning

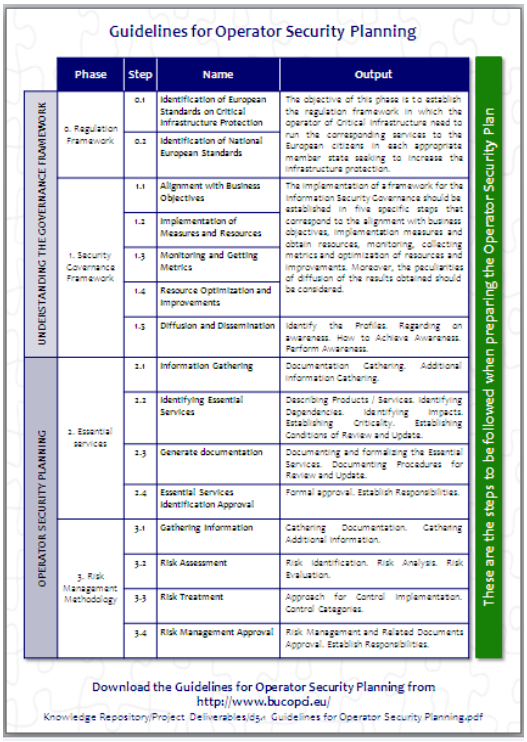
- Starts from an **analysis of European and National regulations** linked to CI Operators Security Plans.
- Includes: Security governance framework, Essential services identification and Risk analysis methodologies
- Aimed to **facilitate the identification and protection** of critical components within Critical Infrastructures.



Guidelines for CI Operator Security Planning

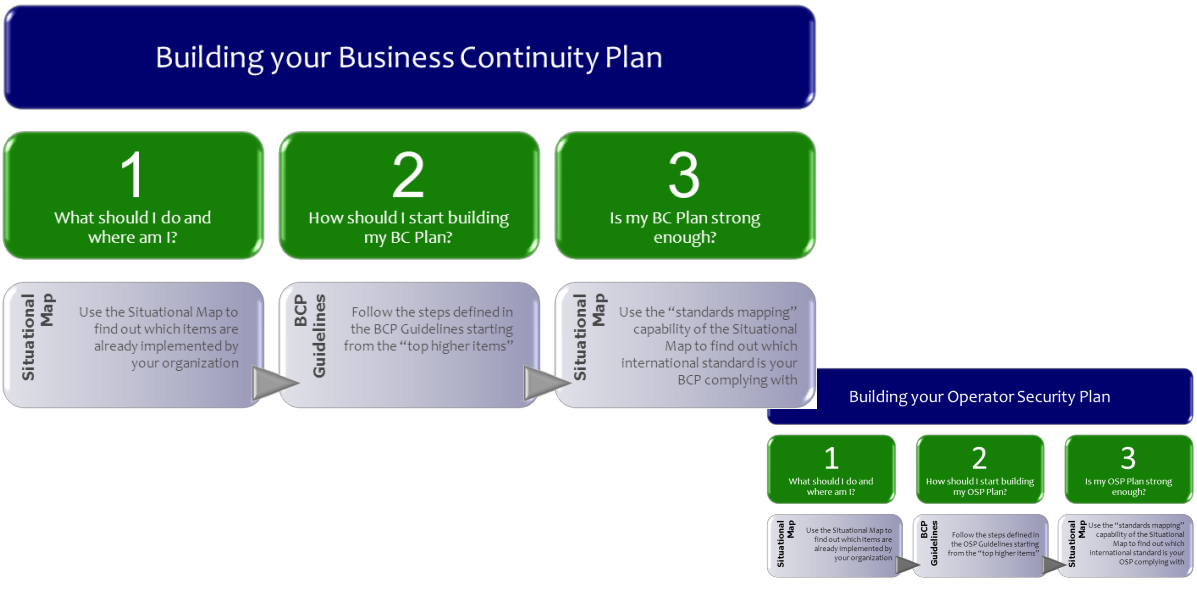
4 Steps Approach:

- Step 0. Regulation Framework
- Step 1. Security Governance Framework
- Step 2. Essential services
- Step 3. Risk Management Methodology



Guidelines for Business Continuity Planning and CI Operator Security Planning

How to use these Guidelines?



Secondary Results

The process of building both guidelines required transversal/secondary studies to be conducted. These studies resulted in:

- Which are the accepted standards?
- What are the practices in BCP and OPS followed by Critical Infrastructures Operators?
- Is there a need for developing Guidelines for BCP and OSP?

- State of the Art Analysis
  - Review of **international standards in Business Continuity Plan** (e.g. BS-25999-1, BS-25999-2), **Contingency Planning-IT** (e.g. ISO-24762, SS-507, ITIL, ISO-20000), **Disaster Recovery Plan-IT** (e.g. ISO-27002, NIST 800-34, ISO 24031, ISO-27001)
  - Assessment of **current implementation of BC and OSP** to Critical Operators in Transport Sector (via CNPIC)
  - Identification of **Common Continuity Practices** in Critical Operators.

Isdefe
Project Results

Secondary Results

- Can we go beyond “theory”?

- Scenarios Definition
  - Describes disruptive chain of events, Triggered through malware; Potentially initiated as an act of cyber terrorism.
    - Compromised Air traffic control system due to malware installation
    - Failed runway lighting (due to malicious activity) causing delivery logistics problems for an international courier service
  - Focused on IT infrastructure of transport sector.
  - Built from the stakeholder requirements/expectations.

Secondary Results

- What are the end-users expectations?
- What are the “minimum contents” the Guidelines should have?
- Are Guidelines covering end-user expectations? Are they “fit-for-purpose”?

- Validation
  - Aimed at demonstrating that guidelines as developed in WP4 and WP5 are fit for purpose
  - Limited to validate the benefits that using the guidelines could bring and not the benefits that applying a BCP and OSP as developed with such guidelines could bring
  - Defines validation objectives from stakeholders expectations
  - Follows the European Operational Concept Validation Methodology (E-OCVM)

Isdefe
Project Results

Secondary Results

- Are Guidelines “cost-effective”?

- Economic Study
  - Aimed at demonstrating the cost-efficiency of Guidelines implementation.
  - Compared the costs (qualitative) of developing BCP and OSP with and without using the guidelines.
  - Built on the assumption that plans developed with or without guidelines are equally correct and their implementation yields to the same recovery times.
  - Built from, at least, one of the scenarios defined in WP2.

Secondary Results

- Reports:
  - Release of: d1.1 – Standards Analysis Report (Public domain)
  - Release of: d1.2 – Business Continuity Best Practices Report (Public domain)
  - Release of: d1.3 – Security Plan Best Practices Public (Public domain)
  - Release of: d2.1 – Scenarios Definition Report (Public domain)
  - Release of: d3.1 – Validation Strategy (project-restricted)
  - Release of: d3.2 – Validation Report (project-restricted)
  - Release of: d6.1 – Business Impact Analysis (public domain)

Isdefe

Project Results

Reports are downloadable from BUCOPCI website:

www.bucopci.eu

Knowledge Repository/Project Deliverables

Project Conclusions.

- How should we remember BUCOPCI?

How should we remember BUCOPCI?

Critical Infrastructures Operators *in the transport sector in Spain, have contributed to the* ***common practices identification.***

How should we remember BUCOPCI?

Guidelines were built to ***adapt their input to any transport sector.***

Isdefe
Project Conclusions

How should we remember BUCOPCI?

Guidelines were ***built from the stakeholders expectations.***

How should we remember BUCOPCI?

Guidelines for Business Continuity and Operator Security Planning are of ***public domain.***

Isdefe

Contact details.

Contact details

If you need any support with the implementation of the guidelines, **we will be happy to assist you.**

- Daniel MOSQUERA-BENITEZ. Project Coordinator
  - dmosquera@isdefe.es

Contact...	For...	At...
Daniel Mosquera **Isdefe**	Project queries on: 1) Validation, Dissemination, Management, Stakeholder Group, etc.	coordinator@bucopci.eu dmosquera@isdefe.es
Daniel Blanco **SIA**	Technical queries on: 1) State-of-the-art Study 2) Guidelines for Business Continuity Planning	dblanco@sia.es
Diego Fernández **Isdefe**	Technical queries on: 1) Guidelines for CI Operator Security Plans	dfernandez@isdefe.es

Isdefe

Contact details

Partners

Project Coordinator

Isdefe (www.isdefe.es)
Daniel Mosquera-Benitez
dmosquera@isdefe.es

Associate Member

Associate Member:
CNPIC (ses.cnpic@interior.es)

Co-beneficiaries

Vicomtech (www.vicomtech.es)
Seán Gaines
sgaines@vicomtech.org

SIA (www.sia.es)
Daniel Blanco
dblanco@sia.es

WIT (www.wit.ie)
Robert Mullins
rmullins@tssg.org

Isdefe

Your best ally

Isdefe
C/ Beatriz de Bobadilla, 3
28040 Madrid
Tel.: +34 91 411 50 11
Email: general@isdefe.es
www.isdefe.es

JRC CIPS research activities

Mr. Georgios Giannopoulos, DG JRC

Mr Giannopoulos gave a presentation on CIPS activities in JRC/IPSC since 2010. He referred to two activities; the EPIC, lab, which is a unique installation for a well-developed activity on cyber-physical systems. It's a real ICT infrastructure which enables virtually any kind of studies in internet topologies on cyber-security issues. This activity constitutes a bottom-up approach, as it has been developed on a very technical level. On the contrary, a second activity, designed with a top-down approach, has been developed since 2010. It's about global models which can represent infrastructures in the European dimension, developed with the less possible detail, however they grasp the essential behaviour. In addition he provided a short presentation on a tool developed by JRC to assess the economic impact of critical infrastructure disruption.

A discussion was set on whether the CIPS consider risk assessment not only for terrorist attacks, but also for natural hazards. HOME stated that the calls of projects are not very descriptive, so covering specific hazards in CIP is up to the applicants, who submit the proposals for projects. There aren't any criteria on the types of hazards that the projects should cover and the list of the projects represents actually all types of hazards, all types of sectors, etc. However, the actual benefit from DG HOME point of view is making the results of the projects as much as possible publicly available.

Another point was the evaluation of the results of the projects and the impact of the out-

come. The response from HOME side was that there are constraints of resources and that they count on JRC's support, not only the scientific one, but also for assessing the outcome of the CIPS program, disseminating the results. It was mentioned that this workshop was a chance to get feedback from the stakeholders in terms of evaluating whether the program is useful or not, focusing on different things, and designing of the new program. It was made clear that CIPS 2013 was the last call and that in the future CIPS will look different, with less money allocated on the new program, as it's necessary to put the priorities right and the results to be used by as much as possible, preferably as guidelines that can be applied in different sectors. It was mentioned that the research should become more operational to support the CIP policy, that the CIPS have built the ground work and the capacities and that it's time to harvest the results of this work, although gaps still exist in the effort of capacity building.

Another point was highlighted by JRC, that instead on focusing on specific hazard types, an all-hazards approach is the way to make the program attractive to the community.

CIPS Research activities by JRC/STA Unit

Georgios Giannopoulos

European Commission

Joint Research Centre

Institute for the Protection and Security of the Citizen

Security Technology Assessment Unit

ISPRA, Italy

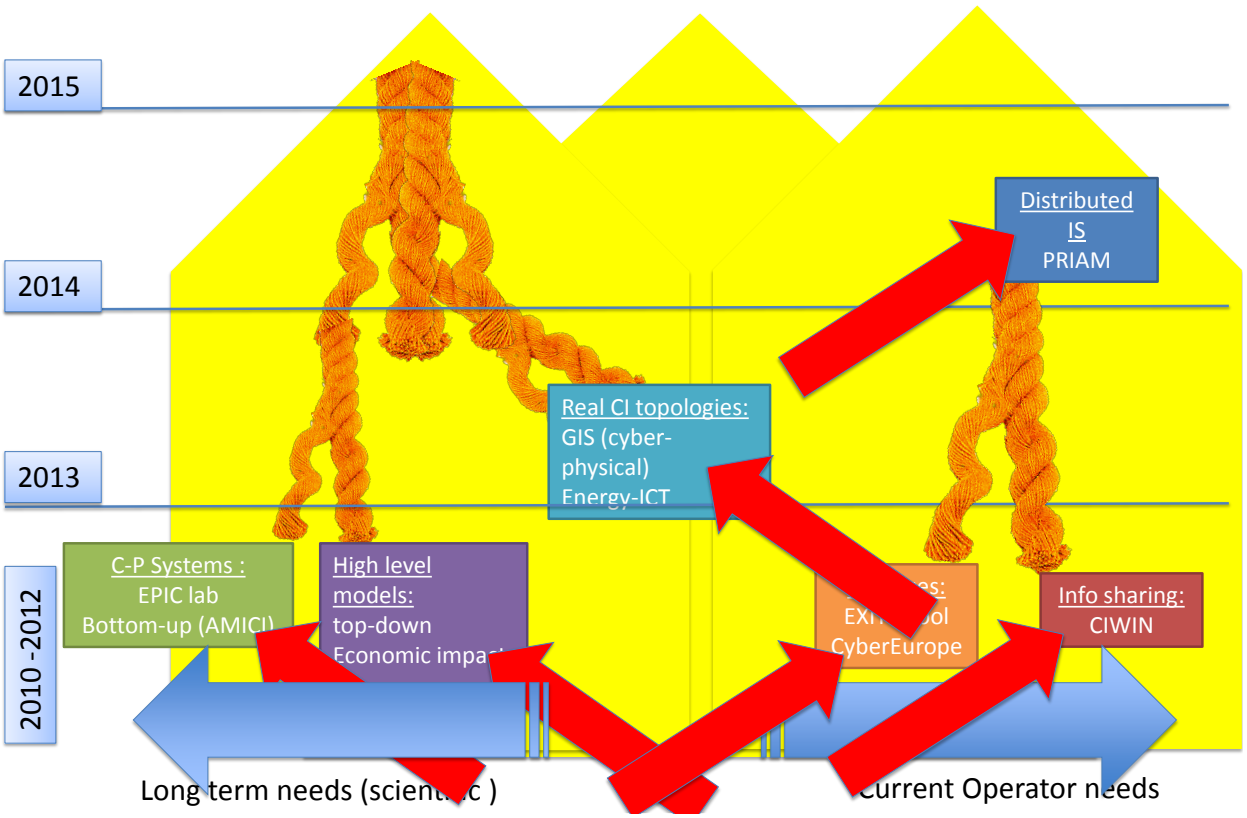
www.jrc.ec.europa.eu

Serving society
Stimulating innovation
Supporting legislation

JRC and CIPS

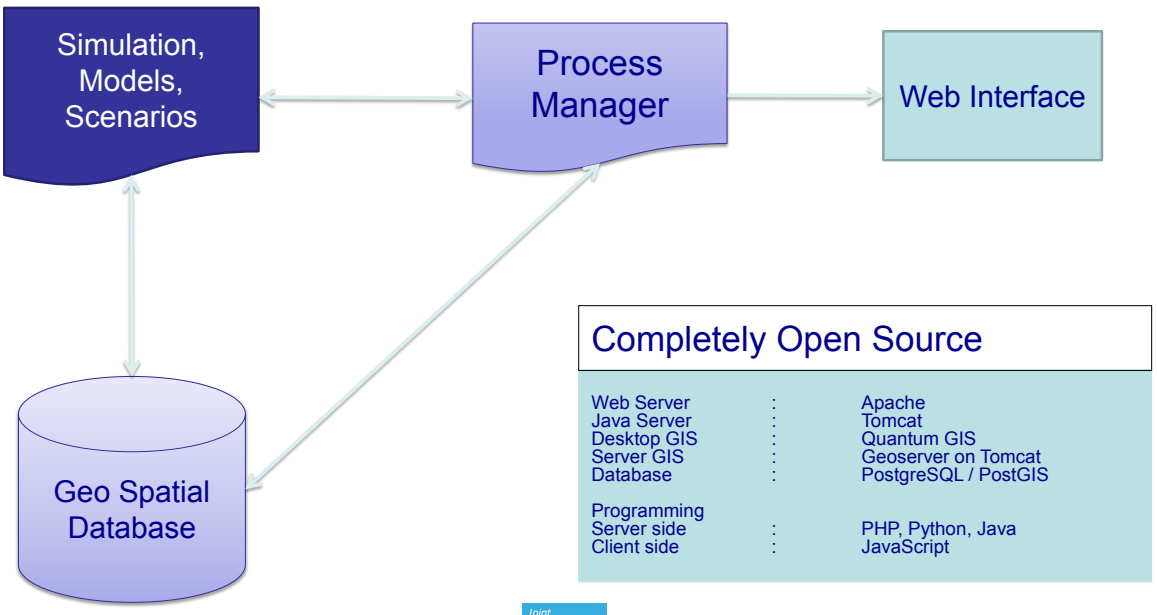
- **JRC**: 7 scientific institutes in 5 countries
- **CIPS projects**: 2 different institutes
  - **Institute for the protection and security of the citizen**
    - Security Technology Assessment Unit
    - European Laboratory for Structural Assessment Unit
  - **Institute of Energy and Transport**
    - Energy Security Unit

CIP work in a nutshell



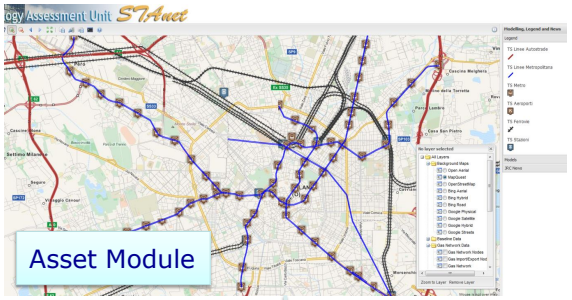
European Commission

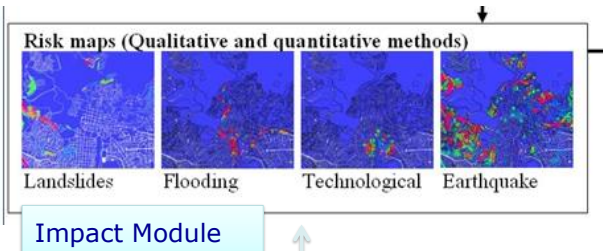
Technology Overview of CI Risk and Resilience Platform

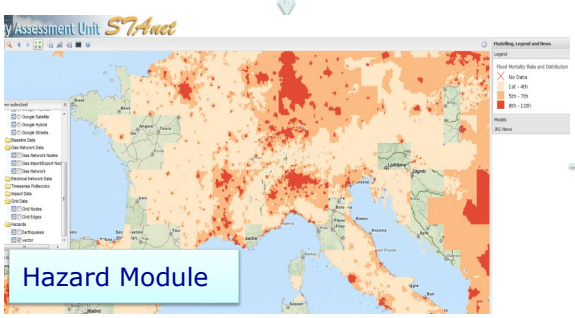


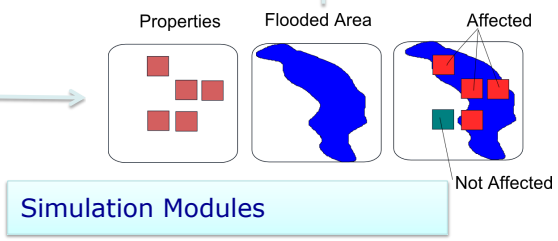
Joint Research Centre

Technology Overview of CI Risk and Resilience Platform









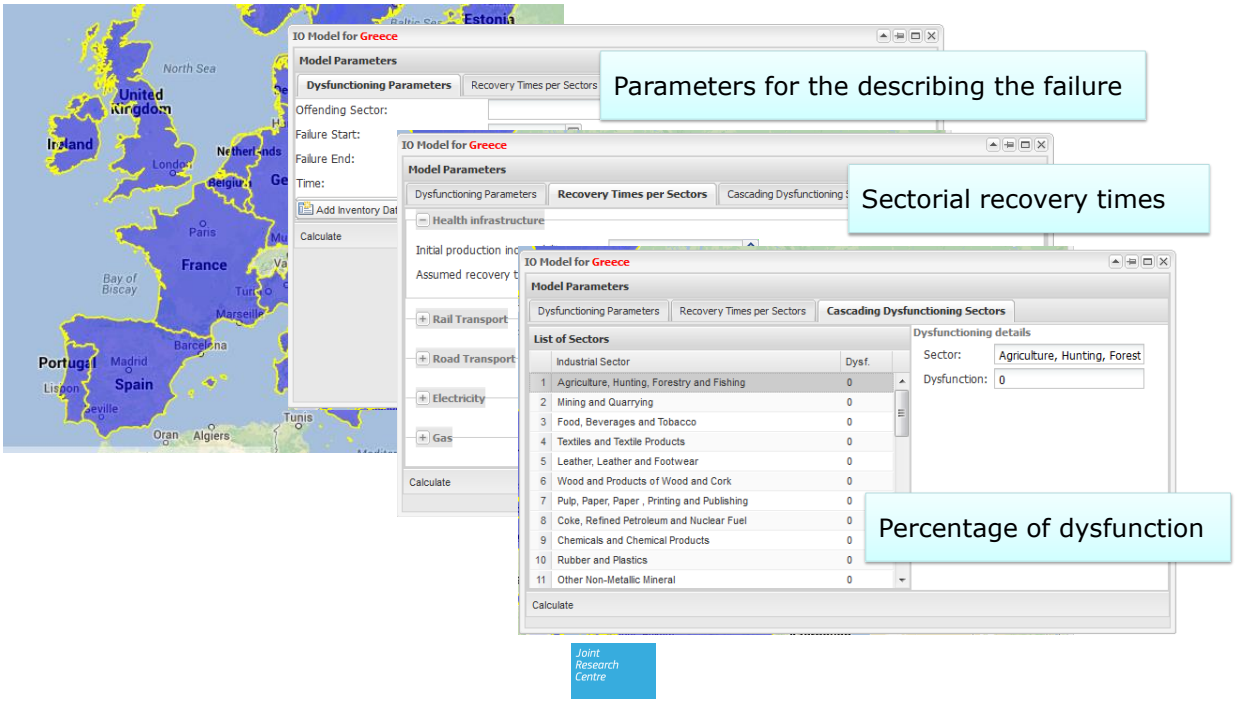
Joint Research Centre

Geospatially Enabled Simulation Models

- **GIS Platform** — Data management
- **Network Criticality** — Prioritization of critical infrastructure for funding allocation procedures
- **Input-Output Model** — Inter-sectoral quantitative economic assessment on European economies in case of disruptive events (based on Wassily Leontief model)
- **Geomagnetic Induced Currents** — Impact assessment on European power networks due to the geomagnetic fields
- **Internet dependencies model** — Interdependencies between Internet and other critical infrastructures (e.g. power grid)

Joint Research Centre

Input–output model and estimation of economic impact



Presentation and open discussion on the future CIP-related research for 2014-2020 financed by DG HOME

Mrs Eva-Maria Engdahl, DG HOME

The presentation by Mrs Engdahl was focused on the new structure of the CIPS program. Among others she referred to the proposed changes, the new structure due to legal particularities, the spending priorities for the period 2014-2020, the ISF-Police objectives and innovations, the distribution of the funding, the exploitation of the policy dialogue for the establishment of the National programs, the FP7-HORIZON 2020 funding for the CIP activities and the links with these purely research funds. Several of the elements shown in this presentation are not final but still under negotiation especially for issues related to budget.

Home Affairs funding 2014-2020

Internal Security Fund - Police

12 November 2013

European Commission
Home Affairs

Current situation:

- Overall budget 2007-2013: EUR 6,449 million
- Fragmented funding: 4 Funds and 2 Programmes
- Asylum, immigration and borders: shared management with annual programming within multiannual framework
- Security: patchy centralised management
- Poor at responding to events / crises
- Lack of synergy with EU agencies
- Complex regulatory framework

The changes we propose:

DRAFT

- **Simplify by reducing the number of instruments:**
  - Asylum and Migration Fund
  - Internal Security Fund
- **Focus on policy needs and results:**
  - Multiannual programming with policy dialogue
  - External dimension (territorial continuity)
  - Faster and more effective response to emergencies
  - Better use of expertise of EU agencies

Spending priorities for 2014-2020:

DRAFT

Fund	EUR million	Key projects
Asylum and Migration Fund	**3,869**	Common European Asylum System, resettlement & relocation, integration at local level, assisted voluntary return
Internal Security Fund	**4,648**	Internal Security Strategy
- Police cooperation, preventing and combating crime and crisis management	1,128	Joint Investigation Teams, TFTS, cybercrime, anti-radicalisation Critical infrastructure protection, risk & crisis management
- Borders & visa	3,520	Integrated border management, EUROSUR, smart borders, consular cooperation, STS

ISF-Police - Objectives

DRAFT

High level of security in the EU

Preventing and combating organised crime and cooperation between law enforcement

- Promote coordination, cooperation & info exchange among MS LEA
- Foster European judicial & law enforcement culture through EU training policy
- Strengthen MS capacity to prevent & combat cross-border, serious & organised crime
- Develop measures for protection & support of witnesses & victims of crime

Enhance capacity to manage security risks and protection of critical infrastructure

- Strengthen MS capacity to protect critical infrastructure in all sectors
- Ensure Effective coordination b/w crisis cooperation actors at EU & national level
- Strengthen MS capacity to develop comprehensive threat & risk assessment

ISF-Police – Distribution of funding

DRAFT

Shared management

Basic amount

National allocations based on the following criteria:
- size of population;
- size of territory;
- number of passengers and cargo processed;
- inverse proportion to GDP
- [European critical infrastructure designated]

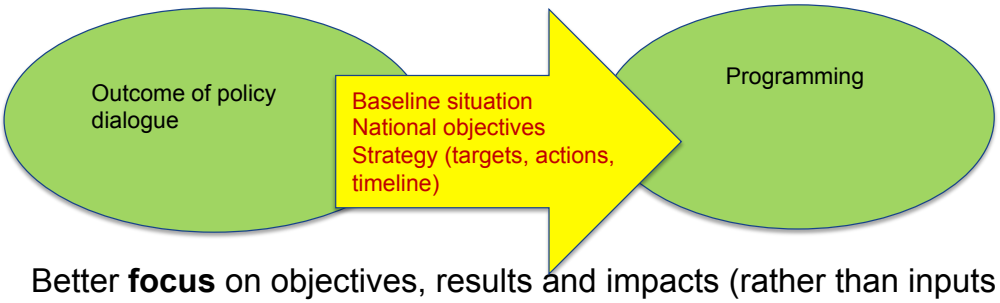
No variable amount + No extra funds at mid-term review

Centralised management

Union actions, emergencies, external actions, TA CION

Translating the outcome of the policy dialogue into national programme

DRAFT



- Better **focus** on objectives, results and impacts (rather than inputs and outputs),
- Greater **coherence** between the national programme and EU level objectives and priorities ("added value of the Union budget")

FP7 funding for CIP activities

- Several research projects under the FP7 Security theme for "Increasing the Security of infrastructures and utilities".
- Total budget: ~300 M€ (2007-2013)
- Ranging from energy, transport, communications grids, cyber crime, surveillance, etc

Horizon 2020 funding for CIP activities

- One of the eight priorities in the "Secure societies" challenge is: *"Protect and improve the resilience of critical infrastructures*"
- The first draft WP includes a call on *"Disaster resilient society",* with currently 6 topics on Critical Infrastructure Protection

Priorities as regards future CIP activities

- Better links to EPCIP policy developments
- Better links between research funding in Horizon 2020 and CIP policy needs
- Better use of existing tools and of results from research

Open discussion, conclusions and future meetings

The last part of the workshop was dedicated to the open discussion. The presentation by Mrs Engdahl on the future of CIPS triggered a number of questions, varying from technical to more generic ones.

A question was referring to the way that the participants will apply in the future, where it was made clear that each applicant should apply in its country, as the money for projects will be allocated to the participants directly by the authority for the National program. The general idea is to move gradually from the centralized management to the so called "shared management".

Another question was about the practical details of transition such as the life of the program, the partner participation and the response to either National or European priorities. HOME's response clarified these issues; The MS will provide HOME with their National programs, which will be adopted for seven years (period 2014-2020). Once the objectives set by the MS are adopted, they can be changed or revised, but these will constitute in any case the priorities for a seven-year period. The leading authority for the CIP activities at each MS will be called Managing Authority and will take under its responsibility the call for the proposals, the allocation of the money, bringing together the experts and evaluating the results. Another concern was about the frequency of the calls which will be decided at National level. The response was that the money allocated for this seven-year period

should be proportionally absorbed each year, so the MS will launch their calls as soon as their National programs are adopted by the Commission.

Another concern was referring to the increase of the budget, however HOME replied that the budget will cover more activities such as external dimension, etc. Another question was made for the budget allocation portion between the tenders and the calls for proposals at National level. The response was that the allocation of budget at National level will lie under the responsibility with the Managing Authority. What is important is that the budget for direct management will decrease in favour of the shared management.

Another question was referring to Managing Authorities and whether they have been selected, if they currently work on their National programs and if experts have been selected to participate somehow in this work, for example through workshops. HOME provided the participants with the transition process; the policy dialogues have taken place, a "Key-priorities paper" was issued, a document which combines the Commission's priorities and National priorities and constitutes the basis of the National programs. At the end of this dialogue phase, the National programs will be finalized. Furthermore, once the final decision for the available budget will be in place, the proportion of the shared over the centralised management will be decided.

Another question was set to identify which are the assessment criteria of the Commission for approving/ rejecting the National programs. HOME replied that the evaluation of the National programs will be based on whether they cover the objectives that the Commission wants to achieve, as described in the presentation by Mrs Engdahl. The latter responded also to the question "which are the authorities who participate in the policy dialogues". The participants of the MS usually come from the Ministry of Interior or the Ministry of Justice, whereas from the Commission's side is the Director general and senior staff.

A discussion opened when a comment was made to suggest the stronger connection between the different projects. HOME expressed their intention to improve this link between projects and stated that JRC has played an important role on that. The workshop itself was considered as a step towards that direction where the stakeholders have the chance

to evaluate the outcome of the projects and move forward with the exploitation of the results. This is a continuous process, to realize what has been achieved and identify the gaps. Under this perspective, it's likely that in the future there will be fewer projects, but more focused ones which will facilitate the link of the projects in order to develop the policy. A balance should be found to decide upon the optimum size of the projects.

Another point of the discussion was the link between the National and the European projects, nevertheless this a challenge as this is the first time that HOME applies shared management practices for CIPS.

The discussion was also focused on role that the Commission should play as a coordinator for the dissemination of best practices and the establishment of the security priorities, with the collaboration of the MS. The National programs will built the national capacity at national level, where the European funds will be focused on what should be shared to increase the benefit at European level.

At the end, it was agreed that the workshops should continue and the CIPS IV was set for next year.

European Commission
EUR 26537 EN – Joint Research Centre – Institute for Protection and Security of the Citizen

Title: **CIPS III workshop on research projects financed by DG HOME CIPS specific programme**

Authors: Athina Mitsiara, Georgios Giannopoulos

Luxembourg: Publications Office of the European Union

2014 – 130 pp. – 21.0 x 29.7 cm

EUR - Scientific and Technical Research series – ISSN 1831-9424
ISBN - 978-92-79-35583-7

Doi: 10.2788/12429

Abstract

The CIPS projects are financed by DG HOME within the framework of the specific programme «Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks». JRC-IPSC organizes for a third time a dedicated workshop for these projects. The audience of this workshop is composed from researchers, policy makers and national authorities. Bringing together these competences is of instrumental importance in order to steer research projects towards policy makers needs and provide to the policy makers the latest research trends in the domain of Critical Infrastructure Protection. In particular the CIPS III workshop, aimed at providing elements of the future security related research funded by DG HOME. This workshop took place in Brussels, and the intention is to continue the organization of these workshops on yearly basis.

LB-NA-26537-EN-N

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new standards, methods and tools, and sharing and transferring its know-how to the Member States and international community.

Key policy areas include: environment and climate change; energy and transport; agriculture and food security; health and consumer protection; information society and digital agenda; safety and security including nuclear; all supported through a cross-cutting and multi-disciplinary approach.

Publications Office

Doi: 10.2788/12429
ISBN - 978-92-79-35583-7