Draft report phase 1:

Analysis of the current security landscape

Mandate M/487 to establish Security Standards

Please note that this report is only sent to the members of the coordination group and the members of CEN/TC 391 for commenting. Circulation of this version of the report is restricted to this group.

All are asked to send in their comments via the comment table provided with the report, no later than 13 February 2012. After handling the comments, a final report will be drafted and ready for public circulation on 17 February 2012.

NEN

CEN CENELEC ETSI

NEN Industry

P.O. Box 5059
2600 GB Delft

Vlinderweg 6
2623 AX Delft
The Netherlands

T +31 15 2690107
F +31 15 2690207

chemistry@nen.nl
www.nen.nl

Netherlands Standardization Institute

In assignment of:

European Commission - DG Enterprise and Industry - Security Research and Development

Draft report phase 1:

Analysis of the current security landscape
Mandate M/487 to establish Security Standards

REPORT VERSION
v1.1

REPORT DATE
31-01-2012

Contents

List of Annexes

1 Introduction

1.1 The mandate M/487 to establish security standards

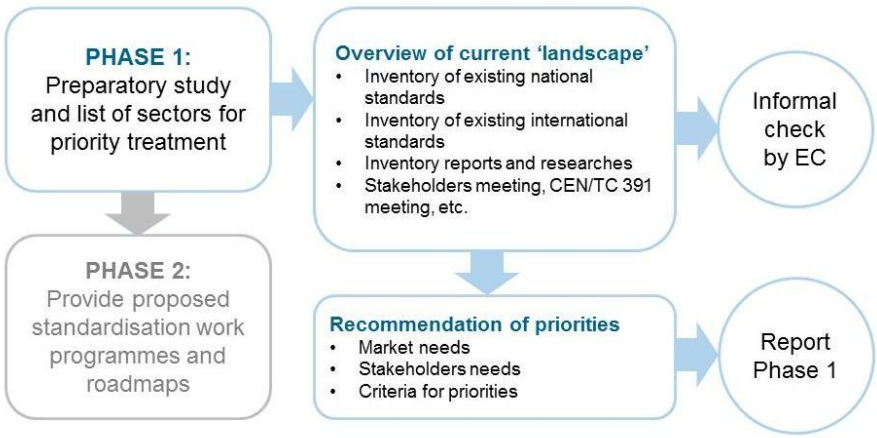
In May 2011 the EC/EFTA launched the mandate M/487 to establish Security Standards. This mandate requests a study to analyse the current standardization 'landscape' in the field of security standards and subsequently, the development of a proposed work programme. The mandate is horizontal, potentially covering all subjects relating to civil security.

The mandate has been accepted by CEN, CENELEC and ETSI, and the work has been allocated to CEN/TC 391 'Societal and Citizen Security' whose secretariat is provided by the Netherlands Standardization Institute (NEN). The mandate consists of two phases:

- Phase 1: to provide the result of a preparatory study and a list of sectors for priority treatment;
- Phase 2: based on EC reaction to the output of Phase 1, to provide proposed standardisation work programmes and roadmaps related to the agreed sectors.

1.2 Phase 1

Phase 1 focuses on first to obtain an overview of the current security landscape and secondly a list of sectors for priority treatment to be agreed by the Commission services. This phase includes an informal check by the European Commission, after which the draft report will be available for stakeholders to comment on before the final report is submitted to the European Commission.



The Commission will endeavour to review the study and select some security sectors within three months, after which phase 2 of this mandate work will start.

2 Scope and framework

As the area of security is a broad field, boundaries needed to be defined first to establish a framework. The mandate defines the following concept for security to focus on:

"The security concept here includes, among others, protection against threats by terrorism, severe and organised crime, natural disasters, pandemics and major technical accidents. It excludes defence and also space technology, for which a programming Mandate has already been issued by the Commission (Mandate M/415)"

With this security concept, an initial list of security areas for analysis is provided (not exhaustive), which is used as a guidance for the research work. In the next table, the research areas are listed with examples of the subareas.

Furthermore, the mandate is more specific on what should and should not be taken into account:

"Human factor issues, privacy concerns and identification of operator requirements for enhancing systems effectiveness are relevant to all the topic areas listed above and should be duly taken into account, not forgetting transversal areas neither.

With the exception of Cryptography, as it is considered a key technology for any security application, the Information and Communications Technologies (ICT) are not covered by this mandate. However, specificities which rise from their adaptation to the field of security should be included in it."

In analysing the current security standard landscape, both national and international standards (and other standardisation deliverables) in the field of security are taken into account; more specific on the international standards, this comprises of the EU standards, as well as ISO and IEC. The types of standards to be included are:

- Technical interoperability standards
- Syntax standards
- Semantic standards
- Organisational interoperability standards
- Performance standards

3 Approach

3.1 Coordination of the work

In coordinating and handling the response to the mandate, several groups have been set up.

An informal coordination group (consisting of representatives of CEN, CENELEC, ETSI, European Commission and the chairman and secretary of CEN/TC 391) has been established which will provide with additional support, information and guidance to CEN/TC 391 in handling the response to the mandate.

Furthermore, CEN/TC 391 has established a dedicated Mandate Working Group, the ad hoc Joint Working Group 'M/487', to prepare the Phase 1 report. The joint working group is also open for members from CENELEC and ETSI.

3.2 Handling of the response

With the coordination group it has been discussed what is and is not expected to be incorporated in the inventory.

For phase 1, the inventory of security standards will consist of:

- National standards: standards in European countries only. This will be done via the members of CEN/TC 391.
- European standards: standards developed at CEN, CENELEC and ETSI.
- Worldwide standards: standards developed at ISO, IEC and ITU.

The inventory of research reports will consist of the reports mentioned in the mandate and one added report:

- ESRIF Report
- Study on Competitiveness of the EU Security Industry
- The Stockholm Programme
- Security research projects under the 7th Framework Programme for Research - Investing into security research for the benefits of European citizens

4 Overview of findings

4.1 Overview of national standards

An inventory of the national standards in Europe has been made by means of a survey, which has been sent out to the members of CEN/TC 391.

Seven out of the 18 member countries have responded to the survey (40%); four countries have submitted their national standards. Other countries indicate not to have national standards in the area of security.

In total, 119 national standards were found. These standards have been categorised in the security areas as defined in the mandate. The result is the below table. The full overview of the national standards submitted by the country members can be found in Annex A.

Country (no. of standards)	Security area			
	Security of the Citizens	**Security of infrastructures and utilities**	**Border security**	**Restoring security and safety in case of crisis**
Austria (16)	4	1		11
Czech (1)	1*			
Germany (54)	27	11	0	17
Netherlands (47)	41	1	0	5

The findings on national standards are:

- In the area of “Security of the Citizens” it is striking that many national standards exist on fire hazard (26 German and 27 Dutch standards), and few in the other subareas.
- In the area of “Security of infrastructures and utilities”, few national standards exist. The German standards in this field are mostly in the subarea of “building design” (5 out of the 11 standards).
- None of the countries have national standards developed on “Border Security”.
- In the area of “Restoring security and safety in case of crisis”, most national standards are in the subarea “preparedness and planning” or “response”. There was only one standard (Germany) that categorized it to be in the area of “recovery”.

Note of the authors:

It is disappointing how few countries have submitted their national standards. At this stage, where comments from the coordination group and CEN/TC 391 is asked, we urge the other countries to still submit their national standards in order for these to be taken into account in this report; especially the UK and France are requested to submit their national standards.

4.2 Overview of international standards

In order to find the existing official European and worldwide standards a database search has been carried out on two places:

- *Database of the Netherlands Standardization Institute*. This database contains the standards of the official international standardization organizations (CEN, ISO, CLC, IEC, ETSI and ITU-T).
  The keywords used for this search were: accident(s), disaster, crime, nuclear accident, disaster, epidem*, pandem*, public safety, border security, fraud, forensic, terroris*, crisis, crises, border control, security biometrics and security guide.
- *'Security Standards Database'*. This database is provided on the website of ITU-T (under study group 17 Security) has been used to filter additionally the security standards developed by ETSI and ITU-T as the above mentioned keywords might not be sufficient for a search through these standards.

All the results from the databases have been categorised in the below table. The full overview of these international standards can be found in Annex B.

Category	CEN	CLC, IEC	ISO	ISO/IEC	ITU	ETSI
SECURITY OF THE CITIZENS						
Organized crime			3			
Counter terrorism			1			
Explosives						
CBRN	1					
Fire Hazard						
*Healthcare**	21		1			
SECURITY OF THE INFRASTRUCTURES AND UTILITIES						
Building design	8					
Energy	18		3			
Transport and transport and communication grids			5			
Surveillance						
Supply chain			1			
*Nuclear**		6	1			
*Finance**			3			
BORDER SECURITY						
Land security			1			
Sea security	1					
Air security	1					
RESTORING SECURITY AND SAFETY IN CASE OF CRISIS						
Preparedness and planning		6	18	17	12	10
Response	1		2	2	4	
Recovery			3	1		
OTHER CATEGORIES						
*Methodology**			3			1
*Techniques**				11	1	
*Biometrics**				3	7	

In general, it was not always clear how to categorise the standards; some standards could be placed in multiple categories, while other standards needed another category that was not defined yet. Thus, not all of the work that has been found could be categorised in the defined categories of the mandate. The new categories are marked in the table with a star (*). Within the area of 'Security of the Citizens' a category 'healthcare' was added. In the area of 'Security of the infrastructures and utilities' the categories 'nuclear' and 'finance' were added. Three categories could not be listed in one of the areas and were listed separately. These are 'methodology', 'techniques' and 'biometrics'.

The table above shows that there are some sectors in which a large number of standards are already developed, such as “energy”, “preparedness and planning” and “healthcare”. Other areas, such as “border security” or “CBRN”, have few to no standards at all. This does not necessarily imply that no standardization activities are done within this area; one can expect a so-called ‘snowball effect’. The category “CBRN” will be taken as an example.

CEN/TC 391 ‘Societal and citizen security’ has recently established a working group on CBRN, in which one project officially started, while it also has one new work item currently under vote. Besides that, CEN/TC 391 has been contacted by companies and consortia that are applying for projects within the 7th Framework Programme of the European Commission. Given the fact that the European Commission also developed a “EU CBRN Action Plan” where standardization plays a role, one can expected that more CBRN projects will be submitted within a year. Thus, we already know that standardization activities are encouraged in this field and first initiatives have taken place. It will not be unexpected if this creates a ‘snowball effect’; once standardization has started in a field, more standardization activities will follow.

Furthermore, the above table only gives a snapshot of the currently existing standards, but it does not include the picture of the most recent discussions and developments in the different areas. It might be concluded that in almost all security areas standardization plays a role.

One can argue that many keywords are still missing, yet the selection of the above mentioned keywords should cover the main area of this mandate. However, the keywords “explosives” and “fire hazard” were not used from a pragmatic perspective; there are a large number of standards in these fields, and they mainly deal with safety instead of security. This was a difficult issue as a database research was conducted; as safety is almost inherent to standardization, hundreds of standards can be found that deal with safety aspects. Some of these cover both the area of safety and security.

Note of the authors:

In discussion with the coordination group, some keywords will be added to the search, being “explosive and terroris*” and “explosive* and device*”. This part will be extended.*

Furthermore, an overview of TCs that develop standards and/or standard deliverables in the area of security is listed in the below table. In total, 11 European TCs and 23 worldwide TCs have been identified.

European TCs that have developed standards on security		Worldwide TCs that have developed standards on security	
CEN/TC 164	Water supply	**ISO/TC 8**	Ships and maritime technologies
CEN/TC 251	Healthcare informatics	**ISO/TC 22**	Road vehicles
CEN/TC 278	Road transport and traffic	**ISO/TC 68**	Financial services

	telematics		
CEN/TC 294	Communication systems for meters and remote reading of meters	**ISO/TC 85**	Nuclear energy, nuclear technologies, and radiological protection
CEN/TC 325	Crime prevention by urban planning and building design	**ISO/TC 145**	Graphical symbols
CEN/TC 354	Ride-on, motorized vehicles intended for the transportation of persons and goods and not intended for use on public roads - Safety requirements	**ISO/TC 190**	Soil quality
CEN/TC 384	PC Airport and aviation security services	**ISO/TC 204**	Intelligent transport system
CEN/TC 391	Societal and citizen security	**ISO/TC 215**	Health informatics
CEN/TC 417	PC Maritime and port security services	**ISO/TC 223**	Societal security
CLC/TC 79	Alarm systems	**ISO/TC 224**	Service activities relating to drinking water supply systems and wastewater systems
ETSI/3GPP	Alarm systems	**ISO/TC 246**	PC Anti-counterfeiting tools
		ISO/TC 247	Fraud countermeasures and controls
		IEC/SC 45A	Instrumentation and control of nuclear facilities
		IEC/SC 45B	Radiation protection instrumentation
		IEC/TC 100	Audio, video and multimedia systems and equipment
		IEC/TC 107	Process management for avionics
		JTC 1/SC 27	IT Security techniques
		JTC 1/SC 31	Automatic identification and data capture techniques
		JTC 1/SC 37	Biometrics
		ITU-T/SG 2	Operational aspects of service provision and telecommunications management
		ITU-T/SG 5	Environment and climate change
		ITU-T/SG 13	Future networks including mobile and NGN
		ITU-T/SG 17	Security

In addition, a survey has been conducted amongst the (relevant) secretaries of CEN/TCs and ISO/TCs. The secretaries were asked to provide the relevant security standards developed within their TCs; these were checked with the database and added where missing. Also, the TC secretaries could leave their comments. Some comments from the secretaries need to be taken into account for this work and are extracted in the below table. See Annex C for all received comments.

TC	Comments
CEN/TC 234	CEN/TC 234 states that no further European standardization on security in gas infrastructure is required at the time being. After completion of the national stipulations required by the SoS Directive which are currently in preparation, further action in CEN/TC 234 will be considered and taken, where necessary.
ISO/TC 247	The focus of TC247 is standardization in the field of the detection, prevention and control of fraud, defined as an intentional act of deception that creates human or economic harm. Examples include counterfeiting, identity theft,

	smuggling or other infringements. Most of the standards developed under this Technical Committee will be related to security issues effecting individuals and organizations for the prevention of fraudulent (criminal) acts. We do not directly develop technology security standards related to cyber security.
ISO/IEC JTC1/SC 27	In general, please note that all SC 27 projects and published standards deal with IT security.

4.3 Overview of researches

Several researches have been carried out over the last years that either incorporate new developments in the field of security and standardization is involved in some way or that try to formulate some guidance or strategy. In the mandate itself the following reports are recommended to be looked at in order to identify possible fields of standardization:

- *ESRIF Report*: the ESRIF report highlighted the importance of an integrated approach to security in order to embrace, among others, interoperability, standardisation, certification, validation and the exchange of best practices.
- *Study on Competitiveness of the EU Security Industry:* in the study delivered by ECORYS (2009) on the Competitiveness of the European Security Industry recommendations were made about the development of new European and common international standards for security as a mean to reduce the Security market fragmentation, which is leading to a lack of competitiveness of the Security European Industry.
- *The Stockholm Programme:* this report, which was adopted by the European Council in December 2009, invites the Council and Commission to develop the internal security strategy, "ensuring that its priorities are tailored to the real needs of users and focus on improving interoperability."

During the project an additional report was added:

- *Security research projects under the 7th Framework Programme for Research - Investing into security research for the benefits of European citizens*; this document summarizes the results of 39 research projects that were carried out under the FP7 programme.

These four reports are summarized on their mentioning on security standardization in the next paragraphs. For an more extensive summary, see Annex D. In addition, the following communications have been looked into (but not separately summarised):

- *EC Communication on reaction to ESRIF:* the Communication COM (2009) 691 "A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations" remarked that in order to harvest innovation and growth tomorrow it is required to invest now in an ambitious industrial policy for the security sector.
- *EC Communication Towards an increased contribution from standardisation to innovation in Europe:* the Communication COM (2008) 133 underlines the contribution standards could and should make to

innovation (policy). This is judged to be important for further strengthening the European economy as well as directly in competition in standard setting from emerging powers, who consider standardization an important strategic asset.

4.3.1 ESRIF report

The European Security Research and Innovation Forum (ESRIF) promotes a more harmonised approach between security, research and innovation. In Europe's fragmented security market, standardisation can contribute to building more harmonisation to improve the region's position on the world market. Thus, ESRIF strongly supports all efforts to identify necessary new standards and their development. The report puts forward several recommendations regarding new policy initiatives, integrated approach to security and the global dimension.

The ESRIF proposes an European Security Research and Innovation Agenda (ESRIA); a strategic plan for security research and innovation over the next 20 years. Standardisation activities are mentioned throughout the agenda. The next table shows the systemic needs, categorised into each of the security areas defined in the mandate.

Security area	Systemic needs
Security of the Citizens & Security of Infrastructures and Utilities	– Analysis of the standardisation needs in the various segments of the security market. – Promotion of dynamic standardization – Rules and integrity standards for a higher transparency of financial systems
Border Security	– Harmonised global border control, in order to manage the technical and legal complexity arising from the increasing number of electronic travel documents, develop standards required to ensure true interoperability of secure documents and systems, and by defining precise common rules of creation, distribution, update, exchange and revocation of certificates between the EU Member States
Restoring Security and Safety in Case of Crisis	– Standardisation of rescuer identity, skills and credential for interoperable command and control cooperation, for a more efficient international cooperation.
Others - Identity management and protection (ICT)	– Develop interoperability requirements (architectural, technical, operational etc.), aiming at agreed processes and standards

In Europe's fragmented security market, standardisation can contribute to building more harmonisation to improve the region's position on the world market. Thus, ESRIF strongly supports all efforts to identify necessary new standards and their development.

ESRIF has put forward a list of policy and operational recommendations, of which the following regard standardisation activities.

Area	Recommendation
Regarding new policy initiatives	New initiatives and programmes should include the early engagement of all stakeholders and transparency of the regulatory environment, including standards to stimulate private sector investments in security research. If upcoming regulations are understood early on, a return on security investments can be

	foreseen and investments can thus be expected to take place.
Regarding integrated approach to security	Effective civil security must embrace interoperability, standardisation, certification, validation, communication with the public, education & training, exchange of best practices, consultations on privacy issues and other factors that cut across public and private spheres and provide synergies between civil security and defence research fields.
Regarding the global dimension	The globally inter-related nature of security calls for giving high priority to security's external dimension and closer home affairs/defence consultation. Research and innovation programmes should support peacekeeping, humanitarian and crisis management tasks, including joint initiatives with other regions and international organisations, notably as regard the development of global standards.

ESRIF has also defined a roadmap. The mentioning of standardization is put in the table below, divided into the security areas defined in this report. A more extensive table can be found in Annex D.

What?	Why?	How?
SECURITY OF THE CITIZEN		
Enhanced resilience and protection of the financial and payment systems	The fraud targeting the financial and payment systems is growing dramatically. New kinds of approaches are needed to address this major problem.	– Rules and integrity standards for a higher transparency of financial systems.
Analysis of forensic traces	Analysing evidence on a crime scene is the basis of the forensic approach. This evidence is, most of the time, composed of various kinds of traces which require sophisticated tools for analysis.	– International standards for trace recovery
BORDER SECURITY		
Standardization, Norms, Interoperability Standardized equipment/elements, similar procedures/protocols, joint operations, education and training	In order to achieve maximum efficiency in operations and reduce costs of technology procurement and operations conduct, standardization where feasible and interoperability are key.	– development of affordable technological solutions, – development of generic interfaces/middlewares, – norms of implementation – research on: development of common operational and procedural guidelines and requirements
CRISIS MANAGEMENT		
Strengthening response forces	Response forces need state-of-the-art technical equipment in the field of sensors, communications and utilities. However, the most promising way to strengthen and enforcing crisis response forces is to bundle and deepen all efforts on European level, in the Member States and by the private sector in the broad area of education, training and exercises.	– provide standardisation of rescuer identity, skills and credential to allow interoperable command and control cooperation for a more efficient international cooperation – address the use of virtual live exercises and other simulation-supported training methods, in particular multi-hazards training simulators, the development of appropriate and sufficient methods and tools for structured ways of lessons learned analysis, exchange and integration into planning and training, and on the education side the development of international degree courses and standards for crisis management leaders aimed at excellence would be recommended.
CBRN		
CBRN integral threat assessment: Surveillance tools for detection of offensive capacity with emphasis on emerging technologies with dual-use potential; analysing actor intention; Intelligent agent data-base and sharing capabilities with high level of standardization using validated accepted data; Systematic identification of	Before prevention or preparation strategies can be applied, a complete and accurate assessment of the CBRN threat is required. Continuous assessments and foresight then helps to ascertain the efficacy of prevention strategies and future investments. An accurate CBRN threat assessment is also important to first responders and other crisis management personnel for setting planning and training agenda and can help prioritize research in this critical security area as well.	– Map, through multidiscipline approaches, relevant potential pathways to CBRN terrorism (including radicalisation mechanisms in a CBRN context) and their unique and specific signatures, sensitive to group dynamics and technological abilities – Through cautious awareness raising-dialogue gain support from civil society, law enforcement, academia etc to detect anomalies – Meta-analysis of the complex threat dilemma and development of new, non-frequentist and nondeterministic analysis methods – Methodology to derive the probability of successful incidents. Input is from actor profiles, actor capabilities, consequence prediction, probabilitics – Intelligent database development and analysis;

vulnerable targets		– Objective/quantitative algorithms – Modelling capabilities for attack simulation and intervention planning (in/out-door; urban, sub-urban, rural, industrial, infrastructure
IDENTIFICATION OF PEOPLE AND ASSETS		
Protection against Identity theft and frauds in both physical and virtual worlds	Identity theft is a major current problem in the world, impacting millions of people and undermining global and financial security. No coherent approach to address this threat is currently in place. It requires a concerted effort involving significant advances in processes and technology.	– Development of agreed processes and standards.
Identification of victims during Disasters and Emergency Management	In case of disaster, it is critical to identify, as soon as possible the identity of the victims (including survivors). In case of major disasters, experience (2004 tsunami, Katrina..) has shown that more solid and efficient solutions are needed for the management and tracking of the survivors. Solid identifications solutions, adapted to the specific context must be developed.	– Standardisation of rescuer identity, skills and credential to allow interoperable command and control cooperation
Intelligent-led border management	The growing need for high security controls at border crossing has a negative impact on the management of the flow of travellers (lengthy waiting time). Solutions are needed for easier and faster processing. A fast and automatic border control process should be put in place for the majority of travellers, and better tools should be developed for support non automatic procedures.	– Develop standards for interoperability of secured ID documents and equipments.
Harmonised global border control	Standards – failure to agree and put in place all required standards continues to hold up our ability to exploit and maximise our use of available and new technologies. Also it hinders innovation and R&D as developers still do not have roadmaps for all requirements as yet.	– Develop standards required to ensure true interoperability of secure documents and systems.
INNOVATION ISSUES		
Standards development	The European security market is highly fragmented, favouring the development of multiple and incompatible solutions. A solid standardisation effort at European level would help promote the development of innovative solutions addressing the overall market, and would strengthen the European industry.	– Analysis of the standardisation needs in the various segments of the security market. – Analysis of the conditions allowing the definition and implementation of a European Security Label. – Analysis of the economical impact. – Promotion of dynamic standardisation.
GOVERNANCE AND COORDINATION		
Standardisation and Certification within a European reference system, co-ordinated by the EU and implemented through national bodies	The existence of a multitude of protection levels and standards across EU Member States increases costs for businesses, which have to incur redundant security investments depending on the jurisdictions under which they operate. The EU must define a security standard notably for strategic infrastructures.	– The “Stable Structure” should be in charge of the development and implementation of concepts, doctrines, procedures and designs in order to achieve and maintain the compatibility, interchangeability and/or commonality that are necessary to attain the required level of interoperability

Summarizing the above, the next list provides an overview of the standardization activities recommended by this report in the security areas defined in the mandate:

- Security of the citizen

  - fraud; standards for higher transparency of financial systems
  - identity theft and frauds (physical and virtual worlds)
  - forensic traces; standards for trace recovery
  - CBRN integral threat assessment; standards for sharing capabilities
- Border security
  - maximum efficiency in operations and reduce costs of technology procurements and operations; standards to ensure true interoperability of secure documents and systems
  - fast and automatic border control process; standards for interoperability of secured ID documents and equipments
- Restoring security and safety in case of crisis
  - identification of victims; standards for rescuer identity, skills and credential to allow interoperable command and control cooperation
  - education, exercise and training; standards for crisis management leaders

Within the three mentioned security areas, ESRIF encourages the development of concrete standards to build more harmonization to strengthen the European security industry and improve its position on the world market. To coordinate this, it argues for a solid standardization effort at European level.

4.3.2 Study on Competitiveness of the EU Security Industry

The final report of this study aims at providing a picture of the current situation of the EU security industry, its structure and organisation, competitiveness position and challenges for the future. With regard to security standardisation activities, one of the most significant problems the industry is facing is the absence of European and common international standards in a fragmented EU market. The report makes several concrete recommendations to enhance the standardisation framework in the field of security in order to strengthen the EU security industry. An extensive summary can be found in Annex D.

One of the most significant problems the industry is facing is the absence of European and common international standards, which creates problems both on the supply and demand side of the security market. The report mentions the absence of common performance standards and the absence of common technical standards.

Enhancing the standardization framework in the field of security at EU and international level is a part of strengthening the EU security industry. Specific recommendations are given by this report to achieve this (see table below).

Recommendation	Concrete initiatives
Industry-based solution for the development of technical standards	– Strengthening of European Standardisation Organisations' work. Public authorities could call for the development of new standards in the security field, providing clear mandates to ESOs based on priorities set out in the European 'vision' for security; – European Security Standards Institute. Either within existing ESO framework or as an oversight body for security standards. For example, following a similar approach as that adopted by ETSI (European Telecommunications Standards Institute) and aimed at

	facilitating the self-development of technical standards; – New Approach legislation for security: The possibility of establishing a system of voluntary standards in the security industry should be considered.
Formal approach for the development of performance standards	– European Security Standardisation Handbook, based on the initiative already in place in the defence sector (i.e. European Handbook for Defence Procurement); – European Security Label, which would increase confidence and act as a catalyst for investment by attracting new investors to the security industry. As mentioned by ESRIF, this will act as a reference point for manufacturers, end-users and other relevant stakeholders and would provide the frame for a dynamic standardisation process.
EU-level testing and certification scheme and improved approvals and certification infrastructure, with the aim at creating a testing protocol and the necessary infrastructure (dedicated labs or testing facilities) to carry out testing practices of security products	
Exchange of formal and informal information on testing facilities as well as best practices, with the objective of increasing transparency and cooperation (e.g. following the example of the CREATIF Network initiative)	
Fast-track system for approval of priority technologies and equipment, to enhance rapid responses to new security threats and challenges	

Concluding, this study points out that the problem of the security industry is the absence of European and common international standards, especially technical and performance standards. The study recommends to set up or develop security standardization efforts, such as an “European Security Standards Institute”, an “European Security Standardization Handbook” or an “European Security Label”. It basically recommends coordinating security standardization efforts more and thematically and also recommends involving the ESOs with these efforts.

However, a note should be placed with the suggestion for a “European Security Standards Institute”: it is possible to do so, but as the ESO’s are coordinating more and more work together, an oversight body for security standards could be neither efficient nor effective. Such initiative should therefore be considered within the existing ESO framework.

4.3.3 The Stockholm programme

The European Council has adopted a new multi-annual programme to be known as the Stockholm Programme, for the period 2010-2014. The programme defines strategic guidelines for legislative and operational planning within the area of freedom, security and justice, addressing the challenges Europe is facing.

Although mostly focused on internal security strategy, the document does mention standardization. The programme indicates the need to develop and promote international standards, especially in the field of personal data protection and border surveillance. It also stresses the external dimension, and the EU and the Member States should also take part in developing and promoting international (worldwide) standards.

4.3.4 FP7 Security research projects

Through the Preparatory Action for Security Research and the Security Theme of FP7, a number of security research projects have been supported under the 7th Framework Programme for Research. The catalogue 'Investing into security research for the benefits of European citizens' (September 2010) presents an exhaustive overview of these projects. This paragraph summarizes the exhaustive overview of all security research projects mentioned in the catalogue related to security standardization. For a detailed analysis of the researches, see Annex E.

Out of the 78 research projects, a large majority of these projects were done in the area of 'security of the citizens' and 'restoring security and safety in case of crisis'. Furthermore, a search was carried out to identify the projects that have addressed the subject standardization in some way. Out of the 78 projects, 19 projects mentioned standardization.

Some of the projects result in specific standardization results, being the following:

- A roadmap for the future development of testing, incl. standardization & certification (CREATIF)
- Strategic R&T and standardization roadmap (ESCoRTS)
- OPERAMAR will suggest to the EC recommendations in terms of future research programs, projects and new standards
- A standardized training curriculum on disaster management for first responders (CAST)
- Standards Mapping and Analysis (CRESCENDO)
- Development of a network/expert body for standardization and regulations harmonization proposals (CAST)
- The standard proposition for a European 2D/3D emergency symbology (INDIGO)
- To create an open, standards based interoperability layer (INFRA)

A survey to all the project coordinators was set out to ask the following questions:

1. Which security area does the project cover?
2. Was standardization part of the project?
3. Are there standardization results?
4. Are there standardization opportunities?
5. Did you use any existing relevant standard?
6. Are there standards missing?

The response to the questionnaire can be found in Annex E. Bottom line is that most of the project leaders recognize the importance of standardization, but they discover that little or no standards are available in the different fields. Reason for that is possibly that there is not that much knowledge of standardization in the different sectors and therefore the benefits of standardization have still to be discovered. All of the project leaders that have thought about standardization state that standards have to be developed in the future.

With respect to the different sectors covered by the projects, it can be concluded that they do not differ from the areas that have been identified by the mandate already. Reason for that might be that the mandate was based on the areas that could already be identified via research fields.

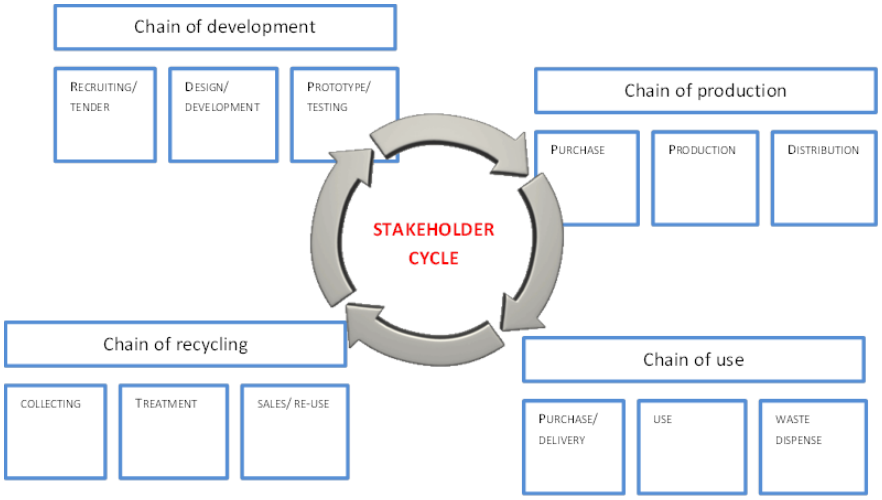
In phase 2 of the mandate work, the results that were given with respect to specific standardization projects and ideas can be used. As some of the project leaders mentioned the development of a roadmap themselves, they can possibly be asked to be part of the further work on the mandate.

4.4 Stakeholders

4.4.1 Identified stakeholders

Developing a map of relevant stakeholders within security standardization is complex, and within the timeframe of the mandate is not possible to come with a complete analysis. Therefore the areas of analysis which are already given in the mandate itself are used in order to structure the stakeholder analysis.

In order to carry out the stakeholder analysis, a model is used as described in the figure below.



What is not given in this cycle are education and training, research and development and legislation. Those are inherent to all parts of the cycle.

The figure shows that, for whatever subject one can choose, a whole cycle of stakeholders can be identified. Depending on the subject, different stakeholder groups will be of different importance. For example, for products, the whole range of stakeholders is relevant. For management standards and system standards, the picture has to be slightly adjusted as there is no production and no recycling involved.

In order to be able to fill in the different fields, the below table is extracted from the figure.

Subject		
Chain of development		
Recruiting/tender		
Design/development		
Prototype/testing		
Chain of production		
Purchase		
Production		
Distribution		

Chain of use		
Purchase/delivery		
Waste dispense		
Chain of recycling		
Collecting		
Treatment		
Sales/ re-use		

In order to carry out the stakeholder analysis for the above defined sectors, the table has been filled in for every sector. The results of the analysis are given in Annex F.

The analysis below is shown here for the example of Security of infrastructure and utilities - Supply Chain:

Subject	**Security of infrastructures and utilities – Supply chain**	
Chain of development		
Recruiting/tender	Responsibles for building design, fire safety and surveillance Transport and storage services (logistics) Private security services	CoESS, Euralarm, EOS
Design/development	Business continuity services Suppliers of technical equipment	
Prototype/testing	Research institutes	
Chain of production		
Purchase	Technical equipment (and parts) for prevention, detection and response in case of fire, explosives, flooding, burglary, smuggling, vandalism, theft or terrorist threat	
Production	Assembly of the equipment (parts)	
Distribution	Installation and surveillance services	
Chain of use		
Purchase/delivery	Responsibles for building design, fire safety and surveillance Transport and storage services (logistics) Private security services Business continuity services	
Waste dispense		
Chain of recycling		
Collecting		
Treatment		
Sales/ re-use		

Please note that the list of stakeholders is a mere indication and does not claim to be complete. The list is open for modifications and suggestions for additions, and experts are invited to complement the list.

Especially for stakeholders in the supply chain (purchase, production, distribution), the exact stakeholders vary and could be described more specific at a later stage when areas for priority treatment are defined.

Furthermore, most of the activities are services and are excluded from the recycling phase. As far as technical solutions are being sought, they either require special treatment (CBRN waste), or they are of a durable nature, e.g. a sprinkler system being maintained, or a fire extinguisher replaced by a new one. Re-use isn't common in this area.

Finally, many of the stakeholders are both involved on the one hand in the design, development and tendering, and are users on the other hand. The market appears user-driven (unlike for example fashion, where the design and manufacture dominate the user descriptions).

4.4.2 Result of the kick-off meeting

To inform the stakeholders about the mandate work and to allow stakeholders to present their perspectives on the work, a kick-off meeting was organised on 29 September 2011 (see Annex G for the report of the meeting).

Mr Malacarne from DG Enterprise and Industry provided the background of the mandate and stresses that an EU wide picture of the standardization landscape is needed; standards can encourage better harmonization and interoperability in security.

The stakeholders presentations indicate the need for security standards and the need for the coordination of the development. The presentations give an idea and some examples what has already been done and what the expectations are from the work. Currently, most standards development done at the end of research; at the meeting however, many stakeholders stress the need of standardization and research being two sides of the same coin. Standards are important tools.

During the meeting, the stakeholders agree on the need for security standardization, and have shown great willingness to contribute to the mandate's work. Suggestions have also been made by the stakeholders.

Examples of initiatives by stakeholders presented during the meeting:

- EOS members, in their White Papers, have long been asking for European standardization, for the different priority domains
- Coordination office for civil security at DIN: industrial policy initiative of the German Federal Ministry of Economics and Technology
- ENISA collaborations with standards development organisations
- ETSI established Operational Co-ordination ad hoc Group on Security (OCG Sec) to coordinate the horizontal structure for security issues
- Euralarm defined European certification scheme "CERTALARM", fighting for market acceptance.

Recommendation highlights from the stakeholders for the mandate:

- Prioritize those areas where standardization is needed more urgently to strengthening the competitiveness of the European security industry;
- Standards are needed for all the areas identified in the programming mandate;
- Focus on harmonization and compatibility;
- Use standards to facilitate information-sharing and cross-border communication are crucial for all security areas;

- Standardization to improve transparency of procedures;
- Improve visibility of results and benefits to stakeholders;
- Standardization to increase European competitiveness in a global market;
- Stimulate the cooperation between the different European technical committees.

4.4.3 First priorities from members of CEN/TC 391/JWG 'M/487'

The CEN/TC 391 members were also asked to state any priorities for security standardization. Only three replies were received (one from Germany and two from liaisons), thus the current collection of the priorities is limited. The detailed overview of the mentioned priorities can be found in Annex H. Here the priorities have also been sorted into categories.

Although limited in the number of responses, the list shows that there are many ideas for priorities. The areas for priorities are:

- Security of the Citizens (10 priority suggestions)
- Security of Infrastructures and Utilities (6 priority suggestions)
- Restoring security and safety in case of crisis (1 priority suggestion)

Thus priority suggestions for all areas are given except for border security.

In addition, during the preliminary CEN/TC 391/JWG 'M487' meeting on 24 October 2011, it was agreed to suggest the following criteria for priority treatment:

- Protect people and facilities
- Promote EU security industry
- Facilitate EU need

5 Analysis of the current landscape

National Standards

A survey with respect to existing national standards within the member countries of CEN/TC 391 produced a reaction of 7 of the 18 member countries (40%). The countries that responded were Austria, Czech Republic, Germany, The Netherlands, Bulgaria, Sweden and Italy. Out of these counties, four countries submitted national standards on the subject. In total 119 national standards were found of which all could be categorised in the four defined security areas.

In the area of “Security of the Citizens”, many national standards exist in the area of fire hazard, and few in the other subareas. In the area of “Security of infrastructures and utilities”, few national standards exist. In the area of “Restoring security and safety in case of crisis”, most national standards are in the subarea “preparedness and planning” or “response”.

Striking was that none of the countries have national standards developed on “Border Security”. This can be explained as most of the border security issues is arranged on national level by the government itself (laws and regulations).

Evidently, the collected data was too little to draw strong conclusions regarding national standards in Europe.

Of the countries that have responded and indicate that they do not have any nationals standards in the area of security, the issue here can be that this depends on the interpretation of what is seen as a security standard. Although the security concept has been defined and used to indicate the area, it can be assumed that the countries interpret security standards differently, and therefore some countries indicated not to have any.

Some data of major countries are missing, such as from France and UK. These should be at least included to be able to draw any conclusions on national standards.

European and international standards

A database research in combination with surveys has been conducted to come with a list of international standards in the field of security. This list does not claim to be complete; keywords have been defined to narrow down the search and by contacting the relevant TC secretaries, the most important standards should be identified.

During the categorisation of these standards, several new ‘categories’ were added as some of the standards did not fit in the security areas defined in the mandate. These are:

- Healthcare (subcategory in the area of “Security of the Citizens”)
- Nuclear (subcategory in the area of “Security of Infrastructures and Utilities”)
- Finance (subcategory in the area of “Security of Infrastructures and Utilities”)

- Methodology
- Techniques
- Biometrics

The category ‘healthcare’ is not mentioned in the list of security areas. This category is primary defined under “Security of the Citizens”, however, it could have also been defined under “Security of Infrastructures and Utilities” or “Restoring security and safety in case of crisis”. It serves in many areas and should be taken into account as an area for priority treatment.

For analysing the category ‘nuclear’, the most recent developments should be taken into account. The accident at the Fukushima nuclear power plant in Japan last year triggered the need for an immediate and coordinated response from the EU. It was concluded that the safety of all EU nuclear plants should be reviewed, on the basis of comprehensive and transparent risk and safety assessments ('stress tests'). Here standardization opportunities can be defined to contribute to the improvement of nuclear safety.

One of the challenges of this search is to determine which keywords are most relevant and will result in the correct results. Keywords such as ‘explosives’ and ‘fire hazard’ have not been included in the first search as these will result in a long list of standards, while many of these deal with safety and not security. However, some cover both safety and security; the inclusion and exclusion of keywords have been discussed and the list will be extended using several selected keywords. This will lead to the creation of a longer and more complete list of standards.

Generally speaking, the inventory shows that there are some sectors in which a large number of standards are already developed, such as energy, preparedness and planning and healthcare. Other areas, such as border security or CBRN, have few to no standards at all. This does not necessarily imply that no standardization activities are done within this area. As the inventory only gives a snapshot and does not show the most recent discussions and developments in these areas, it might be that standardization activities is being discussed. And once standardization has started within a field, a so-called snowball effect might take place; more standardization activities will follow.

Reports and researches

The reports all indicate that the EU security industry is fragmented, and stress a need for standardization to improve strengthen the European competitiveness of this industry in the world market.

There is a lack of standards in many security areas, and a high need for common and European security standards. This is confirmed as security standardization is mentioned for all the security areas identified within the mandate, making all of these areas relevant for the mandate work.

When mentioning concrete standards, many suggestions in each of the areas are given. Striking is still the number of times that standards for personal data protection and border surveillance are mentioned. In general the reports stresses the need for interoperability standards in Europe.

The reports encourage a common understanding of security, research and innovation and to include standardization in all phases, to support a more harmonised approach.

The reports also stress the need to take the external dimension into account. Next to European standards, the development and promotion of global standards are also emphasised. The global dimension also applies to the development and promotion of European standards to become recognised as global standards.

Security standardization needs to be approached in a more structured way, and the reports argue for a solid security standardization (and validation and certification) effort at European level. Many suggestions are given how to coordinate security standardization efforts, and it is recommended involving the ESOs in doing so.

With regard to security researches, the projects described in the catalogue 'Investing into security research for the benefits of European citizens' have been analysed, and one out of four security research projects cover standardization in one way or the other.

The survey amongst project coordinators shows that most of the project coordinators recognize the importance of standardization, but they discover that little or no standards are available in the different fields. Reason for that is possibly that there is not that much knowledge of standardization in the different sectors and therefore the benefits of standardization have still to be discovered. The project leaders that have thought about standardization all state that standards have to be developed in the future.

In phase 2 of the mandate project, the results that were given with respect to specific standardization projects and ideas can be used. As some of the project leaders mentioned the development of a roadmap themselves, they can possibly be asked to be part of the further work on the mandate.

Stakeholders

The kick-off meeting of the mandate showed a lot of support for the mandate and the effort to create a roadmap for security standardization. It also showed the need for coordination of the different activities. The meeting itself showed to be a good illustration of the variation in activities, as many different ideas for various sectors were mentioned. In addition, all of the stakeholders present during the meeting suggested priorities in their field of work; yet they also acknowledged the importance of all the other areas defined in the mandate.

Next to the stakeholders' kick-off meeting, a stakeholder analysis has been carried out. This analysis has been carried out for all the sectors given in the mandate, because the intention was to contact all stakeholders for this inventory. However, the analysis showed that the amount of stakeholders is huge and diverse. This is of course not surprising as many of the earlier mentioned studies indicated the security sector being large and fragmented. Therefore, the authors propose to take a closer look at the stakeholders in the next step of the mandate, when the priority areas are determined. This way, the stakeholders can be

approached more specifically. Also, an inventory of the ideas and wishes of these stakeholders can be done at the same time.

Some initial priority suggestions from the CEN/TC 391 members were submitted. Although the response was not high, the response showed that there are lots of ideas of possible standards in a lot of different security fields. The areas covered were:

- Security of the Citizens
- Security of Infrastructures and Utilities
- Restoring security and safety in case of crisis

Note of the authors:

It is expected that EOS will submit their view on the mandate work, representing many stakeholders in the area of security standardization. This part will be then be modified.

6 Main conclusions and recommendations

The diversity of the security sector made it challenging to come up with a complete list of existing standards. Still, after using many resources, a large majority is covered by this report. Having the 80/20 rule in mind, it was decided there is no need to cover the last 20 per cent, taken time and effort into account. In general standardization activities has been found in all security areas defined in the mandate.

The list of standards however is a snapshot, only presenting what has been found during the research period of this report. To keep an overview of all that is being done, one needs to have a dynamic list in which new and published work should be updated regularly. Also, recent developments needs to be taken into account, in order to estimate the so-called 'snowball effect' in some of the areas.

The EU security industry shows to be fragmented and in need of stimulation and coordination of the standardization work. All the different security areas are mentioned and should be stimulated. However, areas for priority treatment should be defined. Concluding from the research findings, the following list of security areas are recommended to consider priority treatment.

Border security

Border security has been mentioned in many of the research reports to be an area for priority treatment, but no standards have been developed until so far, no national or international initiatives, thus this area should be strongly considered to give priority treatment.

In the area of border security, standardization can contribute to a more harmonised border control, higher efficiency in operations, reduction of costs of technology procurement, ensuring interoperability of secure documents and systems. This can apply to all areas of border security, which is the reason why no specific area (such as land, sea or air) is mentioned. Specific standardization activities in border security have already been started by some of the FP7 research projects. These projects should be looked into for a more in-depth study on the specific needs in this area.

Security of infrastructure and utilities – nuclear

The area of 'nuclear' has been separately identified as one of the subcategories within 'Security of Infrastructures and Utilities'. This area is recommended for priority treatment due to recent developments. Safety of nuclear installations in Europe is high on the EU agenda. Standardization opportunities can be defined to contribute to the improvement of nuclear safety.

Security of the Citizens – CBRN

Security standardization in the area of CBRN is mentioned in the various reports as well as during the stakeholders' meeting. Few standardization activities are in the area of CBRN, while the importance of CBRN standardization is also to be concluded from the 'EU CBRN Action Plan' (DG Home). Focus in this area is an integral threat assessment and standards for sharing capabilities. In addition,

"sampling and detection" and "personal protective equipment (PPE) for first responders" also provide for standardization opportunities.

Restoring security and safety in case of crisis – Preparedness, planning & response

Most importantly in the area of 'Restoring security and safety in case of crisis' is the need to improve the coordination and communication. Reports mention several aspects, such as strengthening response forces, stimulate interoperable command and control cooperation and develop standards in the field of education, training and exercises. These are all issues to be taken into account when regarding this security area. The ESRIF report believes that the most promising way to strengthen and enforcing crisis response forces is to bundle and deepen all efforts on European level, in the Member States and by the private sector in the broad area of education, training and exercises.

In addition, in the priority list of the members of CEN/TC 391 several items in the field of emergency management are mentioned.

Security of the Citizens - Healthcare

The category 'healthcare' is not mentioned in the list of security areas. This category is primary defined under "Security of the Citizens", however, it could have also been defined under "Security of Infrastructures and Utilities" or "Restoring security and safety in case of crisis". This category cannot strictly be divided into one of the security areas. It should be taken into account as an area for priority treatment as this relates to so many of security areas. This allows for a combination of the different areas to be dealt with. For example, developing a protocol for first response by healthcare facilities by coping mass casualties from CBRN contamination covers the area of "CBRN", "Preparedness and response" and "Security of Infrastructures and Utilities".

General coordination of security standardization

Not mentioned as a specific area of security standardization, all reports call for combined efforts and coordination of security standardization. Therefore, this is separately mentioned as an area for priority treatment. Many suggestions have been made on how to coordinate this. These should be looked into when searching for a suitable way of coordination.

Note of the authors:

Please note that the current list of priority recommendations is a draft and could change depending on the information that is being awaited. It is expected some areas for priority treatment will still be added.

Criteria for priority treatment

In selecting areas for priority treatment, the following criteria are recommended:

- Protect people and facilities
- Promote EU security industry
- Facilitate EU need

Although the above list suggests priority areas, it is still believed that all of the areas mentioned in the mandate are in need for standardization stimulation. Therefore, trusting in the ‘snowball effect’, it is recommended at least to stimulate one subarea in each of the security areas.

The choice of priorities will be indicated by the industry itself, especially if they feel strongly about it. However, the choice of priorities for work financed by the European Commission is always a political one as well.

List of Annexes

Annex A: Survey on national standards

Annex B: Overview of international standards including comments from survey

Annex C: Overview of comments from CEN/TC and ISO/TC secretaries

Annex D: Summary of research reports

Annex E: Analysis of FP 7 research projects

Annex F: Stakeholders analysis

Annex G: Report of the kick-off meeting

Annex H: Overview of priorities submitted by CEN/TC 391 members

ANNEX A: SURVEY ON NATIONAL STANDARDS

NEN

Annex A: Survey on national standards

Response type	Country name(s)	Total
Countries with national standards on security	Austria, Czech Republic, Germany, The Netherlands	4
Countries without national standards on security	Bulgaria, Sweden	2
Abstained	Italy	1

TABLE 1: OVERVIEW OF NATIONAL STANDARDS AND OTHER STANDARDISATION DELIVERABLES IN THE FIELD OF SECURITY

Country: AUSTRIA

Contact persons: Mag. Siegfried Jachs, Ministry of Interior, siegfried.jachs@bmi.gv.at
Dr. Hermann Huemer, Austrian Standards Institute, hermann.huemer@as-institute.at

Number	Year of Publication	Title	English title	Type of standard (TEC / SYN / SEM / ORG / PER / …)	Security area	Type of industry/ type of threat	Users	Remarks/ additional info
ÖNORM S 2400	2009	Business Continuity und Corporate Security Management - Benennungen und Definitionen	Business Continuity and Corporate Security Management - Terms and definitions					
ÖNORM S 2401	2009	Business Continuity und Corporate Security Management - Systemaufbau und Business Continuity und Corporate Security Policy	Business Continuity and Corporate Security Management - System structure and Business Continuity and Corporate Security Policy					
ÖNORM S 2402	2009	Business Continuity und Corporate Security Management - Business Continuity Management	Business Continuity and Corporate Security Management - Business Continuity Management					
ÖNORM S 2403	2009	Business Continuity und Corporate Security Management - Corporate Security Management	Business Continuity and Corporate Security Management - Corporate Security Management					

ANNEX A: SURVEY ON NATIONAL STANDARDS

ÖNORM S 2410	2010	Chancen- und Risikomanagement - Analyse und Maßnahmen zur Sicherung der Ziele von Organisationen	Chance and risk management - Analysis and actions intended to ensure the objectives of companies and organizations					
ÖNORM S 2430	2011	Corporate Security Management - Anforderungen und Beschreibung für das Verfahren Corporate Intelligence	Corporate Security Management - Requirements and description for the Corporate Intelligence procedure					
ONR 192400	2009	Business Continuity und Corporate Security Management - Anforderungen an die Qualifikation des Business Continuity und Security Managers	Business Continuity and Corporate Security Management - Requirements for the qualification of the Business Continuity and Security Manager					
ONR 49000	2010	Risikomanagement für Organisationen und Systeme - Begriffe und Grundlagen - Umsetzung von ISO 31000 in die Praxis	Risk Management for Organizations and Systems - Terms and basics - Implementation of ISO 31000					
ONR 49001	2010	Risikomanagement für Organisationen und Systeme - Risikomanagement - Umsetzung von ISO 31000 in die Praxis	Risk Management for Organizations and Systems - Risk Management - Implementation of ISO 31000					
ONR 49002-1	2010	Risikomanagement für Organisationen und Systeme - Teil 1: Leitfaden für die Einbettung des Risikomanagements ins Managementsystem - Umsetzung von ISO 31000 in die Praxis	Risk Management for Organizations and Systems - Part 1: Guidelines for embedding the risk management in the management system - Implementation of ISO 31000					
ONR 49002-2	2010	Risikomanagement für Organisationen und Systeme - Teil 2: Leitfaden für die Methoden der Risikobeurteilung - Umsetzung von ISO 31000 in die Praxis	Risk Management for Organizations and Systems - Part 2: Guideline for methodologies in risk assessment - Implementation of ISO 31000					
ONR 49002-3	2010	Risikomanagement für Organisationen und Systeme - Teil 3: Leitfaden für das Notfall-, Krisen- und Kontinuitätsmanagement -	Risk Management for Organizations and Systems - Part 3: Guidelines for emergency, crisis and business continuity management -					

ANNEX A: SURVEY ON NATIONAL STANDARDS

		Umsetzung von ISO 31000 in die Praxis	Implementation of ISO 31000					
ONR 192420	2009	Influenza-Pandemievorsorge für Organisationen	Occupational health care provisions against influenza pandemic					
ÖNORM S 5207	2003	Strahlenschutzausbildung für Interventionspersonal bei radiologischen Notstandssituationen	Radiation protection training of intervention persons in the case of radiological emergency situations					
ÖNORM S 2604-1	2008	Dekontaminierung von Personen im Fall einer großräumigen radioaktiven Kontamination - Teil 1: Einrichtung und Ausstattung von Baulichkeiten als strahlenmedizinische Notfall- und DEKO-Station	Decontamination of persons in case of extensive radioactive contamination - Part 1: Installation and equipment of buildings to serve as medical emergency and DECON station for radiation					
ÖNORM S 2604-2	2008	Dekontaminierung von Personen im Fall einer großräumigen radioaktiven Kontamination - Teil 2: Ablauforganisation und Verfahrenshinweise in der strahlenmedizinischen Notfall- und DEKO-Station	Decontamination of persons in case of extensive radioactive contamination - Part 2: Organization depending on course and procedure instructions in a medical emergency and DECON station for radiation					

TABLE 1: OVERVIEW OF NATIONAL <u>STANDARDS AND OTHER STANDARDISATION DELIVERABLES</u> IN THE FIELD OF SECURITY

Country: Czech Republic

Contact person: Mr Jiri Kratochvil

Number	**Year of Publication**	**Title**	**English title**	**Type of standard (TEC / SYN / SEM / ORG / PER / …)**	**Security area**	**Type of industry/ type of threat**	**Users**	**Remarks/ additional info**
1	2011	ČSN 342710 Elektrická požární signalizace – Projektování, montáž, užívání, provoz, kontrola, servis a údržba	Fire detection and fire alarm systems - *planning, design, installation, commissioning, use and maintenance*	TEC	Security of the Citizens	Fire hazard	Installers, fire brigade	will be canceled after the introduction of EN 54-14

ANNEX A: SURVEY ON NATIONAL STANDARDS

TABLE 1: OVERVIEW OF NATIONAL STANDARDS AND OTHER STANDARDISATION DELIVERABLES IN THE FIELD OF SECURITY

Country: Germany

Contact person: Stefan Krebs

Document-Number	**Year of Publication**	**Title**	**English title**	**Type of standard** (TEC / SYN / SEM / ORG / PER / …)	**Security area**	**Type of industry/ type of threat**	**Users**	**Remarks/ additional info**
DIN 6280-13		Stromerzeugungsaggregate - Stromerzeugungsaggregate mit Hubkolben-Verbrennungsmotoren - Teil 13: Für Sicherheitsstromversorgung in Krankenhäusern und in baulichen Anlagen für Menschenansammlungen	Generating sets - Reciprocating internal combustion engines driven generating sets - Part 13: For emergency power supply in hospitals and public building		Restoring security and safety in case of crisis	response		
DIN 13024-1		Krankentrage - Teil 1: Mit starren Holmen; Maße, Anforderungen, Prüfung	Stretcher - Part 1: With fixed poles; dimensions, requirements, testing		Restoring security and safety in case of crisis	response		
DIN 13024-2		Krankentrage - Teil 2: Mit klappbaren Holmen; Maße, Anforderungen, Prüfung	Stretcher - Part 2: With foldable spars; dimensions, requirements, testing		Restoring security and safety in case of crisis	response		
DIN 13050		Rettungswesen - Begriffe	Emergency services - Terms and definitions		Restoring security and safety in case of crisis	response		

ANNEX A: SURVEY ON NATIONAL STANDARDS

DIN 13073		Rettungssysteme - Maße für Haltesysteme zur Arretierung von Fahrgestellen und Krankentragen im Krankenkraftwagen	Rescue systems - Dimensions for a maintain system for fastening for undercarriage and stretcher in ambulances		Restoring security and safety in case of crisis	response		
DIN 13160		Erste-Hilfe-Material - Sanitätstaschen	First aid material - Bag with shoulder strap for first aid material		Restoring security and safety in case of crisis	response		
DIN 13164		Erste-Hilfe-Material - Verbandkasten B	First aid material - First aid box B		Restoring security and safety in case of crisis	response		
DIN 13230		Luftfahrzeuge zum Patiententransport (Teile 6 und 10)	Aircrafts for the patient transport Parts 6 and 10)		Restoring security and safety in case of crisis	response		
DIN 13233		Notfall-Arztkoffer für Säuglinge und Kleinkinder	Emergency doctor kit for babies and children		Restoring security and safety in case of crisis	response		
DIN 14142		Erste-Hilfe-Material - Verbandkasten für Feuerwehrfahrzeuge	First aid material - First-aid box for fire-brigade motor cars		Security of the Citizens	fire hazard		
DIN 14405		Kübelspritzen	Bucket pump		Security of the Citizens	fire hazard		
DIN 14420		Feuerlöschpumpen - Feuerlöschkreiselpumpen - Anforderungen an die saug- und druckseitige Bestückung, Prüfung nach Einbau im Feuerwehrfahrzeug	Fire-fighting pumps - Fire-fighting centrifugal pumps - Requirements for the suction-sided and pressure-sided assembly, test after installation in the fire-fighting vehicle		Security of the Citizens	fire hazard		

ANNEX A: SURVEY ON NATIONAL STANDARDS

DIN 14424		Feuerwehrwesen - Explosionsgeschützte tragbare Umfüllpumpe mit Elektromotor - Anforderungen, Typ- und Abnahmeprüfung	Firefighting equipment - Explosion-proof portable transfer pump with electric motor - Requirements, type and acceptance test		Security of the Citizens	fire hazard		
DIN 14425		Feuerwehrwesen - Tragbare Tauchmotorpumpen mit Elektroantrieb	Fire fighting purposes - Portable submersible pumps with electrical motor		Security of the Citizens	fire hazard		
DIN 14427		Feuerwehrwesen - Explosionsgeschützte tragbare Gefahrgut-Umfüllpumpe mit Elektromotor - Anforderungen, Prüfung	Firefighting equipment - Explosion-proof portable transfer pump for dangerous fluids, with electric motor - Requirements, testing		Security of the Citizens	fire hazard		
DIN V 14430		Feuerwehrwesen - Druckzumischanlagen und Druckluftschaumanlagen	Fire fighting - Positive pressure foam systems and compressed air foam systems		Security of the Citizens	fire hazard		
DIN 14502-3		Feuerwehrfahrzeuge - Außenanstrich	Fire brigade vehicles - exterior coating		Security of the Citizens	fire hazard		
DIN 14505		Feuerwehrfahrzeuge - Wechselladerfahrzeuge mit Abrollbehältern - Allgemeine Anforderungen	Fire fighting and rescue service vehicles - Vehicles for roller containers - General requirements		Security of the Citizens	fire hazard		
DIN 14507		Einsatzleitfahrzeuge (Teile 1, 2, 3 und 5)	Command and control appliances (Parts 1, 2, 3 and 5)		Security of the Citizens	fire hazard		
DIN 14530-11		Löschfahrzeuge - Teil 11: Löschgruppenfahrzeug LF 20/16, Hilfeleistungs-Löschgruppenfahrzeug HLF 20/16	Fire-fighting vehicles - Part 11: Group pumping appliance LF 20/16, Group pumping appliance for rescue operations HLF 20/16		Security of the Citizens	fire hazard		

ANNEX A: SURVEY ON NATIONAL STANDARDS

DIN 14530-16		Löschfahrzeuge - Teil 16: Tragkraftspritzenfahrzeug TSF	Fire fighting vehicles - Part 16: Pumping appliance TSF		Security of the Citizens	fire hazard		
DIN 14530-17		Löschfahrzeuge - Teil 17: Tragkraftspritzenfahrzeug TSF-W	Fire fighting vehicle - Part 17: Pumping appliance TSF-W		Security of the Citizens	fire hazard		
DIN 14530-21		Löschfahrzeuge - Teil 21: Tanklöschfahrzeug TLF 20/40, Tanklöschfahrzeug TLF 20/40-SL	Firefighting vehicles - Part 21: Pump water tanker TLF 20/40, Pump water tanker TLF 20/40-SL		Security of the Citizens	fire hazard		
DIN 14530-24		Löschfahrzeuge - Teil 24: Kleinlöschfahrzeug KLF	Fire fighting vehicles - Part 24: Small pumping appliance KLF		Security of the Citizens	fire hazard		
DIN 14530-25		Löschfahrzeuge - Teil 25: Staffellöschfahrzeug StLF 10/6	Fire fighting vehicle - Part 25: Pumping appliance StLF 10/6		Security of the Citizens	fire hazard		
DIN 14530-5		Löschfahrzeuge - Teil 5: Löschgruppenfahrzeug LF 10/6, Hilfeleistungs-Löschgruppenfahrzeug HLF 10/6	Firefighting vehicles - Part 5: Group pumping appliance LF 10/6, Group pumping appliance for rescue operations HLF 10/6		Security of the Citizens	fire hazard		
DIN 14555-1		Rüstwagen und Gerätewagen - Teil 1: Allgemeine Anforderungen	Vehicles carrying tools and gears - Part 1: General requirements		Security of the Citizens	fire hazard		
DIN 14555-12		Rüstwagen und Gerätewagen - Teil 12: Gerätewagen Gefahrgut GW-G	Vehicles carrying tools and gears - Part 12: Damage control tender GW-G		Security of the Citizens	fire hazard		
DIN 14555-21		Rüst- und Gerätewagen - Teil 21: Gerätewagen Logistik GW-L1	Vehicles carrying tools and gears - Part 21: GW- L1 for logistic tasks		Security of the Citizens	fire hazard		
DIN 14555-22		Rüstwagen und Gerätewagen - Teil 22: Gerätewagen Logistik GW-L2	Vehicles carrying tools and gears - Part 22: GW- L2 for logistic tasks		Security of the Citizens	fire hazard		

ANNEX A: SURVEY ON NATIONAL STANDARDS

DIN 14555-3		Rüstwagen und Gerätewagen - Teil 3: Rüstwagen RW	Vehicles carrying tools and gears - Part 3: Emergency tender RW		Security of the Citizens	fire hazard		
DIN 14572		Abgasschläuche und Abgasschlauch-Anschlüsse	Exhaust gas metal hoses and couplings for exhaust gas metal hoses		Security of the Citizens	fire hazard		
DIN 14685		Tragbarer Stromerzeuger 5 kVA und 8 kVA	Portable generating set 5 kVA and 8 kVA		Security of the Citizens	fire hazard		
DIN 14687		Feuerwehrwesen - Fest eingebaute Stromerzeuger (Generatorsätze) kleiner 12 kVA für den Einsatz in Feuerwehrfahrzeugen	Firefighting equipment - Permanently installed generators (generating sets) less than 12 kVA for the use in firefighting vehicles		Security of the Citizens	fire hazard		
DIN 14811		Feuerlöschschläuche - Druckschläuche und Einbände für Pumpen und Feuerwehrfahrzeuge	Fire-fighting hoses - Non-percolating layflat delivery hoses and hose assemblies for pumps and vehicles		Security of the Citizens	fire hazard		
DIN 75079		Notarzt-Einsatzfahrzeuge (NEF) - Begriffe, Anforderungen, Prüfung	Fast emergency car for first aid by special medical doctor - Concepts, requirements, test		Restoring security and safety in case of crisis	response		
DVGW 1002		Sicherheit in der Trinkwasserversorgung - Organisation und Management im Krisenfall	Safe and Secure Drinking Water Supply - Organisation and Management in the Event of a Crisis		Restoring security and safety in case of crisis	Preparedness and planning		
DVGW G 1000		Anforderungen an die Qualifikation und die Organisation von Unternehmen für den Betrieb von Anlagen zur leitungsgebundenen Versorgung der Allgemeinheit mit Gas (Gasversorgungsanlagen)			Restoring security and safety in case of crisis	Preparedness and planning		

ANNEX A: SURVEY ON NATIONAL STANDARDS

DVGW G 1001		Sicherheit in der Gasversorgung - Management von Risiken im Normalbetrieb			Restoring security and safety in case of crisis	Preparedness and planning		
DVGW G 1002		Sicherheit in der Gasversorgung - Organisation und Management im Krisenfall			Restoring security and safety in case of crisis	Preparedness and planning		
DVGW W 1000		Anforderungen an die Qualifikation und die Organisation von Trinkwasserversorgern	Requirements on the qualification and organisation of drinking water suppliers		Restoring security and safety in case of crisis	Preparedness and planning		
DVGW W 1001		Sicherheit in der Trinkwasserversorgung - Risikomanagement im Normalbetrieb	Safe and Secure Drinking Water Supply - Risk Management Under Normal Operating Conditions		Restoring security and safety in case of crisis	Preparedness and planning		
DIN SPEC (PAS) 91291	2013	Notfallkonzept für sensible Logistikagglomerationen - Konfiguration, Simulation und Implementierung	Emergency concept for sensitive logistics hubs - configuration, simulation and implementation		Security of infrastructures and utilities, restoring security and safety in case of crisis	transport, supply chains, preparedness and planning, response, recovery	Carrier of logistic agglomerations for example operator of distribution facilities, traffic management offices and cargo transport centre	
DIN SPEC (PAS) 91284	2012	Grundlagen mikroskopischer Entfluchtungssimulationen	Principles of microscopic evacuation simulations		Security of infrastructures and utilities	Building design	security management	

ANNEX A: SURVEY ON NATIONAL STANDARDS

DIN SPEC (PAS) 91282	2012	Terminologie für das Sicherheitsmanagement von Verkehrsinfrastrukturen	Terminology for security management of public transport infrastructures		Security of infrastructures and utilities	communication grids	security management	
DIN SPEC (PAS) 91287	2012	Datenaustausch zwischen Informationssystemen in der zivilien Gefahrenabwehr	Data interchange between information systems in civil hazard prevention		Security of infrastructures and utilities	communication grids	interface operators, control operators	
DIN SPEC (PAS) 91285	2012	Gesamtheitliche Beschreibung von Sicherheitsprozessen	Holistic characterisation of security processes		Security of infrastructures and utilities	surveillance	security management	
DIN VDE 0833-1 (VDE 0833-1)-1 bis 4	Part_1 & 3: 2009-09, Part_2: 2009-06, Part_4: 2007-09	Gefahrenmeldeanlagen für Brand, Einbruch und Überfall – Teil 1 – 4		TEC	Security of infrastructures and utilities	Building design		
DIN V VDE 0826-1 (VDE V 0826-1)-5	2005-06	Überwachungsanlagen – Teil 1: Gefahrenwarnanlagen (GWA) für Wohnhäuser, Wohnungen und Räume mit wohnungsähnlicher Nutzung – Planung, Einbau, Betrieb und Instandhaltung		TEC	Security of infrastructures and utilities	Building design		
DIN VDE 0834-1 (VDE 0834-1)-6	2000-04	Rufanlagen in Krankenhäusern, Pflegeheimen und ähnlichen Einrichtungen – Teil 1: Geräteanforderungen, Errichten und Betrieb		TEC	Security of infrastructures and utilities	Building design		
DIN VDE 0834-2 (VDE 0834-2)-7	2000-04	Rufanlagen in Krankenhäusern, Pflegeheimen und ähnlichen Einrichtungen – Teil 2: Umweltbedingungen und Elektromagnetische Verträglichkeit		TEC	Security of infrastructures and utilities	Building design		
DIN V VDE V 0825-1 (VDE V 0825-1)-8	2004-08	Überwachungsanlagen – Drahtlose Personen–Notsignal–Anlagen für gefährliche Alleinarbeiten – Teil 1: Geräte– und Prüfanforderungen		TEC	Security of infrastructures and utilities	surveillance		

ANNEX A: SURVEY ON NATIONAL STANDARDS

DIN V VDE V 0825-11 (VDE V 0825-11)-9	2007-12	Überwachungsanlagen – Drahtlose Personen-Notsignal-Anlagen für gefährliche Alleinarbeiten – Teil 11: Geräte- und Prüfanforderungen für Personen-Notsignal-Anlagen unter Nutzung öffentlicher Telekommunikationsnetze		TEC	Security of infrastructures and utilities	surveillance		
DIN 77200	2008-05	Sicherungsdienstleistungen – Anforderungen	Static guarding and mobile patrol services - Requirements		Security of the Citizens	Services		

OVERVIEW NATIONAL STANDARDS THE NETHERLANDS

Please find below an overview of national standards related to societal security in the Netherlands.

Committee	Standard no.	Title / Titel	Type of standard	Security area	Type of industry/ type of threat	Users	Remarks/additional information
Societal Security	NEN 7131:2010	Societal security - Security, preparedness and continuity management systems - Requirements with guidance for use	ORG	Restoring safety and security in case of crisis	Preparedness and planning	All companies and institutions who need to manage their processes to be prepared for incidents and to enhance resillience	
Societal Security	NEN 7132:2008 Ontw.	Societal security - Guidelines for auditing security, preparedness, and continuity management systems with guidance for use	ORG	Restoring safety and security in case of crisis	Preparedness and planning	All companies and institutions who need to manage their processes to be prepared for incidents and to enhance resillience	
Pipelines	NTA 8000:2009	Specification of a Risk Management System (RMS) for pipeline systems for the transport of hazardous substances during operations	ORG	Security of infrastructure and utilities	energy/transport	Transport of energy (critical infrastructure), supply chain	

ANNEX A: SURVEY ON NATIONAL STANDARDS

Hydrogen fuelling stations	NPR 8099:2010	Hydrogen fuelling stations - Guide for safe application of installations for delivery of hydrogen to vehicles and boats with respect to fire, workplace and environment	TEC	Security of the Citizens	energy/transport	Hydrogen fueling stations, local authorities	
Functional requirements drinking water supply	NEN 1006:2007 Concept	General requirements for water supply installations	PER	Security of infrastructure and utilities	supply chains	water supply companies and other actors in the supply chain	
Fire safety of buildings	NEN 1775:1991/C2:1992	Determination of the contribution to fire propagation of floor surfaces	MTV	Security of the Citizens	fire hazard	fire safety authorities, construction sector	
Fire safety of buildings	NEN 3122:1958	Regulations for fire protection of buildings - Part 3: Regulation for garages	PER	Security of the Citizens	fire hazard	fire safety authorities, construction sector	public garages and parking structures
Fire safety of buildings	NEN 3891:1971	Regulations for fire protection of buildings - Part 1: General part	PER	Security of the Citizens	fire hazard	fire safety authorities, construction sector	
Fire safety of buildings	NEN 6050:2009	Conditions for design of fire safety during work on roofs - Roofs with roof waterproofing sheets	TEC	Security of the Citizens	fire hazard	fire safety authorities, construction sector	
Fire safety of buildings	NEN 6065:1991/C1:1992	Determination of the contribution to fire propagation of building products	MTV	Security of the Citizens	fire hazard	fire safety authorities, construction sector	
Fire safety of buildings	NEN 6066:1991/C1:1992	Determination of the smoke production during fire of building products	MTV	Security of the Citizens	fire hazard	fire safety authorities, construction sector	
Fire safety of buildings	NEN 6068:2008	Determination of the resistance to fire movement between spaces	MTV	Security of the Citizens	fire hazard	fire safety authorities, construction sector	
Fire safety of buildings	NEN 6069:1991/C1:1992	Determination of the fire resistance of elements of building constructions	MTV	Security of the Citizens	fire hazard	fire safety authorities, construction sector	
Fire safety of buildings	NEN 6076:1991/C1:1992	Experimental determination of the fire resistance of ventilation ducts without dampers	MTV	Security of the Citizens	fire hazard	fire safety authorities, construction sector	
Fire safety of buildings	NEN 6090:2006	Determination of fire load	MTV	Security of the Citizens	fire hazard	fire safety authorities, construction sector	
Fire safety of buildings	NPR 6059:2009	Scan fire safety of buildings	TEC	Security of the Citizens	fire hazard	fire safety authorities, construction sector	
Fire safety of buildings	NPR 6091:2009	Resistance against external fire spread	TEC	Security of the Citizens	fire hazard	fire safety authorities, construction sector	
Fire safety of buildings	NVN 6050:2006	Requirements on design and detailing for fire safety during working on roofs - Roofs with roof waterproofing sheets	PER	Security of the Citizens	fire hazard	fire safety authorities, construction sector	

ANNEX A: SURVEY ON NATIONAL STANDARDS

Burglary resistance of facades	NEN 5096:2007+C1 :2007	Burglary resistance - Façade elements with doors, windows, shutters and fixed infillings - Requirements, classification and test methods	PER/MTV	Security of the Citizens	organised crime	public safety authorities, installation sector	
Alarm systems	NEN 10839-2-2:1989	Alarm systems - Part 2: Requirements for intruder alarm systems:Section Two: General requirements for detectors	PER	Security of the Citizens	organised crime	public safety authorities, installation sector	
Alarm systems	NPR 8136:2011	Alarm transmission using IP-networks - Guidance for design, installation, inspection and maintenance, based on NEN-EN 50136-1	TEC	Security of the Citizens	organised crime	public safety authorities, installation sector	
Entertainment	NEN 8020-20:2011	Entertainment - Electrical installations	PER	Security of the Citizens	fire hazard	public safety authorities, installation sector	
Entertainment	NTA 8020-30:2004	Event security and crowd management services	ORG	Security of the Citizens	counter terrirism	public safety authorities, event organisers	
Ships and maritme techniques	NEN 3333:1993	Symbols for safety plans of ships	TEC	Security of the Citizens	fire hazard	maritime and inland vessel safety authorities, installation sector	
Ships and maritme techniques	NEN 3333:1993/C1: 1993	Symbols for safety plans of ships	TEC	Security of the Citizens	fire hazard	maritime and inland vessel safety authorities, installation sector	
Safety requirements for low-voltage installations	NEN 1010:2007+C1 :2008	Safety requirements for low-voltage installations	SEM, TEC, PER, MTV	Security of the Citizens	fire hazard	fire safety authorities, installation sector	
Safety requirements for low-voltage installations	NEN 3410:1987	Safety requirements for high-voltage and low-voltage installations in potentially explosive gas atmospheres	PER	Security of the Citizens	fire hazard	fire safety authorities, installation sector	
Safety requirements for low-voltage installations	NEN 3410:1987/C1: 1988	Safety requirements for high-voltage and low-voltage installations in potentially explosive gas atmospheres	PER	Security of the Citizens	explosives	fire safety authorities, installation sector	
Safety requirements for low-voltage installations	NEN 5237:1995	Safety provisions for electric fencing systems	PER	Security of the Citizens	fire hazard	public safety authorities, installation sector	

ANNEX A: SURVEY ON NATIONAL STANDARDS

Safety requirements for low-voltage installations	NTA 8010:2001	Electrical installations for houses	PER	Security of the Citizens	fire hazard	fire safety authorities, installation sector	
Safety requirements for low-voltage installations	NTA 8011:2002	Safety requirements for low-voltage installations - Solar photovoltaic (PV) power supply systems	PER	Security of the Citizens	fire hazard	fire safety authorities, installation sector	
Safety requirements for low-voltage installations	NTA 8012:2003	Limitation of the damage due to fire of electrical wiring systems or flame spread along electrical wiring systems	TEC	Security of the Citizens	fire hazard	fire safety authorities, installation sector	
IT security	NEN 7799-2:2004	Information security management systems - Specification with guidance for use	ORG	Security of the Citizens	organised crime	ICT sector	
IT security	NEN 7799-3:2006	Information security management systems - Part 3: Guidelines for information security risk management (BS 7799-3:2006)	ORG	Security of the Citizens	organised crime	ICT sector	
IT security	NTA 9040-1:2011 Concept	Business records - Part 1: General	TEC	Security of the Citizens	organised crime	ICT sector	
IT security	NTA 9040-2:2011 Concept	Business records - Part 2: Regulation assistance	TEC	Security of the Citizens	organised crime	ICT sector	
IT security	NTA 9040-3:2011 Concept	Business records - Part 3: Reporting and request	TEC	Security of the Citizens	organised crime	ICT sector	
IT security	NTA 9040-4:2011 Concept	Business records - Part 4: Inspection	TEC	Security of the Citizens	organised crime	ICT sector	
IT security	NTA 9040-5:2011 Concept	Business records - Part 5: Business applications	TEC	Security of the Citizens	organised crime	ICT sector	
Health informatics	NEN 7510:2004	Health Informatics - Information security in the Healthcare Sector - General	ORG	Security of the Citizens	organised crime	health care institutions, ICT sector	
Health informatics	NEN 7510:2010 Ontw.	Health Informatics - Information security management in health	ORG	Security of the Citizens	organised crime	health care institutions, ICT sector	
Health informatics	NEN 7511-1	Health informatics – Information security in the healthcare sector – Specification for use of NEN 7510 in complex	ORG	Security of the Citizens	organised crime	health care institutions, ICT sector	

ANNEX A: SURVEY ON NATIONAL STANDARDS

		organisations					
Health informatics	NEN 7511-2	Health informatics - Information security in the healthcare sector - Specification for use of NEN 7510 in cooperating practices	ORG	Security of the Citizens	organised crime	health care institutions, ICT sector	
Health informatics	NEN 7511-3	Health informatics - Information security in the healthcare sector - Specification for use of NEN 7510 in one-man practices	ORG	Security of the Citizens	organised crime	health care institutions, ICT sector	
Health informatics	NEN 7512:2005	Health informatics - Information security in the healthcare sector - Basis for trust for exchange of data	ORG	Security of the Citizens	organised crime	health care institutions, ICT sector	
Health informatics	NEN 7513:2010	Health informatics - Recording actions on electronic patient health records	ORG	Security of the Citizens	organised crime	health care institutions, ICT sector	
In-company emergency services	NEN 4000:2008	In-company emergency services	ORG	Restoring safety and security in case of crisis	Preparedness and planning	site managers, occupational health & safety officers, service providers	
In-company emergency services	NEN 8112: 2010	Guidance on evacuation schemes for buildings	ORG	Restoring safety and security in case of crisis	Preparedness and planning	site managers, occupational health & safety officers, service providers	
Fire fighting equipment - Portable and mobile fire extinguishers	NEN 4001+C1:2008	Fire protection - Planning of portable and mobile fire extinguihers	TEC, ORG	Security of the Citizens	fire hazard	site managers, occupational health & safety officers, fire safety engineers	
Safety colours and safety signs	NEN 1414:2007	Symbols for safety precautions on escape and rescue plans	TEC, ORG	Security of the Citizens	fire hazard	site managers, occupational health & safety officers	
Safety colours and safety signs	NEN 3011:2004 (+C1:2007)	Safety colours and safety signs in workplaces and public areas	PER	Security of the Citizens	fire hazard	site managers, occupational health & safety officers, manufacturers	
Safety colours and safety signs	NEN 3050:1972 (+C1: 2002)	Identification colours for pipes conveying fluids in liquid or gaseous condition in land installations	TEC	Security of the Citizens	fire hazard	site managers, occupational health & safety officers	

ANNEX A: SURVEY ON NATIONAL STANDARDS

Safety colours and safety signs	NEN 6088:2002	Fire safety of buildings - Escape route signs - Characteristics	TEC, PER	Security of the Citizens	fire hazard	site managers, occupational health & safety officers, manufacturers	
Personal protective equipment - Protective clothing NPR 3471	NPR 3471:2003	Selection, care, use and maintenance of high visibility protective clothing	TEC	Restoring safety and security in case of crisis	Preparedness and planning	occupational health & safety officers	
Personal protective equipment - Protective clothing NPR 3471	NPR/CEN/TR 15419:2006	Protective clothing – Guidelines for selection, use, care and maintenance of chemical protective clothing	TEC	Restoring safety and security in case of crisis	CBRN	occupational health & safety officers	

ANNEX B:
OVERVIEW OF EUROPEAN STANDARDS INCLUDING COMMENTS FROM SURVEY

ANNEX B: OVERVIEW OF INTERNATIONAL STANDARDS INCLUDING COMMENTS FROM SURVEY

OVERVIEW OF EUROPEAN STANDARDS

Please note that the *italic* documents refer to work in development and NOT published standards.

Publication no.	Publication no.	TC no.	Category	Remarks / Topics
EN 15975-1	Security of drinking water supply - Guidelines for risk and crisis management - Part 1: Crisis management	CEN/TC 164	Energy	
prEN 15975-2	*Security of drinking water supply - Guidelines for risk and crisis management - Part 2: Risk management*	*CEN/TC 164*	*Energy*	
prEN 16348	*Gas infrastructure - Safety Management System (SMS) for gas transmission infrastructure and Pipeline Integrity Management System (PIMS) for gas transmission pipelines - Functional requirements*	*CEN/TC 234*	*Energy*	*Merger of current TS 15173:2006 and TS 15174:2006* *Management of emergency situations, Emergency preparedness and response (EPR)* *procedures* *Quick restoration of the gas supply* *Public security during construction and* *Continuous monitoring and control of the gas system*
EN 1594	Gas infrastructure - Pipelines for maximum operating pressure up to and including 16 bar - Functional requirements	CEN/TC 234	Energy	Rev 2011/12 in process Design, construction, operation, repair and maintenance Emergency planning/intervention
EN 12007-1	Gas infrastructure - Pipelines for maximum operating pressure up to and including 16 bar - Part 1: General functional requirements	CEN/TC 234	Energy	Rev 2011/12 in process Design, construction, operation, repair and maintenance Emergency planning/intervention Quality and safety management
prEN 12007-5	*Gas Infrastructure - Part 5: Service Lines*	*CEN/TC 234*	*Energy*	*Emergency procedure* *Emergency isolation*
CEN/TS 13599		CEN/TC 234	Energy	Start of revision planned for 2012 Emergency management, including preparedness and response
EN 12583	Gas infrastructure - Compressor stations - Functional requirements	CEN/TC 234	Energy	Rev 2011/12 in process (including consideration of network security and reliability EU Reg 715)
EN 12186	Gas infrastructure - Gas pressure regulating stations for transmission and distribution - Functional requirements	CEN/TC 234	Energy	Rev 2011/12 in process
EN 1775	Gas supply - Gas pipework for buildings - Maximum operating pressure less than or equal to 5 bar - Functional recommendations	CEN/TC 234	Energy	Protection against fire
EN 15001-1	Gas Supply Systems - Gas installation pipework with an operating pressure greater than 0,5 bar for industrial, commercial and non-domestic gas installations - Part 1: Detailed functional requirements for design, materials, construction, inspection and testing	CEN/TC 234	Energy	Isolation in an emergency Protection against mechanical damage
EN 15001-2	Gas supply systems - Gas installation pipework with an operating pressure greater than 0,5 bar for industrial, commercial and non-	CEN/TC 234	Energy	Emergency procedures Isolation of pipework in an emergency

ANNEX B: OVERVIEW OF INTERNATIONAL STANDARDS INCLUDING COMMENTS FROM SURVEY

	domestic gas installations - Part 2: Detailed functional requirements for commissioning, operation and maintenance			
EN 1918-1	Gas supply systems - Underground gas storage - Part 1: Functional recommendations for storage in aquifers	CEN/TC 234	Energy	In revision Emergency procedures
EN 1918-2	Gas supply systems - Underground gas storage - Part 2: Functional recommendations for storage in oil and gas fields	CEN/TC 234	Energy	In revision Emergency procedures
EN 1918-3	Gas supply systems - Underground gas storage - Part 3: Functional recommendations for storage in solution-mined salt cavities	CEN/TC 234	Energy	In revision Emergency procedures
EN 1918-4	Gas supply systems - Underground gas storage - Part 4: Functional recommendations for storage in rock caverns	CEN/TC 234	Energy	In revision Emergency procedures
EN 1918-5	Gas supply systems - Underground gas storage - Part 5: Functional recommendations for surface facilities	CEN/TC 234	Energy	In revision Emergency procedures
ENV 12924	Medical Informatics – Security Categorisation and Protection for Healthcare Information Systems	CEN/TC 251	medical	
CR 13694	Health Informatics – Safety and Security Related Software Quality Standards for Healthcare (SSQS)	CEN/TC 251	medical	
ENV 13729	Health informatics – Secure user identification – Strong authentication using microprocessor cards	CEN/TC 251	medical	
CR 14301	Health informatics – Framework for security protection of healthcare communication	CEN/TC 251	medical	
CR 14302	Health informatics – Framework for security requirements for intermittently connected devices	CEN/TC 251	medical	
EN 14484	Health informatics – International transfer of personal health data covered by the EU data protection directive – High level security policy	CEN/TC 251	medical	
EN 14485	Health informatics – Guidance for handling personal health data in international applications in the context of the EU data protection directive	CEN/TC 251	medical	
EN 12251	Health informatics – Secure User Identification for Health Care – Management and Security of Authentication by Passwords	CEN/TC 251	medical	
CEN/TR 15299	Health Informatics – Safety procedures for identification of patients and related objects	CEN/TC 251	medical	
CEN/TR 15300	Health Informatics – Framework for formal modelling of healthcare security policies	CEN/TC 251	medical	
CEN/TS 15260	Health informatics – Classification of safety risks from health information products	CEN/TC 251	medical	
EN 13606-4	Health informatics – Electronic health record communication – Part 4: Security	CEN/TC 251	medical	
CEN/TR 15640	Health informatics – Measures for ensuring the patient safety of health software	CEN/TC 251	medical	
EN ISO 27799	Health informatics – Information security management in health using ISO/IEC 27002	CEN/TC 251	medical	

ANNEX B: OVERVIEW OF INTERNATIONAL STANDARDS INCLUDING COMMENTS FROM SURVEY

prEN ISO/DIS 27789	*Health informatics – Audit trails for electronic health records*	*CEN/TC 251*	*medical*	
prEN ISO/DIS 21091	*Health informatics -- Directory services for health care providers, subjects of care, and other entities*	*CEN/TC 251*	*medical*	
prCEN ISO/TS 14265	*Health Informatics - Classification of purposes for processing personal health information*	*CEN/TC 251*	*medical*	
prCEN ISO/TS 14441-1	*Health informatics – Security and privacy requirements for compliance testing of EHR systems -Part 1: Foundation*	*CEN/TC 251*	*medical*	
prCEN ISO/TS 14441-2	*Health informatics – Security and privacy requirements for compliance testing of EHR systems -Part 2: Protection profile for small-scale electronic patient record systems*	*CEN/TC 251*	*medical*	
CEN ISO/TS 17574	Electronic fee collection - Guidelines for security protection profiles (ISO/TS 17574:2009)	CEN/TC 278	medical	
Amendment 1 on prEN 13757-3:2011	*Communication systems for and remote reading of meters - Part 3: Dedicated application layer*	*CEN/TC 294*	*Energy*	*Providing the scope extension will be approved by CEN/BT, the working group CEN/TC 294/WG 4 will elaborate an Amendment to prEN 13757-3:2011, to include applications requiring data security, data integrity, authentication and confidentiality. The preparatory work on the Amendment 1 to prEN 13757-3 will start in 2012.*
EN 14383-1	English Prevention of crime - Urban planning and building design - Part 1: Definition of specific terms	CEN/TC 325	building design	Terminology can be used for other standards.
CEN/TR 14383-2	Prevention of crime - Urban planning and building design - Part 2: Urban planning	CEN/TC 325	building design	Standard can be referenced in other security standards
CEN/TR 14383-5	Prevention of crime - Urban planning and building design - Part 5: Petrol stations	CEN/TC 325	building design	Standard can be referenced in other security standards
CEN/TR 14383-7	Prevention of crime - Urban planning and building design - Part 7: Design and management of public transport facilities	CEN/TC 325	building design	Standard can be referenced in other security standards
CEN/TR 14383-8	Prevention of crime - Urban planning and building design - Part 8: Protection of buildings and sites against criminal attacks with vehicles	CEN/TC 325	building design	Standard can be referenced in other security standards
CEN/TS 14383-3	Prevention of crime - Urban planning and building design - Part 3: Dwellings	CEN/TC 325	building design	Standard can be referenced in other security standards Note: standard is under revision, new version to be issued as TR
CEN/TS 14383-4	Prevention of crime - Urban planning and design - Part 4: Shops and offices	CEN/TC 325	building design	Standard can be referenced in other security standards Note: standard is to be changed into TR
FprEN 16029	*Ride-on, motorized vehicles intended for the transportation of persons and not intended for use on public roads - Single-track two-wheel motor vehicles - Safety requirements and test methods*	*CEN/TC 354*	*medical*	

ANNEX B: OVERVIEW OF INTERNATIONAL STANDARDS INCLUDING COMMENTS FROM SURVEY

EN 16082	Airport and aviation security services	CEN/TC 384	air	
	NWI: Security management system for healthcare facilities	*CEN/TC 391*	*Preparedness & planning*	
	NWI: CBRN - Vulnerability assessment and protection of the population at risk	*CEN/TC 391*	*CBRN*	
	NWIP on "Ship, port and maritime-related security services"	*CEN/TC 417*	*sea*	
CWA 15537	Network Enabled Abilities - Service-Oriented Architecture for civilian and military crisis management	CEN	building design	
CWA 15931-1	Disaster and emergency management - Shared situation awareness - Part 1: Message structure	CEN	response	
CWA 15931-2	Disaster and emergency management - Shared situation awareness - Part 2: Codes for the message structure	CEN	response	
prEN 16352	*Logistics - Specifications for reporting crime incidents*	*CEN*	*response*	
prEN ISO 7010	*Graphical symbols - Safety colours and safety signs - Safety signs used in workplaces and public areas (ISO 7010:2003 including Amd 1:2006 and Amd 2:2007)*	*CEN*	*response*	
EN 50132-7	Alarm systems - CCTV surveillance systems for use in security applications - Part 7: Application guidelines	CLC/TC 79	preparedness	
EN 50133-7	Alarm systems - Access control systems for use in security applications - Part 7: Application guidelines	CLC/TC 79	preparedness	
prEN 50132-7	*Alarm systems - CCTV surveillance systems for use in security applications - Part 7: Application guidelines*	*CLC/TC 79*	*preparedness*	
232	Glossary of security terminology	-	Preparedness	Security terminology and glossaries
3G TS 32.371	Telecommunication management; Security Management concept and requirements	3GPP	Preparedness	Security management standards and guidance documents
3G TS 32.372	Telecommunication management; Security services for Integration Reference Point (IRP); Information Service (IS)	3GPP	Preparedness	Security management standards and guidance documents
3G TS 32.373	Telecommunication management; Security services for Integration Reference Point (IRP); Common Object Request Broker Architecture (CORBA) solution	3GPP	Preparedness	Security management standards and guidance documents
3G TS 32.375	Telecommunication management; Security services for Integration Reference Point (IRP); File integrity solution	3GPP	Preparedness	Integrity mechanisms; Security management standards and guidance documents; Security mechanisms; Security services
3GPP TR 33.901	Universal Mobile Telecommunications System (UMTS); 3G Security Criteria for cryptographic Algorithm design process	3GPP	Preparedness	General ICT security guidance documents
3GPP TR 33.902	Universal Mobile Telecommunications System (UMTS); Formal Analysis of the 3G Authentication Protocol	3GPP	Preparedness	General ICT security guidance documents
3GPP TR 33.908	Universal Mobile Telecommunications System (UMTS); Security Algorithms Group of Experts (SAGE); General report on the design,	3GPP	Preparedness	General ICT security guidance documents

ANNEX B: OVERVIEW OF INTERNATIONAL STANDARDS INCLUDING COMMENTS FROM SURVEY

	specification and evaluation of 3GPP standard confidentiality and integrity algorithms			
3GPP TR 33.909	Universal Mobile Telecommunications System (UMTS); 3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions	3GPP	Preparedness	General ICT security guidance documents
3GPP TR 33.941	Presence service; Security	3GPP		General ICT security guidance documents
3GPP TR 33.978	Universal Mobile Telecommunications System (UMTS); Security aspects of early IMS	3GPP	Preparedness	General ICT security guidance documents
TR 102 780 V1.1.1	Methods for Testing and Specification (MTS);Security; Guide to the use of methods in development of ETSI security standards	-	Methodology	General ICT security guidance documents

OVERVIEW OF WORLDWIDE STANDARDS

Please note that the *italic* documents refer to work in development and NOT published standards.

Publication no.	Publication no.	TC no.	Category	Remarks / Topics
ISO 28004	Security management systems for the supply chain - Guidelines for the implementation of ISO 28000	ISO/TC 8	supply chain	
ISO CD 11208	*Ships and marine technology - Large Yachts – Windows and portlights – Security requirements*	*ISO/TC 8*	*sea*	*This item, for the time being, has been deleted from the work programme, waiting for a possible enlargement of the field of application (not only windows and portlights). Today there are no other items in TC 8 SC12 dealing with the security, even if the problem is well known at TC 8 level. In case of restarting of an item about the security a liaison with ISO TC 223 and CEN TC 391 should be evaluated.*
ISO 6546	Road vehicles - Collection of accident data for evaluation of occupant restraint performance	ISO/TC 22	transport	
ISO 12353-1	Road vehicles - Traffic accident analysis - Part 1: Vocabulary	ISO/TC 22	transport	
ISO 12353-2	Road vehicles - Traffic accident analysis - Part 2: Guidelines for the use of impact severity measures	ISO/TC 22	transport	
ISO 13218	Road vehicles - Child restraint systems - Report form for accidents involving child passengers	ISO/TC 22	transport	
ISO 13232-2	Motorcycles - Test and analysis procedures for research evaluation of rider crash protective devices fitted to motorcycles - Part 2: Definition of	ISO/TC 22	transport	

ANNEX B: OVERVIEW OF INTERNATIONAL STANDARDS INCLUDING COMMENTS FROM SURVEY

	impact conditions in relation to accident data			
ISO 19092	Financial services - Biometrics - Security framework	ISO/TC 68	Financial	
ISO/TR 13569	Financial services - Information security guidelines	ISO/TC 68	Financial	
ISO/TR 9564-4	Banking - Personal Identification Number (PIN) management and security - Part 4: Guidelines for PIN handling in open networks	ISO/TC 68	Financial	
ISO 27467	Nuclear criticality safety - Analysis of a postulated criticality accident	ISO/TC 85	nuclear	
ISO 20712-1	Water safety signs and beach safety flags - Part 1: Specifications for water safety signs used in workplaces and public areas	ISO/TC 145	Energy	
ISO 28901	Soil quality - Guidance for burial of animal carcasses to prevent epidemics	ISO/TC 190	recovery	
ISO/TS 17574	Electronic fee collection - Guidelines for security protection profiles	ISO/TC 204	organized crime	
ISO/TR 21548	Health informatics - Security requirements for archiving of electronic health records - Guidelines	ISO/TC 215	medical	
ISO/PAS 22399	Societal security - Guideline for incident preparedness and operational continuity management	ISO/TC 223	preparedness	
ISO/TR 22312	Societal security - Technological capabilities	ISO/TC 223	Methodology	
ISO 22300	*Societal security – Terminology*	*ISO/TC 223*	*Methodology*	
ISO 22301	*Societal security – Business continuity management systems - Requirements*	*ISO/TC 223*	*recovery*	
ISO 22311	*Societal security – Video surveillance – Export interoperability*	*ISO/TC 223*	*preparedness*	
ISO 22313	*Societal security – Business continuity management systems - Guidance*	*ISO/TC 223*	*recovery*	
ISO 22315	*Societal security – Mass evacuation*	*ISO/TC 223*	*response*	
ISO 22320	*Societal security – Emergency management – Incident response*	*ISO/TC 223*	*response*	
ISO 22322	*Societal security – Emergency management – Public warning systems*	*ISO/TC 223*	*preparedness*	
ISO 22323	*Societal security – Organizational resilience management systems – Requirements*	*ISO/TC 223*	*preparedness*	
ISO 22324	*Societal security – Emergency management – Colour coded alert*	*ISO/TC 223*	*preparedness*	
ISO 22351	*Societal security – Emergency management – Shared situation awareness*	*ISO/TC 223*	*preparedness*	
ISO 22352	*Societal security – Emergency management – Shared situation awareness part 2*	*ISO/TC 223*	*preparedness*	
ISO 22397	*Societal security – Public private partnerships – Guidelines to set up partnership agreements*	*ISO/TC 223*	*preparedness*	
ISO 22398	*Societal security – Guidelines for exercises and testing*	*ISO/TC 223*	*preparedness*	
ISO/CD 11830	*Crisis management of water utilities*	*ISO/TC 224*	*Energy*	
ISO 12931	*Performance criteria for authentication solutions used to combat counterfeiting of material goods*	*ISO/TC 246*	*counter terrorism*	
ISO WD 16125	Fraud Countermeasures and Controls-Security Management System	ISO/TC 247	organized crime	
ISO WD 16678	Anti-counterfeiting track and trace method using unique identifier numbering	ISO/TC 247	organized crime	

ANNEX B: OVERVIEW OF INTERNATIONAL STANDARDS INCLUDING COMMENTS FROM SURVEY

IWA 6	Guidelines for the management of drinking water utilities under crisis conditions	ISO	energy	
ISO/IEC Draft Guide 81	*Guidelines for the inclusion of security aspects in standards*	*ISO*	*general*	
ISO/IEC TR 14516	Information technology - Security techniques - Guidelines for the use and management of Trusted Third Party services	ISO/IEC JTC 1	techniques	
ISO/IEC 13335-1	Management of information and communications technology security (MICTS) Part 1: Concepts and models for information and communications technology security management	ISO/IEC JTC 1/SC 27	preparedness	
ISO/IEC 13335-2	Guidelines for the management of IT security Part 2: Managing and planning IT security	ISO/IEC JTC 1/SC 27	preparedness	
ISO/IEC 13335-3	Guidelines for the management of IT security (GMITS) Part 3: Techniques for the management of IT security	ISO/IEC JTC 1/SC 27	preparedness	
ISO/IEC 13335-4	Guidelines for the management of IT security (GMITS) Part 4: Selection of safeguards	ISO/IEC JTC 1/SC 27	preparedness	
ISO/IEC 13335-5	Guidelines for the management of IT security (GMITS) Part 5: Management guidance on network security	ISO/IEC JTC 1/SC 27	preparedness	
ISO/IEC 15408-1	Evaluation criteria for IT security Part 1: Introduction and general model. (Draft Technical Corrigendum 1 to be incorporated into the 2nd edition of 15408-1)	ISO/IEC JTC 1/SC 27	preparedness	
ISO/IEC 15408-2	Evaluation criteria for IT security Part 2: Security functional requirements. (Draft Technical Corrigendum 1 to be incorporated into the 2nd edition of 15408-2)	ISO/IEC JTC 1/SC 27	preparedness	
ISO/IEC 18044	Information security incident management	ISO/IEC JTC 1/SC 27	response	
ISO/IEC 24761	Information technology - Security techniques - Authentication context for biometrics	ISO/IEC JTC 1/SC 27	techniques	
ISO/IEC 24762	Information technology - Security techniques - Guidelines for information and communications technology disaster recovery services	ISO/IEC JTC 1/SC 27	techniques	
ISO/IEC 27000	Information security management systems Fundamentals and vocabulary	ISO/IEC JTC 1/SC 27	preparedness	
ISO/IEC 27001	Information security management systems Requirements	ISO/IEC JTC 1/SC 27	preparedness	
ISO/IEC 27002 (Formerly 17799 First edition)	Code of practice for information security management	ISO/IEC JTC 1/SC 27	preparedness	
ISO/IEC 27003	Information security management system implementation guidance	ISO/IEC JTC 1/SC 27	preparedness	
ISO/IEC 27004	Information security management measurements	ISO/IEC JTC 1/SC 27	preparedness	
ISO/IEC 27005	Management of information and communications technology security	ISO/IEC JTC	preparedness	

ANNEX B: OVERVIEW OF INTERNATIONAL STANDARDS INCLUDING COMMENTS FROM SURVEY

	(MICTS) Part 2: Techniques for information and communications technology security risk management	1/SC 27		
ISO/IEC 27006	International accreditation guidelines for the accreditation of bodies operating certification / Registration of information security management systems	ISO/IEC JTC 1/SC 27	preparedness	
ISO/IEC 27007	Information technology - Security techniques - Guidelines for information security management systems auditing	ISO/IEC JTC 1/SC 27	preparedness	
ISO/IEC 27011	Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	ISO/IEC JTC 1/SC 27	preparedness	
ISO/IEC 27031	Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity	ISO/IEC JTC 1/SC 27	recovery	
ISO/IEC 27033-3	Network security - Part 3: Reference networking scenarios - Threats, design, technologies and control issues	ISO/IEC JTC 1/SC 27	techniques	
ISO/IEC 27035	Information security incident management	ISO/IEC JTC 1/SC 27	response	
ISO/IEC TR 27008	Information technology - Security techniques - Guidelines for auditors on information security controls	ISO/IEC JTC 1/SC 27	preparedness	
ISO/IEC DIS 27013	*Information technology - Security techniques - Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*	*ISO/IEC JTC 1/SC 27*	*techniques*	
ISO/IEC DIS 27037	*Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence*	*ISO/IEC JTC 1/SC 27*	*techniques*	
ISO/IEC 19792	Information technology - Security techniques - Security evaluation of biometrics	ISO/IEC JTC 1/SC 27	techniques	
ISO/IEC TR 15446	Information technology - Security techniques - Guide for the production of Protection Profiles and Security Targets	ISO/IEC JTC 1/SC 27	techniques	
ISO/IEC TR 24729-4	Information technology - Radio frequency identification for item management - Implementation guidelines - Part 4: Tag data security	ISO/IEC JTC 1/SC 31	techniques	
ISO/IEC 24713-1	Biometric profiles for interoperability and data interchange -- Part 1: Overview of biometric systems and biometric profiles	ISO/IEC JTC 1/SC37	biometrics	
ISO/IEC 24713-2	Biometric profiles for interoperability and data interchange -- Part 2: Physical access control for employees at airports	ISO/IEC JTC 1/SC37	biometrics	
ISO/IEC 24714-1	Cross-jurisdictional and societal aspects of implementation of biometric technologies -- Part 1: Guide to the accessibility, privacy and health and safety issues in the deployment of biometric systems for commercial application	ISO/IEC JTC 1/SC37	biometrics	
ITU-T X.1081	The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics	SG 17		Biometrics; Security Architectures, Models and Frameworks; Security mechanisms

ANNEX B: OVERVIEW OF INTERNATIONAL STANDARDS INCLUDING COMMENTS FROM SURVEY

IEC 45B/713/CD*CEI 45B/713/CD*IEC 60860*CEI 60860	IEC 60860, Ed. 2: Radiation protection instrumentation - Warning equipment for criticality accidents	IEC/SC 45B	preparedness	
IEC 107/165/DTS*CEI 107/165/DTS*IEC /TS 62668-1*CEI/TS 62668-1	IEC/TS 62668-1, Ed. 1: Process management - Counterfeit prevention - Part 1: Avoiding the use of counterfeit, fraudulent and recycled electronic components	IEC/TC 107	preparedness	
IEC 60860*CEI 60860	Warning equipment for criticality accidents	IEC/SC 45B	preparedness	
IEC 60951-1*CEI 60951-1	Nuclear power plants - Instrumentation important to safety - Radiation monitoring system for accident and post-accident conditions - Part 1: General requirements	IEC/SC 45A	nuclear	
IEC 60951-2*CEI 60951-2	Nuclear power plants - Instrumentation important to safety - Radiation monitoring system for accident and post-accident conditions - Part 2: Equipment for continuous off-line monitoring of radioactivity in gaseous effluents and ventilation air	IEC/SC 45A	nuclear	
IEC 60951-3*CEI 60951-3	Nuclear power plants - Instrumentation important to safety - Radiation monitoring for accident and post accident conditions - Part 3: Equipment for continuous high range area gamma monitoring	IEC/SC 45A	nuclear	
IEC 60951-4*CEI 60951-4	Nuclear power plants - Instrumentation important to safety - Radiation monitoring for accident and post accident conditions - Part 4: Equipment for continuous in-line or on-line monitoring of radioactivity in process streams	IEC/SC 45A	nuclear	
IEC 61559-2*CEI 61559-2	Radiation in nuclear facilities - Centralized systems for continuous monitoring of radiation and/or levels of radioactivity - Part 2: Requirements for discharge, environmental, accident, or post-accident monitoring functions	IEC/SC 45B	nuclear	
IEC/TS 62045-1*CEI/TS 62045-1	Multimedia Security - Guideline for privacy protection of equipment and systems in and out of use - Part 1: General	IEC/TC 100	nuclear	
ITU-T X.1082 | ISO/IEC 80000-14	Telebiometrics related to human physiology	SG 17		Access Control mechanisms; Authentication mechanisms; Biometrics; Generic security mechanisms; Security mechanisms
ITU-T X.1083 | ISO/IEC 24708	BioAPI interworking protocol	SG 17		Biometrics;

ANNEX B: OVERVIEW OF INTERNATIONAL STANDARDS INCLUDING COMMENTS FROM SURVEY

				Generic security mechanisms; Security mechanisms; Security protocol standards
ITU-T X.1084	Telebiometrics system mechanism - General biometric authentication protocol and profile on telecommunication system	SG 17		Authentication mechanisms; Biometrics; Generic security mechanisms; Security mechanisms
ITU-T X.1086	Telebiometrics protection procedures - Part1: A guideline to technical and managerial countermeasures for biometric data security	SG 17		Biometrics; Generic security mechanisms; Security mechanisms
ITU-T X.1088	Telebiometrics system mechanism - General biometric authentication protocol and profile on telecommunication system	SG 17		Authentication mechanisms; Biometrics; Generic security mechanisms; Security mechanisms
ITU-T X.1089	Telebiometrics authentication infrastructure	SG 17		Authentication mechanisms; Biometrics; Generic security mechanisms; Security mechanisms
ITU-T X.1303	Common alerting protocol	SG 17	Preparedness	Emergency Services; Security protocol standards
ITU-T Y.1271	Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks	SG 13	Response	Emergency Services
ITU-T X.1056	Security incident management guidelines for telecommunications organizations	SG 17	Response	Incident management;

ANNEX B: OVERVIEW OF INTERNATIONAL STANDARDS INCLUDING COMMENTS FROM SURVEY

				Security management standards and guidance documents
ITU-T X.1312	Ubiquitous sensor network (USN) middleware security guidelines	SG 17	Preparedness	Baseline security requirements; Security management standards and guidance documents; Threats and threat assessment; Wireless
ITU-T X.1252	Baseline identity management terms and definitions	SG 17	Techniques	Digital identity; Identity management; Security terminology and glossaries
ITU-T M.3410	Guidelines and requirements for security management systems to support telecommunications management	SG 2	Preparedness	Security management standards and guidance documents
ITU-T X.790	Trouble management function for ITU-T applications	SG 5	Response	Security management standards and guidance documents
ITU-T X.1051	Requirements for Telecommunications of Information Security Management System (T-ISMS)	SG 17	Preparedness	Security Architectures, Models and Frameworks; Security management standards and guidance documents
ITU-T X.1055	Risk management and risk profile guidelines for telecommunications organizations	SG 17	Preparedness	Security management standards and guidance documents
ITU-T X.1275	Guidelines on protection of personally identifiable information in the application of RFID technology	SG 17	Preparedness	Privacy; Security management standards and guidance documents
ITU-T X.1312	Ubiquitous sensor network (USN) middleware security guidelines	SG 17	Preparedness	Baseline security requirements; Security management standards and guidance documents;

ANNEX B: OVERVIEW OF INTERNATIONAL STANDARDS INCLUDING COMMENTS FROM SURVEY

				Threats and threat assessment; Wireless
ITU-T X.Sup8	ITU-T X.1205 – Supplement on best practices against botnet threats	SG 17	Preparedness	Malicious Code; Security management standards and guidance documents
Compendia	Security Compendium	SG 17	Preparedness	General ICT security guidance documents
ITU-T E.408	Telecommunication networks security requirements	SG 2	Preparedness	General ICT security guidance documents
ITU-T E.409	Incident Organization and Security Incident Handling: Guidelines for Telecommunications Organizations	SG 17	Response	General ICT security guidance documents
Security in Telecommunications and IT systems	Security in Telecommunications and IT Systems	SG 17	Preparedness	General ICT security guidance documents

Annex C:
Overview of comments from CEN/TC and ISO/TC secretaries

Annex C: Overview of comments from CEN/TC and ISO/TC secretaries

TC	Comment
CEN/TC 292	CEN/TC 292 'Characterizaion of waste' is not working on security related standards as meant here. However we have published several standards for the determination of compounds in waste and some of them are dangerous substances.
CEN/TC 332	CEN/TC 332 „Laboratory equipment" is not active in the fields of security. But I like to draw your attention to CEN CWA 15793.
CEN/TC 234	Concluding, CEN/TC 234 states that no further European standardization on security in gas infrastructure is required at the time being. After completion of the national stipulations required by the SoS Directive which are currently in preparation, further action in CEN/TC 234 will be considered and taken, where necessary.
ISO/TC 247	The focus of TC247 is standardization in the field of the detection, prevention and control of fraud, defined as an intentional act of deception that creates human or economic harm. Examples include counterfeiting, identity theft, smuggling or other infringements. Most of the standards developed under this Technical Committee will be related to secuirty issues effecting individuals and organizations for the prevention of fraudulent (criminal) acts. We do not directly develop technology security standards related to cybersecurity
ISO/IEC JTC1/SC 27	In general, please note that all SC 27 projects and published standards deal with IT security
ISO/TC 8	I reply you in the attachment as secretary of ISO TC 8 SC12 Large yachts.I am sure that you can obtain a more interesting answer from ISO TC 8 Secretariat, where an important series of standards about security management systems for the supply chain does exist: ISO 28000 series. You can also have a look in ISO Livelink site to see the situation of each document of this series.

Annex D1: Summary of “Study on Competitiveness of the EU Security Industry”

Annex D2: Summary of the “ESRIF report”

ANNEX D: SUMMARY OF REPORTS

ANNEX D1: SUMMARY OF "STUDY ON COMPETITIVENESS OF THE EU SECURITY INDUSTRY"

Final report by ECORYS, November 2009

In short // The final report of this study aims at providing a picture of the current situation of the EU security industry, its structure and organisation, competitiveness position and challenges for the future. With regard to security standardisation activities, one of the most significant problems the industry is facing is the absence of European and common international standards in a fragmented EU market. The report makes several concrete recommendations to enhance the standardisation framework in the field of security in order to strengthen the EU security industry.

SWOT analysis // The report mentions in their SWOT analysis the lack of common EU security standards as one of the weaknesses in the fragmented European security industry and market environment.

Consequently, two opportunities and two threats are identified:

- *Opportunity 1:* Greater EU-level cooperation on development and adoption of common security standards and approvals/certification systems. Eventually leading to adoption of EU-based standards international markets to the advantage of EU suppliers.
- *Opportunity 2:* EU legislation aiming to develop a standardisation framework across all Member States, which would be likely to heighten overall demand for security equipment
- *Threat 1:* US dominance of security supply, creates de facto US-based global security standards
- *Threat 2:* Simpler and better developed system for standardisation of security systems and technologies in the US - and a more focussed stimulation of technological innovation for security – supports de facto US-based global security standards

Absence of standards // One of the most significant problems the industry is facing is the absence of European and common international standards, which creates problems both on the supply and demand side of the security market. Two types of standards are distinguished:

- Absence of common performance standards: often performance standards for security equipment are not clearly defined, or differ across market segments (either geographically defined or by type of user). From a supply perspective, this introduces uncertainties for equipment providers in relation to the expectations of customers regarding required performance and, in turn, for determining investments in technology/product development. From a demand perspective, the absence of performance standards makes it difficult to compare and evaluate security equipment and systems.
- Absence of common technical standards: the absence of technical standards, or differences in technical standards across market segments (either geographically defined or by type of user) tends to result in potential problems of interoperability and further contributes to market fragmentation.

Reason for this absence is often due to the many security technologies that are newly developed or only recently in the security field. Consequently, standards may not exist or may be determined at a national level.

Recommendations // In order to strengthen the EU security industry, the standardisation framework in the field of security at EU and international level should be enhanced. This should aim to provide a framework for performance standards that are aligned to security policy, and for technical standards that promote greater consolidation of currently fragmented markets.

The study proposes several concrete initiatives to achieve this:

- Industry-based solution for the development of technical standards:
    - Strengthening of European Standardisation Organisations' work. Public authorities could call for the development of new standards in the security field, providing clear mandates to ESOs based on priorities set out in the European „vision" for security;

  - European Security Standards Institute. Either within existing ESO framework or as an oversight body for security standards. For example, following a similar approach as that adopted by ETSI (European Telecommunications Standards Institute) and aimed at facilitating the self-development of technical standards;
  - New Approach legislation for security: The possibility of establishing a system of voluntary standards in the security industry should be considered.
- Formal approach for the development of performance standards:
  - European Security Standardisation Handbook, based on the initiative already in place in the defence sector (i.e. European Handbook for Defence Procurement);
  - European Security Label, which would increase confidence and act as a catalyst for investment by attracting new investors to the security industry. As mentioned by ESRIF, this will act as a reference point for manufacturers, end-users and other relevant stakeholders and would provide the frame for a dynamic standardisation process.
- EU-level testing and certification scheme and improved approvals and certification infrastructure, with the aim at creating a testing protocol and the necessary infrastructure (dedicated labs or testing facilities) to carry out testing practices of security products;
- Exchange of formal and informal information on testing facilities as well as best practices, with the objective of increasing transparency and cooperation (e.g. following the example of the CREATIF Network initiative);
- Fast-track system for approval of priority technologies and equipment, to enhance rapid responses to new security threats and challenges.

ANNEX D2: SUMMARY OF THE "ESRIF REPORT"

Final Report by European Security Research and Innovation Forum (ESRIF), December 2009

In short // The European Security Research and Innovation Forum (ESRIF) promotes a more harmonised approach between security, research and innovation. In Europe"s fragmented security market, standardisation can contribute to building more harmonisation to improve the region"s position on the world market. Thus, ESRIF strongly supports all efforts to identify necessary new standards and their development. The report puts forward several recommendations regarding new policy initiatives, integrated approach to security and the global dimension.

Integrated approach // The European Security Research and Innovation Forum (ESRIF), based on a joint initiative of the European Commission and the 27 EU Member States, has spent two years analysing the medium and long-term challenges that Europe faces. These range from natural disasters to organised crime to man-made incidents, whether small-scale in impact or those with potential "mass disruption" effects.

ESRIF promotes a more integrated approach between security, research and innovation, and encourages the EU security industry to invest in essential research and development activities. Europe needs an R&D roadmap, and a mechanism should be set up to implement it in a balanced and rigorous manner. ESRIF thus proposes its European Security Research and Innovation Agenda (ESRIA).

(Systemic) needs for standardisation activities // The European Security Research and Innovation Agenda (ESRIA) proposes a strategic plan for security research and innovation over the next 20 years. Mentioning of standardisation activities for each of the listed areas for analysis defined in the mandate in terms of systemic needs are as followed:

- Security of the Citizens & Security of Infrastructures and Utilities
  - Analysis of the standardisation needs in the various segments of the security market.
  - Promotion of dynamic standardization
  - Rules and integrity standards for a higher transparency of financial systems
- Border Security
  - Harmonised global border control, in order to manage the technical and legal complexity arising from the increasing number of electronic travel documents, develop standards required to ensure

true interoperability of secure documents and systems, and by defining precise common rules of creation, distribution, update, exchange and revocation of certificates between the EU Member States

- Restoring Security and Safety in Case of Crisis
  - Standardisation of recuer identity, skills and credential for interoperable command and control cooperation, for a more efficient international cooperation.
- Others - Identity management and protection (ICT)
  - Develop interoperability requirements (architectural, technical, operational etc.), aiming at agreed processes and standards

In Europe"s fragmented security market, standardisation can contribute to building more harmonisation to improve the region"s position on the world market. Thus, ESRIF strongly supports all efforts to identify necessary new standards and their development. Furthermore, capability-driven standardisation is an important enabler of innovation, and is also a priority in preventing identity theft and enabling interoperability at European borders.

Recommendations // The ESRIF has put forward a list of policy and operational recommendations, of which the following regards standardisation activities:

- Regarding new policy initiatives: new initiatives and programmes should include the early engagement of all stakeholders and transparency of the regulatory environment, including standards to stimulate private sector investments in security research. If upcoming regulations are understood early on, a return on security investments can be foreseen and investments can thus be expected to take place.
- Regarding integrated approach to security: effective civil security must embrace interoperability, standardisation, certification, validation, communication with the public, education & training, exchange of best practices, consultations on privacy issues and other factors that cut across public and private spheres and provide synergies between civil security and defence research fields.
- Regarding the global dimension: the globally inter-related nature of security calls for giving high priority to security"s external dimension and closer home affairs/defence consultation. Research and innovation programmes should support peacekeeping, humanitarian and crisis management tasks, including joint initiatives with other regions and international organisations, notably as regard the development of global standards.

Annex D: Summary of reports

The ESRIF roadmap // The table below shows the mentioning of standardisation activities in the ESRIF"s 11 working groups regarding capabilities and technologies.

No.	What?	Why?	How?	Cluster	Timeline (short-mid-long-term)
WG 1: Security of the citizens					
7	Enhanced resilience and protection of the financial and payment systems	The fraud targeting the financial and payment systems is growing dramatically. New kinds of approaches are needed to address this major problem.	• Rules and integrity standards for a higher transparency of financial systems.	Securing critical assets	short term
17	Analysis of forensic traces	Analysing evidence on a crime scene is the basis of the forensic approach. This evidence is, most of the time, composed of various kinds of traces which require sophisticated tools for analysis.	• International standards for trace recovery	Cross-cutting enablers	Mid term
WG 2: Security of critical infrastructures					
WG 3: Border Security					
30	Standardization, Norms, Interoperability – Standardized equipment/elements, similar procedures/protocols, joint operations, education and training	In order to achieve maximum efficiency in operations and reduce costs of technology procurement and operations conduct, standardization where feasible and	• development of affordable technological solutions, • development of generic interfaces/middlewares, • norms of implementation • research on: development of common operational and procedural guidelines and requirements	Securing identity, access and movement of people and goods	short to mid term

Annex D: Summary of reports

		interoperability are key			
WG 4: Crisis management					
37	Strengthening response forces	Response forces need state-of-the-art technical equipment in the field of sensors, communications and utilities. However, the most promising way to strengthen and enforcing crisis response forces is to bundle and deepen all efforts on European level, in the Member States and by the private sector in the broad area of education, training and exercises.	• provide standardisation of rescuer identity, skills and credential to allow interoperable command and control cooperation for a more efficient international cooperation • address the use of virtual live exercises and other simulation-supported training methods, in particular multi-hazards training simulators, the development of appropriate and sufficient methods and tools for structured ways of lessons learned analysis, exchange and integration into planning and training, and on the education side the development of international degree courses and standards for crisis management leaders aimed at excellence would be recommended.	Security cycle; prevention, protection, preparing, responding and recovering	Short to mid term
WG 5: Foresight and scenarios					
WG 6: CBRN					
48	CBRN integral threat assessment: Surveillance tools for detection of offensive capacity with emphasis on emerging technologies with dual-use potential; analysing actor intention; Intelligent agent data-base and sharing capabilities with high level of standardization using validated accepted data;	Before prevention or preparation strategies can be applied, a complete and accurate assessment of the CBRN threat is required. Continuous assessments and foresight then helps to ascertain the efficacy of prevention strategies and future investments. An accurate CBRN threat assessment is also important to first responders and other crisis management personnel for setting planning and training agenda and can help prioritize research in this critical security area as well.	• Map, through multidiscipline approaches, relevant potential pathways to CBRN terrorism (including radicalisation mechanisms in a CBRN context) and their unique and specific signatures, sensitive to group dynamics and technological abilities • Through cautious awareness raising-dialogue gain support from civil society, law enforcement, academia etc to detect anomalies • Meta-analysis of the complex threat dilemma and development of new, non-frequentist and nondeterministic analysis methods • Methodology to derive the probability of successful incidents. Input is from actor profiles, actor capabilities, consequence prediction, probabilitics • Intelligent database development and analysis; • Objective/quantitative algorithms • Modelling capabilities for attack simulation and	Countering different means of attack	short term

Annex D: Summary of reports

	Systematic identification of vulnerable targets		intervention planning (in/out-door; urban, sub-urban, rural, industrial, infrastructure		
WG 7: Situation awareness and the role of space					
WG 8: Identification of people and assets					
72	Protection against Identity Theft and frauds in both physical and virtual worlds	Identity theft is a major current problem in the world, impacting millions of people and undermining global and financial security. No coherent approach to address this threat is currently in place. It requires a concerted effort involving significant advances in processes and technology.	• Development of agreed processes and standards.	Securing identity, access and movement of people and goods	Short term
73	Identification of victims during Disasters and Emergency Management	In case of disaster, it is critical to identify, as soon as possible the identity of the victims (including survivors). In case of major disasters, experience (2004 tsunami, Katrina..) has shown that more solid and efficient solutions are needed for the management and tracking of the survivors. Solid identifications solutions, adapted to the specific context must be developed.	• Standardisation of rescuer identity, skills and credential to allow interoperable command and control cooperation	Security cycle; prevention, protection, preparing, responding and recovering	Short to mid term
77	Intelligent-led border management	The growing need for high security controls at border crossing has a negative impact on the management of the flow of travellers (lengthy waiting time). Solutions are needed for easier and faster processing. A fast and automatic border control process should be put in place for the majority of travellers, and better tools should be developed for support non automatic procedures.	• Develop standards for interoperability of secured ID documents and equipments.	Securing identity, access and movement of people and goods	Short term

Annex D: Summary of reports

78	Harmonised global border control	Standards – failure to agree and put in place all required standards continues to hold up our ability to exploit and maximise our use of available and new technologies. Also it hinders innovation and R&D as developers still do not have roadmaps for all requirements as yet.	• Develop standards required to ensure true interoperability of secure documents and systems.	Securing identity, access and movement of people and goods	Short to mid term
WG 9: Innovation Issues					
79	Standards development	The European security market is highly fragmented, favouring the development of multiple and incompatible solutions. A solid standardisation effort at European level would help promote the development of innovative solutions addressing the overall market, and would strengthen the European industry.	• Analysis of the standardisation needs in the various segments of the security market. • Analysis of the conditions allowing the definition and implementation of a European Security Label. • Analysis of the economical impact. • Promotion of dynamic standardisation.	Securing critical assets	Short term
WG 10: Governance and coordination					
86	Standardisation and Certification within a European reference system, co-ordinated by the EU and implemented through national bodies	The existence of a multitude of protection levels and standards across EU Member States increases costs for businesses, which have to incur redundant security investments depending on the jurisdictions under which they operate. The EU must define a security standard notably for strategic infrastructures.	• The “Stable Structure” should be in charge of the development and implementation of concepts, doctrines, procedures and designs in order to achieve and maintain the compatibility, interchangeability and/or commonality that are necessary to attain the required level of interoperability	N/A	Short to mid term
WG 11: Human and societal dynamics of security					

NEN

Annex E1: Categorisation of research projects in security area and mentioning of standardization

Annex E2: Response to the survey amongst project coordinators

ANNEX E: ANALYSIS OF PF7 RESEARCH PROJECTS

E1: CATEGORISATION OF RESEARCH PROJECTS IN SECURITY AREA AND MENTIONING OF STANDARDIZATION

Categorisation of research projects in security area

RESEARCH AREA	PROJECTS (ABBREVIATIONS)	TOTAL
Security of the Citizens	ADABTS, BIO-PROTECT, BOOSTER, CBRNEmap, COCAE, CREATIF, DECOTESSC1, DEMASST, DETECTER, EUSECON, FRESP, IMSK, INDECT, LOTUS, MULTIBIODOSE, ODYSSEY, OPTIX, RAPTOR, SecurEau, SECURENV, TWOBIAS	21
Security of infrastructures and utilities	BeSeCu, CPSI, EMILI, ESCoRTS, EURACOM, iDetecT 4ALL, IMCOSEC, ISTIMES, LOGSEC, NI2S3, SAMURAI, SecureCHAINS, SeRoN, STAR-TRANS, SUBITO	15
Border Security	AMASS, CUSTOM, DIRAC, EFFISEC, GLOBE, OPARUS, OPERAMAR, SEABILLA, SECTRONIC, SUPPORT, TALOS, TASS, UNCOSS, WIMA2S	14
Restoring security and safety in case of crisis	CAST, COPE, CRESCENDO, CrisComScore, DITSEF, E-SPONDER, ESS, EULER, FASTID, FESTOS, FORESEC, INDIGO, INFRA, L4S, NMFRDisaster, PANDORA, SAFE-COMMS, SAFIRE, SECRICOM, SGL for USaR, SICMA, STRAW, VIRTUOSO	23

As can be derived from the above table, the research projects cover all the different research areas. Noticeable from this table is that the areas of „Security of the Citizens" and „Restoring security and safety in case of crisis" are more covered by the security research projects than the others. Analysing the areas more specific, the following subareas are covered:

Security of the Citizen (21 research projects)

ANNEX E: ANALYSIS OF PF7 RESEARCH PROJECTS

- Most often mentioned security area: „counter terrorism" and „CBRN(e)"
- Remarkable: projects related to „organised crime" is often taken together with „counter terrorism".

Security of Infrastructures and utilities (15 research projects)

- Most often mentioned security area: „surveillance"
- Remarkable: expect for „building design", all other security areas are mentioned a number of times.

Border security (14 research projects)

- Most often mentioned security area: „sea border"
- Remarkable: many projects cover all areas of border security.

Restoring security and safety in case of crisis (23 research projects)

- Most often mentioned security area: „preparedness and planning"
- Remarkable: very few project focusing on „recovery".

List of projects mentioning standardization

Project Name	Security sub-area	Other area(s)?
CBRNE	CBRNE	
CREATIF	CBRNE detection	
DECOTESSC1	CBRNE, counter terrorism	
FRESP	Counter terrorism, CBRN	Restoring Security and Safety in case of crisis
ODYSSEY	Organised Crime, Counter Terrorism	
EMILI	Energy/Transport communication grids, Supply chains	
ESCoRTS	All	
STAR-TRANS	Energy/transport communication grids	

ANNEX E: ANALYSIS OF PF7 RESEARCH PROJECTS

EFFISEC	Land border/check points, sea border	
OPERAMAR	Sea border	
SEABILLA	Sea border	
SUPPORT	Sea border/ports	SUPPORT concerns upgrading the security of EU ports and although there are elements of boarder security there are also elements of physical security of the transport terminal and security of the supply chain.
CAST	Preparedness and planning, response	
CRESCENDO	Preparedness and planning	
E-SPONDER	Preparedness and planning, response, recovery	
FASTID	Recovery	
INDIGO	Preparedness and planning	
INFRA	Preparedness and planning, response	
EULER		ICT

ANNEX E: ANALYSIS OF PF7 RESEARCH PROJECTS

ANNEX E2: RESPONSE TO THE SURVEY AMONGST PROJECT COORDINATORS

A survey has been sent to the different project leaders asking the following questions:

1. Which security area does the project cover?
2. Was standardization part of the project?
3. Are there standardization results?
4. Are there standardization opportunities?
5. Did you use any existing relevant standard?
6. Are there standards missing?

The below section summarizes question 1 and 2. All the answers to the questions can be found in the table.

Ad 1) Which security area does the project cover?

- Organized Crime
- Counter Terrorism
- CBRNE – Radiological, Biological, Nuclear, Detection
- Surveillance
- Building design
- Surveillance
- Energy/Transport communication grids, Supply chains
- Energy/Transport communication grids, Supply chains
- Land border/check points, sea border, air border,
- Preparedness and planning, response, recovery.

Ad 2) Was standardization part of the project?

- Roadmap including standardization & initiative to produce harmonized EU-wide standards for testing (CREATIF – certification);
- One of the project objectives is to create European Standards for ballistics data collection, storage and sharing (ODYSSEY).
- One of the key objectives is to stimulate convergence of current standardization efforts. Liaising with international efforts and especially with the US Process Control Forum & develop standardization roadmap (Control and real-time systems ESCorTS).
- It aims to develop and apply system analysis methods to assess the risk, vulnerability, safety and security elements of complex systems and critical infrastructures supporting road, and inter-modal transport. Emphasis is given on the study and development of open service-oriented architecture and software standards to support risk management and contingency planning (STAR-trans – risk assessment and contingency).

ANNEX E: ANALYSIS OF PF7 RESEARCH PROJECTS

- EFFISEC is based on the integration of a set of existing and complementary technologies (biometrics, e-documents, signal recognition and image analysis, trace and bulk detection of substances, etc.). It will take into account legal and privacy issues and will also include a standardization step.
- The present situation shows high level of fragmentation, due to many factors: different national procedures, legislations and systems in place, different levels of command and decision making. OPERAMAR (maritime security) will fill an important gap to solve this issue, by supporting the definition of common requirements and operational procedures, as well as new interoperability standards, at the EU level, that should be adopted at national and local level.
- SUPPORT will include policy and standardization proposals and training for participating port personnel as well as dissemination activities for other ports and stakeholders.
- Developing a standardized training curriculum on disaster management for first responders (CAST – training)
- To analyze the policies, the regulations and standardization and encourage the harmonization of European-wide security related regulations and standards by benefiting from the on-going national and European relevant activities with the support of CEN in connection with existing networks and associations (CRESCENDO – R&D roadmap);
- A core system will be developed taking INTERPOL"s paper Ante-Mortem (AM) Disaster Victim Identification (DVI) form and Post- Mortem (PM) DVI together with its Yellow Notice and Black Notice forms, which use the minimum international standards agreed to date for the collection of data for identification of victims and present software as a basis and these will be extended with Rich Internet Application methods and further identification techniques (FASTID – victim identification.
- The preparation of a standard proposition for a European 2D/3D emergency symbology (symbols, indicators, colors) on 2D and 3D maps (Indigo – crisis management).
- Standardization objectives, which includes R&D of a European level proposal for the standardization of the framework of communications and applications as proposed by INFRA (EULER – radio for wireless).

PROJECT TITLE	1. SECURITY AREA?		SURVEY QUESTIONS	3. ANY STANDARDIZATION OPPORTUNITIES?
	Security sub-area	Other area(s)?		
SECURITY OF THE CITIZENS				
CBRNEmap / Road-mapping study of CBRNE demonstrator	CBRNE		2. ADDRESS ISSUE OF STANDARDIZATION?	Yes we do. In one of the suggested demonstrator objects (Enabler) where coordination of Standards brought up in connection to securing a market. We also recommended that one system in the Enabler could be test beds. The Test bed is a virtual interconnection of test facilities and laboratories to support testing, exploration, and validation of new technologies as well as integrated solutions. The Test bed also enables users from different backgrounds to come together, explore potential solutions, share, and discuss organization insight across organizational and jurisdictional boundaries to enhance the development of a common information

ANNEX E: ANALYSIS OF PF7 RESEARCH PROJECTS

				framework, and assist in the development of suitable standards.
			3. ANY STANDARDIZATION OPPORTUNITIES?	See previous answer
			4. ANY EXISTING RELEVANT STANDARDS?	Not directly. CBRNEmap was a pilot study that rewieved all background information about the CBRNE area and gave recommendations for demonstrator objects for phase 2 (CBRNE Demonstrator).
			5. ANY STANDARDS MISSING?	
			6. COMMENTS/ SUGGESTIONS M487?	SLAM (Standardisation of laboratory analytical methods) is a new project in the security area that will start early spring.
DECOTESSC1 / Demonstration of counterterrorism system of- systems against CBRNE phase 1	CBRNE, counter terrorism		2. ADDRESS ISSUE OF STANDARDIZATION?	The project concerned a gap analysis of the CBRNE counterterrorism system as a consisting of Threat Assessment, Prevention, Preparedness, Response and Recovery. Many gap have been identified and prioritized. Some of them explicitly concerned standardization. Under Prevention the following issue was mentioned: Gaps in regulation and deployment around instrumentation and standardisation. Under preparedness the issue: Gaps concerning certification and standards for equipment. This does not mean that in the other area standardization was not an issue, but obviously standardization did not make it to the top level.
			3. ANY STANDARDIZATION OPPORTUNITIES?	Creation of a comprehensive and effective/efficient CBRNE counterterrorism system both nationally and internationally, where resources can be pooled (given the low probability character of the threat) and where security-related countermeasures match or use solutions from the general security, safety, environment. Health and/or defence domain, standardization is a prerequisite. In other words: system approach and standardization go hand-in-hand.
			4. ANY EXISTING RELEVANT STANDARDS?	Standardization in CBRNE counterterrorism is still quite premature, at least not as well developed as in the defence domain.
			5. ANY STANDARDS MISSING?	Many standards are missing. To make an inventory of all of them in the rather complex system required a study on its own.
			6. COMMENTS/ SUGGESTIONS M487?	See the latter part of answer 5. A dedicated study regarding standardization in CBRNE counterterrorism is worth doing. Having said that it is expected that the CBRNE counterterrorism demonstration project of FP7 Security that will start at the end of next year (if elected and granted) will, to a limited extent, deal with standardization issues.
FRESP / Advanced first response respiratory protection	Counter terrorism, CBRN	Restoring Security and Safety in case of crisis	2. ADDRESS ISSUE OF STANDARDIZATION?	Yes, as we are developing an equipment that is situated in a “gap” between the existing standards: a hood with filter for use in a CBRN-environment by First Responders (Police, Emergency Services, Paramedics,…). The requirements are situated in between Escape Hoods (with a very limited protection) and more elaborate full face masks.
			3. ANY STANDARDIZATION OPPORTUNITIES?	See 2
			4. ANY EXISTING RELEVANT STANDARDS?	We partially took into account EN403 and BS 8468 3-2 2009
			5. ANY STANDARDS MISSING?	See 2

ANNEX E: ANALYSIS OF PF7 RESEARCH PROJECTS

			6. COMMENTS/ SUGGESTIONS M487?	No
SECURITY OF INFRASTRUCTURES AND UTILITIES				
EMILI / Emergency management in large infrastructures	Energy/Transport communication grids, Supply chains		2. ADDRESS ISSUE OF STANDARDIZATION?	according to the DoW - yes. At the moment it is under discussion if our results will enable any standardisation effort.
			3. ANY STANDARDIZATION OPPORTUNITIES?	see 2.
			4. ANY EXISTING RELEVANT STANDARDS?	well - there are standards for everything today... we are dealing with rules (W3C standard) - but need extension for our purposes we are dealing with ontologies (W3C standards for languages like RDF/S and OWL) we have some relationships to domain standards (for instance CIM for power grids)
			5. ANY STANDARDS MISSING?	the event and action based approach which is in the focus of EMILI should be standardised - but the maturity of our results may be insufficient for this purpose (see 2)
			6. COMMENTS/ SUGGESTIONS M487?	what do you mean by "programming"? Software development? in this case: I still stand by the goals originally formulated in EMILI. As it seems they are harder to achieve then originally anticipated. But we need them, and we need the standards!
ESCoRTS / European network for the security of control and realtime systems	all		2. ADDRESS ISSUE OF STANDARDIZATION?	One of the deliverables was a standards roadmap – you can download the report (D32) from http://www.cen.eu/cen/Sectors/Sectors/ISSS/Focus/Pages/FG-ESCORTS.aspx
			3. ANY STANDARDIZATION OPPORTUNITIES?	This report contained some standardization opportunities but all a bit too generic to my taste; after the project I tried to launch a CEN Workshop but did not have the resource to go all the way (also a complicated matter considering that we were in the CENELEC area too). I made an initial attempt and received an interesting contribution suggesting there would be value in better aligning IEC 62443-2-1 and ISO/IEC 27001:2005 (see other email)
			4. ANY EXISTING RELEVANT STANDARDS?	D21 contained a list of standards
			5. ANY STANDARDS MISSING?	
			6. COMMENTS/ SUGGESTIONS M487?	
IMCOSEC / Integrated approach to improve the supply chain for container transport and	Supply chain		2. ADDRESS ISSUE OF STANDARDIZATION?	As this project has aimed at proving a roadmap for demonstration, the topic of standards was only considered and discussed in a rather theoretical way. We discussed that any security solution should rely on existing technology standards and must fulfill performance requirements. Therefore standards

ANNEX E: ANALYSIS OF PF7 RESEARCH PROJECTS

integrated security simultaneously				have to be developed! The performance standards must not only include technology aspects (e.g. battery lifetime), but also consider logistic practicability (e.g. mounting times).
			3. ANY STANDARDIZATION OPPORTUNITIES?	not yet.
			4. ANY EXISTING RELEVANT STANDARDS?	a number of standards, but more important are existing regulations in terms of security.
			5. ANY STANDARDS MISSING?	see 2
			6. COMMENTS/ SUGGESTIONS M487?	It is necessary to set some minimum standards for logistic security
SeRoN / Security of road transport networks	Energy/Transport communication grids, Supply chains	Security of the Citizens (road users)	2. ADDRESS ISSUE OF STANDARDIZATION?	The outcome of work in the SeRoN project will be recommendations how to protect road users and road infrastructure from different kinds of threats. These recommendations may make a contribution to the standardization in the security domain.
			3. ANY STANDARDIZATION OPPORTUNITIES?	The recommendations formulated may be incorporated into guidelines set up by road owners and operators.
			4. ANY EXISTING RELEVANT STANDARDS?	The project is based on the related Council directive 2008/114/EC. National standards and guidelines for each type of infrastructure are available (e.g. the German RABT), but so far they have addressed structural aspects rather than security aspects.
			5. ANY STANDARDS MISSING?	The enhancement of the existing guidelines, rules and regulations incorporating security aspects
			6. COMMENTS/ SUGGESTIONS M487?	An integrated consideration in terms of a standardized overall security concept of individual infrastructure objects and complex infrastrucutres should be aspired.
STAR-TRANS / Strategic risk assessment and contingency planning in interconnected transport networks	Energy/transport communication grids		2. ADDRESS ISSUE OF STANDARDIZATION?	The project has produced outcomes which could be standardization relevant, however, no effort has been undertaken in that direction
			3. ANY STANDARDIZATION OPPORTUNITIES?	The project outcomes which should considered during the standardization process, are: a. Transportation Infrastructure Asset typology: hierarchically organized typology of transportation assets related to transportation security b. Strategic Transportation Security Risk Assessment Framework: generic risk assessment methodology adapted to the transportation security domain c. STAR-TRANS Modeling Language (STML): a specific-purpose high-level interface language whose design philosophy emphasizes in the description of the STAR-TRANS framework

ANNEX E: ANALYSIS OF PF7 RESEARCH PROJECTS

			4. ANY EXISTING RELEVANT STANDARDS?	Standards used during the project are: a. EGSA 87: standard for the expression of coordinates b. ISO/IEC 31010:2009, Risk management – Risk assessment techniques, has been developed jointly by ISO and its partner IEC (International Electrotechnical Commission)
			5. ANY STANDARDS MISSING?	Standards needed: Standard descriptions for the following Risk Assessment elements related to Critical Infrastructure protection should be standardized a. Network assets b. Interconnection types between networked assets c. Incident descriptions
			6. COMMENTS/ SUGGESTIONS M487?	
BORDER SECURITY				
AMASS / Autonomous maritime surveillance system	Sea Border		2. ADDRESS ISSUE OF STANDARDIZATION?	The aim of the project was to verfiy the capability of a technical solution. A standardisation was not planned in the project, however, the results of the technical soltuion could very easily lead to a standardisation.
			3. ANY STANDARDIZATION OPPORTUNITIES?	One area of standardisation could be the interfacing with complemtantary and commercially available vessel management systems
			4. ANY EXISTING RELEVANT STANDARDS?	No
			5. ANY STANDARDS MISSING?	currently none identifyable
			6. COMMENTS/ SUGGESTIONS M487?	No
SEABILLA / Sea border surveillance	Sea border		2. ADDRESS ISSUE OF STANDARDIZATION?	There is a dedicated WP on Standardization within the Seabilla workplan: The first objective of this WP is to investigate if the Seabilla solutions proposed are the optimum choices given a set of alternative system configurations, comprising different choices of platforms, sensors and information processing means according to the interoperability and integration issues (data fusion, metadata, VMS, etc.).The second objective is to identify and recommend possibilities for further developments of new standards not covered in this project. A third objective is to approach standardisation and/or regulation bodies with recommendation aiming at improving maritime surveillance.
			3. ANY STANDARDIZATION OPPORTUNITIES?	Possible indications will be raised at the end of the project. To date it is not possible to define a specific need
			4. ANY EXISTING RELEVANT STANDARDS?	not specific for border surveillance applied for civilian purposes. Imo, IALA and military standards may be applicable for subsector
			5. ANY STANDARDS MISSING?	NO, but as indicated in question 2, we have a WP on Standardization which might identify missing or incomplete standards.
			6. COMMENTS/ SUGGESTIONS M487?	NO

ANNEX E: ANALYSIS OF PF7 RESEARCH PROJECTS

SUPPORT / Security upgrade for ports	Sea border/ports	SUPPORT concerns upgrading the security of EU ports and although there are elements of boarder security there are also elements of physical security of the transport terminal and security of the supply chain.	2. ADDRESS ISSUE OF STANDARDIZATION?	No we are not proposing standards in the project. We are providing guidance for ports on how they can comply with current legislation such as the ISPS code.
			3. ANY STANDARDIZATION OPPORTUNITIES?	Perhaps towards the end of the project this may become apparent but we are still in the early stages.
			4. ANY EXISTING RELEVANT STANDARDS?	All current EU and maritime standards and regulations pertaining to port security. See knowledge portal http://www.support-project.eu/supportknowledge/defaultinfo.aspx?areaid=73&index=13 http://www.support-project.eu/supportknowledge/defaultinfo.aspx?areaid=75&index=13
			5. ANY STANDARDS MISSING?	See comment for question 3.
			6. COMMENTS/ SUGGESTIONS M487?	See comment for question 3.
VIRTUOSO / Versatile information toolkit for end-users oriented open sources exploitation		Security of the Citizens (open source watch can be aimed at organised crime and counter terrorism) & Restoring Security and Safety in case of crisis	2. ADDRESS ISSUE OF STANDARDIZATION?	Not directly, but the Virtuoso project proposes a framework which is designed to become the universal system in the security domain, allowing to design interoperable applications.
			3. ANY STANDARDIZATION OPPORTUNITIES?	▪ the architecture of the plaftorm itself can be standardized ▪ the knowledge model (the taxonomy) can also be standardized The opportunities are planned to be developed over the course of the EPISTOLA project (submitted to the FP7 23/11/11). For the moment this new project is under evaluation (with AFNOR as a partner). One of the goals of the project is to define pre-standards for the architecture and the knowledge model.
			4. ANY EXISTING RELEVANT STANDARDS?	Not in Europe, but, concerning the knowledge model, the American UCore model exists. Our knowledge model is an extension of UCore that could be defined as a European standard.
			5. ANY STANDARDS MISSING?	Please see 3.
			6. COMMENTS/ SUGGESTIONS M487?	None.
RESTORING SECURITY AND SAFETY IN CASE OF CRISIS				

ANNEX E: ANALYSIS OF PF7 RESEARCH PROJECTS

CAST / Comparative assessment of security-centered training curricula for first responders on disaster management in the EU	Preparedness and planning, response		2. ADDRESS ISSUE OF STANDARDIZATION?	STANDARDIZATION OF TRAINING CURRICULA FOr FIRST RESPONDERS
			3. ANY STANDARDIZATION OPPORTUNITIES?	NO BECASUE NO FUNDING FOR PUBLIC REALTION CAMPAIGN ANNOUNCING THE AVAILABILITY OF THE NEW "CAST-TRAINING CURRICULUM" TO EU STAKEHOLDERS
			4. ANY EXISTING RELEVANT STANDARDS?	NONE AVAILABLE
			5. ANY STANDARDS MISSING?	ANY EFFORT IN STANDADARIZATION IN SECURIT TRAINING IS VERY MUCH NEEDED IN EU MEMBER STATES (ALREADY EXISTING IN US BY US-DHS)
			6. COMMENTS/ SUGGESTIONS M487?	CREATE EU NETWORK OF SIMILAR EU EFFORTS ON THE TOPIC AREAS TRAINING AND R&D
CrisComScore / Developing a crisis communication scorecard	Preparedness and planning		2. ADDRESS ISSUE OF STANDARDIZATION?	What we did was identify indicators for effective crisis communication and we have provided these in the form of a communication scorecard to enhance learning of governmental organisations aimed at continuous improvement. The scorecard is not filled with metrics but although it delivers score it has a qualitative approach using assessment.
			3. ANY STANDARDIZATION OPPORTUNITIES?	Our work can be considered as setting quality standards for crisis communication. But this is about communication content and not about communicationS which refers to communication means and technology.
			4. ANY EXISTING RELEVANT STANDARDS?	see www.crisiscommunication.fi, but most people would not label this work as providing 'standards', in fact it is more about guidelines then about rules or standards. Guidelines like that besides communicating in crisis situations it is important to monitor citizen views to see what is needed, and that this needs cooperation among the partners in the crisis management network and more adaquate specialised manpower (capacity).
			5. ANY STANDARDS MISSING?	We citisised best practices as not being flexible enough and would prefer to talk about guidelines and quality criteria to be used flexibly. So for the content of communication and the design of communication strategies we do not see fixed standards as recommendable. For example there used to be a best practice to organise press conferences at prime time, but nowadays one can't wait for that and information has to be continous and two-way. Probably standards for technical requirements for communication means make more sense, so that citizens of various EU countries will have similar alarm numbers, a similar meaning of sirens, that there is a minimum capacity set of crisis call centres and crisis websites, and that there is an approach of inclusiveness so that standards make sure that also e.g. blind people will be reached effectively by warning messages.

ANNEX E: ANALYSIS OF PF7 RESEARCH PROJECTS

			6. COMMENTS/ SUGGESTIONS M487?	We wish you success
E-SPONDER / A holistic approach towards the first responder of the future	Preparedness and planning, response, recovery		2. ADDRESS ISSUE OF STANDARDIZATION?	Yes, the Project is developing solutions for communications in emergency scenarios, between the First Responders and the Command units (fixed, central, mobile). Overall architecture will be defined and suitable communication technologies will be proposed. A specific activity monitoring/contributing to standardisation bodies is undertaken within the project (i.e. a separate Work Package of the project).
			3. ANY STANDARDIZATION OPPORTUNITIES?	Initial activities of the project have addressed the possible options of Workshop Agreement within CEN CENELEC, as a way to come up with proposed practical implementation scenarios of the communications channels, and get general acceptance by industry, emergency operators, public authorities, etc. However, further work did identify ETSI EMTEL and other Technical Committees as suitable bodies for the contribution from the E SPONDER project on general communication architectures, specific requirements for the operation, etc.
			4. ANY EXISTING RELEVANT STANDARDS?	Yes, those developed by ETSI EMTEL, as well as some pieces of ETSI TC SES (SatEC) are relevant for E-SPONDER. Our first inputs to Standardisation bodies are pointing to inputs to ETSI EMTEL.
			5. ANY STANDARDS MISSING?	Yes, certainly, currently ETSI EMTEL does mostly cover requirements for the implementation of the communication channels. Therefore, specific standards for the setting up of end-to-end communication channels between the different actors in a crisis environment (to support the needs of the First Responders communication requirements) are opportunities for further standardization. In addition, the standardization of the data structures within the IT systems (used for information dissemination and decision making support) and the higher layers of the communications channel to facilitate interoperability of devices, is a missing element which standardization activities could be undertaken.
			6. COMMENTS/ SUGGESTIONS M487?	Possible workshops with all players working in the field of communications solutions for emergency operations should meet to delineate priorities and a common roadmap in the area. It is not well understood how M/487 mandate does complement or relate to mandate M/496 which does also cover the standardization of emergency communications in the space domain. E-SPONDER specialists on standardization activities would appreciate and thus be grateful to be invited to a future meeting of the CEN/CENELEC TC 391 to better understand the work in front of the mandate M/487.
INFRA / Innovative & novel first responders applications	Preparedness and planning, response		2. ADDRESS ISSUE OF STANDARDIZATION?	In INFRA we addressed the issue of standardisation by developing a document, outlining the requirements and technical specification of the developed INFRA system. In the lack of the corresponding standard Group, the document is used as a basis for technical specification of the product that was developed by Rinicom.

ANNEX E: ANALYSIS OF PF7 RESEARCH PROJECTS

			3. ANY STANDARDIZATION OPPORTUNITIES?	Currently, there is no standardisation activity which address this topic. We suggested this activity within ETSI, as an extension of TETRA/TETRAPOL, however, didn"t receive support from the Group who considered our proposal as beyond the scope of TETRA/TETRAPOL standard.
			4. ANY EXISTING RELEVANT STANDARDS?	Not to our knowledge. We strongly support the activities to establish Security Standard M/487
			5. ANY STANDARDS MISSING?	Standard on the use of UAVs in case of crisis
			6. COMMENTS/ SUGGESTIONS M487?	No
PANDORA / Advanced training environment for crisis scenarios	Preparedness and planning		2. ADDRESS ISSUE OF STANDARDIZATION?	Not really, Pandora s about training senior managers to be able to manage a crisis.
			3. ANY STANDARDIZATION OPPORTUNITIES?	The standardisation issues that arise are more related to those in IT used to develop the system such as our contribution to the emotion markup language, we are not involved n security standards.
			4. ANY EXISTING RELEVANT STANDARDS?	There are none in the security area. Outside of that, there are many IT standards we are working to but I'm assuming you are not interested in these.
			5. ANY STANDARDS MISSING?	N/A
			6. COMMENTS/ SUGGESTIONS M487?	No.
SGL for USaR / Second generation locator for urban search and rescue operations	Recovery		2. ADDRESS ISSUE OF STANDARDIZATION?	It does not develop a standard(which we are interested to do by the way for the different devices we develop in the project). But the project develops procedures for use of the devices in the field and develops guidelines for the use of the devices by the first responders
			3. ANY STANDARDIZATION OPPORTUNITIES?	Yes. We have developed for example a new device called FIRST for use by the rescuers. This is an innovative portable device that combines audio, video and chemical signals for locating entrapped victims in collapsed buildings. We can definitely develop a standard for this device(and we are thinking of doing it in a new project that the device is used in field applications)
			4. ANY EXISTING RELEVANT STANDARDS?	I am not aware if any relevant standards for this integrated devices. Some military standards exist(NATO) for handheld instruments used in detecting chemical threats
			5. ANY STANDARDS MISSING?	Yes. In principle the broad area of non-military applications of detection instruments in physical or man-made disasters is lacking standardization. We would like to see standards in the are of the field chemical analysis for environmental or rapidly evolving phenomena(deliberate release of chemical agents for example)

ANNEX E: ANALYSIS OF PF7 RESEARCH PROJECTS

			6. COMMENTS/ SUGGESTIONS M487?	I know that it will be difficult to develop and establish standards in civil protection issues in general and especially in procedures due to the fact that in many cases Member States think the issues are that of national security(interest). However, developing standards in other than IC systems is possible. As mentioned previously for instruments and sensors used for field chemical detection there is a need and can be realized.
SICMA / Simulation of crisis management activities	Preparedness and planning		2. ADDRESS ISSUE OF STANDARDIZATION?	No
			3. ANY STANDARDIZATION OPPORTUNITIES?	The project could support a simulation based evaluation of alternative candidate standards for the Health Service Crisis Management e.g. MIMMS (Major Incident Medical Management and Support) like
			4. ANY EXISTING RELEVANT STANDARDS?	The project deals with Health Service crisis management. A de facto standard for such domain is MIMMS (Major Incident Medical Management and Support)
			5. ANY STANDARDS MISSING?	It seems that most EU countries have their own best practice to manage a crisis but there is no EU standard for that. This is true at least for the Health Service (which was the main focus of the project)
			6. COMMENTS/ SUGGESTIONS M487?	I would suggest to exploit as much as possible the work done in this field by the military guys

Annex F:

Stakeholders analysis

Annex F: Stakeholders analysis

Stakeholders Analysis

1. Security of the citizens – organized crime

Subject	Security of the citizens – organized crime	
Chain of development		
Recruiting/tender	Police	Interpol, Europol
Design/development	Police Research institutes Software engineers (report protocol, information exchange)	Interpol, Europol
Prototype/testing	Research institutes	
Chain of production		
Purchase	Police Military	
Production	Manufacturers of communication equipment and allied software, Data storage and exchange systems	
Distribution	Specialized contractors	
Chain of use		
Purchase/delivery	Police Military	
Waste dispense		
Chain of recycling		
Collecting		
Treatment		
Sales/ re-use		

2. Security of the citizens – counter terrorism

Subject	Security of the citizens – counter terrorism	
Chain of development		
Recruiting/tender	Public authorities, Critical infrastructure	
Design/development	Critical infrastructure, Technical supply chain Research institutes Police Military	
Prototype/testing	Research institutes	
Chain of production		
Purchase		
Production	Technical supply chain	
Distribution	Technical supply chain	EOS, Euralarm
Chain of use		
Purchase/delivery	Public authorities, Critical infrastructure	
Waste dispense		
Chain of recycling		
Collecting		
Treatment		
Sales/ re-use		

3. Security of the citizens – Explosives

Subject	Security of the citizens – Explosives	
Chain of development		
Recruiting/tender	Public authorities involved in	

Annex F: Stakeholders analysis

	infrastructure and construction	
Design/development	Research institutes	
Prototype/testing	Research institutes	
Chain of production		
Purchase	Chemical industry	
Production	Chemical industry	
Distribution	Chemical industry	
Chain of use		
Purchase/delivery	Public authorities involved in infrastructure and construction Public authorities involved with dismantling of bombs and mines	
Waste dispense	Specialized contractors	
Chain of recycling		
Collecting	Specialized contractors	
Treatment	Specialized contractors	
Sales/ re-use		

4. Security of the citizens – CBRN

Subject	**Security of the citizens – CBRN**	
Chain of development		
Recruiting/tender	Public authorities, Critical infrastructure First responders	EOS
Design/development	Research institutes	
Prototype/testing	Research institutes	
Chain of production		
Purchase	Industry (various)	
Production	Chemical, biological and radiological laboratories Nuclear power plants	
Distribution	Technical supply chain	
Chain of use		
Purchase/delivery	Chemical industry Biolabs	
Waste dispense	Specialized services	
Chain of recycling		
Collecting	Specialized services	
Treatment	Specialized services	
Sales/ re-use	Note: Nuclear waste is a separate issue	

5. Security of the citizens – Fire hazard

Subject	**Security of the citizens – Fire hazard**	
Chain of development		
Recruiting/tender	Public authorities involved in infrastructure and construction	Euralarm, Eurofeu
Design/development	Fire safety engineering services	
Prototype/testing	Research institutes	
Chain of production		
Purchase	Technical supply chain	
Production	Technical supply chain (construction, installation)	
Distribution	Technical supply chain (installation)	
Chain of use		
Purchase/delivery	Public authorities involved in	

Annex F: Stakeholders analysis

	infrastructure and construction Project development, estate agents Building maintenance services Supply of means for fire protection, fire detection, fire extinguishing etc.,	
Waste dispense		
Chain of recycling		
Collecting	Building maintenance services Supply of equipment for fire protection, fire detection, fire extinguishing etc.,	
Treatment	Building maintenance services Supply of equipment for fire protection, fire detection, fire extinguishing etc.,	
Sales/ re-use		

6. Security of infrastructures and utilities – Building design

Subject	**Security of infrastructures and utilities – Building design**	
Chain of development		
Recruiting/tender	Public authorities involved in infrastructure and construction	Euralarm, CoESS
Design/development	Civil engineering services	
Prototype/testing	Research institutes	
Chain of production		
Purchase	Technical supply chain (installation equipment)	
Production	Technical supply chain (construction, installation)	
Distribution	Technical supply chain (construction, installation)	
Chain of use		
Purchase/delivery	Public authorities involved in infrastructure and construction Project development, estate agents Building maintenance services Supply of equipment and services for security (prevention, detection, alarms, follow-up)	
Waste dispense		
Chain of recycling		
Collecting		
Treatment		
Sales/ re-use		

7. Security of infrastructures and utilities – Energy/Transport communication grid

Subject	**Security of infrastructures and utilities – Energy/Transport communication grid**	
Chain of development		
Recruiting/tender	Public authorities Critical infrastructure, Research institutes Business continuity services Software engineers (making programs to locate the area in	EPCIP networks (various)

	case of a disruption)	
Design/development	Critical infrastructure, Technical supply chain Research institutes Police Military	
Prototype/testing	Critical infrastructure, Research institutes	
Chain of production		
Purchase	Technical supply chain (installation equipment)	
Production	Technical supply chain (installation equipment)	
Distribution	Technical supply chain (installation equipment)	
Chain of use		
Purchase/delivery	Public authorities Critical infrastructure, Research institutes Police Military	
Waste dispense		
Chain of recycling		
Collecting		
Treatment		
Sales/ re-use		

8. Security of infrastructures and utilities – Surveillance

Subject	**Security of infrastructures and utilities – Surveillance**	
Chain of development		
Recruiting/tender	Public authorities Estate management	Europol, CoESS
Design/development	Technical supply chain (protective equipment, communication, transport, arms, etc)	
Prototype/testing	Research institutes	
Chain of production		
Purchase	Technical supply chain	
Production	Technical supply chain	
Distribution	Technical supply chain	
Chain of use		
Purchase/delivery	Police Private security services	
Waste dispense		
Chain of recycling		
Collecting	Technical supply chain	
Treatment	Technical supply chain	
Sales/ re-use		

9. Security of infrastructures and utilities – Supply chain

Subject	**Security of infrastructures and utilities – Supply chain**	
Chain of development		
Recruiting/tender	Responsibles for building design, fire safety and surveillance Transport and storage services (logistics) Private security services	CoESS, Euralarm, EOS

Annex F: Stakeholders analysis

Design/development	Business continuity services Suppliers of technical equipment	
Prototype/testing	Research institutes	
Chain of production		
Purchase	Technical equipment (and parts) for prevention, detection and response in case of fire, explosives, flooding, burglary, smuggling, vandalism, theft or terrorist threat	
Production	Assembly of the equipment (parts)	
Distribution	Installation and surveillance services	
Chain of use		
Purchase/delivery	Responsibles for building design, fire safety and surveillance Transport and storage services (logistics) Private security services Business continuity services	
Waste dispense		
Chain of recycling		
Collecting		
Treatment		
Sales/ re-use		

10. Border Security – Land border / Check points

Subject	**Border Security – Land border / Check points**	
Chain of development		
Recruiting/tender	Public authorities involved in border control	CoESS, EOS
Design/development	Security system engineering for check points	
Prototype/testing	Research institutes	
Chain of production		
Purchase	Technical supply chain	
Production	Technical supply chain	
Distribution	Technical supply chain	
Chain of use		
Purchase/delivery	Private security services Police Military	
Waste dispense		
Chain of recycling		
Collecting		
Treatment		
Sales/ re-use		

11. Border Security – Sea Border

Subject	**Border Security – Sea Border**
Chain of development	

Annex F: Stakeholders analysis

Recruiting/tender	Public authorities involved in border control	CoESS, EOS
Design/development	Security system engineering for ports and coast guards	
Prototype/testing	Research institutes	
Chain of production		
Purchase	Technical supply chain	
Production	Technical supply chain	
Distribution	Technical supply chain	
Chain of use		
Purchase/delivery	Private security services Port authorities Port estate management Police Military	
Waste dispense		
Chain of recycling		
Collecting		
Treatment		
Sales/ re-use		

12. Border Security – Air Border

Subject	**Border Security – Air Border**	
Chain of development		
Recruiting/tender	Public authorities involved in border control	CoESS, EOS
Design/development	Security system engineering for airports	
Prototype/testing	Research institutes	
Chain of production		
Purchase	Technical supply chain	
Production	Technical supply chain	
Distribution	Technical supply chain	
Chain of use		
Purchase/delivery	Private security services Airport authorities Airport estate management Police Military	
Waste dispense		
Chain of recycling		
Collecting		
Treatment		
Sales/ re-use		

13. Restoring security and safety in case of crisis – Preparedness and Planning

Subject	**Restoring security and safety in case of crisis – Preparedness and Planning**	
Chain of development		
Recruiting/tender	Public authorities First responders	
Design/development	Risk management, crisis management, supply chain and business continuity services	
Prototype/testing	Research institutes	
Chain of production		
Purchase	Critical infrastructure	

Annex F: Stakeholders analysis

Production	Critical infrastructure	
Distribution	Supply chain (technical and services)	
Chain of use		
Purchase/delivery	Public authorities First responders Risk and crisis management services	
Waste dispense		
Chain of recycling		
Collecting		
Treatment		
Sales/ re-use		

14. Restoring security and safety in case of crisis – Response

Subject	**Restoring security and safety in case of crisis – Response**	
Chain of development		
Recruiting/tender	Public authorities First responders	
Design/development	Risk management, crisis management, supply chain and business continuity services	
Prototype/testing	Research institutes	
Chain of production		
Purchase	Critical infrastructure	
Production	Critical infrastructure	
Distribution	Supply chain (technical and services)	
Chain of use		
Purchase/delivery	Public authorities First responders Private response services	
Waste dispense		
Chain of recycling		
Collecting		
Treatment		
Sales/ re-use		

15. Restoring security and safety in case of crisis – Recovery

Subject	**Restoring security and safety in case of crisis – Recovery**	
Chain of development		
Recruiting/tender	Public authorities First responders	
Design/development	Risk management, crisis management, supply chain and business continuity services	
Prototype/testing	Research institutes	
Chain of production		
Purchase	Critical infrastructure	
Production	Critical infrastructure	
Distribution	Supply chain (technical and services)	

Annex F: Stakeholders analysis

Chain of use		
Purchase/delivery	Public authorities First responders Private recovery services	
Waste dispense		
Chain of recycling		
Collecting		
Treatment		
Sales/ re-use		

ANNEX G: REPORT OF THE KICK-OFF MEETING

DOCUMENT Report of the kick-off meeting M/487	
DATE 2011-10-13	**NUMBER OF PAGES** 3
SUPERSEDES DOCUMENT	
COMMITTEE **CEN/TC 391** Societal and Citizen Security	

Subject:

Report of kick-off meeting M/487 (2011-09-29)

1 Opening – purpose of the meeting

The chairman Mr Cornet opens the meeting and welcomes all attendees. One item will be added to the agenda: Mr Dale from Euralarm will also give a presentation.

2 Setting the scene

Two presentations are given to set the scene.

Mr Malacarne from DG Enterprise and Industry gives the background of the Mandate. Security is becoming more and more important for Europe. He stresses the need for research that produces practical results. Especially for the security theme, which is very much oriented to applications. An EU wide picture of the standardization landscape is needed.

He emphasizes the link between standards, standardization and certification; standards can in this way encourage better harmonization and interoperability in security. This is of course not an easy challenge, but he calls for all to help bringing the world of research and the world of industry together.

Mr Cornet, chairman of both CEN/TC 391 and the coordination group of the mandate work, follows with the second presentation with the ESO's response to the mandate. The slides of this presentation can be found in Annex A.

The issue of whether or not to define limits to the research areas is raised. The European Commission replies that the existing structure with the defined security research areas in FP7 could serve as a starting point. However, this does not exclude other areas and it is open for suggestions.

Another issue discussed is the topic of ICT, whether or not and to what extent it should be included. As mentioned in the presentation, ICT is excluded on a vertical level, except for cryptography. The European Commission states, as mentioned in the Mandate, that ICT should be integrated on a horizontal level.

The chairman stresses that the work for the Mandate is not only within CEN, but also CENELEC and ETSI are heavily involved.

3 Stakeholders presentations – identifying priorities and issues

Four presentations giving the industrial, institutional and national needs are given. The presentations can be found in Annex B.

Mr Rebuffi, CEO of the European Organization for Security, presents the point of view of industry needs for security standards. He notes how difficult it has been for the past four years to mobilize the industry in a coordinated way to work on European standards, and expresses his hopes on the mandate. EOS stresses the need for more standards (especially internationally) on security, and is open to cooperate with and contribute to the mandate work.

Mr Krassnig from DG Home presents his point of view of institutional needs. In this presentation, he stresses the need to keep the scope broad and not to narrow down yet. Also he refers to the Internal Security Strategy. Additionally, he points out that standards are important, yet they should be seen as a tool and not a goal itself.

Mr Sieber from the Joint Research Centre (JRC) presents his point of view of institutional needs. He discusses how standardization and research are two sides of the same coin. Currently standardization is often applied at the end of the product chain. Instead, Mr Sieber encourages looking at this earlier and stresses the importance of standardization.

Ms Schlüter from DIN (German Standardization Institute) presents the point of view of national needs. She underlines that there is a need for strong cooperation between different technical committees. Thus DIN has set up the “Coordination Office for Civil Security”, also providing advice and strategy in this area.

4 Contributions from other participants

Four additional presentations by other stakeholders were given. These presentations can be found in Annex C.

Mr Swenker from Blücher stresses the lack of capabilities, and how standards are a tool that can lead to these capabilities. Standards should serve as guidance, provide a framework and not dictate the user community what to do.

Mr Purser from ENISA expresses willingness of ENISA to build effective bridges between national standards bodies and ENISA, as ENISAs network represent many (security) stakeholders.

Mr Brookson from ETSI shows how ETSI develops standards to meet business needs, and which topics ETSI believes should be included in the mandate. He advises to go through the ETSI White Paper on security (which is soon to be updated) where many aspects are highlighted.

Mr Dale from Euralarm explains how Euralarm has been involved in many standardization processes. He stresses the need to harmonize procedures in Europe, and is willing to contribute to the mandate's work.

5 Discussion, conclusions and next steps by ESOs

Many stakeholders have shown willingness to contribute to the mandate's work and the chairman expresses his gratefulness. The inventory will start with a wide scope using all sorts of sources; options for best practices, standards and technical specifications, ranging from management systems to interoperability and from training to performance standards. After that, priorities can be set, based on the criteria the participants from EC and industry have given in this workshop.

It is suggested to take the results from CEN/BT WG 161 into account, as much was done there as well. Another suggestion is to come up with an end user questionnaire as this group is not well represented today. Also it is advised to use existing networks like IAEA etc. to get up to date information.

The chairman thanks everyone for the suggestions made and encourages all to contact the secretariat of CEN/TC 391 with more ideas and suggestions. Suggestions may also come from the panel discussion on security on the World Standards Day on October the 14th in Brussels.

The ESOs will proceed with the results discussed today in the JWG meeting of CEN/TC 391 in Vienna (members of CEN/CENELEC/ETSI are welcome).

The coordination group will meet after that and a first draft report is expected in December. After collecting the comments, another workshop could be organised to discuss the draft and comments, after which the report of Phase 1 will be finalized and send to the European Commission.

The actions in Phase 2 will depend on the reaction of the European Commission.

6 Closure

The chairman thanks all attendees, and a special thanks to the speakers, for their contributions to this fruitful meeting.

ANNEX H:
OVERVIEW OF PRIORITIES SUBMITTED BY CEN/TC 391 MEMBERS

ANNEX H: OVERVIEW OF PRIORITIES SUBMITTED BY CEN/TC 391 MEMBERS

Priorities categorised in security areas

Priorities mentioned in the field of “Security of the Citizens”:

Type of industry/threat	Priority reason
End-to-end Security	The key aspect “secure end-to-end communication between police, civil services, emergency services, agencies and persons initiating emergency calls” should be considered regarding the existing and future digital and mobile communication services, infrastructures and protocols. Especially agencies should be able to communicate in a secure and sufficient way with third parties. [Germany]
Organized Crime	In line with the ongoing standardisation work of the German Electrotecnical Committee “Hazard alert systems” the following new areas for security standardisation have been identified: – Artificial DNA (identification technologies and methods for criminals), – Gun rampage at schools and terrorist attacks. [Germany]
Emergency Call and Service Centre	Result of discussion in mirror committee for security services. [Germany]
dynamic/smart escape route navigation	preparedness in the case of crisis, incidents. [Germany]
local & wide area alert procedures	alert in the case of crises, natural disaster, etc. [Germany]
Security alarms. Risks include: burglary, personal attack, terrorism, etc.)	Lack of standardization in this specific area is resulting in each state making its own way, forcing product development to be done on national basis with individual certification schemes, etc - resulting in trade barriers. [Euralarm]
Security (and Fire) alarms and other systems. Risks include: burglary, personal attack, terrorism, etc. and fire	Expansion of use of new communications technology is being adopted, but without standardization, so that national independence exists in the manner in which security measures are implemented. This national independence inevitably leads to trade barriers and prevents design of interoperable systems. These variations also leave some systems vulnerable to being compromised because measures adopted are inadequate. [Euralarm]
Major disasters, explosives, CBRN attacks, fires, pandemics	Populations are aging and additional attention will be required concerning the needs of elderly but healthy citizens. [Mr Wood]
Major disasters, explosives, CBRN attacks, fires, pandemics	The combination of aging population and the increasing sophistication of equipment makes it difficult for equipment designers and system specifiers to address the needs of the entire population. The standard would identify the requirements which need to be met to ensure that no one in the population is discriminated against. [Mr Wood]
Major disasters, explosives, CBRN attacks, fires, pandemics	European laws prohibit discrimination against those with disabilities and other vulnerable members of the population – including children. Equipment and systems tend to be designed

ANNEX H: OVERVIEW OF PRIORITIES SUBMITTED BY CEN/TC 391 MEMBERS

	with the young and reasonably fit in mind. This review would examine the special requirements of those members of the population with special needs and determine the requirements whereby their needs can be fully addressed. [Mr Wood]

Priorities mentioned in the field of “Security of Infrastructures and Utilities”:

Type of industry/threat	Priority reason
Constructional measures for the protection of critical infrastructures and utilities	Railroad engineering: Protection of critical infrastructures from explosive events and accidents. For example, this requirement is important for tunnel constructions, where a reliable communication is necessary especially for emergency services. This should also be reinsured for wireless communication services inside the whole tunnel (for example, by harmonization of frequency spectrums for different emergency services). [Germany]
Constructional measures for the protection of critical infrastructures and utilities	Protection of control centers, for example: railroad operating centers, energy supply control centers. [Germany]
Supply chains	The key aspect “lack of components and devices (electrical, electronic, mechanical, etc.) conditioned by natural and industrial disasters (earthquakes, worst-case-scenarios)” should be considered in order to develop an emergency strategy in respect of, for example, a proactive alignment of production processes and capacities, especially for key industry sectors like automotive, etc. [Germany]
Government installations	Result of discussion in mirror committee for security services. [Germany]
Emergency Call and Service Centre	Result of discussion in mirror committee for security services. [Germany]
procedures against amok	schools, public places and buildings, supermarkets. [Germany]

Priorities mentioned in the field of “Restoring security and safety in case of crisis”:

Type of industry/threat	Priority reason
supply structures in the case of pandemics	supply, support in the case of pandemics, realizing transborder cooperation

ANNEX H: OVERVIEW OF PRIORITIES SUBMITTED BY CEN/TC 391 MEMBERS

Priorities as submitted from CEN/TC 391 members

TABLE 2: OVERVIEW OF PRIORITIES IN THE FIELD OF SECURITY STANDARDIZATION

Country: Germany

Contact person: Stefan Krebs

Security area	Type of industry / type of threat	Reason for this priority	Desired deliverable(s)	Users	Additional information
Security of the Citizens	Organized Crime	In line with the ongoing standardisation work of the German Electrotecnical Committee “Hazard alert systems” the following new areas for security standardisation have been identified: – Artificial DNA (identification technologies and methods for criminals), – Gun rampage at schools and terrorist attacks.			Proposal made by the German Commission for Electrical, Electronic & Information Technologies
Security of the Citizens	Emergency Call and Service Centre	Result of discussion in mirror committee for security services			Proposal made by the German Technical Committee for Services
Security of infrastructures and utilities	Government installations	Result of discussion in mirror committee for security services			Proposal made by the German Technical Committee for Services
Security of infrastructures and utilities	Emergency Call and Service Centre	Result of discussion in mirror committee for security services			Proposal made by the German Technical Committee for Services
Security of the Citizens	dynamic/smart escape route navigation	preparedness in the case of crisis, incidents	harmonized European Stnadards	airport, maritime ports, public places, people with limited performance	Proposal made by a big German company
Security of the Citizens	local & wide area alert procedures	alert in the case of crises, natural disaster, etc.	harmonized European Stnadards	goverments, öffentliche Hand	Proposal made by a big German company
Security of infrastructures	procedures against amok	schools, public places and buildings, supermarkets	harmonized European Stnadards, regulatory	öffentliche Hand, private sector	Proposal made by a big German company

ANNEX H: OVERVIEW OF PRIORITIES SUBMITTED BY CEN/TC 391 MEMBERS

and utilities			documents		
Restoring security and safety in case of crisis	supply structures in the case of pandemics	supply, support in the case of pandemics, realizing transborder cooperation	harmonized European Stnadards, regulatory documents	öffentliche Hand	Proposal made by a big German company

TABLE 2: OVERVIEW OF PRIORITIES IN THE FIELD OF SECURITY STANDARDIZATION

~~**Country:**~~
Liaison organization: **EURALARM**

Contact person: **Brian Harrington**

Security area	**Type of industry / type of threat**	**Reason for this priority**	**Desired deliverable(s)**	**Users**	**Additional information**
Citizen and property security – domestic and commercial markets.	Security alarms Risks include: burglary, personal attack, terrorism, etc	Lack of standardization in this specific area is resulting in each state making its own way, forcing product development to be done on national basis with individual certification schemes, etc - resulting in trade barriers.	European standard (PER and ORG) “Alarm confirmation - Methods and principles”	Equipment manufacturers; Installation and maintenance service providers; Monitoring organizations Police forces End Users (Domestic and commercial)	Affects a significant – and growing -proportion of all security alarm systems (hence a high proportion of the population, at home, at work, or both) installed in a number of countries, which is also growing. In some cases this has retrospective implications. The ability of many police forces to ensure adequate response to notified alarms in order to maintain security of citizens has been hampered for many years by the problem of “false” or “unwanted” alarms. Among the measures taken across Europe to minimize this is the process of “alarm confirmation” (sometimes referred to as “alarm verification”) to ensure that only genuine alarms are passed to police for response. As more countries adopt this principle, each adopts different methods, effectively returning to national standards and introducing trade barriers

ANNEX H: OVERVIEW OF PRIORITIES SUBMITTED BY CEN/TC 391 MEMBERS

Security area	Type of industry / type of threat	Reason for this priority	Desired deliverable(s)	Users	Additional information
					to both equipment and services. The most established methods are described in UK standard BS8243.
Citizen and property security – domestic and commercial markets	Security (and Fire) alarms and other systems Risks include: burglary, personal attack, terrorism, etc and fire	Expansion of use of new communications technology is being adopted, but without standardization, so that national independence exists in the manner in which security measures are implemented. This national independence inevitably leads to trade barriers and prevents design of interoperable systems. These variations also leave some systems vulnerable to being compromised because measures adopted are inadequate.	Upgrading of existing "alarm transmission system" standards (EN50136 series and EN54-21) to include requirements for secure remote connection to security (or fire) alarms or other systems for purposes other than simple transmission of alarms (PER). Additional standardization for protocols to permit interoperability (TEC). Adjustments to associated requirements for the alarms / security systems themselves (EN50131, EN50132, etc series and EN54 series) and for the monitoring centres (EN50518 series) and other remote locations from where operations are carried out (PER, ORG).	Equipment manufacturers; Installation and maintenance service providers; Monitoring organizations; Police forces; Fire Brigades; End Users (Domestic and commercial);	Affects a significant – and growing -proportion of all security and fire alarm systems installed – and hence a large proportion of the population, at work, at home or both.. Technology permits management, control, interrogation, upgrading and updating, maintenance and other functions to be performed from remote locations. These possibilities cannot completely eliminate the need for site maintenance, etc, but can significantly reduce it – hence reducing the "carbon footprint" associated with organizations providing such services. Properly used, it can also significantly enhance the services that can be provided and in doing so increase confidence in operation of systems. There is a need for standardization in this area, to ensure the security of the communication link without the introduction of effective trade barriers. Development of this technology in a standardized way will also open the way for true interoperability of systems. Some national documentations in place – UK: DD263 / DE: VDE 0833-1 / FR: APSAD Rule R31

ANNEX H: OVERVIEW OF PRIORITIES SUBMITTED BY CEN/TC 391 MEMBERS

TABLE 2: OVERVIEW OF PRIORITIES IN THE FIELD OF SECURITY STANDARDIZATION

Country: UK

Contact person: John Wood

Security area	Type of industry / type of threat	Reason for this priority	Desired deliverable(s)	Users	Additional information
Security of the Citizens	Major disasters, explosives, CBRN attacks, fires, pandemics	Populations are aging and additional attention will be required concerning the needs of elderly but healthy citizens.	A set of requirements whose application will ensure that the healthy elderly will not be disadvantaged	Emergency planners	*ISO/IEC Guide 71:2001, Guidelines for standards developers to address the needs of older persons and* *persons with disabilities* would provide a framework for the determination of the range and scope of the requirements
Security of the Citizens	Major disasters, explosives, CBRN attacks, fires, pandemics	The combination of aging population and the increasing sophistication of equipment makes it difficult for equipment designers and system specifiers to address the needs of the entire population. The standard would identify the requirements which need to be met to ensure that no one in the population is discriminated against.	Preparation of requirements for those designing equipment and services which will ensure that no-one in the population is disadvantaged by such factors as age, physique and background education from protective measures	Equipment and system specifiers/designers	*ISO/IEC Guide 71:2001, Guidelines for standards developers to address the needs of older persons and* *persons with disabilities* would provide a framework for the determination of the range and scope of the requirements. Products and systems which take account of the wider population will offer a competitive edge to those that do not address these issues
Security of the Citizens	Major disasters, explosives, CBRN attacks, fires, pandemics	European laws prohibit discrimination against those with disabilities and other vulnerable members of the population – including children. Equipment and systems tend to be designed with the young and reasonably fit in mind. This review would examine the special requirements of those members of the population with special needs and determine the requirements whereby their needs can be fully addressed.	A set of requirements, the application of which, will ensure that the no member of the community will be will be disadvantaged	Emergency planners	*ISO/IEC Guide 71:2001, Guidelines for standards developers to address the needs of older persons and* *persons with disabilities* would provide a framework for the determination of the range and scope of the requirements