Project acronym:	CRISP
Project title:	Evaluation and Certification Schemes for Security Products
Grant number:	607941
Programme:	Seventh Framework Programme for Security
Objective:	Topic SEC-2013.5.4-1 Evaluation and certification schemes for security products
Contract type:	Capability project
Start date of project:	01 April 2014
Duration:	36 months
Website:	www.crispproject.eu

Deliverable D1.1:

Glossary of security products and systems

Author(s):	VICESSE: Florian Fritz, Reinhard Kreissl, Roger von Laufenberg. Vrije Universiteit Brussel: Paul de Hert, Alessia Tanas, Rosamunde van Brakel. Technische Universität Berlin – INNO: Simone Wurster
Contributor(s):	Trilateral Research and Consulting Technische Universität Berlin – CTS
Dissemination level:	Public
Deliverable type:	Final
Version:	2
Submission date:	Due 31 May 2014 15 February 2016

Document revision history			
Version number	**Date of submission**	**Sections**	**Name**
Version 1.0	31st July 2014	all	Florian Fritz, Reinhard Kreissl, Roger von Laufenberg (VICESSE), Paul de Hert, Rosamunde van Brakel, Alessia Tanas, (VUB), Simone Wurster, (TUB INNO), Contributors: TUB CTS, Trilateral Research and Consulting.
Version 2.0	15th February 2016	Chapters 3 & 4, Annex	Roger von Laufenberg, Reinhard Kreissl (VICESSE) & contributions from Irene Kamara (VUB), Nathalie Hirschmann (TUB CTS), Cristina Pauner (UJI), Simone Wurster (TUB INNO), Jelena Burnik (IP-RS)

CRISP has received funding from the European Union's Seventh Framework Program for research, technological development and demonstration under grant agreement no 607941.

Table of Contents

1 Introduction 3
2 The creation of the Glossary 4
2.1 Literature 4
3 A function-oriented approach to security 5
3.1 What do we mean with security? 5
3.2 What about safety? 7
4 Our Concept 10
4.1 What are security-PSS? 10
4.2 Functions 10
4.3 Application Areas 12
4.4 Combining the parts – Security PSS, Functions and Application Areas 14
5 Glossary – Functions of security PSS 17
5.1 Primitive Functions 17
5.1.1 Information collection, storage and management to produce intelligence 17
5.1.2 Locate 19
5.1.3 Track 21
5.2 Connective Functions 23
5.2.1 Assess 23
5.2.2 Identify 26
5.2.3 Verify 28
5.3 Performative Functions 30
5.3.1 Authorise 30
5.3.2 Control 32
5.3.3 Create situational awareness (SA) 33
5.3.4 Detain 35
5.3.5 Prevent/Protect 37
6 Conclusion 40
7 References 41
8 Annex 46
8.1 CRISP-related terms and definitions for the Glossary 47
8.2 STEFi criteria terms 57

Table of Figures

Figure 1: Dependency of primitive, connective and performative functions of security PSS. 12
Figure 2: Matrix of the functions of security PSS within the different application areas. 39

1 INTRODUCTION

This Deliverable, a glossary of security products, systems and services (PSS), essentially serves a twofold purpose: on the one hand, it aims to lead to a better understanding of PSS, their typical application areas and core functionalities. On the other hand, such a glossary will help develop criteria that make PSS comparable and facilitate evaluation schemes. The glossary, as laid down in the Description of Work (DoW), "*takes the use of PSS as its starting point*"[1]. Functional requirements will lie at the heart of this deliverable, which is why a straightforward, pragmatic approach has been adopted. This means that concrete application areas of security PSS will be analysed, relying on pre-identified application instances of security PSS. As the DoW makes clear, one such starting point could be the ESRIF Final Report[2] and similar practice-oriented papers, but also more recent results from FP7 projects on-going or concluded, in order to highlight how security research has operationalised security functions.

The aim of the glossary is to display critical functions (see chapter 4.2) of security-related PSS across application areas. This will allow deriving criteria in support of requirements that new PSS will have to meet. Ultimately, it is *functions and capabilities of products, systems and services that are of relevance to security-related standardisation and certification processes*. The glossary is therefore not about detailed lists of individual PSS, but rather, it will contain core performance descriptions in application areas. The main reason for this is that, typically, the technology as such does not have distinctive features that would allow labelling it as a "security technology". Rather, it is the way technology is used and the purposes for its deployment (i.e. the security functions it has to fulfil) that designate *security*-technology. With regard to Work Package 1 as a whole and CRISP's subsequent Work Packages, the glossary will be the main starting point and thus also be important for the creation of the Taxonomy (as set out in project tasks 1.2 and 1.3).

This glossary is conceived of as a living document. This means that after the formal date of its submission, functions and use cases will be added throughout the project's lifecycle and as they are identified by the consortium members. Its content could also be the foundation for a wiki-like structure to increase usability and heighten visibility.

[1] CRISP, Evaluation and certification schemes for security products – Capability Project, Description of Work, p. 4.

[2] European Security Research and Innovation Forum (ESRIF), ESRIF Final report, December 2009. http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf. (Accessed 30.06.2014)

2 THE CREATION OF THE GLOSSARY

CRISP's description of work foresees that "[t]*he main objective* [...] *is to develop a glossary to describe PSS in the field of security*"[3]. The glossary should "*focus on ways of using or applying a given PSS and not on the material, physical or symbolic* [...] *features of the products*"[4]

2.1 LITERATURE

The sources for this analysis include policy documents related to security and security research, such the EU's 2010 Internal Security Strategy, or the European Commission's Security Research Catalogue[5], security research project deliverables and reports, for example of projects like PRISMS[6], SAPIENT[7] or the INDECT[8] project, to show on-going and completed research into security products, systems and services and takes account of security functions. Another important source for the creation of the glossary was the mandate M/487 of the European Commission to establish security standards, resulting of the technical committee CEN/TC 391 on Societal and Citizen Security. The mandate M/487 has produced two final reports, on the one hand analysing the current field of security standardisations[9] and on the other hand contributing to the further development of security standards by proposing work programmes and road maps.[10] This has proved to be useful since it establishes a general insight in the security standardisations and the needs and problems in the field. Furthermore, the mandate M/487 is also a crucial source for the upcoming work packages of the CRISP project and thus has to be taken into account, as it also provides for the general framework of the work package one and the CRISP project as a whole.

Complemented by additional reports such as those mentioned in the DoW, this breadth of literature should ensure sufficiently representative results.

Literature analysis has been guided by the overarching questions

- How are security functions conceived of and envisaged?
- Are there dominant areas (of security) for a given function?
- What are the intended use cases of security-related PSS?

[3] Ib.
[4] Ib.
[5] European Commission, EU Research for a Secure Society, Security Research Projects under the 7th Framework Programme for Research, Brussels, July 2012
[6] http://prismsproject.eu/ (Accessed 30.06.2014).
[7] http://www.sapientproject.eu/about.html (Accessed 30.06.2014).
[8] http://www.indect-project.eu/ (Accessed 30.06.2014).
[9] NEN Industry, *Mandate M/487 to establish security standards*, *Final Report Phase 1: Analysis of the current security landscape*, Delft, 9th May 2012.
[10] NEN Industry, *Mandate M/487 to Establish Security Standards, Final Report Phase 2: Proposed standardization work programmes and road maps*, Delft, 5th July 2013. Online at: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Fields/Defence/Security/M487_FinalReport.pdf.

3 A FUNCTION-ORIENTED APPROACH TO SECURITY

3.1 WHAT DO WE MEAN WITH SECURITY?

As argued in New Security Studies, the evolution of security has led to new concepts, subjects, objects and practices of security[11]. These new practices have, among other things, also to do with security technologies, commercial security practices and have led to new realities on the ground in Europe. Going beyond "classical" tenets of securitisation and speech act theory put forth by the Copenhagen School, such a "widening" of security that increasingly differentiates less between the police and the military and the internal and external dimension of the "security continuum"[12,13], has led to the acknowledgement[14] that "*it is increasingly clear that it is impossible to capture contemporary security practices within the confines of some of the most powerful inherited concepts and analytic specialisations and academic divisions that have traditionally dominated the subject.*"[15]

Part of those new practices is a European security market, with considerable growth projections for both products and services.[16] The security industry associated with this market faces several structural challenges, mainly of institutional nature and also as a result of new regulatory initiatives, e.g. with regard to data protection, but also in a more fundamental sense in the form of the societal dimension of security, which is something that should be considered by "*thoroughly assessing social impacts including impacts on fundamental rights, and by creating mechanisms to test the societal impact during the R&D phase*."[17] This problem – the "societal dimension" of the security market, has been further analysed by the FP7-funded project ASSERT[18] which has also put forth principles for taking societal considerations into account as early as possible in the development process.

As shown below, security practices and the requirements they pose to the development of PSS have been formulated as priorities in security-related policy documents (such as the Stockholm Programme[19] or the EU's Internal Security Strategy[20]) that are less concerned with conceptual problems but, rather, with practical problems as they arise throughout the EU. The glossary envisaged by WP1 is guided by these requirements and focuses on functional, i.e. application areas of PSS and looks at core capabilities these have to fulfil.

---

[11] Burgess, Peter J. (ed.), *The Routledge Handbook of New Security Studies*, Routledge, London, 2010.
[12] See for example the INEX project on conflicting ethical values in the internal/external security continuum in Europe, funded under FP7, http://www.inexproject.eu/ (Accessed 17.04.2014).
[13] Bigo, Didier, "The Möbius Ribbon of Internal and External Security(ies)", in Mathias Albert; Yosef Lapid; David Jacobson (eds.), *Identities, Borders, Orders*, University of Minnesota Press, 2001. p. 91 - 116.
[14] Williams, Michael C., "The new economy of security", *Global Crime*, Vol. 13, No.4, August 2012, pp.312-319.
[15] Williams, op. cit., 2012, p.312.
[16] European Commission, Security Industrial Policy, Action Plan for an innovative and competitive Security Industry, Communication from the Commission to the European Parliament, the Council, and the European Economic and Social Committee COM(2012) 417 final, Brussels, 26.7.2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF .
[17] Ib., p.6.
[18] www.assert-project.eu
[19] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:en:PDF (Accessed 15.7. 2014).
[20] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/internal-security/internal-security-strategy/index_en.htm (Accessed 15.7.2014).

For a common understanding of the glossary it is necessary to first of all provide a general understanding of the term security, with regard to the way it is used in this context. The British Cambridge online dictionary considers security as the *"protection of a person, building, organisation, or country against threats such as crime or attacks by foreign countries."*[21] Sinay provides a definition that centres on the concept's practical manifestations. According to this definition, security is "*a system of measures, including their embodiments and their interactions, designed to ward off intentionally destructive activity resulting in injury or material damage.*"[22]

Although this might already give a glimpse of the meaning of security, it is for the glossary crucial to extend this definition – especially considering the large field of security products, systems and services.

In a presentation on the needs of standards in security in 2006, Alois J. Sieber considered security to be "*the condition (perceived or confirmed) of an individual, a community, and organisation, a societal institution, a state, and their assets (such as goods, infrastructure), to be protected against danger or threats such as criminal activity, terrorism or other deliberate or hostile acts, disasters (natural and man-made).*"[23] While the first definition only relates to crime or attacks by foreign countries, the latter definition includes a wider variety of threats against which a larger range of infrastructures and groups need to be protected. A further interesting addendum to the understanding of security is provided by Auffermann & Kaskinen, who not only describe security as a condition or a state, but include the aspect of security as a political and analytical concept related to policy fields, leaving it flexible to the changing environment of threats.[24]

In the EU FP7 Projects PRISMS and ETTIS the different definitions and concepts of security are already dealt with at large, while not only focussing on the academic field but also on *'official high-level security documents'*[25]. As one of these high-level security documents the EU internal security strategy in action (ISS) plays an important role in the shaping of the area of research, by setting security policy priorities, and thus also of the glossary. In this the European Commission looks for strategies to *"be more effective in fighting and preventing* ***serious and organised crime****,* ***terrorism*** *and* ***cybercrime****, in strengthening the* ***management of our external borders*** *and in building* ***resilience to natural and man-made disasters****."*[26]

With these categories in mind, the different dimensions of security provided in the PRISMS

[21] http://dictionary.cambridge.org/dictionary/british/security_1?q=security (Accessed 16.04.2014).
[22] Sinay, Juraj, "Security Research and Safety Aspects in Slovakia." In: Thoma, Klaus (ed.), *European Perspectives on Security Research*, Springer Berlin Heidelberg 2011, pp. 81-90.
[23] Sieber, Alois J., *Needs for Standards in Security*, 2006, p.2. http://www.euritrack.org/Anglais/A.%20Sieber,%20J.%20Loeschner.pdf (Accessed 30.06.2014).
[24] Auffermann, Burkhard and Juha Kaskinen, "Introduction", *Security in Futures – Security in Change*, Writers & Finland Futures Research Centre, Turku, 2011, p.7.
[25] The Hague Centre for Strategic Studies, *Conceptual foundations of security*, D1.1, ETTIS Project, 30 June 2012, p.7.
[26] European Commission, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, Communication from the Commission to the European Parliament, and the Council, COM (2010) 673 final, Brussels, 22.11.2010, p.2.

deliverable 2.1 further add to the understanding of the notion of security:[27]

- Physical security: as an important aspect of producing secure measures in order to safeguard the *physical characteristics and properties* of citizens, infrastructure, objects, but also abstract/control systems.[28]
- Political security: as the protection of acquired rights such as human rights, established institutions/structures and recognized policy choices.
- Socio-Economic security: as the economic measures in order to grant the functioning and further developing of the economic system, but also its impact on individuals. The international labour organisation of the United Nations even goes further, by including the access to basic social security aspects (e.g. health, education, etc.) and work-place security (e.g. income security) in the socio-economic security and thus not only applying it solely on the more abstract economic system.[29]
- Cultural security: as securing important "traditional schemas of language, culture, associations, identity and religious practices".[30]
- Environmental security: as the producing of measures to provide safety from environmental dangers, as a result of natural, but also human processes, such as intense flooding, or scarcity of water.
- Radical uncertainty security: which deals with measures to exceptional/violent threats which are not deliberate – but can have a large impact.
- Information security: which is needed in order to protect information and information systems from unauthorized (remote) access, modification or disruption, especially in regard cyber security.

3.2 WHAT ABOUT SAFETY?

Conceptualising security also requires a closer look on the term safety in order to be able to make a distinction, but also show the possible overlaps between the two terms. This is especially important in the European context of the CRISP project, where the distinction between security and safety is not always as clear in other languages as it is in English. Just to have some examples: the German term 'Sicherheit' is used to describe both terms, linguistically there is no difference between security ('Sicherheit') and safety ('Sicherheit'). Alternatively the terms 'Schutz' (protection) and 'Gefahrlosigkeit' (safeness) could be used, although 'Sicherheit' is the more common term. Also in French the term 'sécurité' is used to describe both security and safety. Similar as in German, an extra term 'sûreté' is being used for safety in order to make this distinction – although it is not used frequently.

As we have shown already in our discussion on security above, the term is used with a strong

[27] See PRISMS D1.1 and D2.1.
[28] Kovacich, Gerald L. and Edward P. Halibozek, "Physical Security" in Fennely, Lawrence J., *Effective Physical Security*, Elsevier Inc., Waltham, Oxford, 2013, p. 339.
[29] United Nation International Labour Organisation Socio-Economic Security Programme, Definitions: What we mean when we say "economic security", http://www.ilo.org/public/english/protection/ses/download/docs/definition.pdf (Accessed 17.04.2014).
[30] Van Schoonhoven, Bas, Marc van Lieshout, Arnold Rosendaal, "Preliminary report on current developments and trends regarding technologies for security and privacy", Deliverable 2.1, PRISMS Project, 2013.

focus on external, deliberate threats and dangers on individuals, organisations, states, etc. Here is where mostly the differentiation between security and safety is based. Although Sieber includes in his general security definition "*disasters (natural and man-made)"*[31] and also the PRISMS project included in their dimensions of security "*radical uncertainty security*" as "*concerned with measures designed to provide safety from exceptional and rare violence/threats, which are not deliberately inflicted by an external or internal agent, but can still threaten drastically to degrade the quality of life*"[32], in many other conceptualisations of security non-deliberate threats and dangers are specifically excluded.

In 1992 Burns et al.[33] issued already an important contribution to the concepts of security and safety in computer systems, in which a first distinction between safety critical and security critical systems are made on the basis of whether the failure of the system can do *"immediate, direct harm"* or whether the failure *"could enable, or increase the ability of, others to* [do] *harm."*[34] While the first notion is used to describe the failure of safety critical systems, the latter is used for failures in security critical systems. A similar approach was chosen by Aven[35] for risk and vulnerability analyses tools. Aven discusses possible frameworks, methods and models that deal not only with *"the analysis and management of risks caused by accidents"* or "*accidental threats (hazards)*" which are used synonymously with safety related threats, but also enable the application of risk analysis and management on *"threats of intentional origin* (…) *risks related to sabotage and terrorism"* – ergo security.[36]

Sempere[37] has provided upon analysis of the research agenda of the European security industry – which the CRISP project also addresses to some extend[38] – a clear definition of what the security industry consists of, mainly *"as the industry that produces the goods and services required to protect citizens from insecurity."*[39] More specifically and related to insecurity, Sempere highlights five main sources of insecurity: armed conflicts, terrorism, organised crime, pandemics, and natural and man-made disasters. The security industry has a large focus on the first three sources in terms of products and services. Pandemics as a source of insecurity are dealt with in a combination between the security industry (in terms of chemical or biological attacks) and the health industry. Finally natural disasters such as earthquakes, floods, etc., and man-made disasters (technological or industrial accidents), are often dealt with by the safety industry with principal customers from health, civil protection and environmental protection agencies.[40]

---

[31] Sieber, Alois J., op. cit., 2006, p.2.
[32] Van Schoonhoven, et al., op. cit. 2013, p.12.
[33] Burns, Alan, John McDermid, and J. Dobson. "On the meaning of safety and security." The Computer Journal 35.1, 1992, 3-15.
[34] Ibid., p.4.
[35] Aven, Terje. "A unified framework for risk and vulnerability analysis covering both safety and security." Reliability Engineering and System Safety, 92, 2007, 745-754.
[36] Ibid., p.745
[37] Sempere, Martí. "The European Security Industry: A Research Agenda". Economics of Security Working Paper 29, 2010, Berlin: Economics of Security.
[38] CRISP, Evaluation and certification schemes for security products – Capability Project, Description of Work, Abstract.
[39] Sempere, Martí, op. cit., 2010, p.1.
[40] Cf. Ibid., p. 5.

Although there are some ties between the security and safety (and health) industry, mainly by addressing similar sources of insecurity as well as universally applicable equipment in order to mitigate damages, Sempere identifies a more or less clear distinction between intentional damage or threats, which are dealt with by the security industry and non-intentional threats, which are addressed by the health and safety industry.

Thus for the purpose of the CRISP project and the holistic approach a clear understanding of security and it's demarcation of safety has to be provided. While the main difference between security and safety lies in the degree of intention of the threat and damage dealt with, when applying this to security PSS it becomes clear that this distinction does not always hold (as Sempere also shows), since a PSS can contribute to both intentional inflicted damages, as well as unintentional, accidental inflicted damages. This leads to the approach on the security and safety distinction within CRISP – the CRISP *security* functions address primarily PSS with the purpose "*to protect citizens from insecurity*"[41] resulting from deliberate, intentional acts. PSS which additionally have a 'safety'-purpose can also be included within the *security* functions approach, especially regarding natural hazards and technological failures.[42] Similarly the areas of security presented in the next chapter address mainly *security* related topics, with *safety* in terms of non-intentional hazards only playing a bigger role in the area of crisis management. Specific *safety* functions, addressing *safety* PSS and dealing solely with non-intentional threats/hazards & accidents (e.g. work safety, road safety), are not part of the CRISP project and in a later stage also not considered by the CRISP certification.

[41] Ibid., p.1.

[42] This also closely correlates with what is defined as societal security by the ISO 22300:2012 Societal Security – Terminology: "societal security is the protection of society from, and response to, incidents, emergencies and disasters caused by intentional and unintentional human acts, natural hazards, and technical failures."

4 OUR CONCEPT

4.1 WHAT ARE SECURITY-PSS?

For the purposes of this deliverable, security-related products, systems and services are all those PSS which serve a security function (see 4.2), or which, in other words, give operators the capability to perform such functions. This means that it is the *context* that allows us to decide whether a PSS should be framed as "security-related" or not. The technology as such typically does not possess such a distinctive feature.

For the practical purposes of this deliverable, "products" would provide basic building blocks to provide a security function or capability as part of a given security measure or intervention, such as a simple camera or a sensor. Intuitively, "system" would typically refer to more complex combinations of such building blocks, their integration to a higher degree of complexity, coupling several "products", possibly also with a service. Products and systems, therefore, could also be classified in the following way:

- "Front-end" such as a body scanner or "back-end" such as a database;
- Stand-alone such as CCTV camera or integrated such as a CCTV camera coupled with an automated pattern recognition algorithm;
- Used on persons, objects, substances, data structures or processes.

Such a distinction of typologies is important as it influences the functionality and the way and where a security PSS is used. Specific examples elaborating this can be found in the glossary.

4.2 FUNCTIONS

By having a focus on the use case of security related products, systems and services, one has to look at how the specific PSS work or in other words function. Thus the functions describe the intended results of the security PSS as soon as they are in operation. While the glossary aims to precisely define the specific functions and tries to put them into the context of different application areas, one has to keep in mind that of course one specific function is seldom a stand-alone function of a certain security product, system or service which is more a multi-functional tool and needs all the combined functions to provide the intended results. This can end in two different manifestations. On the one hand, a GPS-system for example can fulfil both the locating as well as the tracking function and thus includes two (or more) functions within one security PSS. On the other hand, if one takes for example the iris-scanner – which similar to the GPS-system includes several functions, in this case identification and authorisation – this product also needs a database for identifying and thus includes the function information collection and management.

We start from a set of questions with which one can approach different security PSS proved to be helpful for the identification of the functions. Among them are:

- "What is / are the intended result(s) of the security PSS?"
- "How does the security PSS reach this result?"
- "What functions are needed for the performance of the security PSS?"
- "Can there be any unintended results of a security PSS and what function can be the reason of this?"

The literature review of other research projects[43], policy papers[44] and academic articles also proved useful for further identification of security functions. By this, the following functions have been recognised so far without claiming of being complete:

> locate, identify, verify, control, track, assess, authorise, create situational awareness, information collection, storage and management to produce intelligence, detain, prevent/protect.

It is anticipated that, as Work Package 1 progresses, especially with the creation of the taxonomy, but also as a result of the CRISP project as a whole, more functions will be identified and added to the glossary.

A classification of the functions can be done by choosing the different levels on which functions operate in security products, systems and services. The operational levels can be observed through the dependency of the functions on other functions – for example in order to identify, other security functions like information collection and processing need to be performed beforehand.[45] The categorisation thus is dependent on the interrelationship of the functions, resulting in *primitive*, *connective* and *performative* functions.

Primitive functions are the basic functions of security PSS and are essential for the further performance of other functions. They consist of information collection, storage and management, resulting in databases or other information storages. Locating and tracking can also be classified as a primitive functions, due to the necessity of location and tracking results for the threat assessment, protection of different application areas, or the detention of persons.

Connective functions make use of the primitive functions, mainly through connecting available information with specific criteria which then again can be necessary for the performance of further security related activities and functions. The most prominent example is the identification function, as it highly depends on (primitive) information collected beforehand, which afterwards is needed if one wants to authorise access. Connective functions are 'verify', 'identify' and 'assess.'

Performative functions finally are carried out (security) actions, with a clearly defined and targeted result, making use of one or both of the previous functions. For example in a security related setting, it is not possible to detain a person, if that person has not been identified on basis of available information and has not been located before. Performative functions are 'authorise', 'create situational awareness', 'prevent/protect', 'detain' and 'control.'

[43] E.g. SAPIENT project (Deliverable 1.1); PACT project (Deliverable 1.3); INDECT Project (Deliverable 2.1 and 9.4); SecureCHAINS project (Deliverable 2.3); PRISMS project (Deliverable 2.1), etc.
[44] E.g. EU's 2010 Internal Security Strategy; the European Commission's 2010 Security Research Catalogue.
[45] In the glossary and more specifically in the respective definitions of the functions, the relations and dependencies between the functions are further elaborated.

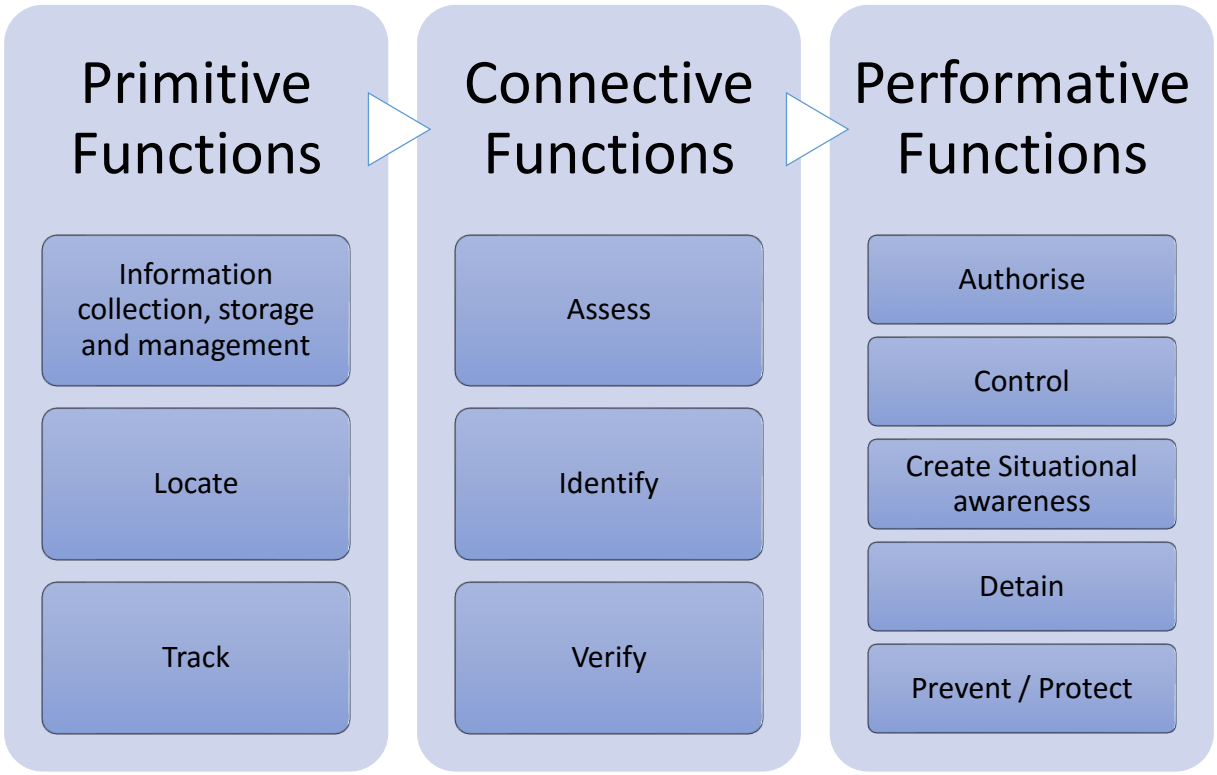

Figure 1: Dependency of primitive, connective and performative functions of security PSS.

4.3 APPLICATION AREAS

Based on the above mentioned definitions and dimensions of security, but also on the different EU Commission working papers, studies and standardisation mandates (e.g. ESRAB[46], ESRIF[47], security industrial policy[48], EU Internal Security Strategy in Action[49], Programming Mandate 487[50]) and also on the latest EU Research and Innovation programme Horizon 2020, we have used a common categorisation for the application areas in which security PSS are deployed. From an EU policy point of view and also with regard to the European security industries, the following categories mainly summarise the biggest security sectors regarding market size on a European and global level[51]: (1) aviation security[52]; (2) maritime security[53];

[46] European Security Research Advisory Board, *Meeting the challenge: the European Security Research Agenda*, Luxembourg Office for Official Publications of the European Communities, 2006.
[47] European Security Research & Innovation Forum, ESRIF Final Report, December 2009. http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf (Accessed 17.04.2014).
[48] European Commission, Commission Staff Working Paper, Security industrial policy, SWD(2012) 233 final, Brussels, 26.7.2012.
[49] European Commission, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, op. cit., 2010.
[50] European Commission, Programming Mandate addressed to CEN, CENELEC, and ETSI to establish security standards, M/487, Brussels 17.02.2011.
[51] C.f. European Commission, Commission Staff Working Paper, Security industrial policy, op. cit., 2012, p. 9.
[52] Examples of security-PSS include airport terminal and perimeter security systems, passenger screening systems, hand-held and checked-luggage screening systems, airport security command, control & communication IT and hardware infrastructure, reinforced blast-proof aircraft containers, explosives detection systems, etc.
[53] E.g. smart container systems, RFID container seal systems, container CBRNE screening systems, cruise ship & ferry passenger screening systems, deepwater security systems, or ship identification systems, etc.

(3) border security[54]; (4) critical infrastructure protection[55]; (5) counter-terror intelligence[56]; (6) physical security protection[57]; (7) protective clothing[58]. Since some of these security sectors within the *Security Industrial Policy* are repetitive, which one can also see in the related security PSS examples, the following application areas include those well without being too redundant.[59]

- Security of the citizens including counter terrorism, crime prevention and organised crime, and public order as necessary subareas. In general it covers all possible threat aiming at European citizens, in public and semi-public spaces as well as in private spaces, as a result of an intended/deliberate attack or a natural hazard, by trying to create a peaceful environment, including the prevention of radicalisation.
- Critical infrastructures includes the security of energy, transportation and telecommunication, supply chains, financing, health infrastructure, and also control systems – general infrastructures which are of high importance of the functioning of a vital society and thus a protection against threats aiming at the disruption or destruction of the like plays an important role in the European policy making and the security industry.[60]
- Border security includes the means for providing security of land, air and sea, but also of borders in embassies in order to prevent the illegitimate crossing of people. Further focus in border security aims also at the detection of illegal products, goods and substances within custom services. Especially after the 9/11 attack, this application area has seen an important increase of measures, mostly related to persons.[61]
- Crisis Management includes mainly the restoration of security in the aftermath of a crisis, which may result from a natural disaster, but also from deliberate attacks. Furthermore a focus within the European Union policy lies on the prevention and preparedness of crisis and disaster.[62] This application area is not to be confused with the crisis management in terms of bank recovery, which is currently being discussed on a

[54]E.g. border-perimeter interoperable communication systems, virtual border systems, checkpoint, fence and barrier hardware, border-perimeter people and workforce screening or biometric identification systems, CBRNE screening portals, etc.

[55]E.g. governmental critical infrastructure, medical and public health infrastructure, communication infrastructure or nuclear facilities terror mitigation security systems. But also critical infrastructure workforce and visitors identification and surveillance systems, governmental and private sector I.T. critical infrastructure security, banking and financial industry business continuity, or energy infrastructure security systems, etc.

[56] E.g. Command, control and communication systems, cyber space monitoring systems, cyber terror remediation systems, perimeter security systems, data fusion IT systems, land-based imagery systems, communication interoperability systems, information analysis software, cyber security and/or cyber surveillance IT systems, etc.

[57]E.g. CCTV systems, fire alarm, intruder alarm systems, burglar alarm systems, communication systems, etc.

[58] E.g. CBRN personal protection gear, CBRN air filtering systems, protective clothing for police forces or fire fighters, search and rescue equipment, etc.

[59] See for example the SecureCHAINS project as one of many security-related projects that also use similar categorisations. Martínez, Cristina, Olaf Poenicke, James Brennan, John Dering, Mahary Ramasindraibe, *"Technology Tree"*, D2.3, SecureCHAINS project, 15th May 2012, p. 15ff.

[60] In the EU Frameworks, there are although some priorities of specific subareas, such as aviation and maritime security compared to ICT security. (c.f. ECORYS, Security Regulation, Conformity Assessment & Certification. Final Report – Volume I: Main Report, ECORYS Nederland BV, Rotterdam, The Netherlands, 2011, p. 33f.

[61] C.f. ib. p. 35.

[62] European Commission, Delivering an area of freedom, security and justice for Europe's citizens, Action Plan Implementing the Stockholm Programme, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 171 final, Brussels, 20.4.2010, p. 6.

European level as well.[63]

Such a delimitation is inevitably to a certain degree arbitrary. Its added value lies, among other things, in showing how different functions play out in different contexts (and by context we mean the application "area").

A somewhat different choice of classification was adopted by FEMA, the US-Federal Emergency Management Agency, in its 2007 "Target Capability List"[64] and the 2011 "Crosswalk of Target Capabilities to Core Capabilities"[65]. This approach does not classify "horizontally" into security areas. Instead, FEMA follows a process-oriented and requirement-driven approach, highlighting which phases an "incident" can be segmented into and then deriving critical capabilities (which pose requirements for security products, systems and services) from each phase. These phases, shown here for illustrative purposes, are:

1. Prevention
2. Protection
3. Mitigation
4. Response
5. Recovery

Strongly driven by logics of disaster management, this approach focuses on chronological priorities. Products, systems and services could assume different functionalities under different priority areas.

CRISP Deliverable 1.2, setting out a taxonomy of security-related PSS, will further elaborate on criteria by which product and services can be further categorised. One source such categorisation could draw on is the security functionality performed by the PSS.

4.4 Combining the parts – Security PSS, Functions and Application Areas

As already described, the glossary aims at showing different functionalities which can be found in different security PSS and also relating them to the broad field of security application areas in which the security PSS are intended to be used. This glossary doesn't claim to be exhaustive and only shows a first glimpse at functions of security-related PSS. By this the glossary should make clear the variety of contexts in which security functions can be put into practice and thus "showcase" the field of security PSS from the perspective of security functions.[66]

A similar approach has been chosen by Pawson & Tilley (1997)[67], by using another terminology – they describe mechanisms (instead of functions) and contexts (instead of application areas) –

---

[63] European Commission, "The EU single market, banking, crisis management" http://ec.europa.eu/internal_market/bank/crisis_management/index_en.htm (Accessed 04.06.2014).
[64] U.S. Department of Homeland Security, Target Capabilities List, A companion to the National Preparedness Guidelines, September 2007, http://www.fema.gov/pdf/government/training/tcl.pdf (Accessed 30.06.2014).
[65] U.S. Department of Homeland Security, Crosswalk of Target Capabilities to Core Capabilities http://www.fema.gov/media-library-data/20130726-1854-25045-1651/crosswalk_1_.pdf (Accessed 30.06.2014).
[66] The final set functions presented in this glossary has been derived from analysis and literature review. An initial body of work was sent out to partners who complemented.
[67] Pawson, Ray and Nick Tilley, Realistic Evaluation, Sage Publications Ltd., London, Thousand Oaks, New Delhi, 1997.

and also including much more the societal impact in general, an area which cannot be covered by the present glossary. The definitions Pawson & Tilley use for their terms might still help us to get a better grasp of how to approach the functions and application areas and what this means for the research, but also for comparison of security PSS.

Program mechanisms, the function-equivalent in 'realistic evaluation', go beyond the question of "whether a program works" to trying to answer the question of "what it is about a program which makes it work." Thereby they reflect the *"embeddedness of the program within the stratified nature of social reality"* (…), providing *an "account of how both macro and micro processes constitute the program"* and *"demonstrate how program outputs follow from the stakeholders' choices (reasoning) and their capacity (resources) to put these into practice."*[68] Thus also here, by aiming to understand how a security function is put in place, both the way and where the measure or technology is implemented all need to be taken into account. The latter takes us to the second term, the context in which such a measure is being deployed, which mainly denotes the conditionality of the effects of a function.

For the purposes of this deliverable, we have refined and adapted Pawson & Tilley's broad conceptual scope. "Functions" here denote intended effects and consequences of technology/service deployment as part of a security measure being taken. "Context" has been distilled to "use cases". Taking the example of the effect of CCTV surveillance in a car park in order to lower crime rates (as in Pawson & Tilley's 'realistic evaluation'[69]): Most of the functions of a CCTV camera are easy to determine, like for example locating or identifying. But on the other hand, secondary functions are much more difficult to determine, to describe, and thus also to certify. Pawson & Tilley for example mention "the 'noisy parker' mechanism" as a function of CCTV surveillance in a car park, which is the increased usage of a car park through the increased security through the surveillance and thus resulting in an avoidance of the car park by potential offenders, since there are more people that could notice a crime – thus resulting in a 'natural surveillance.' What this example nicely demonstrates is the effect of wider contextual factors, creating effects not to be read off the PPS when seen in isolation or a laboratory setting.

For an illustrative purpose, a matrix of the security PSS functions within the application areas has been created[70], which serves especially to on the one hand provide an overview of the functions. On the other hand it can be used to attribute different functions and application areas to one specified security PSS and thus providing a schematic illustration of the use case of specific PSS. Furthermore, the inclusion of 'security threats' against which the security PSS are aimed, could be an extra possibility to classify functions in specific security application areas.[71]

---

[68] Ib., p. 66.
[69] See ib., p. 78.
[70] See Fig. 2 in section 5 Glossary – Functions of security PSS, p.35.
[71] The ECORYS *Study on the Competitiveness of the EU security industry* for example noticed the possibility of a security threat approach in order to define the industry security sector, since security threats are translated in security missions and requirements. In the ECORYS study, the distinction is made between traditional security (e.g. ordinary criminal activity, fire protection, etc.) and new or emerging security (e.g. terrorism, cybercrime, major catastrophic events). C.f. ECORYS, *Study on the Competitiveness of the EU security industry*, Within the Framework Contract for Sectorial Competitiveness Studies – ENTR/06/054, ECORYS Nederland BV, Rotterdam, The Netherlands, 2009, p. 11f.

As we consider the glossary to be a living document, it is envisaged to keep it up to date throughout the project's lifecycle and keep adding functionalities or use cases of security-related products, systems and services. For this, it is envisaged to include the glossary on the CRISP homepage which will be extended and updated on a regularly basis throughout the duration of the CRISP project.

5 GLOSSARY – FUNCTIONS OF SECURITY PSS

5.1 PRIMITIVE FUNCTIONS

5.1.1 Information collection, storage and management to produce intelligence

These functions are a crucial part of security PSS, as without information collection storage and management a lot of the other functions would be limited to a large extent. Mainly, those functions can be found in the area of border security, gathering and storage in ad-hoc databases[72] of biometric data, primarily fingerprints and facial features, belonging to applicants to visas or to illegal immigrants.[73,74] Access by national authorities and international law enforcement agencies (such as Europol) to such data is necessary. Also the gathering and storage in ad hoc databases of passenger data can provide predictions on suspicious passengers.[75] Furthermore, the gathering of intelligence through (tele)communications data of suspected terrorists, related to the storage of (tele)communications data for future analysis is an important part of the functionalities.[76]

Within crime prevention, information collection, storage and management functions are also very diverse and can cover different preventive measures. This can range from the establishment of a platform for exchanging best practices, research and information on different aspects of local crime prevention, to the creation of an observatory for the prevention of crime to gather more information. Also, the predicting on the basis of collected data in databases can result from information collection, storage and management, in order to identify which areas of the city are at higher risk of crime and which types of people have a higher risk to commit crime.[77]

Support to multinational and interdisciplinary research and knowledge dissemination in the field of natural hazards, addressing mainly climate and geological-related hazards such as floods, landslides, avalanches, forest fires, earthquakes and volcanic eruptions in the EU is also an important part of the intelligence production.[78] Similar can also be regarded the development

---

[72] E.g. the Schengen Information System (SIS II), a system for national border control authorities and judicial authorities, easing the access to information on persons and objects; EURODAC, a fingerprint database of asylum applicants in the EU; or the Europol Information system, a database for offences and the individuals involved, in order to fight organised crime, terrorism and other forms of serious crime.

[73] European Parliament and the Council, Regulation (EC) No 767/2008 of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218/60, 13.08.2008.

[74] C.f. eu-LISA, Annual report on the 2013 activities of the Central Unit of Eurodac pursuant to Article 24(1) of Regulation (EC) No 2725/2000. http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010898%202014%20INIT (Accessed 30.06.2014).

[75] European Commission, Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, 2011/0023 (COD), Brussels, 2.2.2011. http://ec.europa.eu/home-affairs/news/intro/docs/com_2011_32_en.pdf (Accessed 30.06.2014).

[76] C.f. Bigo, Didier, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi, Amandine Scherrer, National Programmes for Mass Surveillance of Personal Data in EU Member States and their Compatibility with EU Law, Brussels, October 2013. http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET%282013%29493032_EN.pdf (Accessed 30.06.2014).

[77] European Council Decision 2009/902/JHA of 30 November 2009 setting up a European Crime Prevention Network (EUCPN) and repealing Decision 2001/427/JHA, OJ L 321, 8.12.2009.

[78] European Commission, Directorate General Research and Innovation web-site, web-page:

of regular reviews[79] and threat assessment reports[80] including the access by the European Commission and EU Member States to (sensitive and non-sensitive information) gathered from those reviews and threat reports, aiming at the security of critical infrastructure. This would also include the gathering of expert knowledge for a better understanding of criticalities and interdependencies among infrastructures,[81,82] specifically to counteract terrorism.[83] Within this the existence of a warning information network serving as data repository[84] can also play an important part.

Information-exchange systems designed to improve management of EU external borders and the near real time sharing of border-related data between interested Member States,[85] are essential within border security, which also guarantees the identification and verification functionality.[86]

http://ec.europa.eu/research/environment/index_en.cfm?pg=hazards (Accessed 30.06.2014).

[79] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, article 5.

[80] Ib., article 7.

[81] European Commission, Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection, Making European Critical Infrastructures more secure, SWD(2013) 318 final, Brussels, 28.8.2013. http://ec.europa.eu/energy/infrastructure/doc/critical/20130828_epcip_commission_staff_working_document.pdf (Accessed 30.06.2014).

[82] According to the document of European Commission, Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection, Making European Critical Infrastructures more secure, SWD(2013) 318 final, Brussels, 28.8.2013, the concept of interdependency among infrastructures, deals with the identification and the sharing of information on the state of two cross-border energy infrastructures which are interdependent, meaning that the state of one infrastructure on one side of the border influences or is correlated to the state of the infrastructure on the other side of the border.

[83] Ib., page 6.

[84] Ib., page 5.

[85] Frontex, Best Practice Technical Guidelines for Automated Border Control (ABC) Systems, Research and Development Unit, Last reviewed on 31/08/2012, page 21. http://frontex.europa.eu/assets/Publications/Research/Best_Practice_Technical_Guidelines_for_Automated_Border_Control_Systems.pdf (Accessed 30.06.2014).

[86] European Parliament and the Council, Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013, establishing the European Border Surveillance System (Eurosur) L 295/11, 6.11.2013.

5.1.2 Locate

While generally to locate means to *'discover the exact place or position of"*[87] a certain person, object or substance, the wide variety of things that can be located also give account of the variety of areas where locating-security-PSS can come into play. The locating function of a security-PSS is also often combined with the detection as well as with the tracking function – also from time to time in one 'location tracking' function.[88] A more specific, security related definition of 'to locate' can be found in the PACT project,[89] where the function is already closely linked to the location determination technology itself, which *"enable*[s] *the collection of geospatial data regarding a specific individual, object or area."*[90] The advantage of the latter as against the dictionary definition lies in the exact task that needs to be fulfilled if a security PSS needs 'to locate', as it not only implies the discovery of a position, but also the collection of – geospatial – data.

One example can be found in sea border security, where one of the main security threats is the illegal migration, but also side-effects like organised crime, human, drugs and weapon trafficking play an important role. Here one of the main needs on the level of state authorities is the detection and locating of threats and suspicious objects and subjects, such as small boats within a large maritime environment. This can be achieved on the one hand through manpower in form of coast guard ships, airplanes and helicopters. On the other hand, security products like the autonomous maritime surveillance system (AMASS), use an unmanned sea surveillance platform which is able to automatically detect and locate small boats and submit the information to a control station.[91] The platform works as a front-end but integrated security product, especially used on objects like boats and on persons.

Another, more broader field of locating functionalities in security PSS – also combined with tracking function – is used by navigation and tracking technologies like Radio-Frequency Identification (RFID) tags, Global Positioning Systems (GPS) or GSM triangulation. Especially mobile devices that are switched on can be located through GSM, UMTS and LTE technologies, since "*the device reveals to the telecommunications provider where they are, with an accuracy of several hundred meters."*[92] While the main function is to locate a mobile device and thus also the person to whom the device belongs, the function can only be performed in a system and several other functions are here needed in order to fulfil the locating function. Those might include gathering and processing of data, but also the communication of the device with the system.[93] The locating function in navigation and tracking technologies are needed in several security areas, like in counter terrorism – the GSM location of potential terrorist threads –,

---

[87] http://www.oxforddictionaries.com/definition/english/locate?q=to+locate (Accessed 25.05.2014).
[88] Some of the following examples thus also closely related to the function 'track', described in section 5.10.
[89] PACT: Public perception of security and privacy: Assessing knowledge, Collecting evidence, Translating research into action – a FP7 funded project.
[90] García, et al., op. cit., 2012, p. 111.
[91] Carl Zeiss Optronics GmbH, "AMASS: Autonomous maritime surveillance system". http://www.amass-project.eu/amassproject/content/index (Accessed 27.05.2014).
[92] Van Schoonhoven, Bas, Marc van Lieshout, Arnold Rosendaal, "*Preliminary report on current developments and trends regarding technologies for security and privacy",* D.2.1 PRISMS project, 28th February 2013, p.29.
[93] C.f. Sobański, Grzegorz, Paweł Lubarski, Mikołaj Sobczak, *"Preliminary report on proposed logical structure of the systems"*, D.2.1 INDECT project, 31st December 2009, p.11ff.

supply chains – RFID tags for hazardous products –, but also in crisis management – GPS locators for personnel in high-risk environments.

Further security PSS with locating functions often work in a similar way in a system only, like for example CCTV cameras which need other components in order to detect and locate crimes, like control rooms or the intelligence and communication from the public.[94] The examples thus show, that not only the locating function rarely is a stand-alone function but combined with others and also works within a system of security products.

[94] Gill, Martin, Angela Spriggs, *"Assessing the impact of CCTV",* Home Office Research Study 292, February 2005, p.xii f.

5.1.3 Track

The security function of tracking could be framed as to "*monitor the physical location of an item, a shipment or a vehicle*."[95] Yet this can be easily expanded to also include tracking for persons in different settings. Another definition refers to tracking as to "*determine who was in a geographic area* [...] *at a particular time*,"[96] linking this security function closely to surveillance tasks. The track-function is being scrutinised broadly in the context of smart surveillance. PSS serving this function are used to "*locate or track the movements of a person or object*."[97] A definition of tracking depends heavily on the usage context of the PSS deployed. Tracking functions can be scaled up or down in terms of distance to their object (e.g. PSS directly on perimeter or satellite-baked technology) or across temporal parameters from real-time tasks or lengthier or ex-post tasks involving e.g. RFID travel cards that allow to "*track individuals or items*"[98] (ib.: p.59). Tracking also applies in cyber-environments (in its simplest form, tracking cookies and similar tracking technology used to monitor site visits).

Beyond obvious application areas like surveillance, there is also reference to "Tracking" with regard to staying on top of terrorist money laundering and financing (s. below). PSS serving the security function of tracking are of relevance in any scenario that requires an accurate picture of the position of "tangible" objects such as an item, a person, a cargo shipment, or more of more "abstract" categories such as capital flows. As a popular, non-scientific website puts it, "Location tracking is not one, single technology. Rather, it is the convergence of several technologies that can be merged to create systems that track inventory, livestock or -vehicle fleets. Similar systems can be created to deliver location-based services to wireless devices."[99]

The technological contexts of the tracking functionality Bonsor provides include Geographic Information Systems (GIS), Global positioning systems (GPS), Radio Frequency Identification (RFID) and Wireless Local Area Networks (WLAN). Additional means of delivery of tracking functionality mentioned by the SAPIENT project include Satellite based surveillance, mobile phone tracking and UAVs (unmanned aircraft systems).

FP7 Research projects involving this function include:

- ADABTS: Develop sensors, processing methods and algorithms to (a) detect and (b) track people in complex environments, involving groups of people or crowds. This entire process is to be automated. The use case given is the "protection of EU citizens, property and infrastructure against threats of terrorism, crime and riots."[100]
- ISMK: Applying the tracking functionality on goods, vehicles and individuals should provide for an enhanced situational awareness.[101]
- SAMURAI: providing for a "classical" surveillance setting, this project was about

[95] EN 14943:2005-12: Transport services - Logistics - Glossary of terms
[96] PACT Project D1.3 „Report on Technology Taxonomy and Mapping", p. 25.
[97] Bellanova, et al., op. cit., 2012, p.58.
[98] Ib., p. 59.
[99] Bonsor, Kevin, "How Location Tracking Works", HowStuffWorks.com. http://electronics.howstuffworks.com/everyday-tech/location-tracking.htm (Accessed 27.05. 2014).
[100] European Commission, Investing into security research to for the benefits of European citizens. Security research projects under the 7th framework programme for research, Brussels, September 2010, p.4
[101] Ib., p.76.

developing moving objects segmentation, categorisation and tagging in video feeds captured by multiple cameras. This allowed for the "*tracking of people with luggage between different locations at an airport*."[102]

- SEABILLA (Sea border surveillance): the objective of this border security – related project was to "*Develop and demonstrate on the field significant improvements in detection, tracking, identification and automated behaviour analysis of all vessels, including hard to detect vessels, in open waters as well as close to coast.*"[103] To achieve this objective, the project aimed at **combining** advanced (and already existing) technology. Such assemblages should be targeted against drug trafficking, illegal migration in the Mediterranean, and fighting illicit maritime activities in pursuit of the EU's Maritime Policy. Like technology assemblage, this projects sees a "functionality-assemblage", i.e. putting together and sequencing security functions: to detect what is out there, to provide capabilities to track the findings, and eventually to identify the "target".
- SECTRONIC, another project related to maritime security, "*Accurately observes, characterizes and tracks any object of significance, 360 degrees around an infrastructure, 24 h a day in all weather conditions by means of - Near range equipment; - Far range equipment."*[104,105] It combines this 24/7 tracking capability of maritime objects (port infrastructures, passenger transport, energy transport) with other security functions: it **communicates** its findings to authorities, and it **aggregates** security-related information. To provide tracking functionality, the project relies on the interaction of satellites, servers and onshore control centres.
- SUBITO (surveillance of unattended baggage and the identification and tracking of the owner):[106] having detected abandoned luggage and identified the person having left it, the developed solution tracks this person by retracing and displaying their path. Tracking, in this context, means to establish, possibly ex post, movement patterns and to recreate "the whole picture" of the path followed by the "suspect."

Tracking, as becomes clear from these examples, is a key function that contributes to situational awareness (see entry in this glossary). Tracking is closely related to locating (see entry) – as opposed to the latter, it attempts to establish or retrace movement patterns or paths, while locating focuses on entering an entity in the bigger picture in the first place (you cannot track what you have not previously located, as tracking is about connecting single dots to an overall trajectory). PSS under this functionality could be deployed to track persons, goods but also behaviour or (recurring) movement patterns.

[102] Ib., p.118.
[103] Ib., p.120.
[104] Which again highlights the importance of an important aspect: that the functionality determines and preconditions the deployment of products, systems, and services – long range equipment may refer to an array of technology or systems which are entirely different than short-range solutions, yet the PSS addressed still serves the same functionality: to track objects (here in a maritime scenario) and thereby to contribute to decision support and to enhancing situational awareness.
[105] Ib., p.124.
[106] Ib., p.144.

5.2 CONNECTIVE FUNCTIONS

5.2.1 Assess

Assessing a situation is a widespread function to which systems, products and services across the security areas contribute. While Merriam Webster's dictionary holds that this function relates to making a judgement about something or to officially say what the amount or value of something is[107], the Oxford dictionary defines it as "evaluate or estimate the nature, ability, or quality of"[108]. Collins dictionary defines the term as "to estimate or determine the significance, importance or value of"[109]. "Assessing" usually encompasses risk or threat assessments, but also targeted assessments of behaviour through profiling[110] approaches. The function mainly consists of ascribing a predefined value to a certain situation or a range of hazards or threats. This process is based on information that has to be gathered, merged and displayed (different functions) in a previous phase. This function is about delivering priorities and assigning tasks according to these priorities.

The FP7 project EMPHASIS, aiming at the development of a security system capable of detecting explosives and precursor substances even before their assemblage process, frames "assessing" as "*intelligence-led assessment of an area of a city in order to establish where, and more crucially when illicit bomb-making activity is occurring*"[111] The European Commission's 2012 "*Action Plan for an innovative and competitive Security Industry, Staff working document*"[112] mentions two use cases for the "assess" functionality: threat assessment and risk assessment.[113] The EU's Internal Security Strategy[114] mentions risk and threat assessment in numerous security domains (across the priority areas it identifies), and frames the "assess" functionality of security PSS as a basic decision support tool: *"The EU should establish* [...] *a coherent risk management policy linking threat and risk assessments to decision making*."[115] Risk assessment and threat assessment are seen as key decision support tools, yet knowledge of the modes and approaches to carrying out such assessments is taken as granted. It is not made clear on what mechanisms such assessment procedures would have to rely on. The Strategy mentions the problem of national fragmentation of EU Member States' threat assessments and that the EU would contribute to a mutual understand of threat levels and to improved communication about threat levels.

Another example, taken from the EU's directive on European Critical Infrastructures[116],

---

[107] http://www.merriam-webster.com/dictionary/assess (Accessed 04.07.2014)
[108] http://www.oxforddictionaries.com/definition/english/assess?q=assess (Accessed 04.07.2014)
[109] http://www.collinsdictionary.com/dictionary/american/assess?showCookiePolicy=true (Accessed 04.07.2014)
[110] "Profiling" is a technique described e.g. in Clarke, Roger, "Profiling: A Hidden Challenge to the Regulation of Data Surveillance", *Journal of Law and Information Science*, Vol. 4, No. 2, 1993, pp. 403-419.
[111] European Commission, EU Research for a Secure Society, Security Research Projects under the 7th Framework Programme for Research, July 2012, p.24.
[112] European Commission, Commission Staff Working Paper, *Security Industrial Policy*, op. cit., 2012.
[113] Ib., p.7.
[114] European Commission, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, op. cit., 2009.
[115] Ib., p. 14.
[116] European Parliament and the Council, Directive 2008/114/EC on the identification and designation of European critical infrastructures. OJ L 345/75, 23.12.2008.

illustrates *assessing* as a political act, to be based on and informed by information previously gathered, merged (see *situational awareness* entry in the glossary) and analysed. The directive calls for an assessment of the need to improve the protection of individual infrastructures. This needs assessments leads to a prioritisation.

The EU's "Secret Service", the Intelligence Analysis Centre (EU INTCEN), provides monitoring and assessment of international events. These assessments, again to be framed as value ascriptions, e.g. in terms of "severity" of a threat or a natural hazards, lead to intelligence analyses and early warning reports.[117]

Assessing is also being referred to, in the EU's Internal Security Strategy, as a specific needs assessment, e.g. in the area of border security, where the policy priority is formulated as: "*Enhancing the contribution of FRONTEX at the external borders*"[118]. The service of drawing up a regular report „*as a basis for assessing the need for FRONTEX* [...]" should serve this „*needs assessment.*"

As it becomes clear from these samples, "assess" refers to two types of actions in the field of security (research):

- Assessing a threat, risk or hazard on the basis of data and information collection,
- Assessing the effectiveness and efficiency of a security technology and measure.

While both aspects are important, this glossary focuses on the first case.

What becomes clear is that assessing cannot rely one mode or technology or service. Rather, it is a complex, multi-modal deployment of all of these. Typically, assessment as the conclusions from available information would build on PSS that contribute to creating situational awareness.

Security research projects referring to the "assess"-functionality of PSS (based on analysis of the Commission's Security Research catalogue from 2012[119]) include:

HYPERION: Develops a system for the on-site forensic analysis of an explosion. This system will deliver data that can be used to make an on-site assessment of the improvised explosive that likely caused the detonation. This also includes an assessment of the detonation's point of origin, the size of the explosive charge. Data should also be useable for an assessment whether the bomb was vehicle borne, person borne or was placed in a "left behind" item.

LOTUS: This project aims to locate threat substances in urban societies. The result is a network of sensors across a predefined area, "*producing GPS pinpointed reports on potential explosive or drug manufacture locations for central assessment.*"[120] This shows a typical structure for assessment functions, relying on centrally gathered sensor data. This also suggests the

[117] Van Buuren, Jelle, *Secret Truth. The EU Joint Situation Centre*, Eurowatch, Amsterdam, 2009.
[118] European Commission, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, op. cit., 2009, p. 12.
[119] European Commission, EU Research for a Secure Society, Security Research Projects under the 7th Framework Programme for Research, Brussels, July 2012
[120] Ib., p. 37.

conceptual proximity of the assess-function to situational awareness functionality which typically also operates centrally, relying on incoming data streams.

SUBITO: This project is an example for the use of automated mechanisms for threat assessments: focusing on the problem of unattended baggage, the project carried out research into algorithms used to identify lost luggage, also coupled with novel ways of processing visual images. The processing algorithms were developed to better categorise critical situations that might arise. This should be done by specific use of sensing data on the objects and persons in their environment. Assessment, in this sample, also involved category development and should allow for forecasts based on the information collected and its procession by the algorithms.

FESTOS: Assessment is carried out to priorities threats originating from emerging technologies. This means that in FESTOS they were assessed against the destructive potential. The main methodology is expert surveys.

The project **TWOBIAS** shows another characteristic use case for the "assess"-functionality: to assess user requirements which a security-related system or service have to fulfil. Assessment in this context contributes to increasing the levels of usability and appropriateness of the developed solutions.

Frequently, and as already mentioned above, "assess" is a functionality for self-testing and validating of security-PSS (and whether the developed solutions and measures fulfil the security tasks foreseen). This reflexive understanding of assessment, focussing on the usability and applicability of a given PSS is not of special relevance here. Rather the assess function should be understood in the way it is used in the LOTUS project, as security, vulnerability or threat assessment.

5.2.2 Identify

In the Merriam-Webster dictionary, three different definitions can be found for the verb 'identify' which gives already an idea of the wider implication of the identify function of security PSS. Identify thus means *"to know and say who someone is or what something is; to find out who someone is or what something is; to show who someone is or what something is".*[121]The security related definition specifies already the necessity of a database of some kind, in order to be able to identify a person[122], while this might not entirely be necessary in case of object or substance identification.

Within the DIN terminology portal definitions of 'identify', related to specific security products and systems can be found. The Electronic Registration Identification (ERI) for vehicles defines 'to identify' as the *"action or act of establishing the identity"*[123], the Health informatics - Secure User Identification for Health Care as the *"process that enables recognition of an authorised user described to the system, by the use of a unique user identifier*"[124] and the guidance for the characterization of the genetically modified organism by analysis of the genomic modification as the *"establishment of identity by comparison with a reference*".[125]

Also the PACT project gives a good overview of the different security areas of identification functionality, the security products and systems it is included in and also on the different persons, objects or substances it is aimed at. Visual surveillance[126] – mostly video cameras – is used in a wide variety of security areas, in national or international borders, at critical infrastructures like airports and also for the security of the citizens, especially in the urban area. On the one hand within these areas the identification of people/faces is desired as well as the identification of suspicious behaviour, when the security PSS is aimed at persons. On the other hand, the identification of suspicious objects (e.g. weapons) or substances (e.g. explosives) plays an important role, and even though CCTV systems can come into play, also body scanners play their part in the identification of objects and substances. A step further goes the number plate identification, which has the function to identify a person through the object. All these identifying functionalities need not only a CCTV camera, but also intelligent video analysis,

---

[121] http://www.merriam-webster.com/dictionary/identify (Accessed 30.06.2014).
[122] C.f. Bellanova, Rocco, Matthias Vermeulen, Serge Gutwirth, Rachel Finn, Paul McCarthy, David Wright, Kush Wadhwa, Dara Hallinan, Michael Friedewald, Marc Langheinrich, Vlad Coroama, Julien Jeandesboz, Didier Bigo, Mervyn Frost, Silvia Venier, *"Smart Surveillance – State of the Art",* D.1.1 SAPIENT project, 23rd January 2012, p. 54f.
[123] DIN EN ISO 24534-4: Automatic vehicle and equipment identification - Electronic Registration Identification (ERI) for vehicles - Part 4: Secure communications using asymmetrical techniques (ISO 24534-4:2010); English version EN ISO 24534-4:2010.
[124] DIN EN 12251: Health informatics - Secure User Identification for Health Care - Management and Security of Authentication by Passwords; English version EN 12251:2004.
[125]EN 12687 Biotechnology - Modified organisms for application in the environment - Guidance for the characterization of the genetically modified organism by analysis of the genomic modification.
[126] In the PACT project, visual surveillance are *"surveillance systems which mostly rely on "observer devices" video-camera sensors",* and includes the related *"computational intelligence and data management and storage activities,* […] [making] *heavy use of video analysis techniques."*
García, Alberto Crespo, Aranda, Nuria Ituarte, Tsakonas, Panagiotis, Tsoulkas, Vasilis, Kostopoulos, Dimitris, Domb, Avi, Levinson, Jay, Kyriazanos, Dimitris M., Segou, Olga, Malatesta, Lori, Liatas, Christos, Argyreas, Nikos, Thomopoulos, Stelios C. A. "Report on Technology Taxonomy and Mapping", D.1.3 PACT project, June 5th 2012, p. 21f,

like pattern recognition systems.[127] Further identifying security products within this 'visual surveillance technology' – aiming on objects as well as on persons are unmanned aircraft systems, able to identify from a height of a few hundred feet to as high as 60.000 feet.[128]

Another area, within which the identification function plays a part is what is proposed in the PACT project as 'dataveillance', a term coined by Roger Clarke meaning "*the systematic surveillance of individuals or groups based on the electronic data trails they leave in the information society."*[129] While this is of course closely related to the information collection and management function, one of purposes of the dataveillance technology is to identify persons (or groups of persons) through the information collected, and thus especially used for counter terrorism and crime prevention.

Finally the PACT project includes another important technology, which allows identification for security purposes, which is the biometric[130] identification, a field that has changed in the last years and now allows not only finger-, palm-, and footprint identification but also the *"mapping of veins, body cells and tissues, voice, odours, human scent, dentistry, handwriting, (…) footwear impressions (size, type, defects), ballistics, speech and writing features, and psychological profiling."*[131] Furthermore automated systems have made the biometric identification faster and more efficient, resulting in a spread of application, especially within border security and crossing – the most prominent example being the biometric passport, but also the Schengen Information system, exchanging information between border control, police authorities, customs, visa and judicial authorities of European countries and aiming at the facilitate travelling of citizens but also for security reasons, like counter terrorism, crime prevention and organised crime.[132] Both the PRISMS project, as well as the SAPIENT similarly highlight the importance of biometrics for the identification of humans, especially within border security.[133;134]

Three forms of identification have to be considered: identifying an object/person against a database; identifying a substance, using chemical analysis; identifying an anomaly, by spotting an object/person in an inadequate space/context.

[127] C.f. ib., p. 21f.
[128] Finn, Rachel L. and David Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review,* Vol. 28, Issue 2, April 2012, p.188f.
[129]García, Alberto Crespo, et al., op. cit., 2012, p. 34.
[130] Biometrics can be defined as the use of specific human body physical and behavioural characteristics in order to identify a person or distinguish between persons. Biometrical identification needs the use of a database in which the biometrical data is stored in order to match the individual that needs to be identified – and thus is an integrated security system. (C.f. Ib., p. 66; Bellanova, Rocco, et al., op. cit., 2012, p. 34f.).
[131] García, Alberto Crespo, et al., op. cit., 2012, p. 66.
[132] C.f. ib., p. 68.
[133] C.f. van Schoonhoven, Bas, et al., op. cit., 2013, p.30.
[134] C.f. Bellanova, Rocco, et al., op. cit., 2012, p. 54f.

5.2.3 Verify

Closely related to the identification function of a security PSS is the verification function, defined by the oxford dictionary as to *"*[m]*ake sure or demonstrate that (something) is true, accurate, or justified"*[135], which thus also needs an identification of some kind beforehand. Related to the proposed definitions of the DIN terminology portal, this gets clear when looking at the terminology used for the guidance on assuring the quality of biological and ecological assessments in the aquatic environment, defining 'to verify' as the *"confirmation of an identification, e.g. by a qualified person or an independent expert."*[136] Other definitions provided by the DIN terminology portal show the broad field of areas within which verification functions apply and shows the similarities but also the specification of each use area. The standardisation for Automatic identification and data capture (AIDC) techniques defines 'verify' as *"comparing an activity, a process, or a product with the corresponding requirements or specifications"* or as *"the act of reviewing, inspecting, testing, checking, auditing, or otherwise establishing and documenting whether or not items, processes, services or documents conform to specified requirements."*[137] Similar definitions can also be found for the ISO 9200 Aerospace series[138] and the ISO 19901-7 Petroleum and natural gas industries.[139]

The SAPIENT project provides a good differentiation between the verification and the identification function related to persons since *"identification involves one-to-many matching,"* while *"verification* (…) *involve*[s] *the database system retrieving the features of a single person and performing a one-to-one comparison."*[140] Still similar to the identification functionality, biometrics is an important technology to enable the verification within a security area and can also mostly be found within border control and border security. This again shows the close intertwining of both functions, which can also be seen in the ECORYS 'Security Regulation, Conformity Assessment & Certification' Report, according to which border control "*consists of the verification of people, vehicle and goods at regulated land or maritime check points and involves identity checks and information searches against various databases of persons to be either apprehended or denied entry to the territory and the use of advanced techniques for identifying the risk."*[141] Here again, the intricacy of the usage of security products can be seen and one function in a specific area or of a specific security PSS is seldom on his own.

Access control systems are another security area in which the verification function is the key element and where in comparison to a broader identification system, the database that is used to compare the person with the available data is smaller, as less data is needed.[142]

Another area, in which the verification function often applies are security services as a support

---

[135] http://www.oxforddictionaries.com/definition/english/verify?q=verify (Accessed 02.06.2014).
[136] EN 14996 Water quality - Guidance on assuring the quality of biological and ecological assessments in the aquatic environment.
[137] ISO/IEC 19762-1 Information technology - Automatic identification and data capture (AIDC) techniques - Harmonized vocabulary – Part 1: General terms relating to AIDC.
[138] EN 9200 Aerospace series - Programme management - Guidelines for project management specification.
[139] DIN EN ISO 19901-7 Petroleum and natural gas industries - Specific requirements for offshore structures – Part 7: Station keeping systems for floating offshore structures and mobile offshore units (ISO 19901-7:2013)
[140] Bellanova, et al., op. cit., 2012, p. 55.
[141] ECORYS, op. cit., 2011, p. 102.
[142] C.f. Bellanova, et al., op. cit., 2012, p. 55.

for security systems. A specific example would be when a specific operator is not needed in order to control or monitor, but only to verify as soon as an automated security systems sets of an alarm.[143] This can especially be found within partially automated CCTV systems where on the one hand the partial automation can reduce the total amount of information that reaches the operator, or on the other hand specific information is highlighted for the operator[144] and where the latter serves as a verification of the automated CCTV system.

[143] C.f. Johanning, Nils, Mikołaj Sobczak, Andrzej Figaj, María José Martínez Gil, Jan Derkacz, "Evaluation of Components", D9.4 INDECT Project, 31st December 2009, p. 13.
[144] Macnish, Kevin, "Unblinking eyes: the ethics of automating surveillance", *Ethics and Information Technology*, Vol. 14, Issue 2, June 2012, p. 160f.

5.3 PERFORMATIVE FUNCTIONS

5.3.1 Authorise

For "authorisation" as a security-relevant function, Merriam-Webster has several definitions:

- to give official or legal power to someone
- to give a right to someone

This corresponds with SIEMENS' online glossary on industrial security, which defines "authorization" as the "*access right to system resources.*"[145] In general, "authorise" (or more frequently in American English, "authorize") is most frequently observable in IT security. There, it is about rights of users of a computer system, more precisely – authorisation is a tool of (access) rights management and is the act of granting specific user rights.

Generally, PSS under this function serve to grant specific right to specific persons or groups of persons, or even devices, bots, etc. It could be framed as the conferral of a certain status.

The final report of the European Security and Innovation Forum discuss several aspects of authorisation problems in a nun-structured, rather incoherent manner. To show the breadth of the field, some discussion points should be mentioned here:

- A dominant issue with regard to authorisation is trust, especially with regard to the use of online transactions and the use of credit cards by un-authorised persons[146];
- Biometric systems: there is a severe threat of unauthorised access, e.g. by a false positive identification;
- Secure construction and protection of critical infrastructures requires an enhancement of control technologies, which the report understands as identification, ID verification and **tiered access authorisation**;
- Immigration: visa management as travel authorisation. Already exists in the USA (Electronic System for Travel Authorization) – grants the right to enter the USA.

Elaborating on the "authorise"-function as identity management, the IMPRINTS[147]-project conceives of several core domains and provides samples of "authentication":

- Knowledge: making use of passwords and pincodes which a person has memorised;
- Token: making use of an object or token, such as a passport or an identity card
- Body features: this refers to biometrical markers used to manage identifies, such as facial patterns that can be recognised, or fingerprints.
- During analysis, IMRPINTS also discovered a general expectation of combined deployment of measures ("multifactor identification authentication").

---

[145] SIEMENS Industrial Security, Glossary, http://www.industry.siemens.com/topics/global/en/industrial-security/support/pages/glossary.aspx (Accessed 30.06.2014).
[146] European Security Research and Innovation Forum (ESRIF), op. cit., 2009, p. 174.
[147] Zoonen, Liesbet van; Briggs, Pam; Norval, Aletta; Wilson, Sandra; Flore, Lilia Gomez; Harvey, Jasmine; Prasopoulou, Elpida; Thomas, Lisa; Walker, Sharon, „*Scenarios of identity management*", Brochure IMPRINTS-Project (Public responses to identity management practices and technologies), 2012, http://www.imprintsfutures.org/assets/images/pdfs/Scenarios%20of%20future%20scenarios.pdf (Accessed 14 July 2014).

Sample FP7 security research project:

IDETECT 4ALL[148]: The project developed sensors that could detect intruders. Authorised personnel were given wearable signs of authorisation: tags that could be scanned and read.

In conclusion, the function „to authorise“ could be framed as serving the purpose of lending rights and status to individuals or groups. Being authorised or not determines whether access is granted or not, and whether certain information is shared or not. Any implementations of the “authorise”-functionality evolve mainly around the granting, restricting and managing of rights (to do something, to access something, etc.), entailing e.g. password management or biometrics-related pattern management.

[148] European Commission, EU Research for a Secure Society, op. cit., 2012, p. 86.

5.3.2 Control

The function 'to control' in security PSS is a very broad function and can be found in a large number of different areas and also relates to other functions, like 'identify' 'verify' and 'authorise'. The oxford dictionary provides several definitions of controlling, of which a few also apply to the security-related function of controlling: as such this can be to (1) "*supervise the running of"* especially related to services, for example in crisis management, (2) to "*limit the level, intensity, or numbers of",* but also (3) to "*regulate (a mechanical or scientific process).*"[149] The DIN terminology portal[150] provides a further insight in the meaning of control in a security context, which from a petroleum and natural gas industries perspective denotes controlling as *"limiting the extent and/or duration of a hazardous event to prevent escalation."*[151]

This is closely related to the first and also second definition found in the oxford dictionary and heavily context related to crisis management. Another definition from the DIN terminology portal is the *"verification that acceptance criteria are met*"[152] which – as the definition itself already states – links with the verification function and can especially be found within access control systems in critical infrastructures but also with other control systems.

An important security area in which the control function of security services, but also of products and systems is essential can be found in the domain of border security, especially in controlling the cross-border flow of people and goods and is thus one of the main function in the identification of objects and substances. For example one of the main tasks for security personnel at the airport is access control – the verification or prevention of an unauthorised access to the premises of the airport. Herein lies also the main distinction from the function 'to authorise', which is about the right or the permission entering somewhere, whereas the control function reviews the authorisation status.

[149] http://www.oxforddictionaries.com/definition/english/control?q=control (Accessed 02.06.2014).
[150] http://www.din-term.din.de/cmd?level=tpl-home&languageid=en (Accessed 02.06.2014).
[151] ISO 15544 Petroleum and natural gas industries - Offshore production installations - Requirements and guidelines for emergency response.
[152] ISO 22716 Cosmetics - Good Manufacturing Practices (GMP) - Guidelines on Good Manufacturing Practices.

5.3.3 Create situational awareness (SA)

Aptly captured in an online training course developed by the US coast guard, situational awareness refers to "*the ability to identify, process, and comprehend the critical elements of information about what is happening to the team with regards to the mission. More simply, it's knowing what is going on around you*." [153]

SA essentially relates to cognitive processes as well as outcomes. It centres on and implies a decision-making instance relying on information gathered from a vast array of sources. Such information, in turn, relates to aspects of the world to create a "picture" of a given situation. Conceptually, SA appears as something that can be scaled up and down considerably, concerning, e.g., an aircraft pilot relying on input he receives from the machine he is flying. But this could also relate to an entire "war room" or "crisis room" receiving, fusing and displaying a broad scope of data and information.

SA also has been defined as "*the result of a dynamic process of perceiving and comprehending events in one's environment, leading to reasonable projections as to possible ways that environment may change, and permitting predictions as to what the outcomes will be in terms of performing one's mission. In effect, it is the development of a dynamic mental model of one's environment.*"[154]

Products and systems in support of this security function and in contributing to the creating of such a "mental model of one's environment" therefore could perform several tasks: to fuse existing strands of information, to provide infrastructure that allows for displaying information, but also provide the means to communicate. SA should be seen as an interactive process of negotiating with the decision maker's environment.

The ESRIF-report situates situational awareness in several contexts:

On a temporal dimension, it complements SA with Future Awareness,[155] which implies the capability to assess future developments, as well as how a system's characteristics might possibly change, and which – future – security requirements could be derived. The proximity of this notion to the security function of "assess" is evident. Use-cases include:

- cyber-related situational awareness[156]
- space situational awareness
- Crisis Management[157]: Rescuers need to be able to understand a situation. This is used almost synonymously with situational awareness, to the creation of which new sensors are available. Technology contributes to a more accurate visualisation of a situation ("common operational picture"). SA also relies on command and control (C2)

[153] U.S. Coast Guard, Team Coordination Training Student Guide (8/98), http://www.uscg.mil/auxiliary/training/tct/chap5.pdf (Accessed 06.06.2014), emphasis in the original.
[154] Nofi, Albert A., *Defining and measuring shared situational awareness*. Center for Naval Analysis, Virginia, November 2000. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA390136 (Accessed 26.06.2014).
[155] European Security Research and Innovation Forum (ESRIF), op. cit., 2009, p. 76.
[156] Ib., p. 79.
[157] Ib., p. 22.

infrastructures which in turn build on the capability to compile an ever growing amount of information.

An example from security research:

SCIIMS[158] (Strategic Crime and Immigration Information Management System) aims to develop an information-sharing platform in the domain of transnational crime and migration issues. The key capabilities addressed by the project are searching and mining for, and fusing information from highly heterogeneous sources (such as national, transnational or private). These capabilities then allow for higher order capabilities: to discover trends and patterns. The integration of all these capabilities leads to situational awareness and improved decision-making. Searching, mining, information fusing thus are understood as "pre-cursor" capabilities to SA.

SA refers to the knowledge producing processing of process- and issue relevant[159] information and data. Optimal awareness relies on a vast field of sources. Situational Awareness is among the prerequisites for other, future-oriented capabilities such as to project, to forecast and to anticipate.

[158] European Commission, EU Research for a Secure Society, op. cit., 2012, p. 58.
[159] Relevance with regard to a specific problem space description or task description.

5.3.4 Detain

Detention is a security measure which is applied in the general framework of criminal law but also in other fields such as, for instance the main priorities of the EU internal security strategy: border management and prevention of terrorism.[160] Any PSS operating detain-functionality are deployed under very specific legal and operational compliance requirements. A high degree of knowledge about these compliance requirements is therefore required both for manufacturers and service providers.

Illegal migration

Tackling illegal immigration plays an important role in maintaining security in the EU.[161] According to article 8.3(e) of Directive 2013/33/EU laying down standards for the reception of applicants for international protection,[162] Member States may hold an applicant in detention when, amongst other, "protection of national security or public order so requires". Applicants may be detained if other less coercive alternative measures cannot be applied effectively and when it proves necessary and on the basis of an individual assessment of each case. In this circumstance, the applicant can be detained only for as short a period as possible.[163] Detention can also apply to minors, which can be detained as a measure of last resort and for the shortest appropriate period of time.[164]

Not only EU rules establish the possibility for Member States to detain applicants for international protection when national security requires it. Immigration laws on "return procedures" in some European Countries also contain references to national security considerations. In 2010, the European Union Agency for Fundamental Rights issued an extensive report on "Detention of third-country nationals in return procedures."[165] The report provided an overview of the legal grounds for this type of detention in different Member States. The document reads

> *"In the Czech Republic, aliens in return or removal proceedings can be detained if there is a risk that the person might endanger the security of the state or might materially disrupt public order. This includes, for example, situations in which the foreigner might endanger state security by using violence for political aims or situations in which the foreigner endangers public health, due to his/her suffering from a serious disease. In Finland, an alien may be detained to prevent his/her entry or facilitate removal, if taking*

[160] European Commission, The EU Internal Security Strategy in Action, op. cit., 2012 p.2.
[161] European Council, Internal security strategy for the European Union, Towards a European security model, Publication Offices of the European Union, Luxembourg, March 2010, p. 28. http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ENC.pdf (Accessed 30.06.2014).
[162] European Parliament and the Council, Directive 2013/33/EU of 26 June 2013 laying down standards for the reception of applicants for international protection (recast), OJ L 180/96, 29.06.2013.
[163] Article 9.1 of Directive 2013/33/EU
[164] Article 11.2 of Directive 2013/33/EU. A similar article (art. 17) is also included in Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, OJ L 348, 24.12.2008.
[165] European Union Agency for Fundamental Rights, *Detention of third-country nationals in return procedures*, Publication Offices of the European Union, Luxembourg, 2010. http://fra.europa.eu/sites/default/files/fra_uploads/1306-FRA-report-detention-december-2010_EN.pdf (Accessed 30.06.2014).

account of the alien's personal and other circumstances, there are reasonable grounds to believe that he or she will commit an offence in Finland. In Greece, the provision on administrative expulsion allows detention of an alien considered dangerous for the public order. In Germany, detention can be applied in case of well-founded suspicion of terrorism, although only if the deprivation of liberty is necessary to ensure his/her removal. In Hungary, detention to secure expulsion is admissible in case the third-country national has seriously or repeatedly violated the code of conduct of the place of compulsory confinement."[166]

Detention of terror suspects

Detention measures can apply to terror suspects, even without charge. This has been the case in the UK, for instance, where, in the immediate aftermath of the events in the US of 11 September 2001, the British Government introduced the Anti-Terrorism Crime and Security Act which allowed for a foreign national suspected of involvement in terrorism to be indefinitely imprisoned without charge or trial. In December 2004, the House of Lords held that the indefinite detention of foreign nationals without charge was in breach of the right to liberty and security under article 5(1) of the European Convention.[167]

Anti-terror rules in the UK, still allow the police to detain individuals without charge or prior authorization. This can happen under schedule 7 of the Terrorism Act 2000 which only applies at airports, ports and border areas and allows officers to stop, search, question and detain individuals. A famous case of detention under provisions of schedule 7 is the formal arrest at Heathrow airport in August 2013 of David Michael Miranda. Miranda was the partner of the Guardian journalist Glenn Greenwald who had previously written a series of stories on Edward Snowden, revealing mass surveillance programs by the US National Security Agency. Miranda was held for nine hours, the maximum the law allows before officers must release or formally arrest the individual.[168]

[166] Ib., p. 19.
[167] House of Lords, Opinions of the Lords of Appeal for Judgment in the Cause A (FC) and others (FC) (Appellants) v. Secretary of State for the Home Department (Respondent) X (FC) and another (FC) (Appellants) v. Secretary of State for the Home Department (Respondent), 16 December 2004. http://www.publications.parliament.uk/pa/ld200405/ldjudgmt/jd041216/a&others.pdf (Accessed 30.06.2014).
[168] Guardian staff, "Glenn Greenwald's partner detained at Heathrow airport for nine hours", *The Guardian*, online edition, 19 August 2013. http://www.theguardian.com/world/2013/aug/18/glenn-greenwald-guardian-partner-detained-heathrow (Accessed 30.06.2014).

5.3.5 Prevent/Protect

Traditionally EU Member States have had the prime responsibility for crime prevention matters. With the entry into force of the Lisbon Treaty, the EU now has the possibility to establish measures to promote and support EU States' actions in this field.[169] The European Commission DG Home affairs defines crime prevention as "*all the activities that contribute to halting or reducing crime as a social phenomenon. These activities are undertaken by all the actors that are likely to play a preventive role: local politicians, law enforcement agencies and the judicial system, social services, the education system, civil society organisations, industry, banks, the private sector, research workers and scientists and the general public, supported by the media*."[170]

Prevention means many different things to many different people[171] and is highly dependent on the context and the goal. Concerning the EU's internal security strategy crime prevention is a priority in the following domains: the prevention of serious and organized crime, the prevention of terrorism and radicalization and the prevention of cybercrime[172].

More specifically concerning serious and organized crime measures include disrupting criminal networks and combating the financial incentives that drives them. Measures include: installing legislation and implementation of the collection of passenger name records, revising the EU anti-money laundering legislation, setting up joint investigation teams, ensuring effective implementation of the European Arrest warrant, more effective enforcement of intellectual property rights and proposing legislation to strengthen EU legal framework on confiscation.[173]

Concerning terrorism prevention the main measures include empowering communities to prevent radicalization and recruitment, cutting off terrorist's access to funding and materials and follow their transactions, development of a further regime for maritime and aviation security, which takes into account progress in research techniques and technology, promote a more active approach to land transport security and in particular the security of passenger transport.[174] For instance recently smart video surveillance cameras with behavioural detection software are being deployed in train stations and airports. At Clapham Junction Train Station in London a smart CCTV system has been installed, which is designed to spot intruders and unusual behaviour. Similar systems are being considered by Transport for London. Also in Rome smart CCTV systems have been installed in mass transit systems, here the technology is designed to react to unusual behaviour, such as somebody leaving a bag unattended or an individual moving against the general crowd flow.[175] Those examples show that the usage of

---

[169] See art 84(1) The Lisbon Treaty: "The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may establish measures to promote and support the action of Member States in the field of crime prevention, excluding any harmonisation of the laws and regulations of the Member States."
[170] EU Commission, DG Home Affairs, Crime Prevention, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/crime-prevention/index_en.htm. (Accessed 30.06.2014).
[171] Welsh, B.C. & D.P. Farrington, *The future of crime prevention: Developmental and situational strategies*, Report prepared for the National Institute of Justice, 2010
[172] European Commission, The EU Internal Security Strategy in Action, op. cit., 2010, p.2.
[173] Ib., p. 5-6.
[174] Ib., p. 7-9.
[175] Millward, D. Train station to get terrorist-tracking CCTV, *The Telegraph*, 27 June 2007, http://www.telegraph.co.uk/news/uknews/1555772/Train-station-to-get-terrorist-tracking-CCTV.html. (Accessed

(smart) CCTV often is linked with a crime preventive intention and aimed at the security protection of citizens.

Concerning prevention of cybercrime the following measures have been proposed: establishment of a cybercrime centre and setting up national/governmental Computer, Emergency Response Teams (CERTs), increased working with industry to empower and protect citizens, creating alert platforms, in cooperation with internet services providers, law enforcement authorities, and non-profit organisations develop guidelines on coordination based on authorized notice and take-down procedures.[176]

30.06.2014).

[176] European Commission, The EU Internal Security Strategy in Action, op. cit., 2010, p. 9-10.

Key: Primitive Functions Connective Functions Performative Functions

Application area / Function	Security of the citizens	Critical infrastructure	Border security	Crisis management
Information collection storage and management to produce intelligence				
Locate				
Track				
Assess				
Identify				
Verify				
Authorise				
Control				
Create situational awareness				
Detain				
Prevent/Protect				

Figure 2: Matrix of the functions of security PSS within the different application areas.

6 CONCLUSION

The glossary presented here takes context of application or use cases as a starting point. This approach is based on the idea that any definition of a product, system or service in the field of security technology always entails a discretionary element. Each technological system is comprised of several interconnected elements and each of these elements can itself be analysed as a system of its own. A torch is comprised of a battery, an optical system, a small light bulb and a couple of other elements. Each of these elements can be seen as a system in itself (a battery e.g. is a physical-chemical system to produce energy). Different elements or components, each with systems quality for themselves are assembled into the larger unit of the torch. This unit (or assemblage) can be used to produce light. Starting at this end and looking at functions it is easier to identify products, systems and services. A function-based view also allows for the emergence of higher-level functions, comprised of different interconnected products. Distinguishing primitive, connective and performative functions we account for this composite character of security technology. Finally this approach also allows for a comparative perspective: defining a function first and then investigating the applicability of different products, systems and services the suitability of each product can be assessed against the requirements of the problem to be solved. Hence the use of drones to surveille a maritime area in order to detect vessels with illegal immigrants will score low when the function is to save lives of immigrants (compared to a more comprehensive policy strategy). Depending on how narrow or complex security functions are defined, products, systems and services will be assessed differently.

The approach chosen here allows for sufficient flexibility to evaluate security products, systems and services by defining security areas and functions and then analyse how the PSS under investigation perform. We think such an open conceptual architecture is better suited to the task of this project than a strategy that sticks to the narrowly defined technological standards of performance.

7 REFERENCES

Auffermann, Burkhard and Juha Kaskinen, "Introduction", Security in Futures – Security in Change, Writers & Finland Futures Research Centre, Turku, 2011.

Aven, Terje. "A unified framework for risk and vulnerability analysis covering both safety and security." Reliability Engineering and System Safety, 92, 2007, 745-754.

Bonsor, Kevin, "How Location Tracking Works", HowStuffWorks.com. http://electronics.howstuffworks.com/everyday-tech/location-tracking.htm.

Bellanova, Rocco, Matthias Vermeulen, Serge Gutwirth, Rachel Finn, Paul McCarthy, David Wright, Kush Wadhwa, Dara Hallinan, Michael Friedewald, Marc Langheinrich, Vlad Coroama, Julien Jeandesboz, Didier Bigo, Mervyn Frost, Silvia Venier, "Smart Surveillance – State of the Art", D.1.1 SAPIENT project, 23rd January 2012.

Bigo, Didier, "The Möbius Ribbon of Internal and External Security(ies)", in Mathias Albert; Yosef Lapid; David Jacobson (eds.), *Identities, Borders, Orders*, University of Minnesota Press, 2001. p. 91 - 116.

Bigo, Didier, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi, Amandine Scherrer, National Programmes for Mass Surveillance of Personal Data in EU Member States and their Compatibility with EU Law, Brussels, October 2013. http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET%282013%29493032_EN.pdf.

Burgess, Peter J. (ed.), The Routledge Handbook of New Security Studies, Routledge, London, 2010.

Burns, Alan, John McDermid, and J. Dobson. "On the meaning of safety and security." The Computer Journal 35.1, 1992, 3-15.

Carl Zeiss Optronics GmbH, "AMASS: Autonomous maritime surveillance system". http://www.amass-project.eu/amassproject/content/index (Accessed 27.05.2014).

Clarke, Roger, "Profiling: A Hidden Challenge to the Regulation of Data Surveillance", Journal of Law and Information Science, Vol. 4, No. 2, 1993, pp. 403-419.

CRISP, Evaluation and certification schemes for security products – Capability Project, Description of Work.

DIN EN 12251: Health informatics - Secure User Identification for Health Care - Management and Security of Authentication by Passwords; English version EN 12251:2004.

DIN EN ISO 19901-7 Petroleum and natural gas industries - Specific requirements for offshore structures – Part 7: Station keeping systems for floating offshore structures and mobile offshore units

DIN EN ISO 24534-4: Automatic vehicle and equipment identification - Electronic Registration Identification (ERI) for vehicles - Part 4: Secure communications using asymmetrical techniques (ISO 24534-4:2010); English version EN ISO 24534-4:2010.

ECORYS, Security Regulation, Conformity Assessment & Certification. Final Report – Volume I: Main Report, ECORYS Nederland BV, Rotterdam, The Netherlands, 2011.

ECORYS, Study on the Competitiveness of the EU security industry, Within the Framework Contract for Sectorial Competitiveness Studies – ENTR/06/054, ECORYS Nederland BV, Rotterdam, The Netherlands, 2009.

EN 9200 Aerospace series - Programme management - Guidelines for project management specification.

EN 12687 Biotechnology - Modified organisms for application in the environment - Guidance for the characterization of the genetically modified organism by analysis of the genomic modification.

EN 14943:2005-12: Transport services - Logistics - Glossary of terms.

EN 14996 Water quality - Guidance on assuring the quality of biological and ecological assessments in the aquatic environment.

eu-LISA, Annual report on the 2013 activities of the Central Unit of Eurodac pursuant to Article 24(1) of Regulation (EC) No 2725/2000, http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010898%202014%20INIT.

European Commission, Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection, Making European Critical Infrastructures more secure, SWD(2013) 318 final, Brussels, 28.8.2013.

European Commission, Commission Staff Working Paper, Security industrial policy, SWD(2012) 233 final, Brussels, 26.7.2012.

European Commission, Delivering an area of freedom, security and justice for Europe's citizens, Action Plan Implementing the Stockholm Programme, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 171 final, Brussels, 20.4.2010.

European Commission, EU Research for a Secure Society, Security Research Projects under the 7th Framework Programme for Research, Brussels, July 2012.

European Commission, Investing into security research to for the benefits of European citizens. Security research projects under the 7th framework programme for research, Brussels, September 2010.

European Commission, Programming Mandate addressed to CEN, CENELEC, and ETSI to establish security standards, M/487, Brussels 17.02.2011.

European Commission, Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, 2011/0023 (COD), Brussels, 2.2.2011.

European Commission, Security Industrial Policy, Action Plan for an innovative and competitive Security Industry, Communication from the Commission to the European Parliament, the Council, and the European Economic and Social Committee COM(2012) 417

final, Brussels, 26.7.2012.

European Commission, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, Communication from the Commission to the European Parliament, and the Council, COM (2010) 673 final, Brussels, 22.11.2010.

European Commission, "The EU single market, banking, crisis management" http://ec.europa.eu/internal_market/bank/crisis_management/index_en.htm.

European Council Decision 2009/902/JHA of 30 November 2009 setting up a European Crime Prevention Network (EUCPN) and repealing Decision 2001/427/JHA, OJ L 321, 8.12.2009.

European Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008.

European Council, Internal security strategy for the European Union, Towards a European security model, Publication Offices of the European Union, Luxembourg, March 2010.

European Parliament and the Council, Directive 2008/114/EC on the identification and designation of European critical infrastructures. OJ L 345/75, 23.12.2008.

European Parliament and the Council, Directive 2008/115/EC of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, OJ L 348, 24.12.2008.

European Parliament and the Council, Directive 2013/33/EU of 26 June 2013 laying down standards for the reception of applicants for international protection (recast), OJ L 180/96, 29.06.2013.

European Parliament and the Council, Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013, establishing the European Border Surveillance System (Eurosur) L 295/11, 6.11.2013.

European Security Research Advisory Board, Meeting the challenge: the European Security Research Agenda, Luxembourg Office for Official Publications of the European Communities, 2006.

European Security Research and Innovation Forum (ESRIF), ESRIF Final report, December 2009. http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf.

European Union Agency for Fundamental Rights, Detention of third-country nationals in return procedures, Publication Offices of the European Union, Luxembourg, 2010. http://fra.europa.eu/sites/default/files/fra_uploads/1306-FRA-report-detention-december-2010_EN.pdf.

Frontex, Best Practice Technical Guidelines for Automated Border Control (ABC) Systems, Research and Development Unit, Last reviewed on 31/08/2012, page 21. http://frontex.europa.eu/assets/Publications/Research/Best_Practice_Technical_Guidelines_for_Automated_Border_Control_Systems.pdf.

Finn, Rachel L. and David Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", Computer Law & Security Review, Vol. 28, Issue 2, April 2012.

García, Alberto Crespo, Nuria Ituarte Aranda, Panagiotis Tsakonas, Vasilis Tsoulkas, Dimitris Kostopoulos, Avi Domb, Jay Levinson, Dimitris M. Kyriazanos, Olga Segou, Lori Malatesta, Christos Liatas, Nikos Argyreas, Stelios C. A. Thomopoulos, "Report on Technology Taxonomy and Mapping", D.1.3 PACT project, June 5th 2012.

Gill, Martin, Angela Spriggs, "Assessing the impact of CCTV", Home Office Research Study 292, February 2005.

Guardian staff, "Glenn Greenwald's partner detained at Heathrow airport for nine hours", The Guardian, online edition, 19 August 2013. http://www.theguardian.com/world/2013/aug/18/glenn-greenwald-guardian-partner-detained-heathrow.

House of Lords, Opinions of the Lords of Appeal for Judgment in the Cause A (FC) and others (FC) (Appellants) v. Secretary of State for the Home Department (Respondent) X (FC) and another (FC) (Appellants) v. Secretary of State for the Home Department (Respondent), 16 December 2004. http://www.publications.parliament.uk/pa/ld200405/ldjudgmt/jd041216/a&others.pdf.

ISO 15544 Petroleum and natural gas industries - Offshore production installations - Requirements and guidelines for emergency response.

ISO 22716 Cosmetics - Good Manufacturing Practices (GMP) - Guidelines on Good Manufacturing Practices.

ISO/IEC 19762-1 Information technology - Automatic identification and data capture (AIDC) techniques - Harmonized vocabulary – Part 1: General terms relating to AIDC.

Johanning, Nils, MikołajSobczak, Andrzej Figaj, María José Martínez Gil, Jan Derkacz, "Evaluation of Components", D9.4 INDECT Project, 31st December 2009.

Kovacich, Gerald L. and Edward P. Halibozek, "Physical Security" in Fennely, Lawrence J., Effective Physical Security, Elsevier Inc., Waltham, Oxford, 2013, pp. 339 – 353.

Macnish, Kevin, "Unblinking eyes: the ethics of automating surveillance", *Ethics and Information Technology*, Vol. 14, Issue 2, June 2012.

Martínez, Cristina, Olaf Poenicke, James Brennan, John Dering, Mahary Ramasindraibe, "Technology Tree", D2.3, SecureCHAINS project, 15th May 2012.

Millward, David, Train station to get terrorist-tracking CCTV, *The Telegraph*, 27 June 2007.

Nofi, Albert A., Defining and measuring shared situational awareness. *Center for Naval Analysis*, Virginia, November 2000.

Pawson, Ray and Nick Tilley, Realistic Evaluation, Sage Publications Ltd., London, Thousand Oaks, New Deli, 1997.

Sempere, Martí. "The European Security Industry: A Research Agenda". Economics of Security Working Paper 29, 2010, Berlin: Economics of Security.

Sieber, Alois J., Needs for Standards in Security, 2006, http://www.euritrack.org/Anglais/A.%20Sieber,%20J.%20Loeschner.pdf.

SIEMENS Industrial Security, Glossary, http://www.industry.siemens.com/topics/global/en/industrial-security/support/pages/glossary.aspx.

Sinay, Juraj, "Security Research and Safety Aspects in Slovakia." In: Thoma, Klaus (ed.), *European Perspectives on Security Research*, Springer Berlin Heidelberg 2011, pp. 81-90.

Sobański, Grzegorz, Paweł Lubarski, Mikołaj Sobczak, "Preliminary report on proposed logical structure of the systems", D.2.1 INDECT project, 31st December 2009.

The Hague Centre for Strategic Studies, Conceptual foundations of security, D1.1, ETTIS Project, 30 June 2012.

United Nation International Labour Organisation Socio-Economic Security Programme, Definitions: What we mean when we say "economic security", http://www.ilo.org/public/english/protection/ses/download/docs/definition.pdf.

U.S. Coast Guard, Team Coordination Training Student Guide (8/98), http://www.uscg.mil/auxiliary/training/tct/chap5.pdf.

U.S. Department of Homeland Security, Crosswalk of Target Capabilities to Core Capabilities http://www.fema.gov/media-library-data/20130726-1854-25045-1651/crosswalk_1_.pdf.

U.S. Department of Homeland Security, Target Capabilities List, A companion to the National Preparedness Guidelines, September 2007, http://www.fema.gov/pdf/government/training/tcl.pdf.

van Buuren, Jelle, Secret Truth. The EU Joint Situation Centre, Eurowatch, Amsterdam, 2009.

van Schoonhoven, Bas, Marc van Lieshout, Arnold Rosendaal, "Preliminary report on current developments and trends regarding technologies for security and privacy", D.2.1 PRISMS project, 28th February 2013.

Welsh, Brendon C., David P. Farrington, *The future of crime prevention: Developmental and situational strategies*, Report prepared for the National Institute of Justice, 2010.

Williams, Michael C., "The new economy of security", Global Crime, Vol. 13, No.4, August 2012, pp.312-319.

Zoonen, Liesbet van; Briggs, Pam; Norval, Aletta; Wilson, Sandra; Flore, Lilia Gomez; Harvey, Jasmine; Prasopoulou, Elpida; Thomas, Lisa; Walker, Sharon, „*Scenarios of identity management*", Brochure IMPRINTS-Project (Public responses to identity management practices and technologies), 2012, http://www.imprintsfutures.org/assets/images/pdfs/Scenarios%20of%20future%20scenarios.pdf (Accessed 14 July 2014).

8 ANNEX

Although the main focus of the glossary have been the definitions of specific security functions, products, systems and services should perform, it seems useful to provide here also a chance to create not only a function-based glossary but also a glossary of terms used within the CRISP project. This approach is commonly chosen when developing standards, in which most of the time one of the first documents issued is a vocabulary of important terms which are included in the standards series. Since we will also in CRISP have a large amount of terms which will be used regularly we will also adapt this approach for the CRISP project. Even though it is difficult to include already all the important terms at the beginning of the project, similar to the glossary of security functions, we will update the CRISP glossary in the course of the project – and will result with a final glossary at the end of the project, which can be useful as a starting point for further standardisation and certification work on the basis of the concluded work.

The glossary here also consists of two parts – the first part being the common terms used throughout the project; the second part being a glossary of terms used for the STEFi criteria. These terms are mainly developed and researched during the work package 4 and the deliverable 4.3, but will also be included here into an extra part of the glossary. These terms might also be refined during the course of the CRISP project (mainly in WP6 and WP7 – where the roadmap of the CRISP certification and the CEN Workshop Agreement are developed) and thus also be included in a final version of the glossary at the end of the project.

8.1 CRISP-RELATED TERMS AND DEFINITIONS FOR THE GLOSSARY

Assessment: (see also conformity assessment) The term assessment is used in many contexts, with the general meaning of 'assessment' seldom changes drastically and is thus understood as "the act of judging or deciding the amount, value, quality, or importance of something, or the judgment or decision that is made."[177]

The specific CRISP methodological context of assessment links to this definition. Within CRISP, assessment is especially an important factor for the evaluation part of the CRISP methodology[178], where the STEFi approach is used as an assessment tool, thus a tool for the judging of the quality of security PSS.

Accreditation: In the European Regulation 765/2008 for requirements for accreditation, accreditation is defined as "an attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity."[179]

Alarm systems: Alarm systems include a broad range of different products and systems – they have however some importance for the CRISP project as the scope of the CRISP certification scheme will be at first limited to Alarm systems. The International Electrotechnical Commission Technical Committee 79 on Alarm and electronic security systems provides a clear distinction of what to include into the scope of alarm systems: "The scope includes, but is not limited to equipment and systems, either used by ordinary persons or by trained people in the following residential and non residential applications: Access control systems, alarm transmission systems, video surveillance systems, combined and/or integrated systems even including fire alarm systems, fire detection and fire alarm systems, intruder and hold-up alarm systems, remote receiving and/or surveillance centres, social alarm systems."[180]

Application areas: Application areas are in the CRISP project a way of categorisation for the context in which security PSS are deployed and thus in which security functions perform. Within CRISP we distinguish between four application areas: security of the citizens, critical infrastructures, border security, crisis management.

Attestation: Attestation is "the issue of a statement, based on a decision following review, that fulfilment of specified requirements has been demonstrated."[181]

---

[177] Cambridge dictionaries.
[178] Cf. Hempel, Leon, Nathalie Hirschman, Roger von Laufenberg, Simone Wurster, Thordis Sveinsdottir, Irene Kamara, Paul De Hert (2015): Validated CRISP Methodology. D5.1 CRISP project.
[179] European Parliament and the Council, Regulation EC No 765/2008 of 9.07.2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, OJ L 218/30, 13.08.2008.
[180] International Electrotechnical Commission, TC79 Alarm and electronic security systems, 2016, http://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID,FSP_LANG_ID:1269,25
[181] ISO/IEC 17000:2004 Conformity assessment - Vocabulary and general principles.

Attributes (see also STEFi approach): Attributes are qualities that break down the STEFi evaluation criteria and thus form an important aspect within the STEFi methodology.[182]

Audit: An audit is a "systematic, independent, documented process for obtaining records, statements of fact or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled."[183]

Border security: includes the means for providing security of land, air and sea, but also of borders in embassies in order to prevent the illegitimate crossing of people. Further focus in border security aims also at the detection of illegal products, goods and substances within custom services. Especially after the 9/11 attack, this security application area has seen an important increase of measures, mostly related to persons.[184]

CCTV system: A closed-circuit television (CCTV) system is a "surveillance system comprised of cameras, recorders, interconnections and displays that are used to monitor activities in a store, a company or more generally a specific infrastructure and/or a public place."[185]

CEN Workshop Agreement (CWA): "A CEN Workshop Agreement (CWA) is a document published by CEN in at least one of the CEN three official languages. It is an agreement developed and approved in a CEN Workshop; the latter is open to the direct participation of anyone with an interest in the development of the agreement. There is no geographical limit on participation; hence, participants may be from outside Europe. The development of a CWA is fast and flexible, on average between 10-12 months."[186] Within WP7 of CRISP, the development of a CWA will be aimed it, which will be the most relevant output of the project as it will be the foundation of further standardisation activities after the CRISP project, as e.g. developing a European standard within the next years.

Certification (as part of the CRISP methodology): (See also certification scheme) Certification is one of the subject fields of conformity assessment and is defined as a "third-party attestation related to product, processes, systems or persons", where "a service is covered by the definition of a product".[187] Within CRISP, certification is the second part of the CRISP methodology,[188] consisting of an audit followed by an attestation.

[182] C.f. Kamara Irene, De Hert Paul, Van Brakel Rosamunde, Tanas Alessia, Konstantinou Ioulia, Pauner Cristina, Viguri Jorge, Rallo Artemi, García Mahamut Rosario, Wurster Simone, Pohlmann Tim, Hirschman Nathalie, Hempel Leon, Kreissl Reinhard, Fritz Florian, von Laufenberg Roger (2015): S-T-E-F-I based SWOT analysis of existing schemes. D4.3 CRISP project.
[183] ISO/IEC 17000:2004 Conformity assessment - Vocabulary and general principles.
[184] c.f. ECORYS, Security Regulation, Conformity Assessment & Certification. Final Report – Volume I: Main Report, ECORYS Nederland BV, Rotterdam, The Netherlands, 2011, p. 35.
[185] ISO 22300:2012 Societal Security - Terminology.
[186] www.cen.eu
[187] ISO/IEC 17000:2004 Conformity assessment - Vocabulary and general principles.
[188] Cf. Hempel, Leon, et al., op. cit., 2015.

Certification requirement: Certification requirement are to be met by the client, the product, system or service and need to be assessed by the certification body in order to be able to issue a certification. Within the CRISP methodology, there will be general certification requirements based on existing standards, as well as CRISP-specific requirements.

Certification scheme: The certification scheme is a "certification system related to specified products, to which the same specified requirements, specific rules and procedures apply."[189] It consists of "specified requirements for objects of conformity assessment, such as product/service, system or person, and their characteristics from the requirements related to conformity assessment activities, such as certification except sampling and testing methods related to the specified characteristics."[190]

Certification scheme owner: The certification scheme owner is a "person or organization responsible for developing and maintaining a specific certification scheme."[191] Scheme owners are either certification bodies which develop a certification for the sole use of their clients; or organisations such as a regulatory body or a trade association not being a certification body, which develop a certification scheme in which one or more certification bodies participate.

Certification system: A certification system consists of "rules, procedures and management for carrying out certification"[192]

Client: A client in the context of certification is the party having a product, systems or service certified and thus contracting a certification body for the purpose of issuing a certificate.

Code of conduct/practice: Codes of conduct/practice compared with certification schemes, also contain provisions and requirements although without being their primary focus; generally codes of conduct/practice require several organisational and technical measures to be implemented, but these requirements are quite often limited to a minimum acceptable level. In the field of security, codes of conduct often relate to security services (such as the International Code of Conduct for Private Security Service Providers ICoC).

Configuration: Configuration is again used specifically in the CRISP methodology as part of the evaluation phase. Configuration here means the set-up of a specific scenario by the 'project leader' of a security PSS who has all relevant information about a given security PSS. The configuration phase includes the specification of the security application area, the functions of the security PSS, the specification of the Technology Readiness Level (TRL), basic information of application scenarios, indication of technology specifications and an introduction of a first set of stakeholders.[193]

[189] ISO/IEC 17000:2004 Conformity assessment - Vocabulary and general principles.
[190] Cf. Hempel, Leon, et al., op. cit., 2015.
[191] ISO/IEC 17000:2004 Conformity assessment - Vocabulary and general principles.
[192] Ibid.
[193] Cf. Hempel, Leon, et al., op. cit., 2015.

Conformity: Conformity is the "fulfilment of a requirement."[194]

Conformity assessment: Conformity assessment refers to the acknowledgement that a product, a system, a person or a board fulfils a set of fixed requirements.[195] There are various conformity assessment bodies, such as test laboratories, calibration units, and inspection units in addition to certification and verification bodies. All confirm that the needed requirements are achieved. Those requirements are usually set through standards, laws, specifications and voluntary agreements among parties. On this basis, obtaining a certificate is proof that a product complies to (or "conforms with") specific legislation or other technical specifications or criteria.[196]

Conflict: In terms of CRISP, conflict can be defined as "a situation in which there are opposing demands or ideas and a choice has to be made between them."[197] Conflicts might arise in the evaluation phase of the CRISP methodology, in which interrelations between STEFi criteria might result in conflicts, based on a predefined set of conflict rules.[198]

Consumer: Consumer is "any natural person who is acting for purposes which are outside his or her trade, business or profession."[199]

Crisis management (also emergency preparedness centres): includes mainly the restoration of security in the aftermath of a crisis, which may result from a natural disaster, but also from deliberate attacks. Furthermore a focus within the European Union policy lies on the prevention and preparedness of crisis and disaster.[200] This application area is not to be confused with the crisis management in terms of bank recovery, which is currently being discussed on a European level as well.[201]

CRISP Stakeholder: Key stakeholders identified within CRISP can be divided into two categories: Primary stakeholders (directly involved in security certification, such as security product manufacturers, suppliers and systems integrators, conformity assessment and certification bodies, standardisation organisations, accreditation bodies, data protection authorities and other regulators, end users) and secondary stakeholders (affected by and indirectly involved in security certification, such as watchdogs and civil society organisations, individuals, academics).[202]

---

[194] ISO 22300:2012 Societal Security - Terminology.
[195] ISO/IEC 17000:2004 Conformity assessment - Vocabulary and general principles.
[196] Ensthaler, Jürgen, Kai Strübbe and Leonie Bock, Zertifizierung und Akkreditierung technischer Produkte, Ein Handlungsleitfaden für Unternehmen, Berlin, 2007.
[197] Cambridge dictionaries.
[198] Cf. Hempel, Leon, et al., op. cit., 2015.
[199] European Parliament and the Council, Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000.
[200] European Commission, Delivering an area of freedom, security and justice for Europe's citizens, Action Plan Implementing the Stockholm Programme, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 171 final, Brussels, 20.4.2010, p. 6.
[201] European Commission, "The EU single market, banking, crisis management" http://ec.europa.eu/internal_market/bank/crisis_management/index_en.htm (Accessed 04.06.2014).
[202] Sveinsdottir, Thordis, Rachel Finn, Kush Wadhwa, Rowena Rodrigues, Jolien van Zetten, Simone Wurster,

Critical infrastructures: includes the security of energy, transportation and telecommunication, supply chains, financing, health infrastructure, and also control systems – general infrastructures which are of high importance of the functioning of a vital society and thus a protection against threats aiming at the disruption or destruction of the like plays an important role in the European policy making and the security industry.[203]

Customer: Customer as used in CRISP is in the context of Quality Function Deployment (QDF) and means "external customer" in terms of buyer, as well as everyone involved in the implementation process ("internal customer").[204] Thus a "customer is anyone who receives products or services (outputs) from a supplier. Customers can be either people or organizations and can be either external or internal to the supplier organization. Examples of customers include clients, consumers, users, guests, patients, purchasers, and beneficiaries."[205]

End-users: In the scope of the CIRSP project, end-users are seen as procurers, strategic planners and operators working with security products, systems and services, such as the local authorities, emergency organisations, transport operators, law enforcement authorities, retail organisations, health organisations and educational organisations. The respondents of the end-user (WP3) survey were civil society organisations, consumer rights organisations, procurers of security products, systems and services in the public and the private sector, operators of security products and systems.[206]

Evaluation: Evaluation is the first of the two phases within the CRISP methodology and consists of a configuration and an assessment stage.[207]

Evaluation criteria questionnaire: The evaluation criteria questionnaire is the main tool within the assessment stage of the evaluation phase of the CRISP methodology. The evaluation criteria questionnaire aims towards acquiring information on a specific use case of a security PSS and helps to identify interrelations and uncover potential conflicts within or between STEFi criteria – and hence between different stakeholders and social groups. The evaluation criteria questionnaire is derived from the four level structure introduced as STEFi approach on the highest aggregation level, and thus consist of the four dimensions – security; trust; efficiency; and freedom infringement.[208]

Patrick Murphy, Nathalie Hirschmann, Artemi Rallo, Rosario García, Cristina Pauner, Jorge Viguri, Eva Kalan, Igor Kolar (2015): Stakeholder Analysis Report. D3.1 CRISP project.

[203] In the EU Frameworks, there are although some priorities of specific subareas, such as aviation and maritime security compared to ICT security. (c.f. ECORYS, Security Regulation, Conformity Assessment & Certification. Final Report – Volume I: Main Report, ECORYS Nederland BV, Rotterdam, The Netherlands, 2011, p. 33f.

[204] Hempel, Leon, Nathalie Hirschmann, Tatsiana Haponava, Roger von Laufenberg, Simone Wurster, Kush Wadhwa, Thorids Sveinsdottir, Paul de Hert, Irene Kamara, Cristina Pauner, Jorge Viguri, Rosario García, Jelena Burnik (2016): Report on the scenario-based workshops and the refinement of the CRISP Methodology. D5.2 CRISP project.

[205] http://www.praxiom.com/iso-definition.htm

[206] Sveinsdottir, Thordis, et al., op. cit., 2015.

[207] Cf. Hempel, Leon, et al., op. cit., 2015.

[208] Cf. Ibid.

Evaluation scheme: An evaluation scheme in the CRISP context is a scheme that includes an evaluation of one or more aspects of a security product/system/service against specific requirements, without leading to conformity assessment certification.

Functions: Functions (in the context of CRISP) describe the intended results of the security PSS as soon as they are in operation and are thus the use case of security related PSS. Within CRISP initially 12 security functions have been identified which have been categorized into 3 groups, each group defining the complexity of the functions on the operational level, in an increasing order. While the primitive functions aim at fulfilling basic security tasks, connective functions tend to be more complex and rely already on the primitive functions. Performative functions have an even more complex structure, often relying on primitive as well as connective functions and are also more action orientated.

Freedom Infringement: The freedom infringement dimension of security product evaluation depicts the impact of a product on the freedoms and rights of persons. One of the main impacts of security products and services is enhanced personal data collection, processing, sharing and retention. This effects the rights to privacy and data protection. Additionally, security and safety products have a tendency to affect other rights such as the right to self-determination, right to freedom of movement, right of association; these must all be taken into account in the evaluation of security products.[209]

Information provider: The information provider is one of the three actors within the evaluation phase of the CRISP methodology. The information provider has the task to mainly consult the project leader and is familiar with the security PSS in case configuration questions cannot be answered. In the assessment stage, the information provider can be consulted by the project participants in case evaluation criteria questions cannot be answered.[210]

Mark: A mark – or certification mark – indicates on a product, system or services, that it has been certified according to existing standards or manufactured according to specific, high standards. . The most prominent mark in the European context is the CE-marking.[211]

Non-Conformity: Non-conformity, as opposed to conformity is the "non-fulfilment of a requirement."[212]

[209] Cf. Kamara, Irene, Paul de Hert, Alessia Tanas, Ioulia Konstantinou, Rosamunde van Brakel, Cristina Pauner, Jorge Viguri, Artemi Rallo, Rosario García, Florian Fritz, Roger von Laufenberg, Eva Kalan, Jelena Burnik (2015): Legal analysis of existing schemes. D.4.1 CRISP project.
[210] Cf. Hempel, Leon, et al., op. cit., 2015.
[211] http://ec.europa.eu/growth/single-market/ce-marking/index_en.htm
[212] ISO 22300:2012 Societal Security - Terminology.

Privacy: Roger Clarke defines privacy as "the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations"[213] and identifies five dimensions of privacy: privacy of the person; privacy of personal behaviour; privacy of personal communications; privacy of personal data; privacy of personal experience.[214] In terms of a more legal definition, the European Charta for Human Rights, Art. 8 defines privacy as "the right to respect for one's private and family life, his/her home and his/her correspondence."

Product: A product is "something that is manufactured to be sold, usually in large quantities,"[215] or "a tangible or intangible output that is the result of a process that does not include activities that are performed at the interface between the supplier (provider) and the customer."[216] In the context of CRISP mainly a security product – thus something that is manufactured to be sold and used in a context of fulfilling a security function.

Project leader: The project leader is one of the three actors within the evaluation phase of the CRISP methodology. The project leader is the main actor during the configuration stage of the evaluation phase and creates the scenario for the security PSS in question. The project leader also participates in the assessment stage.[217]

Project participant: The project participant is one of the three actors within the evaluation phase of the CRISP methodology. The project participant mainly contributes to the assessment stage and should answer the questions of the evaluation criteria questionnaire.[218]

Risk: Risk is the effect of uncertainty on objectives, whereof effect a positive and/or negative deviation from the expected is. Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). Risk is often characterized by reference to potential events, and consequences, or a combination of these and is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.[219] In short, *risk is the likelihood combined with the effect of loss, damage or harm.*[220]

[213] Roger Clarke, Introduction to Dataveillance and Information Privacy, and Definitions of Terms. 2013. http://www.rogerclarke.com/DV/Intro.html
[214] Ibid.
[215] Cambridge dictionaries
[216] http://www.praxiom.com/iso-definition.htm
[217] Cf. Hempel, Leon, et al., op. cit., 2015.
[218] Ibid.
[219] Cf. ISO 22300:2012 Societal Security - Terminology.
[220] EN-IEC 62676-1-1:2014 Video surveillance systems for use in security applications - Part 1-1: System requirements – General.

STEFi approach/methodology: The STEFi approach or STEFi methodology requires within a security technology assessment that a security technology or action shall be secure, trustworthy, efficient and respect freedoms and human rights. These are also the basic dimensions of STEFi: Security, Trust, Efficiency and Freedom infringement. For CRISP, the STEFi approach has been adapted and consists of these four dimensions from which each a set of criteria relevant for the specific dimension break down. Each criteria than can again be broken down into attributes and relevant questions – creating a three layer methodology.[221]

STEFi evaluation criteria: criteria to evaluate security products, systems, services from security, trust, efficiency, freedoms and human rights perspective based on the STEFi approach of CRISP.[222]

Safety: Safety is the condition (perceived or confirmed) of an individual, a community, an organisation, a societal institution, a state, and their assets (such as goods, infrastructure), to be protected against dangers or threats resulting from unintended natural and/or man-made hazards or accidents.[223]

Seal: see Mark.

Security: Security is the condition (perceived or confirmed) of an individual, a community, an organisation, a societal institution, a state, and their assets (such as goods, infrastructure), to be protected against danger or threats such as criminal activity, terrorism or other deliberate or hostile acts, disasters (man-made).[224]

Security Demands: Security demands are a category of key requirements within the CRISP Taxonomy and designate necessities in respective security application areas which should be implemented by the function of the security PSS. Examples are cybersecurity, building security, etc.

Security of the citizens: including counter terrorism, crime prevention and organised crime, and public order as necessary subareas. In general it covers all possible threat aiming at European citizens, in public and semi-public spaces as well as in private spaces, as a result of an intended/deliberate attack or a natural hazard, by trying to create a peaceful environment, including the prevention of radicalisation.

Service: A "Service is the result of at least one activity necessarily performed at the interface between the supplier and customer and is generally intangible."[225]

[221] Kamara, Irene, et al., op. cit., 2015, D4.3 CRISP project.
[222] Ibid.
[223] Derived from Chapter 3: A function-oriented approach to security.
[224] Idem.
[225] ISO/IEC 17065:2012 Conformity assessment - Requirements for bodies certifying products, processes and services.

Standards: "A standard is a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose."[226]

Surveillance: Surveillance can have different meanings, depending on the context. When talking about conformity assessment, surveillance is the last step in conformity assessment and "can take place at the point of production or in the supply chain to the marketplace, in the marketplace, at the place of use. Based on the reviewing of the outcome of the determination activities, the referring back to the determination stage may take place to resolve nonconformities. In all other situations this process will end up by drawing up and issuing confirmation of continued conformity."[227] In the context of security, surveillance is mainly used as a form of observing a place or a person – also by technical means – because of a crime that has happened or is expected to be happening.[228]

System: A system is a "set of interrelated or interacting elements."[229]

Testing: Testing is a method in conformity assessment and can include the related activities of calibration and measurement.[230]

Technical specification: A technical specification is another normative document used for conformity assessment beside standards. The main differences in regard to standards are that technical specifications upon development don't need public consultation but can be approved by the developing committee and are usually established for specifications in evolving technologies and experimental markets.[231]

[226] www.iso.org
[227] Wurster, Simone, Tim Pohlmann, Nathalie Hirschmann, Patrick Murphy, Jolien van Zetten, Ying Ying Lau, Tatsiana Haponava, Thordis Sveinsdottir, Rachel Finn, Rowena Rodrigues, Kush Wadhwa, Reinhard Kreissl, Florian Fritz, Roger von Laufenberg, Cristina Pauner, Artemi Rallo, Rosario García Mahamut, Jorge Viguri, Irene Kamara, Paul de Hert, Eva Kalan, Jelena Burnik, Igor Kolar (2015): Consolidated report on security standards, certification and accreditation – best practice and lessons learnt. D.2.2 CRISP Project.
[228] Cf. Cambridge dictionaries.
[229] ISO 9000:2015 Quality management systems - Fundamentals and vocabulary
[230] Cf. Wurster, Simone, et al., op. cit., 2015.
[231] Cf. Ibid.

Transparency: Transparency in CRISP relates to the STEFi dimensions and is a requirement both to security PSS as well as to the evaluation/certification scheme itself. The evaluation scheme should be clear on what the scope of the evaluation, its evaluation procedures, the validity period of its evaluation, its rules, criteria and methodology. And this information should be easily accessible to any interested party, without additional burdens. This provides the consumer with the necessary capability to control and make a conscious choice on the product or systems he or she employs. Transparency is also substantial for building trust to the security measure; the scheme should impose transparency obligations to the security PSS under evaluation, such as open and accessible security and information policies, auditable processes and documentation. The transparency of the results of a certification – in this case through the STEFi model – should be made publicly available. This gives more accountability on what requirements were in the reality achieved, what is the exact level of compliance, instead of simply stating that certain criteria were met and thus the security PSS is certified.[232]

Trust: Trust encompasses the experience of the product provider as well as of the scrutinized in using the product. Beside the experience, the subjective perception defines the way in which a product achieves an appropriate acceptance level. Evaluation criteria for the Trust dimension include, for example, the degree of discrimination regarding the use of product and the potential physiological and psychological invasiveness of the product. For instance, health risks such as DNA damage associated with the ionising radiation used in body scanners or other effects such as claustrophobia and anxiety attacks.[233]

Technology Readiness Level (TRL): TRL is a method of estimating the maturity level of a particular technology and is based on a scale from 0 to 9, 9 being the most mature technology.

TRL 0: unproven concept, no testing has been performed;
TRL 1: principles postulated and observed but no experimental proof available;
TRL 2: technological concept and application have been formulated;
TRL 3: first laboratory tests completed; proof of concept;
TRL 4: small scale prototype built in a laboratory environment;
TRL 5: large scale prototype tested in intended environment;
TRL 6: prototype system tested in intended environment close to expected performance;
TRL 7: demonstration system operating in operational environment at pre-commercial scale;
TRL 8: first of a kind commercial system (manufacturing issues solved);
TRL 9: Full commercial application, technology available for consumers.[234]

Users: see End-users.

[232] Kamara, Irene, et al., op. cit., 2015, D4.1 CRISP project.
[233] Kamara, Irene, et al., op. cit., 2015, D4.1 CRISP project.
[234] Schild, Philippe, "Horizon 2020", no date.
http://ec.europa.eu/research/conferences/2013/energy_infoday/pdf/session_3_summary_of_the_calls_open_in_2014_-_philippe_schild.pdf.

8.2 STEFI CRITERIA TERMS

Accuracy: the condition or quality of being true, correct, or exact; freedom from error or defect; precision or exactness[235].

Adaptability: being able to adapt or be adapted to many different functions or activities.

Anonymisation: rendering anonymous, non-identifiable.

Automated decision making: Assembling personal data, creating disproportionately large datasets that can be used for anticipatory action (decision(s) taken using personal data processed solely by automatic means).

Availability of a security system: property of being accessible and usable upon demand by an authorized entity[236].

Awareness: knowledge that something exists.

Bodily integrity: inviolability of the physical body and emphasizes the importance of personal autonomy and the self-determination of human beings over their own bodies.

Categorisation (in relation to non-discrimination): placing in a category according to sex, race, color, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

Consent: any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed[237].

Data processing: any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction[238].

Data transfer: transfer of personal data to a non-EU country.

Documentation: the management system, including related processes; — information created in order for the organization to operate; — evidence of results achieved (records) ISO 9000:2015.

Due process: fairness in proceedings, in accordance with established and sanctioned principles.

Energy efficiency: The ratio of output energy to input energy during an identified period.

---

[235] http://www.wordreference.com/definition/accuracy

[236] ISO/IEC 27000:2014(en) Information technology — Security techniques — Information security management systems — Overview and vocabulary

[237] General Data Protection Regulation (political agreement text – December 2015): http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/en/pdf

[238]

Equal treatment: Prohibition of any difference in treatment that lacks an objective and reasonable justification art. 14 ECHR and art. 21 Charter of Fundamental Rights of the European Union.

Ergonomics: the security product or system is easy to use or understand, self-explanatory and is designed for practicability and comfort in the environment it is employed.

Fair distribution of security: equal protection of individuals in terms of security.

Freedom from unlawful detention: freedom from being kept or confined in custody without any lawful reason.

Function creep: the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to potential invasion of privacy.

Hazard: Hazard is a source of potential harm, or a source of risk. [239]

Interoperability: ability of systems to provide services to and accept services from other systems and to use the services so exchanged to enable them to operate effectively together[240].

Legality: exercise of a right in accordance with an accessible and foreseeable law (art. 8 ECHR).

Legitimacy: serving a legitimate aim on the grounds of national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others. (art. 8 ECHR)

Lifecycle costs: costs arising from owning, operating, maintaining, and disposing of a security PSS[241].

Location data: data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service[242].

Misuse: Any use other than the intended from the producer, the system owner or the service provider.

Non-discrimination: Avoidance of differential treatment based on the protected grounds of sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

Observability: capability of being or liable to be observed; noticeable; visible; discernible.

Perception: a belief or opinion, often held by many people and based on how things seem.

---

[239] ISO 22300:2012 Societal Security - Terminology.
[240] EN 15213-1:2013-06
[241] 1995 edition of NIST Handbook 135, Life-cycle Costing Manual (adapted definition for CRISP needs) http://fire.nist.gov/bfrlpubs/build96/PDF/b96121.pdf
[242] 2002/58/EC Directive as amended and valid

Performance: Measurable result. It relates either to qualitative or quantitative findings. Performance can relate to the management of activities, processes, products (including services), systems or organizations.[243]

Personal data: Any information relating to an identified or identifiable natural person 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.[244]

Physical freedom: Absence of external compulsion or violence that would coerce a person to act or not act in a certain way.

Physiological invasiveness: intrusion to the physical sphere of the scrutinised, involving touching or the introduction of instruments or other objects into the body or body cavities.

Presumption of innocence: the right to be free from legal wrong unless proven guilty.

Privacy: right to respect for one's private and family life, his/her home and his/her correspondence (art. 8 ECHR, art. 7 Charter Fund. Rights EU).

Profiling: any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements[245].

Reliability: the quality or ability of being able to be trusted to do or provide what is needed/ able to be believed: likely to be true or correct.

Resilience: Resilience is the adaptive capacity of an organization in a complex and changing environment, or the ability of an organization, of citizens, of systems, or of societies to manage disruptive related risk.[246]

Risk assessment: A scientific and technologically based process consisting of three steps, risk identification, risk analysis and risk evaluation[247].

Risk level: magnitude of a risk expressed in terms of the combination of consequences and their likelihood[248].

[243] ISO/IEC 27000:2014(en) Information technology — Security techniques — Information security management systems — Overview and vocabulary
[244] General Data Protection Regulation (political agreement text – December 2015): http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/en/pdf
[245] General Data Protection Regulation (political agreement text – December 2015): http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/en/pdf
[246] ISO 22300:2012 Societal Security - Terminology.
[247] https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
[248] ISO/IEC 27000:2014(en) Information technology — Security techniques — Information security management systems — Overview and vocabulary

Risk management: The process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and selecting appropriate prevention and control options.[249]

Risk: the likelihood, combined with the effect, of loss, damage or harm[250].

Robustness: Ability to detect, handle abnormal situations and continue to operate.

Safety: Safety is the condition (perceived or confirmed) of an individual, a community, an organisation, a societal institution, a state, and their assets (such as goods, infrastructure), to be protected against dangers or threats resulting from unintended natural and/or man-made hazards or accidents.[251]

Self-incrimination: the result of giving testimony in a trial or other legal proceeding that could subject oneself to criminal prosecution.

Sensitive personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life[252].

Threat: potential cause of an unwanted incident, which can result in harm to individuals, a system or organization, the environment or the community.[253]

Transparency: the quality of being clear, open and frank.

Usability: The effectiveness, efficiency and satisfaction with which specified users achieve specified goals in particular environments.

Utilisation: the act of making use of something[254].

[249] European Union Agency for Network and Information security, no date, https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary.
[250] EN-IEC 62676-1-1:2014 Video surveillance systems for use in security applications - Part 1-1: System requirements - General
[251] Derived from Chapter 3: A function-oriented approach to security.
[252] General Data Protection Regulation (political agreement text – December 2015): http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/en/pdf
[253] ISO 22300:2012 Societal Security - Terminology.
[254] Online dictionary, http://www.investorwords.com/11444/utilisation.html