1 Publishable Summary

1.1 Description of Project Context and Objectives

1.1.1 Context

Resource Constrained Embedded systems (RCES) are today integrated in increasingly more sophisticated applications. They require more security and dependability, they require more trust. This complexity is due to integration and functional considerations. First RCES are integrated into systems involving complex supply chains with many different business stakeholders focusing on different subsystems (e.g. processors, ASIC, operating system, middleware, application component) and different integration levels. Secondly, RCES are often used in multipurpose applications involving multiple possibly independent applications. We are switching 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:

- We can find them everywhere, in different application sectors (automotive, aerospace, home, etc.), in different form factors (standalone systems, peripheral subsystems to main computing system, etc.), in many different devices (sensor, automotive electronic control unit, intelligent switches, home appliances e.g. washing machine drum control, meters, ...)
- Computing resources e.g. memory, tasks, buffers are statically determined. For instance the entities managed by the underlying operating systems are typically predetermined. For instance the OSEK-VDX RTOS (www.osek-vdx.org) standard 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). The figure below shows the process used in the automotive industry as recommended in the Autosar initiative (www.autosar.org) to generate the software elements of an electronic control unit (ECU). It includes a configuration phase and a generation phase. Other application sectors will also use similar configuration and build approaches. They could be often simpler, sometimes involving a manual process.
- 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 involving 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 cost and therefore use advanced engineering disciplines (automatic code generation, model-driven developments).

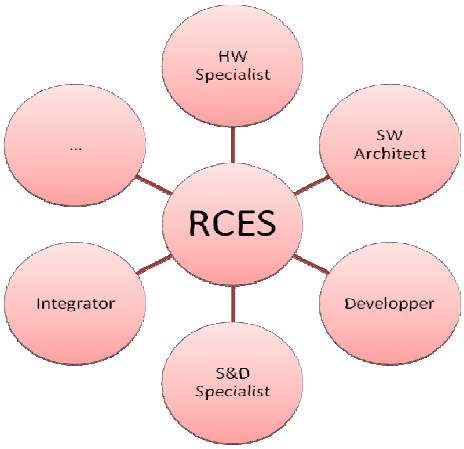

Figure 1 : RCES as a synergy of business

1.1.2 Objectives

The goal of TERESA is to define, demonstrate and validate an engineering discipline for trust that is adapted to resource constrained embedded systems. We define trust 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:

- Application sector trust models are defined as profiles (e.g. UML, SysML profiles), based on a common trust meta-model
- Security and dependability platform independent patterns are identified and defined for each application sectors (some patterns could be used by several application sectors)
- Formal properties on security and dependability are defined and validated for patterns belonging to application sectors requiring that level of assurance
- Platform dependent implementation of the patterns are of the patterns are guided with very precise requirements

TERESA has the following objectives:

- Provide guidelines for the specification of sector specific RCES trusted computing engineering. Software process engineers in a given sector can then use the guidelines to define a trusted computing engineering process that is integrated with the software engineering process used in their RCES sector.
- Define a trusted computing engineering approach that is suited to the following sectors: Automotive, Home control, Industry control and Metering sectors

1.2 Results So Far

1.2.1 Use Case Application Viewpoint, Collection, Challenges and Common Understanding

At the beginning of the project, a set of application use cases has been collected. This will serves as input for future tasks in other work packages as well as a manner to reach a common understanding between partners. A high level template of patterns has been defined according to the state of the art as well as use case application template based on V-Modell XT of the German government as a reference to unify criteria. The use cases collected include information on use of pattern, actors, roles and tasks involved in the domain specific engineering process.

The various templates try to also fit some requirements of formal validation by providing information on the pre-condition, knowledge of agents involved in the use case.

By the same time, an advanced study has been made about the state-of-the-art in three issues that were identified within the context of TERESA as being of a long term interest from a scientific perspective as well as for Security and Dependability (S&D) engineering of embedded systems. The first one is the enforcement of S&D in RCES by model-driven engineering; the second is the usefulness of existing approaches for the integration and composition of systems (e.g. cryptographic protocols) of S&D patterns in the context of security engineering for RCES; the last one is the investigation of S&D related requirements of the metering sector which are candidates to be formalized. An examination of the conformity assessment procedures which could be applied to new metering devices developed using a trusted design process as also be carried. As a result a Roadmap has been presented for these challenges.

1.2.2 Requirements and the TERESA Vision

As a real security engineering process does not exist, the partners have to come up with requirements against several subjects that are totally integrated in the TERESA vision.

S&D requirements are usually fulfilled with a limited set of solutions. The use of patterns can ease the integration of one of these solutions due to reusability, but this has an impact in the engineering process, that have to be completely redesigned to support efficiently the new paradigm.

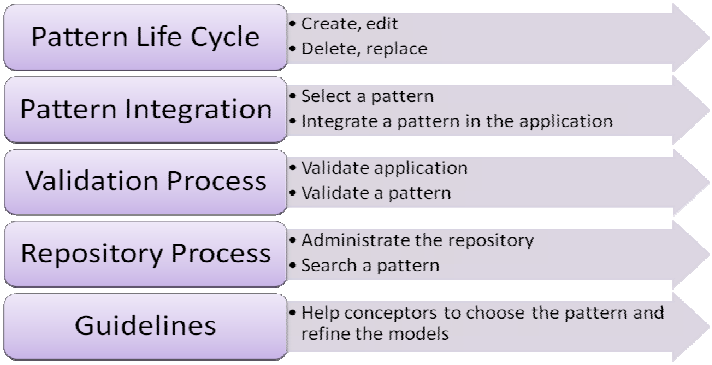

Figure 2 : Various processes in a pattern-based application development

Pattern-based application development needs several kinds of processes. In TERESA we mainly focus the work around several processes:

- The Pattern Life Cycle process corresponds to all the tasks related to the pattern development (create, update, delete, etc). At the end, the pattern is stored in a repository.
- The goal of ***Pattern Integration process*** consists to plug in a pattern in an application. For this, in function of S&D properties, the security engineer can require all patterns stored in the repository which meet his needs. Then, thanks to a model transformation, the pattern is integrated in the application model.
- The ***Validation process*** is transversal and interacts with the pattern life cycle and pattern integration processes. At each step of these processes, it is possible to validate a pattern or an application from an S&D point of view.
- The ***Repository process*** manages the pattern repository and provides a pattern search mechanism.
- At last, ***Guidelines*** are needed in order to help designers during the pattern life cycle and pattern integration processes.

The TERESA vision will consist in developing application by pattern construction. The TERESA vision is based on two main streams centralised around a repository. The repository provides S&D patterns which can be use during the application development. In order to design patterns, some guidelines help the security specialists. At the end of the pattern development, formal validation guarantees that the pattern achieved S&D properties

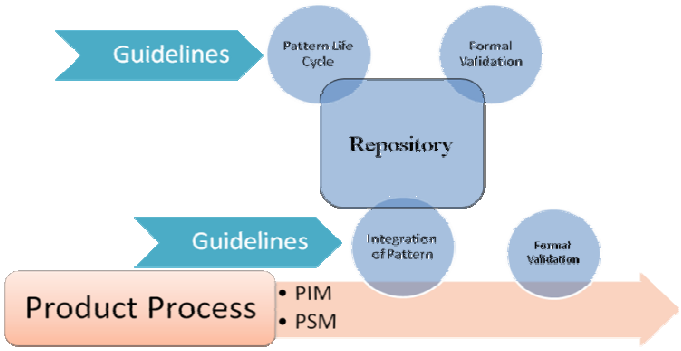

Figure 3 : The TERESA Vision

From that, and based on Fault Propagation Model, a Trust Model and a S&D Properties Model, the partners come up with a list of requirements from the engineer viewpoint, the engineering process viewpoint concerning each process, the repository, the pattern and artefact definition and the structure of a pattern including validation and verification issues.

1.3 Expected Results

Category	Today	Planned Innovation
Engineering separation of concern	Growing complexity of applications makes the integration of security and dependability an issue, as not all RCES application designers have the overall expertise.	TERESA will define an engineering approach based on a repository of models and patterns. It ensures separation of engineering roles between (1) application experts, (2) S&D experts and (3) MDE experts
	There are RCES cases where S&D expertise is not available. This prevent application engineers to integrate S&D solutions	As the repository can be populated independently by a community of security experts and MDE experts, application engineers will be provided with ready to use S&D designs, possibly at different levels (e.g. platform independent level, platform dependent level)
	There are RCES cases where MDE expertise is not available. This prevent application engineers to take advantage of the benefits of MDE	Access to repository will be supported by tools providing application level viewpoints of the repository elements (models, patterns). In other word, the access tool will not require modeling specification expertise. These tools can provide documenting capability (i.e. the involved model is documented, or the integrated S&D pattern documented) as well as administration capability (i.e. the application designer may wish to enrich/modify a model).

Category	Today	Planned Innovation
Supporting domain specific processes	Engineering approaches based on variety of static allocation of computing resources	TERESA will define a common engineering process meta model from which domain specific engineering process models can be defined (e.g. the automotive engineering process model). This will allow when possible the reuse of common parts in processes.
	There is a wide variety of high integrity systems with assurance requirements, including formal validation requirements	Domain specific engineering process models may include different assurance capability. When formal validation is required in the process, patterns involved will be formally validated, and automated guidelines will be provided to assure the consistent transformation to platform dependent implementations.
	Wide variety of implementation cases (reuse an implementation without change, optimizing an existing implementation for resource constraint reasons, implementing for a new platform)	Different levels of engineering process allowed, including one where the S&D patterns are just considered as documented specification to be used by engineers to carry out a manual implementation.
Research	Model driven engineering is still not well established in particular for RCES applications	Study specific challenges that may help improve gaps at the level of MDE for RCES trusted computing engineering
	Integration of S&D patterns is not well supported	Study specific challenges raised by the combination of two patterns.
	Formal validation of metrology requirements is needed	Study methods for the validation of metering software regarding type approval.

1.4 For More Information

Contact the project coordinator or its deputy :

Project Coordinator :	Deputy Coordinator :
Antonio Kung, TRIALOG SA 25 rue du Général Foy, 75008 Paris, France +33 (0) 1 44 70 61 00 antonio.kung@trialog.com	Cyril Grepet, TRIALOG SA 25 rue du Général Foy, 75008 Paris, France +33 (0) 1 44 70 61 00 cyril.grepet@trialog.com

You can also following us on www.teresa-project.com