Theme [ICT-2009.1.4]

Trustworthy ICT

effectsplus

European Framework for Future internet – compliance, Trust, security and Privacy through effective clustering.

Project Nº 258750

THE INNOVATION POTENTIAL OF

FP7 SECURITY AND TRUST PROJECTS

Responsible: **Fabio Massacci (University of Trento)**

Contributors: Gloria Comper, Bruno Crispo (University of Trento), Keith Howker (TSSG), Nick Papanikolau (HP Labs)

Document Reference: D2.2 – THE INNOVATION POTENTIAL OF FP7 SECURITY AND TRUST PROJECTS

Dissemination Level: PU

Version: 42.8

Date: 2011-10-07

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

This report presents a comprehensive study on the innovation potential of FP7 projects funded by the ICT Call 1 for Trustworthy ICT and the Joint ICT and Security Call. This study is based on documental evidence (deliverables, publishable reports, etc) and ethnographic research (interviews and feedback from project coordinators).

The analysis of the ***industrial landscape*** showed a connected community (a scale-free network) with few major players, but without a clear market dominance:

- few general *software producers and integrators* act as bridges and hubs between different interests groups (such as privacy and critical infrastructure protection);
- *specialized IT security companies* are emerging as actors involved in two or more projects, but are still at SME stage.

The cross-call analysis shows that the field is very dynamic as the priorities of the call can significantly change the type of partners and their collaborative relations.

The study of the ***innovation potential*** identified many research results which can stimulate product, service and process innovation in Europe. In synthesis:

- some projects have produced research *results that are directly usable by citizens* (for example in the realms of biometrics and privacy);
- most projects have delivered significant innovations in *tools and methods for ICT specialists* (from consultants on IT governance to IT administrators) that are widely usable beyond the project's consortium. Such contribution is mostly in the area of command, control and compliance (of networks and IT systems).

An interesting contribution by some research projects is represent by an improved *community knowledge* of the security echo-system. This knowledge can be used by decision makers to shape their agenda.

The Security and Trust projects also contributed to the ***achievement of the objectives of the Digital Agenda***, in particular on those focusing on instruments for self-regulation and for improving privacy and security of infrastructures and services.

The analysis also showed that two major issues are only addressed partially and indirectly by the projects of Call 1, Call5 and the joint Security and ICT Security Call::

- *cyber-security and -preparedness to counter cyber-crime and cyber- attacks*
- *children protection on the internet*

Initiatives such as Joint Calls might be an option to pursue in these sectors.

The analysis also identified gaps in the "last mile" to a product that could be addressed by a mixture of organizational, funding, and regulatory measures such as

- set-up of *structured relations with product groups or users* from the project's start,
- specific *funding measures by the EC for experimenting in large scale trials* with a simplified funding procedure,
- European *regulatory initiatives on the controlled disclosure of security incidents*.

The adoption of these measures might ensure that ICT progress is rapidly transformed into products for the benefits for Europe's citizens, businesses, industry and governments.

2 THE COSTITUENCY OF FP7 SECURITY AND TRUST PROJECTS

2.1 METHODOLOGY FOR THE STUDY

This study has been carried out by the University of Trento in cooperation with the EFFECTPLUS partners by combining documents' analysis (projects' publishable summary, deliverables, and web sites) and personal focused interviews - at first with project officers (currently or previously in charge of the project) and then with project coordinators or technical leaders. A parallel analysis has been conducted, based on the above material on the digital agenda to further refine and specify the indications of the project coordinators on how their project contributed to the digital agenda.

Table 1 shows the list of projects that have been considered so far which also explicitly reference the particular area of the calls addressed by the project (FP7 ICT Call 1 on Security and Trust, and the Joint ICT and Security Call on critical infrastructures).

Table 1 - Projects Considered in the Study

Acronym	Start date	Project Name	Project area
ACTIBIO	March 2008	Unobtrusive Authentication Using Activity Related and Soft Biometrics	Research activities in trust, privacy and identity in the digital economy. Research activities in enabling technologies for security and trustworthiness of ICT
AVANTSSAR	January 2008	Automated VAlidatioN of Trust and Security of Service-oriented ARchitectures	Research activities in trustworthy and secure service infrastructures
AWISSENET	January 2008	Ad-hoc pan and WIreless Sensor SEcureNETwork	Research activities in secure and trustworthy network infrastructures
CACE	January 2008	Computer Aided Cryptographic Engineering	Research activities in enabling technologies for security and trustworthiness of ICT
CONSEQUENCE	January 2008	Context-aware data-centric information sharing	Research activities in trustworthy and secure service infrastructures
ECRYPT II	August 2008	European Network of Excellence for Cryptology II	Research activities in enabling technologies for security and trustworthiness of ICT
GEMOM	January 2008	Genetic Message Oriented Secure Middleware	Research activities in secure and trustworthy network infrastructures
INSPIRE	November 2008	INcreasing Security and Protection through Infrastructure REsilience	Research activities in critical information infrastructure protection
INTERSECTION	January 2008	INfrastructure for heTErogeneous, Resilient, SEcure, Complex, Tightly Inter-Operating Networks	Research activities in secure and trustworthy network infrastructures
MASTER	February 2008	Managing Assurance, Security and Trust for Services	Research activities in trustworthy and secure service infrastructures
MICIE	September 2008	Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures	Research activities in critical information infrastructure protection
MOBIO	January 2008	Mobile Biometry	Research activities in trust, privacy and identity in the digital economy. Research activities in enabling technologies for security and

Acronym	Start date	Project Name	Project area
			trustworthiness of ICT
PICOS	February 2008	Privacy and Identity Management for Community Services	Research activities in trust, privacy and identity in the digital economy
PRIMELIFE	February 2008	Privacy and Identity Management in Europe for Life	Research activities in privacy and identity in the digital economy
PRISM	March 2008	PRIvacy-aware Secure Monitoring	Research activities in secure and trustworthy network infrastructures. Research activities in trust, privacy and identity in the digital economy.
SECURESCM	February 2008	Secure Supply Chain Management	Research activities in trustworthy and secure service infrastructures
SERSCIS	October 2008	Semantically enhanced resilient and secure critical infrastructure services	Research activities in critical information infrastructure protection
SHIELDS	January 2008	Detecting known security vulnerabilities from within design and development tools	Research activities in enabling technologies for security and trustworthiness of ICT
SWIFT	January 2008	Secure Widespread Identities for Federated Telecommunications	Research activities in secure and trustworthy network infrastructures. Research activities in trust, privacy and identity in the digital economy.
TAS3	January 2008	Trusted Architecture for Securely Shared Services	Research activities in trustworthy and secure service infrastructures, in privacy and identity in the digital economy
TECOM	October 2008	Trusted Embedded Computing	Research activities in trustworthy and secure service infrastructures
TURBINE	February 2008	Trusted revocable biometric identities	Research activities in trust, privacy and identity in the digital economy. Research activities in enabling technologies for security and trustworthiness of ICT
UAN	October 2008	Underwater acoustic network	Research activities in critical information infrastructure protection
VIKING	November 2008	Vital infrastructure, networks, information and control systems management	Research activities in critical information infrastructure protection
WOMBAT(*)	January 2008	Worldwide observatory of malicious behaviors and attack threats	Research activities in secure and trustworthy network infrastructures
WSAN4CIP	January 2009	Wireless sensor networks for the protection of critical infrastructures	Research activities in critical information infrastructure protection

(*) The WOMBAT project coordinator and technical leader could not be interviewed, but not for lack of trying on EFFECTSPLUS's side.

2.2 The Landscape of Partners, Industries and Collaborations

The projects considered in this study included more than 200 partners. This section briefly analyzes the structure of this constituency.

The graph in Figure 1 describes the "social relationship" among the projects in order to understand synergies and group dynamics. To ease readability we decided to show only the partners who participated in two or more projects. The size of a node is determined by the number of links - i.e. the number of projects - and it is not determined by the budget of the partner. Thus, a partner represented by a large node is not necessarily a well-funded organization; rather it is a well-connected organization in this research community. Obviously partners that belong to many IPs tend to be more funded than a partner doing a single STREP, but that's not necessarily true.

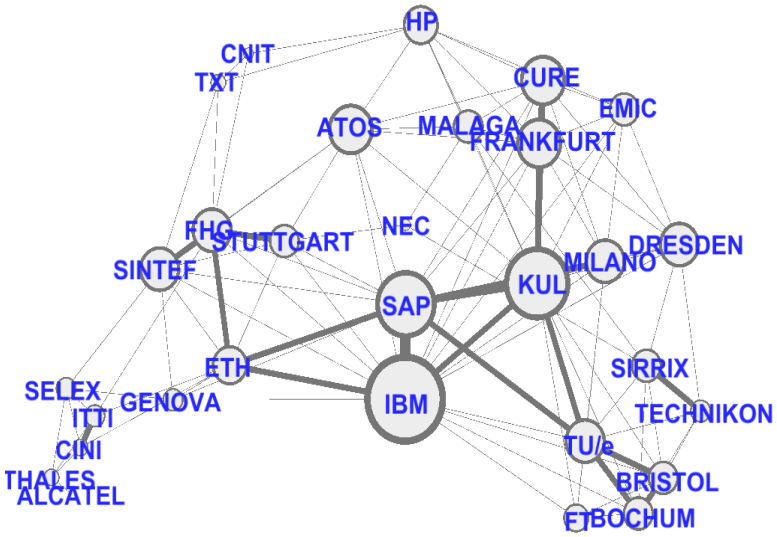

Figure 1 - Key Partners in Call 1 and Joint Call Projects

The structure of the network is a scale-free graph: few major hubs act as bridge between minor partners. An interesting observation is that there are no disconnected components. In policy terms disconnected components would mean that the constituency is built by separate communities each pursuing its own R&D activities.

On the bottom right one can recognize a "crypto-corner" (KUL, TU/e, Univ. of Bochum and Bristol, plus FT) and on the top/center right a "privacy group" (KUL, Univ. Milano, Frankfurt, and Dresden, up to HP). KUL and Dresden universities act as bridges between the groups. On the far bottom right we find the partners working on "critical infrastructure protection" (SELEX,THALES, Alcatel, CINI). Software Engineering partners are more scattered on the center left (ETH, SINTEF, FHG, up to ATOS and TXT).

Another observation is that the core of the community is represented by few general software companies and IT integrators. Telecom and critical infrastructure operators play a significantly minor role in call 1 and the joint call Security and ICT. This is only true for what concerns their ability of playing the role of research hubs. Indeed, later in Figure 2 we see that Telecom operators are more than seventeen and almost the same number of software integrators.

The major role of some academic partners can be explained by their ability to contribute to different fields (such as legal and IT experts). The same can be said of IT integrators and software companies. On the other side, no player has a significant social dominance and rather large players tend to cooperate. Interestingly, there is no large hub which is a specialized IT security company, only SIRRIX and SEARCH-LAB are present in both Call 1 and Call 5. In contrast, specialized IT security companies are a significant share of the participants (See Figure 2). In other words, IT security company do participate to the call but they are not the hubs of the community. This phenomenon might be explained by the fragmented nature of the IT security market.

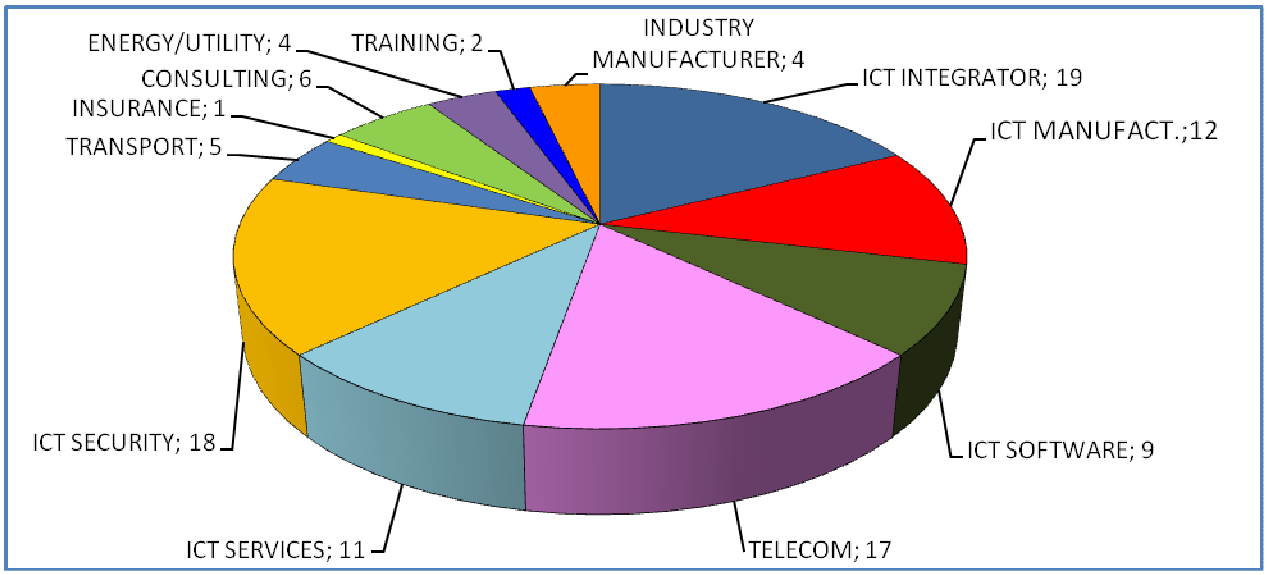

Figure 2 - Global Call 1 Breakdown by industry sector -

The analysis of Call5 shows the same trend with a large domination of software vendors and integrators, but with a significantly larger participation of telecom operator. This might be explained by the greater emphasis on critical infrastructure of Call5wrt Call 1 which had a greater emphasis on privacy. This is also reflected in the academic partnership.

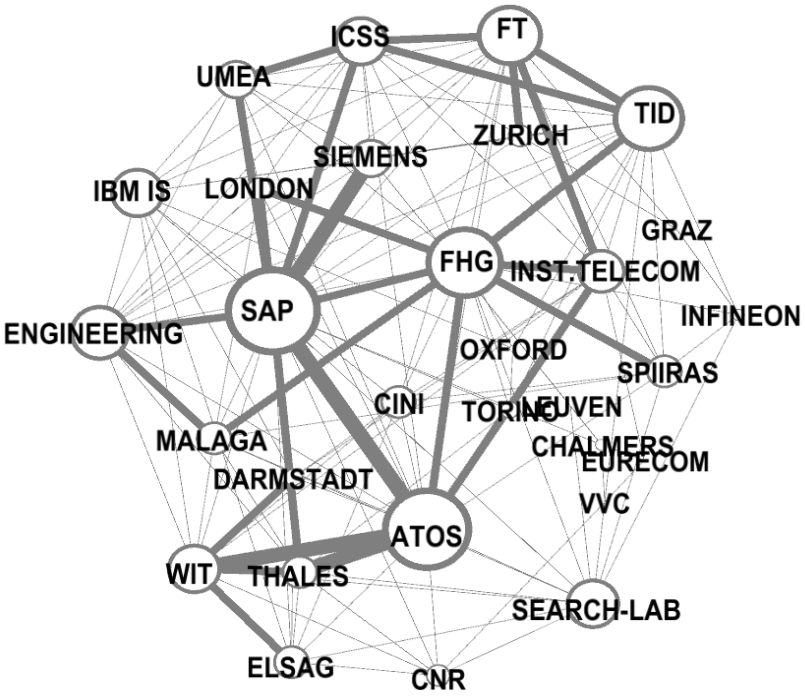

Figure 3 – The Key Partners of Call 5

The graph in Figure 4 represents the aggregated breakdown per type in the projects over the total funded by Call 5. It confirms a significant role of academic partners. - for the preparation of this report we had no access to the financial breakdown of individual partners, so we cannot determine whether a different picture would be obtained by considering funding instead of just participation.

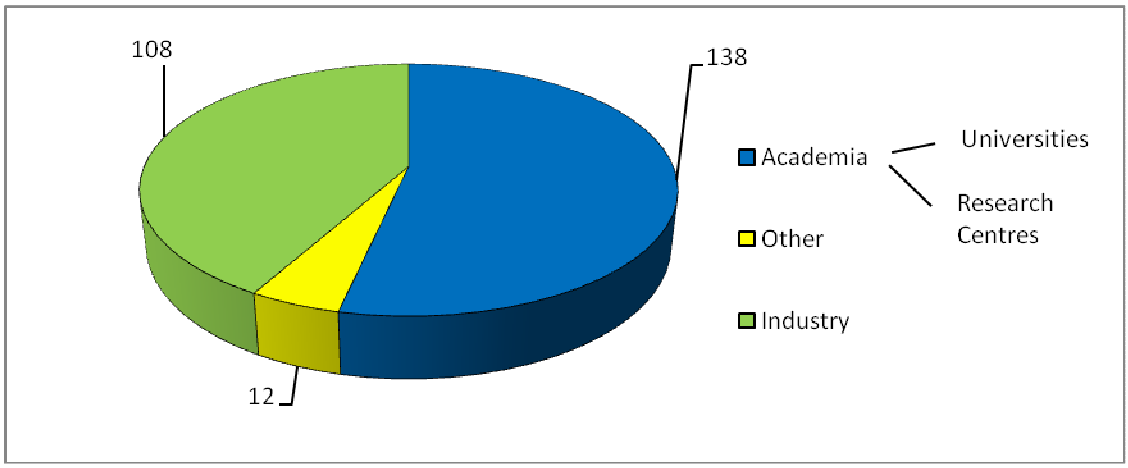

Figure 4 - Global Call 1 Breakdown by partner type –

The graph in Figure 5 shows the distribution of the different category of academic partners, large industries and SMEs for project.

The upper dash per category represents the maximum number of partners of that type per project, while the lower dash represent the minimum number. The solid box represents how the majority of projects (25%-75%) is distributed. The academia column is the aggregate value for research centres and universities. Since they are sometimes considered in different categories we also give the individual columns for both universities and research centres. Clustering together research centres and universities we see that the large majority of projects (in the 25%-75% percentile) has between 1 to 6 academic partners with a maximum of 12 academics partners.

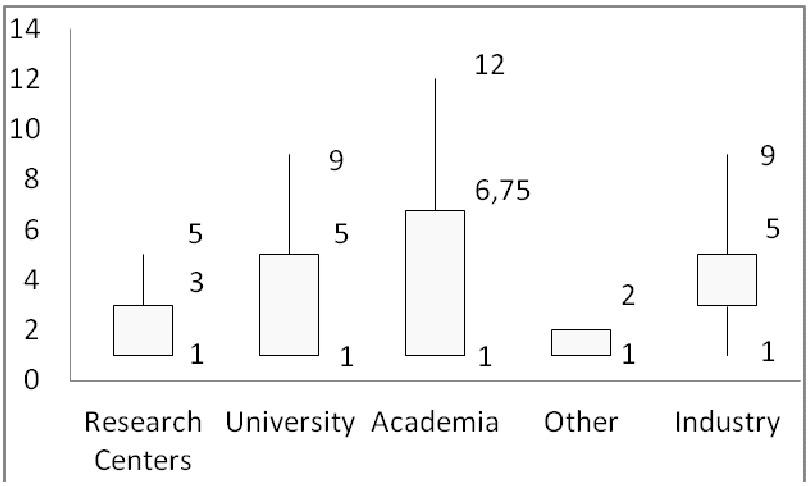

Figure 5 - Distribution of Partners per Project

2.3 DIRECT BENEFICIARIES OF PROJECT RESULTS

Most projects include case studies that are used to validate their R&D activities. All interviewed coordinators stressed the importance of those pilots to validate their results. In this section, we discuss the first immediate potential buyers of a technology that were tried during the project. For example, a government might mandate a privacy- (or escrow-) preserving architecture, but it is not the actual buyer of the technology. The actual direct buyer of the marketable version of the R&D result would only be the telecom operator complying with the mandate.

From this perspective we can identify the main industries as follows:

- An important target is the **Security Industry** as such. These companies are the natural buyers of research results which provide mechanisms and devices to monitor an environment or

recognize a human being. For example **ACTIBIO**'s biometrics technology recognizing humans by their face dynamics was tested in the control rooms of a security company (Group4) and a transport company (Gotthard tunnel). The **UAN** project used sensors networks for underwater monitoring of a port. The **MOBIO** project also had case studies of similar nature.

- A refined target is the **IT Security Industry** which is the natural buyer of most cryptographic and authentication solutions. **PRIMELIFE**'s digital credentials are a good example as well as the techniques for confidentiality-preserving benchmarking in **SECURESCM**. The enforcements mechanisms of **MASTER** could also be used to broaden offering in compliance. Methods and tools for **embedded Systems Security** were the targets of the **TECOM** and **WSAN4CIP** projects.
- The **Telecommunication industry** is the key target of many research projects . For example the **INTERSECTION** project focused on vulnerabilities (or better removing them) from telecom infrastructure by using distributed testbeds and the collaboration of TELESPAZIO - the Italian satellite network operator - TELEFONICA, the Spanish Telecom operator, and cellular and mobile operators. A similar focus (albeit with different partners) is also present in the **INSPIRE** and the **SWIFT** projects and partly also on the **MICIE** project.

A number of research projects also target the **IT Integration Industry** which is the case of all projects that in a way or another deals with policy-compliance. For example **PRIMELIFE** developed and standardized policies to guarantee the compliance with EU data protection legislation. **MASTER** provided infrastructures to facilitate compliance management

The **Energy Sector Industry** might also be considered a potential beneficiary for all projects which focus on infrastructural threats or attacks to SCADA systems (such as electricity meters). For example **MICIE** tested its results at the Israel Electric Corporation (IEC) facilities, simulating a real piece of an Electrical grids. Also the **VIKING** project simulated its research results on an electrical grid which uses SCADA systems. **INSPIRE** will also test specific security features of SCADA systems.

In the broad area of the **Service Industry** the following areas could benefit from some of the projects: **Social-Network Providers** might use directly a number of techniques from the projects focusing on privacy and identity management such as **PICOS** or **PRIMELIFE**, **Logistics** services could use the results of **SECURESCM**.

Remark. With few exception, such as the Energy Sector Industry, the Logistics or Social Network provider services the transfer of research results to market requires mediation. This gap might be addressed by actions that try to reach and experiments directly with final users.

A side observation is that the prima-facie documentary evidence (e.g. the publishable summary) is still far from being satisfactory from almost all projects (**PICOS** being a notable exception). Many important questions are not addressed: who participated to the validation? Are members of the product groups or members of the research department? Did users[1] of research results actually used the research techniques or just looked at results produced by researchers[2]? How many people participated into these activities? Since the publishable report is the road to the project results by third parties, this lack of information might stifle further innovation.

This unsatisfactory state might be also be explained by the relatively young nature of IT as experimental discipline: there is not yet a community understanding on what is the "right"

[1] Notice that a "user" of a research result is not necessarily a "end-user" in the IT sense (such as a teenager using a mobile phone). It might be a security engineer in a software company or a SCADA expert in a power company.

[2] For example did the researchers set-up the test-bed or the actual users did this job?

presentation of the results from pilots trials and from experiments. This lack of clarity is also present in many deliverables on pilots where threats to validity are not described[3].

In absence of this information, the direct applicability of a research results to a specific industry must be understood as a target and as a proof-of-concept demonstration for which more evidence is needed (we will return on this issue later in the gaps section).

Recommendation: Projects should report in more effective and consistent way the methodology and actual dimension of pilots and trials with end users or product groups.

[3] While a medical study might report that "The drug was distributed to 100 volunteers by 10 general practitioner and 5 specialist of internal medicine, and 80 patients survived", a IST project would only report "The drug was distributed to some patients who survived.".

3 KEY RESEARCH RESULTS WITH INNOVATION POTENTIAL

3.1 RATIONALE FOR A CLASSIFICATION

A rough classification of the technical results with innovation potential can divide them into three major classes: at one end of the spectrum we find results that can appeal to ***product innovation in ICT for citizens*** and at the other end the results which address ***product/process innovation for ICT specialists*** of critical importance. As simple examples of the extremes we can consider a driver authentication module for a car (mass market) and a security protocol verification tool kit (niche market).

The innovation barriers that must be overcome vary depending on the position in the innovation spectrum. Consider the opposite cases of a secure software verification tool and a biometric device for operating a car. Advocate of the former result must be able to tailor their toolkits to very specific customers' needs and internal quality processes. Still, they face less inertia as the adoption of a technology is essentially a single decision: if they can prove that the technology saves money or improves product's quality the steps to adoptions are short. The major obstacle for results targeting innovation for citizens is the strong force of inertia. Convincing tens of (more or less stubborn) engineers from a verification group in a company to use a new tool is far different than convincing millions of customers to pay a higher price for a car they can no longer lend to their friends by a simple hand-over of a key. Results targeting product innovation in ICT for citizens must consider wider societal acceptance issues, but once they are accepted the law of inertia will play in their favor. In contrast, innovations for specialized markets must be able to adapt their technologies to the underlying dynamics of the product/process of their specialized markets.

An intermediate area between these two extremes is the wide area of ***software developers*** **and** ***system administrators***. Efforts to transform research results in this area must also overcome the hurdles of inertia as they need a vector for the distribution of their technology to a large (albeit not mass) market. At the same time they must be able to maintain and adapt the technology as the underlying IT languages and systems evolve.

A separate case are **knowledge-based contributions**: they do not identify a specific result that can be transformed into a product, but they are a tangible manifestation of an increased knowledge that can be concretely used by the community. Projects that produce databases of information (attacks trends, vulnerabilities etc.) belong to this category.

3.2 PRODUCT INNOVATION IN ICT FOR CITIZENS

Among the results that have the potential to reach a product innovation in ICT for citizens, we can list the (car) driver authentication module that **ACTIBIO** has developed biometric technologies that complements traditional biometrics (such as fingerprints' or iris' recognition). The technology makes use face dynamics, gait and activity-related actions to recognize the user when someone is on the move. This technology can be used to improve the results of other biometrics models or to provide an alternative way to access to services by disabled people. What is still missing is a large study of the social acceptability of the technology or the impact that this proposal could have on the whole production chain. A similar approach to complementary biometrics for mobile devices has been pursued by the **MOBIO** project. However, so far, most results of the latter are still at the research stage (e.g. a public database for research purposes). This is also due to a problem of societal acceptance of biometric as an authentication mean.

Another very large market that can be affected by research results of security project is the domain of controller devices in critical infrastructures (or SCADA networks for short). For example, the **MICIE** project has developed a tool that helps to increases the QoS in the supply of energy between the energy producers and customers. The validation activities of the project has demonstrated a considerable reduction in the time of unsupplied power when the **MICIE** tool is used, thus allowing to improve QoS to final customers. This is also made possible by the overall approach that allows to better predict events and consequences of cascade failures on the system state. In the same area of SCADA system assessment, the INSPIRE and **VIKING** projects

provided systems for assessment of the security state of the SCADA network by integrating suitable semantic information from databases reporting intrusions, faults, attacks or other relevant societal information. However, the performance of such systems is highly dependent on the presence of updated vulnerability and attack information which is often not available. This lack of shared data about attacks and vulnerabilities has been raised by many project coordinators and is one of the main hurdles to performance assessment for ICT security products and is therefore discussed in the section on potential innovative measures.

The other domain in which there is a potential for the product innovation in ICT for citizens is the realm of social networks and privacy protection. For example, the **PRIMELIFE** project has developed a theory and technology for the privacy management of users by using anonymous digital credentials and encryption based on a web of trust . This project's result has got major media attention in the Netherlands like, for i.e. radio coverage, and a pilot live system with a sizeable number of users (also thank to the media coverage). The **PICOS** project has carried out a similar experience for the community of anglers developing a client for location services that respects the privacy wishes of the individual angler. Those results are particularly promising as they have involved a large numbers of end-users which helps to identify features. However, it is still unclear which part of the research's results is the marketable one. For example, in the case of the **PRIMELIFE** project the anonymous digital credential might be the final marketable results (which is currently under trial in the ABC4Trust EU project) rather than the overall architecture.

3.3 Product Innovation for IT System Administrators

This class of users is significantly large. According a 2011 EURES survey of the most requested professional jobs in Europe, the 5th and 6th top-most positions are respectively for IT programmers and IT administrators. They belongs to the class of technical savvy users that could be easily targeted by owners of FP7 security and trust research results. Many projects have produced management and monitoring tools for complex IT system. These results have the potential to improve the overall echo-system, but it is unclear from the evidence supplied by the projects whether there is enough economic margin for distributors (in the same way that RedHat and SuSe distribute variants of the Linux operating system).

For example, the **PRISM** project has produced specific probes for network monitoring. Those probes allow to reduce the data that telecom operators needs to process and store in order to be compliant with the conflicting claims of privacy protection and cyber crime laws.

More specific results includes the development of novel intrusion detection, tolerance or anyhow monitoring systems (IDS for short). This is a frequent result of many projects that focus on protocols, networks and location based services. Another example: **AWISSENET** has implemented an IDS that builds upon its results on service discovery and traffic analysis.

3.4 Product Innovation for Software Developers

"Plug-and-play" security libraries and toolkit for mainstream software and Information systems developers is a technical results that has been frequently the target of many projects funded by the F5 Unit in the past and is present today.

For example the experts in the **CACE** project has provided a number of advanced crypto-libraries ranging from fast secure networking, including tools for automatically compiling zero-knowledge protocols, to secure multi-party computations. Secure multi-party computation libraries (applied to supply-chain information systems) are also among the results of the **SECURESCM** project. Other repositories of efficient implementations of secure system that covers both software and hardware implementations has been provided by the **ECRYPT II** project which has been able to achieve significant contributions from outside the consortium.

The **TECOM** project provided similar integrated packages for trusted operating systems, security layers, and trusted protocols focusing for developers of embedded security-critical applications. In the case of the **TECOM** project also some hardware solution were considered and implemented. The **WSAN4CIP** provided similar solutions for wireless sensors network for software attestation and secure execution environments. Since the project is still at the second year at that time of

writing it is not clear yet whether these results will fall in the library for developers or rather in the architecture results (see later the Hard-to-market subsection).

3.5 Product and Process Innovation for ICT Specialists

Protocol designers can use the **AVANTSSAR** platform for protocol verification based on the idea of Verification-as-a-Service. In order to facilitate interoperability the platform provides a translation services back-and-forth different protocol design languages into a core intermediate specification language that acts as a bridge between the different verification services. The ability of the project to overcome the performance barrier has been demonstrated by verification of a protocol by Google (not a member of the consortium). The **AWISSENET** project has directly produced some routing protocols that are based on geographical routing guides that can be used for location based services. In the latter case the evidence for the ability of providing those services outside the consortium is not clear yet.

Another slate of projects focused on information system compliance covering the product/process innovation for ICT specialists market area of information system analysts, architects and auditors (for the design phase). The main result of those projects is typically a methodology which is supported by a tool. This is a market with significant potential as it is at the high-end of the value chain of IT system development. However, it is also very fragmented and it is not clear which efforts have been done by the projects in the area to advertise the results in places such as the ISACA Conferences. An example is the **MASTER** methodology that describes how to refine control objectives from high level regulations down to the specific protection activities. The methodology is supported by a design workbench that transform high-level policies into low level used by the monitoring tool. Another example is the methodology for the development of security metrics proposed by the **GEMOM** project which is supported by a monitoring tool.

The latter monitoring tool produces an output that can be used by decision makers such as CIOs, or CISOs. A similar audience can also be targeted by the supply chain risk simulator from **SECURESCM**, which deals with the risks associated with supply chain information disclosure during the process of data sharing.

Projects focusing on embedded systems can produce brittle but directly marketable results. For example the **UAN** project produced a sensor network working on acoustic channels for underwater surveillance.

3.6 Knowledge Based Contributions

A special category is represented by projects which contributed some research results that cannot be easily (if at all) transformed in products, but that represent a significant contribution to some objectives of the digital agenda such as the development of databases of vulnerabilities (e.g. the **INTERSECTION** and the **SHIELDS** projects) or models of reaction of the society under attacks (e.g. the **VIKING** and **WOMBAT** project). Their contributions are discussed separately in the section devoted to the digital agenda.

3.7 Other Innovation Contributions

Many projects produced among their results **security and privacy architectures and frameworks** of different kind (e.g. **CONSEQUENCE** for the protection of shared data, **GEMOM** for the financial sector, **INSPIRE** for controller devices in critical infrastructures, **INTERSECTION**, **PRISM** and **SWIFT** for telecommunication networks, **PRIMELIFE**, **PICOS** and **TAS3** for collaborative systems, **TURBINE** for pseudo-identities, etc.). Those results are the most difficult ones to be transformed into innovative products: while an IDS system can be transformed and marketed into a product that third parties can buy, a security architecture can only be adopted within the main IT architecture. Therefore, the potential users are limited to the mainstream software integrators and producers (e.g. IBM, ATOS etc) or public entities (that can mandate the architecture in their products). Since those integrators have their own security architecture and the benefit of different architectures are hard to evaluate, the barriers to market are significant for adoption outside the members of the consortium.

In many cases the project that developed an architecture also developed a **policy and specification language**. Some of these languages have been standardized through OASIS, but their commercial adoption is subject to even more uncertainties than novel IT architectures: the adoption of a policy language requires the adoption of the corresponding enforcement engine and therefore the existence of a company that commits to provide an open source or a commercial engine.

4 PROJECTS' CONTRIBUTION TO THE DIGITAL AGENDA

4.1 RATIONALE FOR A CLASSIFICATION

Our aim here is to highlight the links between the research projects funded under the Seventh Framework Program in the area of trust and security and the planned actions and objectives in the Digital Agenda in this area[4].

At first we started with a top-down classification, where we identify the key feature of the Digital Agenda objectives and see what would be the most natural criteria for projects to support it. In order to complete this part we have classify the criteria, numbered using labels of the form [CRIT i] for easy reference in later sections, as Table 2 shows. The result of this preliminary analysis is shown in the appendix.

Table 2 - Criteria related to the Digital Agenda actions -

Criterion name	Digital Agenda Actions	Criterion description
[CRIT 1]	28, 38	Projects which actively engage the ENISA and/or promote the EU's proposed basic principles for internet resilience and stability contribute to the implementation of Digital Agenda Actions 28 and 38.
[CRIT 2]	29, 41	Projects which develop new, and interpret existing, EU and national laws relating to the protection of citizens online (against all forms of cybercrime, including identity theft and breaches of privacy), actively contribute to the implementation of Digital Agenda Actions 29 and 41.
[CRIT 3]	29, 41	Projects which promote the development of tools and techniques for understanding, enforcing laws and regulations on cybercrime actively contribute to the implementation of Digital Agenda Actions 29 and 41.
[CRIT 4]	30, 41	Projects which advance the state of the art in malware detection, prediction of threats and the spreading of threats, contribute to the implementation of Digital Agenda Actions 30 and 41.
[CRIT 5]	31	Projects which develop tools and techniques for detecting attacks on national infrastructure, or which model modes of response to cyber attacks may be deemed to contribute to the implementation of Digital Agenda Action 31.
[CRIT 6]	32, 37, 39	Projects which involve simulations of cyber attacks and which assist in the EU's overall cyber-preparedness contribute to the implementation of Digital Agenda Action 32, 37 and 39.
[CRIT 7]	32, 37, 39	Projects which actively engage with non-EU partners (including where applicable national authorities) to develop principles and methods of cyber preparedness contribute to the implementation of Digital Agenda Action 32, 37 and 39.
[CRIT 8]	33, 39	Projects which involve simulations of, and/or access to, critical national infrastructure for the purpose of helping with the EU's cyber preparedness contribute to the implementation of Digital Agenda Actions 33 and 39.
[CRIT 9]	34, 35, 41	Projects whose output assists in the understanding of citizens' privacy, includes the implementation of privacy-enhancing technologies, models the effect of data breaches, or explicitly develops tools for monitoring/preventing breaches and notifying citizens, contribute to the implementation of Digital Agenda Actions 34, 35 and 41.
[CRIT 10]	36, 37, 40	Projects which develop architectures and tools for detecting, filtering and

[4] Trust and Security is identified as action area 2.3 of the Digital Agenda in document COM(2010) 245, and has subsequently been referred to as "Pillar III", with 13 specific actions, numbered from 28 to 41 and detailed in later sections of this document.

Criterion name	Digital Agenda Actions	Criterion description
		removing objectionable content online contribute to the implementation of Digital Agenda Actions 36, 37, and 40.
[CRIT 11]	36, 37, 40	Projects whose outputs are directly relevant or practically useful to law enforcement authorities in tracing and prosecuting child abuse offenders contribute directly to the implementation of Digital Agenda Action 36.
[CRIT 12]	38	Projects which study the function and operations of CERTs or whose research may directly help in the design of a pan-European cyber emergency response platform contribute directly to the implementation of Digital Agenda Action 38.
[CRIT 13]	39	Projects involving direct participation in the EU's cyber preparedness exercises will help actualize Digital Agenda Action 39.

In a subsequent phase we worked bottom up and projects itself were asked to identify which action item they would support. Project Coordinators or other representatives for the project identified and motivated the relationships between Actions and projects results. The results of this analysis is shown in the appendix as well (**Table *5***). These two contributions have been merged together and distilled in the remaining part of the section.

In order to make the document self contained we list here the key relevant points of the Digital Agenda with a brief summary of the Agenda point and a possible project contribution. It is obvious that for broad action points all project presented in this report can indirectly contributed to its achievement. This is exemplified by the following action point.

ACTION 54 (*DEVELOP A NEW GENERATION OF WEB-BASED APPLICATIONS AND SERVICES*) is focusing on the development of a new generation of web-based applications and services, including for multilingual content and services, by supporting standards and open platforms through EU-funded programs. Industry is increasingly in need of open and interoperable solutions, standards and platforms for new web-based products and services to exploit ICT across all industry sectors and increase their competitiveness on the web.

Clearly all innovative results in terms of architectures, methodologies, and tools listed in the previous section can be used to implement key parts of the open platform envisaged by this action.

4.2 ACTIONS TARGETING POLICIES AND REGULATIONS

For the next agenda points we focus more specifically on security and trust issues and try to mention only direct contributions.

ACTION 17 (*STAKEHOLDER PLATFORM FOR EU ONLINE TRUSTMARKS*) is related to the idea of the Commission to create an "EU online trustmarks" to reassure consumers on the reliability of accredited traders. If certified by an EU trustmark, such sites would help consumers to make informed decisions, when using online retail services. Consumers would benefit from the knowledge that the price comparison site and the listed merchants are accredited and trustworthy.

- The project TAS3 has participated in the SIMS proposal to develop a European Trust Observatory (ETO), which will aim towards the development of trust compliance policies and procedures for Service Providers. Many aspects, such as audit requirements, claims and damages procedures, back-up requirements, personnel vetting procedures etc. will not be implemented by technical protocols, but by organizational and procedure measures. However, such "policy and procedure specifications" need to be technically observable and auditable by the proposed new profession of Trust Auditor. Together these will deliver the information to certify and build trustworthiness into the systems, services and their providers.

The next two actions focus on the establishment of ENISA and pan-european CERTs and the contribution of R&D project will be mostly in terms of sharing knowledge.

ACTION 28 (*REINFORCED NETWORK AND INFORMATION SECURITY POLICY*) relates to the establishment of a pan-European CERT (Computer Emergency Response Team), and particularly

focuses on the enhancement and empowerment of ENISA (European Network Information and Security Agency). There are some potential links to trust and security research that can form the basis of success criteria for FP7 projects, specifically the part of Action 28 that stipulates the development of a set of principles for internet resilience and stability at European and international levels.

- One of the result of **INTERSECTION** project was the definition of a roadmap of best practices for the protection of network system and communication network to guide Telecom operators in the adoption of security strategies. This work stemmed from the initial contacts with the European Policy Office of Network Information Security (NIS). **INSPIRE** participated in the working groups on SCADA security and on network security, and informed ENISA about the project's results. The Consortium has also contacted the Policy Office of the European Commission and it is still in touch with it.

ACTION 29 (*COMBAT CYBER ATTACKS AGAINST INFORMATION SYSTEMS*) requires EU member states to make changes to their legislation to enable law enforcement authorities to combat cybercrime nationally and internationally. The changes are intended to empower the authorities and protect EU citizens online. From this action we infer that research leading to the development of law and regulation for the security of citizens, and work that enhances understanding and interpretation of existing laws related to cyber security, is very relevant to the goals of the Digital Agenda.

- The use of cryptography make it possible to share data without revealing details. Several countries in Europe have already cryptographic guidelines, used by governments and users, but there are many small countries where this gap is present and it's more difficult for government to make recommendations. The white papers, consensus workshops and training activities by the **ECRYPT II** project, try to involved industry experts and help individual users in Europe.

4.3 ACTIONS AIMING AT IMPROVING KNOWLEDGE OF CYBERATTACKS

ACTION 30 (*ESTABLISH A EUROPEAN CYBERCRIME PLATFORM*) underlines the importance of a mechanism for collecting and storing information about Internet-related offences, as well as for obtaining statistics on cybercrime. Such a mechanism would be an essential means of predicting and preventing cybercrime in the future. The next agenda point has the similar objective for national member states.

ACTION 41 (*MEMBER STATES TO SET UP NATIONAL ALERT PLATFORMS*) focuses on the development of platforms for citizens to alert others as to online threats and dangers. The emphasis is on notification and on giving citizens the ability to police the Internet themselves.

- **SHIELDS** has created a service (Security Vulnerability Repository Service) that can be used to create statistics on current threats, and a subscription/notification service provides information about new threats and vulnerabilities, as well as mitigating security activities that can be performed. This service could be directly used to provide notifications. The **WOMBAT** project has a similar database of emerging threats and root cause analysis, but it is not clear whether this would be made available to the public after the project.

The next two actions focuses on the protection of critical national infrastructures and advocate the direct preparation against cyber security attacks and the organization of cyber attack simulations. In this case some of the project results provide an indirect support.

ACTION 33 (*SUPPORT EU-WIDE CYBER-SECURITY PREPAREDNESS*) involves organizing and conducting the first EU cyber preparedness exercise. The action specifies further development of the EU's Critical Information Infrastructure Protection plan, and planning for the execution of the actual exercise. It is clear that if any research projects are to have an impact here, they would have to involve the authorities and other partners with access to such resources. Projects that simulate and/or test the robustness of (parts of) EU ICT infrastructure certainly are relevant here.

ACTION 39 (*MEMBER STATES TO CARRY OUT CYBER ATTACK SIMULATIONS*) is very specific – the criteria we have previously defined for cyber attack detection and prevention, as well as those specifically on simulation of cyber threats and cyber preparedness apply here.

- The tools developed in **VIKING** and **MICIE** can definitely be used for cyber attack simulations and impact analysis as they model the societal impact of attacks on critical infrastructure and on how effective are the response to it.

4.4 ACTIONS FOCUSSING ON PRIVACY

Albeit research projects do not work specifically on supporting the revision process of data protection legislation they can provide technical tools for the implementation of such provisions and also experience with potential problems with users adoption. This means that their results are also directly relevant to the following three action points.

ACTION 34 (*EXPLORE THE EXTENSION OF SECURITY BREACH NOTIFICATION PROVISIONS*) has the goal to revise data protection legislation so that it is more protective of citizens in cases of data breaches; specifically there is an emphasis on mechanisms for notification of citizens when breaches do occur. The implementation of action 34 will be assisted by research projects that take into consideration users' privacy needs and implement suitable protections and commonly agreed means of notification if/when a user's privacy may be compromised.

- Here the experience of the pilots carried by the projects **PRIMELIFE** and **PICOS** might provide an important avenue to understand what users really considers a violation of their privacy. The specification languages developed in those projects and the notification mechanism indentified by the **TAS3** project can then be used by organizations to easily implement those regulations.

ACTION 35 (*GUIDANCE ON IMPLEMENTATION OF TELECOMS RULES ON PRIVACY)* is closely related to action 34 (and also other non-security-specific Digital Agenda Actions). There is a risk of incorrect and/or inconsistent implementation and the intent is to achieve an effective protection of ePrivacy rights and legal certainty for industry.

- The recommendations for telecom operators developed by the **INTERSECTION** directly applies here. We can also find a direct application of all project results that focus on compliance. Organizations seeking guidance on how to implement those rules can directly use the **MASTER** methodology and the **MASTER** tools for deploying specific IT policies derived from the "rules on privacy". The **PRISM** solutions for telecom operators, in particular for network monitoring might also be used directly. In a similar trend one could use the policy languages and technologies developed by the **PRIMELIFE** project. To make sure that operations are implemented correctly the **AVANTSSAR** platform could also be used in order to identify vulnerabilities as soon as possible.

ACTION 37 (*FOSTER SELF-REGULATION IN THE USE ONLINE SERVICES)* focuses on the protection of minors with regards to their use of the Internet and online services and in particular the usage of special protection mechanisms for minors in social networks.

- The **PRIMELIFE** project did not explicitly focused on children protection, but their research results on social networks that we have discussed in the previous sections can be directly adapted to this case.

4.5 ACTIONS NOT SUPPORTED BY PROJECT RESULTS

For some points of the Digital Agenda, there was no project result that could contribute directly to its implementation, but only indirectly to provision of results to industry and the echo-system in general. We briefly list them below and what the current research projects can do for them.

ACTION 31 *(ANALYZE THE USEFULNESS OF CREATING A EUROPEAN CYBERCRIME CENTER)* aims to conduct a study of the advantages and disadvantages of establishing a European cybercrime center, and is strongly tied with actions 30 and 41. We believe that trust and security research projects can only contribute indirectly to the implementation of this action, particularly through research on different attack vectors on national infrastructure, and models of different types of response to attacks.

ACTION 32 (*STRENGTHEN THE FIGHT AGAINST CYBERCRIME AT INTERNATIONAL LEVEL*) is concerned

with enhancing collaboration between EU member states – particularly the authorities – on matters relating to the fight against cybercrime; it also emphasizes the importance of collaboration on an international scale, due to the fact that cyber attacks and threats may originate from anywhere in the world. Collaboration with the US on such matters is also underlined. The description of action 32 also mentions the EU's participation as an observer in the US's cyber preparedness exercise, Cyber Storm III. Clearly, there is much attention on the simulation of real-world cyber attacks and on collaboration with US partners on cybercrime detection and prevention. The organization of joint events/workshops on these matters is also mentioned.

The next three actions are focusing, in different ways, to the protection of children on the internet. Obviously many of the project results listed in the previous chapter can be used to strengthen the security and trust of internet services and therefore make the internet a safer place. However, there were no projects whose outputs are directly relevant the issue of child protection. Only action 37 (mentioned above) has been partly supported by the PRIMELIFE project.

ACTION 36 *(SUPPORT REPORTING OF ILLEGAL CONTENT ONLINE AND AWARENESS CAMPAIGNS ON ONLINE SAFETY FOR CHILDREN)* is intended to help tackle child abuse and related crimes as facilitated by means of the Internet. There are several ways in which the Commission plans to implement action 36, including raising awareness and promoting the idea of a Safer Internet. Part of this includes monitoring and enforcement activities for removing objectionable material (cf. implementing take-down notices online etc.) from websites. Security and trust projects can only contribute indirectly to this agenda point as we noted for agenda point 17.

ACTION 40 (*MEMBER STATES TO IMPLEMENT HARMFUL CONTENT ALERT HOTLINES*) is linked to actions 36 and 37, and is also concerned with protecting children online. It is not focused, however, on preventing child abuse, but on assisting the detection of harmful content online and on providing mechanisms for notifying the authorities when such content is found.

5 INNOVATION GAPS AND INSTRUMENTS

5.1 GAPS TO BE FILLED BY IMPROVED USE OF EXISTING INSTRUMENTS

The first problem that was raised by project coordinators is the lack of perception by IT industries and governments that security is a major issue that can make the difference in the market. As one project coordinator observed “the main issue… is the lack of awareness of the need to protect ICT critical infrastructure” by many critical infrastructure operators, starting from telecom companies.

Also in the realm of privacy the most important problem is the perception of privacy features by operators. When a research result concerns privacy, especially in network monitoring, the actual implementation of privacy protecting measures is always perceived as an extra cost. Therefore it is difficult to convince operators to adopt or even pilot solutions whose goal is to better protect the privacy of the customers.

To this extent the role of governments and public entities could be not only to mandate the usage of privacy features or security protection mechanism in private corporations, but also to adopt the innovative features for their own usage. Public procurement contracts are a significant market and making security and privacy feature mandatory in those contract might tilt the perception of security and privacy as a cost into an added value making the difference in a securing a bid.

Recommendation: use and promote the existing instrument of pre-commercial procurement to create long term pilots supported by public administrations.

Another issue that emerged was the lack of structured and documented relations with product groups within the industry partners. Each projects had a number of industry partners that provided requirements and eventually implemented some solutions. These activities are well described in the deliverables of the project. However, they were carried mostly by the research arm of the company. Most projects pointed out that product groups considered the results of the project, and some projects also set up “experts’ panels” to provide feedback and requirements to the consortium.

Yet, very few projects pointed to a deliverable where a structured relations with product groups “users’ trial”-style is described[5]. **PICOS**, **SECURESCM, and PRIMELIFE** described direct contacts with final end users. **AVANTSSAR**, and partly **AWISSENET**, **PRIMELIFE** and **VIKING**, described (orally) the process of involving product groups within some companies part of the consortium. Indeed it was noted “that was the most challenging part, because these groups were not part of the consortium explicitly. First of all we had to convince them to give us the case studies and to listen to our results”. The process was successful because the contacts were established since the very beginning and was therefore possible to obtain a commitments from product groups.

Obtaining early feedback from the product groups during the lifetime of the projects might actually help to shorten the path from research to innovation.

Recommendation: Push projects to establish a structured and visible relations with products group of the companies within the consortium from the very start. Results of product groups trials should then be reported appropriately in the same way user trials (if any) are reported. Obviously, some results of the pilots would not be public for IPR reasons, but lessons learned should be visible. It is of course difficult for a product group to buy in advance a story line such as "we have this great, vague, idea that in a couple of years will be prototyped!" typically the real discussion starts when you have something to show..." The objective of an early and progressive engagement is to understand the actual needs which might later lead to a prototype that actually addresses some those needs.

[5] Some projects mentioned the exploitation deliverable, but this deliverable usually describes in very generic terms what a partner will possibly do. It does not described whether the research result was actually tried and who participated to the trial.

5.2 New Instruments for Supporting Trials and Pilots

We have already observed in Section.**Error! Reference source not found.** and Section.3 that security and trust research result requires mediation in order to be demonstrated and appreciated. We need to weave the security solution into a "normal" application, or to "adapt" the base system of the final target beneficiaries in order to accommodate the solution. In other words, nobody buys a flexible privacy policy as such. In contrast, people might buy a social network with a flexible privacy policy if it improves one's user experience.

The problem here is that the technological or operational base might not be yet ready to incorporate a new security feature or use a new security model. The main idea might be really interesting, but the technical gaps in the target system requires additional efforts in order to be tried out. For example, accessing a web system with facial biometrics instead of passwords requires a high resolution webcam to be present on the client system. Notice that we are not speaking here of the additional effort needed in order to transform research results into full-fledged products, but of the efforts that is needed to have a full fledged pilot system.

This additional effort cannot usually done within the timeframe and the resources of the research project for two reasons. At first, this gap is not interesting from the viewpoint of research or technological development (it won't increase the project rating by the reviewers, or the research standing of the academics participating to the project) and, second and foremost, it requires significant efforts for the integration at operational level that needs to be done ***after*** the research results have been completed and validated.

As summarized by a project coordinator, "there is never enough time for users' trials."

Occasionally some projects "continue" the work of a previous research project with a strand dedicated to more detailed experiments in a new research project (for example the informal follow-ups **PRIME**, **PRIMELIFE**, **ABC4TRUST** sequence of projects). However this line of action is sub-optimal from the view point of innovation. At first they are "new" projects and thus subject to all hurdles in the competition as if they were never reviewed before, second and foremost being "research" projects they need to come out with new research results were the majority of effort needs to go.

Recommendation: Introduce a specific financial instrument where (a subset of) the consortium could go ahead with a simplified procedure for project whose only focus is a medium or large scale user-trial with a focus on commercialization.

This could still be a competitive call available to all concluded or near completion projects but, considering the narrower focus (user trial) and the obligatory starting point (a result from a research project), could be simplified along the calls for international cooperation or enlargement to partners from new member states.

5.3 A New Regulatory Initiative Alike Safety Initiatives in Avionics

All project coordinators agreed that a major problem in the innovation path is the secretive approach to disclosure of security problems in industry. The lack of information significantly hampers the generality of the research results. Without data it is difficult to evaluate whether a research result it is actually able to make in difference in reality.

For example the management value of security metrics still needs to be proved, in spite of the significant research results for visualization and business intelligence. However, for research results to be valuable, one needs to validate the proposed metrics across a variety of companies. If we compare security metrics to thermometers and companies to patients, then the current status of practice would be that each company has its own thermometer and tests it only on itself.

Also in the case of critical infrastructures, all projects coordinators noted the unavailability of operators to disclose and to share information about their infrastructure, about any attacks happening against their network. This was also true for telecom operators. The default answer was often "Our network is intrinsically secure, we don't need any research product to increase the security protection of our infrastructure". Obviously, this is far from true.

The need for mechanisms for disclosure also become relevant if **ACTION 30 (*ESTABLISH A EUROPEAN CYBERCRIME PLATFORM*)** and **ACTION 41 (*MEMBER STATES TO SET UP NATIONAL ALERT PLATFORMS*)** are to be concretely achieved. As we have described in the previous section, those actions advocate the set up of information platforms on security and privacy threats: the actual availability of the information is therefore a key condition.

Such reticence across industries is clearly not due to the need of protecting the infrastructure. Disclosing statistics or research level information on vulnerabilities or attacks present on the infrastructure does not allow attackers to replicate an attack or exploit a vulnerability. A huge amount of low level and operational information needs to be disclosed in order for an exploit to be possible. Here is an example on open source software: several hundreds of vulnerabilities of Mozilla Firefox across 5 main versions and 6 years have been reported, but only around 30 are actually exploited.

Beside the pride in one's own orchard, this phenomenon can be rather attributed to the risk of liabilities and reputation losses if the presence of security problems is admitted. As a project coordinator observed "Every incident that gets public may damage the reputation of the company. […] From an economic point of view, a company will not disclose its incidents if they don't have to." The results is an eco-system in which, worse than in the fable on the emperor's new clothes, everybody goes naked but nobody what to say it first. Most project coordinator noted that this could only be solved by regulatory initiatives, and we agree.

The effect that non-disclosure of security breaches can have on the overall ecosystem and its citizens has become apparent with the DigiNotar security breach[6]:

The DigiNotar firm was a consulting firm that provided certificates to the Dutch Government websites. It was hacked (allegedly by the Iranians) and a number of root keys has been stolen. It has become apparent from subsequent investigations that the registrar knew that they have been hacked and that their certificates could therefore be falsified. However, they have not done anything about it. The breach was discovered only after Iranian citizens reported to Google that Google Chrome would block an invalid Google Certificate issued by DigiNotar. The certificate was clearly used to spy on Gmails accounts on Iranian citizens. Notice that in the meantime the Dutch government believed to provide security to its citizens while using in reality a certificate authority that was no longer secure. When the scandals erupted to the public, the Dutch government was forced to put down a notice that its web site where no longer secure[7].

The story of DigiNotar is a perfect example of "rational" behavior of an individual well described in economic theories for selfish agents maximizing utility. In absence of legal obligations (i.e. serious fines or penalties for lack of disclosure of security breaches) why should have the registrar notified the authorities that they had a problem? With a better luck, they could have silently waited for the next browser update to change their certificate…

Recommendation: A European-wide regulatory initiative is necessary to mandate the controlled disclosure of security incidents in the same fashion of what happens for safety in avionics.

[6] See http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf

[7] See http://news.cnet.com/8301-27080_3-20098894-245/fraudulent-google-certificate-points-to-internet-attack/

6 CONCLUSIONS

This document reported the results of a comprehensive study on the innovation potential of FP7 projects funded by the ICT Call 1 for Trustworthy ICT and Joint ICT and Security Call.

The analysis of the constituency revealed a dynamic, collaborative environment (i.e. a scale-free network such as the web) with few major players, but without a clear market dominance. A variety of companies representing the software industry, the telecommunication sector, and proper security services participate to the research projects.

The collaborative structure of the community shows that ***general software producers and integrators act as hubs*** between different interests groups (such as companies and universities interested in privacy or in critical infrastructure protection), while Telecom operators have a minor role. New ***specialized IT security companies are emerging actors*** but still play a limited role due to their SME status. This is also an indicator that the market is young and full of potential.

The study of the innovation potential identified many research results which can stimulate product, service and process innovation in Europe. Some projects have clear ***innovative results that are usable by citizens*** (in the realms of biometrics and privacy) **and IT industries** (for example in the realm of security and compliance of infrastructures). Many projects also delivered ***important potential innovations in tools and methods for ICT specialists*** (from consultants on IT governance to IT administrators). These results have the potential to be used well beyond the consortium that produced them, albeit the path to commercial product might be fraught with difficulties.

A weakness of the field, with few notable exceptions, is the ***lack of well reported empirical trials*** and pilots. Indeed, the results of well designed pilots could provide crucial information to potential investors in the technology, and thus act as a spur to innovation.

The FP7 Security and Trust projects also **contributed to the *achievement of the objectives of the Digital Agenda***, in particular on those focusing on instruments for self-regulation and for improving privacy and security of infrastructures and services such as Action 35 (Guidance on implementation of Telecoms rules on privacy).

Two major issues in the Digital agenda are only addressed partially and indirectly by the projects and namely the actions referring to ***cyber-security and -preparedness*** to counter cyber-crime and cyber- attacks and those referring to ***children protection on the internet are only indirectly covered*** *or not at all.* Initiatives such as Joint Calls might be the options to pursue in these sectors.

The analysis also identified gaps in the “last mile” that could be addressed by a mixture of organizational, funding, and regulatory measures. Many project coordinators stressed the importance of setting up structured relations with product groups or users from the project’s start. However, to cover the distance from a research result to a product, it was felt that more work was necessary **after** the research results have been achieved. A possible solution could be a specific ***co-funding mechanism by the EC for experimenting large scale follow-up trials*** of research results with a simplified funding procedure.

A key weaknesses of the field of security technology at large emerged from the investigation: ***the lack of information on security incidents and benchmarks***. Without information on past incidents it is not possible to learn from them as a community. In avionics safety accidents are thoroughly investigated and the recommendations become new industry requirements or prescribed operational procedures. Security is still very far from this level of knowledge sharing. This can only be achieved by an ***European regulatory initiative on the controlled disclosure of security incidents***.

Adopting these measures might ensure that ICT progress is rapidly transformed into benefits for Europe's citizens, businesses, industry and governments.

6.1 ACKNOWLEDGEMENTS

We would like to thank the Head, the current and past Project Officers of the F5 Unit, and the project and technical coordinators of the FP7 security and trust projects for providing us the necessary bootstrapping information. Without their guide and their support this report would not have been feasible.

At the University of Trento F. Dalpiaz, O. Gadyaskaia, G. Oligeri, and F. Paci contributed to the analysis of project deliverables. From the EFFECTS+ consortium the suggestions from M. Bezzi, F. Clearly and N. Wainright were extremely helpful.

7 APPENDICES

7.1 DISTRIBUTION OF PROJECT PARTNERS BY TYPE

Table 3 - Distribution of Partners per Type -

	Research Centers	University	Other	Industry
ACTIBIO	3	3		5
AVANTSSAR	2	6		4
AWISSENET	1	3		4
CACE	1	8		3
CONSEQUENCE	3	1	1	2
ECRYPT II	1	8		2
GEMOM	2	1	1	6
INSPIRE	2	1		5
INTERSECTION	3	2		6
MASTER	1	4	2	8
MICIE	5	3		3
MOBIO	2	5		1
PICOS	1	5		4
PRIMELIFE	4	8		3
PRISM	5			3
SECURE SCM	1	4	1	1
SERSCIS	1	1		4
SHIELDS	3	1	2	2
SWIFT	1	2	1	5
TAS 3	1	9		7
TECOM		1		9
TURBINE		3		6
UAN	2	1	1	2
VIKING		3		4
WOMBAT	2	3	1	4
WSAN4CIP	2	3	2	5
Total	**49**	**89**	**12**	**108**

7.2 CONTRIBUTION TO THE DIGITAL AGENDA BY PROJECT

Table 4 - Top-Down Classification for the contribution to the Digital Agenda -

Project name	Matching Criteria	Justification
ACTIBIO	[CRIT 4], [CRIT 9]	ACTIBIO deals with threats and attacks on biometric systems.
MASTER	[CRIT 6], [CRIT 9]	MASTER deals with compliance aspects and possibilities of different types of cyberattack.
MICIE	[CRIT 5], [CRIT 8]	MICIE involves simulations of different attacks.
PICOS	[CRIT 9]	PICOS covers a wide range of privacy issues.
PRIMELIFE	[CRIT 9]	PRIMELIFE covers a wide range of privacy

Project name	Matching Criteria	Justification
		issues.
PRISM	[CRIT 9]	PRISM covers a wide range of privacy issues.
SHIELDS	[CRIT 4]	SHIELDS involves testing infrastructure and finding vulnerabilities and flaws.
SWIFT	[CRIT 2], [CRIT 9]	SWIFT covers a number of privacy issues and user concerns.
TAS3	[CRIT 6], [CRIT 7]	The techniques proposed in TAS3 are directly relevant for the cyberpreparedness.
TURBINE	[CRIT 2], [CRIT 9]	TURBINE handles important privacy concerns.
VIKING	[CRIT 3], [CRIT 5], [CRIT 8], [CRIT 6], [CRIT 7]	VIKING, due to its multi-disciplinary nature covers a wide range of issues relevant to cyberpreparedness and the prevention of attacks.
WOMBAT	[CRIT 4], [CRIT 12]	WOMBAT does deal with cyberattack prevention and so matches these criteria.

Table 5 - Contribution to the Digital Agenda identified by Project Coordinators -

Project name	Digital Agenda from P.C.	Justification from P.C.
ACTIBIO	Actions 30, 35, 41, 54	Novel dynamic, multimodal and activity related biometrics everywhere. [Actions 30, 35, 41]. Secure access to Always-On infrastructures and services. [Action 54]
AVANTSSAR	Actions 28, 29, 32, 34, 54	In terms of policy and regulation, government could require that services and protocols are certified and validated before being deployed. Using the Avant-platform, vulnerability could be identify as soon as possible and it's possible to prevent a lot of mistakes.
AWISSENET	Actions 17, 28, 30, 54	The focus of the project is in the area of Trust and Privacy in wireless sensor networks so this can be part of security plan.
CACE	Actions 17, 28, 32, 33, 35, 54	
CONSEQUENCE	Actions 17, 28, 29, 35, 54	Whenever data-sharing agreements rise, it could be a regulation like data privacy policy. The framework that can be used is a referent framework to implement assumptions. Specific policies that are present in the project related to data centric framework are very usable.
ECRYPT II	Actions 30, 33	Several countries in Europe have already cryptographic guidelines, used by governments and users, but there are a lot of small countries where this gap is present and it's more difficult for government to make recommendations. The publication of documents and the consent of the academic and researchers, coming from the ECRYPT II II project, try to involved industry experts and help individual users in Europe. The second element that the project can support is in the area of privacy, with the development of cryptographic techniques that keep the data, the control of users, make profiles. That cryptography determines a minimal disclosure of information and create applications to share data without revealing details, with high privacy and data remains under the control of minimal techniques.
GEMOM	Actions 29, 33, 34, 54	Many current critical applications and services suffer from poor resilience, adaptability (to the security situation and the context), and scalability. The results and experiences of GEMOM can be used to pave the road towards offering advances in these issues. GEMOM shows a measurable step in enhancing the mentioned issues. European policy and regulation should recognize the potential of GEMOM technology and methodologies. GEMOM has shown the potential of integrating (resilience, security and context) to complex communication systems. The advantages to

Project name	Digital Agenda from P.C.	Justification from P.C.
		European industries, end-users and governments are obvious.
INSPIRE	Actions 28, 33	It can contribute to the activities performed by the ENISA, European Network and Information Security Agency, which is in charge of investigating in security issues and supporting the European Commission in identifying strategies to be adopted for policy definitions and research supports. INSPIRE contributes to the activities by participating in the working groups on SCADA security, on network security, by informing ENISA about the INSPIRE results and the technique and technologies used in INSPIRE project to make critical infrastructure more secure and more reliable and more resilient. The Consortium has also contacted the Policy Office of the European Commission and it is still in touch with it.
INTERSECTION	Actions 28, 29	During the project INTERSECTION was in touch with the European Policy Office of Network Information Security (NIS), because it was responsible for policy definitions based on European initiative on critical information infrastructure protection, just for an exchange of information and documents. One of the result of INTERSECTION project was the definition of a roadmap of best practices for the protection of network system and communication network to guide Telecom operators in the adoption of security strategies, for ensuring security in transmission of data over that communication infrastructure.
MASTER	Actions 32, 35, 37	The MASTER compliance management framework can aid to assess and ensure compliance to potential regulations/policies that might be enacted to protect from cybercrime at organizations and critical infrastructures. [Action 32] Action 35 is clearly a target for the MASTER applicability. The risk of incorrect implementation of regulations and provisions can be mitigated and controlled using the compliance management framework of the MASTER. The MASTER might be proposed as the methodology on how to implement those rules, using the MASTER methodology and the MASTER tools for deploying specific IT policies derived from the "rules on privacy". [Action 35] The MASTER could be introduced as one suitable method and toolset to use within those self-regulated organizations to ensure compliance to the regulations relating to protection of minors. [Action 37]
MICIE	Actions 28, 33	The production of specific tools (MICIE is one of these) has already received the interest of governmental authorities, aware that the adoption of tools enabling business decision will enable in medium term the continuous improvement of crisis management at national level, or in the specific case at national across borders Implementing, as in MICIE, a Policy Based Management Architecture. The CI operators can define policies that will address the relations among CIs, including defining how each particular CI can connect and data access policies. The uses of Policies support writing, verification and deployment of security policies related to the information exchanged by different CI. The CI Operators define policies using a policy specification language and/or using a graphical user interface (GUI). The policies are represented in a formal way using a policy specification language.
PICOS	Actions 35, 36, 37	
PRIMELIFE	Actions 28, 35, 54	If we consider privacy as part of security, **PRIMELIFE** is contributing for the development of a new generation of web-based applications and services, that might apply because privacy remove trust and security barriers. In addition to that, the generation of more private investment for ICT research establishes an increase of trust that can bring more information

Project name	Digital Agenda from P.C.	Justification from P.C.
		and be a potential to enlarge the scale of pilots.
PRISM	Action 35	The project is specifically in the field linked to the implementation of Telecoms rules on privacy because the basic work was on privacy issues for telecom operators, especially for network monitoring parts.
SHIELDS	Actions 17, 29, 30, 33, 34, 40, 54	**SHIELDS** set up a certification programme for security software that is compatible with the **SHIELDS** services and for software that has been analysed with SHIELDS compatible software. [Action 17]. **SHIELDS** was not targeting changes in legislation, but provided new tools and technology to harden information systems against cyber attacks. [Action 29]. **SHIELDS** has created a set of tools for security testing ICT infrastructure, but an even stronger focus has been to give developers a security focus from day one of the development. In order to strengthen the infrastructure the software must be made more resilient than what is the case today. [Action 33]. **SHIELDS** has created a service that is able to record vulnerability instances found in **SHIELDS** compatible security tools. This information can be used to create statistics on current threats, and a subscription/notification service provides information about new threats and vulnerabilities, as well as mitigating security activities that can be performed. [Action 34] Security tools from the **SHIELDS** project can be used to detect attack trends and ways of exploiting online software and services. Notifications can be used to inform the service owners as well as authorities. The most important contribution is nevertheless support for creating secure software so that it cannot be so easily exploited by malicious users (e.g. someone who want to capture your server to spread harmful content such as child pornography or viruses). [Action 40]. The **SHIELDS** Security Vulnerability Repository Service (SVRS) is an online and Web-based service that enables security tools to interface it through standardized interfaces. These tools can then benefit from new security information that enables them to find new vulnerabilities and prevent them both before and after deployment. The SVSR has two types of Web-interfaces, one for humans (HTML) and the other for software tools (machine interface based on REST). [Action 54]
SWIFT	Actions 17, 28, 35, 37, 54	**SWIFT** is very oriented for privacy and for looking for those regulatory issues and their support. Building a new policy is not the aim of the project, so SWIFT did not have a legal component. Although it was done in the state of the art an analysis to make sure that all the technology did not negatively conflict with the regulation.
TAS3	Actions 28, 37, 54	In view of the new EU directive the project has therefore participated in the SIMS proposal to develop a European Trust Observatory (ETO), which will aim towards the development of trust compliance policies and procedures for Service Providers. A lot of this will not be manifest in technical protocols. For example audit requirements, claims and damages procedures, back-up requirements, personnel vetting procedures etc. will all be at the policy and procedure level. Such “policy and procedure specifications" need to be observable and auditable by the proposed new profession of Trust Auditor. Together these will deliver the information to certify and build trustworthiness into the systems, services and their providers. In its last year TAS3 will contribute to the preparation of such an ETO.

Project name	Digital Agenda from P.C.	Justification from P.C.
TECOM	Actions 28, 29, 30, 35	Results allow trusted building blocks which can act as a platform for enhanced or reinforced security policy but they do not reinforce policy by itself. [Action 28]. The TECOM project combat cyber attacks against information systems especially against embedded information and communication modules. [Action 29]. Results will generate new trust, security and safety relevant products which will be bought through private investments. [Action 30]. Results will be further used for developing new or enhanced ICT products and work will continue as standardization work at the trusted computing group (TCG). The TECOM results will allow extended privacy rules , eg. the results are used for extende privacy in smartGrids. [Action 35]
TURBINE	Actions 28, 54	There is an expectation from the civil society to have more trusted identity, to protect the identity and to be able to demonstrate that the identity is reliable. This project is done to demonstrate that the identity protects your personal data, without expose too much information which have a private character and this can answer very well to the expectations of the European directive.
VIKING	Actions 29, 33, 39	The purpose of VIKING is to investigate vulnerabilities to propose mitigation of control system for critical infrastructures. This is to combat cyber attacks. [Action 29]. One of the objectives of VIKING is to increase awareness of the danger from cyber attacks. The purpose of this is to support preparedness against cyber attacks on critical infrastructures. [Action 33]This is not a direct objective of VIKING but tools developed in VIKING can definitely be used for cyber attack simulations and impact analysis. [Action 39]
WSAN4CIP	Actions 28, 29, 32, 33	

7.3 RESEARCH RESULTS AND PILOTS BY PROJECT

Table 6 - Research Results -

Project name	Interviewed	Technical Results	Pilot and Case Studies
ACTIBIO	DIMITRIOS TZOVARAS	W.P.5.	W.P.7.
AVANTSSAR	VIGANO' LUCA	FINAL PROJECT REPORT W.P.2. for languages W.P.3. for the different models techniques that are presented W.P.4. for platforms	W.P.5.
AWISSENET	ZAHARIAD THEODORE	D.2.3., D.4.1., D.6.4. and D.6.5.	D.6.2.
CACE	AHMAD REZA SADEGHI	D.2.3. and D.2.5., D.4.7.	D.5.3., D.5.4. and D.5.5.
CONSEQUENCE	MARTINELLI FABIO	D.1.3. and W.P. of dissemination and exploitation	D.2.1., D.3.1. and D.4.1.
ECRYPT II	BART PRENEEL		
GEMOM	SAVOLA REIJO	W.P.6.	D.6.5.
INSPIRE	SALVATORE D'ANTONIO	W.P.2. and W.P.3. D.2.3. for the security assessment	D.5.2 and D.5.3

Project name	Interviewed	Technical Results	Pilot and Case Studies
		framework D.3.4 for the online automated INSPIRE security framework	
INTERSECTION	SALVATORE D'ANTONIO	W.P.2. and W.P.3.	W.P.6. and D.6.1, D.6.2 and D.6.3
MASTER	PEDRO SORIA-RODRIGUEZ	Activity 2 Activity 3	W.P.1.3
MICIE	CAPODIECI PAOLO	W.P.6.	W.P.6.
MOBIO	SEBASTIEN MARCEL	W.P.2.	W.P.6.
PICOS	KAI RANNENBERG	W.P.2. requirements W.P.4. architecture W.P.6. client implementation	W.P.7.
PRIMELIFE	DIETER SOMMER	Identity Mix D.2.4.1. and D.3.3.2 D.4.3.4 and D.6.3.1 for policy language D.1.2.2. and D.1.3.3. for privacy	D.1.1.3., D.4.1.5 and D.4.1.6.
PRISM	GIUSEPPE BIANCHI	W.P.3.1, W.P.3.2 for data protection mechanism and traffic analysis techniques W.P.4.1 for probe technologies and the actual implementation of the data protection and traffic analysis mechanisms W.P. 4.2. for access control W.P.1.2 for achievements regarding standardization	W.P.4.3.
SECURESCM	FLORIAN KERSCHBAUM	D.2., and W.P.8., W.P.1., and W.P.6.	W.P.5. and W.P.6. D.6.2. for the logistic use case D.5.2. for the aerospace scenario
SERSCIS	MIKE SURRIDGE		
SHIELDS	PER HAKON MELAND	D.1.4.	D.5.1, D.5.2. and D.5.3
SWIFT	JOAO GIRAO	W.P.2. for architectural part W.P.3. for security part W.P.2. summary of results	W.P.5.
TAS3	SEGURAN MAGALI	W.P.2. for architectural part	W.P.9.

Project name	Interviewed	Technical Results	Pilot and Case Studies
		W.P.7. for security, authorization, policy and aggregation infrastructure	
TECOM	HANS BRANDL	D1.1. and D.1.2. for trusted and secure processor as integratable package for easily building trusted embedded hardware D.2.1. and D.2.5. for trusted operating systems	D.5.1.
TURBINE	NICOLAS DELVEUX	D.4.1., D.4.2., D.4.3. and D.6.	D.5.2.1. and D.5.2.2.
UAN	ANTONIO SORIA	D.6.3.	D.2.1.
VIKING	GUNNAR BJORKMAN	W.P.3. for model based on tool W.P.4. for mitigation W.P.4. for the secure communication structures	W.P.5.
WSAN4CIP	PETER LANGENDORFER	W.P.2. and W.P.3.	W.P.5. and W.P.7.

7.4 INDEX OF FIGURES

7.5 INDEX OF TABLES

7.6 INDEX OF PROJECTS