Trusted Computing Engineering for Resource Constrained Embedded Systems Applications

Deliverable D8.3
Plan for Use and Dissemination Year 1

Project: TERESA
Project Number: IST-248410
Deliverable: D8.3
Title: Plan for Use and Dissemination Year 1
Version: v1.0.
Confidentiality: Confidential
Author: Cyril Grepet (Trialog)
Date: 3 December 2010

Part of the Seventh Framework Programme
Funded by the EC - DG INFSO

Table of Contents

1 Document History

Version	Status	Date
v0.1	draft	16/09/2010
v1.0	final	03/12/2010

Approval		
	Name	**Date**
Prepared	Cyril Grepet	19/11/2010
Reviewed	All Project Partners	03/12/2010
Authorised	Antonio Kung	03/1/ 2010
Circulation		
Recipient	**Date of submission**	
Project partners	19/11/2010	
European Commission	03/12/2010	

2 Executive Summary

2.1 Contact Information

No.	Consortium Partners
1	**TRIALOG (Trialog) - Co-ordinator** 25 rue du Général Foy 75008 Paris France
2	**Université de toulouse 2 – le Mirail (UTM-IRIT)** Université de Toulouse 2 - Le Mirail Département de Mathématiques-Informatique 5 allées Antonio Machado 31058 Toulouse France
3	**Fraunhofer SIT (SIT)** Fraunhofer Institut SIT Rheinstr 75 64295 Darmstadt Germany
4	**Escrypt** escrypt GmbH - Embedded Security Lise-Meitner-Allee 4 D-44801 Bochum Germany
5	**U.Siegen (Siegen)** Universität Siegen Hoelderlinstrasse 3 57076 Siegen Germany
6	**Ikerlan-K4 (Ikerlan-k4)** Ikerlan Pº J.M. arizmendiarrieta 20500 Mondragon Spain

Table 1: TERESA contact information

2.2 Intended Audience

This deliverable is the first version of D9, the Plan for Use and Dissemination (PUD). It is intended for use within the TERESA project and the European Commission.

2.3 Abbreviations and Conventions

The Project Handbook includes a glossary that lists abbreviations and definitions that are common to all deliverables in the TERESA project.

2.4 Summary

This document presents an initial version of the Plan for Use and Dissemination for the TERESA Project. It consists of three parts:

An overview chapter

A chapter on the dissemination plan

A chapter on the use plan.

3 Overview

3.1 Introduction

TERESA is a collaborative project (generic) funded under the Seventh Framework Programme, in the research area ICT-2009.3. The 3-year project runs from 1 November 2009 to 30 November 2012.

3.2 TERESA Scope and Objectives

The objective 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.

Resource constrained embedded systems are characterized as follows:

They belong to different application sectors

Computing resources are mostly statically determined and allocated through a process consisting of a configuration phase and a build phase

They are generally high integrity systems with strong assurance requirements. They therefore use advanced engineering disciplines.

The proposed approach is to use a model-based repository of security and dependability 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

The engineering process for resource constrained embedded systems will be validated in four application sectors: automotive systems, home control systems, industry control, and metering.

The table below summarises TERESA activities related to these objectives, the associated milestone and the way these objectives can be verified.

Activ -ity	Description	Type of Activity	Milestone	Verification in Project
A1	Model-driven RCES trust engineering approach	Engineering process	M2, M3, M4	D3.2, D3.3, D3.4
A2	Integration into RCES engineering approaches		M5	D6.4
A3	Trust meta-models and models	Repository for RCES trust engineering	M2, M3, M4	D3.2, D3.3, D4.3, D4.4
A4	S&D patterns		M3, M4	D4.3, D4.4
A5	Platform dependent implementations of S&D patterns		M3,M4	D4.3, D4.4
A6	Formal Validation of S&D patterns	Formal validation of RCES trust engineering	M3,M4	D5.2, D5.3
A7	Derived guidelines for platform dependent implementation of the patterns		M3, M4	D5.4, D5.5
A8	S&D Engineering process for RCES in Automotive systems	Specialisation to specific RCES sectors	M4	D5.3, D5.5
A9	S&D Engineering process for RCES in Industry control systems		M4	D5.3, D5.5

Activ -ity	Description	Type of Activity	Milestone	Verification in Project
A10	S&D Engineering process for RCES in Home control systems		M4	D5.3, D5.5
A11	S&D Engineering process for RCES in Metering systems		M4	D5.3, D5.5
A12	Advance on MDE for RCES	Challenges for RCES engineering	M5	D7.1, D7.2, D7.3
A13	Advance on integration of S&D patterns		M5	D7.1, D7.2, D7.3
A14	Advance on formal validation of metrology requirements		M5	D7.1, D7.2, D7.3

Table 2: Overview of TERESA Activities.

Note that TERESA objectives precisely address the issues related to data protection explained in the press release from the European Commission published on 2 May 2007.

3.3 Overview of Expected Results

The table below shows the project objectives, the related expected results and an assessment on exploitation. The description of the results and of the assessment will be refined in subsequent versions of this deliverable.

Objectives and Expected Results	Assessment on Exploitation
G: provide guidelines for the specification of sector specific RCES trusted computing engineering. Software process engineers in a given sector use the guideline to define a trusted computing engineering process that is integrated to the software engineering process used in the RCES sector	Potential for consulting on other application domain to instantiate MDE based on patterns and TERESA repository process and potential for resulting tools.
S: Define a trusted computing engineering approach that is suited to a number of sectors: the automotive sector, the home control sector, the industry control sector, the metering sector	Consulting in the domain to apply TERESA guidelines. Supply of tools. Creation of a community to populate the repository

Table 3: Expected Results.

3.4 Market Situation and Overview

It is useful here to repeat a number of statements made earlier in the document to understand the target market and market potential (in italics):

Resource constrained embedded systems (RCES) can be found 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. This involves complex development environments dealing with many software components (e.g. the AUTOSAR standard)*
- *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).*

TERESA target market is the following:

- Expertise and Engineering activities for RCES systems
  - RCES core software engineering activities: TERESA will offer a process allowing reuse of S&D expertise using patterns and models
  - S&D pattern engineering: S&D experts can use TERESA approach to provide patterns for multiple sectors
  - MDE engineering: MDE experts can use TERESA approach to store models and patterns in the TERESA repository
  - Security formal validation: Security properties of a given S&D pattern can be formally defined and verified
- S&D components for RCES components
- MDE based tools for the engineering of RCES applications

TERESA market potential is viewed as follows:

- Each of the 4 addressed application domains are high-volume markets. The metering, home control, industry control sectors are fragmented and very little has been achieved in terms of S&D. The automotive sector is more mature with strong standardization initiatives (e.g. AUTOSAR) but it has not taken advantage yet fully of the MDE and pattern approaches. We believe that the availability of TERESA proof of concepts in the 4 addressed domains could trigger significant market opportunities for expertise and tools
- TERESA results could also be exploited in other application areas.
- New innovative product need to be certicified to be competitive. 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), The certification process will help to get this certification . This will needed in all the application sectors where a safety function could be.
- Time to market is key point for competitiveness. The TERESA approach will help to reuse Paterns and models improving the development time. This is also important in all the application sectors.

3.5 Business Model Considerations

To be done in a later version

4 Description of Dissemination Plan

4.1 Approach to Dissemination and Use

The overall objectives for the dissemination and use task within TERESA are as follows:

- To establish effective mechanism for continuous communication and dissemination
- To follow-up standardisation activities and submit standardisation proposals to the relevant bodies as an outcome of the project
- To organise and attend meetings to liaison with related projects and initiatives
- To support the organisation of specific workshops
- To help ensure that TERESA results will be fully exploited.

Dissemination and liaison is paramount for the success of the TERESA undertaking. This involves activities at the industry and academic level:

- Industry level. Dissemination and liaison will take place (1) and the MDE level, (2) at the security level, (3) at the dependability level, (4) at each domain specific level.
- Research level. It is expected that a number of significant results will be produced in the course of the project. Academic partners (UTM-IRIT, USiegen, SIT, Ikerlan-K4) will disseminate results of the TERESA project by targeting the most relevant conferences of its domain. In particular, UTM-IRIT will have to attend technical and research meetings (OMG...).

The target groups of the TERESA dissemination activity have been the following:

4.1.1 Industrial Companies

The following industrial companies could benefit from the S&D engineering approach in metering, automotive, home control and industrial domain:

- Ikerlan-IK4 organized several meetings with differerent companies to show the result of the first year of TERESA project. During the meeting, different topics like models, patterns, methodology among others were discussed. Some 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 a 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 inprovements 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 (PTB)

U.Siegen attended to a meeting with Dr. U. Grottker of the PTB (Federal Physical-Technical Institute), who is the person in charge for 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 type approval procedure today
- 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 has been that the use of well-known S&D patterns in the design of new Smart Meters would be very helpful for the type approval, since these patterns wouldn't 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 Siegens' part of the D7.1 deliverable.

4.1.2 Academic Organisations

The following academic organisations are or could be involved in Security and Dependability in RCES and Model Driven Engineering for RCES**:**

- ICTEI, Chisinau: The ICTEI 2010 International Conference on Telecommunications, Electronics and Informatics has been organized 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" has been 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. Especially lightweight cryptography will become important for resource constrained systems like embedded systems in metering devices. Focussed target is the upcoming standard ISO 11770-5 (Key Management: Group Key Management).
- Artistdesign NOE (www.artistembedded.Org): With regard to dissemination in Embedded Systems Design, we plan through our IRIT-U. Of Toulouse partner to establish links with Artist network, in particular with community of Modeling and Validation. This is in order to confront 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. As a relevance to this community, we outline the following: Modeling, formal and semi-formal methods, and tools for security and dependability in embedded systems, domain specific languages for trust Resource Constrained Embedded Systems (RCES) applications, Engineering processes for Resource Constrained Embedded Systems (RCES).
- EWICS TC7 (European Workshop on Industrial Computer Systems, Technical Committee 7 : Reliability, Safety, Security): B. Hamid is accepted to join this Working group. This is a good opportunity to disseminate the results of TERESA project around this community. In particular challenges and advances in enforcing S&D in RCES by model-driven engineering.

4.1.3 Liaison with Other EU Projects

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

The project TERESA's results on expressing Security Properties / Requirements was brought as input to the projects SecFutur and Assert4SOA. Input from these discussions will again be utilized within project 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 works of TERESA with respect to the involved processes and generic structure. TERESA will profit from the inputs 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 very related to the tasks in TERESA though based on a more narrow variety of underlying system models. However in provides yet another application domain for modeling of security properties / requirements.

4.2 Introduction and Practical Information

4.2.1 Role and Responsibilities of the WP8 Manager

The manager of WP8 (Link to Industry and Reach Out) will also take the role of Communication Manager, defined as follows:

- Ensure proper dissemination of TERESA specific results
- Ensure proper consistency of communication w.r.t TERESA dissemination

The responsibilities of the Communication Manager are as follows:

- Identify items of communication
- Identify communication targets

Ensure liaison with security and dependability related initiatives, RCES initiatives, and standardisation initiatives.

4.2.2 Key Personnel

Title	Company	Name
WP8 Manager	Trialog	Antonio Kung
WP8 Deputy Manager	Trialog	Cyril Grepet
TERESA website manager	Trialog	Barbara Raither

Table 4: Personnel of WP5.

4.3 Communication Strategy

4.3.1 Communication Objectives

The communication objectives for TERESA are 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

4.3.2 Communication Sources

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

4.3.3 Project Identity

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

This logo is used with the following standard documents:

- Press release
- Fact sheet
- Deliverable
- Presentation
- Templates
- Flyer
- Web site.

Standard documents and templates for these documents are maintained on the project workspace (https://bscw.sit.fraunhofer.de/bscw/bscw.cgi/1336593).

4.3.4 Communication Channels and Media

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

Communication channel/media	Characteristics
Web	TERESA home page (www.TERESA-project.org)
Brochure	A flyers was created, one version in January 2010
Standard project presentation	A standard project presentation is available in the TERESA web site.
Specific presentations	Ad hoc presentations are prepared for specific workshops. Other presentations with more focused information have been made
News	The website includes a regular update on news
TERESA workshops	TERESA plans to organise a number of workshops throughout the project. The first S&D4RCES organized by TERESA partners took place in Vienna on September, the 14th in conjunction with SAFECOMP 2010.
Other workshops and conferences	TERESA will participate to a number or workshops and conferences (see list below).

Table 5: Overview of communication channels use.

4.4 TERESA Dissemination Highlights

4.4.1 Highlights of 2009-2010

Date	Description	Communication Activity	Impact & Audience
1 – 7.11.2009	meeting of ISO/IEC JTC 1 SC 27 (“Security Techniques”) in Redmond/USA	Liaison with standardisation organism in security domain	SC 27 standardizes cryptographic algorithms, modes, methods and protocols. Recent proposals cover also lightweight cryptography, which will become important for resource constrained systems like embedded systems in metering devices. Mr. Ruland acts as project editor for the upcoming standard ISO 11770-5 Key Management: Group Key Management.
10.02.10	eWorld in Essen (Smart Metering Fare)	Escrypt: Visiting of eWorld in Essen and discussion of	

		TERESA approach with different companies from the metering industry	
26.02.10	Visit of a PayTV solution provider	Escrypt: Discussion of potential applications of security patterns	
02-04.03.10	embedded world conference in Nurnberg	Escrypt: Distribution of the TERESA factsheet	
04.03.10	NRW-IKT meeting ZENIT – Successful R&D in Europe in Düsseldorf	Escrypt: Search for new partners interested in the TERESA engineering approach	
29.03.10	Visit of a Bank terminal solution provider	Escrypt: Discussion of potential applications of security patterns	
	Meeting with the Physikalisch-Technische Bundesanstalt	Discussion about the idea of a validated engineering process to simplify the type approval procedure	
February-April	Preparation of the IEEE international DANCE workshop (http://www.irit.fr/DANCE2010) Discussion to join the to join the IFIP Working Group 10.2 on Embedded Systems	IRIT-U. Of Toulouse	
04.05.- 05.05.10	OVERSEE Meeting in Bochum	Escrypt and Trialog: Liason activity with other FP7 projects	
20-23.05.2010	Preparation of a paper for the 3-rd International Conference "Telecommunications, Electronics and Informatics" ICTEI in CHISINAU	Usiegen	
07.06.10	EVITA Meeting in Munich	Escrypt and Trialog: Liason activity with other FP7 projects	
16.06.10	WO?-Kongress (Logistics & Transport) in Duisburg	Escrypt: Objectives of TERESA have been discussed with potential customers	
May and June 2010	Visitation of potential customers in different business areas and discussion of TERESA objectives	Escrypt: Transportation industry (11.05.10) Government (25.05.10) Banking industry (28.05.10) Communication industry (16.06.10)	
May and June 2010	Establishing contacts to the metering industry in Germany	Siegen : Contact with target industry	
May and July	Host of the IEEE international DANCE workshop (http://www.irit.fr/DANCE2010). Preparation of a paper for the 8th Nordic Workshop on Model Driven Software Engineering-ECSA Preparation of a paper for the IEEE/IFIP EUC 2010 conferene Preparation of the ACM international SD4RCES workshop (http://www.irit.fr/SD4RCES)	IRIT-U. Toulouse	The focus of the DANCE workshop is to use model-driven engineering to build new component based software architecture for embedded systems. Our participation in the ECSA conference and workshops allows us to learn more about advances in software architecture and in particular in challenges and advances in enforcing reconfiguration in embedded systems by model-driven engineering.

04.08.2010	Research Project RESIST in Darmstadt	Escrypt: Discussion of TERESA ideas with RESIST partners	
17-20.08.2010	Participation at the Workshop on Cryptographic Hardware and Embedded Systems 2010 (CHES 2010, Santa Barbara, USA)	USiegen	
02.09.2010	BITKOM Workshop for Smart Energy, Smart Metering in Bonn	Escrypt: Discussion about the idea of a validated engineering process to simplify the type approval procedure	
14 September 2010	First S&D4RCES Workshop organized by TERESA partners and hosted by IRIT-U. Toulouse in conjunction with SAFECOMP conference, Vienna, Autriche	Presentation of the TERESA approach Presentation of related project (SecFuture) Discussion about MDE for RCES Discussion about S&D in RCES Towards the Integration of Advanced Eng. Paradigms into RCES: Raising the issues for the Safety-Critical Model-Driven Product-Line Case by Ikerlan & IRIT-Univ of Toulouse	This first workshop provides us a platform to collect contributions from different areas and foster the collaboration towards suitable SD engineering for RCES . The workshop brings together 18 researchers from 8 countries and the proceeding is published y ACM. In addition this event opens new collaborations with with the safecomp community and B. Hamid is accepted to join the EWICS TC7 working group (European Workshop on Industrial Computer Systems, Technical Committee 7 : Reliability, Safety, Security).
14.09.2010	Presentation of the paper “Formalization of Smart Metering Requirements” at the S&D4RCES workshop of the Safecomp 2010 Conference in Vienna	USiegen & SIT – first workshop organized by the TERESA project	
14.09.2010	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 ” at the S&D4RCES workshop of the Safecomp 2010 Conference in Vienna	IKERLAN-IK4 & Univ of Toulouse – first workshop organized by the TERESA project	
21.09.2010	Industry workshop for security	Escrypt: Visiting of an industry workshop for security and discussion of TERESA approach with potential customers	
22.09.2010	Metering and Billing Europe in Vienna	Escrypt: Discussion of TERESA ideas with potential customers	
22.09.2010	Visitation of potential customers from railway and wind turbines sector and discussion of TERESA objectives	Ikerlan-Ik4: CAF (1.09.2010) Alstom Wind (2.09.2010)	
August - September 2010	Visitation of potential customers in different business areas and discussion of TERESA objectives	Escrypt: Mobile Communication Industry (25.08.2010) Government (16.09.2010)	

August-September 2010	Participation on the 8th Nordic Workshop on Model Driven Software Engineering (NW-MODE 2010) and presentation of a paper titld “Model-Based Engineering for Dynamic Reconfiguration in DRTES” Authors:Brahim Hamid, Fatma Krichen (IRIT) Host of the ACM international SD4RCES workshop (http://www.irit.fr/SD4RCES). 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-U. Toulouse	
06.10.2010	Security 2010 in Essen	Escrypt: Discussion of TERESA ideas with potential customers and distribution of the TERESA factsheet	
19.10.2010	ITSA in Nuremberg	Escrypt: Search for new partners interested in the TERESA engineering approach	
14.10.2010	Video Conference with Projects TERESA, SecFutur, Assert4SOA	(hosted by SecFutur)	Discussion on Approaches for (Meta-)Modelling of Security
17 .10.2010	Decision to link with the SecFutur project to create a sustainable community that understand Security as an Engineering Discipline. This follows the Serenity Manifesto concept	First contact and proposition to organize a joint meeting Proposition to organise a joint workshop in 2011	

Table 6: TERESA dissemination activities.

4.4.2 Publications

During the first year of the project, TERESA partners published:

- 1 article in an international conference with review committee
- 1 article in an international workshop with review commitee
- 2 short papers and 2 invited papers in the 1st International Workshop on Security and Dependability for Resource Constrained Embedded Systems (S&D4RCES) organized to promote the project and create a community on security engineering for RCES

Formalization of Smart Metering Requirements

Authors: Andreas Fuchs,Sigrid Gürgens (Fraunhofer SIT), Donatus Weber, Christian Bodenstedt,Christoph Ruland (University of Siegen)

Publisher: Proceedings of S&D4RCES '10 Workshop, in the Proceedings of the International Workshop on Security and Dependability for Resource Constrained Embedded Systems (SAFECOMP 2010)

Date: September 2010

Text: paper, ACM DL Digital Library

Model-Based Security and Dependability Patterns in RCES – the TERESA Approach

Authors: Brahim Hamid, Nicolas Desnos (IRIT, University of Toulouse), Cyril Grepet, Christophe Jouvray (Trialog)

Publisher: Proceedings of S&D4RCES '10 Workshop, in the Proceedings of the International Workshop on Security and Dependability for Resource Constrained Embedded Systems (SAFECOMP 2010)

Date: September 2010

Text: paper, ACM DL Digital Library

Towards the Integration of Advanced Engineering Paradigms into RCES: Raising the Issues for the Safety-Critical Model-Driven Product-Line Case

Authors: Salvador Trujillo, Antonio Perez, David Gonzalez (Ikerlan- IK4), Brahim Hamid (IRIT, University of Toulouse)

Publisher: Proceedings of S&D4RCES '10 Workshop, in the Proceedings of the International Workshop on Security and Dependability for Resource Constrained Embedded Systems (SAFECOMP 2010)

Date: September 2010

Text: paper, ACM DL Digital Library

Enforcing Trust in Embedded Systems Using Models

Authors: Christophe Jouvray, Miche SallAntonio Kung

Publisher: Proceedings of S&D4RCES '10 Workshop, in the Proceedings of the International Workshop on Security and Dependability for Resource Constrained Embedded Systems (SAFECOMP 2010)

Date: September 2010

Text: paper, ACM DL Digital Library

Model-Based Engineering for Dynamic Reconfiguration in DRTES

Authors: Brahim Hamid, Fatma Krichen (IRIT)

Publisher: 8th Nordic Workshop on Model Driven Software Engineering (NW-MODE 2010)

Date: August 2010

Text: paper

Integration of Security and Dependability into Resource Constrained Embedded Systems

Authors: Christian Bodenstedt, Christoph Ruland, Donatus Weber (University of Siegen), Antonio Kung (Trialog)

Publisher: 3rd International Conference on Telecommunications, Electronics and Informatics (ICTEI 2010)

Date: May 2010

Text: paper

5 Description of Use Plan

5.1 TERESA as Part of a Roadmap

5.1.1 Deployment Stages on the Roadmap

Roadmap to be identified in a later version

5.1.2 The Contribution of TERESA

Contribution with respect to the roadmap to be identified in a later version

5.2 Consortium

The consortium consists of a combination of research and industry partners with extensive background in the topics related to TERESA objectives:

- **Trialog** is a SME. It has extensive co-ordination experience. It also has extensive experience in the development and integration of embedded system platforms and on testing for automotive systems and home connectivity systems. It also markets embedded software technology (automotive RTOS, home network protocol).
- **UTM-IRIT** is a research organisation. It has extensive involvement in model driven engineering.
- **SIT** is a research organisation. It has extensive experience on formal validation of security. It was one of the leading partners of the Serenity project (pattern based security engineering).
- **escrypt** is a SME. It has extensive experience on security for embedded systems including for automotive systems. It is the leading technical partner of the EVITA project (protection against vehicle intrusion)
- **USiegen** is a research organisation. It has extensive involvement on security of metering systems
- **Ikerlan-K4** is a research branch of the MCC co-operative. It has extensive embedded systems experience in the area of home control and industry control.

5.3 TRIALOG

5.3.1 Trialog's Background

TRIALOG is a system and software engineering company in the fields of real-time and embedded systems. It focuses on innovative systems for the automotive and home / consumer electronics marketplaces. Most of the devices being developed for these markets today have networking capabilities and can communicate with their environment, such as other peer devices and Internet access. Trialog core competencies are therefore oriented towards the right combination of real-time embedded software and networking technologies that are the keys to building such communicating devices and their interfaces to large business information systems. TRIALOG engineering process focuses on system, network and software architecture, design-to-cost and design-to-security.

Some work carried out recently includes:

- Network protocols and connectivity solutions, in the area of automotive applications (VAN, CAN, TTP, Flexray, etc.), in the area of home networking including control buses such as the EHS/KNX bus, in the area of audio/video high-speed buses such as the IEEE1394 / HAVI bus, Hiperlan 2, etc. Connectivity solutions focus on embedded gateways with Internet Capabilities (integration of OSGi technology) and wireless communications (GSM./GPRS, 802.11, Bluetooth, etc.).
- Coordination of security projects such as e-PASTA IST project (e-Protection of Appliances through Secure and Trusted Access) or GST-SEC (security subproject of GST IST IP). Technical coordination of the TEAHA (The European Home Application Alliance) IST project with support of security aspects. Coordination of the Sevecom (Secure Vehicule Communication) IST Project. Technical coordination of the e-Inclusion MonAMI IST project.

More information on Trialog can be found at http://www.trialog.com.

Trialog has been involved in automotive applications and home control applications since 1987 and 1992 respectively. It has been working on the integration of security in RCES since 2000. Trialog will participate to the following:

- Management of the project (WP1).
- Use case and requirements (WP2)
- Engineering process metamodels, trust metamodels (WP3),
- Home control and automotive trust models, patterns (WP4)
- Repository access tools (WP4)
- Automotive and Home control application evaluation (WP6)
- Dissemination and liaison (WP7)

5.3.2 Trialog's Interest in TERESA

The interests in Trialog are of several kinds.

Trialog want to use the TERESA models and patterns for the development of home control and automotive applications with security and dependability needs

Further development related to repository access tools in order to transform them into industry products are also planned

Along the years, Trialog has collected requirements and needs on Model Based Engineering in term on consistency checking

In the past, Trialog has developed some proof of concept for tools for consistency checking that will use as foreground for Teresa project. The main principle is to acquire the modelled information coming from various modes and tools involved in the development of one product and to check their consistency. The heterogeneity of modelling language leads to build language translator into an internal format to ensure the consistency of the original models.

We want to use these approach and resulting tools in the future for any domain specific needs. The starting point of this exploitation is the TERESA project. For instance, we can try to ensure the consistency between the formal model and the home control application description model.

5.4 UTM-IRIT

5.4.1 UTM-IRIT's Background

IRIT (Institut de Recherche en Informatique de Toulouse) was founded in 1990. Since then, it plays a prominent role in Toulouse computer science research. It gathers together more than 500 members among which 400 researchers, faculty members, and Ph.D. students affiliated to CNRS (Centre National de la Recherche Scientifique), INPT (Institut National Polytechnique de Toulouse), UPS (Université Paul Sabatier), UT1 (Université Toulouse 1 Sciences Sociales) and UTM (Université Toulouse le Mirail).

UTM-IRIT is the part of IRIT that belongs to Université Toulouse le Mirail. Research at UTM-IRIT covers most of the fields where computer and information science is in progress, be it in its core, ranging from computer architecture to software engineering and computer networks, or in its most contemporary developments like artificial intelligence and cognitive systems, multimedia man-machine interaction, image interpretation and synthesis. UTM-IRIT has long experience in participating and managing collaborative and networking projects.

Within UTM-IRIT, MACAO team focuses its researches on Model Driven Software Engineering (MDE). The diversity of skills of its members allows it to study a large set of paradigms of programming including objects / components, formal methods applied to the MDE, process development and modeling real-time, and the integration of these paradigms in a method of design and engineering systems. MACAO team is an active actor within the community working on software development based on model transformations,

Besides its community involvement, MACAO team has also participated in the TOPCASED project in which the contribution aims to use meta-models expressed by attribute grammars, which allows a declarative approach in the form of semantic rules leading to an executable specification. The skills of the UTM-IRIT-MACAO about the verification of models have been developed within the framework of the NEPTUNE project in which research has been focused both on the study of ways of testing consistency rules of UML models and on the expression of high-level constraints- especially time. UTM-IRIT-MACAO

produced the definition of a functional and operational guide for the analysis and design dedicated to the development of software applications following an MDE process-based model in the scope of the DOMINO project.

The contributions of the team in these projects are done in collaboration with very important industrial partners (CEA LIST, Airbus, Astrium, CS, SOFT-MAINT ...). This allows to the team, in addition to its skills that ensure a reputation in the world of academic research, to enhance its knowledge about technologies and tools involved in the TERESA project.

More information on UTM-IRIT/MACAO can be found in http://www.irit.fr/-Equipe-MACAO-

UTM-IRIT brings its research expertise on MDE, with a focus on dependability support. UTM-IRIT will participate to the following:

- Use case and requirements (WP2)
- Engineering process metamodels, trust metamodels (WP3),
- Repository structure (WP4), Repository population with models and patterns (WP4)
- Formal validation approach (WP5)
- MDE Support to evaluation (WP6)
- Challenges on MDE (WP7)
- Liaisons on MDE, disseminaton on research (WP8)

5.4.2 UTM-IRIT's Interest in TERESA

Designing, implementing and deploying of applications in the different field considered in the project will allow UTM-IRIT and particularly MACAO team to confront, to validate and to extend these skills about trusted computing systems. These actions contribute to the definition of new systems engineering technologies with development centered on the models and based on the repository of SD patterns for trust RCES applications. Our interest may be summarised in the following:

5.4.2.1 Enforcing SD in RCES with Model Driven Engineering.

Model-Driven Engineering (MDE) provides a very useful contribution to the design of RCES applications since it bridges the gap between design issues and implementation concerns. Used properly, MDE can potentially maintain the separation of concern between application and SD, by ensuring that SD designs can be reused at a later stage by application designers. Significant research is being carried out concerning MDE for embedded systems, at the level of system architecture, design techniques, testing, validation, proof of correctness, modeling, software reliability, operating systems, parallel processing and real-time processing. Of particular interest is the use of MDE to enforce the integration of SD requirements into the engineering process and to support the reuse of SD mechanisms through patterns. Topics of interest include:

- Variability support. Implementations derived from the same design pattern could differ in their details, while remaining similar in their principles.
- RCES development and engineering processes based on the integration process of SD patterns
- Customisation of application sector specific processes
- Support tools for assisting modeling, deployment and configuration of SD by design
- Extending SysML, AADL and UML(through profiles) for security and dependability modeling.
- Code generation from a model, using transformation based on templates

5.4.2.2 Transfer of know-how within the MDE community.

- One of the objectives of this project is to foster the exchange of ideas among industrial and academic researchers involved in the deployment of secure and dependable resource-constrained embedded systems. Special emphasis will be devoted to promote discussion and interaction between researchers and practitioners focused on the particularly challenging task related to the development of models and tools to support the inclusion of security and dependability (SD) issues into the RCES engineering process.

- This project will provide a platform to confront contributions from different areas and foster the collaboration towards suitable SD engineering for RCES. It aims to bring together researchers from various fields including actors from Embedded Systems Design, Modeling and Validation, Security and Dependability, Model-Driven Engineering and MDE-based tool chain.

5.4.2.3 Repository Availability

The project worked on the availability of the repository as a prototype for industry stakeholders which wish to use the approach. One important focus of this project is on the potential benefits of the combination of model-driven engineering with pattern-based representation of security and dependability solutions. SD solutions are stored in the repository in the forms of patterns as an output of the project; then, what are really domain specific outputs are included in the repository as models and model transformation activities. Furthermore, we provide tool support for assisting the users to choose their patterns and to deploy and configure them on computing platforms. We focus on design tools based on the repository of SD pattern with some view of the possible implementation frameworks providing run time support, especially the dependability and security services and some additional control components. The overall objective of this workshop is to present significant information to define, to use and reuse SD solutions in the form of patterns:

- Design process of SD patterns
- Model-based repository of SD patterns for RCES
- Formalization of SD properties at the pattern and the design level
- Study the issue of reusing SD mechanisms in RCES

5.5 Fraunhofer SIT

5.5.1 Fraunhofer SIT's Background

The Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer) is an autonomous research organization with a decentralised organisational structure, which currently maintains 56 research institutes in locations throughout Germany. Whilst the administrative headquarters are in Munich, the legally non-independent research institutes operate from different locations in 15 of the German states. A staff of approximately 12,500 works with an annual research budget of about 1,2 billion Euro. Commissioned by customers in industry, Fraunhofer scientists provide rapid, economical and immediately applicable solutions. Work focuses on specific tasks across a wide spectrum of research fields including communications, energy, microelectronics, manufacturing, transport and the environment.

The Fraunhofer Institute for Secure Information Technology (Fraunhofer SIT) provides scalable IT security in conformance with the needs of the marketplace. Fraunhofer SIT is one of the pioneers within the field of IT-Security in Germany and Europe and has experience in development and promotion of security technologies and in embedding of security technologies into already established applications to make them trustworthy. The working areas of the about 165 employees range from basic applied research through the development of prototypes to product testing and customizing and implementing tailored security concepts and solutions. So Fraunhofer SIT helps clients in industry, commerce and public administration to eliminate security problems, minimize risks and damage, and implement innovative business concepts efficiently.

Fraunhofer SIT has worked and is working in a number of projects that are particularly relevant for TERESA. In particular the FP6 project SERENITY (IST-027587), in which Fraunhofer SIT, among other work, developed a security and dependability engineering approach based on a new notion of S&D patterns together with a formal framework for security requirements specification, and FP7 project EVITA (IST-224275) where Fraunhofer SIT is currently working on a security and trust model for solutions within the context of electronic control units for cars.

SIT will rely on its work on the development of methods and tools to model, simulate and validate systems at different levels of abstraction. These methods and tools have been deployed for example in in the FP6 project SERENITY for the development and validation of solutions based on Trusted Computing functionality. In order to facilitate simulation of solutions, a TPM emulator was integrated into the simulation tool. Previous and current work in the TPM working group provided the necessary background.

The research role of Fraunhofer SIT in TERESA will be focused on formal validation of security and dependability properties of S&D patterns to be used in S&D engineering process of TERESA.

Furthermore, Fraunhofer SIT will investigate the validation of the integration of S&D patterns and the representation of integrated solutions. SIT will participate to the following:

- Participation to use case and requirements (WP2), and engineering process definition (WP3)
- Responsibility for formal validation (WP5)
- Further research in integration of S&D patterns (WP7)

5.5.2 Fraunhofer SIT's Interest in TERESA

5.5.2.1 Exploitation goals in general

As the leading organisation of institutes of applied research and development in Germany, the primary objective of Fraunhofer-Gesellschaft is to improve information and technology transfer from research institutes to industry.

The Fraunhofer-Institute for Secure Information Technology SIT is the major IT security research institute in Europe serving industry and government with a strong focus on supporting the development of European SMEs. Fraunhofer SIT contributes with scientific research and prototypical development to all areas of IT security in close co-operation with industry and academic partners worldwide.

Dissemination and exploitation of results achieved through research and development at Fraunhofer SIT are organised in three pillars in accordance to the Fraunhofer mission:

- Knowledge and technology transfer: By developing technological innovations and novel systems solutions for their customers, Fraunhofer SIT help to reinforce the competitive strength of the economy in our region, throughout Germany and in Europe. Research activities are aimed at promoting the economic development of our industrial society, with particular regard for social welfare and environmental compatibility.
- Scientific dissemination and exploitation: Fraunhofer-Gesellschaft supports efforts directed toward the sustainable development of society, industry and the environment. The Fraunhofer Institutes play an active part in such efforts through a responsible approach to the implementation of new technologies and through research and studies conducted on behalf of public-sector clients. In its research work, Fraunhofer-Gesellschaft observes the principles of good scientific practice. Clearly defined procedures are used to investigate any cases of suspected scientific misconduct.
- Patents and licences: The purpose of Fraunhofer-Gesellschaft is to transform scientific findings into useful innovations. In this way, it helps to further economic growth, structural evolution and full employment. Fraunhofer SIT's own patents and licenses are exploited and brought to the market in close co-operation with strategic industry partners.

For the TERESA project, Fraunhofer SIT aims at strengthening the position in the areas of resource constraint embedded systems' security and dependability engineering but in a more generic view. Together with other major academic and industrial players, Fraunhofer SIT works towards establishing ICT security engineering as a well-founded discipline.

Expected results of TERESA can be summarized as follows:

- Prototypical security and dependability patterns for resource constraint embedded systems with a strong focus on re-usability.
- Security requirements specification methods and Security engineering processes.
- Methods and processes for formal validation of re-usable security and dependability patterns.

5.5.2.2 Mid and Long-Term Exploitation

As a research organisation, Fraunhofer is concentrating on mid-term and long-term exploitation in related parallel research projects as well as subsequent research activities in particular concentrating on knowledge transfer and co-operation with industry partners (SMEs as well as major industry players.)

Fraunhofer SIT is planning with slightly distinguished exploitation strategies for the three main results mentioned above.

- Security and dependability patterns for resource constraint embedded systems can be subject to mainly short-term and mid-term exploitation directly after the project or even during the lifetime of the project. Main goal is direct knowledge transfer towards industrial project development in order to enable industry to build embedded systems with higher security guarantees. Further, Fraunhofer SIT will co-operate with security consultants to increase the uptake of advances in security technology to be provided through TERESA pattern and process specifications.

- The exact specification of security requirements is essential during the development of secure and dependable resource constraint embedded systems. Fraunhofer SIT plans to use the results of TERESA to develop (in co-operation with industry partners) tools supporting such requirements specifications. These tools will most likely be extensions to existing software engineering tools (e.g. model-driven development tools). This activity is mid-term to long-term.
- Clearly, a long-term exploitation with a strong involvement of other European and international research players is the establishment of a security and dependability-engineering process for resource constraint embedded systems to complement existing engineering processes. In addition to the definition of the process, the development of tools, and the integration with existing tools, one main challenge is to reflect possible increased assurance in standardisation and regulation.
- Together with the modularization and the increasing application of pattern driven approaches in the design of resource constraint embedded system with growing complexity the methods and processes for formal validation need to be adapted as well. Especially the growth in complexity demands for an integration of the derived formal validation approaches with the tools used for engineering of system in the mid to long future.

5.5.2.3 Influence on Science, Research, Products and Know-how

TERESA is an integrated part of the Fraunhofer SIT research strategy. It is complementary to other existing research activities. These include the FP7 projects SecFutur (Design of Secure and energy-efficient embedded systems for Future internet applications) and MASSIF (security information and event management) and several German national projects. The integration of the results of these projects aims at realising the vision of a holistic view on embedded systems security and dependability.

5.5.2.4 Cooperation

Fraunhofer-Gesellschaft is a major player in the European research area. The Fraunhofer Institutes network with other centres of excellence, and together help to assure the competitive strength of European research.

Fraunhofer-Gesellschaft collaborates with other research organizations and institutions in Germany. Of particular importance are its intimate ties with selected universities, which represent a key element in its integration in the scientific community as a whole. Fraunhofer SIT is also actively involved in industry forums (e.g. TCG,BitKom,Teletrust), research communities (e.g. WWRF, ERCIM, eMobility, Nessi) and standardisation bodies (e.g. IEEE, ISO, 3GPP). Fraunhofer SIT plans to increase research co-operations towards security engineering based on the TERESA results. Further, TERESA results will strengthen the knowledge transfer to industry partners, in particular on the application of security and dependability engineering of resource constraint embedded systems.

5.6 escrypt GmbH

5.6.1 escrypt's Background

As a system provider, escrypt offers solutions for all aspects of embedded security from one source. The services include system design, specification, prototyping up to product development and certification. escrypt works in all areas of embedded applications with need for security. escrypt's unique branch expertise and technical competence is based on many years of experience in the field of embedded security and an extensive number of successful projects in different industry domains.

Over the past years, escrypt has effectively expanded its competence in the area of embedded Trusted Computing. Moreover, escrypt has successfully demonstrated its real-world-oriented know-how in the area of Trusted Computing in numerous projects devoted to design and implementation of such systems. escrypt has various Trusted Computing demonstrators for x86-desktop systems as well as for different embedded platforms (e.g. ARM 920T). The necessary link between Trusted Computing hardware mechanisms and the software security architecture was successfully, theoretically as well as practically, demonstrated using different approaches (e.g. L4 micro kernel, Xen-virtualisation).

escrypt has successfully worked in recent embedded security projects covering the following application areas:

- secure flashing
- trusted computing and virtualisation for different application domains (e.g. automotive, multimedia, mobiles)
- controlled and secure activation of software features and digital content

- protection of digital content (e.g., infotainment data, tachographs, proprietary embedded software, IP protection etc.)
- theft protection and personalisation
- security analysis in different application domains
- Back-End security to support the embedded applications
- network security within and outside of cars
- theft protection and personalisation in vehicles
- security for telematic applications
- fast implementation of cryptographic primitives in software and hardware (e.g. elliptic curve cryptography (ECC) on smart cards or ECC in VHDL)

More information on escrypt can be found at http://www.escrypt.com

escrypt will leverage on its considerable experience on security for embedded systems in particular for the automotive industry. escrypt will amongst others participate to the following:

- support in finding use cases for the automotive sector as well as analyzing their requirements (WP2)
- provision of patterns and proof of concepts for automotive applications (WP4)
- specification of automotive specific engineering processes (WP3)
- integration of previously defined patterns into proof of concept automotive applications (WP6)
- dissemination of the TERESA approach to the automotive industry (WP8)

5.6.2 Escrypt's Interest in TERESA

In TERESA escrypt aims to make use of TERESA models and patterns for the development of automotive applications with security and dependability needs in order to ease the integration of one of these solutions due to reusability.

While the engineering process for the development of dependability or safety functionalities is already well-defined in the automotive domain, by now, the security engineering is an accepted challenge in the development of most vehicular IT systems. However, even though many security threats and effective protection measures are already known in general, automotive engineers have difficulties to concretely realize efficient security solutions such that the costs for protection measures actually suit the identified threats in order to avoid "under protection" as well as "over protection", which both is unacceptable particularly in the automotive domain. 0

Hence, we are mainly interested in developing patterns for the security engineering process. Within the TERESA project we intend to improve the security engineering process of the automotive domain and achieve an efficient redesign that is based on the usage of patterns.

As part of the automotive security engineering process, especially the steps "System Model Design" and the "Architectural Design", needs to be improved by the usage of patterns. These engineering steps are strongly depending on a security analysis, which is geared to the approach of CC evaluations, and require a very deep knowledge of security. Usually an intensive cooperation with security experts of another company that is entrusted with the security analysis is essential.

In order to simplify the "System Model Design" development, involving the security analysis process, as well as its implementation, we aim to develop reusable patterns for basic, frequently used security functionalities for which the integration can be validated.

5.7 University of Siegen

5.7.1 University of Siegen's Background

The Institute for Data Communications Systems of the University of Siegen's main research area is the integration of security and cryptography in communications systems considering all layers of the ISO model. Encryption devices for SDH (622 MBit/s) and ATM (155 MBits/s) have been developed as well as secure multimedia applications or XML signatures. The institute was already responsible for the security aspects of 7 EU projects (SCARAB, WEBSIG, ELIAS, GNIUS, USBCRYPT, SETIC, eMAYOR). It is member of ISO/IEC SC 27 (Security Techniques) for more than 20 years and was editor of more than 5

international standards. The team includes more than 10 scientific assistants and around 20 persons in total. More than 20 doctors and 180 graduates finished their studies at the institute.

The institute works on security of metering systems since 2001. It was responsible for the security architecture and design in the SELMA (secure electronic data collection of metering) project funded by the German ministry of Economy and included all stake holders in the metering business. The institute implemented the security infrastructure of the system, which resulted in two Dr.-dissertations and many publication about secure metering in the liberalized metering market and in secure software download of regulated software. In further projects the institute implemented the firmware of a Cryptocontroller for metering devices, and is working now on the design and realization of a MUC platform (Multi Utility Communication, see (www.m-u-c.org). The institute provides a very close contact to different departments of the Physical-Technical Federal Institute of Germany (technical department and approval department) and cooperates with manufacturers of metering devices (electricity, gas, water). Actually the institute started to develop a SYM2-Meter (see www.sym2.org), which will become a standard metering type in Germany. The technology to be developed in the applied project TERESA should be mapped and applied to this new type of meters.

More information about DCS can be found at http://www.uni-siegen.de/fb12/dcs/index.html?lang=de

DCS will leverage on its considerable research experience on metering. It will participate to the following tasks:

- support in finding use cases for the metering sector as well as analyzing their requirements (WP2)
- collection of requirements for metrology specific engineering processes and help with the development of an unified Smart Meter design process considering S&D (WP3)
- provision of patterns and proof of concepts for metering applications (WP4)
- formal validation of different metrology requirements (WP5)
- integration of previously defined patterns into proof of concept applications for metering (WP6)
- approaches towards the formalization of metrology requirements from catalogues (e.g. the European Measuring Instruments Directive) (WP7)
- dissemination of the TERESA approach to the metering industry (WP8)

5.7.2 University of Siegen's Interest in TERESA

There are two main objectives defining University of Siegen's interest in the TERESA project. On the one hand support for the development of Security and Dependability related patterns and their integration into engineering processes for all kinds of smart meters. On the other hand a research approach towards formalization of lawful Security and Dependability requirements found in catalogues like the Measuring Instruments Directive (MID).

Both objectives comprise the transfer of expertise within the metrology community.

5.7.2.1 Patterns and Engineering Process

Today's Smart meters require certain Security and Dependability related functions correctly implemented to gain the type approval. The development of patterns, as for example the Secure Software Download, and their distribution to the metering industry with help of the TERESA repository helps smaller companies to satisfy S&D related requirements.

As the use of resource constrained embedded systems for Smart Meters is relatively young, there is no unified engineering process available yet. So the definition of S&D related patterns and their integration into existing development schemes could be a step towards this process.

5.7.2.2 Formalization Research Approach

By now, it is often hard to correctly interpret the verbally formulated requirements for measuring instruments regarding Security and Dependability relevance of their hardware and software parts. The approach comprises to exemplarily formalize different requirements like the MID Annex I 8.4.

Research in this field could be the basis for easing the type approval procedure of modern measuring instruments.

5.8 Ikerlan

5.8.1 Ikerlan's Background

IKERLAN-K4 (www.Ikerlan-K4.es) is a Spanish private not-for-profit Technology Centre, with a vocation for public service. It was set up in 1974 in the heart of what today is Mondragon Cooperative Corporation (MCC). This Corporation is the leading business group in the Basque area and is one of the top-ranking groups in Spain. It consists of 82 industrial companies, 5 financial entities, 3 research centres, 1 university and 12 insurance companies and international trade services. It has a turnover of more than 6 billion Euros and a workforce of more than 50,000 people. Ikerlan-K4 is located in the North of Spain and is a preferred Research Centre for innovation and comprehensive product development (mechatronics), with more than 25 years of experience in combining and applying mechanics, electronics and computer science. IKERLAN-K4 is a point of reference for innovation, dedicated to advanced technology transfer to industry and comprehensive product development (from concept to implementation) for a wide variety of domains: transportation (railway and vertical), automation, industrial, medical, home appliances, etc. IKERLAN-K4 works closely with companies to improve their competitiveness, through the application of technological knowledge to develop innovative products and new tools and methodologies for implementation in design and production processes. It has a staff of more than 200 qualified researchers and engineers, with experience in interdisciplinary work and capable of tackling complex problems. It is the key technological R&D actor within the Grupo Mondragon (www.mcc.es), Spain's sixth-largest industrial corporation.

The Embedded Systems Group is composed by different technology knowledge areas such as Electronics, Communications and Software. The group has a track record of proven R&D projects for national / international R&D programs and projects under contracts for different companies that required embedded intelligence in their new product developments.

Some of the main research topics in the embedded systems group are:

Real-Time, distributed, dependable embedded systems

Embedded systems on chip: SoCs, FPGAs, ASICs based

Connectivity and interoperability for embedded systems

The group has also a proven experience in the development of safety-critical / safety–related embedded systems, and certification based on the IEC-61508 standard. This knowledge has been applied in the development of dependable product(s) for some of our most important clients such as Orona (lift and escalators), CAF (railway systems) and Alstom-Ecotecnia (Wind turbines). Also the group has a proven experience in the development of embedded systems connectivity and interoperability this experience has been applied in the home appliances interoperability using topics like middleware, wireless and ambient intelligence for some of our most important clients such as FAGOR (Home appliances), OSATU (Electro medical devices) and Orona (lift and elevators).

IKERLAN-K4 has worked and is working in a number of projects that are particularly relevant for TERESA these are some examples of European projects where Ikerlan-K4 has participated or is participating: Gap, Elecline, InHoMNet, Robocop, Space4u, Trust4All, Teaha, Amigo, Genesys and TECOM. Since 1990, Ikerlan-K4 has been working in close cooperation with Fagor Electrodomesticos in Home Domotica. Main activities are focused on developing the electronic and software aspects required in the new products for this field. Because of this Ikerlan-K4 can provide thorough knowledge of this domain and therefore, they will facilitate the process of incorporating the new TECOM technologies in this application domain.

Ikerlan-K4 has thirty years of expertise in software, acquiring new methodologies, participating in some standardization organizations and, occasionally, prototyping customers' devices and software to make new products.

In this project IKERLAN-K4 will be focused on a methodology aimed to be aligned with IEC-61508 for safety-relevant embedded systems development in this case oriented to SIL0 (e.g. IEC-61508), it means not certificated embedded systems but more robust than current embedded systems. Based on SysML and UML and including embedded system testing. IKERLAN-K4-IK4 will participate to the exploitation on industry control patterns.

Ikerlan-K4 has been working on a methodology for dependable embedded system with appropriate tools that reduce development time / cost, ease certification, enable "right-first-time-every time" developments, system-level design, abstract application from the underlying technology, seamlessly integrate verification and provide seamless co-development of hardware for Real-time embedded system design modeling, embedded system Testing and Virtual Prototyping.

Ikerlan-K4 will amongst others participate to the following:

- support in finding use cases for the industry control sector as well as analyzing their requirements (WP2)
- specification of industry control specific engineering processes (WP3)
- provision of patterns and proof of concepts for industry control applications (WP4)
- integration of previously defined patterns into proof of concept industry control applications (WP6)
- participation to research work on MDE with a focus on assurance problems for dependability (WP8)

5.8.2 IKERLAN-K4's Interest in TERESA

Use of TERESA models and patterns for the development of industry control and home control applications with security and dependability needs. Special focus in the use of the models and patterns for the development of safety critical embedded systems in those application areas.

Transfer of expertise within the 82 industrial companies of the Mondragon Cooperative and others outside the Mondragon group.

Use of TERESA methodology aimed to be aligned with IEC-61508 for safety-relevant embedded systems development in this case oriented to SIL0 (e.g. IEC-61508), it means not certificated embedded systems but more robust than current embedded systems. Based on SysML and UML and including embedded system testing. IKERLAN-K4-IK4 will participate to the exploitation on industry control patterns.

Research in system-level design, abstract application from the underlying technology, seamlessly integrate verification and provide seamless co-development of hardware for Real-time embedded system design modeling, embedded system Testing and Virtual Prototyping will be also and objective.

6 References

M.Scheibel, M.Wolf: Security Risk Analysis for Vehicular IT Systems — A Business Model for IT, escar 2009