JRC TECHNICAL REPORTS

European Reference Network for Critical Infrastructure Protection:

ERNCIP Handbook 2017 edition

Gattinesi, P
Larcher, M
Lazari, A
Ruzzante, GL
Theocharidou, M

Version 1.0 – 7 June 2017

EUR 28659 EN

Contact information
Name: Peter GATTINESI
Address: Via Enrico Fermi, 2749, Ispra (VA), Italy I-21027
Email: peter.gattinesi@ec.europa.eu
Tel.: +39 0332 785949

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

JRC107049

EUR 28659 EN

PDF ISBN 978-92-79-69734-0 ISSN 1831-9424 doi:10.2760/186173

Luxembourg: Publications Office of the European Union, 2017

How to cite this report: Author(s), Gattinesi Peter, Larcher Martin et al, European Reference Network for Critical

Infrastructure Protection: ERNCIP Handbook 2017 edition Version 1.0*Title*, EUR 28659, doi:10.2760/186173

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 2016.

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 State.

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, 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 2016.

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 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, 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, 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) of the European Commission, so that participation by experts at planned meetings can be funded through 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.

1.3 Summary of active thematic groups

ERNCIP has three sponsoring Commission Directorates:

- DG HOME B4 (Innovation and Industry for Security), sponsoring four thematic groups:
  - Detection of weapons and explosives in secure locations (DEWSL)

    producing European-level guidelines for vehicle screening at entry checkpoints, through a CEN workshop agreement process, and considering the feasibility and benefits of producing European-level guidelines for detecting explosives and weapons at open locations, i.e. without a controlled perimeter (see 2.1).

  - Chemical & biological risks to drinking water

    producing guidance on production of Water Security Plans (see 2.2).

  - Radiological & Nuclear threats to critical infrastructure

    identifying how best to utilise the new list-mode data acquisition standard and emerging detection technologies to improve nuclear security, and defining the characteristics of a centralised system to support assessment and adjudication of radiation alarms (see 2.3).

  - Protection of Buildings (see 2.4)

    updating the risk assessment process for building design standards for explosive threats (see 2.4).

  All these thematic groups will run for 24 months from June 2017 to May 2019.

- DG HOME D2 (Terrorism and Radicalisation), sponsoring two thematic groups:
  - Detection of Indoor Airborne Chemical & Biological Agents

    providing security managers with assistance in planning risk mitigation against these threats by use of available technologies (see 2.5).

  - Extended Virtual Fencing – use of biometric and video surveillance technologies

    producing a "State of the Art" report on the feasibility of integrating biometric technology with other information to provide extended virtual boundaries, including the societal impact of wider use of biometric/video data (see 2.7).

  Both these thematic groups will run for 24 months from May 2017 to April 2019.

- DG CNECT, sponsoring the thematic group on the European IACS Cybersecurity Certification Framework (ICCF)

  enhancing the proposed framework by exercises to simulate the behaviouristic and governance model. This thematic group will run for 12 months from March 2017 to February 2018 (see 2.6).

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 downloaded at DEWSL TG

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

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 report addresses the need of facility operators and security managers who need to mitigate the threat of explosives and weapons attacks at facilities with a secure perimeter at which screening for explosives and weapons threats can take place. These include 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 identified by the experts 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 the 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 transportations 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 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

The Group has now been commissioned by DG HOME (Innovation and Industry for Security) to undertake the activities necessary to create the relevant standardisation mechanism, probably a CEN workshop agreement (CWA), for production of European-level guidelines for security managers regarding the screening of vehicles at entry checkpoints, for weapons and explosives.

The Group will also consider the feasibility and benefits of producing European-level guidelines for protecting crowded places/mass transportation locations (i.e. open locations without controlled perimeters against the threats from explosives and weapons attack.

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 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 for 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 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 (JRC89741, 2014).

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 against 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 (JRC85442, 2014).

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 (JRC88228, 2014).

4. Methods for the rapid identification of pathogens in water

Microbiological water contaminants represent an acute health risk. There is 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.

This 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 (JRC92395, 2015).

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 (JRC100531, 2016).

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, although little information is available for biological monitoring, with few microorganisms 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) (JRC100533, 2016).

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

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. This document summarises the key findings from reviews of the current situation regarding water security planning with the European Union.

The Water Safety and Security Workshop organised in Brussels on the occasion of the 10th anniversary of the Groundwater Directive provided the opportunity to present the recommendations for validation (JRC105388, 2016).

2.2.4 Other Achievements

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

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.

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 State

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 States on the requirement 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 gave the opportunity to present proposals for the basis of a Water Security Plan. The plan 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 has now been commissioned by DG HOME (Innovation and Industry for Security) to produce a European-level guidance document that will support water utility operators to produce a water security plan, devoted to improving the 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 different aspects associated with 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 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.

- Novel detection technologies for nuclear security:

  Systems emerging from innovations on new materials and signal processing capabilities.

2.3.2 Highlight – New work item for a new 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.

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 March 2019.

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 Achievements - Reports

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

General Reports

1. A summary of the activities of the RN Thematic Group of ERNCIP in 2016 is reported. The Group organized its work in three sub-topics: raising awareness on a new standard on list-mode data acquisition, robotics in RN field and reachback (expert support to field teams) (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

Recent developments of digital data acquisition systems allow real-time pre-processing of

detector signals at a high count rate. 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. (JRC93260, 2015).

4. 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' (JRC100408, 2016).

Reachback reports

5. Remote Expert Support of Field Teams

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 (JRC94535, 2015).

6. Information sharing in a nuclear security event

In response to a simple questionnaire devised by the Group, sent to relevant authorities in the Member States, the 10 answers received came from very diverse organisations working in the domains of security, safety or the military. 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 (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 Finnish case is a holistic approach to Nuclear Security Detection Architecture, as defined by the International Atomic Energy Agency. 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.

The case studies of Finland and France show that efficient European reachback is manageable and technically possible on a country-wide basis (JRC98711, 2016).

Unmanned detection systems reports

8. 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 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).

9. 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 from incidents involving radioactive material. 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).

10. 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. For additional sensors, most responders suggested inclusion of position and time for radiation measurements (JRC100475, 2016).

11. 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. Search and rescue robotics is the closest domain to the radiation measurement scenarios. The report defines search and rescue robots and outlines their major subsystems, followed by a review of deployment scenarios for search and rescue robots 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).

2.3.4 Current Objectives

The Group has now been commissioned 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 Explosive Effects (Protection of Buildings)

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 future introduction of regulations or guidelines should support the resilience of the buildings and infrastructure against explosive 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 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 (JRC87202, 2014).

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 (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 basic 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

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 (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).

2.4.3 Other Achievements

1. Consultation Meeting with CEN TC 33 WG1 (28 November 2016)

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 WG agreed to start a review process of both standards and to use the expert knowledge that the ERNCIP group has prepared. The group was requested to submit a detailed change request to the WG.

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

The determination of the blast protection level of laminated glass windows and façades 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. This paper outlines 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 emphasised. (doi 10.1155/2016/2604232, http://www.hindawi.com/journals/ace/2016/2604232), 2016.

2.4.4 Current Objectives

This Group has now been commissioned 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 point of concern. Earlier studies and actual experience from incidents have provided some insight into relevant exposure scenarios. Initiation of appropriate countermeasures to be taken as 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 first started in September 2015 and is coordinated by the Aristotle University of Thessaloniki. It investigates issues that can be addressed in the EU level regarding Detection, Identification and Monitoring of airborne chemical and biological agents in enclosed spaces. During its initial year of work, this Group has identified the major issues to be addressed in the EU level, based on reviews of chemical and biological sensors, and of numerical simulation.

2.5.2 Achievements – Reports

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

1. Definition of relevant scenarios of indoor airborne threats (chemical and biological) in critical infrastructure

The report identifies the types of infrastructures most vulnerable to indoor-type attacks with chemical or biological agents. It reviews previous experiences (both in terms of case studies and in terms of past research projects) and identifies the most pertinent CB agents. Generic (representative) scenarios of indoor airborne contamination are listed. The report concludes that much can be gained by re-analysis of prior experiences and fictitious scenarios involving CB agent attacks (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. It overviews the technologies currently available and evaluates their characteristics. The review is restricted to gas/vapour detectors, since the inhalation threat is considered to be the most important in chemical terrorism incidents. The review is organised around eleven technology monographs, covering the basic principles of the detection technology, followed by a description of the specific characteristics of commercially available detection equipment employing that technology (JRC106323, 2016).

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

The increased threat of bioterrorism attacks has stimulated a continuously growing demand for rapid and accurate detection of biological warfare agents. This report presents scenarios of realising biological agents in indoor infrastructures. The bio-detection system capacity depends on the characteristics of the release and dispersion of the building envelop. This report provides a technology update of biological detection technology for indoor use. It focuses on technologies employed in devices and systems that are close to market or already on the market. At the moment, no single sensor or detection technology today fulfils the requirements of an ideal detection system. Moreover, there are not any existing standardization methods for the evaluation of sensing methods. Ideally, the next-generation automated analysers will include both handheld and high-throughput devices working in Real-Time. Integration of bioinformatics and metagenomics tools for determining various gene segments will result in decreased time for testing and identification with low cost, increased accuracy and early detection of airborne biological threats (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 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 uses the conclusions obtained from the three pillars of work done so far (reviews of chemical and biological sensors, as well as numerical simulations) in order to identify gaps and needs for further work. The report identifies that, at the moment, there is no sensor technology with detection and identification characteristics, able to cover a large space with a reasonable cost. Moreover, the spatial variability of contamination within a building envelop remains high during the first minutes of the evolution of the event, resulting in blind spots where contamination levels are below the detection limits, hence life threatening. Identification of the threat is of particular importance for both chemical (especially for lipophilic and non-rapidly metabolised compounds) and biological compounds, clearly affecting the post-event treatment and the minimization of fatalities. These conclusions highlight the need for additional work to be done, in order to tackle more efficient, the problem of detection and identification (JRC106321, 2016).

2.5.3 Current Objectives

The Group has now been commissioned 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. As part of this the Group will investigate sensor systems, including interoperability requirements of components, and the optimal combination of technologies for early and effective detection and identification. In the first year, the group will expand its research to issues such as the use of omics techniques for the post-event identification/verification of threats.

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, is now underway to support DG CNCT's "Roadmap toward the ICT security certification framework". The TG, following the initial proposal issued in 2015, has released, in February 2017, a feasibility study on a sectorial response dedicated to Industrial Automation Control System's components cybersecurity certification.

2.6.2 Achievements - Reports

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 produced 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).

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 been commissioned by DG CNECT to operate from March 2017 to February 2018, on the following objectives:

- "challenge" the current stage of development of the ICCF;
- organise exercises that will simulate "the behaviouristic and governance model" of the Framework, in cooperation with national stakeholders operating in "National Exercise Groups";
- the conclusion of the following activities will contribute to further enhance the ICCF's feasibility study as potential "sectorial response" to the "Roadmap toward a European ICT security certification framework for product and services".

2.7 Thematic Group – Extended Virtual Fencing – use of biometric and video surveillance technologies

2.7.1 Background

Recent security incidents directed at 'soft targets', and attacks that have caused damage at infrastructure access control points, have highlighted the need to identify threats at a distance. Earlier identification of such threats could provide quicker alerts and allow for the deployment of measures to counter or reduce the impact of these threats. Biometric technologies provide the promise of such identification through a number of methods.

Standard CCTV systems can now provide imagery that can be analysed and used for direct biometric analysis via face or gait recognition, or indirect recognition through behavioural biometric approaches. These can provide identification at a relatively long range from the sensor, potentially enabling more efficient access control processes.

2.7.2 Current Objectives

This new group will produce a "state of the art" report at the end of the first year to outline the work needed to move from isolated point systems for biometric recognition to complete solutions that integrate the biometric elements with other information sources within a cognitive framework to provide extended virtual boundaries.

This group will also research the societal impact of these technologies, such as privacy issues associated with the use and storage of biometric/video data. It is likely that there will need to be a balance struck between the privacy needed by citizens, and changing threat levels.

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 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. 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 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) 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 (JRC85509 – 2013).

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 (JRC81650 – 2013).

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.

The findings from this Group's work led to the formation of a 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.

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 (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 the topic of surveillance, describing what is required to create an understanding of surveillance systems and video analytics. The approach taken uses a morphological analysis of the surveillance domain. The report describes 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 (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.

The specific use cases are based on the needs of infrastructure operators and respective law enforcement agencies tasked with this protection throughout the EU (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. A detailed description and analysis of critical issues of the data sets are provided, along with commentary on existing data sets (JRC103341, 2016).

5. Video surveillance standardisation activities, process and roadmap

This document provides an overview of standards in video surveillance, including the need for standards, an overview of existing relevant standardisation efforts including gaps, 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 history of relevant initiatives is provided, including details on specific programmes, projects, and methodology, and on prior work on certification of video surveillance systems. The gap analysis of standards in video surveillance includes lack of standards at different levels of interoperability, lack of a universally agreed set of performance evaluation benchmarking metrics for video analytics, and the lack of European level certification for surveillance systems or its components. Finally, the report makes a number of 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 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 (JRC95455, 2015).

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 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. 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 (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'.

This report describes why biometrics confronts us with profound challenges regarding the protection of citizens' data and associated privacy concerns due to the collection and sharing of such data by private entities (such as search engines, credit registrars, data brokers, web shops, website trackers and optimisers, social media, chambers of commerce, health care institutions) and public entities (such as tax authorities, public administrations, driver licence authorities, social care agencies, and police and justice authorities) (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 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.

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.

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 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 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.

During 2016, the activities on the ERNCIP Inventory continued 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.

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 with ERNCIP. Ideally, there would be a representative from each of the 28 Member States. Up to 2016, 19 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. For instance, this Handbook is the direct consequence of a request emanating from this group.

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. Three operator-focussed workshops have been held; in September 2013, May 2014, and April 2016.

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

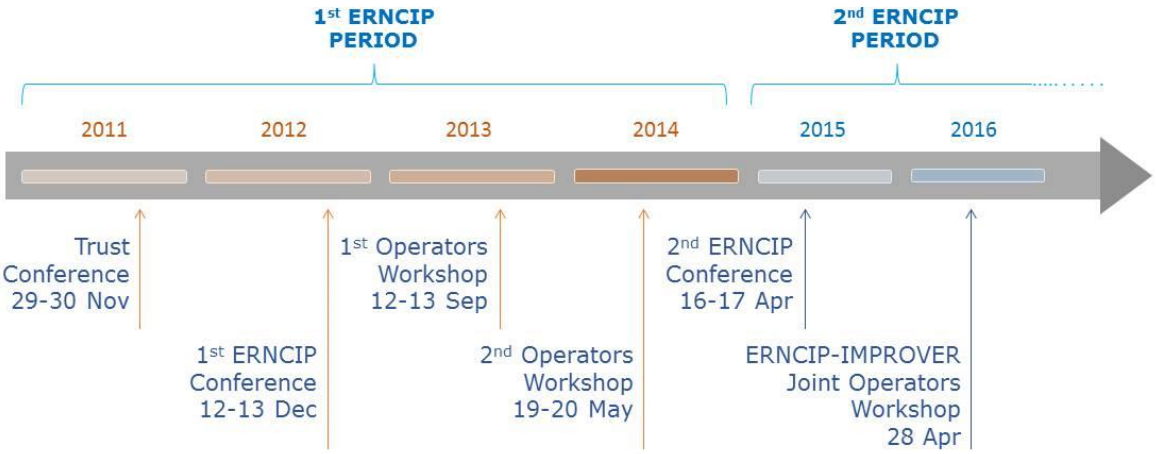

Figure 1: Timeline of ERNCIP organised events

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.
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 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
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 EC (DG Environment, JRC and Eurostat) and the European Environment Agency, providing information on European water issues.

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-28659-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:10.2760/186173

ISBN 978-92-79-69734-0