JRC TECHNICAL REPORTS

European Reference Network for Critical Infrastructure Protection:

ERNCIP Handbook 2018 edition

Gattinesi, P

Version Final – 31 May 2018

EUR 29236 EN

Contact information
Name: Georgios Giannopoulos
Address: Via Enrico Fermi, 2749, Ispra (VA), Italy I-21027
Email: JRC-ERNCIP-OFFICE@ec.europa.eu
Tel.: +39 0332 786211

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

JRC111880

EUR 29236 EN

PDF ISBN 978-92-79-85967-0 ISSN 1831-9424 doi:10.2760/245080

Luxembourg: Publications Office of the European Union, 2018

How to cite this report: Gattinesi P., *European Reference Network for Critical Infrastructure Protection: ERNCIP Handbook 2018 edition*, EUR 29236 EN, doi:10.2760/245080

Contents

Abstract

The ERNCIP network has been established to improve the protection of critical infrastructures in the EU. The European Reference Network for Critical Infrastructure Protection (ERNCIP) therefore works in close cooperation with all types of CIP stakeholders, focusing particularly on the technical protective security solutions.

This handbook aims to assist the dissemination of the activities and results of ERNCIP.

It is intended that the document 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 2017.

The report summarises the achievements of all 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 is distributed to all ERNCIP Group of EU CIP Experts for onward dissemination within their Member States.

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 the ERNCIP thematic groups. Our sincere 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, Geel
- STUK, FI
- Thales, FR
- TNO/CPNI, NL.

1. Introduction

1.1 Purpose of the ERNCIP Handbook

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

It is intended that this handbook 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 2017.

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

This document is publicly available via the ERNCIP web site, and is distributed to all ERNCIP Group of EU CIP experts for onward dissemination within their Member State. The role of this ERNCIP advisory group is described below.

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 technical protective security solutions.

ERNCIP has established a large network of experts to improve the availability of security solutions through common European testing standards, harmonisation of test methodologies and protocols, and common user guidelines. When ERNCIP was formally instigated in 2011, the first step was to create an online information repository of EU CIP-related experimental capabilities, the ERNCIP Inventory, further explained in Section 4.

The initial network of research institutions has been expanded through 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 subject-matter experts are recruited from organisations that have a recognised expertise in the subject matter, including from academia, research institutes, the security industry, infrastructure operators, government authorities and security agencies.

1.3 Governance arrangements – ERNCIP Group of EU CIP experts

ERNCIP is primarily funded by sponsoring European Commission Directorates, which specify their priority thematic areas to be researched. Additional Member State direction is provided to ERNCIP through its advisory forum, the ERNCIP Group of EU CIP experts. These CIP experts are nominated 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 also having the important role to link ERNCIP to their Member States' CIP communities. Ideally, there would be a representative from each of the 28 Member States. Up to 2017, 19 Member States have participated in this forum, which normally meets bi-annually 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. For instance, this Handbook is the direct consequence of a request emanating from this group.

Oversight of the work of the thematic groups by the JRC is effected through the ERNCIP Office which monitors the annual work programmes produced by each thematic group, detailing its activities planned for the coming year. These activities are arranged into tasks, each task having a nominated lead expert, specific objectives and timescale, and identified volunteer expert contributors. The work programme is approved by the ERNCIP Office and coordinated with the sponsoring Directorate General (DG) of the European Commission.

Most written outputs from the Groups are published through the JRC's publication system, and also made available through the ERNCIP web site. However, a few reports cannot be made publically available, and for further details of these reports, please contact the ERNCIP Office.

1.4 Summary of active ERNCIP thematic groups

ERNCIP currently has three sponsoring Commission Directorates:

1. DG HOME B4 (Innovation and Industry for Security), sponsoring four thematic groups:

   - *Detection of weapons and explosives in secure locations (DEWSL) TG*
     on European-level guidelines for vehicle screening at entry checkpoints (see 2.1).

   - *Chemical & biological risks to drinking water TG*
     producing guidance on production of Water Security Plans (see 2.2).

   - *Radiological & Nuclear threats to critical infrastructure TG*
     identifying how best to utilise the new list-mode data acquisition standard (IEC 63047) and emerging detection technologies to improve nuclear security, and defining the characteristics of a centralised system to support assessment and adjudication of radiological alarms (see 2.3).

   - *Resistance of Structures to Explosion Effects TG* (see 2.4)
     updating the risk assessment process for building design standards for explosive threats (see 2.4).

   All these thematic groups are running for 24 months from June 2017 to May 2019.

2. DG HOME D2 (Terrorism and Radicalisation), sponsoring two thematic groups:
   - *Detection of Indoor Airborne Chemical & Biological Agents TG*
     providing security managers with assistance in planning risk mitigation against these threats by use of available technologies (see 2.5).

   - *Early Warning Zones for Critical Infrastructure Protection: use of biometric and video technologies TG*
     identifying the state of the art on moving from isolated short-range systems used for biometric recognition to complete solutions that integrate the biometric elements with other information sources within a cognitive framework (see 2.7).

   Both these thematic groups are running for 24 months from May 2017 to April 2019.

3. DG CNECT, sponsoring the thematic group on the *European IACS (Industrial Automation and Control Systems) Cybersecurity Certification Framework (ICCF)*
   enhancing the proposed framework by exercises to simulate the behaviouristic and governance model. This thematic group completed in February 2018 (see 2.6). Discussions are underway in respect of the next phase of work within ERNCIP on improving IACS cybersecurity.

2. Currently-active ERNCIP Thematic Groups

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

2.1.1 Background

Explosives and weapons attacks are an increasingly common threat to the security of the citizen and society within the EU, as in other parts of the World. 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.

2.1.2 Achievements - Reports

NB The Group's published reports can be accessed via DEWSL TG, while for the other reports please contact the ERNCIP Office.

1. ERNCIP Detection of Explosives and Weapons in Secure Locations (DEWSL): Final Report Phase 1

This report addresses the requirements of facility operators and security managers who need to mitigate the threat of explosives and weapons attacks at locations with a secure perimeter at which screening for explosives and weapons threats can take place. Typical locations are critical infrastructure sites, secure government and commercial buildings, sports and entertainment venues, major political and cultural event venues. The report incorporates the conclusions from a consultation workshop held in December 2015 (JRC102800, 2016).

2. Research Needs for High Throughput Locations - Working Paper ERNCIP thematic group Detection of Explosives and Weapons at Secure Locations

This document presents a set of research topics to help mitigate 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). It also contains descriptions of four research topics recommended for consideration in future Horizon 2020 Calls for Proposals (JRC105353, 2016).

3. User Needs for High Throughput Locations: Working Paper ERNCIP thematic group Detection of Explosives and Weapons at Secure Locations

This working paper discusses the challenges and user needs for guidelines and research mitigating the risk of explosives and weapons attacks at secure locations with high throughput (e.g. large sporting and entertainment events) and at open sites with no secure perimeters (e.g. mass transportation locations with many entrances and exits) (JRC105354, 2016).

2.1.3 Other Achievements

Consultation workshop

The consultation workshop was held in Brussels on 15 December 2015, and was attended by infrastructure 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 participants strongly supported the Group's recommendations and priorities.

2.1.4 Current Objectives

The Group was commissioned in July 2017 by DG HOME (Innovation and Industry for Security) to undertake the activities necessary to create the relevant standardisation mechanism for production of European-level guidelines for security managers regarding the screening of vehicles at entry checkpoints, for weapons and explosives.

However, as it has not been possible to assemble sufficient experts prepared to work on this topic, other options are being explored to incept a thematic group within the broad area of detection of weapons/explosives, possibly in line with the other recommendations the DEWSL Group made in 2016.

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. The focus of this Group, coordinated by the Environment Agency, Austria, is harmonising real-time alarm systems, to help to prevent or mitigate harm caused by malicious 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 Highlight – Water Safety & security Workshop

Proposals to facilitate the use of Water Security Plans by water utilities were validated by the wider community (including National Authorities) at the Water Safety and Security workshop in December 2016. These proposals had been drafted from the outcomes of consultations during 2016 with national authorities, manufacturers of contamination sensors, and water utility operators.

2.2.3 Achievements - Reports

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

1. Screening for chemicals in water

This report provides an overview of the methods for the non-targeted screening of organic compounds in water samples by means of mass spectrometry (JRC89741, 2014).

2. Review of sensors to monitor water quality

This review of sensors being introduced to the market that detect chemical and microbiological compounds identified the main impediments against effective implementation of sensors as:

- 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 (JRC85442, 2014).

3. Monitoring techniques for biological contaminants

There are 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 future (JRC88228, 2014).

4. Methods for the rapid identification of pathogens in water

This desk study describes technologies that 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 (JRC92395, 2015).

5. Overview of Vulnerability Assessment of Drinking Water in Europe

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 (JRC100531, 2016).

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

A specific focus is made on biological risks, although little information is available for biological monitoring, with few microorganisms recommended for monitoring (JRC100533, 2016).

7. Proposals for a guidance related to a Water Security Plan to protect Drinking Water.

This document summarises the key findings from the reviews undertaken of water security planning in the EU. The recommendations for water security planning were discussed at the Water Safety and Security Conference, organised in Brussels by DG HOME, and positively received by the stakeholders, including policy makers (JRC105388, 2016).

2.2.4 Other Achievements

1. Consultation workshop on Early Warning Systems (27 April 2015)

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 reviewed.

2. Surveys on requirements for real-time monitoring systems related to CB threats to drinking water

Two surveys were conducted during 2016 to investigate the availability and suitability of online monitoring techniques to detect variations in water quality caused by intentional and unintentional contamination of drinking water distribution networks. The first survey was held among European water utilities; the second survey was distributed among more than 260 sensor manufacturers worldwide (JRC105463, 2016).

3. ERNCIP Survey of Security Provision for Drinking Water in Member States

This survey was conducted in 2016 to establish the status in Member States of drinking water supply as a critical infrastructure in national risk assessments. It identified, in broad terms, the extent to which security measures have been implemented and the views of Member State authorities on the requirements for further activities at EU level (JRC105403, 2016).

4. The Water Safety and Security Workshop (11-12 December 2016)

The Water Safety and Security Workshop organised in Brussels on the occasion of the 10th anniversary of the Groundwater Directive provided the platform for the discussion of proposals setting out the basis of a Water Security Plan. The concept was positively received by the stakeholders (including policy makers and other actors of the EU regulatory framework). The key outcomes were:

(i) the concept of a Water Security Plan being developed in line with existing Water Safety Plans is validated;

(ii) preference for guidance rather than further legislation emerged from the discussions, security being primarily a matter for Member States;

(iii) the concept of a demonstration project captured the audience's interest, and various issues related to online monitoring were addressed.

2.2.5 Current Objectives

The Group was commissioned in July 2017 by DG HOME (Innovation and Industry for Security) to produce a European-level guidance document that will support water utility operators who choose to produce a water security plan, thereby improving their control of water security. The format of this guidance will use the CEN Workshop Agreement template, as far as is possible.

In particular, the group will identify the current approaches to screening for contamination using online monitoring and event detection systems, investigating in particular issues to operators arising from the reliability of the detection methods and taking into account additional analytical procedures.

2.3 Thematic Group - Radiological and Nuclear Threats to Critical Infrastructure

2.3.1 Background

This Group, coordinated by HT Nuclear OY, FI, addresses these aspects concerning the 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, through central alarm adjudication:

  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 can be very risky for humans to carry out. Applications envisaged are: reactor and other accidents, 'dirty' bombs before and after explosion, search for sources out of regulatory control, etc.

- Novel detection technologies for nuclear security:

  New solutions are emerging from innovations in new materials and signal processing capabilities.

2.3.2 Highlight – New standard instigated by ERNCIP

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.

A new work item proposal produced by this group for the development of a standard was submitted on 15th October 2015, and accepted by IEC Technical Committee (TC) 45 "Nuclear Instrumentation" in February 2016. The First Committee Draft for the list-mode data format standard (IEC63047) was accepted by IEC TC 45 in October 2016, with a forecast publication date of July 2018.

The work on list-mode data format standards instigated by this thematic group is now continuing 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 TC 45.

2.3.3 Highlight – JRC/ GICNT workshop on expert support and reachback

In collaboration with the Global Initiative to Combat Nuclear Terrorism (GICNT), the JRC organised a two and a half-day workshop on expert support and reachback entitled *Magic Maggiore* at the JRC Ispra, Italy in 28-30 March 2017 see workshop details .

Through a series of presentations, case studies, panel discussions, and a demonstration exercise, *Magic Maggiore* helped raise awareness and build commitment towards technical reachback. The workshop presented best practices to address key challenges, and identified areas for future work in this field. The workshop included a real-time detection and reachback exercise for a hypothetical nuclear security incident, organised by the JRC (Ispra) and CEA France (Paris). The demonstration focused on core components of alarm adjudication and information exchange between front-line officers, a national reachback centre, and an advanced centralised reachback centre located in Paris.

2.3.4 Achievements - Reports

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

General Reports

1. This provides a summary of the activities of the RN Thematic Group of ERNCIP in 2016 (JRC105547, 2016).

List-mode data acquisition reports

2. 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 (JRC90741, 2014).

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

The report introduces digital data acquisition, and discusses the critical parameters which affect the performance in the lab and in the field. 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 (JRC93260, 2015).

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

The report presents the results of a survey of users of digital data acquisition for nuclear instrumentation to investigate their needs with respect to the standardisation of the data format. The survey served as 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' (JRC100408, 2016).

Reachback reports

5. Remote Expert Support of Field Teams

The report suggests 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 approach to respond to future nuclear emergencies (JRC94535, 2015).

6. Information sharing in a nuclear security event

The report presents the results of a questionnaire sent to Member States on information sharing in a nuclear security event. 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 (JRC98706, 2016).

7. National reachback systems for nuclear security

This review of the operational systems for nuclear security covers Finland, France, Denmark, UK, US and Canada. The case studies of Finland and France indicate that efficient European-level reachback is manageable and technically possible (JRC98711, 2016).

8. After-action Analysis of the Magic Maggiore Workshop on Expert Support and Reachback

This joint JRC/ GICNT workshop helped raise awareness and build commitment towards technical reachback in the event of a radiological incident. This list of post-workshop activities paves the way for the identification of the next steps towards development of European capabilities for nuclear security and in more general, for CBRNE security (JRC108920, 2017).

Unmanned detection systems reports

9. Use of unmanned systems for radiation measurements and sampling

The report provides the state-of-the-art of unmanned systems that could be used for radiation measurements and sampling. It also includes 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 (JRC95779, 2015).

10. 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. 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 (JRC95791, 2016).

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

The report describes a survey of experts in the radiological/nuclear and robotics communities. Most responders agreed with the scenarios identified by ERNCIP (JRC100475, 2016).

12. Report on use of robotics scenarios, ELROB Land Trials 2016

This report describes the state of the art of the unmanned systems with potential for radiation measurements and sampling. The report defines search and rescue robots and outlines their major subsystems, reviewing deployment scenarios and outlining case studies of major emergencies at which robots have been deployed. Additionally, research and development in search and rescue robotics, including current projects, testing environments and search and rescue robotics competitions, are outlined (JRC104392, 2016).

2.3.5 Current Objectives

The Group was commissioned in July 2017 by DG HOME (Innovation and Industry for Security) to identify how nuclear security can benefit from emerging technologies, such as new materials and segmented detectors, and to identify how they can utilise the new list-mode data acquisition standard. The Group will also define the characteristics of a centralised data management system that will efficiently support assessment and adjudication of nuclear alarms and alerts.

2.4 Thematic Group - Resistance of Structures to Explosion 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 or other malicious behaviour. Normal building regulations and guidelines do not usually take into account these threats. The future introduction of regulations or guidelines should support the resilience of the buildings and infrastructure against explosion incidents.

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 blast simulators called shock tubes. Additionally, the potential of numerical simulations is highlighted in terms of their applicability to the different glass materials (JRC87202, 2014).

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

The report summarizes existing good 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. (JRC94928, 2015).

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 recommendations for the future development of the suite of European standards in this area (JRC 94930, 2015).

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 (JRC98372, 2015).

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

This report gives a view of possible standardisation concerning numerical simulations of the blast protection level of laminated glass windows and facades. The need to validate the numerical models against reliable experimental data, some of which are indicated, is underlined (JRC100438, 2016).

6. A Report on the recommended strategies to improve standards for testing the resistance of windows and glazed facades

This report summarises the activities of the Group in 2016, and reports the agreement for the actual modification of the standards EN 13123 and EN 13124, to be accomplished within the CEN TC 33 (JRC105812, 2016).

7. Suggestions for adaptations of existing European norms for testing the resistance of windows and glazed façades to explosive effects

This report formulates suggestions for improvements to existing testing standards for the evaluation of explosive resistance of security glazing products, using the structure and the format of the existing testing standards EN13123-1 and EN13124-1 as the basis (JRC107655, 2017).

2.4.3 Other Achievements

1. Consultation Meetings with CEN TC 33 WG1 (November 2016, March 2018)

The Group presented its recommendation at the CEN Technical Committee 33, Working Group 1 for a revision of the standards for testing of blast protecting windows (EN 13123 and EN 13124) and proposed many

changes in order to ameliorate them. The Working Group agreed to start a review process of both standards and to use the expert knowledge that the ERNCIP Thematic Group has prepared.

2. Journal publication "Design of blast-loaded glazing windows and facades: a review of essential requirements towards standardization" in ADVANCES IN CIVIL ENGINEERING

This paper outlines possible standardisation concerning numerical simulations of the blast protection level of laminated glass windows and facades (doi 10.1155/2016/2604232, http://www.hindawi.com/journals/ace/2016/2604232), 2016.

2.4.4 Current Objectives

This Thematic Group was commissioned in July 2017 by DG HOME (Innovation and Industry for Security) to conduct the pre-normalisation activities that will produce updates to the risk assessment for building design standards, by 2019. In addition, the group will further support the revision of EN 13123 and EN 13124.

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

2.5.1 Background

Vulnerability of critical indoor infrastructures to chemical and biological (CB) agents poses a significant concern. Earlier studies and experience from incidents have provided insight into relevant exposure scenarios. Initiation of appropriate countermeasures to be taken in response to CB attacks is highly dependent on rapid and reliable detection of the threat agent. The ideal detection capability is extremely fast, ultimately reliable, covers the entire agent spectrum and is easy to use. However, an overview of the current European detection capability is missing.

The Group is coordinated by the Aristotle University of Thessaloniki. It investigates issues that can be addressed at the EU level regarding detection, identification and monitoring of airborne chemical and biological agents in enclosed spaces.

2.5.2 Achievements – Reports

NB More information about this Group can be accessed via AIRBORNE TG. To access the reports, please contact the ERNCIP Office.

1. Definition of relevant scenarios of indoor airborne threats (CB) in critical infrastructure

The report identifies the types of infrastructures most vulnerable to indoor attacks using chemical or biological agents, and identifies the most pertinent CB agents. Generic (representative) scenarios of indoor airborne contamination are listed (JRC102091, 2016).

2. Technology Review for Detection of Airborne Chemical Agents in Critical Infrastructures

This report gives an evaluation of chemical detection technology for the specific purpose of protecting critical buildings against airborne chemical threats. The review is restricted to gas/vapour detectors, since the inhalation threat is considered to be the most important in chemical terrorism incidents (JRC106323, 2016).

3. Technology Review for Detection of Airborne Biological Agents in Critical Infrastructures

This report provides a technology update of biological detection technology for indoor use. At the moment, no single sensor or detection technology today fulfils the requirements of an ideal detection system (JRC106322, 2016).

4. Dispersion modelling of chemical or biological indoor airborne threats in critical infrastructures

Based on the scenarios identified in JRC102091, different facets of the indoor dispersion modelling are presented: the computations are performed (a) with a multi-compartment model or with computational fluid dynamics (CFD) models; (b) for three kinds of infrastructures (high-rise building; large room with its venting system; metro station with contiguous parts of tunnels); and (c) for short (near instantaneous) and long (continuous) unit mass releases of a (passive) tracer gas or micrometric aerosol particles (JRC106324, 2016).

5. Identification of gaps and requirements definition for next generation detectors in the EU

This report summarises the work done so far in order to identify gaps and the needs for further work. There is no sensor technology with detection and identification characteristics able to cover a large space at a reasonable cost. Moreover, the spatial variability of contamination within a building envelope remains high during the first minutes of an incident, resulting in undetected blind spots where contamination levels could be life threatening (JRC106321, 2016).

2.5.3 Current Objectives

The Group was commissioned in May 2017 by DG HOME (Terrorism and Radicalisation) to assist security managers in implementing a comprehensive plan for protection against such threats, through the application of a combination of available technologies. The Group is investigating sensor systems, including interoperability requirements of components, and the optimal combination of technologies for early and effective detection and identification.

The main output of the Group will be guidance (in the form of a report, plus a summary version in leaflet form) to security managers on the optimal setup of sensor systems against airborne threats. This will be the first step towards a more comprehensive security plan to protect critical infrastructure against such threats, covering prevention, as well as identification and response after a malicious event. The Group will also identify the needs for harmonising the protocol for evaluating sensor systems.

2.6 Thematic Group - European IACS Cyber-security Certification Framework (ICCF)

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, has recently completed an assessment of the feasibility of its previous proposals for IACS components cybersecurity certification, thereby supporting DG CNCT's "Roadmap toward the ICT security certification framework".

2.6.2 Achievements – Reports

NB The Group's published reports can be accessed via ICCF TG

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

In 2015, 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. 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?*" (JRC94533, 2014).

2. Introduction to the European IACS components Cyber-security Certification Framework (ICCF)

In 2017, the European IACS Cyber-security Certification Framework Thematic Group issued a feasibility study in view to propose an initial set of common European requirements and broad guidelines that will help fostering IACS cybersecurity certification in Europe. It describes the IACS component Cybersecurity Certification Framework (ICCF) and its elements and makes suggestions for its governance, adoption and implementation (JRC102550, 2016).

3. Feasibility of the IACS Cybersecurity Certification Framework (ICCF). - lessons from the 2017 study

This assessment of the feasibility of the ICCF was completed by challenging the ICCF through various exercises executed at national level. Five National Exercise Teams (ERNCIP NETs) were established in France, Germany, Netherlands, Poland and Spain and tasked with exercises aimed at simulating "the behaviouristic and governance model" of the ICCF. Each NET comprised representatives from national cybersecurity agencies, national certification bodies, national accreditation bodies, evaluation labs, IACS manufacturers, and infrastructure operators (report available in June 2018).

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

2.6.4 Current Objectives

This Group has recently completed its last commission from DG CNECT. Negotiations are currently underway on the potential follow-up work which could be undertaken by an ERNCIP Thematic Group in 2018 and 2019:

1. To produce a usable scheme for IACS in the framework of the Proposal;
2. To give practical support to the ICCF by involving further stakeholders;
3. To perform a full-scale pilot of the ICCF;
4. To implement the ICCF requirements under an observable protocol;
5. To close identified gaps between current practices and ICCF guidelines;
6. To launch an ICCF standardisation new work item with CEN/Cenelec on “common methodologies for evaluation”;
7. To establish a joint virtual lab at the JRC in order to perform the pilot and follow the future maintenance of the IACS scheme;
8. To create an exportable ICCF scheme to be used in other sectors.

2.7 Thematic Group – Early Warning Zones for Critical Infrastructure Protection: use of biometric and video technologies

2.7.1 Background

Recent security incidents involving 'soft targets', including those that have caused casualties and damage in (semi-)public spaces such as infrastructure access control points, have highlighted a need to identify known hostile persons at some distance from potential targets. Traditional security doctrine dictates that an additional perimeter with access control at a sufficient range is considered. However, this is not always feasible, and may just result in the creation of an additional potential (soft) target: namely the queues of people congregating at that additional access control.

Early Warning Zones for Critical Infrastructure Protection: use of biometric and video technologies (EWZ) is investigating an alternative approach. Successful early detection of such threats through the detection and recognition[1] of persons, objects or behaviours of interest in the vicinity could provide alerts, and allow for a quicker deployment of measures to counter or reduce the impact of these threats. There will need to be a balance struck between the effective warning distance (and therefore warning time) achievable and the cost, usability, and complexity of solutions. Managing potential false alarms that such systems will generate will also need to be assessed.

2.7.2 Current Objectives

This new Group was commissioned in May 2017 by DG HOME (Terrorism and Radicalisation) to produce a report on "factors to consider" that will outline the issues involved and provide good practice guidance on measures needed to move from isolated short-range systems used for biometric recognition to complete solutions that integrate the biometric elements with other information sources within a cognitive framework.

As part of this work, the Group will provide a clear description of EWZ by describing the concept of operations through selected use cases for extended virtual boundaries. The use cases being considered will cover an underground station in a metropolitan area, and a secure site that includes nuclear facilities. These use cases will provide the context for the evaluation by the Group of the current capability of relevant biometric modes, identifying their strengths and weaknesses. Capability gaps will be assessed against technology trends to determine whether they can be addressed in the short term for individual use cases. Specific elements of this developing capability include:

- Resolution and sensitivities of devices and the algorithms used to process data;
- Capability of biometric algorithms to find and identify persons of interest in wide-scale CCTV coverage;
- Other techniques that could be used to obtain data at a distance, both long and short ones.

This state of the art of the biometric technologies will include the commercial availability of solutions that could be directly applicable or adaptable for EWZ.

Video analytic and biometric technologies cannot provide the complete answer to the range of EWZ use cases that will be outlined. The inclusion of artificial intelligence (AI)/cognitive elements, as well as robotics and autonomous systems, into the overall system solution will enhance the capability to generate alerts (e.g. early warning) and indicators in the EWZ use cases. AI-oriented and systems-oriented areas of cognitive video surveillance and biometrics cover many factors: learning and adaptation; sensory understanding and interaction; reasoning; autonomy and extracting knowledge and predictions from diverse multisensory data

[1] The term recognition is used to denote the process of recognising that someone in included in a pre-determined set of people, e.g. from a watch list. Identification is a special case of recognition where the set includes all people and refers to the process of determining someone's identity, which is not the case in recognition. Depending on the use case, the privacy implications are different. For EWZ, recognition is often sufficient.

(e.g. activity recognition, behaviour analysis of people/vehicles under surveillance). Robotic and autonomous systems include sensing and operation in unpredictable environments, fusing multisensory data with paradigms ranging from machine-learning driven sensing to deployment of (semi-)autonomous platforms (ground and aerial).

This analysis of the relevant AI methods, cognitive, robotics and autonomous systems will also provide a state of the art assessment, identifying the gaps relevant to the identified use cases.

The use of new technologies for public surveillance can create tension between the rights to privacy and the need for security. The Group will assess the relevant European legislation and European law cases (European Court of Justice and European Court of Human Rights) that have enunciated legal principles in scenarios where the right to privacy has required careful balance with social security and public safety. The identified privacy implications will be applied to the emerging scenarios being developed by the Group, identifying relevant data protection impact assessment (DPIA) methodologies and standards.

A specific prototype of an EWZ-DPIA methodology will be considered as a tool for correctly documenting and reviewing decisions for the way regulatory requirements and risks are managed in the specific use case.

The conclusions of all these strands of work will be incorporated into a 'Good Practices' and 'Things to consider' guide, aimed at infrastructure operators. Areas where there is a need for further standardisation to support the realisation of the benefits of EWZ will also be identified.

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 called 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 thematic 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. 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 Highlight - A single EU certification procedure for aviation security screening equipment

The work undertaken by this Aviation Security Thematic Group in 2012 and 2013 has contributed to the recent introduction of an EU certification procedure for aviation security screening equipment.

The Regulation on an EU certification scheme for aviation security equipment was adopted by the Commission in September 2016. The creation of an EU system of mutual recognition for security equipment will help overcome market fragmentation, strengthen the competitiveness of the EU security industry, and contribute to improving aviation security across Europe. The introduction of an EU certificate will allow security equipment approved in one Member State to be marketed in others.

3.1.3 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) indicate presence of explosives by detecting trace amounts of explosives, either in the form of particulate material or as a vapour. The study is 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 (JRC85509 – 2013).

2. Detection Requirements and Testing Methodologies for Aviation Security Screening

The study assessed the performance requirements and testing methodologies for screening equipment at airports in the EU and EFTA Member States, including the procurement of 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 (JRC81650 – 2013).

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

3.2.1 Background

Since the 2006 transatlantic aircraft plot, disrupted by the UK security agencies, 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, France, 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.

The findings from this Group's work led to the formation of the subsequent ERNCIP thematic group, Detection of Explosives and Weapons in Secure Locations (DEWSL).

3.2.2 Achievements - Reports

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

1. Statement of User Needs – non-aviation explosives detection

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. For further details, please contact the ERNCIP Office

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 (JRC84076, 2013).

3.3 Thematic Group - Video Surveillance for Security of Critical Infrastructure

3.3.1 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 invested in 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 purpose.

3.3.2 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 introduces surveillance, providing an understanding of surveillance systems and video analytics, with examples of how a morphological analysis of the surveillance domain can describe key aspects of surveillance and video analytics (JRC100399, 2015).

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 (JRC100401, 2015).

3. Video analytics adoption: Key considerations for the end-user

This report outlines the basics of video analytic technology, how it is used and its advantages. It draws end-user attention to the key factors to be taken into account when considering its adoption. It is aimed at managers, security personnel, law-enforcement officers and other end-users whose knowledge of video analytics may be limited. This report should help the end-user engage with the providers of video analytics technology (JRC102121, 2016).

4. Access to data sets

This report presents a critical analysis of video analytic data sets and describes the importance of video analytics, the growth of the related market, and the aspects that make video analytics so complex, demonstrating the importance of having common and widespread data sets (JRC103341, 2016).

5. Video surveillance standardisation activities, process and roadmap

This document provides an overview of standards in video surveillance and a roadmap for future standards development. A case study on post-event investigative video analysis illustrates the requirements for such standards, especially on interoperability aspects. The report makes recommendations for video surveillance standards, including new work items to develop:

- one or more EU standards for surveillance of critical infrastructure, and
- a harmonised certification procedure for video surveillance systems and components for protection of critical infrastructure at EU level (JRC103650, 2016).

6. Surveillance and video analytics: work accomplished from 2012 to 2016

This report summarises all the work undertaken by the group (JRC103279, 2016)

3.4 Thematic Group - Applied Biometrics for Security of Critical Infrastructure

3.4.1 Background

Biometric technologies allow for the automated identification of individuals based on their biological and behavioural characteristics and provide the promise of the unique identification or classification of individuals interacting with critical infrastructures.

This Group, coordinated by IBM UK, 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.

3.4.2 Achievements - Reports

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

1. Experiences from Large Scale Testing of Systems using Biometrics

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). 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 (JRC95455, 2015).

2. Application of Biometrics: Guidance for Security Managers

The report provides information about the application of biometric technologies to achieve secure recognition of individuals by organisations operating critical infrastructures e.g. guidance on implementing physical access control systems using biometric technologies. The report aims to help managers and security officers 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 (JRC95453, 2015).

3. Summary of the activities of the Biometrics Thematic Group: 2012 to 2015

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 (JRC95665, 2015).

4. Biometrics, surveillance and privacy

There are a number of issues associated with privacy and biometrics that need to be addressed for successful and responsible implementation of biometric technology. This report articulates these issues, explores their impact and identifies the activity needed to address them. This assessment is made in the context of the new international standard currently under development for video surveillance systems using biometrics, ISO 30137, 'Information technology — Use of biometrics in video surveillance systems' (JRC104392, 2016).

5. Summary of applied biometrics TG activities: October 2015 to August 2016

This report outlines the work of the thematic group between October 2015 and August 2016 (JRC103172, 2016).

3.4.3 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 moved through to the committee draft stage.

The final ballot on "prCEN/TS 17261 Biometric authentication for critical infrastructure access control – Requirements and evaluation" will run until July 2018, and it is expected that the standard will then be achieved later in 2018. It is anticipated that this technical specification will then be made available to ISO/IEC JTC1 SC37 as a base document to address a broader standard to support biometric product certification, i.e., covering not only this CEN work, but also the development of biometric product certification in FIDO.

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 most Internet browsers using the 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 more than 138 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 assessed the information in the Inventory on standards, best practices and guidelines used by the labs. Based on this, ERNCIP defined a directory of existing international standards for security as 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.

Since then, the activities on the ERNCIP Inventory continue to focus on the dissemination and promotion of the tool. Additional CIP-related standards have been added to the ERNCIP Standards Directory improving and enhancing the quality of the data. The access community has reached almost 350 registered organisations.

4.3 How laboratories can participate

European laboratories can participate in the ERNCIP Inventory by following the registration procedure directly on the web. From the URL for the ERNCIP Inventory 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. From the URL for the ERNCIP Inventory complete the "Access for Searching" section.

5. Other ERNCIP Activities

5.1 ERNCIP Operator workshops

The purpose of the ERNCIP operator 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. Four operator-focussed workshops have been held; in September 2013, May 2014, April 2016, and May 2017. A fifth is planned for May 2018.

Details at operator workshops

5.2 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

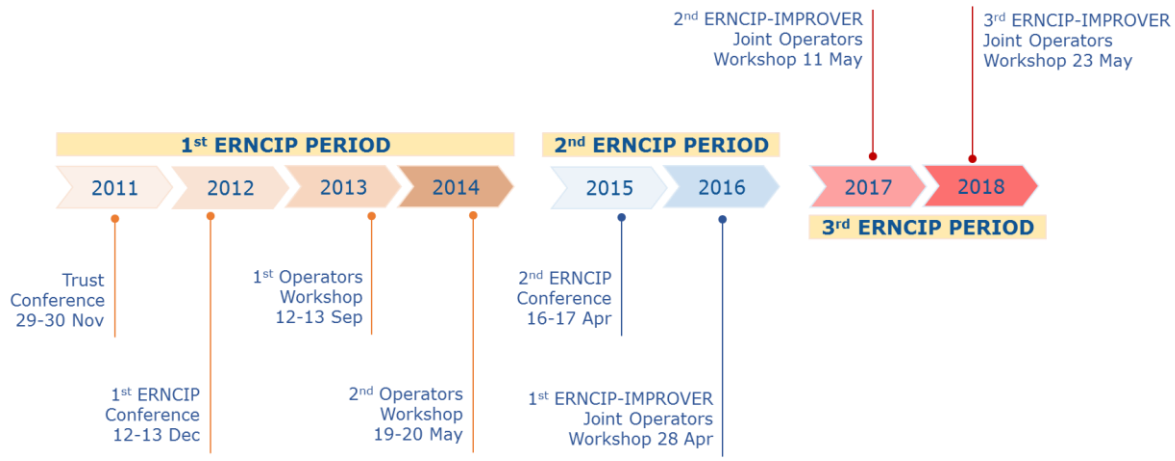

Figure 1: Timeline of ERNCIP organised events

5.3 CIPRNet

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

This was 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 completed in March 2017.

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

More details at www.ciprnet.eu

5.4 IMPROVER

ERNCIP is 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 September 2018.

The JRC and the IMPROVER partners, in collaboration with the CIPRNet project, have created a lexicon of definitions (March 2017). On November 2017, they have released a Framework for implementation of resilience concepts to Critical Infrastructure.

More details at http://improverproject.eu/

Abbreviations and definitions

AI	Artificial Intelligence
AIRBORNE TG	ERNCIP Thematic Group - Detection of Indoor Airborne Chemical & Biological Agents
CCTV	Closed-circuit TV
CEN	European Committee for Standardisation
CENELEC	Standardisation association comprised of members who are the National Electro-technical Committees of European Countries.
CFD	Computational Fluid Dynamics
CIP	Critical infrastructure protection
CIPRNet	Critical Infrastructures Preparedness and Resilience Research Network
CTM	Common testing methodologies
DEWSL TG	ERNCIP Thematic Group - Detection of Explosives and Weapons in Secure Locations
DG	Directorate General (functional department of the EC, 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
DPIA	Data protection impact assessment
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
EWZ	Early Warning Zone
FIDO	Global Ecosystem for Standards-Based, Interoperable Authentication
GICNT	Global Initiative to Combat Nuclear Terrorism
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
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
WATER TG	ERNCIP Thematic Group - Chemical and Biological Risks to Drinking Water

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*)**:**

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

More information on the European Union is available on the internet (http://europa.eu).

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
  via EU Bookshop (http://bookshop.europa.eu);
- more than one copy or posters/maps:
  from the European Union's representations (http://ec.europa.eu/represent_en.htm);
  from the delegations in non-EU countries (http://eeas.europa.eu/delegations/index_en.htm);
  by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm) or
  calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

  (*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (http://bookshop.europa.eu).

KJ-NA-29236-EN-N

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2760/245080

ISBN 978-92-79-85967-0