PROJECT FINAL REPORT

Grant Agreement number: ICT-248410

Project acronym: TERESA

Project title: Trusted Computing Engineering for Resource Constrained Embedded Systems Applications

Funding Scheme: Collaborative Projects

Period covered: from 1 November 2010 **to** 31 January 2013

Name of the scientific representative of the project's co-ordinator[1], Title and Organisation: Antonio Kung, Director, TRIALOG SA

Tel: +33 1 44 70 61 00

Fax: +33 1 44 70 05 91

E-mail:antonio.kung@trialog.com

Project website: http://www.teresa-project.org

[1] Usually the contact person of the coordinator as specified in Art. 8.1. of the Grant Agreement.

4.1 Final Publishable Summary Report

Executive Summary

Resource Constrained Embedded Systems (RCES) are systems for Information and Communication Technology (ICT) that are integrated into a wide variety of applications, such as automotive and railway electronics, appliances, sensors, building control systems, and smart meters. They often have also stringent cost constraints in some domains as in the automotive one. They are often integrated into critical applications (e.g. a car breaking system) which may require strict certification.

RCES must increasingly integrate additional features for Security and Dependability (S&D), such as a secure communication mechanism due to the growing up of the communication capabilities. The development of such features requires specialised expertise and skills, but the cost of designing them can be a major item in the overall cost of developing the system. TERESA's key innovation is an approach that supports the re-use of previously developed S&D features without having to re-engineer them.

The TERESA approach supports the independent development of S&D solutions (Patterns) for subsequent integration into an overall RCES design. S&D engineers can specify patterns that capture specialized solutions and store those in a shared repository using the TERESA toolset. The RCES engineers can then reuse and integrate these S&D patterns during their applications design. This is supported by a set of dedicated tools which allow for adaptation of the generic S&D solution to the specific technology platform and engineering process, corresponding to their application domain. Two sets of tools were developed. The first allows S&D experts to design an S&D subsystem and store it in a repository of patterns to be reused. The second tool allows developers of RCES in a specific application sector to reuse the S&D pattern during their application design process

TERESA has specified a Pattern Based System Engineering (PBSE) methodology based on Model Driven Engineering (MDE). A set of languages was developed for the specification the repository structure and content, consisting of S&D patterns, S&D properties and processes. The use of formal validation based on the Security Modelling Framework SeMF was also integrated into the methodology; it guarantees that the pattern correctly provides its properties.

Two applications use cases were developed: 1) a railway use case integrating a redundant architecture and voting capability to monitor distance and speed of the train, and 2) a smart grid use case integrating a smart meter gateway conforming to the common criteria protection profile defined by the BSI in Germany.

TERESA’s general benefit is the assurance that critical Information and Communication Technologies (ICT) infrastructures including RCES will be based on sound and cost-effective engineering approaches.

TERESA’s contribution will allow the industry to increase competiveness by applying cost and time effective reuse approaches.

TERESA now provides opportunities to industry partners to enhance and market the repository access tools developed during the project, and to provide consulting services to develop and reuse components. It also provides a sound basis for academic partners to create an engineering methodology based on the results of TERESA, and to provide a broader education in the RCES domain to the students.

TERESA started on November 2009 and ended in January 2013. It involved the following partners: Trialog (coordinator), IK4-Ikerlan, Fraunhofer SIT, USiegen, escrypt, and IRIT.

4.2 Description of Project Context and Objectives

Context

Resource Constrained Embedded Systems (RCES) are today integrated in increasingly more sophisticated applications. They require more security and dependability and they require more trust. This complexity is due to integration and functional considerations. Firstly, RCES are integrated into systems involving complex supply chains with many different business stakeholders focusing on different subsystems (e.g. processors, ASIC, operating systems, middleware, and application components) and different integration levels. Secondly, RCES are often used in multipurpose applications involving multiple and possibly independent applications. There is a switch from simpler value chains/ecosystems to fairly complex ones, where it is needed to define specific measures to protect individual computing assets.

Resource Constrained Embedded systems (RCES) are characterised as follows:

- They can be found everywhere, in different application sectors (automotive, aerospace, home, etc.), in different form factors (standalone systems, peripheral subsystems to a main computing system, etc.), in many different devices (sensors, automotive electronic control units, intelligent switches, home appliances e.g. washing machine drum control, meters, etc.)
- Computing resources, e.g. memory, tasks and buffers, are statically determined. For instance, the entities managed by the underlying operating systems are typically predetermined. Another example is the OSEK-VDX RTOS (www.osek-vdx.org) standard which defines tasks, resources, alarms entities. These entities are identified statically at design time (e.g. 3 tasks, 4 resources, 2 alarms would make up a given system).
- Most RCES are high integrity systems, or systems which must meet assurance requirements. Depending on application requirements, different levels of assurance can be involved from the most stringent which involve certification (e.g. DO178, IEC-61508 for safety-relevant embedded systems development), to lighter levels of assurance (e.g. industry practices). As a matter of fact, many RCES involve very significant software development costs and therefore use advanced engineering disciplines (automatic code generation, model-driven developments).

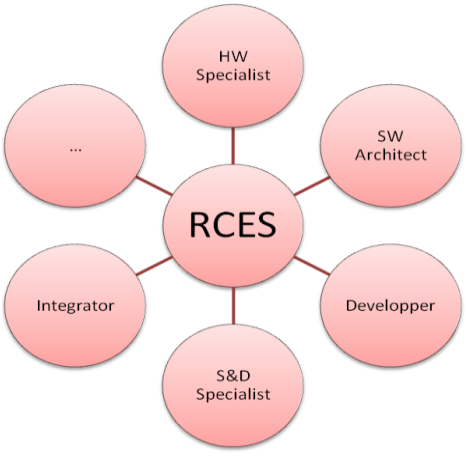

Figure 1 **: RCES as a synergy of business**

The TERESA target market covers all expertise and engineering services associated with the development, validation of S&D subsystems and their integration in inRCES systems. The value proposition is to use MDE engineering and tools to design, develop and validate S&D patterns, and to follow a domain specific engineering process to integrate the pattern..

A TERESA market potential is identified in three different types of segments. A first market potential exists for the segment of tools development (creating repository and customising access tool, maintenance and support). A second market potential exists at the level of S&D pattern developments (development, maintenance and support to integrate into the main development process). Finally a third market potential exists at the level of application domains for the deployment of S&D pattenrs. Five application domains were addressed in the project: smart metering, automotive, home control, industry control and railways.

Objectives

The goal of TERESA is to define, demonstrate and validate a cost-effective engineering discipline for trust that is adapted to resource constrained embedded systems. Trust is defined as the degree with which security and dependability requirements are met.

The TERESA approach is to use a model-based repository of Security and Dependability (S&D) patterns:

- Security and dependability platform independent patterns are identified and defined for each application sector (some patterns could be used by several application sectors).
- Formal properties on security and dependability are defined and validated for patterns.
- Platform dependent implementations of the patterns are guided with very precise requirements.

TERESA has the following objectives:

- **O1:** Support for S&D pattern reuse in a railways sector use case.
- **O2:** Support for S&D pattern reuse in a metering use case.
- **O3:** Ensuring the genericity of TERESA approach by providing guidelines for the specification of sector specific RCES trusted computing engineering. Software process engineers in a given sector, e.g. automotive, will use the guidelines to define a trusted computing engineering process that is integrated to the software engineering process used in the sector.

(C) Main S&T Results/Foreground

This section explains the results achieved by the project. The results are presented as follows:

- The TERESA theoretical contribution to engineering (methodology, language, formal validation)
- Demonstration in specific application domains (case studies, demonstrator and genericity of approach)
- Supporting toolset (tools for the approach)
- Example patterns

A PBSE Theoretical Foundation

A Pattern Based System Engineering (PBSE) methodology based on a repository was specified. This engineering methodology fully takes into account the need for separation of roles by defining three distinct processes, the pattern modelling process, the repository specification process, and the pattern integration process. A set of languages was specified for the repository structure and content. The latter consists of specifications of patterns, S&D properties and processes.

The use of formal validation in the process was successfully carried out. The formal validation is based on the SeMF framework. A validation methodology was defined to ensure that S&D patterns provide the expected properties with respect to their interfaces. The methodology was applied on a number of example patterns. Guidelines derived from the validation results defined how to help integrating any pattern in a system.

Application Domain Examples

Requirements for the project (engineering viewpoint, process viewpoint and repository viewpoint) were defined by studying use cases in four application domains corresponding to a partner's expertise, and S&D patterns of interest were identified.

Two case studies were studied in depth: Safe4Rail and a secure gateway for smart metering:

- The railways domain demonstrator (Safe4Rail) was developed to validate the TERESA. This domain involves strong constraints with well-defined and mature engineering processes.
- The metering domain demonstrator was developed to validate the TERESA approach in domains where new engineering approaches need to be established. This domain is increasingly prominent, but without the long history of the railway sector.

Implementations were done in two versions. These demonstrators showed that TERESA objectives O1 and O2 were reached.

A study was carried out in the automotive domain to assess the ease with which the TERESA approach could be adapted to the toolset provided by the automotive tool provider company ETAS. This study validated the genericity of TERESA (objective O3).

An evaluation study was carried out, consisting of presentations to stakeholders and of analysis of Key Performance Indicators (KPIs). They confirmed the potential of the TERESA approach, and the rising interest for Model Driven Engineering (MDE) and pattern based engineering.

TERESA MDE Tool Chain

TERESA has produced a model driven engineering (MDE) tool chain. The following tools targeted to the S&D developer, i.e. the engineer who creates S&D patterns, were developed:

- **Gaya**: a repository based on MDE technology was developed. This repository allows for the storage of engineering and process knowledge associated with S&D patterns.
- **Arabion:** a tool for the creation and edition of S&D patterns. Such patterns must be stored in such a way that they can be reused later, enhanced and modified.
- **Tiqueo:**a tool for the creation and edition of S&D properties and constraints. The focus is on the non-functional requirements that are associated with S&D patterns

The following tool targeted to the S&D integrator, i.e. the engineer who uses S&D patterns, were developed:

- **Naravas:** a tool for the design of repository-centric engineering processes targeting RCES applications. Engineering processes are often domain specific (i.e. they could be based on different standards) and stakeholder specific (i.e. specific corporate processes)
- **Access tools for railway domain.** The tool transforms the Gaya representation of S&D patterns into a representation that is consistent with the Safe4Rail set of tools (mostly Rhapsody[2]-based) and the Safe4Rail process.
- **Access tools for metrology domain.** The tool transforms the Gaya representation of S&D patterns into a representation that is consistent with the associated set of tools (mostly Rhapsody-based) used in the railways use case.

The following contributions on engineering processes were made:

- an example railways process based on the Safe4Rail use case
- an example metering process based on the Secure gateway protection profile
- a study of feasibility in an automotive process based on the ETAS toolset
- guidelines on how to use common engineering metamodels.

Examples Patterns

In order to demonstrate and validate the TERESA approach for S&D reuse-based on patterns, the project has contributed to the specification of pattern information (or artefacts) to be stored in the TERESA repository. The flexibility of the repository comes from the possibility to have different levels of representations, depending on 1) the application domain supported, and 2) the engineering process phase supported. Overall, **59 S&D patterns were developed**, consisting of 20 system level patterns, 25 architecture level patterns, and 14 design level patterns.

Forty-one patterns were developed and used while working on the railways and metrology use cases. The 18 remaining patterns were added to the repository for generic or training purposes.

The table below presents the 41 used patterns. A pattern is based on the name of the solution and the phase in the process where it is available. Some have only a domain-specific version (mostly for metrology), but others are also described in a domain independent version.

[2] Rhapsody is an engineering tool from IBM

Pattern (composed of a name and a development lifecycle stage)		Domain Supported	Security / Dependability
SafetyCommLayer	System Concept	Domain Independent	Dependability
	System Architecture		
	Software Architecture		
	Module Detailed Design		
	System Concept	Railway Domain	
	System Architecture		
	Software Architecture		
	Module Detailed Design		
Hypervisor	System Concept	Domain Independent	Dependability
	System Architecture	Railway Domain	
Majority Voter	System Concept	Domain Independent	Dependability
	System Architecture		
	Software Architecture	Railway Domain	
	Module Detailed Design		
Reciprocal Monitoring	Software Architecture	Domain Independent	Dependability
	Software Architecture	Railway Domain	
	Module Detailed Design		
TMR	System Concept	Domain Independent	Dependability
	System Architecture		
	System Concept	Railway Domain	
	System Architecture		
Security Comm Layer	System Concept	Domain Independent	Security
	System Architecture		
	System Architecture	Railway Domain	
	Software Architecture		
	Module Detailed Design		
Watchdog	System Architecture	Domain Independent	Dependability
	Software Architecture		
	System Architecture	Railway Domain	
Data Agreement	System Concept	Railway Domain	Dependability
	System Architecture		
	Software Architecture		
	Module Detailed Design		
Secure Remote Readout	Detailed Design	Metrology Domain	Security
	Implementation		
Wakeup Service	Detailed Design	Metrology Domain	Security
Secure Communication	Detailed Design	Metrology Domain	Security
Secure Logger	Detailed Design	Metrology Domain	Security
Key Manager	Detailed Design	Metrology Domain	Security
RNG Test	Unit Test	Metrology Domain	Security
Smart Meter Gateway Skeleton	Architecture Design	Metrology Domain	Security

(D) Potential Impact

This section describes the potential impact of TERESA by elaborating on how the project results contribute to a number of outcomes which were described in the FP7 work programme, and by explaining the impact of such outcomes, directly and indirectly. The resulting analysis approach is summarised by the figure below.

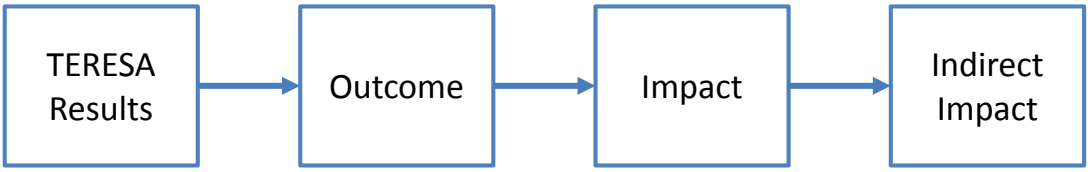

Figure 2 : Impact Analysis Approach

Results

As explained in the previous section, TERESA results are the following:

- **R1**: a theoretical PBSE engineering foundation based on a repository-centric methodology and integrating a formal validation approach based on SeMF
- **R2**: two example use cases, one on railways and one on secure gateways for smart metering and guidelines for supporting other engineering processes,
- **R3**: an initial tool set for pattern editing, and supporting access tools for the two example use cases,
- **R4**: a strong collection of 59 S&D example patterns.

Outcomes

TERESA results contribute to the following outcomes:

- **O1:** The results of TERESA (R1, R2, R3, R4) contribute to the *theory and novel methods for embedded system design.* This is consistent with the description of ICT-2009.3.4 target outcome in the work programme:

> ***Theory and novel methods for embedded system design*** *New methods and tools that can increase system development productivity while achieving dependable, safe and secure embedded systems with predictable properties. Key issues encompass heterogeneity, i.e. building embedded systems from components with different characteristics; predictability of non-functional properties such as performance, fault tolerance, life expectancy and power consumption; comprehensive methods for robustness validation; adaptivity and self-awareness for coping with uncertainty, upgrades of components and self-configuration concepts; and, where appropriate, unification of approaches from computer science, electronic engineering and control.*

  TERESA contributes to embedded systems designs in the area of trusted computing for resource constrained embedded systems (RCES).It contributes theory and novel methods based on a repository of models and patterns which 1) ensure engineering separation of concern, and 2) support the domain specific process. It addresses the key issue: the predictability of non-functional properties (security and dependability).

- **O2:** The results of TERESA (R3) contribute to *integrated design environment that can be extended and customised.* This is consistent with the description of ICT-2009.3.4 target outcome in the work programme:

An integrated design environment for embedded systems that can be extended and customised. *This covers software, hardware/software and system design tools for holistic design, from applications down to component and platform level. Important challenges encompass flexibility of the platform to support different applications, increased interoperability of tools primarily from SME vendors and openness in order to facilitate the entry of new industry players, support associated standardisation, easily import existing components and/or handle upgrades. Key issues include: (i) technology for efficient resource management, (ii) tools supporting design space exploration, in particular trade-offs when co-developing hardware and software; and (iii) advanced model-driven development.*

TERESA contributes to an integrated design environment that can be extended and customised. Customisation is based on common engineering process metamodels from which domain specific extensions can be integrated, and on the development of access tools that are dedicated to a given development environment. The design environment takes into account the following key issues: technology for efficient resource management, and advanced model-driven development.

- **O3:** The results of TERESA (R2,R3,R4) contribute to the creation of *a security engineering discipline.* This is consistent with the description of ICT-2009.3.4 target outcome in the work programme:

Initiatives to advance the European Research Area and to align research agendas *in the field of embedded systems.*

By defining an engineering methodology for security and dependability that can be applied in different application domains (the railways, metering, and automotive domains have been analysed, and guidelines for other domains have been provided), TERESA has contributed to a common transversal approach for security and therefore to the possibility of creating an engineering community. To this end, in 2011 TERESA participated in the creation of the Security Engineering Forum (http://www.securityengineeringforum.org/) in order to continue the promotion of TERESA results.

Impacts

The described outcomes will have the following impacts:

- **I1:** TERESA contributes to a **potentially significant increased productivity of embedded system development.** The engineering process promotes the separation of engineering concerns. It allows application designers to benefit from the reuse of state-of-the-art security and dependability solutions, to benefit from the advantage of Model Driven Engineering (MDE) and pattern based approaches. The MDE approach allows reuse of S&D artefacts at an earlier stage of design. Furthermore, the repository access tools allow application designers to benefit from the advantage of MDE even though they do not use MDE for application design. The engineering process also takes into account domain specific processes. This allows the support of specific standards, and assurance approach.

- **I2:** TERESA contributes to the **defragmentation of the embedded system industry** by fostering the creation of a common security engineering community in multiple industry domains. This in turn would have a benefit in job offers as the same security engineer could transfer more easily from one domain to another.

- **I3:** TERESA contributes to **the advent of open ecosystems** for security engineering. The repository is an instrument to store S&D patterns provided by different stakeholders. This will allow the emergence of a community of S&D pattern designers. The ecosystems could be engineering centric, i.e. a proprietary repository based on open representations is used to allow for multiple S&D pattern designers. The ecosystems could also be repository centric, i.e. an open repository is used to allow for multiple S&D pattern designers.
- **I4:** TERESA contributes to the **emergence and growth of new companies that supply design tools and associated software**. The open repository built up by TERESA will allow the emergence of new tools for repository access. This will allow the emergence and growth of new companies which supply tools. European SMEs will have the possibility to market engineering tools (based on R3) and to extend them.
- **I5:** TERESA contributes to the **continued European leadership in embedded system design**. TERESA enriches the model driven engineering state of the art. R1, R2, R3 and R4 contribute to the reinforced European scientific and technological leadership in the design of complex embedded systems.

Indirect Impact

It is also useful to explain TERESA's indirect impact.

- TERESA indirectly contributes to ICT initiatives (e.g. Future Internet, EIP-AHA, alternative paths to ICT components and systems, ICT for sustainable development). Many systems in these initiatives will be resource constrained embedded systems (RCES). By focusing on the trusted computing engineering aspects of such systems, TERESA indirectly contributes to the objectives of these initiatives.
- TERESA fosters strong SME based economy. The foreseen ecosystems and business models (repository-centric model of engineering-centric model) is adapted to SME stakeholders as the entry barrier will be lower.
- TERESA contributes to standardisation by separating pattern editing tools (used by pattern engineers) from access tools (used by application engineers). Access tools are adapted to the engineering process standards in use in a given application domain.

Main Dissemination Activities

Overall, TERESA was involved in 106 presentations and produced 24 publications. In addition, TERESA organised:

- the First S&D4RCES workshop in Vienna, co-located with the Safecomp 2010 Conference,
- the Second S&D4RCES workshop in Naples, co-located with the Safecomp 2011 Conference,
- a workshop panel on secure gateways for smart meters during the Think Smart – Security in Metering Conference in Dusseldorf (Nov 2012),
- three advisory board meetings with the following experts: Jon Alzate (SEINALIA), Paris Avgeriou (U.Groningen), Arnaud Cuccuru (CEA), Christophe Jacquet (Supélec), Peter Jensen (EDF), Antonio Maña (U.Malaga), Marga Marcos (U.Basque Country), Mike Rennie (Deimos Space), Alistair Ruddle (MIRA), Didier Van den Abeele (Alstom), Oliver Weissmann (TÜV Rheinland), Norbert Zisky (PTB),
- several meetings with smart meter manufacturers (EMH, Elster, SagemCom) in 2012,

- the creation with external partners of the Security Engineering Forum,
- the preparation of the third edition of the S&D4RCES workshop, planned for June 2013 in Pisa, in conjunction with the 13th International conference on software reuse.

Main Exploitation of Results

The four results of TERESA will be exploited as follows:

- **R1**: a theoretical PBSE engineering foundation based on a repository centric methodology and integrating a formal validation approach based on the SeMF framework. It will be exploited as follows:
  - Dissemination of Pattern Based Engineering(PBSE) repository centric methodology, further research (IRIT)
  - Training and dissemination of the formal validation approach (Fraunhofer SIT)

- **R2**: two example use cases, one on railways and one on secure gateways for smart metering, and guidelines for supporting other engineering processes. These results will be exploited as follows:
  - Using an internal repository for corporate S&D reuse (IK4-Ikerlan)
  - Applying the TERESA approach in smart grid and metrology research projects (USiegen, Trialog)
  - Consulting in covered domains to apply TERESA guidelines for S&D reuse (Trialog, escrypt)
  - Consulting in other domains to apply TERESA guidelines for S&D reuse (Trialog, escrypt).

- **R3**: an MDE (Model Driven Engineering) tool chain for the implementation, population, access and management of S&D patterns repositories. The tool chain is validated through two example use cases. These results will be exploited as follows:
  - Enhancing the maturity of repository tools by creating a community to maintain and enhance the MDE tool chain and to integrate it with existing MDE frameworks and integrated development environments (IRIT)
  - Access tools for specific development environments (Trialog, escrypt)
  - Further tools (Trialog, escrypt).

- **R4**: a strong collection of 59 S&D example patterns. These results will be exploited as follows:
  - Creation of an open repository targeting the academic community and MDE students. The goal is to populate the repository from the literature and teaching experience, share expertise and subsequently enhance the tool chain and the underlying modelling frameworks (IRIT).

Market Assessment

Section 4.2 highlighted the following characteristics concerning RCES:

- Resource constrained embedded systems (RCES) can be found everywhere.
- Computing resources are scarce, generally statically determined.
- Most RCES are high integrity systems, i.e. systems which must meet assurance requirements.

The TERESA target market covers all expertise and engineering services associated with the development, validation of S&D subsystems and their integration in RCES systems:

- services to allow the reuse of S&D components using patterns and models,
- services for the development of S&D components in multiple application sectors,
- services for the creation of S&D components and their storage in a reuse repository (based on MDE engineering where models and patterns associated with a S&D components are stored),
- services for formal validation of S&D components (i.e. security properties of a given S&D pattern can be formally defined and verified),
- development of supporting engineering tools (model creation tools, access tools adapted to an application sector process).

A TERESA market potential is identified in three segments:

- R&D activities to develop tools:
  - Creating repositories, customising access tools
  - Maintenance
  - Support
- R&D activities to develop S&D subsystems:
  - Developing an S&D subsystem
  - Maintenance of an S&D subsystem
  - Support for use, i.e. integration in the main development process.
- R&D activities to develop applications. Five application domains have been considered in the initial phase of the project: smart metering, automotive, home control, industry control and railways.

Here is a short assessment of each application sector:

Smart metering	• This is a high volume market. In-house expertise is not available in general. • The TERESA approach would make sense if the cost of integrating an S&D subsystem is a fraction of the cost of the smart meter development, while ensuring device approval requirements. • A community repository would allow cost sharing between smart meter companies. But this approach is probably new in this area. In order to maintain a competitive edge, we would assume that the repository is shared, while access tools are specific and customized. • A corporate repository is possible. It would, however, require steady internal investment from a smart meter supplier.
Automotive	• This is a high volume market, In-house available expertise on security and dependability is not general, but probably available since large R&D teams are involved. • The TERESA approach would make sense if the cost of integrating an S&D subsystem is a fraction of the cost of the automotive subsystem development, while ensuring automotive assurance requirements. • A community repository would allow cost sharing between automotive suppliers. The automotive domain is used to co-opetition (collaboration and competition) approaches. It would make sense to share both repositories and access tools, for instance by integrating them into a specific AUTOSAR development environment. • A corporate repository is also feasible. Suppliers today have major diversity issues. Having an internal repository could help them reuse. It could be envisaged that a supplier maintains a single repository and a set of customized access tools.
Home control	• This is a high volume market. In-house expertise on security or dependability is not likely to be available. • The TERESA approach would make sense if the cost of integrating an S&D subsystem is a fraction of the cost of the home control development, • A community repository would allow cost sharing between developers. This community could be quite large. It would make sense to integrate a repository and access tool to a

	mainstream community development (e.g. the Android community). • It is not likely that corporate repositories will happen, except for very large companies (e.g. mobile phone manufacturer).
Railway control	• This is a low volume market, where in-house expertise on dependability is available. Security expertise is probably less available. • The TERESA approach makes sense if it is well integrated in the in-house development process. Its value is to help internal reuse. • A community repository is unlikely to take place since the community is small and competition is fierce. • A corporate repository with customized access tools makes sense.
Industry control	• This is a medium volume market (e.g. lift systems), where in-house expertise on security expertise is in generally not available. • The TERESA approach would make sense if the cost of integrating an S&D subsystem is a fraction of the cost of the control system development. • A community repository would allow cost sharing. The conditions to create such repository have to be investigated. • A corporate repository is possible, if it involves a large company.

Market Assessment Per Domain

Business Models

This section provides an analysis of the business models that can be used to exploit the results of the TERESA approach. We assume that a repository and associated tools are available for the management of patterns.

In order to create an innovation ecosystem for the engineering of S&D patterns and their integration into domain specific applications, the following stakeholders are needed:

- S&D experts involved in the creation of patterns
- TERESA experts involved in the extension and maintenance of the TERESA repository and tools
- Domain specific engineers involved in the selection of patterns and their integration into an application.

Two approaches have been identified: a *business model where the repository is managed by a community* and *a business model where the repository is proprietary*.

Repository Managed by a Community

In this model, the central role is played by organisations in charge of managing the repository of patterns. Three types of organisation are involved as illustrated in the figure below:

- *Repository managers* or organisations responsible for the management of a repository and of tools. They are the responsible from the business offer.
- *Pattern users* or organisations responsible for using patterns and integrating them in their applications. They are the customers in the business model.
- *Pattern developers* or organisations responsible for populating the repository with patterns. They get revenue through business deals with *Repository managers*.

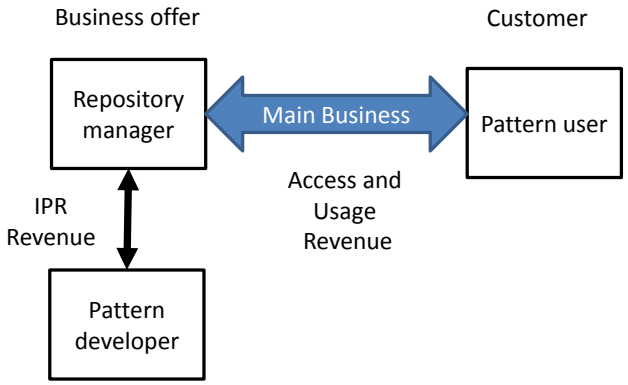

Figure 3: Stakeholders in a Community Model

Repository managers can generate revenues through two different approaches:

- Open community business: *Repository managers* are communities or companies which manage the repository for free.
- Broker business: *Repository managers* create revenue by storing patterns developed by *pattern developers* and selling access to *pattern users*. In this approach, patterns could even be associated with Intellectual Property Rights (IPR).

Revenue could be generated from several sources:

- Access to repository. *Repository managers* organisations get revenue from *Pattern users*
- IPR broker: *Pattern developers* get revenues from *Repository managers* which collect IPR fees from *Pattern Users*.

The advantage of the community model is the **leverage from the community effect**. There are also a number of risks and barriers. First the **ecosystem is difficult to create**. We need to start the repository with a wealth of products for many domains. Restricting it to a single domain would be of interest, but it is likely that the stream of revenue would then be very limited. The **repository would also need constant extension** resources (for new patterns and for access tools). Finally the **licensing approach could create problems**. For instance, licensing each pattern could help sell IPR from third parties, but legal enforcement through the repository might not be as easy to reach.

Repository Managed Individually

In this model, the central role is played by organisations in charge of supplying engineering services. Four types of organisation are involved as illustrated in the figure below:

- *Engineering services providers* or organisations that are providing development services to *Pattern users*. They are the responsible from the business offer.
- *Pattern users* or organisations responsible for using patterns and integrating them in their applications. They are the customers in the business model.
- *Pattern developers* or organisations responsible for populating the repository with patterns. They get revenue through business deals with *Pattern users*.
- *Repository managers* or organisation for the management of a repository and tools. They get revenue through business deals with *Pattern users*.

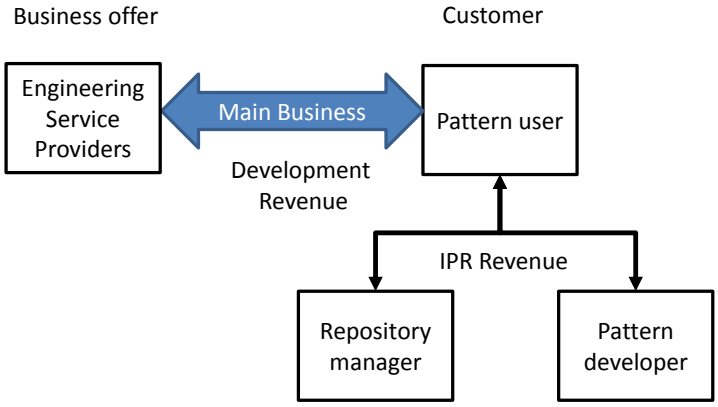

Figure 4: Stakeholders in an Individual Model

Engineering services providers can generate revenues through different approaches:

- Open or proprietary repository. In the open approach, *engineering services providers* provides services around an open community responsible for the repository and tools. In the proprietary approach, *engineering services providers* provides services around its own repository and set of tools, which are instantiated from the open community version.
- Open or proprietary use. In open use, several companies share a common repository. In proprietary use, the repository is owned by a company.

Revenues are engineering services.

The advantage for the engineering centric business model is the **ecosystem is easier to set up**. One customer could be sufficient to start the ecosystem. In that case, licensing issues could be solved. Further, the lack of genericity of the resulting repository will not be a barrier for domain specific exploitation.

The risk and barrier for the engineering-centric business models is that **lack of standardisation** or agreement on approach could yield to solutions that in the long term are more costly, (i.e. a company has focused on its **own isolated engineering approach**).

Exploitation Strategy Selection

The **individual approach** is based on providing services to other companies as:

- developing patterns on demand,
- developing patterns and integrating patterns in their customers' applications
- developing patterns to populate an own-by-customers repository
- developing repository and the associated tools dedicated to a customer use.

The **individual approach** is easier to establish for industrial partners and more realistic since competition conflict between companies and IPR issues forbid most of the time to build a common shared repository of useable patterns.

It should therefore be the typical first step of industrial stakeholders.

The **community approach** relies on organisations in charge of creating, populating and managing the repository or patterns. This approach can be very valuable in its open community version for academic partners being used as leverage. It is appropriate in an academic research purpose

It should therefore be the typical first step of academic stakeholders.

TERESA Resulting Value

This section provides a description of the targeted value of TERESA (what), a description of how we plan to get to the value (how), and the role and contribution of the partners (who).

The Targeted Value (What)

The targeted value of TERESA can be described as *advances beyond the state of the art* on security and dependability engineering. These advances are the following:

- **Approach for reuse S&D recognized by the embedded computing community**. TERESA is defining an approach for the reuse of S&D in RCES by using patterns and models that are recognized by the research and industry community. Contributions from research on MDE, patterns, and S&D are taken into account. In addition research outside of the project will use TERESA as a starting point.

  The TERESA approach is a reusability-centric methodology based on 3 basic concepts:

  - *Pattern engineering*: the engineering of patterns which result in reusable subsystems that can be integrated in RCES.
  - *Pattern-based engineering of RCES*: the engineering of RCES which integrate security and dependability features through the use of patterns
  - *Repository based engineering*: the management and editing of patterns based on a repository of elements (i.e. artefacts) describing a pattern. This engineering follows the model–driven engineering approach.
- **Set of core technologies for the methodology**. TERESA will provide a set of core technologies that will allow the application of the methodology. This set includes:
  - *Repository management of models*. Tools for editing a pattern will be available. Patterns will be stored in a repository. Tools for accessing and integrating a pattern into an RCES process will be available. Access tools are customized according to the application process.
  - *Formal Validation framework*. This is based on a positive formulation of properties that are formally proven to hold throughout the engineering activities. The engineering of a pattern includes the definition of properties and associated proofs, and the integration of a pattern into an RCES system includes activities that ensure that these properties are kept valid.
- **Examples for illustration**. TERESA will provide a number of S&D patterns that are stored in a working repository. Two example use cases with associated access tools will be provided, one for railways applications, and the other for metering applications.
- **Exploitation in industry**. TERESA will ensure that its methodology and associated technology can be used in industry through the following business activities:
  - Consultancy: helping developers to apply the methodology for effective reuse
  - Tools : developing and customizing access tools since application developers could have different set of tools. This enriches the TERESA toolset (e.g. to manage the repository).
  - Development of reusable S&D patterns and storing them in a repository.

The Targeted Value (How)

This section explains how the consortium plans to reach the targeted value:

- Concerning the approach for reuse for security and dependability, we will

- initiate the creation of a community of researchers and industry developers that are interested in using the TERESA based approach (i.e. pattern engineering, pattern based engineering of RCES, repository based engineering)
- contribute to existing communities. Liaison with standardisation communities could be carried out. Liaison with the MDE community or with the software engineering community could also be undertaken.
- publication targeted to the scientific community could also be undertaken (software engineering, pattern engineering, model driven engineering, security, dependability).

- Concerning the building of a set of core technologies for the methodology, we consider that the following phases must be supported:
  - Development of proof of concept tools. This will be carried out in the project.
  - Creation of an initial community interested in the core technology. It is planned that academic partners outside the consortium will be interested to carrying out research in the following areas:
    (1) related to the repository system itself, for instance by contributing new features, on performance improvement
    (2) related to patterns, for instance by developing new patterns or extending them
    (3) related to pattern editing tool capabilities, for instance by developing modification capability for a group of patterns when the standard to which they comply has undergone a specific modification
    (4) related to access tool capabilities. Since access tools are used in existing RCES development processes, they can depend on the domain or on the stakeholder's focus and set of tools. There can be many access tools.
    (5) related to the operation of a repository. For instance, a group of researchers are interested in working in common on a given area of security.
- Concerning exploitation in industry, the following actions are planned:
  - ensure growing proof of the maturity of the approach. This can be achieved by having a sufficient number of stakeholders using the repository. To make this happen, public release of the repository and of patterns must take place.
  - consulting and support activities must be made available to help newcomers use of the repository
  - defining and implementing a plan for adoption. This would include training, the set up of a customised repository, the development of access tools and the development of patterns

Application Specific Domains

In order to obtain “design wins”, it is important to focus on specific domains. The consortium plans to have dissemination activities in several domains:

- The railways domain would focus on dependability aspects. We would expect in-house use, i.e. a company wishes to practice reuse to manage its own internal diversity (as demonstrated by Ikerlan).
- The metering domain could focus on issues related to the involvement of many stakeholders for which the metering domain could accept some federation. This could be the case of the smart meter gateway and its conformance to the associated Common Criteria protection profile.
- The automotive domain needs to address the combination of security and safety in the engineering process, so escrypt could integrate security elements that it develops into the

automotive process by applying the TERESA approach. It could also develop specific access tools for the ETAS development tools.

The Targeted Value (Who)

This section focuses on the specific role of the consortium partners in implementing the actions that will lead to the creation of the targeted value.

- Escrypt was acquired in 2013 by ETAS, which is itself part of the Bosch company. It will keep its own identity in order to provide consulting to automotive organisations that might be competing with Bosch. It will also be able to focus on other domains such as metering. It already has activities with Secutanta, which is a spinoff from U.Siegen providing consulting and services in the area of metering. Its exploitation will consist of consulting, development of security patterns for all domains, and development of access tools adapted the ETAS development environment. It plans to pursue collaboration with Trialog, U.Siegen and Secutanta.
- Trialog focuses on the RCES industry in general. It has been active in the smart metering domain since 2007 in the area of interoperability (for instance in the G3 alliance). It has also strong research background in the area of MDE (some of its members were research colleagues of IRIT members). It has identified the domain of access tools as an important one for consulting and services because of the diversity of stakeholder specific processes (domain specific, stakeholder specific). It intends to develop tools using its MyArtifacts technology. It plans to collaborate with MDE tool vendors and with IRIT in the area of repository and access tools. It plans to collaborate with escrypt and ETAS in the area of automotive and smart metering. It plans to collaborate with U.Siegen and Secutanta in the area of metering and smart grids. It plans to collaborate with Fraunhofer SIT on the operation of the security engineering forum.
- Ikerlan is the research branch of the MCC organization. It has activities in many RCES domains (railways, industry control, and home control). Within its customer base, it plans to use TERESA methodology in the railways and in other domains. It plans to have a two-phase roadmap with the phase focusing on the internal use of patterns and the second phase where the repository approach is used.
- IRIT research focuses on MDE for RCES. It plans to carry out research in the area by consistently promoting the TERESA approach, by maintaining TERESA core technology not only for its own use, but also for its use by research partners. It also plans to customize TERESA technology in other undertakings such the SIRSEC, a French national project. It will also collaborate with Trialog on the combination of pattern editing tools and access tools.
- Fraunhofer SIT focuses on the state-of-the-art for security engineering at research and industry level. It plans to promote the TERESA approach, to promote its formal validation framework, and to provide training to industry.
- U.Siegen focuses on the state-of-the-art of metering at research and industry level. It plans to promote the TERESA approach in the smart meter domain, and to link with the industry through its Secutanta spinoff. It will collaborate with escrypt/ETAS and with Trialog.

IPR Issues

TERESA considered IPR issues and has reached the following position:

- There is no IPR reused from other related projects (e.g. SERENITY).
- There is no need to protect the repository IPR. An open source approach will be use. This is consistent with the current consortium preference to adopt a business model based on engineering services

Market Potential

Railway: A Very Specific Market

Railway transportation is a competitive mean of transport. The investment made by European countries has been representative. It should be mention that there is a European initiative towards the deployment of European width high-speed train traffic management system and interoperability of trains and trackside across Europe, called ERTMS (European Rail Traffic Management System). Based on this, a high speed train should for example be able to go from Madrid to Munich without stop, removing current limitations of national signaling systems and standards.

The railway sector is dominated by a few global manufacturers such as Bombardier, Alstom and Siemens.

The rail vehicle architecture is federated, which means that major rail vehicle functions are implemented in different interconnected subsystems such as: Traction system, Braking Control Unit, Central Control Unit, railway signaling ETCS (European Train Control System), etc. All these subsystems are usually interconnected by two railway specific communication protocols. TCN (Train Control Network) at train level and MVB at vehicle level.

Railway manufacturers are composed of different subsidiaries. Some of them are transversal but others are only linked to a given subsystem of this federated architecture.

Railway is a very appropriate sector to apply the TERESA approach. It is not uncommon to find situations in this industrial domain where TERESA could accelerate and support the development of safety related subsystems.

Two different railway industry scenarios are described. One takes place in a railway manufacturing group and the second takes place in an SME:

- For a railway industry group, there is a good opportunity to build on the scarce number of qualified safety or security engineers patterns in reusable format (e.g. using modelling language) to achieve dependability requirements without being forced to rely on providers or competitors. Thus, TERESA can be suitable to build a pattern repository to be reused with the following benefits:
    - Reduce product development cost and time, with the reuse of design patterns across projects and companies.
    - Reduce probability of systematic faults by reducing ambiguity.
- For a safety **related embedded systems development SME** with a deep expertise of IEC-61508 standard, the potential is based on the specialization of patterns. An infrastructure allowing for the cross-domain reutilization of techniques to achieve the target safety level is a real opportunity for this kind of company to reuse its expertise. This reutilization for a variety of domain where the standards are derived from IEC-61508 with well-know differences can be achieved with the main benefits:
    - Among projects.
    - Reduce probability of systematic fault by reducing ambiguity.
    - A cross domain arsenal of design patterns that can be used in new domains.

Figure 5 Relations between Safety Standards

Automotive: Market is Characterised by a Specific Supply Chain

In the automotive domain there are several stakeholders taking part on the manufacturing process of embedded systems. The identified stakeholders are for instance the OEM or the Tier 1 Supplier.

The OEM assembles all components to the finished product from electronics to chassis and all other car parts. Several tier 1 suppliers deliver their parts to one or several OEMs, these parts are then assembled with the other parts from other Tier 1 suppliers and must be compatible to each other. On the lower levels additional software and hardware are developed in different companies which lead to even more integration effort. Hardware changes from time to time and is becoming more complex and integrated. For an efficient embedded system development software tools are mandatory.

AUTOSAR based Development

AUTOSAR has been developed by a group of automotive vendors and stake holders. Its goal is to provide an open standard for automotive software development which improves the efficiency and quality of automotive software.

The AUTOSAR software architecture abstracts the hardware components and has several layers. These layers provide common functionality for AUTOSAR applications which run in a runtime environment (RTE). For special functionality of the underlying hardware Complex Drivers can be written and made accessible for the RTE.

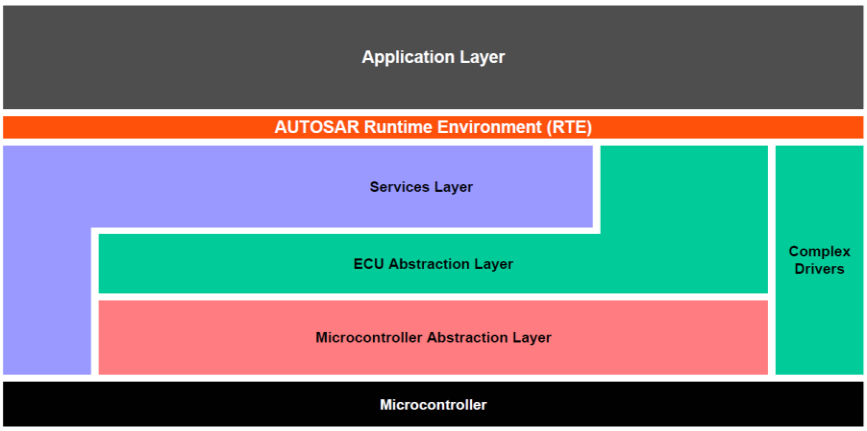

Figure 6: AUTOSAR Software Architecture, Source: "http://www.autosar.org"

The goals of AUTOSAR are supporting the implementation and standardization of basic system functionality, as well as scalability for different vehicle platforms. Furthermore, the integration of functional modules from different suppliers and the consideration of availability and safety requirements are aimed. These goals can be reached by choosing an architecture supporting the right design model, e.g. a component based design supported by an automated methodology. With this mechanism the executable software for ECUs is created.

The AUTOSAR framework is a specification of standards and not a "tool set" **it is possible to use different tools from different vendors**. This together with the fact that the implementation of components is done by different manufacturers supports the competition between them.

Model-Based Development is widely used

Tool Assisted Design, Model Based Development as well as System Validation are very important in that context, because the systems, which are often safety critical, need to be dependable and valid. In the case of engine or other driving relevant ECUs calibration needs to be done. The control algorithms need to be fine-tuned to guarantee low fuel consumption as well as enough power for an adequate driving experience. Active steering, active braking and accelerating and other ECU functions have hard real time constraints. To all of these points come that the hard and software must be robust to tough environmental conditions. Therefore embedded systems software manufactures

are involved in every phase of the development process with their tools. These standardized tools help to deal with the large number of stake holders and available standards and their integration as well as the severe requirements hardware and software components in the automotive domain have.

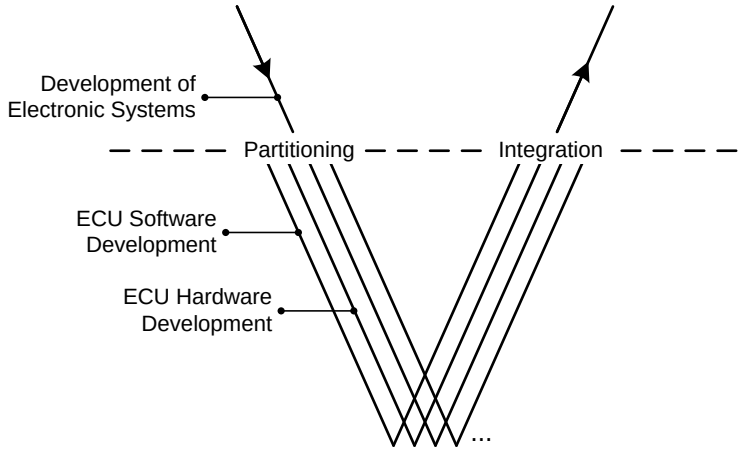

Figure 7: Overview of the development of electronic systems

Security is an Increasing Concern

With increasing complexity and functionality of the systems, security is moving more and more into the focus. Multimedia and entertainment functionalities as well as their connectivity features open potential gateways for attacks on the cars. It has to be guaranteed that no harmful software can be injected through this new attack points.

Because the systems are so complex and the development of these components is very costly, the IP protection also plays a larger role. Together with that the protection against chip tuning or manipulating the kilometre counter is another security relevant topic. So cryptography is needed and will find its way into modern cars.

TERESA Approach is well Adapted

The TERESA approach could be applied to all of these requirements. Verified and tested patterns can support the development of dependability and safety related subsystems and they can accelerate recurring tasks and evaluation. As the need of secure communication is rising with the growing number of communication interfaces in a modern vehicle, the integration of security related functions becomes a demand already in the design phase.

To explain the envisioned market, it is useful to explain an automotive ecosystem scenario. It involves the following stakeholders:

- a tier 1 supplier,
- a software developing tool manufacturer,
- Embedded security specialist.

The scenario is the following: the tier 1 supplier wants to upgrade its ECUs with a "secure update" mechanism. It should be possible to execute this firmware update on a remote way as well as by an injection during car maintenance or even at production level. The firmware update mechanism must verify the authenticity and integrity of the firmware.

The tier 1 supplier uses the AUTOSAR framework as a de facto framework. It uses the software tool chain from the tool manufacturer which is an "embedded automotive software development tools" vendor. The tool manufacturer integrates the TERESA access tool into their products to be able to

exchange information with the TERESA repository. The TERESA repository contains security & dependability patterns developed and validated by the embedded security specialist.

Smart Metering: A Market That Is Profoundly Impacted By New Needs

The Metrology domain is originally purely mechanical, but it has changed through the time to electrical and now it is a communicating embedded system. This latter change comes with the new needs of Smart grids.

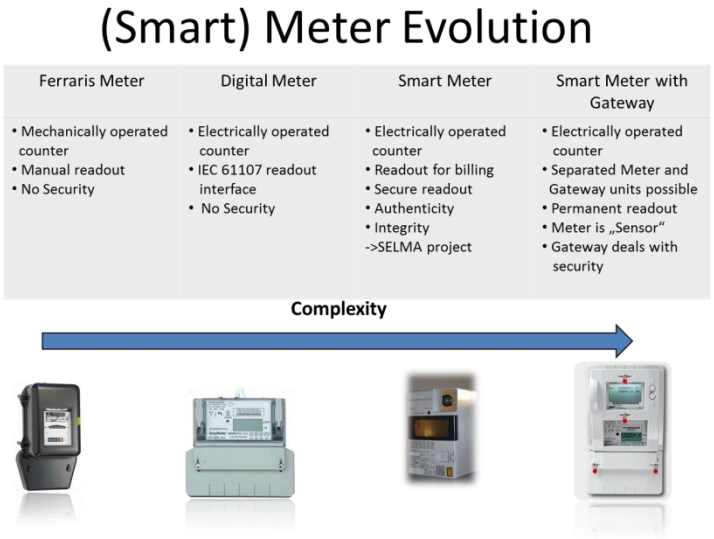

Figure 8 Evolution of electricity meters

Security and Model-Based Development are New Concerns

With the debut of smart meters, offering additional functionalities like a secure readout, security for metering became an arising question. Therefore, techniques like digital signatures (to ensure authenticity and integrity of measurements were introduced to the metrology domain. Complexity of the formerly pure measurement devices increased. Besides providing different communication interfaces, cryptographic algorithms needed to be implemented as well as secure memory for key material. Communicating different information (readouts, consumption data, parameters, energy generated etc.) with several entities and not only one remote entity is a main functionality of a modern smart meter. The meter is nowadays equipped with a communication module providing the connectivity to the different networks called smart meter gateway. Depending on the type, the security functionality is completely shifted into this gateway which is acting as first line of defence for the metering system in a network.

Since complexity of embedded systems in metering systems increased, software development following a well-defined process gained more and more importance for this domain. In the past days, Model Driven Engineering was not used at all. Now the main stakeholders are moving progressively toward MDE to enhance the quality of their products.

Metrology Market

As depicted in Figure 9, the European metrology domain can be divided into three markets:

- The manufacturer market that comprises all the manufacturers of measurement devices and components as well as the software to run these devices.
- A group of providers like the utility and grid operators, the service providers (e.g. remote readout of measurements) and the providers of software for that market.

- Telecom market, comprising: telecommunication companies, telecommunication component manufacturers and their software providers.

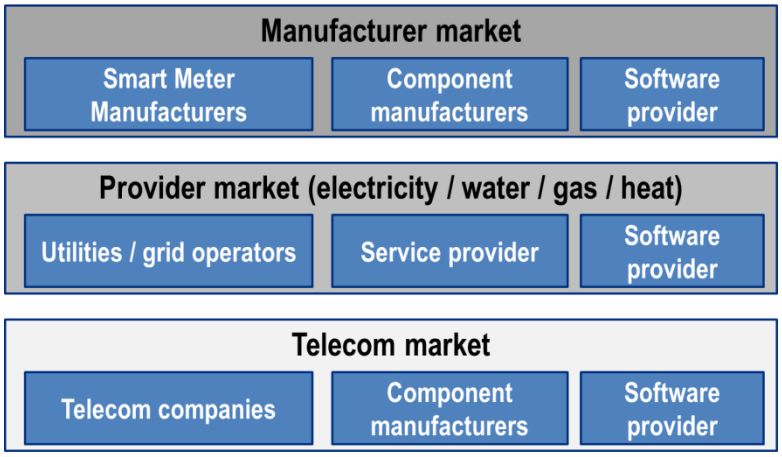

Figure 9 Metrology domain markets [Source: TÜV SÜD AG – Embedded Systems]

The more promising potential is located in the manufacturer market in the following three main scenarios.

In case of an **international meter manufacturing** company (as Sagemcom or Elster) the need of security experts with specific country or region knowledge is critical. But the contribution of the security expert can be reduce by using patterns and reducing the time spent by experts on each product. The benefits expected are:

- Reduction of product development cost and time, with the reuse of design patterns to address security issues.
- Reduce the time to market for new metering devices, since evaluation and certification are time consuming processes, which may be sped up with a detailed and clear development documentation of the product. This may directly be mapped to type approval of the device. The type approval procedure may be sped up by providing detailed product documentation, especially for the security related parts.
- Reduce the number of full time security experts by providing the security knowledge with patterns since experienced security experts in this domain are rare and cost intensive.

If a **meter manufacturing SME** is considered, in most of the case they only work for one national market and due to their limited size do not have in-house security experts. The use of security patterns at every level of the development of a meter or gateway can reduce the extra cost of using security subcontractors as one benefit among:

- Reduce product development cost and time, with the reuse of design patterns to address security issues.
- Competitive advantage towards other manufacturers and market participants in terms of having expert security solutions in their products, having been evaluated in depth.
- Reduce the time to market for new metering devices, since evaluation and certification are time consuming processes, which may be sped up with a detailed and clear development documentation of the product. This may directly be mapped to type approval of the device. The type approval procedure may be sped up by providing detailed product documentation, especially for the security related parts.
- Keep structured expert knowledge inside the company by using a repository with patterns, even if employees change. This also helps to shorten down training periods of newly employed engineers

Another potential benefits in this market is to support the security evaluation time by providing well written evidence of the security properties that are enforce and so on. It is both interesting for the Metering Manufacturer company and for the **mandated expert company** that have to certify or qualify the product according some standards (as the EAL X for the Common Criteria) by reducing the cost of the expertise for the manufacturer and to be allow to have more client as the same time for the certifying company.

Main Exploitation Paths

- IK4-Ikerlan main exploitation is based on the following activities:
  - Customer-specific creation and maintenance of patterns
  - Development (and certification) of safety systems by using an internal pattern repository (the internal pattern repository is a selling argument)
  - Dissemination of the TERESA approach and assistance in the deployment of pattern repositories at customer sites
- ESCRYPT main exploitation path is based on the following activities in a first time:
  - Customer-specific creation and maintenance of patterns
  - Creation of access tools for integration in ETAS tool set
- Trialog main exploitation path is based on the following activities:
  - supplying, maintaining and extending access tools to specific development environments
  - Seeking development opportunities for access tools in other development environments, i.e. other domains.
  - Specific consulting for S&D pattern development

Communication Strategy for Open Source

The following table presents the specific communication channels used for the TERESA tool suite.

Website Tool Suite	http://www.semcomdt.org
Download of Tools	http://www.semcomdt.org/semco/tools/updates/1.2
Community Tools	Bugtracking Enhancement/Feature Requests Wiki http://www.semcomdt.org/bugtracker/
Presentations Videos	Teresa Tool Suite http://www.semcomdt.org/semco/demo/video_semco/toolsuite/ToolSuiteIRIT.mp4 Access Tool http://www.semcomdt.org/semco/demo/video_semco/viewer/viewer.htm

Code Hosting	https://bitbucket.org/bhamid/semcomdt
Public Repository	A public repository will be made available at tcp://www.semcomdt.org/ Primary contact: Brahim HAMID IRIT-University of Toulouse hamid@irit.fr http://www.irit.fr/~Brahim.Hamid
Presentations, Posters and Tutorials on Conferences	In addition to the previous events(after March 2103): SDL Forum 2013 (Poster & Presentation), EuroPLoP 2013 (Poster & Workshop), SERA 2013 (Presentation), ACME 2013 (Presentation), IRI 2013 (Presentation), Coming up: PLoP 2013 ESSoS 2013

Contacts

Antonio Kung, project co-ordinator, antonio.kung@trialog.com,

Cyril Grepet, technical co-ordinator, cyril.grepet@trialog.com

Barbara Raither, administration, barbara.raither@Trialog.com

TRIALOG

25 rue duGénéral Foy

75008 Paris, France

Tel: 33 (0) 1 44 70 61 00

Fax: 33 (0) 1 44 70 05 91

Project website:www.teresa-project.org

Youtube presentations: http://www.youtube.com/user/TeresaFP7/videos

Project Logo :

4.3 Use and Dissemination of Foreground

Section A (public)

Approach to Dissemination and Use

Dissemination and liaison have been paramount for the success of the TERESA undertaking. This has involved activities at the industry and research level.

Industrial Companies

Several meetings were organised with different companies to show the current results of the TERESA project. During the meetings, different topics such as models, patterns, and methodology were discussed. Among them were:

- FAGOR (Home appliances). Is interested especially in the use of patterns for different groups of engineers distributed in all Europe. They are waiting for more information during TERESA development.
- CAF (Railways). Is interested especially in the use of patterns and models for safety critical systems. The key point to have an easy methodology for the different roles during the development process. They are also waiting for more information during TERESA development.
- Alstom Wind (Wind turbines). Is interested especially in the use of patterns and models in two different level application level and embedded system level (Platform level), they think that TERESA approach is going in the correct direction. They are also waiting for more information during TERESA development.
- ORONA (Elevators) is interested especially in the use of patterns and models during the full process and taking into account the RCES requirement, they think that TERESA approach is going in the correct direction but some improvements are needed in the embedded system Testing and Virtual Prototyping. They are also waiting for more information during TERESA development.
- Physical Technical Institute of Germany (Physikalisch-Technische Bundesanstalt PTB) USiegen attended a meeting with Dr. U. Grottker of PTB who is the person in charge of the assessment of Smart Metering Systems in the German Metrology Institute. During the meeting, different topics according to dissemination of TERESA results in the metrology domain were discussed. Some among them were:
    - Relevant catalogues containing security and dependability related requirements for Smart Meters
    - Accomplishment of the current type approval procedures
    - What is considered as a remote readout of measurement data and what are the requirements for a remote readout
    - How is software downloaded to Smart Meters treated by existing requirement catalogues and how far is the German Verification Act (EichG) involved
    - How can the TERESA project help to ease type approval?

  One of the conclusions of the meeting was that the use of well known S&D patterns in the design of new Smart Meters would be very helpful for type approval, since these patterns would not have to be checked again each time. Also this could make the use of the H1-

assessment more prominent. Further results of the meeting influenced the contents of University of Siegen's part of the D7.1 deliverable.

Academic Organisations

The following contacts were taken during the project**:**

- ICTEI, Chisinau: The ICTEI 2010 International Conference on Telecommunications, Electronics and Informatics has been organised by the Technical University of Moldova, which has a partnership with the Data Communications Systems (DCS) Institute of the University of Siegen. The paper "Integration of Security and Dependability into Resource Constrained Embedded Systems" was submitted by Mr. Bodenstedt, Mr. Ruland and Mr. Weber to present one of the research topics of the DCS Institute and to enhance the awareness of the TERESA project.
- ISO - Technical committees - JTC 1/SC 27 - IT Security Techniques: Cooperation with this working group is important for S&D related to RCES. Lightweight cryptography will become important for resource constrained systems like embedded systems in metering devices. Thus the target is the upcoming standard ISO 11770-5 (Key Management: Group Key Management).
- ArtistDesign NoE (http://www.artist-embedded.org/artist/): With regard to dissemination in Embedded Systems Design, IRIT established links with the ArtistDesign NoE network, in particular with community of Modeling and Validation. This is in order to compare our results with those of projects supervised by ARTIST community and to disseminate TERESA outputs through ARTIST tools.
- SAFECOMP conference: beyond the existing SAFECOMP community, we believe that synergy between researchers working in different aspects of security and dependability will produce important benefits. Given the relevance of our work to this community, we outlined the following: modelling, formal and semi-formal methods, tools for security and dependability in embedded systems, domain specific languages for trust Resource Constrained Embedded Systems (RCES) applications, engineering processes for RCES.
- EWICS TC7 (European Workshop on Industrial Computer Systems, Technical Committee 7: Reliability, Safety, Security): B. Hamid of IRIT joined this Working group. This is a good opportunity to disseminate the results of TERESA in this community in particular the challenges and advances in enforcing S&D in RCES by model-driven engineering.

Liaison with Other EU Projects

TERESA has liaison activities with other EU projects that are focused on engineering and modelling secure systems:

TERESA’s project results on expressing Security Properties / Requirements were presented to the projects SecFutur and Assert4SOA. Input from these discussions will be utilized within TERESA. SecFutur and ASSERT4SOA have the following objectives:

- SecFutur aims to "Unleash the potential of security in embedded environments through the provision of standardised security building blocks and application models fit for use."
- "ASSERT4SOA will fill this gap by producing novel techniques and tools – fully integrated within the SOA lifecycle – for expressing, assessing and certifying security properties for complex service-oriented applications, composed of distributed software services that may dynamically be selected, assembled and replaced, and running within complex and continuously evolving software ecosystems."
- SecFutur can therefore directly benefit from the basic work of TERESA with respect to the involved processes and generic structure. TERESA will profit from the input of yet another

application domain and incorporation for security models. ASSERT4SOA includes a task for the certification of services based of formal models. This is closely related to the tasks in TERESA, though based on a narrower variety of underlying system models. However it provides yet another application domain for modelling of security properties and requirements.

Security Engineering Forum

During the International Workshop on Security and Dependability for Resource Constrained Embedded Systems (SD4RCES) in Naples on 22 September, 2011, Carsten Rudolph of Fraunhofer SIT presented "The Vision of a European Engineering Forum."

The objective of the forum was to create a community on security engineering. This forum was structured by activities (e.g. pattern engineering, model-driven engineering, privacy). TERESA decided to support this initiative as an instrument for dissemination and exploitation for the project.

It was agreed that a further workshop would be organised in Malaga on 2 February 2012 in order to continue the work the forum. Three persons were nominated to manage the organisation of the workshop: Carsten Rudolph from Fraunhofer SIT, Antonio Maña from University of Malaga, and Antonio Kung from Trialog and TERESA.

The web site for the forum is www.securityengineeringforum.org

TERESA stakeholders will be involved in activities related to S&D pattern engineering. The following snapshots show the blog page and the list of work groups.

Figure 10: Security Engineering Forum Blog Entry

Figure 11: Security Engineering Forum Work Groups

Communication Strategy

The communication objectives for TERESA were as follows:

- Disseminate TERESA contribution in terms of engineering process, modelling and S&D mechanisms integration in the RCES community
- Disseminate TERESA academic contribution in terms of research
- Communicate about possible further challenges that TERESA has identified in the area of RCES Trust engineering
- Disseminate specific innovation in the RCES and S&D community.

The communication sources for TERESA were as follows:

- Deliverables
- Project progress information
- Workshop results
- Event information and presentations
- Information related to other relevant projects/initiatives.

The TERESA project created the following logo, which is available in various sizes:

Figure 12: Project Logo

This logo was used with the following standard documents:

- Press releases
- Fact sheet
- Deliverables
- Presentations
- Templates
- Flyer
- Web site.

Standard documents and templates for these documents were maintained in a project workspace.

Communication Channels and Media

The following table presents an overview of communication channels used for TERESA.

Communication channel/media	Characteristics
Web site	TERESA web site: www.teresa-project.org
Brochure	A flyer was created in January 2011
General project presentation	A general project presentation is available on the TERESA web site.
Presentations	Ad hoc presentations targeted to specific workshops have been made. Other presentations with more general information have been made.
News	The website includes a regular update on news
Youtube presentations	TERESA has published two presentations in youtube (http://www.youtube.com/user/TeresaFP7/videos) • A presentation of the overall approach • A presentation of the railways use case TERESA also plans to publish two further presentations • A presentation of the TERESA toolset • A presentation of the metrology use case
TERESA workshops	TERESA plans to organise a number of workshops throughout the project. The first S&D4RCES organised by TERESA partners took place in Vienna on 14 September 2010in conjunction with conference SAFECOMP 2010. The second S&D4RCES organised by TERESA partners took place in Naples on 11 September 2011 in conjunction with conference SAFECOMP 2011 The third S&D4RCES will take place in Pisa during the 13th international conference on software reuse "Safe and secure reuse" 18-21 June 2013.

	http://softeng.polito.it/ICSR13/ http://www.irit.fr/SD4RCES/SD4RCES13/
Other workshops and conferences	TERESA has participated to a number or workshops and conferences (see list below).

Table 1: Overview of communication channels use.

The following table presents the specific communication channels used for the TERESA tool suite.

Website Tool Suite	http://www.semcomdt.org
Download of Tools	http://www.semcomdt.org/semco/tools/updates/1.2
Community Tools	Bugtracking Enhancement/Feature Requests Wiki http://www.semcomdt.org/bugtracker/
Presentations Videos	Teresa Tool Suite http://www.semcomdt.org/semco/demo/video_semco/toolsuite/ToolSuiteIRIT.mp4 Access Tool http://www.semcomdt.org/semco/demo/video_semco/viewer/viewer.htm
Code Hosting	https://bitbucket.org/bhamid/semcomdt
Public Repository	A public repository will be made available at tcp://www.semcomdt.org/ Primary contact: Brahim HAMID IRIT-University of Toulouse hamid@irit.fr http://www.irit.fr/~Brahim.Hamid
Presentations, Posters and Tutorials on Conferences	In addition to the previous events(after March 2103): SDL Forum 2013 (Poster & Presentation), EuroPLoP 2013 (Poster & Workshop), SERA 2013 (Presentation), ACME 2013 (Presentation), IRI 2013 (Presentation), Coming up: PLoP 2013 ESSoS 2013

Template A1: list of scientific (peer reviewed) publications, starting with the most important ones

NO.	Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of public-cation	Year of publica tion	Relevant pages	Permanent identifiers (if available)	Is/Will open access provi-ded to this publicat ion?
1	First Experiment on Modeling Safety Life Cycle Process in Railway Systems	Brahim Hamid	International Journal of Dependable and Trustworthy Information Systems Vol. 2 N° 2 (IGI Global)	N° 2	IGI Global	USA	2011	17-39	Dependable and Trustworty Information Systems	Yes
2	**Enforcing S&D Pattern Design in RCES with Modeling and Formal Approaches**	Brahim Hamid	Proceedings of the ACM/IEEE 14th International Conference on Model Driven Engineering Languages 2011 (MODELS 2011)	14th	Springer-Verlag	Heidel berg	2011	319-333	ACM DL Digital Library	Yes
3	**An Environment for Design Software and Hardware Aspects of Clock Synchronization and Communication in DRTES**	Brahim Hamid	Proceedings of IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC 2010)	8th	IEEE	China	2010	60-67	IEEE Xplore	Yes
4	**Towards a Unified Meta-Model for Resources-Constrained Embedded Systems**	Adel Ziani	37th EUROMICRO Conference on Software Engineering and Advanced Applications (SEAA), 2011	37th	IEEE	Finland	2011	485-492	IEEE Xplore	Yes
5	**A Model-Driven Engineering Framework for Fault Tolerance in Dependable Embedded SystemsDesign**	Adel Ziani	Euromicro Conference on Software Engineering and Advanced Applications (SEAA 2012)	38th	IEEE	Turkey	2012	166-169	IEEE Xplore	Yes
6	**A Proven Pattern Integration Process**	Damien Gouteux	European Conference on Pattern Language of Programs (EuroPlop 2012)	17th	Hillside	Germany	2012		Europlop2012	Yes
7	Redefining Security Engineering	Carsten Rudolph	5th International Conference on New Technologies, Mobility and Security (NTMS)	5th	IEEE	Turkey	2012	1-6	IEEE Xplore	Yes
8	Supporting Security Engineering at Design Time with Adequate Tooling	Jörn Eichler	The 15th IEEE International Conference on Computational Science and Engineering (CSE 2012)	15th	IEEE	Cyprus	2012	194-201	IEEE Xplore Digital Library	
9	**A Metamodel for Representing Safety LifeCycle Development Process**	Yulin Zhang	ICSEA 2011, The Sixth International Conference on Software Engineering Advances (ICSEA 2011)	6th	IARIA	Spain	2011	550-556	Think Mind	Yes
10	**Integration of Security and Dependability into Resource Constrained Embedded Systems**	Christian Bodenstedt	3rd International Conference on Telecommunications, Electronics and	3rd	ICTEI	Moldova	2010		TERESA website	Yes

			Informatics (ICTEI 2010)							
11	**Towards a Model-Based Approach for Reconfigurable Distributed Real Time Embedded Systems**	Fatma Krichen	Proceedings of the European Conference on Software Architecture (ECSA)	5th	I. Crnkovic, V. Gruhn, M. Book	Germany	2011	295-302	IEEE Xplore	Yes
12	**Formalization of Smart Metering Requirements**	Andreas Fuchs	Proceedings of S&D4RCES '10 Workshop, in the Proceedings of the International Workshop on Security and Dependability for Resource Constrained Embedded Systems (SAFECOMP 2010)	1st	ACM	Austria	2010	N°4	ACM DL Digital Library	yes
13	Model-Based Security and Dependability Patterns in RCES – the TERESA Approach	Brahim Hamid	S&D4RCES & SAFECOMP 2010: see above	1st	ACM	Austria	2010	N°8	ACM DL Digital Library	yes
14	Towards the Integration of Advanced Engineering Paradigms into RCES: Raising the Issues for the Safety-Critical Model-Driven Product-Line Case	Salvador Trujillo	S&D4RCES & SAFECOMP 2010: see above	1st	ACM	Austria	2010	N°9	ACM DL Digital Library	yes
15	Enforcing Trust in Embedded Systems Using Models	Christophe Jouvray	S&D4RCES & SAFECOMP 2010: see above	1st	ACM	Austria	2010	N°1	ACM DL Digital Library	Yes
16	Towards Variability Support for Security and Dependability Patterns	Brahim Hamid	Proceedings of the 3rd International Workshop on Model-driven Approaches in Software Product Line Engineering and Software Product Line Conference (SPLC/MAPLE/SCALE 2011)	3rd	ACM	Germany	2011	Vol 2, N°27	ACM DL Digital Library	Yes
17	Safety Lifecycle Development Process Modeling for Embedded Systems - Example Railway Domain	Brahim Hamid	4th International Workshop on Software Engineering for Resilient Systems (SERENE)	4th	Paris Avgeriou	Italy	2012	63-75	IEEE Xplore	Yes
18	Security Engineering Based on Structured Formal Reasoning	Carsten Rudolph	RISE Workshop on Redefining and Integrating Security Engineering (RISE'12)			USA	2012		Proceedings	Yes
19	Model-Based Engineering for Dynamic Reconfiguration in DRTES	Brahim Hamid	Proceedings of 8th Nordic Workshop on Model Driven Software Engineering	8th	Nordic workshop	Denmark	2010		NW-MODE 2010	yes
20	Security Engineering for Embedded Systems: the SecFutur Vision	Sigrid Gürgens	Proceedings of S&D4RCES 2011 Workshop, in the Proceedings of the International Workshop on Security and Dependability for Resource Constrained Embedded Systems (SAFECOMP 2011)	1st	ACM	Austria	2010	N°7	ACM DL Digital Library	Yes

21	Analysis of the SYM2 Smart Meter Remote Software Download Using Formal Methods Reasoning	Andreas Fuchs	Proceedings of S&D4RCES 2011 Workshop, in the Proceedings of the International Workshop on Security and Dependability for Resource Constrained Embedded Systems (SAFECOMP 2011)	2nd	ACM	Italy	2011	N°3	ACM DL Digital Library	Yes
22	Pattern based Trusted Engineering for a Smart Meter Gateway	Donatus Weber	The 2nd think smart Conference on Secure Communication for Mobile Networks	2nd	Escrypt	Germany	2012			Yes
23	Herausforderungen und Lösungsansätze zur Integration von Safety und Security aus der Perspektive Formaler Methoden.	Andreas Fuchs	Zertifizierung und modellgetriebene Entwicklung sicherer Software (ZeMoSS Workshop)			Germany	2012		BibTeX	Yes
24	Vers une Technique de Développement de Patrons de Sécurité et de Fiabilité pour les Systèmes Embarqués Contraints en Ressources	Brahim Hamid	Génie Logiciel, GL & IS			France	2011			Yes

Template A2: list of dissemination activities

N°.	Type of activities[3]	Main leader	Title	Date/Period	Place	Type of audience[4]	Size of audience	Countries addressed
1	Meeting of ISO/IEC JTC 1 SC 27 (“Security Techniques”)	USiegen		1-7 Nov 2009	Redmond, USA	SC 27 standardizes cryptographic algorithms, modes, methods and protocols.		
2	Visiting of eWorld in Essen and discussion of TERESA approach with different companies from the metering industry	Escrypt		10.02.10	Essen, Germany	eWorld in (Smart Metering Fare)		
3	Distribution of the TERESA factsheet	Escrypt		02-04.03.10	Nurnberg, Germany	Embedded world conference		
4	Discussion of potential applications of security patterns	Escrypt		26.02.10		Visit of a PayTV solution provider		
5	Discussion of potential applications of security patterns	Escrypt		29.03.10		Visit of a Bank terminal solution provider		
6	Search for new partners interested in the TERESA engineering approach	Escrypt		04.03.10	Dusseldorf, Germany	NRW-IKT meeting ZENIT – Successful R&D in Europe		
7	Discussion about the idea of a validated engineering process to simplify the				Germany	Meeting with the Physikalisch-Technische Bundesanstalt		

[3] A drop down list allows the choice ofthe dissemination activity: publications, conferences, workshops, web, press releases, flyers, articles published in the popular press, videos, media briefings, presentations, exhibitions, thesis, interviews, films, TV clips, posters, Other.

[4] A drop down list allows the choice ofthe type of public: Scientific Community (higher education, Research), Industry, Civil Society, Policy makers, Medias, Other ('multiple choices' is possible).

	type approval procedure							
8	Preparation of a paper	USiegen		20-23.05.2010	Chisinau, Moldova	3rd International Conference "Telecommunications, Electronics and Informatics" ICTEI		
9	Preparation DANCE workshop, Discussion to join the to join the IFIP Working Group 10.2 on Embedded Systems	IRIT		February-April 2010		IEEE international DANCE workshop (http://www.irit.fr/DANCE2010)		
10	Escrypt and Trialog: Liaison activity with other FP7 projects			04.05- 05.05.10	Bochum, Germany	OVERSEE Meeting		
11	Liaison activity with other FP7 projects	Escrypt and Trialog		07.06.10	Munich, Germany	EVITA Meeting		
12	Objectives of TERESA have been discussed with potential customers	Escrypt		16.06.10	Duisburg, Germany	WO Kongress (Logistics & Transport)		
13	Visitation of potential customers in different business areas and discussion of TERESA objectives	Escrypt		May & June 2010		Transportation industry (11.05.10) Government (25.05.10) Banking industry (28.05.10) Communication industry		
14	Establishing contacts to the metering industry in Germany	USiegen		May & June 2010				
15	Discussion to join the to join the IFIP Working Group 10.2 on Embedded Systems	IRIT		Feb-April 2010		Preparation of the IEEE international DANCE workshop http://www.irit.fr/ DANCE2010		
16	Participation at the Workshop on Cryptographic Hardware and Embedded Systems:	USiegen		2010	Santa Barbara USA	CHES 2010		
17	Presentation of the paper "Formalization of Smart Metering Requirements", first workshop organized by the TERESA project	USiegen & SIT		14.09.2010	Vienna Austria	S&D4RCES workshop of the Safecomp 2010 Conference		
18	Presentation of the talk: Towards the Integration of Advanced Eng. Paradigms into RCES: Raising the issues for the Safety-Critical Model-Driven Product-Line Case	IK4-IKERLAN & IRIT		14.09.2010	Vienna Austria	S&D4RCES workshop of the Safecomp 2010 Conference		
19	Discussion of TERESA ideas with RESIST partners	Escrypt		04.08.2010	Darmstadt Germany	Research Project RESIST		
20	Discussion about the idea of a validated engineering process to simplify the type approval procedure	Escrypt		02.09.2010	Bonn Germany	BITKOM Workshop for Smart Energy, Smart Metering		
21	Visiting of an industry workshop for security and discussion of TERESA approach with potential customers	Escrypt		21.09.2010		Industry workshop for security		
22	Discussion of TERESA ideas with potential customers	Escrypt		22.09.2010	Vienna Austria	Metering and Billing Europe		
23	Discussion of TERESA ideas with potential customers and distribution of the TERESA factsheet	Escrypt		06.10.2010	Essen Germany	Security 2010		
24	Search for new partners interested in the TERESA engineering approach	Escrypt		19.10.2010	Nuremberg Germany	ITSA		
25	Visitation of potential customers in different business areas and discussion of TERESA objectives	Escrypt		Aug & Sept 2010		Mobile Communication Industry, Government		

26	Visitation of potential customers from railway and wind turbines sector and discussion of TERESA objectives	IK4-Ikerlan		22.09.2010		CAF & Alstom Wind		
27	Presentation of a paper "Model-Based Engineering for Dynamic Reconfiguration in DRTES"	IRIT		Aug 2010	Vienna Austria	SAFECOMP 2010		
28	Host of the ACM international SD4RCES workshop and participation in the SAFECOMP conference. Discussion to join the EWICS TC7 (European Workshop on Industrial Computer Systems, Technical Committee 7 : Reliability, Safety, Security) Discussion to join the ARTIST network Models conference attendee	IRIT		Sept 2010	Vienna Austria	SAFECOMP 2010		
29	Presentation of a "Model-Based Security and Dependability Patterns in RCES – the TERESA Approach"	IRIT & Trialog		14.09.2010	Vienna Austria	SAFECOMP 2010		
30	Illustration of TERESA ideas and procedure to several automotive companies. Illustration of ESCRYPT competence and potential interest in outcomes of TERESA. Raise some company's interest from the automotive domain for TERESA, and esp. for TERESA's advisory board.	Escrypt		16-17/11/2010	Bremen, Germany	ESCAR conference		
31	Publication and presentation: An Environment for Design Software and Hardware Aspects of Clock Synchronization and Communication in DRTES	IRIT		11-13/12/ 2010		EUC 2010: Conference IEEE/IFIP communication		
32	Present TERESA to the partners of 2 new proposals of FP7 call January 18th, defined as a important link for those proposals	IK4-Ikerlan		20/12/2010		Link with all the partners of the two new proposals, 12 partners in total.		
33	Visitation of potential customers of the medical industry domain, Illustration of ESCRYPT competence in the domain of software development by means of TERESA for a Medical company.	Escrypt		21/12/2010		Raise a medical company's interest for TERESA.		
34	TERESA contents presentation to the potential partners for the advisory board	IK4-Ikerlan		12/01/2011		ALSTOM WIND, wind turbines manufacturer.		
35	TERESA contents presentation to the potential partners for the	IK4-Ikerlan		13/01/2011		Company FAGOR home appliances.		

	advisory board							
36	Presentation of TERESA ideas at meeting of ESCRYPT with potential Turkish customers. Raise a government customer's interest for TERESA.	Escrypt		14/01/2011		Visitation of potential customers of the Government, Nutrition domain (industry and private university).		
37	TERESA contents presentation to the potential partners for the advisory board	IK4-Ikerlan		14/01/2011		Company Orona, elevator manufacturer.		
38	Provide information about the idea of TERESA, Contact Smart Meter companies	USiegen		10/02/2011	Essen, Germany	E-World		
39	Invited talk about embedded security challenges. Discussions with interested companies (IT and communication) about TERESA project, about ongoing research and work in the domain of embedded security.	Escrypt		10/02/2011	Berlin Germany	EICT "IT-Sicherheit zwischen Regulierung und Innovation", approx. 200 people from communication domain and government		
40	Illustration of TERESA ideas and procedure to several companies of different domains. Illustration of ESCRYPT competence and potential interest in outcomes of TERESA. Raise the interest of some embedded device manufacturer with need in IT Security from different domains for TERESA during a security workshop Prospects are interested in TERESA results since there is a need to simplify the integration of IT security in their design process, as it is not their core business.	Escrypt		1-2/03/2011	Nürnberg Germany	Embedded World 2011 Fair and Conference,		
41	Discussions with medical eletronic device manufacturers and system integrators about the development process in the medical domain, which is very structured and often regulated. According to the prospects, a TERESA-like approach is extremely interesting since IT-Security is difficult to handle for manufacturers since this topic is not their core business. Meetings with several prospects and potential customers of ESCRYPT.	Escrypt		23/03/2011	Stuttgart Germany	European trade fair for medical technology "MEDTEC Europe",		
42	Objectives of TERESA have been discussed with potential customer, Raise an automotive company's	Escrypt		28/03/2011		Raise an automotive company's interest for TERESA		

	interest for TERESA							
43	Send paper to MDPLE 2011 Conference: Towards the Variability of S&D Patterns	IK4-Ikerlan		04/04/2011		MDE Community		
44	Safety Industrial application presentation of Safe4Rail application	IK4-Ikerlan		05/04/2011	Vienna Austria	TU Wien – Vienna University of Technology		
45	Safety Industrial application presentation of Safe4Rail application	IK4-Ikerlan		15/04/2011		IKUSI - Information and Communication Technology.		
46	Visit industry trade fair, contact exhibitors ,Provide information about the idea of TERESA	USiegen		01-02/03/2011	Nuremberg Germany	Embedded World		
47	Submission: "Modélisation à base de patrons de sécurité et de sûreté pour les systèmes embarqués contraints en ressources – l'approche TERESA"	Trialog		10/03/2011		French Neptune seminary about MDE involving the major actors in MDE both industrial and academic participants		
48	Invited talk about Industrial IT-Security and Design Methodology for security design with field programmable logic devices. Discussions with field application engineers about TERESA concept and requirements.	Escrypt		04/05/2011	Munich, Germany	Workshop IT-Security, 25 field application engineers about work in the domain of embedded security and design methodology.		
49	Project presentation on mobile security, Illustration of TERESA ideas and procedure to project partners in a project about security for android-based mobiles. Raise the interest of partners of ESCRYPT for the TERESA idea during a project presentation.	Escrypt		06/05/2011	Bochum, Germany			
50	According to the prospects, a TERESA-like approach is interesting since IT-Security is difficult to handle for manufacturers since this topic is not their core business.	Escrypt		12/05/2011	Velbert Germany	Workshop on security locks, with applications engineers from electronic lock manufacturers. Discussion of pattern-based approach for dependable system engineering.		
51	Presentation of the TERESA approach	IRIT		17/05/2011	Paris France	French NEPTUNE days about MDE, French MDE academia and Industrial community		
52	Objectives of TERESA have been discussed with potential customers during a meeting for a joint project on secure and safe system design. Raise interest for TERESA.	Escrypt			Munich, Germany	potential customers in avionics in		
53	Publication: Vers une Technique de Développement de Patrons de Sécurité et de Fiabilité pour les	IRIT-Trialog		06/2011	France	Journal: Génie Logiciel, GL & IS. N°97. Meudon - France, Juin 2011. French MDE academia and industrial community – TERESA approach is presented.		

	Systèmes Embarqués Contraints en Ressources. p53-58							
54	Discussion with engineers from an automotive electronic manufacturer about pattern-/ repository-based security design.	Escrypt		06/06/2011	Neuss, Germany	Applied IT-Security Workshop		
55	Contacting stakeholders of the metrology domain	USiegen		07/06/2011		BSI CC-Profile Workshop, Meter Manufacturers		
56	Safety Industrial application presentation of Safe4Rail application	IK4-Ikerlan		08/06/2011		Traintic – Spin-off of CAF, working in the Railway sector		
57	Contacting stakeholders of the metrology domain and publishing the TERESA idea	USiegen		08/06/2011		Smart Meter Gateway Certification workshop, Meter Manufacturers, Certification Bodies		
58	Discussions with several people from the "Connected Life" domain about structured and pattern-driven security engineering	Escrypt		30/06/2011	Cologne, Germany	Conlife-Conference, among engineers and managers of companies from the domain of connected living (e.g., consumer electronics, ambient assisted living, smart metering).		
59	Safety Industrial application presentation: Safe4Rail application	IK4-Ikerlan		11/07/2011		Alstom Wind – Wind Turbines manufacturer.		
60	Safety Industrial application presentation: Safe4Rail application	IK4- IK4-Ikerlan		18/07/2011		CAF– Train manufacturer		
61	Presentation of the TERESA approach	IK4-Ikerlan		25/07/2011	Trento Italy	ARTIST Network of excellence community, Advanced School on ICT for Future Energy Systems		
62	Discussion with participants in the domain eMobility regarding pattern-based security engineering, Raise interest for TERESA.	escrypt		15/08/2011		Workshop at Federal Ministry of Economics		
63	Towards variability support for security and dependability patterns: a case study	IRIT		22/08/2011	Munich Germany	MAPLE workshop (accompanying event of SPLC conference, Software Product Line community		
64	Towards a Unified Meta-model for Resources-Constrained Embedded Systems	IRIT		01/09/2011		IEEE communication, SEAA conference		
65	Host the 2nd S&D4RCES workshop (accompanying event of SAFECOMP conference)	IRIT		20-24/08/2011		Safety , Reliability and Security community, Security Engineering Forum		
66	Presentation: Importance of the correct integration of security features into embedded systems applications	USiegen		20-24/09/2011		S&D4RCES workshop in conjunction with the Safecomp 2011 conference, Security Experts from different domains		
67	Meeting with global player in automation. According to the prospects, a TERESA-like approach is interesting since IT-Security is difficult to handle for manufacturers since this topic is not their core business.	escrypt		22/09/2011		Development engineers and responsibles from a global leading company in automation about pattern-/ repository-based security design.		
68	Presenation Paper "Analysis of the SYM2 Smart Meter Secure Software Download using formal methods reasoning	SIT		22/09/2011		SAFECOMP 2011 - S&D4RCES		
69	Invited talk about Safety	escrypt		26/09/2011	Stuttgart,	EUROFORUM, approx.. 10		

	and Security design. Discussions with attendees (mostly engineers) about TERESA concept and requirements.				Germany	engineers about work in the domain of embedded safety and security and design methodology.		
70	Discussion with software developers from a worldwide leading embedded OS company about pattern-/ repository-based security design.	escrypt		28/09/2011		Embedded OS provider		
71	Invited talk about Safety and Security design. Discussion with attendees about TERESA principles. Raise interest for TERESA.	escrypt		12/10/2011	Magdeburg, Germany	MAHREG Symposium		
72	Enforcing S&D Pattern Design in RCES with Modeling and Formal Approache	IRIT-Trialog-SIT		18/10/2011		Models Conference, ACM /IEEE, International MDE- UML-DSL community		
73	A Metamodel for Representing Safety LifeCycle Development Process	IRIT		25/10/2011		ICSEA, Process Model community		
74	Discussion with development engineers and responsibles from a global leading company mobile phone production. Raise interest for TERESA.	Escrypt		08/11/2011		Mobile phone manufacturer		
75	Technical discussion about integration of pattern-based security design methodology with hardware-based security implementations, Discussion about potential links between EVITA and TERESA with involved engineers.	Escrypt		23/11/2011	Germany	EVITA presentation event		
76	Talk about security requirements in the metering domain and discussion with smart meter manufacturers. Raise interest for TERESA by illustrating the benefits of reducing development costs and simplifying the certification process.	Escrypt		29-30/11/2011	Essen, Germany	Think Smart – Security in Metering Conference		
77	Presentation "Data Protection in Legal Metrology and Related Challenges"	USiegen		01/12/2011		PTB Workshop, International meter manufacturers, metrology domain experts		
78	Presentation: From PIAs to Engineering Practices	Trialog		25/01/2012	Brussels, Belgium	Workshop on Privacy Impact Assessment: Past, Present, and Future, at CPDP 2012		
79	Presentation of Teresa	escrypt		03/02/2012	Malaga Spain	SecFutur Meeting		
80	Presentation	escrypt		15/02/2012	Munich Germany	Elektronik Automotive Congress		
81	Introduction to TERESA approach to ETAS, Discussion about optimizing tools with the TERESA approach	escrypt		26/02/2012		Embedded World		
82	Presentation: Towards a Security and	IRIT		01/2012	Vienna, Austria	Software Quality. Process Automation in Software		

	Dependability Pattern Development Technique for Resource Constrained Embedded Systems					Development - 4th International Conference, SWQD 2012, Test and Agile development community		
83	Discussion with Mr. Norbert Zisky from the PTB in Germany about the feasibility of the TERESA MDE approach in the metrology domain	SIT		03/02/2012	Malaga Spain	Discussion with PTB in Germany about the feasibility of the TERESA MDE approach in the metrology domain		
84	Publication and presentation: Herausforderungen und Lösungsansätze zur Integration von Safety und Security aus der Perspektive Formaler Methoden.	SIT		28/02/2012	Clausthal-Zellerfeld Germany	Zertifizierung und modellgetriebene Entwicklung sicherer Software (ZeMoSS Workshop),		
85	Discussion of the goal, and future steps of the TERESA Project Validation of the current TERESA work and direction	Trialog		03/02/2012	Malaga Spain	Teresa advisory board memebers		
86	Presentation of the TERESA project. Participation to the board of the S.E.F. Promotion of TERESA	Trialog		02/02/2012	Malaga, Spain	Security Engineering Forum kick off meeting,		
87	Publication and presentation: Redefining Security Engineering	SIT		07/05/2012	Istanbul Turkey	5th International Conference on New Technologies, Mobility and Security (NTMS)		
88	Presentation of Teresa and further discussion about approach and expected benefits (KPIs)	escrypt		27/06/ 2012		Management of EMH metering GmbH & Co. KG		
89	Repository Training: Organization of 1 day meeting to discuss opportunities to use the results of the TERESA project by the SIRSEC consortium and vice-versa	IRIT		06/ 2012	Toulouse France	SIRSEC consortium		
90	Introduction of Teresa to ELSTER Messtechnik GmbH, Presentation of Teresa and further discussion about approach and expected benefits (KPIs)	SIT		16/07/2012		ELSTER Management		
91	First discussion with ETAS about TERESA approach.	escrypt		25/07/ 2012		ETAS product manager and engineers		
92	Publication and presentation: A Proven Pattern Integration Process.	IRIT		11/07/2012	Kloster Irsee, Germany	17th European Conference on Pattern Languages of Programs (Europlop 2012), Pattern community in Europe		
93	Visit at EMH metering GmbH & Co. KG, Introduction of the TERESA approach and discussion about engineering process and demonstrator use case	USiegen		27 Jun 2012		EMH engineers and developers		
94	Visit at elster instromet, Introduction of the TERESA approach and discussion about engineering process and demonstrator use case	USiegen		16/07/2012		Elster instromet engineers and developers		

95	Meeting with EMH, Presentation of the TERESA project	Trialog		27/06/2012		EMH management		
96	Meeting with Elster Instromet	Trialog		16/07/2012		Collection of the expectation, comments, feedback of the stakeholders		
97	Introduction of Teresa to ETAS GmbH, Presentation of Teresa and further discussion about approach and expected benefits (KPIs)	escrypt		08/08/2012		Product Manager (Gupta Manabendra) and Engineers		
98	Discussion on EMF model repositories	escrypt		09/10/2012		Mr. Christof Hammel of Bosch		
99	Publication and presentation: A Model-Driven Engineering Framework for Fault Tolerance in Dependable Embedded Systems Design	IRIT		05/09/ 2012		Euromicro Conference on Software Engineering and Advanced Applications (SEAA) conference, Izmir, Turkey, IEEE communication		
100	Publication and presentation: Safety Lifecycle Development Process Modeling for Embedded Systems - Example Railway Domain	IRIT		27/09/2012	Pisa Italy	Software Engineering for Resilient Systems (SERENE), the ERCIM Working Group on Software Engineering for Resilient Systems		
101	SagemCom Meeting, Presentation of the TERESA project Collection of the interest, feedback, and possible collaboration with SagemCom	Trialog		26/10/2012		Head of the R&D in the Energy Domain of SagemCom		
102	Panel Discussion “Smart Meter Gateway”, Discussion about different topics	escrypt		20/11/2012		Audience related to secure communication for mobile networks.		
103	Presentation: Pattern based Trusted Engineering for a Smart Meter Gateway	escrypt, USiegen		21/11/2012	Dusseldorf, Germany	Thinksmart 2012: Secure Communication for Mobile Networks, Audience related to secure communication for mobile networks.		
104	Organization of one day meeting in Toulouse with Obeo to discuss opportunities to disseminate the results of the TERESA project under the Eclipse community.	IRIT		11/ 2012		MDE and Eclipse tools community		
105	Publication and presentation: Supporting Security Engineering at Design Time with Adequate Tooling	SIT		05/12/2012	Nicosia, Cyprus	The 15th IEEE International Conference on Computational Science and Engineering (CSE 2012)		
106	Publication and presentation: Security Engineering Based on Structured Formal Reasoning	SIT		14/12/2012		RISE Workshop on Redefining and Integrating Security Engineering (RISE'12), Washington DC, USA		

Use and Dissemination of Foreground: Section B (Confidential)

Part B1

Project TERESA has not produced patents, trademarks, registered designs.

Part B2

Type of Exploitable Foreground[5]	Item	Description of exploitable foreground	Con-fiden-tial	Fore-seen embar-go date	Exploitable product(s) or measure(s)	Sector(s) of application [6]	Timetable, commercial or any other use	Patents or other IPR exploit-tation (licences)	Owner & Other Beneficiary(s) involved
General advancement of knowledge	A	Pattern Based System Engineering Theoretical Foundation: Repository centric methodology	No	No	Methodology, Set of languages.	All embedded domains	Dissemination and further research	None	IRIT
General advancement of knowledge	B	Pattern Based System Engineering Theoretical Foundation: Formal validation approach	No	No	Guidelines	All embedded domains	Dissemination and further research	None	Fraunhofer SIT
Commercial exploitation of R&D results	C	Example process for railways	No	No	Prototype toolset applied to specific IK4-Ikerlan SAFE4Rail	Railways	Corporate use of TERESA reusability approach	None	IK4-Ikerlan
Commercial exploitation of R&D results	D	Example process for smart metering	No	No	Prototype toolset applied to specific process for development of CC protection profile for secure gateways in smart metering	Smart metering	Future development of secure gateways in smart metering	None	USiegen, escrypt
General advancement of knowledge	E	Guidelines for RCES domains	No	No	Guidelines	All embedded domains	Dissemination and further development	None	IRIT, Trialog, Escrypt, USiegen

[19] A drop down list allows choosing the type of foreground: General advancement of knowledge, Commercial exploitation of R&D results, Exploitation of R&D results via standards, exploitation of results through EU policies, exploitation of results through (social) innovation.

[6] A drop down list allows choosing the type sector (NACE nomenclature) : http://ec.europa.eu/competition/mergers/cases/index/nace_all.html

Type of Exploitable Foreground[5]	Item	Description of exploitable foreground	Con-fiden-tial	Fore-seen embar-go date	Exploitable product(s) or measure(s)	Sector(s) of application [6]	Timetable, commercial or any other use	Patents or other IPR exploit-tation (licences)	Owner & Other Beneficiary(s) involved
Commercial exploitation of R&D results	F	Tools for Pattern Based System Engineering	No	No	GAYA, NARAVAS, ARABION, TIQUEO tools	All embedded domains	Dissemination and further development	None	IRIT
Commercial exploitation of R&D results	G	Access tools	No	No	Access tool for railway and metering use case and for other domains	All embedded domains	Dissemination and further development	None	Trialog, escrypt, USiegen
General advancement of knowledge	H	Example patterns	No	No	S&D patterns	All embedded domains	Dissemination and further development	None	IRIT, Trialog, escrypt, USiegen, IK4-Ikerlan, SIT

Repository Centric Methodology (Item A)

Purpose	Pattern Based System Engineering Theoretical Foundation: Repository centric methodology • Pattern modelling process • Repository specification process • Pattern integration process • Set of languages (pattern, properties, process, repository)
How the foreground might be exploited, when and by whom	The main exploitation will be to foster the use of the PBSE repository centric methodology by making the technology available in the academic community first and then in the industry community. This exploitation will be carried out by IRIT and will take place in 2013
IPR exploitable measures taken or intended	Not relevant
Further research necessary, if any	Further research is foreseen in the following area: DSL languages, processes, pattern composition.
Potential/expected impact (quantify where possible)	Consolidation and adoption of PBSE repository centric methodology

Formal Validation Approach (Item B)

Purpose	Pattern Based System Engineering Theoretical Foundation: Formal validation approach • Validation method based on the SeMF framework • Application on a number of patterns

	• Guidelines
How the foreground might be exploited, when and by whom	Training and dissemination of formal validation approach (Fraunhofer SIT). This exploitation will be carried out by Fraunhofer SIT and will take place in 2013
IPR exploitable measures taken or intended	If appropriate, patents and licences will be submitted to prepare for exploitation with industry partners.
Further research necessary, if any	Further research is foreseen in enhancing the SeMF framework
Potential/expected impact (quantify where possible)	Contribution and adoption of validation approach based on the SeMF framework

Example process for railways (Item C)

Purpose	Example process for railways
How the foreground might be exploited, when and by whom	A two phase approach is planned: • Development and reuse of dependable patterns, using a repository already used in the (safety) engineering processes. • Development and reuse of dependable patterns using TERESA repository or a customized version that integrates with the safety engineering process of a given customer This action will be carried out by IK4-Ikerlan in 2013.
IPR exploitable measures taken or intended	Not relevant
Further research necessary, if any	Not relevant
Potential/expected impact (quantify where possible)	Practice of S&D reuse in the railways domain

Engineering process for Metering (Item D)

Purpose	Engineering process for Metrology
How the foreground might be exploited, when and by whom	Applying TERESA approach in smart grid and metrology research projects (USiegen, Trialog) Consulting in covered domains to apply TERESA guidelines for S&D reuse (Trialog, escrypt) Consulting in other domains to apply TERESA guidelines for S&D reuse (Trialog, escrypt).

IPR exploitable measures taken or intended	Not relevant
Further research necessary, if any	Further research is needed to integrate the artefacts needed for a common criteria protection profile.
Potential/expected impact (quantify where possible)	Practice of S&D reuse in the metrology domain

Guidelines for RCES domains (Item E)

Purpose	Guidelines for other domains. Example of automotive process
How the foreground might be exploited, when and by whom	Consulting in other domains to apply TERESA guidelines for S&D reuse (Trialog, escrypt).
IPR exploitable measures taken or intended	Not relevant
Further research necessary, if any	Further research in the area of domain specific reuse.
Potential/expected impact (quantify where possible)	Practice of S&D reuse in additional application domain

Tools for pattern edition (Item F)

Purpose	Tools for pattern edition • Gaya : repository • Naravas : edition of process • Arabion: edition or patterns • Tiqueo: edition of S&D properties and constraints
How the foreground might be exploited, when and by whom	Enhancing the maturity of pattern edition tools by creating an academic community to populate the repository and to enhance tool set (IRIT) in 2013
IPR exploitable measures taken or intended	Not relevant
Further research necessary, if any	Further extensions to editing tools
Potential/expected impact (quantify where possible)	Creation of the conditions for a security engineering ecosystem.

Access tools (Item G)

Purpose	Access tools for the two case studies • Access tools for Safe4 Rail • Access tools for secure gateway for smart metering
How the foreground might be exploited, when and by whom	Access tools for specific development environments (Trialog, escrypt) Further tools (Trialog, escrypt).
IPR exploitable measures taken or intended	Not relevant
Further research necessary, if any	Supporting tools to new advance in engineering.
Potential/expected impact (quantify where possible)	Creation of the conditions for a security engineering ecosystem.

Example patterns (Item H)

Purpose	Example S&D patterns • 20 system level patterns, • 25 architecture level patterns • 14 design level patterns
How the foreground might be exploited, when and by whom	Creation of an academic community to populate the repository and to enhance tool set (IRIT)
IPR exploitable measures taken or intended	Not relevant
Further research necessary, if any	S&D pattern representation
Potential/expected impact (quantify where possible)	Creation of the conditions for a security engineering ecosystem.

4.4 Report on Societal Implications

Replies to the following questions will assist the Commission to obtain statistics and indicators on societal and socio-economic issues addressed by projects. The questions are arranged in a number of key themes. As well as producing certain statistics, the replies will also help identify those projects that have shown a real engagement with wider societal issues, and thereby identify interesting approaches to these issues and best practices. The replies for individual projects will not be made public.

A General Information (completed automatically when Grant Agreement number is entered.	
Grant Agreement Number:	ICT-248410
Title of Project:	Trusted Computing Engineering for Resource Constrained Embedded Systems Applications
Name and Title of Coordinator:	Antonio Kung, Director

B Ethics	
1. Did your project undergo an Ethics Review (and/or Screening)? • If Yes: have you described the progress of compliance with the relevant Ethics Review/Screening Requirements in the frame of the periodic/final project reports? Special Reminder: the progress of compliance with the Ethics Review/Screening Requirements should be described in the Period/Final Project Reports under the Section 3.2.2 *'Work Progress and Achievements'*	No
2. Please indicate whether your project involved any of the following issues (tick box):	NO
Research on Humans	
• Did the project involve children?	
• Did the project involve patients?	
• Did the project involve persons not able to give consent?	
• Did the project involve adult healthy volunteers?	
• Did the project involve Human genetic material?	
• Did the project involve Human biological samples?	
• Did the project involve Human data collection?	
Research on Human embryo/foetus	
• Did the project involve Human Embryos?	
• Did the project involve Human Foetal Tissue / Cells?	
• Did the project involve Human Embryonic Stem Cells (hESCs)?	
• Did the project on human Embryonic Stem Cells involve cells in culture?	
• Did the project on human Embryonic Stem Cells involve the derivation of cells from	

Embryos?	
Privacy	
• Did the project involve processing of genetic information or personal data (eg. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)?	
• Did the project involve tracking the location or observation of people?	
Research on Animals	
• Did the project involve research on animals?	
• Were those animals transgenic small laboratory animals?	
• Were those animals transgenic farm animals?	
• Were those animals cloned farm animals?	
• Were those animals non-human primates?	
Research Involving Developing Countries	
• Did the project involve the use of local resources (genetic, animal, plant etc)?	
• Was the project of benefit to local community (capacity building, access to healthcare, education etc)?	
Dual Use	
• Research having direct military use	No
• Research having the potential for terrorist abuse	

C Workforce Statistics

3. Workforce statistics for the project: Please indicate in the table below the number of people who worked on the project (on a headcount basis).

Type of Position	Number of Women	Number of Men
Scientific Coordinator		7
Work package leaders	1	6
Experienced researchers (i.e. PhD holders)	3	6
PhD Students		3
Other	2	4

4. How many additional researchers (in companies and universities) were recruited specifically for this project?	3
Of which, indicate the number of men:	3

D Gender Aspects

5. Did you carry out specific Gender Equality Actions under the project?	○ X	Yes No

6. Which of the following actions did you carry out and how effective were they?

	Not at all effective				Very effective
❑ Design and implement an equal opportunity policy	○	○	○	○	○
❑ Set targets to achieve a gender balance in the workforce	○	○	○	○	○
❑ Organise conferences and workshops on gender	○	○	○	○	○
❑ Actions to improve work-life balance	○	○	○	○	○
○ Other:					

7. Was there a gender dimension associated with the research content – i.e. wherever people were the focus of the research as, for example, consumers, users, patients or in trials, was the issue of gender considered and addressed?

○ Yes- please specify

X No

E Synergies with Science Education

8. Did your project involve working with students and/or school pupils (e.g. open days, participation in science festivals and events, prizes/competitions or joint projects)?

○ Yes- please specify

X No

9. Did the project generate any science education material (e.g. kits, websites, explanatory booklets, DVDs)?

X Yes- please specify: Youtube movies

○ No

F Interdisciplinarity

10. Which disciplines (see list below) are involved in your project?

X Main discipline[7]: 2.2 Research and Innovation

○ Associated discipline7: | ○ Associated discipline7:

G Engaging with Civil society and policy makers

11a Did your project engage with societal actors beyond the research community? *(if 'No', go to Question 14)*	○ X	Yes No

11b If yes, did you engage with citizens (citizens' panels / juries) or organised civil society (NGOs, patients' groups etc.)?

○ No
○ Yes- in determining what research should be performed
○ Yes - in implementing the research
○ Yes, in communicating /disseminating / using the results of the project

11c In doing so, did your project involve actors whose role is mainly to organise the dialogue with citizens and organised civil society (e.g. professional mediator; communication company, science museums)?	○ ○	Yes No

12. Did you engage with government / public bodies or policy makers (including international organisations)

○ No
○ Yes- in framing the research agenda
○ Yes - in implementing the research agenda
○ Yes, in communicating /disseminating / using the results of the project

13a Will the project generate outputs (expertise or scientific advice) which could be used by policy makers?

○ Yes – as a **primary** objective (please indicate areas below- multiple answers possible)
○ Yes – as a **secondary** objective (please indicate areas below - multiple answer possible)
○ No

13b If Yes, in which fields?

[7] Insert number from list below (Frascati Manual).

Agriculture Audiovisual and Media Budget Competition Consumers Culture Customs DevelopmentEconomic and Monetary Affairs Education, Training, Youth Employment and Social Affairs		Energy Enlargement Enterprise Environment External Relations External Trade Fisheries and Maritime Affairs Food Safety Foreign and Security Policy Fraud Humanitarian aid		Human rights Information Society Institutional affairs Internal Market Justice, freedom and security Public Health Regional Policy Research and Innovation Space Taxation Transport	

13c If Yes, at which level?

- ○ Local / regional levels
- ○ National level
- ○ European level
- ○ International level

H Use and dissemination

14. How many Articles were published/accepted for publication in peer-reviewed journals?		26
To how many of these is open access[8] provided?		0
How many of these are published in open access journals?		
How many of these are published in open repositories?		
To how many of these is open access not provided?		
Please check all applicable reasons for not providing open access:		
❑ publisher's licensing agreement would not permit publishing in a repository ❑ no suitable repository available ❑ no suitable open access journal available ❑ no funds available to publish in an open access journal ❑ lack of time and resources ❑ lack of information on open access ❑ other[9]: ……		X
15. How many new patent applications ('priority filings') have been made? ("Technologically unique": multiple applications for the same invention in different jurisdictions should be counted as just one application of grant).		0
16. Indicate how many of the following Intellectual Property Rights were applied for (give number in each box).	Trademark	0
	Registered design	0
	Other	0
17. How many spin-off companies were created / are planned as a direct result of the project?		0
Indicate the approximate number of additional jobs in these companies:		

18. Please indicate whether your project has a potential impact on employment, in comparison with the situation before your project:

[8] Open Access is defined as free of charge access for anyone via Internet.

[9] For instance: classification for security project.

X	Increase in employment, or	X	In small & medium-sized enterprises
❑	Safeguard employment, or	❑	In large companies
❑	Decrease in employment,	❑	None of the above / not relevant to the project
❑	Difficult to estimate / not possible to quantify		

19. For your project partnership please estimate the employment effect resulting directly from your participation in Full Time Equivalent (*FTE = one person working fulltime for a year*) jobs:	Indicate figure:
Difficult to estimate / not possible to quantify	X

I	Media and Communication to the general public		
20. As part of the project, were any of the beneficiaries professionals in communication or media relations?			
	○ Yes	X	No
21. As part of the project, have any beneficiaries received professional media / communication training / advice to improve communication with the general public?			
	○ Yes	X	No
22 Which of the following have been used to communicate information about your project to the general public, or have resulted from your project?			
❑	Press Release	❑	Coverage in specialist press
❑	Media briefing	❑	Coverage in general (non-specialist) press
❑	TV coverage / report	❑	Coverage in national press
❑	Radio coverage / report	❑	Coverage in international press
❑	Brochures /posters / flyers	❑	Website for the general public / internet
X	DVD /Film /Multimedia	X	Event targeting general public (festival, conference, exhibition, science café)
23 In which languages are the information products for the general public produced?			
❑	Language of the coordinator	X	English
❑	Other language(s)		

***Question F-10*:** Classification of Scientific Disciplines according to the Frascati Manual 2002 (Proposed Standard Practice for Surveys on Research and Experimental Development, OECD 2002):

Fields of science and technology

1. Natural Sciences

1.1 Mathematics and computer sciences [mathematics and other allied fields: computer sciences and other allied subjects (software development only; hardware development should be classified in the engineering fields)]

1.2 Physical sciences (astronomy and space sciences, physics and other allied subjects)

1.3 Chemical sciences (chemistry, other allied subjects)

1.4 Earth and related environmental sciences (geology, geophysics, mineralogy, physical geography and other geosciences, meteorology and other atmospheric sciences including climatic research, oceanography, vulcanology, palaeoecology, other allied sciences)

1.5 Biological sciences (biology, botany, bacteriology, microbiology, zoology, entomology, genetics, biochemistry, biophysics, other allied sciences, excluding clinical and veterinary sciences)

2 Engineering and technology

2.1 Civil engineering (architecture engineering, building science and engineering, construction engineering, municipal and structural engineering and other allied subjects)

2.2 Electrical engineering, electronics [electrical engineering, electronics, communication engineering and systems, computer engineering (hardware only) and other allied subjects]

2.3. Other engineering sciences (such as chemical, aeronautical and space, mechanical, metallurgical and materials engineering, and their specialised subdivisions; forest products; applied sciences such as geodesy, industrial chemistry, etc.; the science and technology of food production; specialised technologies of interdisciplinary fields, e.g. systems analysis, metallurgy, mining, textile technology and other applied subjects)

3. Medical Sciences

3.1 Basic medicine (anatomy, cytology, physiology, genetics, pharmacy, pharmacology, toxicology, immunology and immunohaematology, clinical chemistry, clinical microbiology, pathology)

3.2 Clinical medicine (anaesthesiology, paediatrics, obstetrics and gynaecology, internal medicine, surgery, dentistry, neurology, psychiatry, radiology, therapeutics, otorhinolaryngology, ophthalmology)

3.3 Health sciences (public health services, social medicine, hygiene, nursing, epidemiology)

4. Agricultural sciences

4.1 Agriculture, forestry, fisheries and allied sciences (agronomy, animal husbandry, fisheries, forestry, horticulture, other allied subjects)

4.2 Veterinary medicine

5. Social sciences

5.1 Psychology

5.2 Economics

5.3 Educational sciences (education and training and other allied subjects)

5.4 Other social sciences [anthropology (social and cultural) and ethnology, demography, geography (human, economic and social), town and country planning, management, law, linguistics, political sciences, sociology, organisation and methods, miscellaneous social sciences and interdisciplinary , methodological and historical S1T activities relating to subjects in this group. Physical anthropology, physical geography and psychophysiology should normally be classified with the natural sciences].

6. Humanities

6.1 History (history, prehistory and history, together with auxiliary historical disciplines such as archaeology, numismatics, palaeography, genealogy, etc.)

6.2 Languages and literature (ancient and modern)

6.3 Other humanities [philosophy (including the history of science and technology) arts, history of art, art criticism, painting, sculpture, musicology, dramatic art excluding artistic "research" of any kind, religion, theology, other fields and subjects pertaining to the humanities, methodological, historical and other S1T activities relating to the subjects in this group]

2. FINAL REPORT ON THE DISTRIBUTION OF THE European Union FINANCIAL CONTRIBUTION

This report shall be submitted to the Commission within 30 days after receipt of the final payment of the European Union financial contribution.

Report on the distribution of the European Union financial contribution between beneficiaries

Name of beneficiary	Final amount of EU contribution per beneficiary in Euros
1.	
2.	
n	
Total	