European
Commission

The European Reference Network for Critical Infrastructure Protection

Project First phase (2011-2014):

from concept to implementation

Joint Research Centre

Luxembourg: Publications Office of the European Union, 2016

Print	ISBN 978-92-79-44402-9	doi:10.2788/51273	LB-06-14-182-EN-C
PDF	ISBN 978-92-79-44401-2	doi:10.2788/569811	LB-06-14-182-EN-N

EUROPEAN COMMISSION

The European Reference Network for Critical Infrastructure Protection

Project First phase (2011-2014):

from concept to implementation

Contents

Table of figures

Table of tables

Contributing authors

William Billotte, JRC/NIST exchange programme
Sandro Bologna, researcher
Carl-Johan Forsberg, JRC
Peter Gattinesi, JRC
Georgios Giannopolous, JRC
Maria Giuliani, JRC
Philipp Hohenblum, Environment Agency Austria
Daniele Kashani-Rad, Engineering
John Keightley, NPL
Naouma Kourti, JRC
Martin Larcher, JRC
Alessandro Lazari, JRC
Göran Lövestam, JRC
Martin O’Farrell, NPIA
Kari Peräjärvi, STUK
Georg Peter, JRC
Aikaterini Poustourli, JRC
Christer Pursiainen, JRC
Gian Luigi Ruzzante, JRC
Alexander Stolz, Fraunhofer Institute
Marianthi Theocharidou, JRC
Paul Théron, Thales
David Ward, JRC

1. Introduction

1.1. Background

The Joint Research Centre (JRC) is the European Commission's in-house science service, providing policy areas with independent, evidence-based scientific and technical support throughout the whole policy cycle. Within the JRC, the Institute for the protection and security of the citizen (IPSC) provides scientific and technology advice on safety, security and stability within and outside the EU, collaborating with European and international expert communities.

In support of EU efforts to protect critical infrastructures (CIs), the JRC coordinates the ERNCIP, which was first established by the IPSC in 2009. This took place under the mandate of Directorate-General (DG) Migration and Home Affairs, in the context of the European programme for critical infrastructure protection (EPCIP) (COM, 2006) and with the agreement of Member States.

ERNCIP's mission is to 'foster the emergence of innovative, qualified, efficient and competitive security solutions, through networking of European experimental capabilities'. In order to achieve this, The ERNCIP maintains an online inventory of critical infrastructure protection (CIP)-related experimental capabilities in Europe, and in thematic networks of experts that identify and promote good practices as the basis for common European testing standards, aiming at the harmonisation of test methodologies and test protocols, where practical.

1.2. Purpose and structure of this book

As the ERNCIP project has concluded its first phase, this book documents and consolidates the work performed by the network, particularly the work of its thematic groups (TGs) between 2011 and 2014. It is co-authored by some of the TG coordinators and the ERNCIP office.

Moreover, this book outlines important lessons learned, and outlines the objectives for the next phase of the ERNCIP (2015 onwards). Finally, the book serves as a single point of reference for the activities of the first phase of the ERNCIP, thereby contributing to the communication and promotion of the ERNCIP to the CIP community.

The ERNCIP book is organised into five sections. Initially, the ERNCIP project, its context and its history are summarised, followed by a description of the current structure and implementation status of the network. Subsequent sections focus on the ERNCIP inventory and platform (Section 3), and the ERNCIP TGs (Section 4). The text illustrates the hands-on approach of each TG, starting with a specific area of concern, creating a work programme to address the problem using subject-matter experts. The book concludes with the lessons learned and a brief outlook on the future for the ERNCIP network.

1.3. Acknowledgements

The ERNCIP Office would like to express its gratitude to all the contributors to this book and particularly to the members of the TGs, whose contributions have made this book possible, and to the many other ERNCIP stakeholders who have played an active role in making the ERNCIP a success.

The authors also wish to acknowledge the many colleagues in the JRC whose support continues to provide the ERNCIP with a valued and valuable contribution.

1.4. References

(COM, 2006) Communication from the Commission on a European programme for critical infrastructure protection, COM(2006) 786 final, Brussels, 12.12.2006. Available online: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN

2. ERNCIP overview

2.1. The context for the ERNCIP

The ERNCIP was established under the mandate of DG Migration and Home Affairs, in the context of the EPCIP, and with the agreement of Member States.

The ERNCIP was established with the goal of improving the protection of CIs in the EU. The ERNCIP therefore works in close cooperation with all types of CIP stakeholders, focusing particularly on the technical protective security solutions. The ERNCIP has created and maintains an online information repository of EU CIP-related experimental capabilities, and has established a large network of experts to improve availability of security solutions through common European testing standards, and harmonisation of test methodologies and test protocols.

This is important for two reasons. First, harmonised test methodologies and protocols throughout Europe will ensure that the security solutions will be properly tested across the EU, according to agreed-upon standards, leading to better and more reliable protection of CIs. Secondly, harmonised test protocols are a prerequisite for a mutual acceptance scheme for security solutions, thus enhancing the development of the European security industry and security market and related standardisation efforts.

Encouraged by the EU security industrial policy (EC, 2012), which highlights the problem to the EU of a fragmented security industry market and its lack of harmonised certification procedures and standards, activity is under way towards more harmonised European regulatory frameworks and standards in the field of security. In particular, this is taking place within the European Committee for Standardisation (CEN)/European Committee for Electrotechnical Standardisation (Cenelec) framework under Mandate M/487 on security standards (M/487, 2011), where 'security' refers to the protection against threats by terrorism, serious and organised cross-border crime, natural disasters, pandemics and major technical accidents. The ERNCIP and its TGs have been, and continue to be, facilitators and participants in activities tied to these priorities, especially those dealing with chemical, biological, radiological, nuclear and explosive threats (CBRN-E) threats, and the application of biometrics for CIP.

In 2013, an ERNCIP report (Gattinesi and Pursiainen, 2013) provided a broad picture of European CIP-related test capabilities [1]. It identified that testing of security solutions can serve two main purposes: (a) verifying that procurement

[1] The relevant analysis was primarily based on an online, questionnaire-based survey circulated at the end of 2012, which was completed by 65 respondents representing different types of ERNCIP stakeholders. The ERNCIP TGs also provided information about their respective capabilities and perceived gaps in their respective sectors.

specifications are met by the security solution, and (b) managing the risk associated with the need for the security solution. Furthermore, there are many forms of testing associated with security solutions, such as prototype tests; design approval; factory test of products; acceptance tests; operational/site tests; certification, and evaluation of the testing process itself.

This work also concluded that while, in some sectors, the EU has impressive CIP-related testing capabilities, there still appears to be a lack of certain capabilities. There is no detailed picture available of existing test capabilities, and even less of specific gaps, with no single actor having a holistic, cross-sector view of the EU experimental and test capabilities for CIP-related security solutions. Even within specific infrastructure sectors, the available data is fragmented and superficial; the laboratories are usually only aware of their own capabilities. If capabilities cannot be listed, gaps cannot be identified. It was also revealed that while many ERNCIP stakeholders use non-EU experimental facilities and test laboratories in order to receive certification for access to that non-EU country's markets, some do this because they cannot find the required test capabilities in the EU.

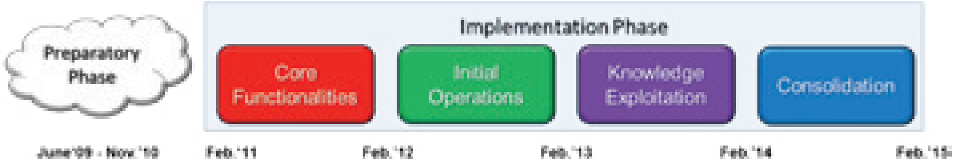
Some users of EU-based test laboratories are concerned with the near monopoly position some conformity assessment and certification bodies often have in their Member State. Those users would like increased competition for the provision of certification services, on the assumption that a harmonised and mutually-recognised certification system in the EU would reduce the cost and raise the quality and professionalism of services provided. Ideally, it should be sufficient for a security product to be tested in one accredited European test laboratory in order to have access to the whole EU market. It would also indirectly enhance the competitiveness of the European security industry in its export efforts, were the European standards (EN) and certification schemes to become more generally recognised.

2.2. Establishment of ERNCIP

The JRC was commissioned to launch the ERNCIP in 2009. The preparatory phase was successfully completed in November 2010 and the project started its implementation phase in February 2011. During the preparatory phase, design options for the ERNCIP network were defined and an extensive consultation process with Member State government authorities, infrastructure operators and security experts was conducted, enabling the JRC to set out a roadmap for the project's first 4 years.

Implementation was divided into four 1-year sub-phases as illustrated in Figure 1:

Figure 1: ERNCIP project timeline



Core functionalities (1 March 2011 to 29 February 2012): The first year of implementation was devoted to the establishment of the mechanisms for the ERNCIP office, the TGs, the inventory and the expert group.

Initial operations (1 March 2012 to 29 February 2013): During the second year, eight TGs were initiated, the ERNCIP inventory was implemented, and the first ERNCIP conference held (Ispra, December 2012).

Knowledge exploitation (1 March 2013 to 29 February 2014): During the third year, the TG work programmes were finalised and approved. Results started to be delivered and the inventory achieved a critical mass of members. Other milestones included the launch of the ERNCIP operators' workshop and the ERNCIP academic committee.

Consolidation (1 March 2014 to 29 February 2015): During the final year, the ERNCIP platform was launched, most TGs completed their work, in some cases planned for a second phase. The second operator workshop was held in Ispra in May 2014, and the second ERNCIP conference was prepared. From the outset, ERNCIP has been established around the following values:

- Being pragmatic and keep its focus on results: the main focus of ERNCIP is the efficient generation of (TG) deliverables.

- Being demand- and customer-driven: this entails not only ‘doing things right’ but also to ‘doing the right things’ by ensuring that all relevant stakeholders are involved in the project.
- Being built around the existing facilities: the ERNCIP uses only already-existing facilities.
- Having a light management structure: to avoid time-consuming decision-making processes.
- Keeping its ‘applied’ approach: even though areas for R & D can be proposed ERNCIP is not a research project.
- Continuing to be voluntary: with a high level of personal commitment and also with obvious benefits for those involved.
- Continuing to cultivate trust and confidence: a prerequisite in order to cooperate around security.

2.3. The ERNCIP at the end of Phase I

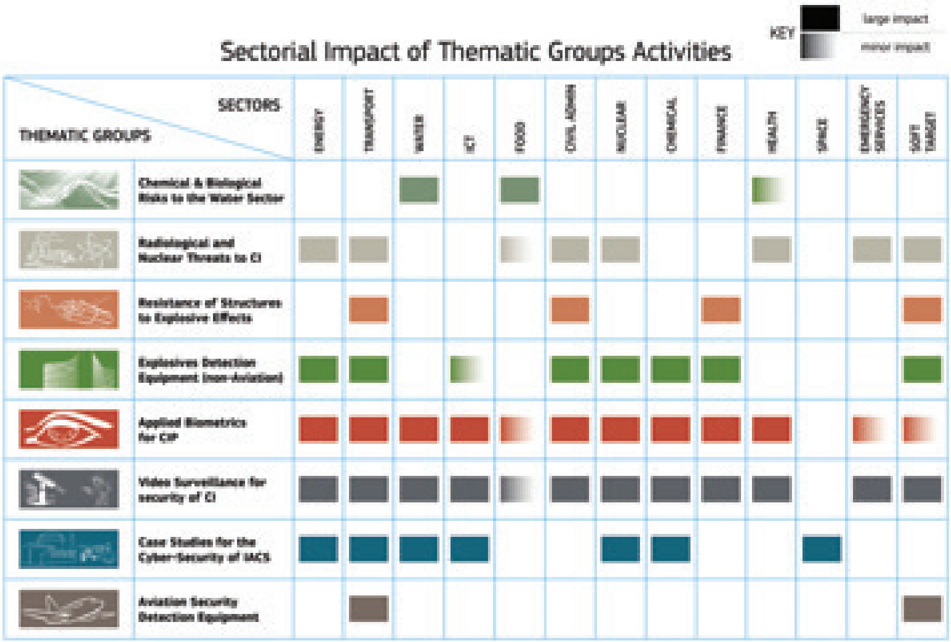
During the course of the ERNCIP, Member States and the European Commission identified priority CIP-testing areas of concern for ERNCIP to address at the EU level. Consequently, ERNCIP thematic areas (TAs) have been identified, covering a wide range of CIP subjects; some sector-specific, while most cut across many infrastructure sectors (see Figure 2).

For each TA, ERNCIP has formed one or more TGs comprising nominated experts, drawn from relevant experimental facilities and laboratories, manufacturers and vendors of security solutions, government authorities, academia, and operators of CIs. Each TG is led by a coordinator appointed by ERNCIP, in some cases assisted by one or several deputy coordinators, who manage the work of the group, through a work programme that is established and approved in the initial stage of the TG life cycle.

ERNCIP TGs are directed to identify and evaluate the existing testing capabilities and gaps, as relevant to their given scope. The TGs will then analyse the different options for meeting the capability gaps, including EU-led and/or EU-funded approaches, Member State-based approaches, market-based approaches, or viable combinations thereof. The overall aim of TGs is to produce recommendations for the relevant funding and implementation bodies, including the respective EU policy areas, so that specific policy conclusions can be articulated in the relevant EU policy.

So far, the ERNCIP has brought together over 200 subject matter experts to address the specific issues of the TGs from the perspective of testing security-related solutions, thereby capitalising on the existing knowledge provided by the experts from their work, or from other relevant research projects, for example projects under the seventh framework programme for research and technological development (FP7) or the research and innovation programme Horizon 2020.

Figure 2: Sectoral impact of thematic group activities



Sectorial Impact of Thematic Groups Activities

KEY ■ large impact ▨ minor impact

THEMATIC GROUPS \ SECTORS	ENERGY	TRANSPORT	WATER	ICT	FOOD	CIVIL ADMIN	NUCLEAR	CHEMICAL	FINANCE	HEALTH	SPACE	EMERGENCY SERVICES	SOFT TARGET
Chemical & Biological Risks to the Water Sector			■		■					▨			
Radiological and Nuclear Threats to CI	■	■			▨	■	■			■		■	■
Resistance of Structures to Explosive Effects		■				■			■				■
Explosives Detection Equipment (non-Aviation)	■	■		▨		■	■	■	■				■
Applied Biometrics for CIP	■	■	■	■	▨	■	■	■	■	■		▨	▨
Video Surveillance for security of CI	■	■	■	■	▨	■	■	■	■	■		■	■
Case Studies for the Cyber-Security of IACS	■	■	■	■			■	■			■		
Aviation Security Detection Equipment		■											■

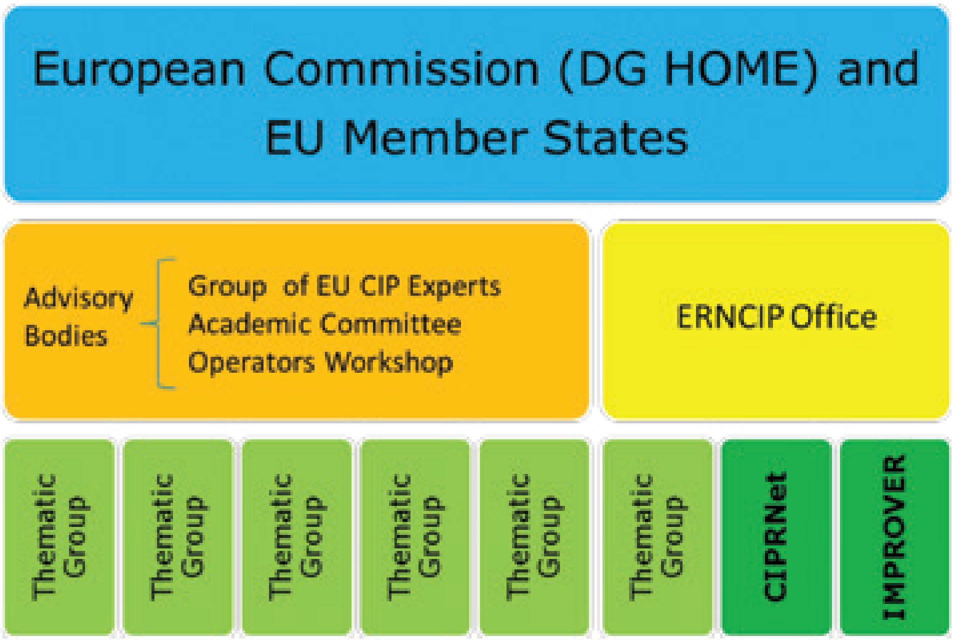
The ERNCIP was also tasked to develop a system to identify laboratories that operate in the specific context of testing CIP-related security solutions. The ERNCIP inventory was released online in June 2012, and by February 2015, had 115 registered testing facilities, allowing the community of users to search for general information about the services offered (experience, competencies and accreditations).

In 2014 a new portal, the ERNCIP platform, integrating previous work, and including access to the inventory of labs, offered new functionalities to improve synergies throughout Europe among European experimental facilities, manufacturers and CI operators.

The ERNCIP is managed by the ERNCIP office, a small team staffed by the IPSC's Security Technology Assessment unit (G5) in Ispra, Italy. The ERNCIP office oversees the activities of all of the ERNCIP TGs, supports the logistics of membership recruitment and meetings, and monitors the production of deliverables against TG work programmes. The ERNCIP also manages the ERNCIP academic committee, the ERNCIP group of EU CIP experts, and hosts events like the ERNCIP conferences and operators' workshops. The ERNCIP organisation is illustrated in Figure 3. In addition, ERNCIP is an active partner of major CIP-related research projects funded by the EU under FP7 and Horizon2020, namely CIPRNet (CIPRNet, 2015) and Improver ([2]) respectively.

The ERNCIP advisory bodies comprise representatives from Member State CIP authorities, academia, and infrastructure sectors, as illustrated in Table 1 below. Their activities are described in more detail in the following sections.

Figure 3: ERNCIP organisation



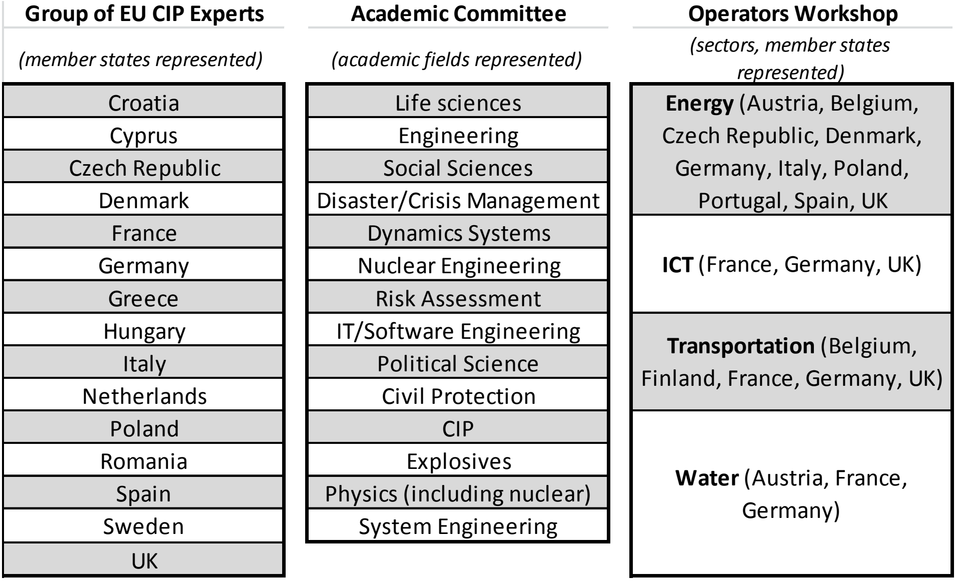
2.3.1. The ERNCIP group of EU CIP experts

The members of this group are appointed by Member States from government authorities relevant to national CIP, for their knowledge on existing European and national CIP policies and programmes. This group acts as an advisory body to the ERNCIP, with each member having the important role of linking the Member States' CIP communities and the ERNCIP, and normally meets bi-annually. The role of this group is to discuss, and offer strategic advice to the ERNCIP office and TGs on the following.

- Development and use of the ERNCIP inventory and platform.
- Creation, membership, and termination of ERNCIP TGs.

[2] http://improverproject.eu

Table 1: ERNCIP advisory bodies



Group of EU CIP Experts	Academic Committee	Operators Workshop
(member states represented)	*(academic fields represented)*	*(sectors, member states represented)*
Croatia	Life sciences	**Energy** (Austria, Belgium, Czech Republic, Denmark, Germany, Italy, Poland, Portugal, Spain, UK
Cyprus	Engineering	
Czech Republic	Social Sciences	
Denmark	Disaster/Crisis Management	
France	Dynamics Systems	**ICT** (France, Germany, UK)
Germany	Nuclear Engineering	
Greece	Risk Assessment	
Hungary	IT/Software Engineering	**Transportation** (Belgium, Finland, France, Germany, UK)
Italy	Political Science	
Netherlands	Civil Protection	
Poland	CIP	**Water** (Austria, France, Germany)
Romania	Explosives	
Spain	Physics (including nuclear)	
Sweden	System Engineering	
UK		

- Progress and outcomes of the TGs.
- Main documents produced by ERNCIP.
- ERNCIP governance issues.
- Creating and maintaining trust within ERNCIP.
- ERNCIP's external communication strategy, including cascading of the ERNCIP outputs.

The group members are expected to be a conduit for ERNCIP activities to the CIP communities in their Member State.

2.3.2. The ERNCIP academic committee

The ERNCIP academic committee, consisting currently of 12 renowned senior scientists in fields relevant to CIP, was first convened in 2013. It is a multidisciplinary advisory body to the ERNCIP office and the TGs, and in that capacity it has an important role as a link between academia and the ERNCIP. It is also a forum for further development of CIP-related knowledge in the academic community in Europe.

2.3.3. ERNCIP Operators' workshops and cross-sector conferences

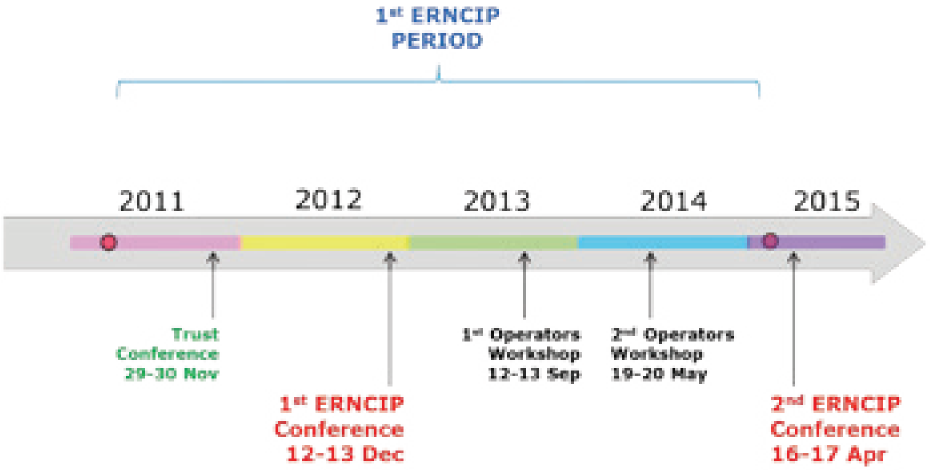
Unlike the other advisory groups organised with a standing panel of members, the third advisory area of the ERNCIP is facilitated through workshops in order to provide more flexibility for participants. Participation in workshops does not require any formal regular commitment, so that operators can participate according to their specific CIP interests and availability. The purpose of the operator workshops is to provide an 'end-user pull' for the ERNCIP work, whereby ERNCIP results and findings can be disseminated and discussed. In this way, the ERNCIP and its TGs can obtain immediate feedback on their work, and build further relationships with infrastructure operators, who in essence are the end-users of CIP solutions.

2.3.4. Other ERNCIP events

In addition to organising dedicated workshops for operators, the ERNCIP held a trust conference on 29-30 November 2011 and two ERNCIP conferences (12-13 December 2012 and 16-17 April 2015 ([3])). These multi-stakeholder events gathered representatives from all ERNCIP stakeholder groups, inter alia Commission DGs, Member State authorities, industry, academia, research facilities, and operators.

As illustrated in Figure 4 below, ERNCIP has organised a major event each year.

Figure 4: ERNCIP conferences and workshops


1st ERNCIP PERIOD
2011
2012
2013
2014
2015
Trust Conference 29-30 Nov
1st ERNCIP Conference 12-13 Dec
1st Operators Workshop 12-13 Sep
2nd Operators Workshop 19-20 May
2nd ERNCIP Conference 16-17 Apr

[3] Even though this conference technically took place after the first ERNCIP period, the conference was mainly focussed on the achievements and results of ERNCIP's activities 2011-2014.

More information on these events is presented in Appendix C.

2.4. References

(Council, 2008) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF, p. L 345/77.

(EC, 2012) Available online: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0417&from=EN

Gattinesi, P. and Pursiainen, C., *European CIP-related testing capabilities: Gaps and Challenges*, EUR 26229, Luxembourg (Luxembourg): Publications Office of the European Union, 2013, JRC85192

SWD(2012) 233, Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Security industrial policy, Action plan for an innovative and competitive security industry, Brussels, 26.7.2012. SWD(2012) 233 final. COM(2012) 417 final, Available online: http://ec.europa.eu/enterprise/policies/security/files/communication_from_the_commission_-_security_industrial_policy_action_plan_for_an_innovative_and_competitive_security_industry_en.pdf

M/487 (2011), Programming mandate addressed to CEN, Cenelec and ETSI to establish security standards, M/487 EN, Brussels, 17 February 2011, Available online: ftp://ftp.cencenelec.eu/CENELEC/EuropeanMandates/M_487.pdf

(CIPRNet, 2015) ‘Critical infrastructure preparedness and resilience research network, project summary’, Available online: https://www.ciprnet.eu/summary.html

3. The ERNCIP inventory and the ERNCIP platform

From the outset, the ERNCIP focused on the need to identify the European laboratories capable of testing security solutions for CIP. Consequently, the ERNCIP developed a system to identify those laboratories with the competence and the experimental/testing equipment to operate in this specific field.

The inventory was released online in June 2012 with an information campaign inviting EU laboratories to place their profile into the inventory.

In 2014 a new portal, the ERNCIP platform, integrating previous work, including access to the inventory of labs, offered new functionalities to improve synergies throughout Europe among European experimental facilities, manufacturers and infrastructure operators. As at February 2015, 115 testing facilities had registered on the inventory, allowing the community of users to search for general information about the services offered (experience, competencies and accreditations) via a web application.

3.1. Concept for the inventory

The ERNCIP inventory is a repository of information. It contains profiles and services of European laboratories, public and private, which are developing relevant tests within the field of CIP. It was primarily developed to meet the needs of operators and CIP decision-makers. The objective of the inventory is to help all types of CI stakeholders to identify and contact CIP-related experimental facilities which have competence in their areas of interest. The inventory addresses this by storing relevant data and providing users with the capability to search this data.

To be eligible to store information in the inventory, facilities need to have a legal status and provide evidence that they work on CIP-related matters. Registration in the inventory is analysed and validated by the ERNCIP office according to specific conditions.

The profile of laboratories includes basic details such as the name of the organisation, address and contacts, the number of employees, the services provided, specific competences and accreditations. Under 'experience' labs can profile their participation in networks and associations. Additionally, facilities can list their test equipment, test beds and test range, and upload supporting documents for publications, certificates, etc.

Consultation of the inventory is limited to organisations that conduct activities related to CIP, e.g. infrastructure operators, governments, research organisations, security-solution providers, all of whom need to register as a 'search user'. The decision to allow access to the ERNCIP inventory search services is made by the ERNCIP office. Successful registration of an organisation will authorise every employee to access the ERNCIP inventory's search services, simply by using the organisation's email address domain.

3.2. Development process: user requirements, design, and implementation

The user requirement phase of the inventory involved initially the ERNCIP team who gathered the ideas and guidelines from various experts and operators of CIs. With the support of DG Migration and Home Affairs, the ERNCIP team visited many representatives of the Member States, particularly those with responsibility for the protection of CI. These meetings were extremely helpful in identifying the overall objectives of the system.

In 2011, the ERNCIP group of EU CIP experts (expert group) agreed on the business objective for the ERNCIP inventory. A system-requirements specification was formally conducted to drive the implementation of the proposal. The process was based on a large-scale consultation done via direct interviews and through a survey that was sent to: the members of the expert group, the inventory key user group, a group of experts that were chosen from a representative group of laboratories, academia and government stakeholders for detailed business requirements.

After completion of the requirement gathering and analysis of the needs, the software design preparation started. The process also included visits to the key user group members with the objective of gathering feedback on the quality of the design and validating the activities to be included within the implementation phase.

A software development team converted the system design to a software solution, according to the requirements of the European Commission for the definition of the architecture, infrastructure and security of the software solution. The first pilot of the system with the core functionality was delivered in January 2012.

The expert group members expressed positive comments about the solution provided, and accepted the implementation of the core functionalities. Before the ERNCIP inventory was made public, an independent security assessment was required: the assessment of the system design and security controls was implemented and penetration tests performed.

The first official release of the system for end-users went live on the 4 June 2012.

Development on the inventory has continued, providing significant improvement and extension of the functionality of the system. Further releases improved the search capabilities, profile editing capabilities, geographic information system (GIS) functionality and reporting functionality, as well as improving the security of the system.

3.3. Data population

When the system went into operation, the ERNCIP office launched a marketing campaign to encourage laboratories to add their profiles in the system, and to promote the use of the system among organisations that have interest in the area of CIP. Various marketing channels were used, including inviting the national points of contact (POCs) for the EPCIP to become involved in the process.

Particular effort has been made to encourage all relevant members of the ERNCIP TGs to register in the system.

3.4. Benefits of the inventory

Membership of the inventory offers CIP-related experimental or testing laboratories greater visibility among CIP communities. The benefits for the laboratory are as follows.

- To promote the experimental facilities to CIP communities around the world.
- To increase business potential, as the inventory is used by public and private sector.
- To seek innovative solutions to complex problems within the network.
- To increase potential for cooperation and exchange of knowledge with similar experimental/testing organisations.

The inventory helps all types of CI stakeholders (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 the following.

- 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).

3.5. The ERNCIP platform

The ERNCIP platform was launched in summer 2014. It is a comprehensive solution for sharing knowledge and expertise in order to harmonise test protocols throughout Europe. The platform, built on previous ERNCIP work including the inventory, has integrated new functionalities to improve synergies among European experimental facilities, manufacturers and CI operators; providing better opportunities to connect through testing standards and guidelines. The ERNCIP now offers an updated repository of standards and guidelines, linking them to relevant labs, making their testing capabilities more accessible and transparent. This is intended to open up new business opportunities for testing labs by better connecting them to organisations needing their testing services. Using a content management system, the platform provides integrated access to:

- the inventory of labs, a free-to-use search tool for open-source information on European security experimental and testing facilities;
- a list of standards, best practices and guidelines relevant to CIP;
- the activities of ERNCIP's networks of experts, describing the TAs and the work of the TGs;
- a download area containing all of the ERNCIP's deliverables;
- an outline of the ERNCIP and its governance.

3.6. Conclusions

The use of common methodologies and standards for testing security products and technologies may contribute to enhancing competitiveness of the EU security industry by reducing the fragmentation of the EU market and make security-solution needs more accessible for public authorities, CIP operators and citizens.

The experience shows that the ERNCIP initiative is an effective technical cooperation example among CIP actors. Awareness of the existing and specific competencies in the European Union is, through the development of the inventory, one of the initiative's essential starting points. The platform, including the inventory, facilitates knowledge and innovation exchange based on the availability of technical expertise and other key attributes declared by the EU facilities involved.

The variety of tools that have been put in place in the form of the ERNCIP platform now facilitates the creation of active communities of CIP-related experts from the public and private sector, research organisations, academia and national authorities.

The ERNCIP will continue to proactively invite CIP stakeholders to explore the facilities available through the ERNCIP platform to learn more about security-related issues and to discover opportunities to collaborate to improve the quality of security products, services and processes.

4. The ERNCIP thematic groups

The core activity of ERNCIP has been to address priority CIP-testing areas of concern at the EU level through the operation of the ERNCIP thematic groups (TGs). These comprise a small network of nominated experts, drawn from relevant experimental facilities and laboratories, and other stakeholders such as manufacturers and vendors of security solutions, government authorities, academia, and operators of critical infrastructures. Each TG is led by a coordinator appointed by ERNCIP (in some cases assisted by one or several deputy coordinators) who manage the work of the group.

ERNCIP TGs are directed to identify and evaluate the existing testing capabilities and gaps, as relevant to their given scope. The TGs analyse the different options for meeting the capability gaps, including EU-led and/or EU-funded approaches, Member State-based approaches, market-based approaches, or viable combinations thereof. The overall aim of TGs is to produce recommendations to the relevant funding and implementation bodies, including the respective EU policy areas, so that specific policy conclusions can be articulated in the relevant EU policy.

ERNCIP TGs are encouraged to identify other relevant projects or networks, particularly at EU level, in order to build on previous work and cooperate to avoid overlaps.

Experts provide their time on a voluntary basis while ERNCIP funding supports their travel and accommodation costs for participating in pre-approved meetings. Additionally, the coordinator/deputy coordinator (or his/her organisation) can be compensated for up to 30 working days annually for pre-approved work on the TG.

4.1. Applied biometrics for critical infrastructure protection

4.1.1. Purpose

Biometric identity technology, such as fingerprint, iris or face recognition, is expected to become more and more common for access control to critical infrastructure. Testing and evaluation of solutions 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 of biometric technologies. There are also issues of privacy and data protection to consider.

The reliability of biometric technologies is generally unknown. In particular the following criteria are often unknown or impossible to compare against those of competitors.

- The performance of the underlying biometric system.
- The robustness to vulnerabilities such as direct (spoofing) or indirect attacks.
- The strength of privacy preservation techniques.

The lack of standard operational evaluations is the reason that we cannot measure the reliability of these biometric technologies. Some initiatives exist in Europe, the United States, and Asia. However, these initiatives are isolated (focusing only on one or two biometric modalities), disorganised, or limited in time (very few are organising ongoing evaluations). This leads to discontinuous and non-integrated efforts which have a limited life span.

Thus there is a need for establishing a framework to evaluate, in a systematic way, the performance of biometric technologies using several metrics and criteria (performance, vulnerability, privacy).

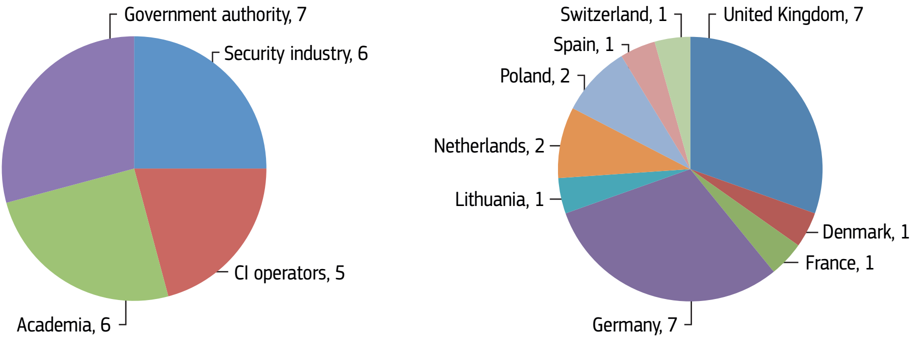
Two principle objectives were identified for this group:

- To develop resources that highlight the appropriate use of biometric technologies and systems in application to critical infrastructure protection (CIP); and
- To contribute to the standardisation, evaluation, testing and certification initiatives in key application areas.

4.1.2. General description of the thematic group

Coordinator: Marek Rejman-Greene, United Kingdom Home Office Centre for Applied Science and Technology (CAST), United Kingdom

Figure 5: Applied biometrics for critical infrastructure protection — Constitution of thematic group organisations in terms of stakeholder group and country



The group met nine times between December 2012 and January 2015.

4.1.3. Way of working

The group decided to split its work into a number of tasks, organised under two broad headings.

- Work on awareness, elicitation of priorities, and promotion of appropriate use of biometrics for security of infrastructure.
- Work on standardisation, evaluation, testing and certification to meet the requirements of infrastructure operators and other stakeholders.

Specifically, the group identified the following applications where biometrics can particularly support security processes.

- Automated border controls.
- Physical access control (particularly to special zones within a restricted area of operation of critical infrastructure).
- Logical access control (additional security for access to information and communication technology (ICT) systems).
- Mobile identity checks ('on-the-spot challenge'/virtual zones in restricted areas of operation of critical infrastructures).
- Biometric recognition of individuals from closed-circuit television (CCTV) (link with the ERNCIP TG on video analytics and surveillance).

4.1.4. Results and deliverables 2011-2014

The main achievement of the group was the consolidation of the input from EU experts into standardisation work on the use of biometrics, at International Standards Organisation (ISO) level for use of face recognition in CCTV systems, and at CEN level in the creation of a new work item on standards on the use of biometrics for physical access control.

ERNCIP TG members made significant contributions to a new work item for a multipart standard (ISO/International electrotechnical commission (IEC) 30137), accepted by ISO/IEC technical committee SC37 for use of face recognition in CCTV systems, by helping to develop a base document in support of the main submission, comprising recommendations on design and specification and on testing and reporting practices. In addition, the ERNCIP TG coordinated EU-level input at the regular SC37 working group meetings during 2014 and 2015.

Similarly, ERNCIP TG members developed a proposal for the biometric part of a European standard for physical access control within a secure area. This led to a new work item being presented to the CEN technical committee 224 working group 18 in 2014.

Additionally, two reports were published by the group, both aimed at increasing the awareness of end-users about the potential and the limitations of biometric technology for improved security.

The report, 'Experiences from large-scale testing of systems using biometric technologies' ([4]), is primarily aimed at organisations looking to implement very large-scale identification systems (e.g. national systems which may run to many millions of individuals), but is also useful for any organisation looking to develop systems based on biometric technology. It describes a systematic approach to testing based on a case study of large-scale testing of biometric systems, which enables the performance of the proposed biometric matching system to be characterised to ensure that it is 'fit for purpose'.

The report 'Application of biometrics in critical infrastructures operations: guidance for security managers' ([5]) is principally addressed at managers and security officers of organisations operating critical infrastructure in the EU. It provides an overview of the application of biometric technologies to achieve secure recognition of individuals, and offers guidance about the implementation of physical access control systems using biometrics.

[4] Waggett P., *Experiences from Large Scale Testing of Systems using Biometric Technologies*, EUR 27190, Luxembourg (Luxembourg): Publications Office of the European Union, 2015, JRC95455.

[5] Rejman-Greene M. et al, *The Application of Biometrics in Critical Infrastructures Operations: Guidance for Security Managers*, EUR 27191, Luxembourg (Luxembourg): Publications Office of the European Union, 2015, JRC95453.

4.1.5. Expected future focus

The activities initiated with ISO and CEN for biometric CCTV and for physical access control will need to be continued in order to reach the objective of developed standards in 2016. In addition, it is being planned to consult with stakeholders on their areas of concern around European norms for data privacy and biometrics that are being challenged by current and proposed implementations of systems using biometric data.

4.2. Aviation security detection equipment

4.2.1. Purpose

The European Commission is defining legally binding technical specifications and performance requirement standards for various types of security detection equipment used at EU airports. The introduction of eligible instruments and performance standards in EU legislation [6] 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 [7] are that there is no legally binding testing and approval procedure in place in the EU for aviation detection screening equipment.

Consequently, a common EU certification, testing and trialling scheme for aviation security equipment is required. The European Commission is studying the feasibility of a regulation laying down rules on the organisation and operation of accreditation of conformity assessment bodies for aviation security. As the common testing is envisaged to be carried out at several accredited test centres in EU Member States, a system to test the quality of test centres will be required.

[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2010R0185:20120321:EN:PDF

[7] Presentation at ERNCIP conference, December 2012 http://ipsc.jrc.ec.europa.eu/fileadmin/repository/sta/cinet/docs/erncip/1sterncipconference/Session1-Michael_Hill.pdf

4.2.2. General description of the thematic group

The Aviation security (AVSEC) detection equipment thematic group (TG) was coordinated by the JRC's Institute for Reference Materials and Measurements (IRMM) and was one of the largest TGs in the ERNCIP, bringing together all types of stakeholder groups. The full group met three times between February 2012 and November 2012. However, the main form of collaboration was through smaller working groups, including those for explosive trace detection (ETD), CTMs, and on procedures for approval employed in the EU for aviation security detection equipment, with three additional sub-group meetings held in 2013.

The AVSEC group worked in a high-profile area which was already extensively regulated and where some common test methodologies and a test and evaluation process have been established by the European civil aviation conference, although this is not legally binding. The challenge was to transform these to legally binding procedures to be embedded in EU legislation.

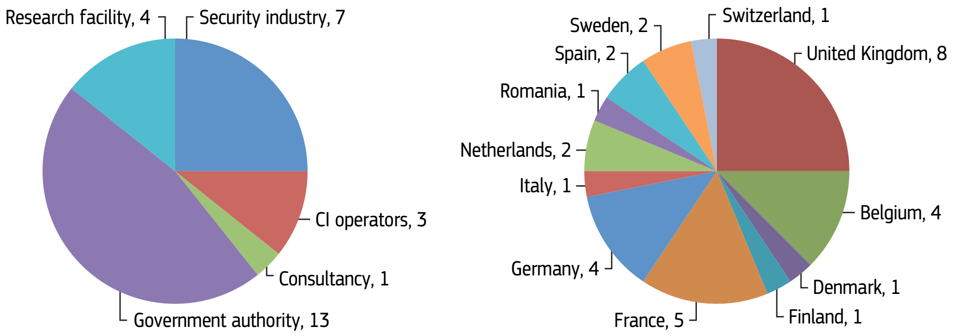
The TG was thus focused on the aviation sub-sector, with the scope of potential activities covering:

- technical specifications and detection requirements,
- common testing methodologies (CTM),
- development of an EU certification system,
- technical exchanges with third countries (non-EU and non-EFTA) and international organisations.

Coordinator: Göran Lövestam, JRC IRMM, Geel

Deputy: Michael Berglund, JRC IRMM, Geel

Figure 6: Aviation security detection equipment — Constitution of thematic group organisations in terms of stakeholder group and country



4.2.3. Way of working

Close cooperation within the European Commission, between the JRC, DG Enterprise and Industry (now DG Internal Market, Industry, Entrepreneurship and SMEs), DG Migration and Home Affairs and DG Mobility and Transport, was essential, and the TG provided technical/scientific support to the Commission regulatory committee on aviation security. The work was also aligned to the work programme of the European civil aviation conference (ECAC) technical task force, and the rolling programme annexed to the cooperation arrangement between the European Commission and ECAC.

The work of the TG was undertaken by dedicated working groups, according to the defined work programme, monitored at the full TG plenary meetings.

Working groups are as follows.

- Inventory of approval procedures for aviation security detection equipment used in the EU.
- Explosives trace detection.
- Validation of existing common test methodologies.

4.2.4. Results and deliverables 2011-2014

The group analysed the ECAC common testing methodologies (CTM), providing them with comments (all classified at EU restricted/EU confidential level) for:

- security scanners,
- explosive detection systems,
- liquid explosive detection systems.

In addition, the group also produced the following reports (also classified EU restricted):

Technical considerations on explosives trace detection in EU Legislation *(JRC85509)*

Explosives trace detection (ETD) indicate presence of explosives by detecting trace amounts of explosives, either in the form of particulate material or as a vapour. Due to its high sensitivity, ETD is today regarded as an essential tool for airport security screening. The EU regulator has also included ETD as eligible equipment, sometimes as a supplementary technique, for practically all regulated screening situations at EU airports. However, detailed measures for its actual use are rather sparse and not consistent across the various chapters of the regulation. There are measures detailed for its use in some situations but not for others. Guidelines on sampling are not consistent and sometimes missing. Furthermore, detection performance standards remain to be defined. This 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.

Detection requirements and testing methodologies for aviation security screening devices in the European Union and the European Free Trade Association *(JRC81650)*

The European Commission is laying down legally binding technical specifications and performance requirements for aviation security screening equipment used at EU airports. Introducing such performance standards in legislation requires a harmonised single European conformity assessment mechanism. As preparation for such a certification scheme, this study was carried out by the TG to get a better view of the performance requirements and testing methodologies for screening equipment at civil airports employed in the EU and the European Free Trade Association (EFTA) Member States today, including the process of acquiring equipment. The study was based on the responses to a questionnaire that was distributed via the Regulatory committee on aviation security to EU and EFTA states' authorities in November 2012. The results from the study 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. Usually two entities are responsible for adjusting sensitivity settings: the airport operators and the appropriate authorities.

4.2.5. Expected future focus

The continued involvement in the ERNCIP in this thematic area was discussed at an internal multi-service Commission meeting in December 2013. DG Mobility and Transport was grateful for the progress made by the AVSEC TG, which had successfully achieved cooperation between the Commission and ECAC. It was agreed that the next steps in this area could proceed efficiently and effectively through direct contact between DG Mobility and Transport and the JRC IRMM at Geel, and therefore all activities were successfully transferred to JRC IRMM from ERNCIP.

4.3. Case studies for the cybersecurity of industrial automation and control systems

4.3.1. Purpose

Industrial automation and control systems (IACS) increasingly constitute a target for cyberattacks. Such attacks could have a wide range of repercussions including disrupting Member State economies, disabling critical infrastructures or disrupting the daily lives of citizens. Such hostile acts could take place within the context of geostrategic tension, or for the purposes of organised crime, or in support of various activist causes.

Indeed recent incidents and reports show that IACS can be vulnerable to cyberattacks leading to disruptions of physical systems, networks and ultimately the services they provide. This makes security for IACS an important part of CIP.

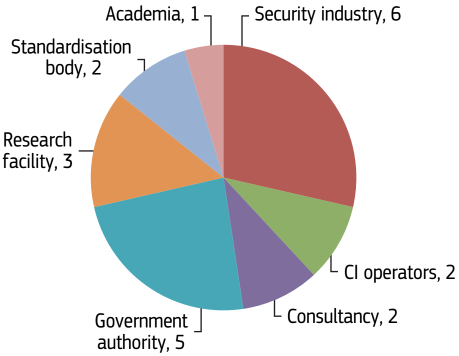
Against this backdrop, the ERNCIP TG Case studies for the cybersecurity of industrial automation and control systems, coordinated by Paul Théron and Sandro Bologna (deputy), was established specifically to answer the question: With regard to their cybersecurity do European critical infrastructure operators need to get their IACS components or subsystems tested and certified? If 'yes', a second question: Generally speaking, what are the conditions of feasibility for successfully implementing a European IACS testing and certification scheme?

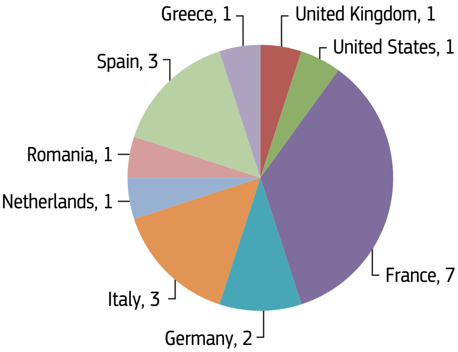
4.3.2. General description of the thematic group

This was the second ERNCIP thematic group (TG) in this thematic area. It was established in late 2013 to investigate the need for testing and certifying the cybersecurity of IACS components and subsystems that may play a role in the vulnerability of critical infrastructures.

The group has accordingly mobilised representatives of IACS vendors, industrial operators and national cybersecurity authorities, who are interested and skilled in this area. The members of the group met three times between March 2014 and September 2014.

Figure 7: Case studies for the cybersecurity of industrial automation and control systems — Constitution of thematic group organisations in terms of stakeholder groups and countries





4.3.3. Way of working

The TG's work was organised in three successive phases:

Phase 1: Needs identification — 19 March 2014 (Kick-off) to 18 June meeting, seeking to do the following.

- Set a common work plan for phase 1.
- Identify case studies understood as points of potential cyber vulnerability within IACS: five case studies were identified. They refer to IACS components that can embed security functions and solutions but are not security products themselves.
  - Supervisory control and data acquisition (SCADA) [8] systems that supervise entire industrial systems.
  - Programmable logic controller (PLC)/intelligent electronic device, i.e. field process automation and control equipment.
  - Engineering/programming workstations that staff connect to in order to program the field servers and components of an IACS.
  - Databases used for process control (if corrupted, that may create safety issues, e.g. in airport luggage handling).
  - Telecommunication links (for instance for remote equipment maintenance).
- Each case study was to be situated in a sector of activity.
  - Hospital, airport, electricity distribution, car manufacturing, chemicals, etc.
- Phase 1's method consisted of the following arrangements.
  - A questionnaire was elaborated in order to understand stakeholder views of the cyber threat and to analyse their background concerns behind

[8] See (ENISA, 2011a) for detailed definitions of IACS components.

the question of IACS cybersecurity certification. This questionnaire was dispatched to TG members and other industrial operators. On reception of answers (13 in total) only basic statistics were performed in order to 'profile' the positions expressed by the respondents.

- A literature review took place, including: (European Union Agency for Network and Information Security (ENISA), 2011), (ENISA, 2013a), (ENISA, 2013b), reports from the supervisory control and data-acquisition laboratory (Scadalab) project [9], (MITRE, 2011), cybersecurity certification standards (Common criteria — ISO 15408, ISA Secure [10] and its derived Wurldtech communication robustness testing scheme [11]).
- The project's core team met to analyse and synthesise results and to elaborate findings before the June meeting.
- The thematic expert group met in June (Ispra) to discuss phase 1's findings and to conclude on the need for IACS testing and certification in Europe. This meeting also discussed existing cybersecurity schemes (Common criteria, ISA secure, Wurldtech). It confirmed the need for a European IACS certification scheme. It concluded that the focus of the scheme had to be on IACS components, i.e. individual products rather than subsystems or systems.

Phase 2: Conditions of feasibility — 18 June 2014 to 24 September meeting, seeking to do the following.

- Define the concept of IACS testing and certification if phase 1 answered 'yes' to the question of the need for such a scheme in Europe.
- Perform the corresponding feasibility study.
- Define a plan of action towards the possible implementation of the scheme over the next 5 years.
- Phase 2's method consisted in the following arrangements.
  - The project's core team first worked to elaborate a basic scheme proposal.
  - Face-to-face meetings with TG members (national cybersecurity authorities, industrial operators, vendors) were then organised to react to and to amend the proposed scheme; significant modifications were then brought to the original proposal and helped to specify the goals and the broad characteristics of the scheme.
  - The project's core team then finalised phase 2's findings and elaborated a plan of action for the period 2015-2020, and prepared the 24 September meeting of the TG experts.
  - The thematic expert group met on 24 September 2014 (Ispra) to discuss and finalise the proposed Compliance and certification (C&C) scheme.
  - The proposed scheme was discussed with ENISA at the September meeting (video conference) and later presented at the Easy e-services to shape and empower SME networks in central Europe (Essence) project's

[9] https://www.scadalab.eu/index.php/mod.documentos/mem.listado/relmenu.3

[10] Managed by the ISA security compliance institute (ISCI); www.isasecure.org

[11] www.wurldtech.com

meeting of 14 October 2014. This latter presentation did not generate any revision of the scheme.

Phase 3: Report — 24 September 2014 to 1 November 2014, seeking to do the following.

- Deliver to the JRC the report of the TG's work.
- Phase 3's method consisted in the following arrangements:
  - TG coordinators worked to write the final report of the study;
  - This report was reviewed by TG members and by the JRC.

4.3.4. Results and deliverables 2011-2014 [12]

This TG had three outcomes.

(1) Short case studies (13) complemented by TG experts' discussions to answer the first question. They concluded to industry operators' appetence for cybersecurity-certified IACS products. They also showed that, provided a European certification scheme was in line with state-of-the-art cybersecurity, supported by mutual-recognition agreements between Member States (and beyond Europe), and not mandatory, it would be viable for vendors.

(2) A set of research directions in the form of a possible European IACS cybersecurity C&C scheme as an answer to the corollary question.

- Two levels [13] of increasingly trustworthy compliance assessment.
  - Level 1: Compliance self-assessment.
  - Level 2: Compliance third-party assessment.

- Two levels of increasingly demanding certification.
  - Level 3: Third-party product certification.
  - Level 4: Third-party full certification.

- This C&C scheme relies on three assumptions.
  - Assumption 1: a common logic exists among existing cybersecurity certification standards.
  - Assumption 2: a set of common testing and certification bricks need to be established to create a European scheme.
  - Assumption 3: a multi-level scheme is needed to engage stakeholders towards testing and certification.

- This C&C scheme would entail no obligation, unless otherwise specified by law or regulation.

[12] As stated in 4.3.2 this thematic group was established late 2013.

[13] It has been suggested that the first two levels (1 and 2) could be combined into a single one, making the total number of levels 3 only.

  - Levels 1 and 2 would depend on clients' requests (e.g. in calls for tenders).
  - Vendors' choice would be made by marketing teams.
  - Level 1 can be a starter approach, and level 2 can be chosen to increase clients' trust.
  - Levels 3 and 4 would depend on clients' requests or on legal/regulatory obligations in specific domains or applications (e.g. defence, nuclear industry, etc.).
  - Level 3 adds cybersecurity robustness tests to level 2's assessment 'on paper'.
  - Level 4 adds process certification to the product certification provided at level 3.
  - The choice of the C&C level could depend on vendors' target markets and their willingness to go for the best cost/advantage ratio.

(3) A research and action roadmap towards the possible implementation of the proposed European IACS cybersecurity C&C scheme. This road map articulates a set of seven actions to be run, by the JRC or not, over the 2015-2020 period. This plan is starting with an action aiming at prioritising work, at engaging a wider set of stakeholders, and at creating the conditions for an effective implementation of a European IACS product C&C scheme.

The TG showed that on a European level some form of agreement can be reached between stakeholders. It also highlighted the need to identify which elements are common to existing standards used for cybersecurity certification such as IEC 62443 and ISO 15408.

It also highlighted some limits to IACS' cybersecurity certification.

- Technical and semantic limits.
  - The certification of IACS products does not mean an IACS system, as a whole, is cybersecure. It only testifies that a component does the following:
    - Complies with a cybersecurity profile's requirements (levels 1 to 4).
    - Resists cyberattack tests (levels 3 and 4).
    - Has been developed through a satisfactory engineering process (level 4).

- Limits of validity as the 'quality' of certificates will:
  - depend on a process of accreditation of third-party assessors/labs (levels 2, 3, 4);
  - depend on IACS vendors' regulators/syndicates to guarantee fair practices (Level 1);
  - depend on mutual recognition across Europe and beyond.

4.3.5. Expected future focus

The 5-year plan of action proposed to the JRC will involve all parties and stakeholders concerned by IACS cybersecurity certification.

4.3.6. References

ENISA (2011), *Protecting industrial control systems. Recommendations for Europe and Member States.*

ENISA (2011a), *Enabling and managing end-to-end resilience,* Retrieved from http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/e2eres

ENISA (2011b), *Protecting industrial control systems. Annex I: Desktop research results.*

ENISA (2013), *ENISA Threat landscape 2013. Overview of current and emerging cyber-threats.*

ENISA (2013a), *Good practices for an EU ICS testing coordination capability.*

Eurocontrol (2012), *Manual for national ATM security oversight document — Directorate single sky,* DSS/CM/SEC/DEL/12-044.

Mahan, R. E., Fluckiger, J. D., Clements, S. L., Tews, C., Burnette, J. R., Goranson, C. A., and Kirkham, H. (2011), *Secure data transfer guidance for industrial control and SCADA systems,* Richland, Washington: Pacific Northwest National Laboratory.

MITRE (2011), *Cyber resiliency engineering framework,* Report MTR110237.

MITRE (2013), *Cyber resiliency and NIST special publication 800-53 Rev.4 controls, Technical report,* MTR130531.

4.4. Chemical and biological risks in the water sector

4.4.1. Purpose

By definition critical infrastructures are vital for the provision of essential societal services which are delivered and maintained by specific assets pertaining to a sector. The supply of water represents such a service and is identified by a network of assets that form infrastructures and clearly contribute to the well-being of European society.

Further, since water is a limited and a vital societal resource, any form of contamination of water systems can have a huge impact, permanent or otherwise, on society. Indeed several incidents in the past testify to the global vulnerability of drinking water systems.

The triggering of such events is mostly due to human errors, accidents or extreme weather. However, malicious acts are also reported in literature and affirm that the threat of terrorist attacks on water supplies is real. Historical evidence of attacks to water supply systems is abundant and goes back 4 500 years. An early example of chemical warfare is the siege of the city of Kyrrha in 595 BC where hellebore roots were used by the Greeks (Mayor, 2003) to poison the local water supply in order to eventually force the city to surrender (Borchers, et al., 2013).

Fortunately, massive casualties as a result of an attack on water networks are difficult to produce. Nevertheless the risks of societal disruption, disarray and loss of trust in public authorities and resulting safety, all remain high (Gleick, 2006).

An additional layer of complexity is tied to environmental issues and how these impact the sources of quality water which is intended for human consumption. Not surprisingly, environmental water bodies today govern and protect drinking water supply through specific legal frameworks, such as the water framework directive (European Union, 2000) which aspires to keep chemical pollution at a safe level so as to guarantee ‘good’ chemical and ecological status. Consequently, Member States are obliged to carry out continuous monitoring of the water, document the stipulated ‘good’ status and, if necessary, take action through appropriate measures.

Once water is taken from the environment and provided as drinking water, its suitability for human consumption needs to be monitored regularly. This is done against predetermined quality standards set out in the same drinking water directive. This directive addresses the health of the consumers in the European Union and makes sure that drinking water is healthy and clean. Supplementary regulations deal directly or indirectly with the protection of drinking water.

The current regulations take a long-term monitoring perspective. As a consequence, short-term events or incidents are likely to go unrecognised, without the capabilities of detecting such changes in real time. This requires the installation of real-time 'event detection' systems that warn operators and decision-makers of potential contamination directly at the site where such conditions develop or where incidents are perpetrated.

Nevertheless, classical and lengthy analytical approaches are still required to identify and quantify the type of contamination.

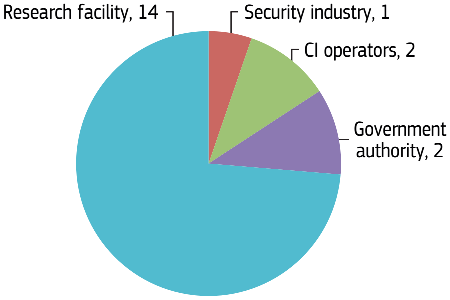
This ERNCIP TG identified three priorities considered to be highly relevant to drinking water.

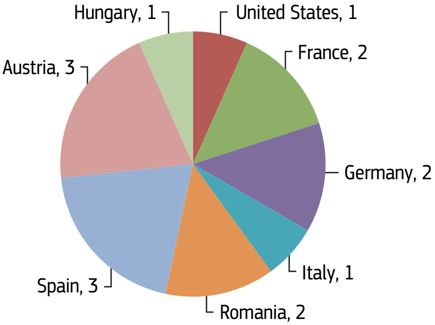
- Event detection systems, which indicate in real time a change of the water quality in piping systems used for the distribution of drinking water supply.
- Rapid identification and quantification of biological and chemical contaminants in water samples by means of sophisticated analytical techniques.
- Innovation and use of innovative systems to safeguard water quality.

4.4.2. General description of the thematic group

The group was coordinated by the Austrian environment agency, with the members of the group meeting 10 times between April 2012 and January 2015. Participating organisations per stakeholder group as shown.

Figure 8: Chemical and biological risks in the water sector — Constitution of thematic group organisations in terms of stakeholder group and country





4.4.3. Way of working

The group decided to take a comprehensive approach, starting from the environmental source of water, its subsequent sanitation and distribution in pipe networks and concluding at the return of waste water to the environment. Furthermore, the reuse of water is considered as far as its effects on drinking water quality are concerned.

The relevant scenarios that can cause direct contamination such as floods, droughts, malicious acts or indirect contamination by interruption of the drinking water supply (blackout, SCADA attack, etc.) were considered. Therefore, the TG sought to contact and liaise with as many other projects and researchers as possible, with members participating in various conferences in the fields of security, CIP and CBRN-E. One such opportunity was provided by the fifth water contamination emergencies conference 2013 in Mülheim/Ruhr, Germany (Hohenblum, 2013). During this conference the TG became aware of the SecurEau project consortium which was funded under FP7.

The main objective of SecurEau (Fass, 2013) is to launch an appropriate response for rapidly restoring the use of the drinking water network after a deliberate contamination. Its focus is on sensors, the design of methodologies to identify new relevant contaminants and developing methods to decontaminate polluted drinking network and installations.

The group decided to present its findings to water utility operators, and organised a workshop in Arona (Italy), in June 2014 (see Appendix C, C5). The workshop focused on the needs of the operators and sought views on the use of event detection devices in the future.

In preparation for the workshop, a questionnaire was developed with the intent to explore the degree of use of event detection systems at water utilities. The questionnaire, covering relevant security issues and translated into Spanish, German, English, French, Italian, and Romanian, was circulated via the 'Your voice for Europe' platform, and also disseminated by some national drinking water associations to their members and direct contacts (including outside the EU).

4.4.4. Results and deliverables 2011-2014

Event detection systems

In order to detect changes in water quality the continuous monitoring, in real time, of chemical and/or physical and/or biological parameters is necessary. To this end, sensors and probes which can be placed at any conceivable location in a utility or in a network are already available on the market.

One of the first outputs from this group was an appraisal of state-of-the-art existing sensor technology (Raich, 2013), which included performance data, manufacturers, and costs of relevant sensor systems.

All of the detection devices discussed in the report trigger an alarm when a specific threshold is exceeded. On the basis of these triggered events the water utility operator is alerted and then takes measures to protect the distribution system and its users. Although this rationale appears simple, in reality it is a complex process since various criteria have to be met and there are numerous factors that may hinder the smooth operation of the devices mentioned.

The most problematic part of the process is to distinguish between contamination and the natural fluctuation of water composition. Furthermore, continuous monitoring also produces an outstanding amount of data and in order to keep the output simple, intelligent software solutions are needed to process and evaluate the data.

Currently, no standard approach is available which sets out criteria for the testing of such solutions.

Another review produced by this group provided an overview of the major technologies that could monitor biological pathogenic agents in the near future (Hufnagl, 2014).

These outputs were discussed in the TG's events detection workshop held in June 2014 with water operators (Hohenblum, 2014).

Rapid identification and quantification

Alarms are usually triggered by post-event detection systems, but also by consumer complaints or cases of sickness that suggest drinking water contamination with an unknown chemical and/or biological hazard. Hence rapid identification and quantification of the hazard is needed in order to take appropriate measures. The overall analytical process involves time-consuming and painstaking steps and most routine laboratories are not prepared to scrutinise for the 'unknown'.

Several initiatives exist which aim at bringing together expert knowledge to provide advanced analytical methods in the event of an incident. Indeed screening techniques seem to be promising when it comes to identifying unknown contaminants in a reasonable amount of time.

To this end, an overview covering different screening approaches for chemicals in water was compiled by the TG (Rodriguez-Moza and Llorca, 2013). Another report concerning the rapid identification of pathogens was also prepared by the TG (Tancho, 2014).

The idea behind the TG's work was to further focus on the applicability of targeted screening methods which exploit automated output spectra associations by comparing output with proof-of-identity libraries of contaminants. Similarly, other systematic approaches already address different groups of chemical and biological hazards.

The TG also found that, in response to emergency incidents, some laboratories apparently act under a mutual aid agreement or are indeed already preparing to establish laboratory networks to share competencies in this field. Meanwhile, proficiency tests are being created in order to test and improve the quality assurance of laboratory output (Kroll, 2011) (May, 2011).

4.4.5. Expected future focus

The reports completed by the group (Raich, 2013; Hufnagl, 2014) together with the outcome of the water utility operator workshop in June 2014 (Hohenblum, 2014) have helped to articulate the key issues concerning the validation of event detection systems.

The TG's future activities will be to identify critical parameters for event detection systems, and for validation by external testing facilities under 'close to real life' conditions, aiming at a workshop agreement under the Commission's M487 mandate. This should be embedded in a guideline comprising all elements of drinking water security as holistic approach. Uses of event detection systems only make sense when utilities follow a process from making decision to establish a water security plan, execution of a vulnerability assessment, definition of a protection level, design of event detection system and elaboration of an emergency response plan. The final document would be a unique guideline to raise awareness to events of low probability, but high impact.

Furthermore, the group will consider the identification work conducted by laboratories in emergency situations, by bringing together key laboratories at a workshop to discuss harmonisation of methods and procedures for identification of unknown contaminants. Further actions include valuing the outcomes of other activities like the FP7-funded standardisation of laboratory analytical methods (SLAM) project [14] (Plamboeck, 2014).

4.4.6. References

Borchers, U., Thompson, K. C. and John, G., 2013, *Water contamination emergencies: Managing the threats,* Cambridge, United Kingdom: Royal Society of Chemistry.

[14] http://www.cbrnecenter.eu/project/slam

ERNCIP Water TG, 2014, [Online] Available at: http://ec.europa.eu/yourvoice/consultations/index_en.htm [Accessed January 2015].

Fass, S., 2013, *SecurEau: drinking water,* [Online] Available at: http://www.secureau.eu/ [Accessed January 2015].

Gleick, P. H., 2006, 'Water and terrorism', *Water policy,* Volume 8, pp. 481-503.

Hohenblum, P., 2013, 'Chemical and biological risks in the water sector — A thematic area in the European Commission's ERNCIP', In: Borchers, U., Gray, J. and Thompson, K. C., eds. *Water contamination emergencies: managing the threats,* Cambridge, United Kingdom: RSC, pp. 330-333.

Hohenblum, P., 2014, Workshop on early warning systems, Brussels: European Union, JRC 94436.

Hufnagl, P., 2014, *Review of monitoring techniques for biological contaminants*, EUR 26495, Luxembourg (Luxembourg): Publications Office of the European Union, 2014, JRC88228. http://publications.jrc.ec.europa.eu/repository/handle/JRC88228

Kroll, D., 2011, *Is It Real or Isn't It? Addressing Early Warning System Alarms,* Cambridge, Royal Society of Chemistry, pp. 82-87.

May, B., 2011, 'Potable water contamination emergency: the analytical challenge', *Water contamination emergencies monitoring, acting and understanding,* Cambridge, United Kingdom: RSC, pp. 110-116.

Mayor, A., 2003, *Greek fire, poison arrows, and scorpion bombs: Biological and chemical warfare in the ancient world*: Peter Mayer Publishers Inc.

Plamboeck, A. H., 2014, *SLAM report summary,* [Online] Available at: http://cordis.europa.eu/result/rcn/143600_en.html [Accessed January 2015].

Raich, J., *Review of sensors to monitor water quality*, EUR 26325, Luxembourg (Luxembourg): Publications Office of the European Union, 2013, JRC85442.

Rodriguez Moza, S. and Llorca, M., *State of the art of screening methods for the rapid identification of chemicals in drinking water*, EUR 26325, Luxembourg (Luxembourg): Publications Office of the European Union, 2013, JRC83768.

Tanchou, V., *Review of methods for the rapid identification of pathogens in water samples*, EUR 26881, Luxembourg (Luxembourg): Publications Office of the European Union, 2014, JRC92395.

Thompson, K., Jacobson, G. and Chamberlain, K., 'Improving quality and saving dollars using real-time online water quality monitoring, in *Water contamination emergencies monitoring, acting and understanding*' RSC, Cambridge, 2011, 59-69.

Water framework directive: European Parliament and the Council of the European Union, 2000, Directive 2000/60/EC of the European Parliament and of the Council establishing a framework for Community action in the field of water policy.

4.5. Explosives detection equipment (non-aviation)

4.5.1. Purpose

Since the 2006 transatlantic aircraft plot, the EU has defined legally binding technical specifications and performance requirement standards 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. There are different needs among the stakeholders which hinder harmonisation and so it is currently not possible to propose a single scheme for the certification, testing and trialling of explosive detection equipment outside aviation.

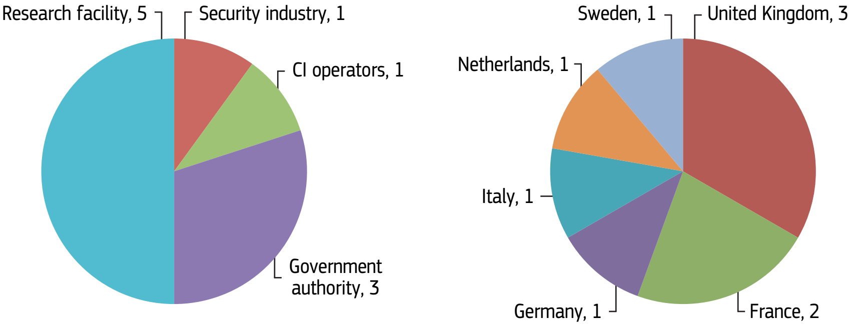
Although a CTM for testing liquid explosives for aviation security has been applied for a few years, a common methodology does not exist for the other non-aviation applications (mass transport, crowded places, etc.). A CTM requires an operational configuration and the technology that is designed to meet this requirement. In 2012, a common CTM for non-aviation security was considered to be a too-challenging task for an ERNCIP TG. Instead it was thought that, a common methodology to evaluate the capabilities of the available detection equipment (e.g. does it detect explosives?) and check the claims of manufacturers would be helpful, as it would provide an indicator to the potential of detection systems.

4.5.2. General description of the thematic group

The TG for explosives detection equipment (non-aviation) (DEMON) was coordinated by the French alternative energies and atomic energy commission (CEA). As it covered many similar issues as the AVSEC TG, it had some overlap in membership.

The TG met five times between April 2012, and December 2013.

Figure 9: Explosives detection equipment (non-aviation) — Constitution of thematic group organisations in terms of stakeholder group and country



4.5.3. Way of working

The first step planned by the group was the compilation of the operational needs for explosive detection outside the aviation security area, involving end-users (police, customs, transport operators, etc.) and national detection experts. It was intended that the technical requirements of a European CTM (to evaluate the general capabilities of detection equipment and the requirement to validate manufacturers' performance claims to meet these needs) would subsequently have been identified, leading to recommendations for the initial elements for a European common testing methodology for the capabilities of equipment to detect explosives.

4.5.4. Results and deliverables 2011-2014

Towards the end of 2013, the coordinator realised that it could not continue to meet the commitment of coordinating the group, and the group then ceased its planned activities.

During this time, the group did complete two of its planned reports.

State-of-the-art report on European legislation relating to explosives and explosive detection system for non-aviation configurations ([15]): This 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

[15] http://ipsc.jrc.ec.europa.eu/fileadmin/repository/sta/cinet/docs/erncip/downloads/deliverables/demon/European_Legislation_relating_to_explosives_and_explosive_detection_systems_for_non-aviation_configurations.pdf

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.

Statement of user needs final report: This report (classified EU restricted) identifies user needs in the area of explosives detection for infrastructure protection applications outside aviation security. It spans guidance, training, equipment development, canine capability and assurance, and considers various categories of infrastructure sites reflecting different detection needs.

4.5.5. Expected future focus

A new TG has now been formed which is looking at opportunities for benefits from standardisation activities in the detection of explosives and weapons in a secure location.

4.6. Industrial automated control systems and smart grids

4.6.1. Purpose

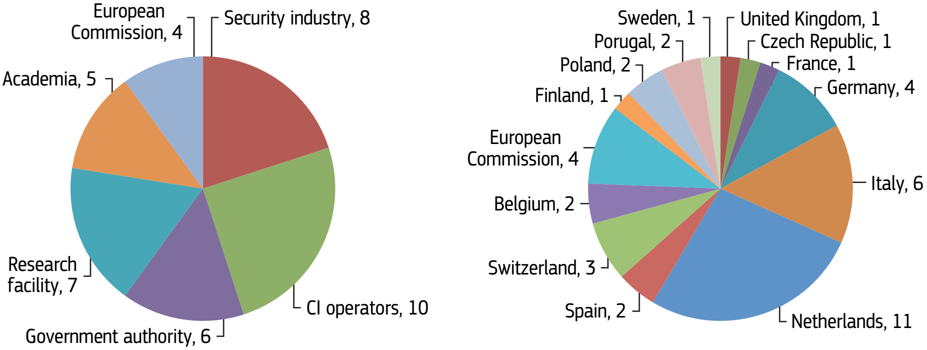
Information and communications technology (ICT) is becoming more and more important in the delivery of essential services. Recent incidents have shown that industrial automated control systems (IACS) can be vulnerable to cyberattacks and that such attacks can lead to disruptions of physical systems and networks. This makes security for IACS an important part of critical information infrastructure protection (CIIP).

For energy transmission in the future, smart grids (SG) will be a central element. The growing role of ICT in the energy infrastructure requires that cybersecurity must be taken into account in the development of SG from the outset.

4.6.2. General description of the thematic group

The IACS and SG TG was coordinated by the Netherlands organisation for applied scientific research (TNO) and was the first to hold a formal thematic group (TG) meeting in early February 2012. The group had the second-largest set of interested experts, including manufacturers, vendors and integrators of security solutions; infrastructure operators and government agencies seeking to improve security in this area; research organisations and academia. A great deal of information and diverse views were shared in the meetings.

Figure 10: Industrial automated control systems and smart grids — Constitution of thematic group organisations in terms of stakeholder group and country



4.6.3. Way of working

The original name for this thematic area was the CIIP and SCADA TA, which covers all types of cybersecurity. However, the priority was quickly established as being the SCADA elements of IACS and SG, and the name was subsequently changed to reflect this.

Discussions at TG meetings on the scope of the work to be conducted were sometimes side-tracked into discussions on common definitions for IACS, SG, and on whether to test at component or system level. With diverse views provided by the different types of organisation, consensus has been difficult to achieve on the scope of the work streams that the TG should undertake. Options include focus on the human vulnerabilities of IACS systems, and investigating the need for work on testing and certification of technology components.

4.6.4. Results and deliverables 2011-2014

Human vulnerabilities of IACS systems

During 2013 this TG contributed to the global information assurance certification (GIAC) initiative that led to the launching of the Global industrial cyber security professional (GICSP) certification ([16]).

Testing and certification of technology components

Discussions occurred around the testing and certification needs for system components, subsystems and full systems; however the group did not manage to produce any systematic analysis of the subject. Subsequently, the ERNCIP office launched a new TG 'Case studies for IACS', described in Section 4.3.

4.7. Radiological and nuclear threats to critical infrastructure

4.7.1. Purpose

The scope of the group is to identify and work on currently unaddressed protection issues such as certification of radiation detectors, standardisation of deployment protocols, response procedures and communication to the public, e.g. in the event of a radioactive object being found. Since the field is broad and the time frame very limited, the group has concentrated its efforts on the following topics.

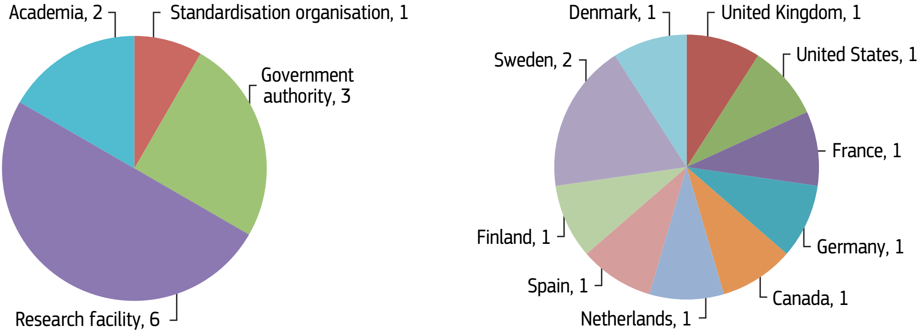
(1) List-mode data acquisition based on digital electronics.
(2) Remote expert support of field teams.
(3) Remote-controlled radiation measurements and sampling using unmanned vehicles.

4.7.2. General description of the thematic group

The Finnish radiation and nuclear safety authority (STUK) was invited by the JRC to establish and coordinate an ERNCIP TG on the protection of critical infrastructure from radiological and nuclear threats. The members of the group met nine times between April 2013 and February 2015.

[16] http://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp

Figure 11: Radiological and nuclear threats to critical infrastructure — Constitution of thematic group organisations in terms of stakeholder group and country



4.7.3. Ways of working

The kick-off meeting of the radiological and nuclear (RN) group was organised in April 2013 at Ispra, and lead scientists for the different topics were selected during this meeting from the volunteer expert members of the TG. During 2013-2014, two meetings per topic were organised. The first meeting for each topic concentrated on analysis of the state of the art and the second meeting focused on testing aspects, as well as identifying recommendations for future activities. These meetings were supplemented with a limited number of smaller sub-group meetings.

4.7.4. Results and deliverables 2011-2014

In line with its original work programme, the group has issued its analyses and recommendations.

Topic 1 — List-mode data acquisition based on digital electronics

Lead Scientist: John Keightley (National Physical Laboratory, United Kingdom)

The state-of-the-art report produced by the group on this topic (Keightley et al., 2014) identifies that future RN data-acquisition systems shall ultimately enable the movement of detection data (from first responders) electronically to analysis centres, rather than the costly and time-consuming process of moving experts and/or samples. This new technology is especially useful in crisis events, when time and resources are sparse and increased analysis capacity is required.

In order to utilise the opportunities opened by these new technologies, the systems have to be interoperable, so that the data from each type of detector can be readily analysed by different analysis centres. Successful interoperability of the systems requires that European and/or international standards are devised for the data formats.

The basis of such a format is a digital file, containing a list of registered events detailing an estimate of the energy of the detected radiation, along with an accurate time stamp for recorded events (and optionally other parameters describing each event). Such data is commonly referred to as list-mode data. List-mode data acquisition using digital electronics offers many advantages over traditional acquisition methods for the detection and assay of radioactivity. The digitisers employed are equipped with sophisticated firmware running real-time data reduction algorithms that extract only the relevant information contained in a detection pulse, e.g. its time stamp, pulse height and/or pulse shape properties. Without such data reduction, all signal samples need to be transferred which requires a data connection with a large throughput, and ultimately limits the maximum permissible count rate(s).

There are many advantages of digital list-mode data acquisition in radiation detection including the following.

- Improved radiation-detection systems can be developed for nuclear security.
- Border monitoring of nuclear materials will result in fewer false alarms.
- Novel detection systems can be built based on active interrogation of the material.
- Cross-disciplinary applications become possible.
- Improved data analysis capabilities are possible.
- Detection sensitivity is improved by optimising data-acquisition times.
- Source localisation is more effective.
- More robust, transparent and efficient calibration standards can be provided.
- Data security is improved.
- New techniques become available for nuclear safeguards.

Even though list-mode data acquisition based on digital electronics is rapidly increasing in popularity, at present, there are no suitable standards related to list-mode data formats. This is a hindrance to enabling efficient interoperability and the ‘pooling of resources’ to provide a rapid and robust means of analysing list-mode data sets. In our state-of-the-art report we propose a draft list-mode data format for further discussion within the standardisation community.

The need for such standardisation of list-mode data has been recognised by CEN/TC 391, which executes the Commission mandate M/487 to establish European security standards. In their final Phase 2 report addressed to the Commission, CEN/TC 391 assigned a high priority to the standardisation of list-mode data. The RN TG of the ERNCIP launched an initiative in 2014 to develop a standard list-mode digital data format for nuclear instrumentation, under the auspices of the IEC. A second report, entitled 'Critical parameters and performance tests for the evaluation of digital data-acquisition hardware' (Paepen et al., 2014), was produced by the group to support this initiative.

Topic 2 — Remote expert support of field team

Lead Scientist: Harri Toivonen (STUK, Finland)

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. The state-of-the-art report produced by the group on this topic (Toivonen, 2015) identifies that this could be achieved by 'reachback' centres across Europe (built upon existing national facilities and expertise) and would provide analysis services for alarm adjudication. Efficient data sharing and processing across EU Member States requires the use of standard data formats and protocols.

There is a need to improve standardisation at the data management level, requiring a technical standard for data-handling protocols, which may be a non-trivial effort. For spectrometric data, no such protocol has been defined at the international level. The group therefore proposes the use of a database as a basis to develop a European standard for data storage protocols on nuclear and radiological data exchange, particularly with regard to reachback.

National nuclear security regimes involve frontline officers operating detection instruments at borders or other critical sites. Although skilled at the operation of the instruments and procedures for response to a nuclear security event, they are typically non-experts on radiation detection. When an instrument alarm or an information alert is triggered, standard response procedures, including dedicated measurements, may need to be conducted for assessment of the event. The operator or frontline officer may not be able to interpret the results of the instrument, and require timely support from experts, i.e. reachback should be called upon. A reachback system is of vital importance not only for nuclear security, but also improves the effectiveness and efficiency of missions regarding emergency response, nuclear safety, safeguards and environmental monitoring. Technically this is provided remotely via data exchange between frontline officers and off-site experts.

There are two related international standards (based on extensible markup language (XML)) that are intended for data exchange between radiation-detection instruments and analysis software: IEC 62755 and ANSI/IEEE N42.42, but these do not address the benefits associated with modern and powerful data-acquisition methods (i.e. list-mode, see Topic 1). The purpose of standard data formats is to facilitate manufacturer-independent transfer of data and information from radiation-measurement instruments to the analysis resources which could be located on-site or far away in a reachback centre. Complementary to standard data formats, there is a need for standard procedures to handle the information within the formats.

Development of a protocol into a technical standard may be a very large effort, since communication and data-processing systems vary, including computer-security solutions. However, common data structures within data-processing systems would create an ideal prerequisite for efficient and sustainable information sharing, with common data management structures in the form of a standard database which all stakeholders would implement within their jurisdiction.

The database creates a solid foundation for the communication of data, analysis results and advice in various phases of the detection and alarm-adjudication process. All software processes must obey the rules of the database. The advantages of a data-handling protocol, based on a standard database, are as follows.

- Efficient interoperability becomes possible between competent authorities and Member States.
- Data or information provided by the instrument grows to knowledge through expert analysis (via reachback).
- The changes needed to be made in existing data-acquisition systems are minimal.
- Remote-analysis capability may change the way the instruments operate in the future. Instead of local analysis, the data are processed at a remote server and the results are returned in real time via cell (mobile) phone, email or web page.
- A rapid and high-quality response can be achieved with fewer experts.

The open-source database Linssi is used for data storage in many institutions, for example in Canada (HC), Finland (STUK), France (ISRN), Germany (BfS) and Ukraine (SSTC NRS). Linssi implicitly defines a protocol defining data handling, as well as information and knowledge created in various phases of the detection and alarm adjudication processes. All users 'talk' to the database, not to each other. The starting point of the work for defining a common data structure could be the open-source database Linssi. In addition, the new system should be designed to incorporate list-mode data.

Topic 3 — Remote-controlled radiation measurements and sampling using unmanned vehicle

Lead Scientist: Frank Schneider (Fraunhofer Institute, Germany)

The state-of-the-art report produced by the group on this topic (Schneider, 2015) identifies that there are several measurement and sampling scenarios that are too risky for humans to carry out. For these scenarios remote-controlled radiation measurements and sampling using unmanned vehicles need to be developed. Notice that the use of remote-controlled devices, such as unmanned ground vehicles (UGVs) and small-size unmanned aerial vehicles (UAVs), may be more cost effective than the use of manned vehicles or planes. Decontamination of the measurement system and related costs should not be forgotten. Applications envisaged for the remote-controlled measurement and sampling devices are: reactor and other accidents, such as Chernobyl and Fukushima, dirty bombs before and after explosion, CBRN-E crime-scene investigation, search of sources out of regulatory control, as well as long-term measurements.

Lessons learned from incidents such as Fukushima and Chernobyl, as well as decommissioning of old nuclear power plants, show UGVs have some advantages. They can operate in areas with high radiation or danger of explosives (e.g. boiling liquid expanding vapour explosion (BLEVE), collapsing structures, intelligent electronic device, booby trap, heat). Additionally, they have the ability to manipulate the environment and to take potentially heavy samples, as they usually have a high payload. UGVs can also be used for long-time surveying in contaminated areas and monitoring the movements of a threat with real-time data from multiple mobile sensor sources.

It is clear that the remote-controlled radiation measurements and sampling using unmanned vehicles will become a well-established technique in the future. As an example, a standardised capability for UAV-based air sampling from the radioactive release plume would be a tremendous improvement for the emergency preparedness. Such empirical information would be used as input data in atmospheric transport modelling calculations that are an important part of the decision support systems. So, this topic contributes to CIP by enhancing the in-field operation capability. Currently there are no standards related to remote-controlled radiation measurements and sampling using unmanned vehicles. In addition to standards, future research and development around the topic is also called for, see for example Horizon 2020 secure societies FCT-3-2015 call. Studies related to the simultaneous use of several robots with CBRN-E detection payloads are required. One interesting idea is related to the promoting competitions for robots with the CBRN-E payloads.

4.7.5. Expected future focus

The group will continue with the topic of list-mode data format based on digital electronics, although the actual standardisation work will be progressed through other projects. The group will now pave the way for the standardisation of formats and protocols for information sharing regarding nuclear events, in support of reachback. While it is probably still too early to start standardising robot-based RN detection and sampling, the group will aim to increase the interaction of robotics and RN communities and promote further R & D. To achieve these goals, the group intends to develop and promote human/robot RN exercises and competitions, based on the earlier work on scenarios.

4.7.6. References

Paepen, J. et al, *Critical parameters and performance tests for the evaluation of digital data acquisition hardware*, EUR 26976, Luxembourg (Luxembourg): Publications Office of the European Union, 2014, JRC93260.

Peräjärvi, K. et al, *List-mode data acquisition based on digital electronics*, EUR 26715, Luxembourg (Luxembourg): Publications Office of the European Union, 2014, JRC90741.

Schneider, F. et al, *Current state of the art of unmanned systems with potential to be used for radiation measurements and sampling*, EUR 27224, Luxembourg (Luxembourg): Publications Office of the European Union, 2014, JRC95779.

Toivonen, H. et al, *Remote expert support of field teams*, EUR 27099, Luxembourg (Luxembourg): Publications Office of the European Union, 2014, JRC94535.

4.8. Resistance of structures to explosive effects

4.8.1. Purpose

It is important to protect critical buildings (malls, shopping centres, governmental buildings and embassies), infrastructure and utilities, train and subway stations against deliberate acts of terrorism, criminal activity and malicious behaviour. While current regulations and building guidelines do not normally take these threats into account, the introduction of new regulations or guidelines should support the resilience of the buildings and infrastructure against explosive incidents.

Methods are required to quantify the resistance of structural elements against explosive loading, and to assess the hazards resulting from failure of an element. Applicable techniques may be either experimental or numerical simulation methods or a combination of both.

The TG on resistance of structures to explosion effects was therefore formed to bring the required expertise together, in order to define harmonised methods and solutions which can be provided to the decision-makers responsible for CIP.

The goal of the TG is to develop guidelines to harmonise test procedures in the testing of structural elements against explosion induced loads.

4.8.2. General description of the thematic group

In general, the loading characteristics of an external and an internal explosion are quite different and need to be considered separately. The TG therefore focused on testing methods for external detonations.

In the civil security sector only the EN regulations for windows, doors and shutters (EN13123 (1+2) and EN 13124(1+2) are established to certify products with an explosion-resistance class. For other structural building elements no European-wide-accepted regulations are available, although ISO and the International developer of voluntary consensus standards (ASTM) have been published. In addition to the EN regulations, some publicly available specifications (PAS) do consider explosive loading scenarios (e.g. PAS 97 has guidelines on how a valid procedure has to be carried out in order to test a structural element against a certain explosive loading).

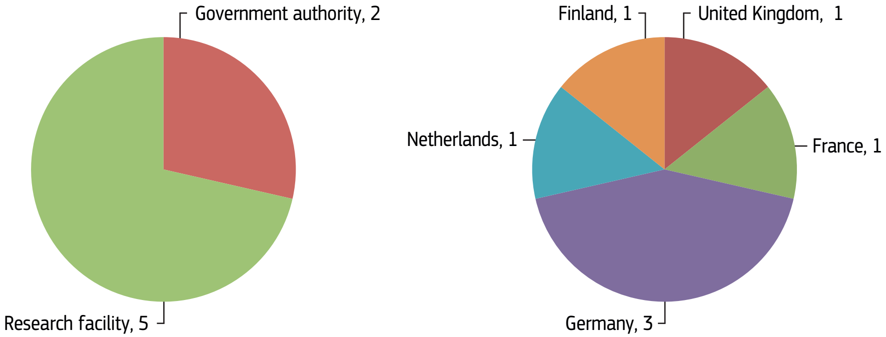
In contrast, the military sector has the North Atlantic Treaty Organisation (NATO) standardisation agreement Stanag 2280 which considers the design threat levels and handover procedures for temporary protective structures. The military also has the International test operation procedures (ITOP), developed by, for use by, the governments or authorised agents/contractor personnel of France, Germany, the United Kingdom, and the United States, i.e. the participants of the four-nation memorandum of understanding (MOU) on mutual acceptance of test and evaluation. Therefore summarising guidelines have been derived for the military sector in which harmonised experimental-test procedures have also been derived. But the experimental-test procedures are related to the military hazards and are not transferred easily to the protection of civil critical infrastructure.

For dynamic numerical simulation test methods in general, no regulations or accepted guidelines have been established. In contrast, the knowledge of valid testing methods to qualify the resistance of build infrastructure against explosive loading cases is embodied by the members of this TG. The members of the TG have significant experience of testing the resistance of structural elements against extraordinary loading, e.g. from impact or explosion. However, as each member's testing facilities uses its own testing methods, there are no harmonised experimental procedures.

Based on the summarised state of play, the overall goal of this TG is to derive a first essential input for a harmonisation of the testing procedures, numerical and experimental, in order to make the results of the testing comparable and reliable within the Europe and available to the stakeholders.

The group was coordinated by Fraunhofer European Monetary Institute (EMI), with the members of the group meeting 13 times between March 2012 and February 2015.

Figure 12: Resistance of structures to explosive effects — Constitution of thematic group organisations in terms of stakeholder group and country



4.8.3. Way of working

The different methods of testing the blast resistance of structural elements has been the main topic of the work carried out by this group, i.e.:

- direct high explosive testing
- shock tube testing
- numerical simulations.

The approach taken was to review these methods when used to test a type of element for which a regulation is available that describes a relevant test procedure. The group therefore decided to review the basic capabilities and limitations of the methods, in relation to their application for structural elements made of glass, assessing the common practices, the gaps, and the scope for improvement.

4.8.4. Results and deliverables 2011-2014

This TG produced three reports:

(1) Review report of testing methods (van Doormaal et al., 2013).

This report explains the experimental methods of testing using high explosives and testing using blast simulators called shock tubes. In addition, 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. Based on this, each method is described together with its requirements, realisation and the related measurement techniques. Furthermore, an interpretation of the measurements is highlighted.

For the numerical simulations, the basic discretisation and calculation schemes are presented in combination with the available constitutive material descriptions for the different significant materials. Finally the chances for verification and validation of the numerical results are presented. Hence the report builds the basis for an actual evaluation of the different test methods and their applicability to certain problems, and provides helpful information for critical infrastructure stakeholders, owners and operators, considering the structural resistance of the infrastructure to the effects of explosion in a comprehensive document.

(2) Numerical simulations for classification of blast loaded laminated glass: possibilities, limitations and recommendations (Stolz, 2014).

The report summarises 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.

(3) A comparison of existing standards for testing blast-resistant glazing and windows (Bedon et al., 2014).

This 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 EN in this area.

The consideration of protective structures aspects is still not mandatory in contrast to the other more common demands on a CI. Furthermore the creation of further regulations and standards is undesirable for the manufactures of protective structure solutions.

However, the work of the TG within the context of the ERNCIP project showed a promising potential to enhance the existing standards in an efficient way so that current shortcomings can be improved.

4.8.5. Expected future focus

In the next phase, the TG will concentrate on the creation of recommendations to modify the existing standards for glazing and windows, and to create new guidelines for the application on facade elements. Furthermore fundamental guidelines for the use of numerical simulation within this context shall be elaborated.

4.8.6. References

Bedon C. et al, *A comparison of existing standards for testing blast-resistant glazing and Windows*, EUR27133, Luxembourg (Luxembourg): Publications Office of the European Union, 2014, JRC94930.

CEN, 2001, EN 13123-1: *Windows, doors and shutters — explosion resistance — requirements and classification — Part 1: Shock tube.*

CEN, 2001, EN 13123-2: *Windows, doors and shutters — explosion resistance — shock-tube requirements and classification — Part 2: Range test.*

CEN, 2001, EN 13124-2: *Windows, doors and shutters — explosion resistance — test method — Part 1: Shock tube.*

CEN, 2001, EN 13124-2: *Windows, doors and shutters — explosion resistance — test method — Part 2: Range test.*

ISO 16934: 2007 *Glass in building — explosion-resistant security glazing — test and classification by shock-tube loading.*

ISO 16933:2007/Cor1:2008 *Glass in building — explosion-resistant security glazing — test and classification for arena air-blast loading.*

GSA-US General Services Administration 2003, *Standard test method for glazing and window systems subject to dynamic overpressure loadings*, GSA-TS01-2003.

Stolz A., *Numerical simulations for classification of blast loaded laminated glass: possibilities, limitations and recommendations*, EUR 27137, Luxembourg (Luxembourg): Publications Office of the European Union, 2014, JRC94928.

Van Doormaal P. et al., *Review report of testing methods*, EUR26449, Luxembourg (Luxembourg): Publications Office of the European Union, 2013, JRC87202.

4.9. Video analytics and surveillance

4.9.1. Purpose

The Group has defined ‘video analytics’ as:

‘The analysis of video content to generate a search index or to provide automatic alerts to specific events or activity, through the categorisation of objects or behaviour appearing in video’.

This technology is currently widely used within governments and industry to assist in the protection of CI. It is extensively used to supplement or replace human guarding in highlighting security threats such as unauthorised perimeter access but also offers advantages across crime detection, prevention and investigation, and can be used in many scenarios such as detecting unusual body or crowd movement and is used extensively in static surveillance.

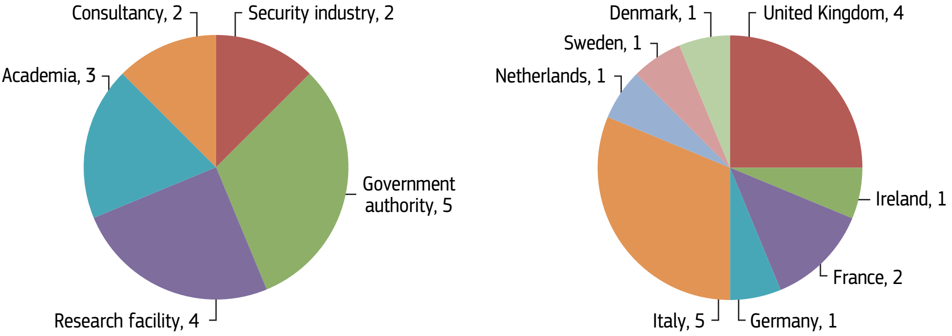
In recent years there has been an inordinate growth in the use and application of video analytics, with academia and industry investing time and effort innovating in the area. Because of the varying needs of the customer (predominately CI sites), there has been a lack of structure and standardisation and little or no accreditation to ensure products are fit for purpose.

This TG for video analytics and surveillance was formed to create the basis of EN for video analytics within the security sector.

4.9.2. General description of the thematic group

The initial group was formed with experts in the use of video technologies for security, drawn from eight European countries, and led by the CAST, the scientific arm of the United Kingdom's Home Office. The group met seven times between November 2012 and February 2015.

Figure 13: Video analytics and surveillance — Constitution of thematic group organisations in terms of stakeholder group and country



The main task of the group was to develop a common approach to the testing and evaluation of video analytics standards for the purposes of security and to encourage the development of innovative technology in this area.

4.9.3. Way of working

The initial approach of this TG was planned around exploring the possibility of using a modified existing national specification as the basis of a new European standard.

Subsequently, it became apparent that a European master set of data that could be accessed by all EU countries for testing could be problematic due to the differing privacy laws in each country.

As there was no consensus within the TG on how to best approach the issue, the group refocused on identifying what harmonisation activities could be feasibly addressed at EU level. An early discovery by the group was that the European Commission framework programme (FP7) was already involved with many projects that impacted directly or indirectly on video analytics. The group decided that a comprehensive list of research projects related to video analytics would be very useful, in order to build on existing work and reduce the risk of duplication.

4.9.4. Expected future focus

This ERNCIP TG will focus on European level issues with the use of video surveillance technologies for security, with the aim of assisting operators of CI to improve their protective security. This will build on the work already started by the group to identify the relevant factors to be considered by users of video analytics, using contemporary use cases for video surveillance and analytics. Potential objectives include the following.

- To determine how EU standards activities could best support user needs for the evaluation of video surveillance systems.
- To produce a guide for end-users of security systems describing the operational requirements for the implementation of video surveillance systems.
- To determine how best to enable collation/common access to data sets in the EU for the testing/evaluation of video surveillance software.

5. ERNCIP looking forward

5.1. Lessons learned from ERNCIP thematic groups

The core activity of the thematic groups (TGs) is to work towards EU-wide harmonisation of testing methodologies for security solutions. The ERNCIP has continuously monitored the effectiveness of its approach of establishing small networks of experts within TGs, operating on a mainly voluntary basis. In 2013, an internal review was completed into the effectiveness of its TG approach. This summarises the initial results of the ERNCIP TGs, describing why they were prioritised, how the work is organised, and summarising the focus and challenges of each TG.

Another ERNCIP review assessed the state of European CIP-related test capabilities. The analysis shows that the issue of testing security solutions at European level is very complex, and particularly problematic because of the lack of harmonised security standards at the European level; if there is no agreed-upon performance standard to test against, it is difficult to agree upon a common test methodology.

This dilemma has affected the nature of the work of some of the ERNCIP TGs, wherein the experts have identified that there is much to be done at European level to analyse gaps, review existing test methodologies, and create good practice guidelines. This has resulted in the wide range of activities across the TAs, as documented in this book.

The strengths of the ERNCIP TG approach include organisational flexibility, a bottom-up approach, availability of a wide pool of experts to undertake small-scale work, and the facilitation of the voluntary participation of experts in a trusted environment.

Paradoxically, these characteristics can also be problematical. Organisational vagueness and a slower speed of delivery can result from the bottom-up approach. As ERNCIP functions through a network of experts and not as a fully-funded research project, there are not the resources for small-scale research or technological development that could help to accomplish some of the required tasks. Also, a common problem has been the lack of commitment which is an inevitable result from reliance on voluntary participation.

One of the requirements of ERNCIP TGs is that they should not duplicate or compete with other networks. This has generally been achieved by the TGs, which are often populated with experts from other networks, projects and initiatives.

For example, the challenge that the ERNCIP AVSEC TG had was to define its role vis-à-vis the ECAC technical task force that had a similar scope, i.e. developing common test methodologies for aviation security solutions. The role identified for the AVSEC TG was to validate the ECAC recommendations.

For the first incarnation of the ERNCIP IACS and SG TG, the challenge was more complex as there are several platforms where issues such as cybersecurity standardisation, common test methodologies and certification schemes are discussed, such as European Network and Information Security Agency (ENISA), senior official group information systems and its mutual-recognition agreement (SOGIS-MRA). The solution was to attempt to align the work plans of this TG with those of ENISA in this area, and to encourage cross-project representation, and information updates.

In the field of the ERNCIP chemical and biological risks to the water sector TG, there existed other projects looking at the same issues, such as the FP7 project SecurEau, which was completed in February 2013. In this case, cooperation with these other projects was specifically identified in the TG's work programme, in order to avoid duplication and to make use of existing expertise.

A more systematic approach for establishing the TAs to be addressed has now been adopted, by ensuring they reflect Commission priorities and that they are aligned with the action plans of the European Commission DGs. All TGs are encouraged to create synergic relations with the key research initiatives in the thematic area, especially past and current FP7 projects, and now with Horizon 2020 projects.

New groups are not initiated until clear objectives are agreed by the experts who have committed to contributing to their achievement. The ERNCIP now exercises greater oversight over the progress of all the TGs, monitoring the status of the planned outputs, and working with the coordinators of the groups to ensure that all participants are actively contributing. Wherever possible, commitment by the key task leaders within all groups is enhanced by use of the limited funding opportunities, and by seeking a clear mandate from their respective organisations for their work within the ERNCIP TGs, especially the coordinators, enabling them to justify the time they need to allocate to ERNCIP. Experience has shown that smaller groups, comprising up to 20 committed members, will achieve more than larger groups, although this does require ERNCIP to guard against the risk that a group is perceived as being a closed shop. Larger groups will have a diverse set of stakeholders, who may have quite different perspectives on the key issues or the direction that should be taken, leading to great difficulty to achieve consensus.

Many TGs have made good use of sub-groups of the members; a small number of experts in a particular topic working together on that topic, who then report on their conclusions to the full plenary of TG members. The work of sub-groups has been efficiently achieved by face-to-face meetings, teleconferencing, or by email.

An issue encountered by some groups was reluctance by end-users, i.e. infrastructure operators, to participate, either in person, or even to respond to surveys, thereby creating a vacuum in terms of user requirements. The ERNCIP responded by creating a trusted forum for infrastructure operators to more efficiently provide guidance, through operator workshops.

The IACS case studies TG showed that agreement can be reached between stakeholders at a European level, even in a highly complex and fast-changing area such as cybersecurity, if the work of the TG is clearly focused from the outset.

The main challenge now is to maximise the value of the results from the TGs, so that tangible benefits are gained, and that the ERNCIP networks are fully connected into the wider developments related to security and testing standards in the EU.

There now exists a valuable pool of expertise in the TGs that could be utilised outside the current ERNCIP framework (for other CIP initiatives, projects, and international cooperation). In addition the ERNCIP office has achieved significant knowledge and established a blueprint for building networks, engaging experts and linking this with DG policies which can be useful in the CIP domain and beyond.

5.2 Lessons learned from the ERNCIP inventory and platform

During the ERNCIP strategy process in 2013 the inventory was assessed in terms of customer value. The following development areas were identified.

- Comprehensiveness: the inventory must be adequately populated with labs to be useful.
- Content development: the inventory should not be merely a database of facilities but should also contain other relevant information for the CIP community e.g. standards, certification requirements, guidelines, CIP events, ERNCIP TG findings, etc. For this purpose the inventory was merged with the ERNCIP web page and the content of the web page was developed content-wise.
- Interactiveness: the inventory should not only be a database/marketing channel but should be developed in terms of interactivity (which is reflected in the name change from ‘inventory’ to ‘platform’). It should be a platform for knowledge exchange, training, discussion, etc. for the CIP community.

The ERNCIP platform was launched in summer 2014 to implement these identified improvements. It has integrated new functionalities to improve synergies among European experimental facilities, manufacturers and CI operators, providing better opportunities to connect through testing standards and guidelines. The second phase of ERNCIP will involve maintenance and further development to support the users of the ERNCIP inventory.

5.3. Future strategy

The ERNCIP project will continue to work towards advancing common technology standards that will improve the protection of CIs in the EU from a wide range of threats (including cyberthreats as well as CBRN-E threats). These technology standards will be in the form of CEN/Cenelec workshop agreements, CEN/Cenelec technical reports and standards, or proposals for international standards, wherever appropriate.

The main tools to be used to achieve this will continue to be the ERNCIP platform and the operation of TGs.

As outlined in section 5.1 ERNCIP is, based on lessons learned, already undertaking activities in order to optimise the delivery of harmonised security-test methodologies within the TGs. Regarding the ERNCIP platform, a number of activities have also been identified to optimise its comprehensiveness, content and interactiveness with the ambition of providing the framework necessary to create a European CIP experimental community and help focus, harmonise and enhance Europe’s overall CIP capabilities.

In addition to contributing to the effectiveness of security technology and the single market for security technology, the ERNCIP project will also indirectly benefit research and innovation within security technology as the TGs in their daily work will inevitably continue to encounter ‘technology gaps’ that correspond to areas in need of research and innovation. Gaps can also be identified by the different advisory bodies of ERNCIP such as the group of EU CIP experts, the academic committee or fora like the ERNCIP conferences or the operator workshops. These bodies and fora together form a ‘gap indication radar’ as they involve relevant stakeholder groups around CIP topics in a structured way.

Likewise, the ERNCIP constitutes in its current shape, a platform for EU foreign cooperation both on a general level (regarding CIP topics) and on thematic level as the TGs constitute natural focal points for the respective areas. Several of the TGs already include non-EU members. The ERNCIP has also developed a strong working relationship with the National Institute of Standards and Technology (NIST), the United States (US) federal technology agency that works with US industry to develop and apply technology, measurements and standards. This cooperation will continue, particularly where TGs identify that international standardisation might be more appropriate for their activity, or where NIST can offer expertise that would benefit the development of EN.

In the future, ERNCIP could provide a platform for EU foreign cooperation, particularly in research technology development (RTD) and training, by extending the framework for participation in ERNCIP TG meetings. Collaborations with the FP7 project 'CIPRNet' (Critical infrastructure preparedness and resilience research network) and with the Horizon 2020 project 'Improver' (Improved risk evaluation and implementation of resilience concepts to critical infrastructure) have been established.

ERNCIP aims to be the reference point for testing evaluation and certification of security solutions in Europe. It will therefore seek to expand its activities to new TAs and more inventory services to cover future EU policy needs, and to strengthen the EU's single market for security products.

5.4. References

Gattinesi, P. and Pursiainen, C., *Erncip Thematic areas: state of the art*, EUR 26017, Luxembourg (Luxembourg): Publications Office of the European Union, 2013, JRC82093.

Gattinesi, P. and Pursiainen, C., *European CIP related testing capabilities: gaps and challenges*, EUR 26229, Luxembourg (Luxembourg): Publications Office of the European Union, 2013, JRC85192.

Appendices

Appendix A — Glossary of terms, abbreviations and acronyms

ANSI	American National Standards Institute
ASTM	International developer of voluntary consensus standards (United States)
AVSEC	aviation security
BfS	German federal office for radiation protection
CAE	French alternative energies and atomic energy commission (French: Commissariat à l'énergie atomique et aux énergies alternatives)
C&C	Compliance and certification
CAST	Centre for Applied Science and Technology
CBRN-E	chemical biological radiological nuclear explosive
CCTV	closed-circuit television
CEN	European Committee for Standardisation (French: Comité européen de normalisation)
Cenelec	European Committee for Electrotechnical Standardisation (French: Comité européen de normalisation électrotechnique)
CI	critical infrastructure
CIIP	critical information infrastructure protection
CIP	critical infrastructure protection
CIPRNet	Critical infrastructure preparedness and resilience research network
CTM	common testing methodology
DG	directorate-general
EC	European Commission
ECAC	European civil aviation conference
EFTA	European Free Trade Association
EMI	European Monetary Institute
EN	European standards
EOS	European Organisation for Security
ENISA	European Union Agency for Network and Information Security
Epcip	European programme for critical infrastructure protection
ERNCIP	European reference network for critical information infrastructure protection
Essence	Easy e-services to shape and empower SME networks in central Europe
ETD	explosive trace detection
ETSI	European Telecommunications Standards Institute

FP7	Seventh framework programme for Research and Technological Development — The European Union's Research and Innovation funding programme for 2007-2013
GIAC	Global information assurance certification
GIS	geographic information system
Horizon 2020	EU framework programme for research and innovation 2014-2020
HC	Health Canada
IACS	industrial automation and control systems
IEC	International electrotechnical commission
IEEE	Institute of electrical and electronics engineers (United States)
Improver project	Improved risk evaluation and implementation of resilience concepts to Critical Infrastructure
IPSC	Institute for the protection and security of the citizen
IRMM	Institute for reference materials and measurements
ISO	International Standards Organisation
ISRN	French institute for radiological protection and nuclear safety
JRC	Joint Research Centre, European Commission
Linssi	structured query language (SQL) database for gamma-ray spectrometry
MSB	Swedish civil contingencies agency
NATO	North Atlantic Treaty Organisation
NEN	Normalisatie en normen (Netherlands national standards institute)
NIST	National institute of standards and technology (United States)
PAS	publically available specification
PoC	point of contact
R & D	research and development
RN	radiological and nuclear
RTD	research technology development
SCADA	supervisory control and data acquisition
SSTC NRS	Ukraine state scientific technical centre on nuclear and radiation safety
Stanag	NATO standardisation agreement
STUK	Finnish radiation and nuclear safety authority
TG	thematic group
UAV	unmanned aerial vehicle
UGV	unmanned ground vehicle

Appendix B — ERNCIP conferences and workshops

B1: The ERNCIP trust conference, 29-30 November 2011

The purpose of the ERNCIP trust conference, which was the first ERNCIP multi-stakeholder event, was to build a common platform of trust within the ERNCIP network which was deemed a crucial building block to be established. The goal was to define trust in the ERNCIP environment. The conference was divided into four sessions, half a day each.

During the first day, experts explained the theory behind the concept of trust and examples were presented of how other complex trust networks had been built. The second day focused on the quantifying and controlling of a trust relationship and ended with issues around quality.

B2: The first ERNCIP conference, 12-13 December 2012

The European Commission JRC held its first ERNCIP conference in Ispra on 12-13 December 2012. Over 100 CIP experts attended the conference, included officials from Member State governments, test laboratories, academic organisations, security product manufacturers and the European Commission.

The conference was organised by the ERNCIP office with the objective of providing a forum for the widest range of ERNCIP stakeholders to meet and exchange information about the current challenges of testing protocols, standardisation, certification and investment issues. All the ERNCIP TAs were presented and discussed, the subjects being as diverse as explosive detection and cybersecurity.

The conference discussions underlined the importance of testing security solutions and offered a number of practical suggestions such as that more testing capabilities should be developed, or that investment is required to improve the lab capabilities and lab availability in the EU.

B3: The first ERNCIP operator workshop, 12-13 September 2013

On 12-13 September 2013, the first ERNCIP operator workshop took place, at Centre Albert Borschette in Brussels, Belgium and was attended by 50 people representing mainly infrastructure operators industry, government bodies, the Commission, laboratories and research facilities.

The workshop was organised in three sessions

Session 1: Risk assessment, protection, and resilience — implications for testing. The moderator for this session was Luigi Rebuffi (European Organisation for Security (EOS)). The session contributed to identifying the risk management needs from the operators' point of view. More specifically, testing and certification is needed not only on a component basis, but also on a systems and subsystems footing. The operators stressed the need for performing exercises to increase preparedness and highlighted the need for scenario building and scenario-based stress tests. From an economic perspective, the operators highlighted the need to avoid wasting resources, by focusing on the essential. A gap identified was the scarce exchange among operators of good practices on how to prevent cyberattacks.

Session 1 presentations included the following.

- From risks assessment to security capabilities: the need for a comprehensive approach. Example for a multimodal hub, by Jean-Luc Planchet, RATP.
- Current EU initiatives — the JRC: GIS by Fabio Lana, JRC.
- ERNCIP TG: Detection equipment materials for operational needs by Pierre Charrue, CEA.
- Building capacities for resilience by Bengt Sundelius, MSB.
- Operator view, aviation by Francis Morgan, Heathrow.
- Critical infrastructure preparedness and resilience research network by Erich Rome, CIPRNet.
- Operator view, energy by Gaetano Condorelli, Enel.
- ERNCIP TG industrial automated control systems and smart grids by Annemarie Zielstra, TNO.
- A manufacturer's perspective by Chris Sandford, Wurldtech.

Session 2: Crisis management and recovery — implications for testing. The moderator for this session was Bengt Sundelius (Swedish civil contingencies agency (MSB), Sweden). This session explored the arrangements that operators need to make in anticipation of serious operational problems, particularly the testing requirements associated with solutions that support crisis management and operational recovery. The presentations and resulting discussions also highlighted the need for communication among relevant parties, both in terms of terminology and connectivity. Further, the need to use forecasting systems, intelligence and maps to improve disaster management was also identified, thus urging the JRC to work towards actions in this direction. Again, the need to consider cybersecurity implications during a crisis was a theme emerging in this session too.

Session 2 presentations included the following.

- Recovery management in practice: The case of a major airport by Rob Peters, Miracle.

- ERNCIP TG: Radiological and nuclear threats to critical infrastructure by Kari Peräjärvi, S.
- Opening of the second day by Naouma Kourti, JRC.
- Overview of selected national (US) and international standards in support of ERNCIP TGs by Bert Coursey, NIST.
- Operator view, Energy by Jan Bucki, ČEZ, a.s.
- ERNCIP TG: Resistance of structures to explosion effects by Alexander Stolz, Fraunhofer.
- Operator view, aviation by Jens Sanner, Frankfurt Airport.
- Current EU initiatives in the field of civil protection by Alexander Kopke, DG Humanitarian Aid and Civil Protection (ECHO).
- Real-time technologies for early contamination warning in water security systems by Andreas Weingartner, S::can.
- Operator view, Water by Michaela Schmitz, BDE.
- ERNCIP TG: Chemical and biological risks in water sector by Philipp. Hohenblum, Austrian Env. Agency.

Session 3: Future technological challenges, needs and solutions. The moderator for this session was Jos Menting. Session 3 focused on the implementation and exploitation of technological solutions and the conditions that contribute to their use by operators, and how to adapt protection and resilience measures to ever evolving threats. Session 3 raised several issues posed in the following questions.

- What new technologies are available out there and how can these be used to fulfil our requirements for protection and resilience?
- How can new technology be deployed in a manner that fulfils requirements on time-to-market and cost efficiency, without jeopardising the need of thorough testing and validation?

Session 3 presentations included the following.

- Innovation in cabin baggage screening process by Wilfried Covent, Brussels Airport.
- ERNCIP TG Aviation security detection equipment by Göran Lövestam, JRC.
- Emerging Technologies for CIP: can they deliver on your requirements? By Marek Rejman-Greene, Home office.
- Possible future steps to increase industrial competitiveness via pan-European tests, validations and certifications by Luigi Rebuffi, EOS.

B4: Second ERNCIP operator workshop, 19-20 May 2014

Moreover, to strengthen its link with the market, a first step was taken by ERNCIP, by organising the ERNCIP operators’ workshop on experimental and test capabilities in the EU with regard to CIP-related security solutions. Building on the success of the first operator workshop in 2013, ERNCIP decided to organise a second operator workshop in 2014, this time in Ispra. The workshop focused on the needs and practices of operators regarding the assessment, selection and deployment of technological security solutions. The workshop gathered 31 professionals representing operators from several sectors like energy, ICT, transport and water.

The workshop was structured into three closely linked sessions during which the operators interacted actively both in the flow of discussions and in the joint work on the questions posed by the three dedicated moderators (one for each session). Each session was centred on a driving question.

Session 1 (moderator: Klaus Keus) focused on the question ‘What are today's challenges for operators regarding assessment, selection and deployment of technological security solutions?’

Session 2 (moderator: Carmine Rizzo) focused on the question ‘What tools are available for operators and how can these be best utilised in order to address the above challenges regarding the assessment, selection and deployment of technological security solutions?’

Session 3 (moderator: Alois Sieber) mapped the topics raised in the previous two sessions against ERNCIP to explore ‘how the ERNCIP network can help to address these challenges on an EU level’.

Based on the feedback from the first workshop the ERNCIP decided to allow more time for discussions and facilitate for discussion on sectoral as well as general level. Therefore the participants were divided into three sectoral working groups each chaired by a rapporteur.

The workshop facilitated the exchange among operators and sectors, and provided guidance for ERNCIP in its efforts to develop and leverage its role for the benefit of operators.

B5: Workshop dedicated to chemical, biological, radiological, nuclear and explosive threats (CBRN-E) 11-12 April 2013.

The European Commission issued a programming mandate addressed to CEN, Cenelec and the European Telecommunications Standards Institute (ETSI) to establish security standards (M487) in February 2011. One of the main aims for this mandate is to facilitate the establishment of a better functioning internal European market for security technologies. The mandate was accepted by the EN organisations, and allocated to CEN/TC 391 'Societal and citizen security' whose secretariat is provided by the Netherlands standardisation institute (NEN).

As the issue of standardisation comes very close to the work of ERNCIP, NEN invited the ERNCIP to participate in the mandate's second phase, where, among other activities, three workshops were organised in order to identify the priority standardisation issues. The ERNCIP hosted the workshop dedicated to chemical, biological, radiological, nuclear and explosive threats (CBRN-E), and the ERNCIP has also been active in the two other selected sectors, namely border control and crisis management.

CEN provided the final report to the Commission in November 2013, proposing lists of prioritised standardisation issues and roadmaps. Many of these standardisation issues cover the same subject areas where the ERNCIP and its TGs are already active. This project proposes the extension of the ERNCIP contribution to the implementation of the M487, by addressing the specific standardisation requirements as identified in M487.

Appendix C — Biographies of contributing authors

Dr-Ing. Alexander Stolz studied civil engineering at University of Wuppertal and wrote his doctoral thesis about mobilisation of bedding stresses in granular soil at the professorship for geotechnique. As head of the department of safety technologies and protective structures he is specialised in the experimental investigation and numerical modelling of materials, components and structures under dynamic loads (also taking into account force-protection engineering). Additionally, he is substantially experienced in the contribution and management of national and European research projects, among which are: the security of bridges and tunnels (Skript), the autonomous risk and information system for structural analysis and monitoring of critical infrastructure (AURIS) and safety and protection of built infrastructure to resist integral threats (Spririt).

Philipp Hohenblum studied chemical engineering at Vienna University of Technology where he graduated in the field of physical chemistry. He has been working at Umweltbundesamt (the environment agency, Austria) since 1998, where he started his career in the environmental testing laboratory and later moved to the surface water department. He has broad experience with pollutants in the environment and their analytical assessment. He led and completed in 2012 the Austrian project Aquasec-AUT, which dealt with the establishment of a national crisis laboratory in case of drinking water incidents. In parallel, he passed a technical expert training course in the frame of the EU Civil Protection Mechanism and is part of the Austrian civil protection expert pool. Mr Hohenblum has been coordinating a thematic expert group within the ERNCIP project since 2012. He is also part of an expert group at the Austrian association for gas and water and author of publications in the field of security.

Dr Kari Peräjärvi graduated with a PhD from the University of Jyväskylä, Finland in 2001. After graduation Kari worked as a postdoctoral fellow at CERN, Geneva (2 years) and Lawrence Berkeley National Laboratory, Berkeley, California (2 years). From the United States he returned to Finland in 2005 to work as a researcher and project coordinator at the Helsinki institute of physics (HIP). The HIP stationed Kari at the University of Jyväskylä from where he moved to the Finnish radiation and nuclear safety authority (STUK) in 2006. At STUK Kari has been working as a scientist and senior scientist. Among other things, the work at STUK has included coordination of R & D projects, supervision of students, participation in operational safety, security and safeguards missions, and expert roles in different committees. In 2007 Kari Peräjärvi became an adjunct professor at the University of Jyväskylä and since 2013 he has been coordinating ERNCIP's radiological and nuclear threats TG.

Dr Göran Lövestam has a Master of Science in applied physics and a PhD in nuclear physics from Lund University in Sweden. He has been engaged as a researcher and research leader in a wide range of scientific areas, including analytical sciences, aerosol physics, isotope geology, microwave technologies, neutron and nuclear physics, nanotechnology, and security detection technologies. Before joining the Commission he was director of the Chalmers Centre for High Speed Technology in Gothenburg, Sweden. He joined the JRC in 2000 as the head of the IRMM Van de Graff accelerator and neutron physics laboratory. In 2009 he was appointed manager of the JRC thematic programme on nanotechnology and in 2011 he took up position as head of the JRC standards for security group, an activity providing technical/scientific policy support on aviation security and CBRN-E threats detection for EC counter terrorism. In 2014 he was appointed JRC chief scientist.

Dr Paul Théron, PhD in computing science from the University of Glasgow, Fellow of the Business Continuity Institute, is Thales communications and security's cyberdefence bids manager and expert on cyber-resilience. He has been a member of ENISA's permanent stakeholders group and, in 2014, he coordinated the JRC's ERNCIP TG on 'Case studies for the cybersecurity of industrial automation and control systems' that published a report on 'A proposal for a European IACS components cybersecurity C&C scheme'. In the 2014-2015 SESAR strategy and management framework study for information cyber-security he was in charge of the cybersecurity threat and vulnerability assessment of the future system wide information management-enabled European air traffic management system, and has contributed to the design of its cybersecurity governance framework. Author of several reports (Information Society and Media DG (now DG Communications Networks, Content and Technology), 2011; ENISA, 2011; ARCEP, 2011) on the resilience of telecommunications, he has co-edited with Sandro Bologna, published by IGI Global, the book 'Critical information infrastructure protection and resilience in the ICT sector' (http://www.igi-global.com/book/critical-information-infrastructure-protection-resilience/70773). He also teaches these matters in universities and takes part in ISO TC 292 standardisation activities.

Dr Sandro Bologna, graduated in physics from Rome University, has 35+ years' experience at the Italian national agency for new technologies, energy and sustainable economic development (ENEA) and abroad, where he has held positions as researcher, head of research units, and head of research projects at national and international levels. Recent main research activities deal with CIP and resilience, with a special emphasis on vulnerability and interdependencies modelling, simulation and analysis. Former president of the Italian association of critical infrastructure experts, at present he is an independent researcher and freelance expert for participation in national and international research projects in the field of CIP and resilience. In the year 2014 he covered the position of deputy chair of the ERNCIP case studies for the cybersecurity of industrial automation and control systems TG.

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).

LB-06-14-182-EN-N

Publications Office

ISBN 978-92-79-44401-2