JRC SCIENCE AND POLICY REPORTS

Technology Certification for Critical Infrastructure Protection

Current Procedures in EU and EEA Member States

Adam M. Lewis

2014

Report EUR 26808 EN

Table of Contents

Summary

Within Europe, there is a very high level of knowledge and experience in product and facility certification necessary or useful for CIP. The European Union New Legislative Framework has helped to drive the development of the sector, because of the important role given to "notified bodies": organisations selected by the Member States to carry out assessments of conformity with harmonized standards. There are many highly-competent certification bodies, including some world-leaders, and accreditation is well-organised through the national accreditation organisations, coordinated by the European cooperation for Accreditation. At the moment, most of this expertise is directed to general security and safety, and business continuity. Relatively little is focused on CIP.

For terrorist threats, the best developed sectors are aviation security and radiation detection. For the former, the Commission is working with ECAC to address the limitations of its current Common Evaluation Process and integrate fully with European aviation security legislation. For the latter, ITRAP+10, a collaborative project with the USA, will present its conclusions shortly. For alarm systems, a basic certification system exists and is under further development.

The IT sector has a well-developed framework for security certification based around ISO standards and European legislation. Although certification to the ISO 27000 series is widely carried out, in the most economically and technologically developed Member States other standards are used as well. Specific ISO and IEC standards exist for industrial control systems and networks. The situation for certification of personnel in IT security is confused, with a number of overlapping and competing standards.

One group of certification bodies with strong and highly-relevant expertise are the classification societies, who have expanded beyond their historic ship-classification role into sectors such as offshore installations, transport infrastructure and information and communication technology.

Audit companies have also started to offer certification services in information security and business continuity. Payments systems are a critical part of the financial infrastructure for which a regulatory regime exists, under the leadership by the Bank for International Settlements. The establishment of a certification process appears to be the natural next step for these systems.

1. Introduction

1.1 Background and Purpose

An overall picture of procedures used within Member States to certify technology relevant to critical infrastructure protection (CIP) was identified by ERNCIP as something which would be useful to help EU institutions and national governments define best practice and plan future policy in this area.

Several earlier studies [1],[2],[3],[4] have drawn attention to the lack of harmonised certification procedures and standards as a contributory factor in the fragmentation of the European security market and this view is taken officially in Commission Communication COM 2012 (417) on Security Industrial Policy.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF

CEN/CENELEC and ETSI received from the European Commission in February 2011 Mandate 487 to establish security standards[5], the work programme for which was to encompass other standardisation deliverables, including specifically test methods and certification requirements.

ERNCIP itself is a direct response to the lack of harmonised EU-wide testing or certification for CIP products and services.

While ERNCIP's primary interest is in the requirements for CIP, it is intended for this work to contribute to the Commission's general efforts to develop a single market for security products and services.

The report is intended to be a living document. It is hoped that it will be updated at least annually. Liberal use has been made of hyperlinks to websites, to help the reader find the latest information.

1.2 Scope and definitions

This report concerns the certification of devices, materials and systems which are, or clearly could be, used for protection of critical infrastructure.

The following definitions are adopted:

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.

Council/Parliament Directive 114/2008 Article 2(a)

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

According to ISO:

Certification is the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements.

Accreditation is the formal recognition by an independent body, generally known as an accreditation body, that a certification body is capable of carrying out certification. Accreditation is not obligatory but it adds another level of confidence, as ‘accredited’ means the certification body has been independently checked to make sure it operates according to international standards.

http://www.iso.org/iso/home/standards/certification.htm

Regulation (EC) No 765/2008 of the European Parliament and of the Council setting out the requirements for accreditation and market surveillance relating to the marketing of products, uses the definitions

Accreditation is an attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity.

A *Conformity assessment body* is a body that performs conformity assessment activities including calibration, testing, certification and inspection;

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:en:PDF

Overall, the concept of accreditation in EU law, although compatible with the ISO definition, is both broader in scope and subject to more stringent requirements. Regulation 765/2008 does not contain a definition of certification and the concept of conformity assessment used in it is broader than certification as defined by ISO.

Certification, in general, is a field of growing importance. ISO has recently published new and updated standards which specify requirements for certification bodies, distinguishing between three types of certification: for products, processes and services; for persons and for management systems. All of these are relevant to critical infrastructure protection.

ISO/IEC 17021:2013 Conformity Assessment - Requirements for Bodies Providing Audit and Certification of Management Systems.

ISO/IEC 17024:2012 Conformity Assessment - General Requirements for Bodies Operating Certification of Persons

ISO/IEC 17065:2012 Conformity Assessment – Requirements for Bodies Certifying Products, Processes and Services
This last was previously covered by ISO Guide 65, the new full standard is therefore an important upgrade.

1.3 Method

The method adopted to construct this report evolved over time as experience was gained. When planning the work, we were aware that some sectors had already been covered. A survey of detection requirements and testing methodologies for aviation security screening devices [6] had been conducted by the ERNCIP Aviation Security Thematic Group, which paid particular attention to certification processes. The European Commission's Directorate-General for Enterprise and Industry has recently launched a public consultation on certification of alarm systems and components. For nuclear and radiation detection equipment, determining the status of certification processes is the subject of ongoing work in the ITRAP+10 project and by the ERNCIP Thematic Group on radiation detection equipment. Those of their results which are currently available are summarised below. Technologies which had not been addressed by the earlier studies were grouped into three themes:

1) Information technology security relevant to critical infrastructure protection
2) Detection, surveillance and identity equipment used to prevent attacks

   on critical infrastructure
3) Special structures and structural materials used to protect critical infrastructure

Three questionnaires were drafted for the three themes above, based very loosely on the model of the questionnaire used for the civil aviation study [6]. These were sent out to the ECIP Contact Points in August 2013, with a reminder in early September. Contact Points of Countries from which no replies had been received at all were telephoned in October and early November.

The two special topics mentioned above, nuclear and radiation detection equipment and alarm systems and components, were excluded from the questionnaires, since information available from the existing sources could be incorporated into the analysis.

The initial response to the questionnaires was slow. Most Member States did not respond at all. In other cases, the Contact Points replied to say that they had written to appropriate bodies but had received no replies. The relevant information therefore would not appear to be immediately known to the Contact Points nor easily available. Nevertheless, the information that had been received from the Member States which replied was a very good starting point from which fruitful web searches could be made.

Three other themes were identified as relevant and included in the discussion.

4) Pressure equipment, machinery, welding and equipment for use in explosive atmospheres
5) Business continuity and risk management
6) Payment systems

The method used by the Aviation Security Thematic Group, of making a statistical analysis on the official responses, was deemed inappropriate because an insufficient number had been received and most of the data had been obtained from other sources.

Since the scope of this present report is wider, the key information is the state of development of certification, sector by sector. The method adopted was therefore to attempt to identify the most important initiatives, the relevant legislation and standards, and as many as possible of the active organisations.

On the basis of this, the largest private sector certification bodies and the classification societies were contacted directly and asked to confirm the information found on their websites, adding anything else they felt relevant.

The information collected was analysed in the light of the earlier general studies and assimilated with available results from the sector-specific studies to derive conclusions.

2. ANALYSIS BY TECHNOLOGY THEME

2.1 Information technology security standards for CIP

Amongst the numerous standards which concern IT security, the most prominent are ISO/IEC 27001, which defines the requirements for information security management systems, ISO 27002, which defines a code of practice, and ISO 15408 which defines evaluation criteria, known as “the Common Criteria”.

Many organisations, both private and public, seek certification to these standards and many bodies offer certification services for them.

Of particular importance for Critical Infrastructure Protection are IT systems used to control large industrial plant. ENISA has published a report “Protecting Industrial Control Systems” [10] which describes this. Two series of standards are of key importance. The IEC 62351 series defines detailed technical specifications for security of supervisory control and data acquisition systems meeting the standards of IEC’s Technical Committee 57. The IEC 62443 series are standards for industrial network security, developed by the Industrial Automation Society. It is now possible to obtain certification to IEC 62443 e.g. from TÜV SÜD (see Section 3.1 below).

2.2 The EU approach to information technology security certification

EU *acquis communautaire* for IT security certification has quite a long history, beginning with Council Decision 92/242/EEC, and Council Recommendation 1995/144/EC.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31992D0242:EN:NOT

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995H0144:EN:NOT

Under this legislation, the Senior Officials Group, Information Systems Security (SOGIS) was established, one of whose responsibilities is to advise the Commission on development of specifications, standardization, evaluation and, specifically, certification in respect of security of information systems.

A subsequent Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security stressed the importance of ISO 15408 and the then ISO 17799, now renumbered as ISO 27002.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002G0216(02):EN:HTML

Today, SOGIS’s functions are to

- Coordinate the standardisation of Common Criteria protection profiles and certification policies between European certification bodies in order to have a common position in the international Common Criteria Recognition Arrangement (CCRA) group.
- Coordinate the development of protection profiles whenever the European Commission launches a directive that should be implemented in national laws as far as IT-security is involved.

See the two related sites www.sogisportal.eu and www.commoncriteriaportal.org for details.

As of June 2011, the national bodies participating in the SOGIS agreement are:

Austria, Bundeskanzleramt
Finland, FICORA - Finnish Communications Regulatory Authority
France, ANSSI - Agence Nationale de la Sécurité des Systèmes d'Information
Germany, BSI - Bundesamt für Sicherheit in der Informationstechnik
Italy, OCSI - Organismo di Certificazione della Sicurezza Informatica
The Netherlands , NLNCSA - Netherlands National Communications Security Agency, Ministry of the Interior and Kingdom Relations
Norway, SERTIT - Norwegian National Security Authority operates the Norwegian Certification Authority for IT Security
Spain, CCN - Centro Criptológico Nacional, Organismo de Certificación de la Seguridad de las Tecnologías de la Información
Sweden, FMV - Försvarets Materielverk
United Kingdom, CESG - Communications-Electronics Security Group

The agreement provides for member nations to participate in two ways, as in the CCRA:

1. As certificate consumers
2. As certificate producers

The current participation status of each of the national bodies is tabulated at: http://www.sogisportal.eu/uk/status_participant_en.html.

For certificate producing nations there are also two levels of recognition within the agreement: certificate recognition up to ISO 15408 Evaluation Assurance Level 4, and certificate recognition at higher levels for defined technical areas when schemes have been approved by the management committee for this level. To date two such technical domains have been addressed:

> Smartcards and Similar Devices - devices where significant portions of the required security functionality depend upon hardware features at chip level. Examples: smart card hardware, smart card composite products, Trusted Platform Modules and digital tachograph cards.
>
> Hardware Devices with Security Boxes - products produced from discrete parts on printed circuit boards whereby significant proportions of the required security functionality depend upon a hardware physical envelope with counter-measures against direct physical attacks. Examples: payment terminals, tachograph vehicle units, smart meters, taxi meters, access control terminals and Hardware Security Modules. At the moment this domain is in use only to support the certification of products evaluated using the SOGIS recommended protection profiles and supporting documents managed by the SOGIS Joint Interpretations Working Group.

SOGIS's Mutual Recognition Agreement of Information Technology Security Evaluation Certificates is one of the most developed agreements of its type and can reasonably be considered a document of reference for the entire European security field, beyond the IT sector alone.

ENISA published the report "Security certification Practice in the EU –Information Security Management Systems – A case study" [12] in October 2013, based on a survey of 11 EU countries. Various approaches to achieving auditable information management security management were delineated and certification bodies for the 11 surveyed countries are listed. The authors lament the absence of reliable statistics on the number of certificates which have been issued. They recommend that best practices are developed for security and for data protection, with a view to avoiding duplication for the two certification areas, and that new initiatives should be linked with existing national accreditation structures. Finally they call for enforcement measures at national level.

2.3 IT Security Professional Certification

Entirely absent from the SOGIS programme at the moment is any initiative on staff certification.

The Barcelona-based Institute for Security and Open Methodologies (www.isecom.org) has developed an open-source IT security methodology and certifies professional staff in several different roles within this scheme, working with training companies in Austria, Germany, Greece, Italy, Spain and Switzerland (and in USA, Canada and Chile).

CESG (www.cesg.gov.uk) operate an Information Assurance certification scheme, which includes certification of competence in various roles at different levels of competence.

They state that their scheme is consistent with ISO17024, but do not advertise any accreditation.

The Agence Nationale de la Sécurité des Systèmes d'Information (http://www.ssi.gouv.fr/fr/anssi/) trains and certify staff as « Expert en sécurité des systèmes d'information », a qualification registered with the French "Répertoire national des certifications professionnelles".

LSTI (www.lsti-certification.fr) is a private company based in Saint Malo which offers personnel certification for auditor and implementer roles in ISO 27001 and ISO 22301 and risk manager in ISO 27005. It is accredited by COFRAC and is a member of the IPC.[1]

The European Information Technologies Certification Institute http://www.eitci.org/ is a Brussels-based non-profit body which offers an e-learning programme in IT security, leading to their own EITC-S certificate. No accreditation is claimed.

European IT professionals may also seek certification via two well-known US programmes. The Certified Information Systems Security Professional (CISSP) certification, is run by the Florida-based International Information Systems Security Certification Consortium (ISC)^2, www.isc2.org which is ISO 17024 accredited by ANSI. The Global Information Assurance Certification (GIAC, www.giac.org) offer professional certification schemes for a number of IT security roles. They have recently added a Global Industrial Cyber Security Professional (GICSP) certification, which is specifically targeted at staff working in critical infrastructure. The ERNCIP Thematic Group on Industrial Automated Control Systems contributed to it. GIAC is an initiative of the privately-owned US SANS Institute and is ISO 17024 accredited by ANSI.

Overall, it appears that IT security professional certification schemes have proliferated so vigorously that a confused landscape of competing, non-complementary certifications has come into being. There are too many types and levels of certification and not enough common agreement and recognition. It remains to be seen whether market forces will drive consolidation.

2.4 Detection Equipment for Civil Aviation Security

The study[6] conducted by the ERNCIP Thematic Group on Detection equipment for Civil Aviation Security in 2012-13, was undertaken to get a better view of the performance requirements and testing methodologies for screening equipment at civil airports employed in the EU and EFTA Member States today, including the process of acquiring equipment.

Security in this sector is very closely regulated, with a dedicated body of European legislation which defines procedural and performance requirements for equipment. The

[1] The International Personnel Certification Association (www.ipcaweb.org) is an industry body which has been established for the entire personnel certification sector. It has, at present, 17 members.

base regulation is Parliament/Council Regulation 300/2008, which defines the common rules and basic standards. Commission Regulation 185/2010 defined the detailed implementation; it has subsequently undergone a number of amendments. Regulation 300/2008 states that measures and procedures which contain sensitive security information should be regarded as EU Classified Information and not published. These take the form of Commission Implementing Decisions, with the sensitive information in annexes which are classified “EU Confidential”.

The latest status of the Aviation Security regulations is published on the Directorate General for Mobility and Transport website aviation security page.

http://ec.europa.eu/transport/modes/air/security/index_en.htm

where may be found a note on the regulatory framework [7] which lists and summarises the legislation in force .

The authors of [6] asserted that implementing the performance standards defined in this legislation requires a harmonised single European conformity assessment mechanism, and the report was conceived as preparation for such a scheme.

A questionnaire was distributed via the Regulatory Committee on Aviation Security to EU and EFTA states' authorities. 27 countries responded, of which 18 have an approval procedure in place for aviation security equipment, regarding threat detection performance, however, only four countries issue product certificates. The most commonly used criterion for obtaining an approval or certificate is that the equipment has successfully passed the European Civil Aviation Conference Common Evaluation Process (ECAC CEP) which currently applies to Explosives Detection Systems, Liquids Explosives Detection Systems and Security Scanners. However**,** four countries require additional criteria based on the ECAC CEP level 2 and 3 test reports, which give detailed data on the test results, and one country is considering doing so. The majority of the countries inform manufacturers and vendors directly or via legal documents on approvals and certifications. Very few however, inform other Member States.

Procurement of equipment for passenger screening check point and hold baggage is typically handled by airports while for in-flight supplies and cargo it is sometimes handled by a regulated agent. The most common requirements for an eligible tender are 'Passed ECAC CEP' and 'Complies with EU Regulation' , which in combination was chosen by 16 respondents. Out of those 16 countries four have additionally ticked 'TSA approved', i.e. certified by the U.S. Transportation Security Administration, and eight 'Used by other Member State(s)'.

In conclusion, the requirements for aviation security equipment are well defined and a widely-recognised evaluation process exists. However, it still falls short of the ideal of a fully harmonised and European-wide certification mechanism, linked with legislation.

2.5 Radiation Detection Equipment

The Illicit Trafficking Radiation Assessment Programme (ITRAP+10) is a joint project between the European Commission (DG Home Affairs) and the US Department of Homeland Security (Domestic Nuclear Detection Office) to carry out an evaluation and comparison of the performance of available radiation detection equipment relevant to nuclear security, develop testing and categorisation procedures and methods to contribute to standardisation/harmonisation processes in the field. The tests are executed by the JRC's Institute for Transuranium elements (ITU) and Savannah River, Pacific Northwest and Oak Ridge National Laboratories in the USA. The types of equipment tested are radiation portal monitors, spectrometric radiation portal monitors, personal radiation detectors, spectrometric personal radiation detectors, radioisotope identifiers, gamma search detectors, neutron search detectors, portable radiation scanners– backpack type and mobile vehicular detection systems. ITRAP+10 is currently in the final reporting phase. It is expected that more information will be made public within the next months. The project is intended to lead to the establishment of an EU certification scheme, an accreditation system for EU laboratories and mandatory certification of instruments. To reach this goal an extension of the project (phase II) has been launched in January 2014; this new phase aims to:

- supplement tests done in the previous phase
- transfer testing know-how to European MS laboratories
- provide feedback to international and European standards
- integrate technologies for RN and explosive detection.

The ERNCIP Thematic Group on radiation threats to CI is focusing on developing a data standard for list-mode radiation detectors i.e. those with digital output, following discussions with the ITRAP+10 management to identify new areas not addressed by the existing project.

For professional staff, the JRC also operates a European Nuclear Security Training centre, intended to be the cornerstone of an EU and international training network aiming to ensure, in the most appropriate way, the transfer and the dissemination of knowledge necessary to spread a worldwide rigorous security culture.

2.6 Detection and Identification Equipment (non-nuclear, non–aviation)

Outside the above two highly security-conscious and highly regulated sectors, things are less developed. Schemes do exist for certain classes of equipment.

CCTV and video technology is well covered by the EN 50132 series of standards. It will be superseded in the near future by the new IEC 62676 suite. The situation for access control systems is similar, with the present EN 50133 series to be replaced by the IEC 60839 series.

Details of both of these may be found at

http://www.cenelec.eu/dyn/www/f?p=104:30:1637711928657846::::FSP_ORG_ID,FSP_LANG_ID:73,25

Certification is offered by e.g. Security systems and Alarms Inspection Board www.ssaib.org and National Standards Authority of Ireland www.nsai.ie .

Advanced CCTV systems are now able which carry out intelligent processing on CCTV to infer useful security information – referred to as video analytics and the subject of another ERNCIP Thematic Group. The UK Home Office Centre for Applied Science and Technology (CAST) has developed a standard called iLIDS for these advanced capabilities, and offers certification to it.

The UK has also developed a national standard for vehicle automatic number plate recognition (ANPR) systems, which must comply with the national ANPR standard if they are to be connected to the national ANPR data centre.

For biometrics, NPL undertake testing of the biometric component of physical access control systems to secure an area within a building against a UK government standard. A revised version of this standard is being considered by the ERNCIP TG on Applied Biometrics for CIP for inclusion in the work programme of the CEN working group TC224 WG18.

One very important gap which has been identified by ERNCIP is that there is no European certification process for the performance of explosive detection equipment in non-aviation contexts, nor are there any known standards to certify to. The ERNCIP DEMON Thematic Group has produced a statement of user needs [13] which spans guidance, training, equipment development, canine capability, and assurance, and considers various categories of infrastructure sites reflecting different detection needs. It may be thought of a first step towards a test, evaluation and certification system.

2.7 Alarm Systems

DG ENTR conducted a public consultation in mid-2013 in which they collected the views and opinions of relevant alarm systems stakeholders on the possibility of creating a harmonised certification procedure for alarm systems and system components at the EU level. At the time of writing, results are being analysed. The main conclusion is that there appears to be support for the establishment of a harmonised certification system for alarm systems among the main stakeholder groups.

The consultation was orientated towards the possibility of proposing “New Approach” legislation for the sector, i.e. with technical requirements defined in harmonised standards and with obligatory conformity assessment performed by “notified bodies”; organisations selected for the task by the Member States and notified to the Commission by them. The findings of the public consultation will be part of the impact assessment report that will accompany a possible Commission legislative proposal in this sector, as foreseen in Communication COM 2012 (417).

Latest information and the public report of the results of the consultation, may be found at http://ec.europa.eu/enterprise/policies/security/industrial-policy/consultation-on-alarm-systems/index_en.htm

2.8 Structures and Structural Material

No system of certification of structures and structural materials specific to critical infrastructure exists in the EU, however, some parts of general legislation and standards for structures and structural materials are relevant.

Council/Parliament Regulation 305/2011 lays down harmonised conditions for the marketing of construction products

It states that “in the absence of objective indications to the contrary, Member States shall presume the declaration of performance drawn up by the manufacturer to be accurate and reliable”. If a new specific procedure for independent certification of key construction products required for critical infrastructure was created, it might require an amendment, depending on whether the use in CIP was considered an “objective indication ”.

Since details are already published on the DG Enterprise website, there was no need to gather the information from the Member States. Questionnaire 3 clarified that it was not the intention to survey all buildings certification but only that relevant to CIP.

The regulation places the onus on manufacturers themselves to guarantee conformity to harmonised standards, indicated by the CE mark. However, verification of constancy of performance must be carried out by a product certification body, notified to the Commission by the Member States. This is ordinarily performed by inspection of the factory and sampling of the product. The regulation allows more than one notified body per Member State

In order to allow a manufacturer of a construction product to draw up a declaration of performance for a construction product which is not covered or not fully covered by a harmonised standard, it is necessary to provide for a European Technical Assessment. This assessment is carried out by Technical Assessment Bodies (TAB’s), notified to the Commission by the Member States and listed on NANDO. The function of the TAB’s is therefore not certification of conformity to an existing standard, but technical assessment where no adequate standard exists.

2.9 Pressure equipment, machinery, welding and equipment for use in explosive atmospheres

The Pressure Equipment Directive 97/23/EC harmonises national laws of Member States regarding the design, manufacture, testing and conformity assessment of pressure equipment and assemblies of pressure equipment. The Directive concerns items such as vessels, pressurised storage containers, heat exchangers, steam generators, boilers, industrial piping, safety devices and pressure accessories. Such pressure equipment is widely used in the process industries, high temperature process industry, energy production and in the supply of utilities, heating, air conditioning and gas storage and transportation. It is therefore relevant to some critical infrastructure. A separate Directive, 2010/35/EU, covers transportable pressure equipment, such as that fitted on road and rail vehicles.

The Simple Pressure Vessels Directive 2009/105/EC covers welded vessels subjected to an internal gauge pressure greater than 0.5bar, intended to contain air or nitrogen and not intended to be fired. Because of its restricted scope, it is less relevant to critical infrastructure protection.

Directive 2006/42/EC on machinery contains provisions regarding safety of equipment and working practices, identification of hazards and risk assessment which are relevant to CIP.

Pipelines and offshore rigs are commonly constructed using welded connections whose reliability depends strongly on the skill of the welder. The European Federation for Welding, Joining and Cutting (EWF) manages a harmonized system for training qualification and certification of welding personnel. It is also responsible for the Certification System of companies using welding. In EWF, 31 European member countries are represented by their national welding societies. See www.ewf.be.

The two ATEX Directives concerning equipment for use in explosive atmospheres are relevant to CIP. Certification is mostly handled by specialist organisations, sometimes part of a large group.

ATEX 95 equipment directive 94/9/EC, Equipment and protective systems intended for use in potentially explosive atmospheres

ATEX 137 workplace directive 99/92/EC, Minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres

2.10 Business Continuity and Risk Management

ISO 22301:2012 defines Business Continuity (BC) as the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident. The standard specifies the requirements of a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents. Certification is widely available and frequently sought by commercial companies.

Critical infrastructure *resilience* is often thought of as a new approach going beyond the established notion of critical infrastructure protection. But it can also be thought of as business continuity on a very large scale.

Traditionally, the term business continuity has mainly been used in for-profit businesses. A key requirement is to maintain profitability in the face of an unexpected disruption. However, the requirements specified in ISO 22301:2012 are generic and intended to be applicable to all organizations regardless of type, size and nature. They do apply directly to many organisations operating critical infrastructure. An analysis of business continuity planning for protection of critical infrastructures, with a particular emphasis on IT and transport, was undertaken by the European project BUCOPCI, funded under the CIPS programme [14].

The Business Continuity Institute www.bci.org operates a system of professional certification but is not independently accredited. It is mainly active in the English-speaking countries, and Switzerland.

Another relevant standard is ISO 31000:2009, Risk management – Principles and guidelines, which provides principles, framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector. ISO states that ISO 31000 cannot be used for certification purposes, but some bodies do offer professional certification schemes for competence in implementing it.

2.11 Payment Systems

Payment systems are one of the most significant critical infrastructure sectors for which certification of security has been, until now, poorly developed. The terrorist attack on the World Trade Center on 11 September 2001 caused significant disruption to the payments system in the US and drew attention to the vulnerability of this type of infrastructure [8]. There is currently a move to close regulation of the security of payment systems, which is likely to drive a large effort in certification.

Eurosystem[2] has stated the need for critical infrastructure protection in its sector as follows. "A series of major incidents and disruptions over the last few years (terrorist attacks, power outages, etc.) has shown to what extent the payments industry is critically dependent on a resilient payment system infrastructure with appropriate operational and communication procedures. The Eurosystem considers that business continuity preparedness is crucial for all financial market participants across Europe due to the existence of common infrastructures and the high degree of interdependencies between them."

The Bank for International Settlements has established 10 Core Principles for Systemically Important Payment Systems (SIPS). In June 2013 the European Central Bank published a proposal for a regulation to implement the Core Principles in the Eurozone.

http://www.ecb.europa.eu/press/pr/date/2013/html/pr130607.en.html

Amongst many other things, this proposal includes the following provisions:

"A SIPS operator shall establish comprehensive physical and information security policies that adequately identify, assess and manage all potential vulnerabilities and threats. It shall review the policies at least annually.

A SIPS operator shall establish a business continuity plan that addresses events posing a significant risk of disrupting the SIPS' operations. The plan shall include the use of a secondary site and be designed to ensure that critical information technology systems can resume operations within two hours of those events. The plan shall be designed in such a way that the SIPS is always able to settle all payments due by the end of the operational day on which the disruption occurs. The SIPS operator shall test the plan and review it at least annually."

[2] Eurosystem consists of the European Central Bank and the central banks of the Eurozone countries.

No explicit requirement for certification is stated.

It must be stressed that the Core Principles are international in scope and apply outside the Eurozone (and outside the EU). See [9] for a description of their implementation in the non-Eurozone UK Clearing House Automated Payment System.

Within the EU, the requirements of Council Parliament Directive 2007/64/EC places some significant demands on payment system infrastructure: all payment orders initiated by the payer should be subject to a maximum one-day execution time and any payment service provider must be able to access the services of technical infrastructures of payment systems.

3. ACCREDITATION AND CERTIFICATION BODIES IN EUROPE

Under Regulation 765/2008 a single accreditation body exists in each EU country, whose task is to monitor the correct operation of conformity assessment bodies, under the coordination of the European cooperation for Accreditation (EA). All Member States, EFTA States and several neighbouring states are represented in EA. The list of EA members may be found on the EA website at http://www.european-accreditation.org/ea-members

Many certification bodies exist in Europe, with different scopes, sizes and geographical range. It must be stressed that these factors do not determine the credibility of a certification body: this is the purpose of accreditation. A smaller or more local certification body may be a legitimate and appropriate choice for a critical infrastructure operator. On the other hand, claims of certification bodies to be accredited should not be believed without verification. See http://www.abcb.org.uk/abcb-news.php for some examples of fraudulent claims and misleading presentation.

Associations of certification bodies have been established in a number of Member States. The European Federation of Associations of Certification Bodies was set up in 2002, currently with membership from Bulgaria, Germany, Greece, Ireland, Italy, Romania, Slovakia and UK.

Listed below are some of the European certification bodies, together with brief descriptions of the services which they offer in areas relevant to Critical Infrastructure Protection. It is not exhaustive, the intention is to give concrete examples of what is available for certification for critical infrastructure protection today in Europe.

The descriptions are based on public information on the internet websites cited.

3.1 Industrial and Product Safety Certification Bodies

The British Standards Institution (BSI) offers product certification services in construction products including safety glass, windows, doors and locks, flood protection and waterproofing products. The BSI kitemark is the most widely-recognised UK product certification marking. BSI also offers management system certification for IT security to ISO 27001 and risk management to ISO 31000, and operates a Security Industry Authority - Approved Contractor Scheme (SIA-ACS). http://www.bsigroup.com/en-GB/

BRE Global offers independent, third-party certification and listing of fire and security products under its Loss Prevention Certification Board (LPCB) brand, its market being architects, specifiers, manufacturers and suppliers. Testing is conducted to international, UK national and LPCB's own standards at their UKAS accredited laboratories, see www.bre-global.co.uk. Their Red Book of approved products is publicly available on-line at http://www.redbooklive.com/ .

DEKRA provides certification services for industry, for materials, systems and personnel. Originally an automotive industry body, based in Stuttgart, it has expanded into other sectors including rail and aviation and has a presence throughout Europe and internationally www.dekra.com.

DQS GmbH are specialists in certification of management systems. They offer information security certification to ISO 27001, information systems management to ISO 20000, business continuity to ISO 22301 and risk management to ISO 31000. http://de.dqs-ul.com/en

Intertek is the world's largest consumer product testing organisation, but also offers a number of infrastructure certification services: building products, cabling, piping, upstream oil and gas, refineries, renewable energy, power generation, food safety to FSSC 20000, IFS, BRC,SQF, GFSI standards. www.intertek.com

The Istituto Certificazione Europea Prodotti Industriali, based in Piacenza, offers certification for the pressure equipment and simple pressure vessels directives, machinery directive, certification of welders, products for explosive atmospheres to ATEX, and verification of electrical earthing, including in the presence of explosive atmospheres. www.icepi.com

The Physikalisch-Technische Bundesanstalt (PTB) is the German national metrology institute. It is responsible for certification of equipment for use in explosive atmospheres (ATEX) www.ptb.de

SIRA Test and Certification Ltd. is a UK-based subsidiary of CSA (see below) which offers ATEX certification for products for use in explosive atmospheres, based on the Dangerous Substances and Explosive Atmospheres Regulations, the UK's framework to facilitate compliance with the European directive. It also offers IECex certification and has recently introduced staff certification for IECex. Their services include training & competence, functional safety, quality assurance, laboratory testing and MCERTS http://www.siracertification.com

SGS, based in Geneva, is the world's largest inspection, testing and verification company, with more than 80 000 employees. Amongst the many certification services that they offer, relevant are: certification of scanners used for border security, certification of pipes, tanks and pressure vessels, rigs, and wind energy projects, welder certification, waste and waste water systems certification and certification of business continuity, risk management and financial systems. They are a notified body for nearly all EU product safety directives. www.sgs.com.

SGS BASEEFA Ltd. is a UK certification body for explosion-protected equipment, which has been a subsidiary of SGS since 2011. In addition to product certification, it also certifies the activities of repair workshops and the competence of personnel working in the explosion-protected field and provides plant inspection and zoning services. http://www.baseefa.com.

The TÜV's (Technischer Überwachungs-Verein) are amongst the best known industrial certification organizations. Originally local bodies devoted to steam boiler inspection, they have merged into five large groups which carry regional names but are international.

TÜV SÜD offer a wide range of infrastructure testing and certification services including for bridges and engineering structures, building systems, cableways, electrical installations, power generation, roads, railways, water and waste water, construction products, products for explosive atmospheres, pipelines, food, security systems, alarm receiving centres and performs penetration testing of communications systems.

TÜV Nord lists certification services in the road, rail, health, food and feed, aviation and oil and gas sectors, including for explosion-protected equipment and machinery.

TÜV Rheinland mentions industrial plant and pressure equipment, explosives products on its site.

SG-TÜV Saarland lists machinery, buildings, pressure equipment, water systems and staff, and IT security to ISO 27001 and the BSI Grundschutz as well as IEC 62433.

TÜV Austria lists food, transport, fire protection and IT systems sectors. The personnel certification division certifies IT managers, food managers, welders, and risk managers.

IQNet - The International Certification Network has been active since 1990, and has almost 40 Partner certification bodies, of whom 17 are EU-based, with more than 200 subsidiaries worldwide. Their website states that each of the partners is a leader in their region and collectively represent the most extensive and reputable network of certification bodies worldwide. The IQNet partners offer certification of railways to the IRIS standard, food system certification to ISO 22000, FSSC 22000, BRC and IFS standards, IT system security to ISO 27001 and business continuity to ISO 22301.

http://www.iqnet-certification.com/index.php

Accredited certification of IT security systems can also be obtained from smaller, specialist organisations. Two examples are:

Bremen-based Datenschutz-cert GmbH offers certification to ISO 27001 and the Common Criteria, accredited by BSI, Bundesnetzagentur and the Deutsche Akkreditierungsstelle. www.datenschutz-cert.de

Dublin-based Certification Europe launched the first accredited certification scheme for information security in Ireland and certified the first organisations in the country to both BS 7799 and ISO 27001. It also offers business continuity certification to ISO 22301.

http://certificationeurope.com/

Finally, it should not be omitted that two large North American certification organizations have a substantial European presence.

Underwriters Laboratories, which has more than 10 000 employees, has branches in 9 EU countries and Switzerland. http://www.ul.com/global/eng/pages/ .

The CSA group, headquartered in Ontario, has subsidiaries in Germany, UK, Netherlands, Italy and Switzerland. www.csagroup.org

3.2 Classification Societies

Classification Societies are bodies which set rules and standards for the design and construction of ships and survey ships to assess compliance. A vessel that has been designed and built to the appropriate rules of a Society may apply for a certificate of classification from that Society. Today, Classification Societies are also able to offer certification of other things as well, including some critical infrastructures. They are a particular strength for Europe, where this type of organisation has a very long history. The following members of the International Association of Classification Societies (IACS www.iacs.org.uk) are European-based. All of them now offer certification services beyond their traditional ship-classification role, including in several sectors relevant to critical infrastructure protection, and are all listed as Notified Bodies for the purpose of specific European regulations and directives.

The certification services of Bureau Veritas's www.bureauveritas.com include government/public sector and construction and buildings. They also offer consultancy for X-ray security inspection devices. Bureau Veritas Certification is the first global independent certification body to receive International Railway Industry Standard accreditation from the Union of the European Railway Industries (UNIFE).

CRS (Croatian Registry of Shipping - Hrvatski Registar Brodovar www.crs.hr) has 50-years experience in the certification of products and a long-term experience in the certification of the safety management system in the marine economy. .

RINA www.rina.org offer certification service in infrastructure and real estate, international funding institutions, transportation, ports and logistics, petroleum, power generation, welfare, manufacturing, food and catering, public administration, security systems to ISO 27001, supply chain security to ISO 28000:2007 and business continuity certification to ISO 22301:2012, and also offer certification of personnel.

DNV GL www.dnvgl.com (formed by the September 2013 merger of Det Norske Veritas and Germanischer Lloyd) certify offshore petroleum installations, pipelines, offshore wind energy, solar systems, biosystems, equipment for use in potentially explosive environments, pressure equipment, electrical and electronic equipment and machinery of almost any description.

Lloyds Register www.lr.org lists certification services in aerospace, automotive, food, “upstream” petroleum, built environment, healthcare and medical, IT and telecommunications, marine and thermal power sectors, covered by its subsidiaries as follows.

Lloyd’s Register LRQA:

ISO 22301 Organisational Resilience (previously BS 25999)
ISO 27001 Information security management
ISO 28000 Supply chain management and ISO 28007 Armed Guarding for Ships
Asset Management under the ISO 55000 series (in your list as Facility certification)
ISO 22000 Food safety (and FSSC 22000, PAS220, HACCP, IFS and BRC)

Lloyd’s Register Energy:

ATEX 95 and 137
ASME boiler codes
Pipeline certification and verification
Pressure Equipment (97/23/EC) and Simple Pressure Vessels (2009/105/EC)

Lloyd’s Register Verification:

Construction Products Regulation (EU 305/2011)

Lloyd’s Register Rail:

Interoperability of European Railway Systems Directive (2008/57/EC)

PRS (Polish Registry of Shipping – Polski Regestr Statków) offers assessment of conformity with Pressure Equipment Directive (97/23/EC), Simple Pressure Vessels Directive (2009/105/EC) and Electromagnetic Compatibility directive (2004/108/WE), certification for Directive 2001/95/EC on general product safety and certification of management systems for conformity with ISO/IEC 27001. PRS also provides certification of quality systems for conformity with ISO 3834-2, -3, -4 (Quality requirements for fusion welding of metallic materials) and certification of Factory Production Control for conformity with the Construction Products Regulation (EU 305/2011) , in the scope of steel and aluminium constructions.

Some classification Societies which are not IACS members do certify relevant products. The Hellenic Register of Shipping is the notified body for pressure equipment and simple pressure vessels.

3.3 Audit companies

The “big four” audit groups (KPMG, PWC, Deloitte and Ernst and Young) have evolved beyond their original accounting role to provide other services, including in information security and business continuity. All offer certification to ISO 27001, except Deloitte which offers preparation and training for it. KPMG also now offer certification to ISO 22301.

Although they are all global organisations, they can be considered another area in which Europe is strong. KPMG is headquartered in Amstelveen, PWC and Deloitte in London, and Ernst and Young’s member company for certification, EY CertifyPoint B.V, is based in Amsterdam.

4. CONCLUSIONS

Many private and public companies, government and quasi-government agencies, industry bodies and standardisation-related non-governmental organisations are able to certify products, systems and staff to standards concerning safety, security and business continuity. It has been possible to identify around 100 in Europe from enquiries to Member State contact points and simple web searches. European legislation and the EU's new legislative framework have helped to drive the growth in certification services. While little of the capability is explicitly dedicated to critical infrastructure protection, much of the know-how is relevant and applicable. To develop a system of certification for critical infrastructure protection, it would therefore be most efficient to build on the existing safety, security and business continuity competence. The organisations mentioned in this report, and others like them, should be considered stakeholders whose views should be solicited when devising a strategy.

5. LIST OF ABBREVIATIONS

("Formerly" indicates that only the acronym is now used.)

ATEX	Appareils destinés à être utilisés en ATmosphères EXplosibles
BAM	Bundesanstalt fuer Materialforschung und -pruefung (German Federal Institute for Materials Research and Testing)
BASEEFA	Formerly British Approval Service for Electrical Equipment in Flammable Atmospheres
BSI	Bundesamt fuer Sicherheit in der Informationstechnik (German Federal Office for Information Security)
BSI	British Standards Institution
CAST	UK Home Office Centre for Applied Science and Technology
CESG	Formerly Communications-Electronics Security Group
CEP	Common Evaluation Process
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
CTM	Common Testing Methodology
DEKRA	Formerly Deutscher Kraftfahrzeug-Überwachungs-Verein
DIN	Deutsches Institut fuer Normung (German Standards Institute)
DNV	Det Norske Veritas
DQS	Formerly Deutsche Gesellschaft zur Zertifizierung von Qualitätssicherungssystemen mbH
DVW	Deutsche Vereinigung fuer Wasserwirtschaft, Abwasser und Abfall (German Association for Water, Wastewater and Waste)
EA	European cooperation for Accreditation
ECAC	European Civil Aviation Conference
ECI	European Critical Infrastructure
EDS	Explosives Detection System
ENISA	European Union for Network and Information Security
ETD	Explosives Trace Detection
EEA	European Economic Area (EU+ Iceland, Lichtenstein and Norway)
EFTA	European Free Trade Association (Iceland, Lichtenstein, Norway and Switzerland)
EFACB	European Federation of Associations of Certification Bodies
ERNCIP	European Reference Network for Critical Infrastructure Protection

GL	Germanischer Lloyd
IPSC	Institute for the Protection and Security of the Citizen
IRMM	Institute for Reference Materials and Measurements
ITRAP	Illicit Trafficking Radiation Assessment Programme
ITU	Institute for Transuranium elements
JRC	European Commission’s Joint Research Centre
NANDO	Notified and Designated Organisations information system
NPL	UK National Physical Laboratory
SOGIS	Senior Officials Group, Information and systems Security
SGS	Formerly Societé Générale de Surveillance
SIRA	Formerly Scientific Instrument Research Association
TÜV	Technische Überwachungsverein
UL	Underwriter’s Laboratories
UKAS	United Kingdom Accreditation Service
VDE	Verband der Elektrotechnik, Elektronik und Informationstechnik (Association for Electrical, Electronic and Information Technologies)
VDI	Verein Deutscher Ingenieure (German Association of Engineers)

6. References

[1] Main Conclusions and Recommendations on the European Security Equipment Market (ESEM) and Executive Summary of the Final Study Report
STACCATO – Stakeholders Platform for Supply Chain Mapping,
Market Condition Analysis and Technologies Opportunities
A study funded by the European Commission in PASR Call 3
September 2008

[2] Study on the Competitiveness of the EU security industry
Final Report for European Commission, DG Enterprise & Industry
ECORYS, DECISION Etudes & Conseil and TNO, Brussels, November 2009
http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item_id=3931

[3] P Myers, F Strebl, A Plecis, R Olivier and P Wästerby
The future of testing security related products
CREATIF Project Report D.5.1, July 2011

[4] P Baker, R Piers, J Rekiel, D Wielenga, J Edwards, I Gomez,
S Rospide, G Briard, T Montoroi, M Klaver, I van de Voorde, T Teichler,
A Gok, A James, A Eriksson, R Warwick, S Mezzadri and R Willems
Security Regulation, Conformity Assessment & Certification
Final Report for European Commission, DG Enterprise & Industry
ECORYS, Brussels, July 2011
http://ec.europa.eu/enterprise/policies/security/files/doc/secerca_final_report_volume__1_main_report_

[5] CEN-CENELEC-ETSI
Mandate M/487 to Establish Security Standards
Final Report Phase 2
Proposed standardization work programmes and road maps
July 2013 Netherlands Standardization Institute, Delft

[6] G Lövestam, S Lehto, J-C Guilpin, S Olivier, J M Peral Pecharromán, J de Ruiter,
R Weinzierl, B Wong, A Żukowski
Detection Requirements and Testing Methodologies for Aviation Security Screening Devices in the EU and EFTA Draft 0.2 March 2013

[7] Marc Thomas
Notes on The EU Regulatory Framework Applicable to Civil Aviation Security
European Commission Directorate-General for Internal Policies
May 2013 PE 495.860
http://ec.europa.eu/transport/modes/air/security/index_en.htm

[8] R B Johnston and O M Nedelescu
The Impact of Terrorism on Financial Markets
IMF Working Paper 2005

[9] IMF Country Report No. 11/237
United Kingdom: Observance by CHAPS of CPSS Core Principles for Systemically Important Payment Systems. Detailed Assessment of Observance
International Monetary Fund July 2011

[10] Protecting Industrial Control Systems: Recommendations for Europe and Member States, Annex III
European Network and Information Security Agency (ENISA), 2011

[11] Appropriate security measures for smart grids: Guidelines to assess the sophistication of security measures implementation
European Network and Information Security Agency (ENISA), 2012
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services

[12] Security certification practice in the EU
Information Security Management Systems – A case study
Version 1, October 2013
European Network and Information Security Agency (ENISA), 2013

[13] Statement of User Needs Final Report
Detection of Explosive Materials for Operational Needs (DEMON) Group
Explosives detection in other (non-aviation) sectors
ERNCIP Office, 2013. Limited Distribution

[14] Business Continuity Planning for Protection of Critical Infrastructures BUCOPCI
Fund CIPS, Topic CIP, 13/07/2011 - 12/07/2013
Project Coordinator Isdefe - Systems Engineering for the Defence of Spain http://www.bucopci.eu/

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Adam Lewis
Address: Joint Research Centre, TP 720 Via E. Fermi 2749, Ispra (VA) 21027 Italy
E-mail: adam.lewis@jrc.ec.europa.eu
Tel.: +39 0332 785786

https://ec.europa.eu/jrc

Legal Notice
This publication is a Science and Policy Report by the Joint Research Centre, the European Commission’s in-house science service. It aims to provide evidence-based scientific support to the European policy-making process. The opinions expressed do not imply a policy position of the European Commission. Descriptions of services offered by other organisations are for illustrative purposes only and do not represent an endorsement by the JRC or by the Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication

JRC90412

EUR 26808 EN

doi:10.2788/11691

Abstract
Within Europe, there is a very high level of knowledge and experience in product and facility certification necessary or useful for CIP. The European Union New Legislative Framework has helped to drive the development of the sector, because of the important role given to ”notified bodies”: organisations selected by the Member States to carry out assessments of conformity with harmonized standards. There are many highly-competent certification bodies, including some world-leaders, and accreditation is well-organised through the national accreditation organisations, coordinated by the European cooperation for Accreditation. At the moment, most of this expertise is directed to general security and safety and business continuity. Relatively little is focused on CIP. For terrorist threats, the best developed sectors are aviation security and radiation detection. For the former, the Commission is working with ECAC to address the limitations of its current Common Evaluation Process and integrate fully with European aviation security legislation. For the latter, ITRAP+10, a collaborative project with the USA, will present its conclusions shortly. For Alarm Systems, a basic certification system exists and is under further development. The IT sector has a well-developed framework for security certification based around ISO standards and European legislation. Although certification to the ISO 27000 series is widely carried out, in the most economically and technologically developed Member States other standards are used as well. Specific ISO and IEC standards exist for industrial control systems and networks. The situation for certification of personnel in IT security is confused, with a number of overlapping and competing standards. One group of certification bodies with strong and highly-relevant expertise are the classification societies, who have expanded beyond their historic ship-classification role into sectors such as offshore installations, transport infrastructure and information and communication technology. Audit companies have also started to offer certification services in information security and business continuity. Payments systems are a critical part of the financial infrastructure for which a regulatory regime exists, under the leadership by the Bank for International Settlements. The establishment of a certification process appears to be the natural next step for these systems.

European Commission
EUR 26808 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: Technology Certification for Critical Infrastructure Protection: Current procedures in EU and EEA States

Author: Adam M. Lewis

Luxembourg: Publications Office of the European Union

2014 – pp. 30 – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831- 9424 (online)
ISBN 978-92-79-39774-5

doi: 10.2788/11691

LB-NA-26808-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

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

Serving society

doi:10.2788/11691

ISBN 978-92-79-39774-5

Publications Office