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).
- 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).

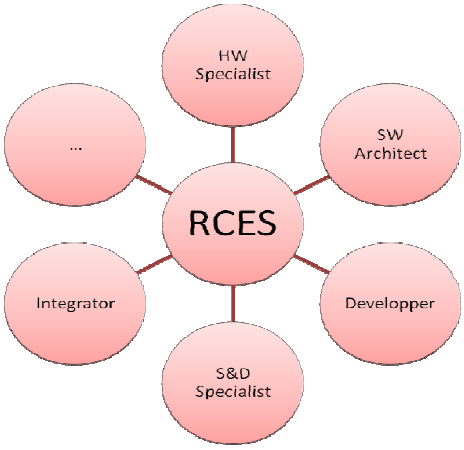

Figure 1 : RCES as a synergy of business

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 sector (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 guided with very precise requirements.

TERESA has the following objectives:

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

1.2 Results So Far

1.2.1 Case Studies

During the first year, the use cases and the partners' expertise of four domains have been used to define the requirements for the project: engineering viewpoint, process viewpoint and repository viewpoint.

Moreover, the identification of various patterns of interest has been done.

To ensure the success of the project, the decision was taken to focus the work on the Railway domain and the Metrology domain. The former has strong constraints and is well-known and the latter is increasingly prominent, but without the long history of the Railway sector. It will allow TERESA to stress its interest for both well-established and new engineering domains.

To illustrate the benefits of TERESA, two case studies have been studied in depth, including current practice and process and the improvement by TERESA practice and process: Safe4Rail and a secure electrical smart meter.

The former will be used to validate the TERESA approach from an already existing dependable system where security is taken into account, and the latter will be used to validate the improvement of the system realisation in a new kind of system.

1.2.2 Repository and Processes

Currently, the MDE approach is currently used for the Safe4Rail development, but is not used to improve a smart meter with security capabilities. A storyboard has been elaborated for both cases illustrating "one day in the life of an engineer" before and after the use of TERESA.

Both domain processes have been studied to elaborate and validate a metamodel by modelling the two processes.

This study has also permitted the identification and specification from an MDE point of view the representation of the patterns, the structure of the repository, and all the necessary information to allow the instantiation of patterns in different phases of an engineering process.

Moreover, the mock-up and a prototype of the access tool that will connect the repository to the used-in-the-process tool have been implemented from the domain engineer expectations.

1.2.3 Patterns and Formal Validation

- Since we can rely on a complete case study, a subset of patterns has been modelled. It enables the formal validation using the SEMF framework to ensure that the patterns provide the expected properties with respect to their interfaces.
- At the same time, the first guidelines document was established to help validate any patterns.

1.3 Expected Results

Category	Current	Planned Innovation
Engineering separation of concern	The 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 prevents application engineers from integrating 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 prevents application engineers from taking advantage of the benefits of MDE.	Access to the repository will be supported by tools providing application level viewpoints of the repository elements (models, patterns). In other words, 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 is documented) as well as administration capability (i.e. the application designer may wish to enrich or modify a model).
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 the 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 capabilities. 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, e.g. reuse of an implementation without change, optimizing an existing implementation for resource constraint reasons, implementing for a new platform.	Different levels of engineering process are allowed, including one where the S&D patterns are considered as a 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

For more information, contact the project co-ordinator or the project deputy co-ordinator:

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

You can also visit the TERESA website: www.teresa-project.com