European Reference Network for Critical Infrastructure Protection: Thematic areas

State of the Art

Peter Gattinesi
Christer Pursiainen

May 2013
CONTENTS

EXECUTIVE SUMMARY .................................................................................................................. 5

1. INTRODUCTION ..................................................................................................................... 7

2. ORGANISATIONAL ASPECTS OF THEMATIC GROUPS .................................................... 10
   2.1 Prioritisation .......................................................................................................................... 10
   2.2 Different levels of maturity .................................................................................................. 13
   2.3 The choice of the coordinator and members ...................................................................... 14
   2.4 Cooperation and overlaps with existing networks .............................................................. 17
   2.5 Financial arrangements ....................................................................................................... 18

3. THE FOCUS OF THEMATIC GROUPS ....................................................................................... 19
   3.1 An all-hazard approach with a focus on malicious threats ............................................. 19
   3.2 General aims and objectives of thematic groups ............................................................... 20
   3.3 Aviation Security Detection Equipment .............................................................................. 21
   3.4 Explosives Detection Equipment (non-Aviation) ............................................................... 22
   3.5 Industrial Automation and Control Systems & Smart Grids ........................................... 24
   3.6 Structural Resistance against Seismic Risks ........................................................................ 26
   3.7 Resistance of Structures against Explosion Effects ........................................................... 27
   3.8 Chemical & Biological Risks to the Water Sector ............................................................... 29
   3.9 Video Analytics and Surveillance ......................................................................................... 31
   3.10 Applied Biometrics for CIP ............................................................................................... 32
   3.11 Radiological and Nuclear Threats to Critical Infrastructure .............................................. 34
   3.12 Conclusions ....................................................................................................................... 35

4. SWOT ANALYSIS OF THE ERNCIP THEMATIC AREAS ................................................. 37
   4.1 Internal strengths .................................................................................................................. 37
   4.2 Internal weaknesses ............................................................................................................. 38
   4.3 External opportunities ......................................................................................................... 39
   4.4 External threats .................................................................................................................... 40
5. RECOMMENDATIONS .................................................................................................................41

5.1 Short-term recommendations (2013-2014) ........................................................................41

5.2 Long-term recommendations (2015-2020) ..........................................................................42
EXECUTIVE SUMMARY

The Institute for the Protection and the Security of the Citizen of the Joint Research Centre of the European Commission set up the European Reference Network for Critical Infrastructure Protection (ERNCIP) project in 2009. This took place under the mandate of the DG HOME, and with the agreement of Member States. The preparatory phase was successfully completed in November 2010. The project started its implementation phase in February 2011, which is due to complete at the end of 2014.

This report reviews the achievements to date in the ERNCIP Thematic Areas, describing why they were prioritised, how the work is organised, and summarising the focus and challenges of each thematic group. The report contains a SWOT-analysis of the current way of organising the work of the thematic groups. The report concludes with recommendations, divided into those applicable in the short term, i.e. to the current ERNCIP period (2013-2014), and those applicable for the longer term for preparing the (possible) next ERNCIP period (2015-2020).

The core activity of ERNCIP and its Thematic Groups is to create harmonised, common test methodologies in the EU for security solutions. Analysis of the thematic area they represent shows that the task is very complex and problematic, particularly because of the lack of harmonised security standards on European level; if there is no agreed-upon performance standard against which one should test, it is difficult to agree upon a common test methodology.

While this dilemma puts some limits to the work of some of the ERNCIP TGs, their work programmes testify that there is still much to be done on gap analyses, comparative reviews of existing test methodologies, and creating good practice guidelines for common testing methodologies.

The SWOT-analysis conclude that the ERNCIP strengths include organisational flexibility, the bottom-up approach, availability of resources to facilitate meetings and small-scale work, and the voluntary participation of experts in this work in a trusted environment.

Paradoxically these characteristics can be ambiguous, with some strengths also being weaknesses. Organisational vagueness and lower speed of delivery can result from the longer time a bottom-up approach can take. As ERNCIP is a network of experts and not a research project, there are not the resources for small-scale research and technological development that could help to accomplish the planned tasks. In some cases, a lack of commitment results from reliance on voluntary participation.
External factors provide opportunities and threats to ERNCIP and its Thematic Groups. There now exists a valuable pool of expertise in the Thematic Groups that could be utilised outside of the current ERNCIP framework (for other CIP initiatives, projects, and international cooperation). The main threat is that the results that the Thematic Groups produce will not become tangible if they are not connected into wider developments related to security and testing standards in the EU.

Short-term recommendations are made on monitoring the deliverables, the use of existing resources, improving the commitment of participants, ensuring the tangibility of the results, and involving all stakeholders. These will enhance ERNCIP without requiring any significant changes to the overall framework.

In the longer term, first, a more systematic basis for prioritisation of the areas and possibly broader functionalities that are covered should be considered. Second, a thorough preparation phase in establishing new Thematic Groups is needed to avoid overlaps and shortening the time needed to define the exact focus of the group. Third, it should be investigated whether and through which mechanisms the Thematic Groups could be provided with such small-scale funding for research and technological development that is justifiable for implementing their objectives. Fourth, commitment should be also enhanced with an arrangement, whereby the work of experts in the ERNCIP Thematic Groups is clearly mandated and empowered by their respective organisations, thus better justifying the time they are allocating to ERNCIP. Fifth, the Thematic Groups should create synergic relations with the main on-going and upcoming policy and research initiatives within the EU context, better involving all relevant European Commission Directorates-General and services. Sixth, from the perspective of efficiency, one should favour smaller groups of up to 20 committed members. Seventh, in order to ensure tangible results there needs to be a clear-cut mechanism for ERNCIP outputs to lead to better European testing standards. Eighth, the opportunities to capitalise on the extensive ERNCIP pool of expertise, in terms of individual experts and their institutions, should be actively sought. Finally, the opportunity for ERNCIP and its Thematic Groups becoming a real focal point for wider international cooperation should be taken.
1. INTRODUCTION

The Institute for the Protection and the Security of the Citizen of the Joint Research Centre of the European Commission set up the European Reference Network for Critical Infrastructure Protection (ERNCIP) project in 2009. This took place under the mandate of the DG Home, in the context of the European Programme for Critical Infrastructure Protection (EPCIP), and with the agreement of Member States. The preparatory phase was successfully completed in November 2010 and the project started its implementation phase in February 2011.

The definition provided for a critical infrastructure within the EPCIP context states that a critical infrastructure “means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.” As with EPCIP, ERNCIP’s general objective is to improve the protection of critical infrastructures in the EU, both national and those defined as European critical infrastructure, in close cooperation with all stakeholders, focusing particularly on the technical protective security solutions.

The specific mission of ERNCIP is to “To foster the emergence of innovative, qualified, efficient and competitive security solutions, through networking of European experimental capabilities”. In order to achieve this, ERNCIP puts its efforts in maintaining an online inventory of experimental capabilities in Europe, and in developing networks of experts to identify and promote good test practices to form the basis of common European testing standards, aiming at harmonisation of test methodologies and test protocols, where practical.

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 critical infrastructures. Secondly, harmonised test protocols are a prerequisite for a mutual acceptance scheme for

---

3 While EPCIP’s scope includes also supporting the protection of national critical infrastructures in wider sense, the EPCIP Directive focuses only on European critical infrastructures and concentrates on the energy and transport sectors, where the “Europeanness” is defined as follows: “‘European critical infrastructure’ or ‘ECI’ means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States.”
security solutions, thus enhancing the development of the European security industry and security market\textsuperscript{4} and related standardisation efforts\textsuperscript{5}.

Testing of security solutions can serve two main purposes:

- Verifying that procurement specifications are met by the security solution
- 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.

Member States have identified some priority CIP testing areas of concern for ERNCIP to address at the EU level. Currently nine ERNCIP Thematic Areas (TAs) cover a wide range of CIP subjects, some sector-specific, while others are cross-cutting.

A TA is dealt with by a Thematic Group (TG) of nominated experts, representing mostly experimental facilities and laboratories but also other stakeholders such as manufacturers and vendors of security solutions, government authorities, academia, and operators of critical infrastructures. Each TG is led by an appointed coordinator, in some cases assisted by one or several deputy coordinators.

Currently, ERNCIP brings together over 180 stakeholders to address the specific problems of each TA from the perspective of testing related security solutions. The aim is not to undertake large-scale Research & Technological Development (RTD) within the TGs, but instead to mobilise the existing knowledge provided by the experts from their work or from other relevant projects, such as EU 7\textsuperscript{th} Framework Programme for Research and Technological Development (FP7) projects.

The day-to-day management of ERNCIP activities is taken care of by the ERNCIP Office, a staff of nine persons located in the JRC. The role of the ERNCIP Office is, inter-alia, to oversee the activities of all of the ERNCIP thematic groups, support the logistics of their membership


\textsuperscript{5} PROGRAMMING MANDATE ADDRESSED TO CEN, CENELEC AND ETSI TO ESTABLISH SECURITY STANDARDS, M/487 EN, Brussels, 17th February 2011, to be found at ftp://ftp.cencenelec.eu/CENELEC/EuropeanMandates/M_487.pdf
recruitment and meetings, and monitor the production of deliverables against TG work programmes.

This state-of-the-art report, prepared by the ERNCIP Office, reviews the achievements to date within the nine ERNCIP TGs, describing how the work is organised and summarising the focus and challenges of each TG. The information provided in this report comes mainly from the work programmes and minutes of the TGs, and other ERNCIP meetings.

While the work programme of each TG focusses on its respective theme, this report makes an effort to systemize the information across the themes in order to identify the common challenges and to draw a comparative picture of the ERNCIP TGs. In so doing, it also assesses the current state of the EU’s capabilities to implement effective security solutions for the protection of critical infrastructure, and puts forward some conclusions and recommendations that can be used in the future work of ERNCIP. Similar reviews on the progress of ERNCIP thematic areas, updating this report, may be undertaken in future years.
2. ORGANISATIONAL ASPECTS OF THEMATIC GROUPS

ERNCIP started with a preparatory phase in 2009-2010, and its initial implementation phase runs from February 2011 till the end of 2014. Although ERNCIP has not yet been authorised to continue beyond 2014, the activities of the TGs are continuous and therefore the TGs have been encouraged to plan their activities beyond 2014 if relevant. This section discusses how the current TAs/TGs came about, and reports the current status of each group from an organisational point of view.

2.1 Prioritisation

While there is no defined maximum number of TAs that ERNCIP could address, it is clear that some prioritisation has to be made, as resources, i.e. time, people and available funding, are limited.

The original concept was that the TAs would mirror the priorities of the Member States. It was agreed with the European Commission (DG HOME) that ERNCIP would identify its priorities by directly addressing the relevant national authorities and other stakeholders in the Member States, as this approach should be more productive by achieving commitment and ownership from Member States.

One of the founding documents, the 2010 *ERNCIP Summary Report*[^6], reports the ERNCIP Task Force organising workshops in May 2010 in four priority areas, as a precursor to identifying the key thematic areas:

- Interdependencies and Experimental Security (jointly with MSB[^7], Sweden)
- Experimental Facilities for Critical Information Infrastructure Protection (CIIP)
- Roadmap for a European Testing, Trialling and Certification Scheme for Explosive Detection
- Intentional Electromagnetic Interference (jointly with CEA[^8], France).

Additionally, the 2010 *ERNCIP State of Play*[^9] reports that during the ERNCIP Task Force’s Member State visits in 2009 and 2010 a number of critical infrastructure sectors were prioritised by the host countries. The infrastructures mentioned most frequently were:

[^6]: Can be found in the ERNCIP Document management system under Preparatory Phase.
[^7]: Swedish Civil Contingencies Agency
[^8]: French Alternative Energies and Atomic Energy Commission
[^9]: Item 3.1.1. Can be found in the ERNCIP Document management system under Preparatory Phase.
• Transportation, including rail, roads, aviation and waterways
• Energy sector, including the services concerning generation, transmission, distribution and storage – in regard to electricity, gas and oil
• Information and communication technologies (ICT), including information systems, e-Government applications, industrial control systems (SCADA), Internet, communications (fixed and mobile) and broadcasting.

The ERNCIP State of Play report also concludes that other sectors, most notably space, water, food, finances, health and government should be considered as particularly critical. Furthermore, the report states that the need for further work related especially to explosives were mentioned during the country visits, and also that control and surveillance systems came up in several occasions.

Following the agreement with the European Commission, the formal prioritisation procedure has largely taken place through the ERNCIP Expert Group (EXG), which is an advisory body created by ERNCIP by invitation to all Member State CIP authorities. On the basis of the common themes identified by the ERNCIP Task Force during their national visits, the 1st ERNCIP Expert Group meeting on 15-16 February, 2010\textsuperscript{10} selected the following for thematic workshops:

• Explosives
• Perimeter defence
• Critical Information Infrastructure Protection (CIIP) including supervisory control and data acquisition. (SCADA)
• Interdependencies
• Electromagnetic interference.

\textsuperscript{10} Minutes can be found in the ERNCIP Document management system under Preparatory Phase.
At the Expert Group meeting on 24 March 2011\(^1\), the participants agreed the priority ERNCIP TAs as:

- Explosives detection in airports
- Explosives detection in other sectors
- Cyber attacks directed towards CIIP and SCADA
- Structural resistance against seismic and explosive
- CBRN, in particular Chemical and Biological risks in the water sector.

This prioritisation was also roughly in line with priorities received from the European Commission. In September 2011, ERNCIP issued a public *Call for an Expression of Interest from EU experimental installations and CIP actors with strong expertise in CIP security*. Beside the above-mentioned five priorities, the Call also mentions two additional TAs:

- Space Security
- Security Scanners.

On the basis of the Expert Group endorsement as well as results of the Call and subsequent consultations, the first six TGs were established (as listed in Table 1), starting their work at the beginning of 2012, with two more TGs subsequently established at the end of 2012. The most recently identified TG organised its first meeting in spring 2013.

One can conclude that while there originally was not any master plan for prioritisation based on any defined CIP priorities and risk assessments of the Member States and the European Commission, a concerted effort was made to collect inputs from the Member States about their interests and priorities. These inputs were reported in the 2010 *ERNCIP State of Play*. In the current set of ERNCIP TAs, most of those priorities have been covered.

\(^1\) Minutes can be found in the ERNCIP Document management system under Preparatory Phase. From March 2011 to March 2013, the following eleven Member States have been actively participating in the Expert Group: Czech Republic, Denmark, France, Germany, Hungary, Italy, The Netherlands, Poland, Romania, Sweden, The United Kingdom. In March 2013, the ERNCIP Office launched a new invitation to the Member States to extend the Member State representation on the Expert Group.
2.2 Different levels of maturity

The current status of the ERNCIP TAs is listed in Table 1. The different life spans explain some of the differences between the TAs in terms of their progress. Also a factor is that the TAs are at different levels – in some fields international or European cooperation already existed, whereas other fields have hitherto been only considered at national level, if at all.

Table 1: Status of ERNCIP TAs/TGs as at May 2013

<table>
<thead>
<tr>
<th>TG</th>
<th>Nr of full TG meetings</th>
<th>First meeting</th>
<th>Nr of subgroup meetings</th>
<th>Status of work programme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aviation Security Detection Equipment (AVSEC)</td>
<td>3</td>
<td>17 Feb 2012</td>
<td>2</td>
<td>Approved in March 2013</td>
</tr>
<tr>
<td>Explosives Detection Equipment (non-Aviation) (DEMON)</td>
<td>4</td>
<td>11 Apr 2012</td>
<td></td>
<td>Approved in February 2013</td>
</tr>
<tr>
<td>Industrial Automation and Control Systems &amp; Smart Grids (IACS&amp;SG)</td>
<td>5</td>
<td>3 Feb 2012</td>
<td></td>
<td>Pending</td>
</tr>
<tr>
<td>Structural Resistance against Seismic Risks (SERIES) FP7 project</td>
<td>1</td>
<td>10 Feb 2012</td>
<td></td>
<td>Based on on-going FP7 project. The TG aims at finalising its ERNCIP-related work programme in the autumn 2013</td>
</tr>
<tr>
<td>Resistance of Structures Against Explosion Effects</td>
<td>5</td>
<td>14 Mar 2012</td>
<td></td>
<td>Approved in February 2013</td>
</tr>
<tr>
<td>Chemical &amp; Biological Risks to the Water Sector</td>
<td>5</td>
<td>16 Apr 2012</td>
<td></td>
<td>Approved in February 2013</td>
</tr>
<tr>
<td>Video Analytics and Surveillance</td>
<td>2</td>
<td>6 Nov 2012</td>
<td></td>
<td>Pending. The TG aims at finalising its work programme by summer 2013.</td>
</tr>
<tr>
<td>Applied Biometrics for CIP</td>
<td>2</td>
<td>10 Dec 2012</td>
<td></td>
<td>Pending. The TG aims at finalising its work programme after the second meeting in the spring 2013.</td>
</tr>
<tr>
<td>Radiological and Nuclear Threats to Critical Infrastructure</td>
<td>1</td>
<td>22-23 April 2013</td>
<td></td>
<td>The TG agreed on the basic elements and text of its work programme in its first meeting in April 2013. It is expected to be finalised and approved by June 2013.</td>
</tr>
</tbody>
</table>

The 2010 ERNCIP Roadmap correctly anticipated that the levels of maturity of expertise in harmonisation of testing would vary between the thematic groups, with the expectation of exchange of good practices between the thematic groups.15

Other possible ERNCIP TAs have also been discussed. In 2012, a Member State proposed a TA on Smart Cities to the Expert Group, although this proposal was later withdrawn. Another

---

12 Some TG have subgroups divided according to tasks or themes. These sub-group meeting numbers refer to formal meetings, however, not necessarily organised and funded by ERNCIP.
13 A meeting in 2012 was one of SERIES own meetings as a FP7 project, where ERNCIP was briefly presented. The meeting on 4 February 2013 was the first one discussing the relationship of ERNCIP and SERIES.
14 Includes two teleconferences.
15 Item 3.2.4. Can be found in the ERNCIP Document management system under Preparatory Phase.
possible TA discussed within ERNCIP in 2012 was Space Security, with a focus on geomagnetic disturbances and their impact on critical infrastructures, especially on global satellite navigation systems and electricity grids, but this proposal has not yet materialised into an ERNCIP TG. It is not now expected that there will be any new TAs identified during the current ERNCIP period (to the end of 2014), as there would be insufficient time for new groups to deliver tangible results in this period.

2.3 The choice of the coordinator and members

One of the features of ERNCIP is that while its TGs share the same basic purpose – harmonising test methodologies and protocols – they are established and organised in a variety of ways. This has been mainly a deliberate approach, aiming at flexibility to reflect the specific challenges of each TA in a bottom-up spirit, especially over the recruitment of coordinators and members.

The TG coordinator is the chairperson of a specific TG. A TG coordinator’s role, responsibilities and commitments are regulated by the ERNCIP TG Membership Agreement, which simply states that the ERNCIP Office appoints the coordinator (following Commission formalities). The coordinator is recognised as a representative of his or her employer, but at the same time being personally nominated by the JRC. There is no standard way to find a coordinator for an ERNCIP TG, and the ERNCIP Office has used different approaches, based on the different characteristics of the TG.

Three of the coordinators (Water, Biometrics, and Video Analytics) were selected on the basis of suggestions from the Member States, either through the Expert Group or the earlier consultation process during national visits. The obvious advantage of this approach is that the coordinator comes with the backing and commitment of the respective Member State to the work of that particular TG. In two cases, the coordinator has been found from within the JRC (AVSEC, SERIES), motivated by the JRC’s own strong interest and expertise in these fields. In three cases (IACS & SG, Explosives Detection Equipment in non-aviation fields, and Structural Resistance against Explosive Effects), the coordinator has been identified through previous cooperation with the JRC, with the role of coordinator directly proposed to these persons and their organisation. This interpersonal approach helped to set up these TGs, and provided a basis for positive expectations. In one case (Radiological threats), a competent organisation was approached at its highest level and asked to nominate the Coordinator. This approach also ensures the commitment of the organisation, and was facilitated by a comparatively small community of competent organisations in this field.

16 Available at the ERNCIP Document management system, Item 2.
In practice, the coordinators have the autonomy to select their members, but are expected to consider suggestions made by the ERNCIP Office, the ERNCIP Expert Group, or other members of the TG. One group (SERIES) is based on existing FP7 project, and has been formed accordingly. All TG membership is subject to final approval from the ERNCIP Office, although to date, the ERNCIP Office has not had cause to veto any proposed TG member. Membership is formalised by organisations and representatives signing the Membership Agreement, which was prepared to testify commitment, establish the basic principles and rules of cooperation, and, not least, to ensure that the members can share information without concern over intellectual property rights or the sensitive character of some issues, thus creating a trusted environment. In practice, it has taken longer for the TG members to sign the Membership Agreement than initially anticipated.

The TGs differ from each other most notably in two respects: number of members and type of organisations involved. The ERNCIP Office has not put any limit as to the number of members. As can be seen in Table 2, two of the TGs (namely IACS & SCADA, AVSEC) consist of dozens of members whereas in some TGs have only a handful of members. When we look at the composition of the members according to the type of organisation, we can identify a similar diversity.

The heterogeneity of the TGs makes it difficult to evaluate their constellation against other TGs. While a smaller and more homogenous group may not be representative, it might be more efficient than a large group in terms of decision making and practical work. Also, it is harder to ensure contributions are made by all members within a larger group.
Table 2: ERNCIP Thematic Groups Membership as at May 2013

| TG                                              | Coordinator organisation | Nr of participating organisations | Nr of participating representatives | Breakdown of organisations, by type | Avio MS, Detection Equipment (AVSEC) | Explosives Detection Equipment (non-Aviation) DEMON | Industrial Automation and Control Systems & Smart Grids (IACS&SG) | Structural Resistance against Seismic Risks (SERIES) | Resistance of Structures Against Explosion Effects | Chemical & Biological Risks to the Water Sector | Video Analytics and Surveillance | Applied Biometrics for CIP | Radiological and Nuclear Threats to Critical Infrastructure | Total Active participants in TGs18 |
|------------------------------------------------|--------------------------|----------------------------------|------------------------------------|-----------------------------------|--------------------------------------|---------------------------------------|-------------------------------------------------|-------------------------------------------------|-------------------------------------------------|---------------------------------|-----------------------------|-----------------------------|---------------------------------|-------------------------------------------------|----------------------------------|
| Aviation Security Detection Equipment (AVSEC)  | JRC, Geel               | 33                               | 53                                 |                                   | Exp 15% 12% 4%                      | Det 12% 9% 4%                        | Operator 24% 27%                         | Manufacturer 33% 24%                      | Government 33% 12%                      | Consultancy 4% 18%                      | Ac 7% 15% 10%                     | Commission 4% 11%                   |                                   |                                   |                                    |
| Explosives Detection Equipment (non-Aviation) DEMON | CEA, FR                  | 11                               | 12                                 |                                   | Exp 37% 9% 2%                      | Det 9% 9% 27%                        | Operator 9%                           | Manufacturer 27% 9%                      | Government 15%                         | Consultancy 15%                      | Ac 6% 15% 10%                     | Commission 6% 11%                   |                                   |                                   |                                    |
| Industrial Automation and Control Systems & Smart Grids (IACS&SG) | TNO, NL             | 34                               | 39                                 |                                   | Exp 17% 17% 12%                    | Det 17% 17% 15%                      | Operator 15%                         | Manufacturer 21% 9%                      | Government 9%                         | Consultancy 15%                      | Ac 9% 12% 11%                     | Commission 12% 10%                  |                                   |                                   |                                    |
| Structural Resistance against Seismic Risks (SERIES) | JRC, Ispra              | 7                                | 7                                  |                                   |                                      |                                      |                                   |                                   |                                   |                                   |                             |                                   |                                   |                                    |
| Resistance of Structures Against Explosion Effects | Fraunhofer, DE         | 8                                | 11                                 |                                   |                                      |                                      |                                   |                                   |                                   |                                   |                             |                                   |                                   |                                    |
| Chemical & Biological Risks to the Water Sector | Austrian Environment Agency, AT | 13                             | 14                                 |                                   |                                      |                                      |                                   |                                   |                                   |                                   |                             |                                   |                                   |                                    |
| Video Analytics and Surveillance | CAST, UK             | 12                               | 19                                 |                                   | Exp 14% 7% 15%                     | Det 7% 50% 12%                       | Operator 7%                         | Manufacturer 50% 15%                     | Government 7%                         | Consultancy 7%                        | Ac 15% 14% 10%                    | Commission 7% 11%                   |                                   |                                    |
| Applied Biometrics for CIP | CAST, UK             | 13                               | 15                                 |                                   |                                      |                                      |                                   |                                   |                                   |                                   |                             |                                   |                                   |                                    |
| Radiological and Nuclear Threats to Critical Infrastructure | STUK, FI            | 7                                | 10                                 |                                   |                                      |                                      |                                   |                                   |                                   |                                   |                             |                                   |                                   |                                    |
| Total Active participants in TGs18 |                                      | 138                              | 180                                |                                   | Exp 30% 9% 12%                     | Det 9% 12% 24%                       | Operator 12%                         | Manufacturer 24% 4%                      | Government 4%                         | Consultancy 10%                       | Ac 11% 10% 11%                    | Commission 11% 11%                  |                                   |                                    |

17 Number of TG members who have participated in at least one meeting.  
18 There are a further 100 stakeholders who registered interest in a TG in 2012, but have yet to participate.
2.4 Cooperation and overlaps with existing networks

One of the requirements of ERNCIP TGs is that they should not duplicate or compete with other networks. This has been generally achieved by the TGs, with the outcomes reflecting the different standings of the TGs in their respective fields, often populated with other networks, projects and initiatives.

For example, the challenge that the ERNCIP AVSEC TG had was to define its role vis-à-vis the European Civil Aviation Conference (ECAC) Technical Task Force that has a similar scope, i.e., developing common test methodologies for aviation security solutions. The role identified for the AVSEC TG is to validate the ECAC recommendations. For the ERNCIP IACS&SG TG, the challenge is more complex as there are several platforms where issues such as cyber security 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), and others. The solution has been to attempt to align the work plans of this TG with ENISA’s in this area, and to encourage cross-project representation, and information updates. In the field of the ERNCIP Chemical & Biological Risks to the Water Sector TG, there exist other projects looking at the same issues, such as the FP7 project SECUREAU, which completed in February 2013. In this case, cooperation with these other projects is specifically identified in the TG’s work programme, in order to avoid duplication and to make use of existing expertise.

In all cases it is expected that the ERNCIP TGs should identify other relevant networks to avoid overlaps, and to seek to establish contact and cooperate with them to create synergic relations with them where relevant. Basically it is about filling in identified gaps and finding the special niche for the TG. However, it is too early to evaluate how successfully ERNCIP TGs have managed to establish their own niches in their field. These aspects will need to be carefully considered when planning future thematic groups for ERNCIP.
2.5 Financial arrangements

ERNCIP funding supports the travel and accommodation costs of external experts participating in pre-approved TG and sub-group meetings. Additionally, the coordinator (or his/her organisation) can be compensated for up to 30 working days annually for pre-approved work on the TG. Each TG can also have a deputy coordinator, subject to JRC approval, who can also be compensated for up to 30 working days annually. In practice, several members could rotate as deputy coordinators, and divide the available funding. However, some TG members have found the system too complicated to be worth applying in practice.

In one TG, it was discussed whether it would be possible to receive funding for “benchmarking”, i.e. conducting the same test in different laboratories with different methods, and comparing the results, thereby obtaining information that would assist the future direction of the TG. It was concluded that while RTD is not in the scope of ERNCIP, benchmarking that would contribute to the project’s goals could be supported according to the EC rules. However, these rules, which require an open procurement process, proved to be too complex for the TG members to consider progressing this option further, which shows a certain weakness in the current capability of the ERNCIP support model to meet the rational and well-founded needs of the TGs.
3. THE FOCUS OF THEMATIC GROUPS

This section starts by briefly describing the threat focus of all TAs, and then considers in detail the scope and achievements of each TG, mainly by analysis of their work programmes and meeting minutes. To systematise this information, each TG is discussed under these common headings:

- Challenge
- Choice of focus
- Methodology
- Main deliverables and timeline.

3.1 An all-hazard approach with a focus on malicious threats

While EPCIP recognises the threat from terrorism as a priority, the protection of critical infrastructure will be based on an all-hazards approach. Similarly, ERNCIP is based on an all-hazards approach, although the types of threats to be considered are left to the TGs themselves, depending on the perceived challenges in their fields (in terms of testing the related security solutions).

The issue of a threat picture was not discussed in detail in the 2010 ERNCIP Roadmap. However, the ERNCIP State of Play report mentions that, even though all the Member States visited have adopted an all-hazards approach, it was clear that most preferred ERNCIP to focus on malicious threats. Few Member States mentioned natural hazards, and even less technological malfunctions, as topics of concern. IT threats are generally understood as being malicious threats. As can be seen in Table 3, despite the all-hazards approach, the ERNCIP TGs have generally defined malicious threats as their main focus.

---

20 Item 3.1.2. Can be found in the ERNCIP Document management system under Preparatory Phase.
Table 3: ERNCIP Thematic Groups – Threat Focus

<table>
<thead>
<tr>
<th>TG</th>
<th>Malicious/terrorist threat</th>
<th>Non-malicious (human error, technological, natural hazard)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aviation Security Detection Equipment (AVSEC)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Explosives Detection Equipment (non-Aviation) (DEMON)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Industrial Automation and Control Systems &amp; Smart Grids (IACS&amp;SG)</td>
<td>Yes</td>
<td>(Partially yes)</td>
</tr>
<tr>
<td>Structural Resistance against Seismic Risks (SERIES)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Resistance of Structures Against Explosion Effects</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Chemical &amp; Biological Risks to the Water Sector</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Video Analytics and Surveillance</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Applied Biometrics for CIP</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Radiological and Nuclear Threats to Critical Infrastructure</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

3.2 General aims and objectives of thematic groups

In September 2011 ERNCIP issued a Call for an Expression of Interest from EU experimental installations and CIP actors with strong expertise in CIP security. The Call sets out the task for each TG to investigate, and to prepare guidelines, proposals and recommendations for the following five goals: 1) Identification of products/solutions, 2) Common test protocols, 3) Metrology, 4) Certification, and 5) Research and investments.

The exact focus of each ERNCIP TG will be presented below. Generally, one can conclude that most of the TGs focus on identification of the current state of the art of testing procedures in order to develop common test protocols, whereas the other goals are less covered in TG activities, particularly the last two.
3.3 Aviation Security Detection Equipment

TG Aviation Security Detection Equipment (AVSEC), coordinated by the JRC, is currently one of the largest TG in ERNCIP, bringing together all types of relevant stakeholder groups. It started in February 2012 and by March 2013 the whole group had met three times. The main form of collaboration is through smaller working groups.

**Challenge**

The European Commission is defining legally binding technical specifications and performance requirement standards for various types of detection equipment used at EU airports. The introduction of eligible instruments and performance standards in EU legislation\(^21\) 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\(^22\) are that there are no standard approval procedures in the EU for aviation detection equipment, with diverse security equipment standards at Member State level.

Consequently, a common EU certification, testing and trialling scheme for aviation security equipment 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 conformity testing is envisaged to be carried out at several accredited test centres in EU Member States, a test centre quality system will be required.

**Choice of focus**

The focus of this TG is 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 and international organisations.

**Methodology**

Close cooperation within the European Commission, between the JRC, DG ENTR, DG HOME and DG MOVE, is essential, and the TG will provide technical/scientific support to the Commission Regulatory Committee on Aviation Security. The work is also aligned to the work programme of the European Civil Aviation Conference (ECAC) Technical Task Force, and the


\(^{22}\) Presentation at ERNCIP Conference December 2012

Rolling Programme annexed to the Cooperation Arrangement between the European Commission and ECAC.

The work of the TG will be undertaken by dedicated working groups, according to the defined work programme, which will be monitored at the TG general meetings.

**Main deliverables and timeline**

The deliverables of this TG will be in the form of a series of reports to be produced during 2013:

- Report on CTM for Security Scanner
- Report on CTM for Explosive Detection System
- Report on CTM for Liquids Explosive Detection System
- Report on Explosives Trace Detection in policy
- Report on inventory of technical specification and detection requirements as well as conformity assessment documents used in the EU for the approval of aviation security detection equipment.

### 3.4 Explosives Detection Equipment (non-Aviation)

TG Explosives Detection Equipment (non-Aviation) (DEMON), coordinated by CEA (France), deals with many similar issues as AVSEC and it has some overlap in membership. However, DEMON has been kept to a small group compared to AVSEC, as this is expected to be the most efficient approach for the context of this thematic area. More operators would have been welcomed, but there was a lack of volunteers. The TG first met in April 2012, and by March 2013 had met three times.

**Challenge**

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 of aviation.
Choice of focus
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. Although definition of a common CTM for non-aviation security would be, at the moment, a too-challenging task for the ERNCIP TG, a common methodology that would evaluate the capabilities of the 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.

Methodology
The first step is the compilation of the operational needs for explosive detection outside the aviation security area. This work will involve end-users (police, customs, transport operators, etc.) and national detection experts. The work already provided in this field by the European Matrix group and the Network on Detection of Explosives will be used as a basis for this compilation. Subsequently, the technical requirements to meet these needs will be identified.

Main deliverables and timeline
During 2013-2014 the TG will produces the following deliverables:

- Intermediate and final reports on non-aviation configurations with requirements for explosives detection
- Intermediate and final reports on how to stimulate development of required detection technologies
- Intermediate and final reports on the elements of a European CTM required to evaluate the general capabilities of detection equipment, and required to validate manufacturers’ performance claims
- State of the Art report on existing regulations in Europe relating to the deployment of explosive detection equipment in non-aviation configurations
- A final report on the recommended initial elements for a European Common Testing Methodology for the capabilities of equipment to detect explosives based on the needs identified in non-aviation sectors.
3.5 Industrial Automation and Control Systems & Smart Grids

TG Industrial Automation and Control Systems & Smart Grids (IACS&SG), coordinated by TNO (The Netherlands), has been one of the pathfinder groups in ERNCIP, being the first to hold a formal thematic group meeting in early February 2012. By March 2013, it has met five times. The group has 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 have been shared in the meetings.

**Challenge**

Information and Communication Technology (ICT) is becoming more and more important in the delivery of essential services. Recent incidents have shown that Industrial Automation and Control Systems (IACS) can be vulnerable to cyber attacks 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 will be a central element. The growing role of ICT in the energy infrastructure requires that cyber security must be taken into account in the development of smart grids from the outset.

**Choice of focus**

The original name for this thematic area was the CIIP and SCADA TA, which covers all types of cyber security. However, the priority was quickly established as being the SCADA elements of IACS and Smart Grids, 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, Smart Grids, 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.

---

**Methodology**

There are many existing and previous activities that cover this thematic area. This was recognised at the outset, with the intention that the TG will take all these initiatives into account and build on the results achieved. Some of the TG members act as links to these other initiatives, which include:

- Previous EU projects such as ESCoRTS, ESTEC and Viking
- EU Expert Group on security and resilience of Information systems and telecommunications networks for Smart Grids
- Task Force for Smart Grids: Expert Group 2 on Data Privacy and Cyber Security
- Mandate 441 to CEN/CENELEC/ETSI on smart metering
- Mandate 490 to CEN/CENELEC/ETSI- SGIS (Smart Grid Information Security)
- ENISA studies on cyber security of IACS and on cyber security of Smart Grids
- EU-US Working Group on Cyber-Security and Cyber-Crime
- EuroSCSIE (SCADA Control Systems Information Exchange)
- The European Smart Metering Industry Group (ESMIG)
- Working groups on security standards, e.g. IEC62443.

Time in all of the TG meetings in 2012 was dedicated to presentations on the outcomes or current status of these initiatives.

In order to analyse and document the current initiatives and identifying gaps, an overall framework was developed by the TG to position the relevant initiatives relating to standards, testing, and certification, cross-matched against the three areas of vulnerability for cyber attacks: People, Organisational, and the Technology. The latter has especially provoked much discussion within the TG as to whether ensuring security testing of the individual technology components is sufficient, and whether security testing of the end-to-end system is practical, given the pace of change in this area.

Early meetings split into two work streams; one for IACS and the other for Smart Grids. However, work is now being progressed by two main tasks; one is assessing what could be done to reduce the vulnerability from the human factors, while the other task is to identify the main issues relating to trusted test centres for IACS and Smart Grids. Two small core groups of members have been established to work on these two tasks in between TG meetings, for results to be presented and further discussed at the next TG meeting.

**Main deliverables and timeline**

A consequence of the wide range of background of the experts has been lack of consensus as to what the priorities of this ERNCIP thematic area should be, which has contributed to the TG’s...
work programme taking longer to define than originally anticipated. The current draft (20 Jan 2013) anticipates the following outcomes:

- Description of the overall landscape on IACS security
- Description of the main issues and challenges with respect to human factors
- Description of the main issues and challenges for trusted test centres for IACS security
- Description of the main issues with respect to testing and certification for IACS
- High level roadmap on IACS security
- Detailed roadmaps for main testing and certification challenges
- Elaboration of testing and certification protocol guidelines.

3.6 Structural Resistance against Seismic Risks

TG Structural Resistance against Seismic Risks has a unique background and status within ERNCIP as it is an existing FP7 Project called SERIES, with a separate budget of over 10 million euro and 23 partners. The approach taken has been to connect SERIES to ERNCIP, while the current SERIES project concludes, with its final conference in May 2013. Subsequently, starting in autumn 2013 ERNCIP will provide the platform for the network of experts to continue with some elements of their work as an ERNCIP TG.

Challenges

The FP7 project has the following objectives:

- Reduce the gap between Europe and the US/Japan in experimental seismic engineering, via integration.
- Bring together European countries with high seismicity but no research infrastructures and those with large infrastructures but low seismicity
- Foster co-operation of all labs and teams active in European earthquake engineering
- Provide access to the most powerful European research infrastructures to researchers from other countries.
- Collaboration of research infrastructures towards new testing technologies.

When SERIES starts to meet within the ERNCIP context, the challenges will remain the same but the focus might be more restricted. The basic elements of the work programme are to be finalised by November 2013.
**Choice of focus/methodology**

SERIES has, in the context of the FP7 project, worked in two directions especially to ensure tangible results:

- Developing a distributed database which includes two categories of existing data:
  - Those from literature (journals and conference proceedings, research reports, personal contacts, etc.)
  - The experimental data residing in individual laboratories in digital, albeit non-structured, form
- Offering, on the basis of open calls and peer review panel selection, an opportunity for European actors to do experimental research and testing in seven world-class research infrastructures with free-of-charge access (funded by the EU), with full infrastructural, logistical, technological & scientific support for seismic testing. 89 organisations from 22 countries have taken this opportunity.

When the FP7 phase of SERIES ends, it is tentatively planned for the ERNCIP TG to continue to maintain the database as well as exchange best practices, but it will not have resources for further RTD. However, the TG could be used as a preparatory phase of a new large-scale RTD project.

**Main deliverables and timeline (as an ERNCIP TG)**

To be defined in the work programme (by November 2013).

### 3.7 Resistance of Structures against Explosion Effects

This small group, coordinated by Fraunhofer (Germany), is one of the first ERNCIP TGs and first met in March 2012. By March 2013, it had met three times and had two teleconferences. The group agreed its basic approach in its first meeting, namely to concentrate on a very specific challenge and then widening the scope subsequently on the basis of this pilot effort. However, agreeing the details of the work programme took some time, with a comprehensive work programme finalised in late 2012.

**Challenge**

The resistance of civil buildings and building elements against explosive effects has only been considered in the last decade and consequently only now being understood by governments and society. For this reason the number of regulations available is very limited. Consequently, there is no harmonised system of testing the elements. The same goes for dynamic numerical test methods where, in general, no regulations or accepted guidelines have been established. While there is much testing experience in individual facilities and laboratories, each facility has its own testing methods, and there are a very limited number of published harmonised experimental procedures.
Choice of focus
The goal of the TG is to develop guidelines to help to harmonise test procedures in the testing of structural elements against explosion-induced loads. In order to be able to deliver tangible results, the TG has limited its scope, motivated by the view that the harmonisation of test protocols should be a step-by-step approach.

First, as the loading characteristics of an external and an internal explosion are quite different and need to be considered separately, the TG will focus on testing methods for only external detonations. Second, the TG will concentrate on far-field blast loading and the specification of the test methods to define the resistance of structural elements against this loading. Third, the plan is to start with an element for which a regulation is available that enables certification products with an explosion resistance class, which in this case is windows and glazing. In a later phase, the same process of harmonising test methodologies and protocols will be applied to other structural elements.

Methodology
The methodology is based on sequential work packages: a) review of existing testing methodologies; b) derivation of common test procedures; c) evaluation of the test procedures; d) preparing guidelines for harmonised testing procedures; and, e) laying the ground for transmitting the results to other elements.

In all the first four phases, the tasks are repeated by comparing and evaluating three different testing methods applicable for blast resistance testing: a) direct high explosive testing, b) shock tube testing, c) and numerical simulations.

Main deliverable(s) and timeline
The work main deliverable will be guidelines to be produced in 2015 (after the end of the current ERNCIP phase), towards which intermediate deliverables are planned as follows:

- Review report on testing methods
- State of the Art report on testing procedures
- Analysis and evaluation of testing procedures
- Guideline document on testing windows and glazed facades against far blast loading
- Subsequent work in 2015 will seek to transfer these guidelines to other building materials.
3.8 Chemical & Biological Risks to the Water Sector

This small TG, led by the Austrian Environment Agency, started its kick-off meeting in April 2012 by discussing a wide range of related issues, with some initial difficulties in identifying the relevant focus. The first meeting decided not to split the TG into chemical and biological subgroups, because an interdisciplinary approach was considered to be a more fruitful approach. The final focus was developed by the end of 2012, resulting in a comprehensive work programme. The TG had by March 2013 met four times.

Challenge

Today, organisational structures and scientific methods provide a high level control mechanism on environmental water bodies and on drinking water. Well-developed European regulatory frameworks also exist to protect environmental water resources from pollution and to guarantee a good chemical and ecological status of environmental water bodies, as well as to set quality standards for drinking water at the tap. These regulations control specific pollutants in order to guarantee safe drinking water.

However, these methods are designed for long-term decision making and generally not for immediate response in case of an incident. Therefore, innovative water quality monitoring systems have been developed in the last couple of years which allow for real-time control of the overall water quality. These systems react to a number of classes of contaminants and immediately warn operators of potential contamination in the network. Classical analytical approaches are then needed to identify and quantify individual chemical or biological contaminants that caused deterioration of water quality.

While several tools have been developed to measure the water quality in the event of an incident, there are several factors which influence the performance of these tools. There is no EU standard approach that sets out parameters for an overall assessment, which would help to avoid false alarms and ensure that the sensors are performing properly. The testing of sensors for drinking water (raw water, blended water etc.) and the conditions for testing are not yet standardised.

Choice of focus

The focus of the TG is harmonising the testing methodologies for innovative real-time alarm systems, which help to prevent or mitigate damage caused by drinking water contamination. This concentrates on three dimensions of incident management:

- There is a need to use innovative techniques (probes, sensors, etc.) and enabling technologies for online measurement of the water quality in drinking water distribution networks. However, there are several factors influencing the performance of these tools
and there is no standard approach available setting out parameters for an overall assessment. The TG aims to deal with this gap.

• After an alarm, a rapid identification and quantification of chemical and biological contaminations in drinking water by means of sophisticated analytical techniques is needed. The TG will compile available screening methods that identify and quantify unknown substances or pathogens in water samples.

• It is important to enhance the engagement and participation of citizens in sharing relevant observations and by feeding their measurements into an appropriate data network, creating a stronger ownership for water quality assessment. The TG will to deal with this aspect of monitoring.

**Methodology**

The methodology to achieve the planned goals consists of preparing six desk reviews and organising three workshops/events.

**Main deliverables and timeline**

The work programme identifies six reports and three workshops/events as the main deliverables during 2013 and 2014:

• Review of sensors to monitor water quality
• Review of monitoring techniques for biological contaminants
• Review of techniques used for biofilm detection
• Alarm System Workshop
• Innovation Boosting Event
• Review of screening techniques and methods for rapid identification and quantification of unknown chemical contaminations
• Review of methods for the rapid identification of pathogens in water samples
• Workshop on collaboration between institutions in ad hoc identification of contaminants in drinking water (emergency laboratory).
3.9 Video Analytics and Surveillance

This TG has decided to explore the opportunities to establish EU-level performance criteria for automated video surveillance systems.

**Challenge**

An automated video surveillance system must be able to show that it can meet the minimum performance levels for the various types of CIP requirements. These systems therefore need to be tested against a set of prescribed operational scenarios. The main challenge will be to define a harmonised set of scenarios.

**Choice of focus**

While the work programme of this TG is still to be developed, the Group is considering the following:

- Establish and progress common standards and methodologies in the field of video analytics and visual surveillance technology across the EU
- Identify and document common requirements for the development of new standards, or extensions for existing standards, to provide clear guidance to the commercial sector across the EU on the gap between operational needs and commercially available technology
- Draw up statements of common Operational Requirements for video surveillance for public safety, crime investigation, and law enforcement, and for the protection of Critical Infrastructure based on the needs of CI operators and end user organisations throughout the EU
- Develop common methods, protocols and approaches to confirm that solutions comply with requirements
- Share information on the development and evaluation of new technologies, processes and solutions for video surveillance for public safety, crime investigation, law enforcement and for the protection of critical infrastructure.

**Methodology**

In the first meeting, the discussion focussed much on the limitations of the group to achieve the above mentioned ambitious goals within the resources and time limits of the ERNCIP TG:

- One suggestion was to focus on one aspect of standardisation (for example information retrieval, metadata standardisation) to see how well and how quickly this could be achieved.
- It was also proposed that the group should more precisely define what a ‘threat’ constitutes in the context of video analytics and surveillance, with a caution that the process to agree on some common scenarios may be lengthy. The i-LIDS scenarios
from CAST (UK) were used as an example of definitions of scenarios but it was widely anticipated that these would not necessarily represent the requirements of all Member States. The coordinator suggested that instead of focusing on creating standards that are scenario specific, the TG could concentrate on standardising the methodology that systems are tested against and therefore working toward the creation of a European-wide benchmark.

- The idea of members of the TG sharing datasets was also discussed, although this might be difficult owing to differing data protection laws in each country
- Metadata standardisation was also raised by a few members, and was universally agreed that this would be useful
- Video content analysis was also an area that members were interested in progressing.

**Main deliverables and timeline**

To be defined in the Work Programme that is planned to be finalised by the summer 2013.

### 3.10 Applied Biometrics for CIP

This TG had its kick-off meeting in December 2012 and has thus not yet finalised its work programme.

**Challenge**

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

- The performance of the underlying biometric system
- The robustness to vulnerabilities such as direct (spoofing) or indirect attacks, and
- 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 USA, and Asia. However, these initiatives are: isolated (focusing only on one or two biometric modalities), disorganised, or limited in time (very few are organising on-going 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).
Choice of focus

Two principle objectives have been identified:

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

During the first meeting, the TG defined its focus more towards standardisation of testing methods, and decided to address the following areas where biometrics has a particular application:

- 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 IT systems)
- Mobile identity checks ('on-the-spot challenge'/virtual zones in restricted areas of operation of critical infrastructures)
- Biometric recognition of individuals from CCTV (link to TG on Video Analytics and Surveillance).

Methodology

The TG has decided to split its work into a number of tasks, organised under two broad work package headings, namely:

- Work on awareness, elicitation of priorities, promotion of appropriate use of biometrics in CIs
- Standardisation, evaluation, testing and certification to meet the requirements of operators of CIs and other stakeholders.

Main deliverables and timeline

While the TG has not yet finalised its work programme it has decided that it will produce the following main deliverables:

- Awareness document
- Analysis of priorities for use of biometrics by operators of CIs, using the awareness document/DVD to help the CI operators understand the opportunities
- New work item proposals to appropriate standardisation bodies for application profiles and testing / certification methodologies specific to the identified applications areas
- Potentially organise or participate in an international Biometrics conference/conference stream related to the above work packages, such as EU-level conference planned for 2013, or with NIST 2014 (USA).
3.11 Radiological and Nuclear Threats to Critical Infrastructure

The coordinator, nominated in November 2012, invited in January 2013 experts representing several relevant stakeholders to take part in the work and around a dozen experts have agreed to contribute to this TG. The first meeting took place in April 2013 and it was already able to agree upon a draft work programme, to be finalised and approved in May 2013.

Challenge/Choice of focus

The TG will focus on the following three current issues in this field:

• List-mode data acquisition based on digital electronics. Time-stamped list-mode data format produces significant added value compared to more conventional spectrum format. It improves source localisation, allows signal-to-noise optimisation, noise filtering, with some new gamma and neutron detectors requiring list-mode to function. List-mode approach also allows precise time synchronisation of multiple detectors enabling, for example, simultaneous singles and coincidence spectrometry such as singles gamma and UV-gated gamma spectrometry.

• Expert support of field teams, i.e. data moves instead of people and samples. Fast and high quality response can be achieved with less people. Optimal formats and protocols for reach-back.

• Remote-controlled radiation measurements and sampling using unmanned vehicles. There are several measurement and sampling scenarios that are too risky for humans to carry out. Applications envisaged are: reactor and other accidents, dirty bombs before and after explosion, search of sources out of regulatory control etc.

Methodology

The basic ways of working include the following elements:

• For each of the above topics, the group has selected a lead scientist.

• Analysis of current state-of-the-art of knowledge and expertise. This will lead to more elaborate conclusions concerning the selected topics and determination of critical parameters related to them (three meetings, one meeting per topic).

• Conclusions on best practices and guidelines on how to test that the systems and instrumentation fulfil the defined critical performance parameters (three meetings, one meeting per topic).

• In addition to active participation in the work during the meetings, the Group members are expected to prepare, on average, one presentation per year to the meetings and also be willing to do some document editing between the meetings.
Main deliverables and timeline

The work programme identifies that two reports will be produced for each of the three elements listed above. The first reports will review the state of the art of the respective fields, while the final reports will define the optimal test methodologies and formats.

3.12 Conclusions

Based on the pattern of findings from across all of the TGs, we are now able to postulate on the tendencies that currently exist relating to security solutions in the EU, and identify some common challenges these raise for the ERNCIP TGs:

Standards. A common feature in all the ERNCIP fields is the lack of agreed-upon security standards on the European level. However, the landscapes of security standards vary depending on the TA. In some TAs there are many national, European or international standards that are at least partially applicable to a security solution (e.g. cyber security), whereas in other fields there are only a few security standards (e.g. structural elements). The general situation is well known, and the current process in the framework of the European Standardisation Organisations (ESOs), that is, CEN, CENELEC and ETSI under M/487, may lead towards more harmonised European security standards.

Test methodologies. To create harmonised, common test methodologies for security solutions is the core activity of ERNCIP and its TGs. The task becomes problematic particularly because of the lack of harmonised security standards; if there is no agreed-upon standard against which one should test, it is difficult to agree upon a common test methodology. Despite this limit to the ERNCIP TGs, the work programmes testify that there is still much to be done. A common starting point is that the testing facilities working in the same field are not necessarily familiar with the test methodologies of each other, and therefore most TGs start by preparing very basic comparative reviews on the test methodologies used by the different facilities across the EU. Among the stakeholders, there is uncertainty as to the value to CIP of testing components/equipment versus testing the whole security system/processes. A related issue is how to test security solutions in their operational environment, which is an issue in some of the TGs (e.g. aviation security). It is a special challenge to test security against malicious threats, as operational environments vary considerably for CI, and malicious actors can easily modify their tactics.
Research and Technological Development (RTD). The ERNCIP TGs are not dealing with RTD as such, but most of them utilise other projects’ results in implementing their tasks. At the same time, the discussions in ERNCIP TGs reveal that there is a continuous need for new RTD projects in the field of security solutions, because both the threat pictures and related technological security solutions are in flux. The challenge is to keep standards and respective testing methodologies apace with this development.

Test infrastructure. All the main European experimental facilities and test laboratories are represented in ERNCIP. However, the full extent of existing security solution testing facilities in Europe is unknown. The ERNCIP Inventory aims at filling in this gap. The issue is whether the EU lacks some critical capability in the field of testing security solutions. However, without having a harmonised system of standards and test methodologies at the European level, it is hard to identify whether there are some obvious gaps in the test infrastructure in the EU.

---

24 ERNCIP Office is currently preparing a report on European experimental and testing capabilities in CIP-related fields. The report is due to be circulated within the ERNCIP community in June 2013 in order to facilitate a wider debate on the capabilities and gaps.
4. **SWOT ANALYSIS OF THE ERNCIP THEMATIC AREAS**

This section provides a short SWOT (strengths, weaknesses, opportunities, threats) analysis of the current approach to organising and running the ERNCIP thematic areas, based on the findings of this state of the art review. As will be seen in the analysis below, some characteristics can be ambiguous, as factors that can be seen as strengths can also in some sense be weaknesses.

**Figure 1: SWOT of the current ERNCIP Thematic Areas/Thematic Groups**

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisational flexibility</td>
<td>Organisational vagueness</td>
</tr>
<tr>
<td>Bottom up approach</td>
<td>Low speed of delivery</td>
</tr>
<tr>
<td>Resources for meetings and small-scale work</td>
<td>Lack of resources for small-scale RTD</td>
</tr>
<tr>
<td>Voluntary participation in a trusted environment</td>
<td>Lack of commitment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opportunities</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool of expertise for other purposes</td>
<td>No impact</td>
</tr>
<tr>
<td>Platform for RTD project development</td>
<td>Overlaps, duplication and unnecessary competition</td>
</tr>
<tr>
<td>Focal point for international cooperation</td>
<td>Support and sponsorship from main stakeholders weakens</td>
</tr>
</tbody>
</table>

4.1 **Internal strengths**

**Organisational flexibility.** The main internal strength of how the ERNCIP TGs are established and managed is flexibility. First, the current way of establishing ERNCIP TGs enables the different needs, views and priorities of the different types of stakeholders to be identified and included in the thematic group. Second, the way of nominating the TG coordinators is also very flexible, enabling the ERNCIP Office to choose the best approach relevant for that TG. Third, flexible and inclusive nomination of potential TG members, which mainly stem from the known contacts of the coordinator and other TG members, rather than formal requests to every Member States for nomination of experts, speeds up the process, with the added benefit of a group formed where some members already have existing relationships.
**Bottom-up approach.** Within the framework of the general ERNCIP goals and objectives, the thematic groups are left to decide their specific challenges themselves. This motivates the members and focuses their work onto the relevant priorities for the specific thematic area.

**Resources for meetings and small-scale work.** ERNCIP can currently offer the TG members some limited financial support that makes it possible to meet, and to do some work between the meetings. Beside travel and accommodation costs related to the TG meetings, ERNCIP may compensate the coordinator 30 working days per annum as well as 30 working days per annum for the Deputy Coordinator. The flexible practice that within a TG this compensation can be shared by several TG members acting as deputy coordinator (e.g. task leaders, report compilers) facilitates the production of deliverables and can help members justify to their home organisations their time spent on ERNCIP.

**Voluntary participation in a trusted environment.** As the participation in the ERNCIP TGs is completely based on voluntary commitment, the structure of the TG gives each member some flexibility to tailor their contribution within the limits of their availability, thereby accommodating different levels of participation. The Membership Agreement sets the legal boundaries in such a way that no-one needs be concerned about intellectual property rights or lack of confidentiality in information exchange.

### 4.2 Internal weaknesses

**Organisational vagueness.** First, even if it reflects the views of Member States (through the ERNCIP Expert Group) and other stakeholders, the prioritisation and establishment process of the TGs is somewhat random, and is not based on any formal consistent risk assessment. Second, the fact that the coordinators are selected in a variety of ways, has led to different form and levels of commitment. Third, due to the absence of strict rules of how to establish a TG, especially in terms of the number of members, the size of the TGs vary considerably, as do their composition, which makes it difficult to compare the TGs. Nevertheless; there are indications that the bigger groups tend to be less efficient in concluding work, and are harder to manage than the smaller groups. Furthermore, due to the lack of clear rules for including or excluding members, the representativeness, neutrality, excellence or other aspects of the group constellation may become compromised. The disparity in the presentation styles of the initial written deliverables now being produced by the thematic groups is also a consequence of the organisational flexibility. Given the high numbers of written ERNCIP reports to be produced in 2013 and 2014, this would benefit from guidance the ERNCIP Office on how the reports are written and disseminated.
Low speed of delivery. As the decision-making on the challenges and objectives of TGs and their work programmes is based on bottom-up philosophy, it can take time and resources for a TG to come into an agreement on a particular issue. In particular, the strength of having a large and heterogeneous group, representing a variety of stakeholders, is also a weakness that can lead to a disproportionately lengthy process to achieve consensus as to the way forward.

Lack of resources for small-scale RTD. The TG members have limited resources (time), if any, to do any background RTD needed to accomplish the TG tasks (e.g. benchmarking tests), and there is little additional support or resource that ERNCIP can offer, in terms of finance, even for small-scale benchmarking tests.

Lack of commitment. A result of voluntary participation can be a lack of motivation and commitment to achieving the objectives of the TG. Occasionally, work task leaders have had to simply abandon their agreed ERNCIP TG tasks after internal reorganisation of their home organisations or after a change of job, which has temporarily paralysed the TG work. In the larger TGs especially, there are members who attend the meetings only rarely and have not committed to do any work for the TG. The difficulty in getting participants to sign the Membership Agreement is a sign of this weakness. Even when a member is fully committed to the TG, their normal work will understandably take precedence over their voluntary contribution to ERNCIP. There are many examples where members have struggled to find the time to produce papers or to review the work of others, despite the previously agreed timetable in the work programme.

4.3 External opportunities

Pool of expertise for other purposes. Having more than 250 nominated experts, from government authorities and regulatory agencies, CI operators, academia, security solution manufacturers and vendors, and experimental facilities and laboratories, the individual members and the institutions represented in the ERNCIP TGs, separately and as a whole, are an important pool of knowledge and expertise that could be used for other EU-level CIP initiatives, including assessment of criticalities and risks to CI. ERNCIP TGs are already connected to other important initiatives, most notably to the work taking place under CEN/CENELEC in the implementation of the second phase of the Mandate M/487 on security standards in the CBRNE fields. The existing ERNCIP TG organisation structure could be used to quickly establish EU-level groups of experts for technical assessments, e.g. for the needs of DG HOME.

Platform for RTD project development. The existing ERNCIP TGs can be used as platforms to generate new RTD projects in their respective fields within the various EU funding programmes, for instance, in the framework of the forthcoming Horizon 2020 and EPCIP funding calls.
**Focal point for international cooperation.** ERNCIP is one of the focal points for EU/US collaboration in CIP-related affairs, which is generally appreciated by ERNCIP stakeholders. ERNCIP can reinforce these relations with the US, and also widen its non-EU cooperation also towards other non-EU countries known for their role in global security industry business, most notably EEA countries, China, Japan, Russia, Israel. ERNCIP could be an attractive focal point for these non-EU actors, as they could reach a large relevant CIP-related experimental and test community through ERNCIP, rather than separately contacting individual institutions in 27 Member States.

4.4 External threats

**No impact.** ERNCIP may not currently be an authoritative enough brand for its TG recommendations to be universally recognised, especially as there is no specific mechanism of how the ERNCIP recommendations and guidelines would be put into practice.

**Overlaps, duplication and unnecessary competition.** Many of the fields that ERNCIP TGs address are also populated by other organisations, networks, projects and initiatives. However, there has not been any systematic mechanism or preparation when establishing a new TA to ensure that any existing networks, working in the same field, are properly identified and consulted. This may lead to unintended consequences: duplication, re-learning the same lessons; turf wars between competing organisations thus wasting effort instead of achieving objectives; unclear leadership in the thematic area without a clear ownership of responsibility resulting in experts being focused on wrong priorities; too many meetings for the experts resulting in information overload; inappropriate decisions or recommendations because of a lack of necessary information and co-ordination.

**Support and sponsorship from main stakeholders weakens.** A threat exists that the ERNCIP TGs will not continue to enjoy sufficient support from the main sponsors and stakeholders. All the TAs should be seen as relevant from the perspective of at least one European Commission DG, and should be supported accordingly. Member States should continue to ensure that the TGs relevant to them are supported by national organisations. The other stakeholders such as manufacturers, vendors, operators and labs will need to feel that the results achieved in the ERNCIP TGs are worth their continued involvement. This commitment from some of these stakeholders may reduce due to external factors.
5. RECOMMENDATIONS

On the basis of the above, it is possible to make some recommendations, based on the premise that the identified strengths should be fully capitalised, weaknesses can be transferred into strengths, opportunities should be utilised and threats should be avoided. These recommendations can be divided into those applicable in the short term, i.e. to the current ERNCIP period (2013-2014) and those that might be concerned with the longer term when preparing the (possible) next ERNCIP period (2015-2020).

5.1 Short-term recommendations (2013-2014)

**Monitoring.** ERNCIP Office should enhance its control over the TGs to ensure that the TGs plan to deliver results in line with ERNCIP aims and objectives, without interfering with the TGs so that the positive effects of flexibility and bottom-up approach are not lost. The recently established TGs should agree on the work programme within six months, i.e., by their second meeting. ERNCIP Office will also need to monitor that the delivery of the outputs of all ERNCIP TGs is in line with their agreed work programme. The initial production of written deliverables by some thematic groups has identified the need for guidance to be provided by the ERNCIP Office to all thematic groups on the presentation of their deliverables. Advice should be given to ensure the full audience for ERNCIP deliverables is carefully considered in respect of how the reports are written and disseminated.

As a mid-term check, ERNCIP Office should organise a two-day workshop at the end of 2013 where the coordinators present their status and completed deliverables to the relevant European Commission DGs, the ERNCIP Expert Group and the ERNCIP Academic Committee.

**Resources.** The lack of resources for small-scale RTD can partially be mitigated in the short term by using the existing funding available for deputy coordinators (30 working days annually) for task leaders, e.g. for literature review or report writing, in line with the agreed TG work programme.

**Commitment.** The lack of commitment of the TG members, where it creates problems, should be avoided by making the participation in the work of a TG, and the respective reimbursement of travels and accommodation, strictly dependent on adherence to the Membership Agreement. This practice could be applied from the second half of 2013 onwards. This practice should not, naturally, become an obstacle to including guest experts to the meetings, when necessary and justifiable. Also every TG member should explicitly be expected to contribute to at least one of the tasks identified in the TG work programme.
**Tangibility.** ERNCIP has now reached the stage where it should provide guidance on how harmonisation of testing methods could be achieved within the EU, that is, how the forthcoming ERNCIP guidelines and identified best practices could be institutionalised at the European level. Contacts and coordination with the European Standardisation Organisations (ESOs) play a crucial role in this.

**Stakeholder involvement.** In order to avoid the threat of fading support from main stakeholders, ERNCIP needs to maintain a clear strategy on engagement and communication with all the stakeholder groups. Relevant European Commission DGs should be consulted regularly about the progress of the ERNCIP TGs. More Member States should be included in the Expert Group in order to give them a possibility to comment the on-going work of the TGs and inform about their own relevant developments. The forthcoming ERNCIP event for CIP operators (planned for 2013) should result into a better understanding of the operators’ standpoints on ERNCIP-relevant issues and this communication should be in some form become regular or perhaps institutionalised. A similar approach could be applied to the security industry even though there are already representatives from manufacturers and vendors in some TGs.

### 5.2 Long-term recommendations (2015-2020)

**Prioritisation.** In deciding the ERNCIP TAs for 2015-2020, prioritisation should be systematically connected to the CIP priorities and risk assessments of the Member States and the European Commission. It should also be considered whether more emphasis is required on broader functionalities and interdependent systems as well as operational environments, not limiting to laboratory testing of individual security solutions.

**Preparation.** A more “tailored” preparation of each ERNCIP TG is needed to ensure that its work will fill in an existing gap that is not yet covered by activities of other actors. The continuation of current ERNCIP TAs/TGs, and establishment of new ones, should not be formalised without having a clear picture about the related networks and initiatives and having agreed with them about the respective roles, division of labour, synergic relations etc. While avoiding overlaps and unnecessary duplication, this preparation would also increase efficiency of the TGs, once established, by clearly pre-defining their focus and tasks.

**Funding.** It should be investigated whether and through which mechanisms ERNCIP could provide to the TGs such funding for RTD and other studies that is justifiable for implementing their objectives. In general, the funding and other resources of ERNCIP should enable laboratories to see ERNCIP as a way to upgrade their capabilities, such as receiving support to obtain accreditation, support for data exchange and training, developing prototypes, or benchmarking tests in order to compare the testing methodologies and results.
Synergies. ENRCIP and its TGs should create synergic relations with the main on-going and upcoming EU CIP policy initiatives and research projects. Relevant European Commission DGs and services that currently are not involved (such as DG ECHO/Civil Protection) need to play a more prominent role as ERNCIP stakeholders. The opportunity to use TGs as platforms for creating relevant RTD projects should be taken.

Commitment. The Membership Agreement and the compensation available for the coordinator and deputy coordinator (in practice task leaders) is not always enough to ensure the necessary level of commitment of coordinators and members of TGs. This should be further ensured by an arrangement, whereby experts’ voluntary work in the ERNCIP TGs is clearly mandated and empowered by their respective organisations, thus better justifying in their organisations the time they are using for ERNCIP.

Efficiency. The efficiency of the TGs can be enhanced by better preparation of the objectives, as previously mentioned, while keeping the flexibility for bottom up approaches. Even short-term TGs (2-3 meetings) should be considered, where a well-defined task has been identified, e.g. test methodology benchmarking for a specific security solution. Another factor is the size of a TG. The current experience favours small TGs of up to 20 committed members. The results of the current ERNCIP TGs need to be monitored to confirm this is correct. In some TAs with larger stakeholder bases, a large membership TG might be justified, although alternatives (workshops, conferences) need to be considered. The evidence so far indicates that smaller groups can more quickly come to an agreement, and use alternative methods, such as teleconferences to work more efficiently.

Tangibility. In order to avoid the “no impact” threat, ERNCIP Office, together with other actors such as ESOs, should propose a mechanism of how ERNCIP recommendations will result in more effective European common test methodologies in practice for CIP security solutions, and how these could lead to better European testing standards.

Uses of expertise. Opportunities to capitalise on the extensive ERNCIP pool of expertise, in terms of individual experts and their institutions, should be actively sought.

International cooperation. Practical opportunities for ERNCIP and its TGs becoming a real focal point for international cooperation should be actively sought.
Abstract

This report reviews the achievements to date in the ERNCIP Thematic Areas, describing why they were prioritised, how the work is organised, and summarising the focus and challenges of each thematic group. The report contains a SWOT-analysis of the current way of organising the work of the thematic groups. The report concludes with recommendations, divided into those applicable in the short term, i.e. to the current ERNCIP period (2013-2014), and those applicable for the longer term for preparing the (possible) next ERNCIP period (2015-2020).
As the Commission’s in-house science service, the Joint Research Centre’s mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

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

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