JRC TECHNICAL REPORTS

European Reference Network for Critical Infrastructure Protection (ERNCIP)

Annual Report – 2016 edition

Peter Gattinesi
Joint Research Centre

2016

Version Final – 17 May 2016

Joint Research Centre

European Reference Network for Critical Infrastructure Protection (ERNCIP)

Annual Report – 2016 edition

This publication is a Technical report by the Joint Research Centre, the European Commission's in-house science service. It aims to provide evidence-based scientific support to the European policy-making process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

JRC Science Hub
https://ec.europa.eu/jrc

JRC101440

Table of contents

Acknowledgements

The ERNCIP Project is extremely fortunate to enjoy the support of many expert organisations and individuals who share the desire to work collaboratively, and usually on a completely voluntary basis, in order to improve the security of critical infrastructure in Europe.

We are very grateful to all individuals and organisations that have contributed to the work of ERNCIP. In particular, the ERNCIP Office wishes to acknowledge the support of the organisations that have provided the coordination function for an ERNCIP thematic group. Our thanks go to:

- Aristotle University of Thessaloniki, GR
- The Centre for Applied Science and Technology (CAST), UK
- CEA, FR
- Environment Agency, AT
- Fraunhofer-EMI, DE
- HT Nuclear Oy, FI
- IBM, UK
- Iconal Technology, UK
- JRC, IRMM, Geel
- STUK, FI
- Thales, FR
- TNO/CPNI, NL.

Abstract

The ERNCIP network has been established to improve the protection of critical infrastructures in the EU. ERNCIP therefore works in close cooperation with all types of CIP stakeholders, focusing particularly on the technical protective security solutions.

This report aims to assist the dissemination of the results of the European Reference Network for Critical Infrastructure Protection (ERNCIP) activities.

It is intended that the report will be updated and issued by the ERNCIP Office in spring each year. The information provided will be up to date as of the end of the previous calendar year, i.e. in this case as at 31 December 2015.

The report summarises the achievements of the ERNCIP Thematic Groups, providing a convenient way to access information on any specific theme of interest covered by ERNCIP.

The report also describes current thematic group activities, to allow subject-matter experts and critical infrastructure operators to identify ongoing areas of research they might be interested in assisting.

This report is publicly available via the ERNCIP web site, and will be distributed to all ERNCIP Group of EU CIP Experts for onward dissemination within their Member State.

1. Introduction

1.1 Purpose of this Report

This report aims to assist the dissemination of the results of the European Reference Network for Critical Infrastructure Protection (ERNCIP) activities.

It is intended that this report will be updated and issued by the ERNCIP Office in spring each year. The information provided will be up to date, as of the end of the previous calendar year, i.e. in this case as at 31 December 2015.

The report summarises the achievements of ERNCIP, particularly of the Thematic Groups, providing a convenient way to access information on any specific theme of interest covered by ERNCIP.

The current thematic groups are covered in Section 2, with descriptions of the current activities, allowing subject-matter experts and critical infrastructure operators to identify ongoing areas of research they might be interested in assisting. Thematic Groups that have completed their work and have now been concluded are described in Section 3.

This report will be publicly available via the ERNCIP web site, and will be distributed to all ERNCIP Group of EU CIP experts for onward dissemination within their Member State. The role of this ERNCIP advisory group, and of the other ERNCIP forums, is described in Section 5.

1.2 Description of ERNCIP

The ERNCIP network has been established to improve the protection of critical infrastructures in the EU. ERNCIP therefore works in close cooperation with all types of CIP stakeholders, focusing particularly on the technical protective security solutions.

ERNCIP has established a large network of experts to improve the availability of security solutions through common European testing standards, and harmonisation of test methodologies and protocols, and common user guidelines. The approach taken involves the creation of a series of working networks of volunteer European experts, assembled in the form of Thematic Groups. Each Thematic Group is led by a Coordinator organisation, appointed by ERNCIP on the basis of its European standing as a recognised authority in that area. Other experts are recruited from organisations that have a recognised expertise in the subject matter.

Each Thematic Group produces a work programme for its activities planned for the coming year. These activities are broken down into tasks, each with a lead expert, specific objectives, timescale and identified volunteer expert contributors. The work programme is approved by the ERNCIP Office and coordinated with the sponsoring Directorate General (DG), so that participation by experts at planned meetings can be funded by ERNCIP.

Unless classified, all written outputs from the Groups are published through the JRC's publication system, and also made available through the ERNCIP web site.

ERNCIP has also created an online information repository of EU CIP-related experimental capabilities, the ERNCIP Inventory, explained in Section 4.

2. Currently-active ERNCIP Thematic Groups

2.1 Thematic Group - Detection of Explosives and Weapons in Secure Locations (DEWSL)

2.1.1 Background

This Group, coordinated by Iconal Technology Ltd, UK, has analysed the needs for standards and harmonisation in the detection of explosives and weapons at locations that have a secure perimeter, such as government buildings, industrial locations, nuclear sites, ports, and major event venues. This was achieved by a thorough investigation of the following access control categories:

- Checkpoint security screening of people and their belongings;
- Mail screening;
- Vehicle screening;
- Large deliveries screening;
- Building & area search.

2.1.2 Achievements - Reports

NB The Group's published reports can be downloaded at DEWSL TG

1. Summary of Proposed Recommendations – Consultation draft

For each of the access control categories, a series of conclusions and recommendations for standardisation and other activities at a European level to support Critical Infrastructure and other facility operators were identified. Where possible, these activities re-use and build upon material that exists at a local or national level. The draft report was circulated in late 2015 to relevant stakeholders, mainly facility operators and security managers, who were invited to comment and participate in a stakeholder consultation workshop.

2. Report of recommendations

A final report, incorporating the conclusions from the consultation workshop, has been produced, and is in the process of publication.

2.1.3 Achievements – Consultation

1. Consultation workshop

The consultation workshop was held in Brussels on 15 December 2015, and was attended by approximately 15 stakeholder representatives of facility operators and security managers as well as representatives of DG HR (Security directorate), DG TAXUD, DG HOME, DG JRC, a seconded expert from the US NIST and representatives of EOS (European Organisation for Security) representing security equipment manufacturers, system and service providers. The stakeholders strongly supported the TG's recommendations and priorities.

2.1.4 Current Objectives

This Group has been commissioned by DG HOME (Innovation and Industry for Security) to operate from January 2016 to December 2016, with the following high-level goals:

- Propose EU standardisation activities to mitigate the risk of explosives and weapons attacks at secure locations with low to medium throughput, for consideration by the EU standardisation community, and help instigate the CEN-CENELEC Workshop Agreement process;

- Investigate the opportunities for EU standardisation and other support activities that will best support user needs for mitigating the risk of explosives and weapons attacks at secure locations with high throughput (e.g. large sporting and entertainment events) and at public places/mass transportations locations (with no secure perimeters).

2.2 Thematic Group - Chemical and Biological Risks to Drinking Water

2.2.1 Background

Water quality is a critical factor in public health, with the vulnerability of our water supply chain well documented by incidents of accidental contamination. Therefore fast, reliable, sensitive and affordable water-monitoring systems are needed.

The focus of this Group, coordinated by the Environment Agency, Austria, is harmonising the testing methodologies of real-time alarm systems, which help to prevent or mitigate harm caused by drinking water contamination. The work concentrates on:

- The use of innovative techniques (probes, sensors, etc.) and enabling technologies for online measurement of the water quality in drinking water distribution networks
- Rapid identification and quantification of chemical and biological contamination in drinking water.

2.2.2 Achievements - Reports

NB The Group's published reports can be downloaded at WATER TG

1. Screening for chemicals in water

This provides a brief overview of the existing methods for the non-targeted screening of organic compounds in water samples by means of mass spectrometry. This review is based on the studies that can be performed by different mass spectrometry approaches. In addition, the most relevant European institutions working on this topic and contributing to the development of the non-target screening of pollutants are identified.

Report link = Screening for chemicals in water

2. Review of sensors to monitor water quality

In recent years, increased concern that deliberate or accidental contamination will reach the consumer has led to water supply operators considering early warning systems. An early warning system is an integrated system for online monitoring, collecting data, analysing, interpreting, and communicating monitored data, which can then be used to make decisions early enough to protect public health and the environment, and to minimise unnecessary concern and inconvenience to the public. To these ends, new sensors to detect chemical and microbiological compounds are being introduced to the market, especially by small to medium-sized enterprises.

The main impediments to effective implementation of sensors are:

- a lack of standards for contamination testing in drinking water, both in the EU and in the USA
- poor links between available sensor technologies and water quality regulations.

Report link = Review of sensors to monitor water quality

3. Monitoring techniques for biological contaminants

Currently, there are only limited technologies to monitor pathogenic agents available on the market. The report provides an overview of the major technologies being developed and evaluated that could have potential as monitoring systems in the near future.

Report link = Monitoring techniques for biological contaminants

4. Methods for the rapid identification of pathogens in water

Microbiological water contaminants represent an acute health risk. There are a wide variety of bacteria and viruses that can potentially be found in drinking water resulting from either a malicious or a natural contamination. Whatever the origin, rapid identification of the contamination is needed to ensure water quality and citizen safety. Although various detection and identification methods exist, they are mostly time-consuming and unsuited to emergent harmful micro-organisms. New developments are emerging to address this concern.

The desk study describes the main basic technologies to identify pathogens (such as immunological and genetic methods, mass spectrometry, micro-arrays and physical approaches), as well as their applications in the drinking water area. Some promising technologies under development are presented, especially integrated tools and new concepts in mass spectrometry. Additionally, different projects funded by the European Commission are briefly reported in the study, providing some clarity about the various scientific initiatives and networks working on this issue.

Report link = Methods for the rapid identification of pathogens in water

5. Vulnerability Assessment of Drinking Water in Europe

Many Member States have included the security of water supply in their national security plans and conducted vulnerability assessments. Several countries conduct research at the national level aimed at safeguarding water supply. The report identifies a fragmented structure for water infrastructure protection in Europe, with some overlaps in responsibility for security of drinking water across different organisations, because of the wide variety of threats that could potentially compromise the integrity of a water supply system.

The final report has been produced, and is in the process of publication.

6. Synthesis of existing legislation, guidelines, standards, organisations and projects related to drinking water safety and monitoring

In order to define the basic elements for harmonisation in the field of drinking water safety and security, existing European Standards and Directives are presented in the synthesis. A specific focus is made on biological risks. It clearly appears that little information is available for biological monitoring and only a few microorganisms are recommended for monitoring.

Outside Europe, guidelines and directives are available either at the international (WHO) or national (Canada, USA, Australia) levels. Although the risks may vary from one country to another, these documents can be considered as models, as they include reference scientific information.

Various European partnerships also exist to tackle water quality (JPI-Water, EIP-Water, EurEau, WISE, and Mandate/487). All these networks are of great importance because they connect the major stakeholders in the water sector (i.e. institutions, private companies, operators, governmental agencies, regulators).

The final report has been produced, and is in the process of publication.

7. Proposal for the elements of a Water Security Plan.

A Water Security Plan is different to a Water Safety Plan, although the proposals for a Water Security plan will be aligned with the Drinking Water Directive, where possible.

These proposals are intended to be the basis for consultation with stakeholders in Member States, including EurEau members. A Water Security Plan would focus on on-line monitoring, as close to real-time as possible, of drinking water quality supplied from the drinking water treatment plant to consumer, in order to improve protection against contamination. Implementation of a Water Security Plan would also improve the day to day operational management of the supply of drinking water.

The final report has been produced, and is in the process of publication.

2.2.3 Achievements – Consultation

1. Consultation workshop on Early Warning Systems

One priority of this Group is early warning systems that aim at preventing the intake of drinking water from treatment plants and drinking water networks affected by malicious or harmful events. Ideally, these systems trigger an alarm as soon as the quality of the source water or the drinking water differs from normal, allowing the operator to react quickly. A second priority deals with the analytical identification of 'unknown' chemical and/or biological contaminations in drinking water following an incident.

This workshop analysed screening methods used for the purpose of identifying and quantifying the individual contaminants rapidly as a basis for risk mitigation and crisis management. The relevant ERNCIP state-of-the-art reports were also discussed.

Report link = Consultation workshop on Early Warning Systems

2.2.4 Current Objectives

This Group has been commissioned by DG HOME (Innovation and Industry for Security) to operate from January 2016 to December 2016, with the high-level goal of identifying the requirements for harmonisation of real-time monitoring systems related to chemical and biological threats in drinking water in 2016, by scoping the basic elements of event detection systems that form part of a water security plan.

The basic elements to be assessed will comprise mandatory parameters (repeatability, reproducibility etc.), thresholds, other parameters that take into account natural variations of water composition (different raw water sources, blended water, disinfection etc.), chemical parameters as surrogate for biological contaminations (protein markers, metabolites), software requirements, maintenance aspects, and validation aspects (both in the field, and in the laboratory).

2.3 Thematic Group - Radiological and Nuclear Threats to Critical Infrastructure

2.3.1 Background

This Group, coordinated by HT Nuclear OY, FI, is addressing three issues in the field of detection of radiation:

- *List-mode data acquisition based on digital electronics.*

  Time-stamped list-mode data format produces significant added value compared to the more conventional spectrum format. It improves source localisation, allows signal-to-noise optimisation, noise filtering. Some new gamma and neutron detectors require list-mode data acquisition in order to function.

- *Expert support of field teams, i.e. data moves instead of people and samples.*

  Fast and high quality response can be achieved with fewer people (Reach-back).

- *Remote-controlled radiation measurements and sampling using unmanned vehicles.*

  There are several measurement and sampling scenarios that are too risky for humans to carry out. Applications envisaged are: reactor and other accidents, dirty bombs before and after explosion, search of sources out of regulatory control etc.

2.3.2 Achievements - Reports

NB The Group's published reports can be downloaded at RN TG

2.3.2.1 List-mode data acquisition reports

1. List-mode data acquisition

This deals with digital radiation detection systems employing list-mode data collection, which improves data analysis capabilities. Future data acquisition systems will enable the movement electronically of detection data from first responders to analysis centres, rather than the costly and time consuming process of moving experts and/or samples. This new technology is especially useful in crisis events, when time and resources are sparse and increased analysis capacity is required. In order to utilise the opportunities opened by these new technologies, the systems have to be interoperable, so that the data from each type of detector can easily be analysed by different analysis centres. Successful interoperability of the systems requires that European and/or international standards are devised for the digitised data format. The basis of such a format is a list of registered events detailing an estimate of the energy of the detected radiation, along with an accurate time-stamp for recorded events (and optionally other parameters describing each event).

Report link = List-mode data acquisition

2. Critical parameters and performance tests for digital data acquisition hardware

Recent developments of digital data acquisition systems allow real-time pre-processing of detector signals at a high count rate. These so-called pulse processing digitizers are powerful and versatile instruments offering techniques which are important for nuclear security, critical infrastructure protection, nuclear physics and radiation metrology. Certain aspects of digital data acquisition affect the performance of the total system in a

critical way and therefore require special attention. The report presents a short introduction to digital data acquisition, followed by a discussion of the critical parameters which affect the performance in the lab and in the field. For some of the parameters, tests are proposed to assess the performance of digital data acquisition systems. Good practices are offered to guide the selection and evaluation of digital data acquisition systems. More general performance criteria which are not specifically related to digital data acquisition systems are discussed separately.

Report link = Critical parameters and performance tests for digital data acquisition hardware

3. Data format for list-mode digital data acquisition: Survey results

The Group conducted a survey of users of digital data acquisition for nuclear instrumentation to investigate their needs with respect to the standardisation of the data format, based on the findings of the Group's earlier report on list-mode data acquisition. The report presents the results of the survey, which served as an important input for the development of a preliminary draft standard that accompanied a new work item proposal for a new international standard, which was successfully submitted to the IEC in the frame of the EMPIR Project 14SIP07 'DigitalStandard'.

Report link = Survey results

2.3.2.2 Reachback reports

4. Remote Expert Support of Field Teams

One of the main issues facing the EU security industry is its highly fragmented nature, exhibiting a lack of standardisation and of harmonised certification procedures. The need for standardised information sharing between competent authorities and international bodies regarding radiation measurements and data analysis has been recognised by experts in the response to Commission mandate M/487 for the establishment of European security standards.

The report suggests a way forward to develop protocols for more efficient cooperation between competent authorities and remote expert support or reachback centres at the national and international level. Not all EU Member States have the capabilities to process data provided by nuclear security instruments, and thus should consider instigating a coordinated capability yielding a more efficient and comprehensive approach in responding to future nuclear emergencies. This could be achieved by reachback centres across Europe (built upon existing national facilities and expertise) and would provide analysis services for alarm adjudication. Efficient data sharing and processing across EU Member States requires the use of standard data formats and protocols.

Report link = Remote Expert Support of Field Teams

5. Information sharing in a nuclear security event

The Thematic Group designed a simple questionnaire, which was sent to the relevant authorities in the Member States. The answers (10 received) came from very different organisations working in the domains of security, safety or the military. The different backgrounds of the responding organisations imply that responsibility for nuclear and radiological matters, including information sharing in a nuclear security event, varies strongly between different Member States.

It appears that much still needs to be done in raising European awareness regarding the prevention and detection of, and the response to, nuclear security events, including

information sharing nationally and internationally. Some Member States have not yet identified the need for cooperation in sharing nuclear spectrometric data and analysis results.

One of the basic requirements of the proposed new information-sharing system for nuclear security is that advanced national analysis resources be provided for Member States that do not have such capabilities. Even though the future arrangements for information sharing would be based on a standard technological structure, all data exchange would be voluntary and bilateral between the Member States.

Report link = Information sharing in a nuclear security event

6. National reachback systems for nuclear security

This review of the operational systems for nuclear security covers Finland, France, Denmark, UK, US and Canada. The Finnish case is a holistic approach to Nuclear Security Detection Architecture, as defined by the International Atomic Energy Agency; reachback is only one component of the system, albeit an important crosscutting element of the detection architecture. The French and US studies concentrate on the reachback itself. The Danish nuclear security system is information-driven, relying on the cooperation of the competent authorities. The British and Canadian analyses describe nuclear security planning and operations for a major public event, the Olympics, where cooperation between the frontline officers and the reachback centre plays a key role in reducing radiological and nuclear risks.

For the implementation of an efficient reachback system there is a strong need for standardising the data acquisition, storing and final distribution of the analysis results. Major nuclear powers take this activity very seriously, and they have 24/7, all-year national service for information processing. The case studies of Finland and France show that efficient European reachback is manageable and technically possible on a country-wide basis. The case study on Denmark reveals that countries with limited reachback resources need an adequate and standardised technical information-sharing mechanism to aid their national analysis services in a precise and timely manner.

Report link = National reachback systems for nuclear security

2.3.2.3 Unmanned detection systems reports

7. Use of unmanned systems for radiation measurements and sampling

There is a significant potential for the use of unmanned remote controlled vehicles in sampling and measuring radiological events. No attempt to standardise sampling and measurement methods using these types of vehicles has yet been made. Common standards would simplify the use of remote-controlled vehicles in an emergency scenario and therefore would be valuable in critical infrastructure protection. The main advantage with unmanned systems in radiological events is the protection of the people involved.

The report provides the current state-of-the-art of unmanned systems that have potential to be used for radiation measurements and sampling. It is believed that search and rescue robotics is the domain closest to the radiation measurement scenarios. Therefore, a definition for search and rescue robotics is provided, and their major subsystems are outlined. This is followed by a review of deployment scenarios for search and rescue robots, outlining case studies of major emergencies at which robots have been deployed, with an assessment of their value to the emergency services. Additionally, research and development in search and rescue robotics, including current projects, testing environments and search and rescue robotics competitions, is outlined. Furthermore, the report describes sensor systems capable of radiation detection based on state-of-the-art radiation sampling using unmanned ground vehicles, unmanned aerial vehicles with rotary wings or unmanned aerial vehicles with fixed wings.

Report link = Use of unmanned systems for radiation measurements and sampling

8. Possible scenarios for radiation measurements and sampling using unmanned systems

This document focuses on possible scenarios for remote control radiation measurements and sampling using unmanned systems. First, there are prevention scenarios where unmanned systems can be used to prevent incidents involving radioactive material and deterrence. Second, there are response scenarios where unmanned systems can be used to gather information after incidents with radioactive material have occurred. The three main tasks (spatial mapping, search of sources and sampling) for unmanned systems are condensed in the identified scenarios. The report also summarises possible standards for unmanned systems. A very widely recognised standard collection of software frameworks for robot software development is the robot operating system. Further important standards concerning communication with robots and control of unmanned systems are battle management language, interoperability profile and joint architecture for unmanned systems.

Report link = Possible scenarios for radiation measurements and sampling using unmanned systems

9. Use of robots/unmanned systems detecting radiological or nuclear threats

The report describes a survey of experts from the radiological/nuclear and robotics communities. Scientists, especially from the robotics community, are well represented in the survey, although there was a lack of input from industry and end-user communities. Most responders agreed with the scenarios identified in the ERNCIP report "*Possible scenarios for radiation measurements and sampling using unmanned systems*" (EUR 27225). For additional sensors, most responders suggested inclusion of position and time for radiation measurements. Responses on the issues of bottlenecks and future topics point to the manoeuvrability, autonomy and communication of robots, as well as decontamination and human-robot interaction.

Report link = Use of robots/unmanned systems detecting radiological or nuclear threats

2.3.3 Achievements – New work item for a standard

List-mode is data acquisition based on digital electronics. Time-stamped list-mode data format produces significant added value compared to the more conventional spectral data format.

The work on list-mode data format standards instigated by this Group will now continue primarily in the EURAMET EMPIR 14SIP07 – DigitalStandard project. This project builds upon the pre-normative work of this Group, and is specifically dedicated to the development of a draft international standard, including tools to support its implementation, under the auspices of the IEC Technical Committee (TC) 45 "Nuclear Instrumentation". A new work item proposal for the development of a standard was submitted on 15th October 2015, and accepted by IEC/TC 45 in February 2016. The coordination of the DigitalStandard project is managed by the JRC work package 3883 Digital Standards for Nuclear Security (DiSNU).

2.3.4 Current Objectives

This Group has been commissioned by DG HOME (Innovation and Industry for Security) to operate from January 2016 to December 2016, with the following high-level goals:

- Reachback: To raise awareness within EU Member States on the benefits of information sharing nationally and internationally with remote experts (reachback) for detection of, or response to, nuclear security events, and identify the elements for harmonisation of a standard technological structure for spectrometric measurements

- Unmanned detection systems: To support the development of European robotics/RN detection exercises, trials and/or competitions using the Group's work on RN scenarios

- List-mode: to fully support the EMPIR Digital Standard project that will continue the work started by this ERNCIP Group on the development of a standard for list-mode data.

2.4 Thematic Group - Resistance of Structures to Explosive Effects

2.4.1 Background

Critical buildings (e.g. malls, governmental buildings and embassies), infrastructure and utilities, rail and subway stations need protection against being damaged, destroyed or disrupted by deliberate acts of terrorism, criminal activity and malicious behaviour. Normal building regulations and guidelines do not usually take into account these threats. The introduction of regulations or guidelines should support the resilience of the buildings and infrastructure against explosive incidents.

The focus of this Group, coordinated by Fraunhofer EMI, is to develop guidelines to help harmonise procedures in the testing of structural elements against explosion-induced loads. As the loading characteristics of an external and an internal explosion are quite different and need to be considered separately, the Group will focus on testing methods for only external detonations. The Group will concentrate on far-field blast loading and the specification of the test methods to define the resistance of structural elements against this loading. The Group has decided to start with an element for which a regulation is available that enables certification products with an explosion resistance class, which in this case is windows and glazing. In future phases, the same process of harmonising test methodologies and protocols will be considered for other structural elements.

2.4.2 Achievements - Reports

NB The Group's published reports can be downloaded at STRUCTURES TG

1. Resistance of structures to explosion effects - review of testing methods

The report provides a comprehensive summary of the existing experimental methods used to analyse and test the resistance of glazing and windows under blast-loading conditions, using high explosives and using blast simulators called shock tubes. Additionally, the potential of numerical simulations is highlighted in terms of their applicability to the different glass materials.

A short, comprehensive theoretical background is given for each method, covering requirements, implementation and the related measurement techniques, along with an interpretation of the measurements.

Report link = Resistance of structures to explosion effects - review of testing methods

2. Numerical simulations for classification of blast-loaded laminated glass

The report summarizes existing best practices for the numerical finite element modelling of blast loading, including the important topics of domain discretisation, implicit/explicit formulation, Lagrangian/Eulerian solvers, the mathematical description of the material behaviour etc. Furthermore, recommendations for the modelling of laminated glass elements are formulated and knowledge gaps in this application area are pointed out.

The report builds the basis for an evaluation of the different numerical methods, their suitability to certain problems, and their capability to support/complement the experimental testing of glass components. It thus provides information to help design architects and engineers, and more generally for critical infrastructure stakeholders, responsible for the structural integrity and security of the infrastructure in case of an explosion.

Report link = Numerical simulations for classification of blast loaded laminated glass

3. A comparison of existing standards for testing blast resistant glazing and windows

The report discusses the differences between the existing standards for testing blast resistant glazing and windows and presents basic recommendations for the future development of the suite of European standards in this area.

Report link = A comparison of existing standards for testing blast resistant glazing and windows

4. Recommendations for the improvement of existing European norms for testing the resistance of windows and glazed façades to explosive effects

The report formulates the enhancement to the existing standards by way of recommendations for the improvement of the test standards.

Report link = Recommendations for the improvement of existing European norms for testing the resistance of windows and glazed façades to explosive effects

5. Standardisation of the numerical simulation of blast-loaded windows and facades

The determination of the blast protection level of laminated glass windows and facades is of crucial importance, and it is normally done by using experimental investigations. In recent years numerical methods have become much more powerful also with respect to this kind of application. The report gives an initial view of possible standardisation concerning such numerical simulations. Attention is drawn to the representation of the blast loading and of the behaviour of the material of the mentioned products, to the geometrical meshing, as well as to the modelling of the connections of the glass components to the main structure. The need to validate the numerical models against reliable experimental data, some of which are indicated, is underlined.

Report link = Standardisation of the numerical simulation of blast-loaded windows and facades

2.4.3 Current Objectives

This Group has been commissioned by DG HOME (Innovation and Industry for Security) to operate from January 2016 to December 2016, with the following high-level goals:

- To present the Group's findings on existing experimental standards for testing the resistance of windows and glazed facades to explosive effects to national contact points for standardisation, and to consult with them on the feasibility of proposing enhancements to existing CEN standards.

- To consult with CEN and national standardisation bodies on any existing standards for numerical simulation for testing the resistance of windows and glazed facades to explosive effects, and then identify a suitable way forward, possibly through a CEN-CENELEC Workshop Agreement.

2.5 Thematic Group - Detection of Indoor Airborne Chemical & Biological Agents

2.5.1 Background

The overall aim of this group, coordinated by the Aristotle University of Thessaloniki, is to investigate issues that can be addressed in the EU level regarding Detection, Identification and Monitoring of airborne chemical and biological threats in enclosed spaces. Three main activities are underway:

- In order to evaluate the applicability of the current sensor technologies and what has to be done, we need to evaluate what we expect from the sensors against chemical and biological threats in enclosed spaces. The starting point of the overall approach is the definition of relevant scenarios of indoor airborne threats (chemical and biological) in critical infrastructures

- The specific needs that have to be met by sensors will define the criteria for a review on the existing sensors for chemical or for biological agents available in the EU. Computational simulations will provide the spatial and temporal gradients of contamination within indoor critical infrastructures

- Finally, evaluation of capabilities of existing sensors based on the capability to perform early warning, will allow the Group to identify the gaps and to define requirements for next generation detectors in the EU.

2.5.2 Current Objectives

This Group has been commissioned by DG HOME (Terrorism and Crisis Management) to operate from August 2015 to August 2016, with the following high-level goals:

- To define relevant scenarios of indoor airborne threats (chemical and biological) in critical infrastructures

- To perform a critical review on the existing sensors available in the EU and used (a) for chemical agents and (b) for biological agents

- To identify the gaps and to define requirements for next generation detectors in the EU.

The Group started its work in September 2015. Information is available at AIRBORNE TG

2.6 Thematic Group - European IACS (Industrial Automation and Control Systems) Components Cyber-security Compliance and Certification Scheme

2.6.1 Background

Information and Communication Technology is becoming increasingly important for the delivery of essential services. Recent incidents have increased awareness of the vulnerability of Industrial Automation and Control Systems (IACS) to cyber-attacks which could disrupt physical infrastructure systems and networks. This makes security of IACS an important part of critical infrastructure protection.

Work started within ERNCIP on this thematic area with the Thematic Group – IACS & Smart Grids, coordinated by TNO/CPNI, NL. That work led to a second Thematic Group - Case Studies for the Cyber-Security of Industrial Automation and Control Systems, coordinated by Thales, FR, the conclusions of which included proposals for a European IACS Components Cyber-security Compliance and Certification Scheme.

The current thematic group in this thematic area, also coordinated by Thales, is now underway with the support of DG CNCT and ENISA to consult widely on the proposals for the Compliance and Certification Scheme, and to establish the initial steps that will lead to its implementation.

2.6.2 Achievements - Reports

NB The Group's published reports can be downloaded at IACS Case Studies TG

1. Case Studies for the Cyber-security of IACS

Industrial Automation and Control Systems (IACS) increasingly constitute a target for cyber-attacks aiming at disturbing Member States' economies, at disabling our critical infrastructures or at taking advantage from our people. Such hostile acts take place in a context of geostrategic tensions, for the satisfaction of organised crime's purposes, or else in support of possible activist causes. The report addresses the questions: "*Do European critical infrastructure operators need to get IACS' components or subsystems tested and "certified" with regards to their cybersecurity?*" And if so "*What are (roughly) the conditions of feasibility for implementing successfully a European IACS components cybersecurity Compliance & Certification Scheme?*"

Report link = Case Studies for the Cyber-security of IACS

2.6.3 Achievements - Certification

1. Global Industrial Cyber Security Professional (GICSP) Certification

One of the sub-groups of the IACS & Smart Grids Thematic Group directly contributed to the Global Information Assurance Certification (GIAC) initiative that led to the launching of the vendor-neutral Global Industrial Cyber Security Professional (GICSP) Certification scheme in September 2013. This enables professionals working in this field to obtain accreditation in cyber security for IACS and critical infrastructure.

Link to Global Industrial Cyber Security Professional Certification web site

2. Proposals for a European IACS Components Cyber-security Compliance and Certification Scheme

In 2014, the Case Studies for the Cyber-Security of IACS Thematic Group produced an initial proposal for a European IACS Components Cybersecurity Compliance and Certification Scheme.

2.6.4 Current Objectives

This Group has been commissioned by DG HOME (Terrorism and Crisis Management) to operate from August 2015 to August 2016, with the following high-level goals:

- To verify, with the support of ENISA and selected Members, the stakeholders' interest for the European IACS components Cyber-Security Compliance & Certification Scheme proposal, their constraints and priorities, and to detail the plan for the subsequent projects.

- To identify the work to be done in the implementation phase of the Proposal including the experts needed to accomplish the tasks.

- To extract from designated existing standards, their common good practices and requirements and to organize them into a common classification covering an agreed set of domains of Compliance & Certification: the definition of targets of evaluation, cyber-security engineering domains and practices, vulnerabilities assessment, development process assessment, cyber robustness testing, etc.

- To define generic IACS cyber-security profiles including classes of IACS products and target levels of cyber-security, operating and security environments, etc.

- To define a common process for each of the levels of the proposed European IACS components Cyber-security Compliance & Certification Scheme.

- To provide an EC-managed database of compliance & certification evaluated IACS products.

2.7 Thematic Group - Video Surveillance for Security of Critical Infrastructure

2.7.1 Background

Recent years have seen a growth in the use of video surveillance technologies as part of the package of protective security measures used to protect critical infrastructures and other valuable assets. Academia and industry have been investing time and money in relevant technology innovations, but there is a lack of standardisation, testing and accreditation in Europe that would help users to ensure that video surveillance products are fit for their purposes.

This Thematic Group, coordinated by CAST, UK, is identifying the activities at European level on video surveillance technologies that will assist operators of critical infrastructure improve their protective security.

2.7.2 Achievements – Reports

NB The Group's published reports can be downloaded at VIDEO TG

1. Surveillance and video analytics: factors influencing the performance

The report gives a brief introduction into the topic of surveillance, and describes what is required to create an understanding of the relevant factors for surveillance systems and video analytics. The approach taken uses a morphological analysis of the surveillance domain. The report contains a description of this approach and the result of the first step of the analysis: the identification of these factors and the generic nature of their influence. The report gives examples of how this method can be used to describe key aspects in the domains of surveillance and video analytics.

Based on the overview of relevant factors for surveillance systems, it is also possible to describe the relevant factors for the subcomponent of video analytics. This approach facilitates operators of critical infrastructure and their security partners, e.g. Law Enforcement Agencies, to describe their context, environment and threats in a specific manner. Next, they can seek interaction with security partners and industry to specify relevant capabilities that should work there. If certain elements of that solution are not yet available off-the-shelf, then further interaction with research and development partners can be sought, for example by searching for existing video test data sets which match this challenge. If none exist, then a data set can be created based on such a specification.

Report link = factors influencing the performance of video systems

2. Surveillance Use Cases: Video Analytics

The report describes surveillance use cases in the context of protection of critical infrastructure. The focus in the report is on video analytics, with the aim to facilitate the interaction with the relevant communities by providing a limited set of surveillance-use cases, clustered around different surveillance application areas.

The scope of the report is contemporary surveillance in the physical domain for the protection of CI against security incidents. Protection includes the prevention, disturbance, containment, response and investigation of security incidents. The specific use cases are based on the needs of CI operators and respective law enforcement agencies tasked with this protection throughout the EU.

Report link = Video Surveillance Use Cases

2.7.3 Current Objectives

This Group has been commissioned by DG HOME (Terrorism and Crisis Management) to operate from August 2015 to August 2016, with the following high-level goals:

- To determine how EU standards activities could best support user needs for the evaluation of video surveillance systems

- To produce a guide for end users of factors to consider regarding the deployment of automated video surveillance

- To determine how best to enable Collation/Common access to data sets in the EU for testing/evaluation of video surveillance software.

2.8 Thematic Group - Applied Biometrics for Security of Critical Infrastructure

2.8.1 Background

CIP stakeholders have posed a series of security and privacy challenges that will need to be addressed by biometric and other security technologies. Biometrics has capabilities that are difficult to realise in other ways, but there are challenges that need to be addressed to use them successfully.

This Group, coordinated by IBM UK, has focussed on on-going standardisation activities and initiatives, such as the ISO standard on facial recognition from closed-circuit TV images, and the CEN standard on biometric physical access control.

There are also issues associated with privacy and biometric data that will need to be addressed for successful implementation of biometric technology. The activity under this ERNCIP mandate will be to articulate these issues, explore their impact and identify future activities needed to address them.

2.8.2 Achievements - Reports

NB The Group's published reports can be downloaded at BIOMETRICS TG

1. Experiences from Large Scale Testing of Systems using Biometric

The report is aimed at organisations considering the implementation of large-scale identification systems (e.g. national-scale systems which may cover many millions of individuals). Many of the lessons and issues identified will also be useful for organisations looking to develop more general systems based on biometric technology. The report describes a systematic approach to testing, based on lessons learnt from a case study of large-scale testing of biometric systems. This approach will enable the performance of a proposed biometric matching system to be characterised to ensure that it is 'fit for purpose', and that the benefits outlined in justifying the system can be achieved.

Report link = Experiences from Large Scale Testing of Systems using Biometric

2. Application of Biometrics: Guidance for Security Managers

Biometric technologies have advanced considerably over the past decade, and are now widely used by governments, commercial enterprises and, more recently, by the consumer through the introduction of sensors and apps on mobile phones. The report provides information about the application of these technologies to achieve secure recognition of individuals by organisations operating critical infrastructures in the EU. As a specific example, it offers guidance about the implementation of physical access control systems using biometric technologies. It is principally addressed at managers and security officers within these organisations. With this, managers and officers should be in a better position to discuss their specific requirements with technology suppliers, specialist systems integrators and consultants – and therefore lead to applications which are more secure without compromising on their usability. The report emphasises the importance of considering the effectiveness of the entire application – and not just focussing on the performance of the biometric subsystem.

Report link = Application of Biometrics: Guidance for Security Managers

3. Summary of the activities of the Biometrics Thematic Group

The report documents the usage of biometric identity technology, such as fingerprint, iris or face recognition, which is foreseen to become more and more common for access control in critical infrastructure and for travel documents. Test and evaluation presents challenges of scale because the required correct identification rates are often high and the acceptable false alarm rate low, so very many test data records must be run to determine the performance.

Report link = Summary of the activities of the Biometrics Thematic Group

2.8.3 Achievements – Standardisation Activities

1. ISO/IEC Joint Technical Committee (JTC 1/SC 37) for Biometric Standards, regarding biometrics in CCTV

At the January 2014 plenary meeting of ISO/IEC JTC1 SC37 (The international standards subcommittee on biometrics), a new work item was adopted on use of operator-assisted automated face recognition in CCTV systems. This Thematic Group contributed significantly to the development of one of the base documents which complemented the submission from the South Korean national standards body, and continues to discuss and collate comments on the ongoing draft.

The multi-part standard will be applicable primarily to the use of automated face recognition in video surveillance systems for a number of use cases and scenarios of operation. Examples include real-time operation against watch-lists and post-event analysis of video data.

The standard will also support related recognition and detection tasks in video surveillance systems such as:

- estimation of crowd densities
- determining patterns of movement of individuals
- identification of individuals appearing in more than one camera
- use of other biometric modalities such as gait or iris recognition
- use of specialized software to infer attributes of individuals, e.g., estimation of gender and age
- interfaces to other related functionality, such as video analytics for behaviour to measure queue lengths or alerting for abandoned baggage.

2. CEN Technical Committee (TC) 224 Working Group (WG) 18 – Biometrics, regarding biometrics for physical access control

During 2014 a new work item proposal was presented at CEN-TC224 WG 18 for standard development on biometric physical access control activities. The ERNCIP thematic group was represented at WG 18 meetings, supporting the activity as it moves through to the committee draft stage. It is expected that the standard will be achieved in 2017. It is anticipated that this standard will then be made available to ISO/IEC JTC1 SC37 as a base document for development in 2017.

2.8.4 Current Objectives

This Group has been commissioned by DG HOME (Terrorism and Crisis Management) to operate from August 2015 to August 2016, with the following high-level goals:

- To help operators of critical infrastructure (CI) implement better security solutions through the standardisation/evaluation/testing/certification at ISO level of the biometric systems that provide facial recognition from closed-circuit TV images

- To help CI operators implement better security solutions through the standardisation/evaluation/testing/certification at CEN level of the biometric systems (e.g. fingerprints/retina) that support physical access control within a secure area

- To help CI operators implement solutions that address challenges to privacy throughout their implementation and operation.

3. Completed ERNCIP Thematic Groups

3.1 Thematic Group - Aviation Security (AVSEC)

3.1.1 Background

The European Commission has defined technical specifications and performance requirements for various types of detection equipment used at EU airports. The introduction of eligible instruments and performance requirements in EU legislation calls for European common testing methodologies (CTMs) for detection equipment, to facilitate mutual recognition of approved or certified equipment. The challenges associated with the EU Regulation were that there are no standard approval procedures in the EU for aviation detection equipment, with diverse security equipment standards at Member State level.

Consequently, a common EU certification, testing and trialling scheme for aviation security equipment was required. The focus of this Group was on the aviation sub-sector, with activities covering:

- Technical specifications and detection requirements
- Common testing methodologies (CTM)
- Development of an EU certification system
- Technical exchanges with third countries and international organisations.

This Group ran from February 2012 until the end of 2013, and was coordinated by the JRC Institute for Reference Materials and Measurements, Geel. In this period, 55 experts representing 35 organisations participated in the Group. In all, six meetings were held; three full plenaries, and three topic sub-group meetings. Most of the work completed by the Group was undertaken by dedicated working sub-groups, reporting to the full general plenary meetings. Close cooperation within the European Commission (JRC, DG ENTR, DG HOME and DG MOVE) was essential, and representatives from all these DGs participated. The Group directly supported the Commission Regulatory Committee on Aviation Security, the European Civil Aviation Conference (ECAC) Technical Task Force, and the Rolling Programme annexed to the Cooperation Arrangement between the European Commission and ECAC.

3.1.2 Achievements - Reports

NB The Group's published reports are classified EU LIMITE, and therefore cannot be downloaded. More information at AVSEC TG

1. Technical Considerations on Explosives Trace Detection in EU Legislation

Explosives trace detectors (ETD) are security detection equipment which indicates presence of explosives by detecting trace amounts of explosives, either in the form of particulate material or as a vapour. The study gives an overview of the implementation of ETD in Regulation and provides an expert assessment of how it may be improved, particularly regarding guidance on sampling.

2. Detection Requirements and Testing Methodologies for Aviation Security Screening Devices

The study was carried out to get a better view of the performance requirements and testing methodologies for screening equipment at civil airports employed in the EU and EFTA Member States, including the process of acquiring equipment. The study was based on a questionnaire that was distributed via the Regulatory Committee on Aviation Security to EU and EFTA states' authorities in November 2012. The results show that 18

of the 27 countries that responded to the questionnaire have an approval procedure in place for aviation security equipment regarding threat detection performance. Only four countries, however, issue product certificates. Procurement of equipment for passenger and hold baggage screening is typically handled by airports while for in-flight supplies and cargo it is sometimes handled by regulated agents. On-site acceptance tests are required in 11 of the countries while 19 countries conduct daily tests. Two entities are mainly responsible for adjusting sensitivity settings: the airport operators and the appropriate authorities.

3.1.3 Achievements – Feedback to ECAC

1. ECAC proposals for CTMs for Explosive Detection Systems and Liquid Explosives Detection Systems

Comments on the ECAC proposals for CTMs for Explosive Detection Systems and Liquid Explosives Detection Systems (EDS and LEDS) were drafted by the Group, agreed, and delivered to the ECAC secretariat and the Study Group chairs of the ECAC EDS and LEDS groups.

2. ECAC proposals for CTM for Security Scanners

Comments on the ECAC proposals for CTM for Security Scanners (SSc) were drafted by the Group, agreed, and delivered to the ECAC secretariat and the Study Group chair for the ECAC SSc group.

3.2 Thematic Group - Explosives Detection Equipment (non-Aviation) (DEMON)

3.2.1 Background

Since the 2006 transatlantic aircraft plot, the EU has defined technical specifications and performance requirements for various types of detection equipment used in EU airports, which call for European Common Testing Methodologies (CTMs) for detection equipment, to facilitate mutual recognition of approved or certified equipment.

However, this kind of arrangement is not yet at the same maturity level for the detection of explosives outside the framework of aviation security e.g. for mass transport, special events, crowded places. This Group, coordinated by CEA, FR, ran from April 2012 until the end of 2013, and considered the different types of needs among non-aviation operators. In this period, 15 experts representing 11 organisations participated in the Group. In all, five meetings were held.

3.2.2 Achievements - Reports

NB The Group's published reports can be downloaded at DEMON TG

1. Statement of User Needs

The report identifies user needs in the area of explosives detection for infrastructure protection applications (outside of aviation security). It spans guidance, training, equipment development, canine capability, and assurance, and considers various categories of infrastructure sites reflecting different detection needs.
NB This report is classified EU LIMITE, and therefore cannot be downloaded.

2. European Legislation relating to Explosives and Explosive Detection System

The report summarises European legislation relevant to explosive detection equipment, apart from that contained in the Aviation Security regulations. Although few other articles of European Union law directly refer to explosive detection, a number of directives and regulations are relevant to it, in the fields of explosives for civil use and pyrotechnics, dual-use equipment, chemicals and the chemical industry, port and inland transport security, and radiation, electromagnetic and electrical safety. Future European legislation in this field may be expected to conform to the principles of the EU's New Legislative Framework, according to which harmonised standards are used to express detailed technical specifications. Current standardisation work is therefore also briefly described.

Report link = European Legislation relating to Explosives and Explosive Detection System

4. ERNCIP Inventory of Laboratories

4.1 Description

The ERNCIP Inventory of laboratories is a searchable, central repository of information on European experimental and testing facilities with CIP-related capabilities.

The objective of the Inventory is to help all types of critical infrastructure stakeholders to identify and make contact with CIP-related experimental facilities that have competency in their areas of interest.

The Inventory is a web search tool storing comprehensive profiles of European laboratories, accessible via an Internet browser.

URL: https://erncip.jrc.ec.europa.eu

The JRC launched the Inventory of laboratories and facilities operating in the specific context of the protection of critical infrastructure in June 2012.

4.2 Achievements

The Inventory includes 120 registered laboratories and can be consulted via a dedicated web application. This allows the community of inventory users to search for general information about each recorded facility, the services they offer (incl. experience, competencies and accreditations), the available experimental/testing equipment and relevant points of contact.

In 2014, the ERNCIP Office conducted an assessment on the standards, best practices and guidelines that labs with their profile recorded on the ERNCIP have declared to follow in their testing activity.

Based on this, in 2015 ERNCIP started defining a directory of existing international standards for security that could become a reference for CIP-related testing activities, linked to the ERNCIP Inventory, thereby integrating standards in use referenced from the new directory. The aim of the ERNCIP Standards Directory is to make it easier for CI operators to identify the laboratories performing the evaluation of products, systems or services, according to relevant standards for testing against security requirements.

4.3 How laboratories can participate

European laboratories can participate in the ERNCIP Inventory by following the registration procedure directly on the web.

URL: https://erncip.jrc.ec.europa.eu/ and select the 'REGISTER' icon.

Membership of the ERNCIP Inventory provides operators of CIP-related experimental and testing facilities with greater visibility among CIP communities. A presence in the Inventory will result in:

- Promotion of experimental facilities to CIP communities around the world
- Increased business potential, as the Inventory will be used by public and private sector organisations seeking solutions to their problems
- Increased potential for cooperation and exchange of knowledge with similar experimental/testing organisations.

4.4 How users can access information

The Inventory helps all types of critical infrastructure stakeholders from all around the globe (e.g. government authorities, infrastructure operators, and research institutions) to identify and make contact with CIP-related experimental expertise located in the EU, when they have a need for:

- Specific knowledge or expertise on CIP security-related problems (e.g. to consult, cooperate, or hire)
- Certified solutions to CIP security-related problems (e.g. procurement, consultancy, assessment)
- Research partners (e.g. to conduct CIP-related experiments, or to form partnerships to bid for EU funded projects).

Organisations can become Inventory Search Users by registering at the ERNCIP Inventory system. When an organisation has successfully registered as an ERNCIP Search User, any employee of that organisation will have the ability to access the Inventory.

URL: https://erncip.jrc.ec.europa.eu/ and complete the "Access for Searching" section.

5. Other ERNCIP Activities

5.1 ERNCIP Group of EU CIP Experts

Members are nominated for this ERNCIP expert group by the Member State government authorities responsible for national critical infrastructure protection, based on their knowledge on existing European and national critical infrastructure protection policies and programmes. This group acts as an advisory body to ERNCIP, with each member having the important role to link their Member States' CIP communities and ERNCIP. Ideally, there would be a representative from each of the 28 Member States. As at 2015, 17 Member States have participated in this forum, which normally meets bi-annually.

The role of this Group is to discuss, and offer strategic advice to the ERNCIP Office and thematic groups on:

- Creation, membership, and termination of ERNCIP thematic groups
- Progress and outcomes of the thematic groups
- Main documents produced by ERNCIP
- Development and use of the ERNCIP Inventory and Platform
- ERNCIP governance issues
- Creating and maintaining trust within ERNCIP
- ERNCIP's external communication strategy, including cascade of the ERNCIP outputs.

5.2 The ERNCIP Academic Committee

The ERNCIP Academic Committee, comprising renowned senior scientists in fields relevant to CIP, was first convened in 2013, to provide a link between academia and ERNCIP. In 2015, the main activity involved advising on the development of training for professionals involved in the safe and secure design, implementation, operation, management and regulation of critical infrastructures, in respect of protection and resilience against technical failures, man-made attacks and natural hazards.

Details at academic committee

5.3 ERNCIP Operators' workshops

The purpose of the ERNCIP operators workshops is to provide an "end-user pull" for the ERNCIP work, whereby ERNCIP results and findings can be disseminated and discussed in the end-user communities. In this way, ERNCIP and its thematic groups can obtain immediate feedback on their work, and build further relationships with infrastructure operators, who in essence are the end-users of CIP solutions. Two operator-focussed workshops have been held; in September 2013 and May 2014.

Details at operator workshops

5.4 ERNCIP cross-sector conferences

ERNCIP has organised a Trust Conference on 29-30 November 2011 and two ERNCIP conferences (12-13 December 2012 and 16-17 April 2015). These multi-stakeholder events gathered representatives from all ERNCIP stakeholder groups, Commission Directorate Generals, Member State authorities, industry, academia, research facilities, and operators.

Details at ERNCIP conferences

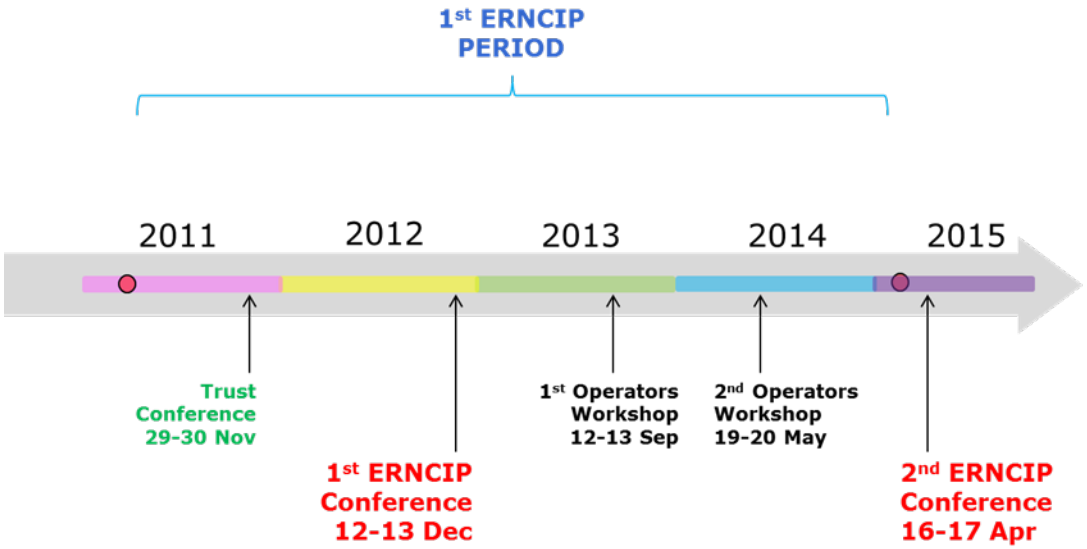

Figure 1 - Timeline of ERNCIP organised events

5.5 CIPRNet

ERNCIP is a partner in the CIPRNet (Critical Infrastructures Preparedness and Resilience Research Network) project, which aims to form the foundation for a European Infrastructures Simulation & Analysis Centre (EISAC).

This is funded through EU FP7-SECURITY/ Call SEC-2012.7.4-2; Networking of researchers for a high level multi-organisational and cross-border collaboration - Network of Excellence. The project started in March 2013 and will complete in March 2017.

CIPRNet has created and maintains CIPedia©, an online glossary of multi-national definitions related to CIP. Also, CIPRNet offers CIP-training activities in the form of lectures and master classes.

More details at www.ciprnet.eu

5.6 IMPROVER

ERNCIP is also a partner in the IMPROVER (Improved risk evaluation and implementation of resilience concepts to critical infrastructure) project, which aims to improve European critical infrastructure resilience to crises and disasters.

This is funded under EU H2020 Secure Societies/ Call: DRS-07-2014 - Crisis management topic 7: Crises and disaster resilience – operationalizing resilience concepts. The project started in June 2015 and will complete in May 2018.

The JRC and the IMPROVER partners, in collaboration with the CIPRNet project, have created a first draft of a lexicon of definitions.

More details at http://improverproject.eu/

Abbreviations and definitions

AIRBORNE TG	ERNCIP Thematic Group - Detection of Indoor Airborne Chemical & Biological Agents
AVSEC TG	ERNCIP Thematic Group - Aviation Security
BIOMETRICS TG	ERNCIP Thematic Group - Applied Biometrics for Security of Critical Infrastructure
CAST	The Centre for Applied Science and Technology, the scientific arm of the UK Home Office
CEN	European Committee for Standardisation
CENELEC	Standardisation association comprised of members who are the National Electro-technical Committees of European Countries.
CI	Critical infrastructure
CIP	Critical infrastructure protection
CIPRNet	Critical Infrastructures Preparedness and Resilience Research Network
CTM	Common testing methodologies
DEMON TG	ERNCIP Thematic Group - Explosives Detection Equipment (non-Aviation)
DEWSL TG	ERNCIP Thematic Group - Detection of Explosives and Weapons in Secure Locations
DG	Directorate General (functional department of the European Commission, which is split into over 30 DGs)
DG GROW	Previously DG ENTR - Internal Market, Industry, Entrepreneurship and SMEs
DG HOME	Migration and Home Affairs
DG HR	Human Resources and Security
DG MOVE	Mobility and Transport
DG TAXUD	Taxation and Customs Union
EC	European Commission
ECAC	European Civil Aviation Conference
EDS	Explosive Detection Systems
EFTA	European Free Trade Association

EIP-Water	The European Innovation Partnership on Water (EIP Water) is an initiative within the EU 2020 Innovation Union. The EIP Water facilitates the development of innovative solutions to address major European and global water challenges.
EMPIR	The European Metrology Programme for Innovation and Research is the main programme for European research on metrology.
ENISA	European Union Agency for Network and Information Security
EOS	European Organisation for Security
ERNCIP	The European Reference Network for Critical Infrastructure Protection
ETD	Explosives Trace Detection
EU	European Union
EURAMET	European Association of National Metrology Institutes
EurEau	EurEau represents Europe's drinking water and waste water service operators.
IACS	Industrial Automation and Control Systems
IACS Case Studies TG	ERNCIP Thematic Group - European IACS (Industrial Automation and Control Systems) Components Cyber-security Compliance and Certification Scheme
IEC	International Electro-technical Commission
IMPROVER	Improved risk evaluation and implementation of resilience concepts to critical infrastructure
ISO	International Organisation for Standardisation
JPI-Water	Launched in 2010, the Joint Programming Initiative *Water challenges for a changing world* (the Water JPI) tackles the challenge of achieving sustainable water systems for a sustainable economy in Europe and abroad, and deals with research in the field of water and hydrological sciences.
JRC	The Joint Research Centre – The DG that provides the Commission's in-house scientific service
LEDS	Liquid Explosives Detection Systems
Mandate 487	Programming mandate issued by the EC addressed to CEN, CENELEC and ETSI to establish security standards.
NIST	The National Institute of Standards and Technology (USA) - the federal technology agency that works with industry to develop and apply technology, measurements, and standards.

RN TG	ERNCIP Thematic Group - Radiological and Nuclear Threats to Critical Infrastructure
SSc	Security Scanners
STRUCTURES TG	ERNCIP Thematic Group - Resistance of Structures to Explosive Effects
TG	(ERNCIP) Thematic Group
VIDEO TG	ERNCIP Thematic Group - Video Surveillance for Security of Critical Infrastructure
WATER TG	ERNCIP Thematic Group - Chemical and Biological Risks to Drinking Water
WHO	World Health Organisation
WISE	WISE is a partnership between the European Commission (DG Environment, Joint Research Centre and Eurostat) and the European Environment Agency, and provides a gateway to information on European water issues.

JRC Mission

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 methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation