QUARTERLY PROGRESS REPORT

Grant Agreement number:	224275
Project acronym:	EVITA
Project title:	E-safety vehicle intrusion protected applications
Funding Scheme:	Collaborative project

Date of preparation of the latest version of Annex I: 4 February 2011

Quarter covered: from 1 October 2011 to 31 December 2011

Project co-ordinator name, title and organisation: Dr.-Ing. Olaf Henniger,
Fraunhofer Institute for Secure Information Technology

Tel.:	+49 6151 869 264
Fax:	+49 6151 869 224
E-mail:	olaf.henniger@sit.fraunhofer.de
Project website address:	http://evita-project.org

1 Work progress and achievements during the quarter

1.1 WP1000 (RTD/scientific coordination and dissemination/ external interfaces)

1.1.1 T1100 (RTD/scientific coordination)

What has been achieved?

– Organisation of meetings and conference calls.

Status: Finished.

1.1.2 T1200 (Public dissemination and external interfaces)

What has been achieved?

- Creation of posters showing the approach and the results of the EVITA project.
- Creation of a promotional animation video about the EVITA project.
- The EVITA desktop and vehicle demonstrators were presented in a special exhibition tent in front of the venue of the *9th escar Conference (International Conference on Embedded Security in Cars)* on 9–10 November 2011 in Dresden, Germany. The conference programme included also an invited talk about EVITA:

  B. Weyl[1], H. Schweppe[2]: The EVITA project – Securing the networked vehicle

- The *Final EVITA Workshop on Security of Automotive On-Board Networks* took place on 23 November 2011. The objective was to present major results of the project to the public. The event took place on the day before the Car 2 Car Forum 2011 at the Honda Academy in Erlensee (near Frankfurt/Main, Germany).

  The workshop had been advertised via various channels (mailing lists of C2C-CC, simTD, PRESERVE and EVITA, serial email, ICT for Transport Newsletter, escrypt e-news, leaflets at the escar conference). The audience of about 60 participants included potential users of the EVITA results from car manufacturers and automotive electronics suppliers.

  The following presentations related to EVITA were given (available at http://evita-project.org/Publications/EVITAD1.2.5.2.pdf):

  - H. Brandl[3]: Keynote address: Trusted computing for mobile and embedded systems
  - Y. Roudier[2]: Motivation, objectives, and approach of the EVITA project
  - M. Wolf[4]: Secure on-board architecture specification
  - H. Schweppe[2]: Secure on-board protocols

[1] BMW Group Research and Technology

[2] EURECOM

[3] Infineon Technologies AG

[4] escrypt GmbH

  - H. Seudié[5]: Integration into AUTOSAR
  - B. Weyl[1]: EVITA prototype and demonstrator overview
  - J. Dumortier[6]: Legal requirements on automotive on-board networks
  - F. Kargl[7]: Uptake of EVITA results in the PRESERVE project

  After presenting the main points of the specifications, the consortium showed the desktop and vehicle demonstrators that were developed in EVITA.

  The project met positive feedback and interesting questions were raised about

  - the relation between TPM and the EVITA HSMs,
  - the choice of cryptographic algorithms for the EVITA prototype,
  - the recommended degree of tamper-protection, and
  - fail-safe cryptographic design.

  The public workshop was framed by two private sessions with the European Commission and the reviewers for the Final Project Review.

- The EVITA desktop and vehicle demonstrators were a major part of the exhibition at the *Car 2 Car Forum* on 24–25 November 2011 at the Honda Academy in Erlensee, Germany. The Car 2 Car Forum is the annual assembly of the members of the Car 2 Car Communication Consortium (C2C-CC). The programme of the Car 2 Car Forum included an invited talk about EVITA in a plenary session:

  H. Seudié[5], M. Wolf[4]: Security & privacy – Results of the EVITA project

  The chairman of the C2C-CC Working Group "Security", Dr. Elmar Schoch of Volkswagen AG, gave a plenary presentation about "EVITA results in C2C-CC". This highlights the impact of the EVITA project on the work of the C2C-CC. EVITA results also had a bearing on the work of the Taskforce "Secure hardware" of the C2C-CC Working Group "Security".

- Further demonstration plans: EVITA partners involved in WP5000 (Demonstration) plan a joint demonstration with the PRESERVE project at the ITS World congress in Vienna in October 2012, based on the EVITA desktop and vehicle demonstrators.
- The deliverables D1.2.6 "Final liaison documentation" and D1.2.7 "Final dissemination strategy" have been drafted and internally reviewed.
- The following papers related to EVITA have been accepted and presented at conferences:

  - H. Schweppe[2], T. Gendrullis[4], M.S. Idrees[2], Y. Roudier[2], B. Weyl[1], M. Wolf[4]: Securing car2X applications with effective hardware-software co-design for vehicular on-board networks. In *27. VDI/VW-Gemeinschaftstagung Automotive Security*, 11–12 October, 2011, Berlin, Germany

[5] Robert Bosch GmbH

[6] K.U. Leuven

[7] University of Twente

    - M. Wolf[4], T. Gendrullis[4]: Design, implementation, and evaluation of a vehicular hardware security module. In *14th International Conference on Information Security and Cryptology*, 30 November – 2 December 2011, Seoul, South Korea

- Liaison activities with
    - C2C-CC Working Group "Security": Active membership in Taskforce "Secure hardware"
    - European project PRESERVE:
        - liaison meeting for discussing the draft of the EVITA/PRESERVE cooperation agreement,
        - personal meetings, telephone interviews and telephone conferences for discussing technical details
    - European project OVERSEE: Personal meetings, telephone interviews, and telephone conferences;
- The results of EVITA and their possible use have been discussed with
    - costumers and potential customers in the automotive industry (OEMs and suppliers)
    - several research institutes
    - conference and workshop participants

Status: Planning of further dissemination activities is ongoing

1.2 WP2000 (Security requirements engineering)

1.2.1 T2100 (E-security relevant use cases)

Status: Finished

1.2.2 T2200 (Dark-side scenarios)

Status: Finished

1.2.3 T2300 (Security requirements analysis)

Status: Finished

1.2.4 T2400 (Legal framework and requirements)

Status: Finished

1.3 WP3000 (Secure on-board architecture design)

1.3.1 T3100 (Adapted security and trust model)

Status: Finished

1.3.2 T3200 (Secure on-board architecture)

Status: Finished

1.3.3 T3300 (Secure on-board protocols)

Status: Finished

1.3.4 T3400 (Model-based verification)

Status: Finished

1.4 WP4000 (Security architecture implementation)

1.4.0 General

What has been achieved?

- Bi-weekly joint conference calls on WP4000 and WP5000

1.4.1 T4100 (Security hardware)

What has been achieved?

- Bug-fixing and updating of the implementation of HSM firmware and library on PowerPC of FPGA

Status: Finished

1.4.2 T4200 (Basic software)

What has been achieved?

- Support for integration of the basic software into the demonstrators
- Testing and debugging
- Institut Télécom has written a public report "LLD modelling, verification, and automatic C-code generation" describing the UML models of the low-level drivers, their verification, and the C code generation from the driver models. The report has been numbered D4.2.3 (it is not listed in the Description of Work). The purpose is to report about work that has been performed, but did not enter D4.2.2 "Basic software prototype".

Status: Finished

1.4.3 T4300 (Security library)

What has been achieved?

- Support for integration of the software framework into demonstrators
- Testing and debugging

- The deliverable D4.3.2 “Implementation of software framework” has been completed. A description of the prototype has been written and submitted to the European Commission in electronic form.

Status: Finished

1.4.4 T4400 (Code validation)

What has been achieved?

- Performing code validation, in particular fuzzing on the Tricore and Xilinx boards
- The deliverable D4.4.2 “Test results” has been drafted.

Status: Finished

1.5 WP5000 (Demonstration)

What has been achieved?

- Bi-weekly joint conference calls on WP4000 and WP5000
- Weekly onsite integration work on demonstration vehicles at BMW premises in Munich.
- Integration of all components into the desktop and vehicle demonstrators
- Testing and debugging
- Setup of a desktop demonstration of secure communication using the HSM FPGA via the HSM LLD in an AUTOSAR environment
- The deliverable D5.1.2 “On-board communication demonstrator” has been completed and demonstrated to the European Commission and the public at the final review and final workshop on 23 November 2011. A description of the demonstrators has been drafted.

Status: Finished

2 Deliverables and milestones tables

2.1 Deliverables

Table 1 lists all deliverables based on the revised Description of Work and indicates whether they have already been delivered.

Table 1 List of deliverables

Del. no.	Deliverable name	WP no.	Lead participant	Nature[8]	Dissemination level[9]	Due delivery date from Annex I	Delivered Yes/ No	Actual/ forecast delivery date	Comments
D0	Final public report	0000	FRAUNHOFER (SIT)	R	PU	2011-12-31	No	2012-02-15	
D1.2.1	Draft dissemination strategy	1000	FRAUNHOFER (SIT)	R	PU	2008-10-31	Yes	2008-12-11	Version 1.1: 2009-12-04
D1.2.2	Public area of project website	1000	FRAUNHOFER (SIT)	O	PU	2008-10-31	Yes	2008-11-7	
D1.2.3	Mid-term liaisons documentation	1000	TRIALOG	R	PU	2010-02-28	Yes	2010-03-01	Version 1.1: 2010-03-11
D1.2.4	Mid-term dissemination strategy	1000	FRAUNHOFER (SIT)	R	PU	2010-04-30	Yes	2010-05-14	Version 1.1: 2011-01-05
D1.2.5	Project workshop	1000	FRAUNHOFER (SIT)	O	PU	2010-06-30	Yes	2010-07-01	
D1.2.6	Final liaisons documentation	1000	TRIALOG	R	PU	2011-12-31	No	2012-02-15	
D1.2.7	Final dissemination strategy	1000	FRAUNHOFER (SIT)	R	PU	2011-12-31	No	2012-02-15	
D2.1	Specification and evaluation of e-security relevant use cases	2000	CONTINENTAL TEVES	R	PU	2009-02-28	Yes	2009-03-04	Version 1.2: 2009-12-30
D2.3	Security requirements based on dark-side scenarios	2000	MIRA	R	PU	2009-03-31	Yes	2009-03-31	Version 1.1: 2009-12-30
D2.4	Legal framework and requirements report	2000	K.U. Leuven	R	PU	2011-06-30	Yes	2011-09-13	Version 1.1: 2011-09-19
D3.1.1	Security and trust model – Draft	3000	TRIALOG	R	PU	2009-06-30	Yes	2009-07-15	
D3.1.2	Security and trust model	3000	TRIALOG	R	PU	2009-11-30	Yes	2009-11-24	
D3.2	Secure on-board architecture specification	3000	BMW F+T	R	PU	2010-02-28	Yes	2010-03-11	Version 1.3: 2011-08-15
D3.3	Secure on-board protocols specification	3000	EURECOM	R	PU	2010-06-30	Yes	2010-07-20	Version 1.4: 2011-06-15
D3.4.1	Architecture and protocols verification and attack analysis – Draft	3000	FRAUNHOFER (SIT)	R	PU	2009-12-31	Yes	2010-03-31	
D3.4.3	Architecture and protocols verification	3000	FRAUNHOFER (SIT)	R	PU	2010-09-30	Yes	2010-12-30	
D3.4.4	Attack analysis	3000	FRAUNHOFER (SIT)	R	PU	2010-09-30	Yes	2010-12-30	

[8] **R** = Report, **P** = Prototype, **D** = Demonstrator, **O** = Other

[9] **PU** = Public
PP = Restricted to other programme participants (including the Commission Services)
RE = Restricted to a group specified by the consortium (including the Commission Services)
CO = Confidential, only for members of the consortium (including the Commission Services)

Del. no.	Deliverable name	WP no.	Lead participant	Nature[8]	Dissemination level[9]	Due delivery date from Annex I	Delivered Yes/ No	Actual/ forecast delivery date	Comments
D4.0.1	Security architecture implementation – Progress report V0.1	4000	INFI-NEON	R	PU	2010-02-28	Yes	2010-04-08	
D4.0.2	Security architecture implementation – Progress report V0.2	4000	INFI-NEON	R	PU	2010-09-30	Yes	2010-10-31	
D4.0.3	Security architecture implementation – Progress report V1.0	4000	INFI-NEON	R	PU	2011-06-30	Yes	2011-07-15	
D4.1.1	Hardware implementation specification	4000	ES-CRYPT	R	RE	2010-06-30	Yes	2010-08-30	
D4.1.2	Security hardware FPGA prototype – Version 1	4000	ES-CRYPT	P	CO	2010-09-30	Yes	2010-09-23	
D4.1.3	Security hardware FPGA prototype	4000	ES-CRYPT	P	CO	2010-12-31	Yes	2011-01-31	
D4.2.1	Basic software – Version 1	4000	FUJITSU	P	CO	2010-09-30	Yes	2010-09-23	
D4.2.2	Basic software	4000	FUJITSU	P	CO	2011-03-31	Yes	2011-05-12	
D4.3.1	Implementation of software framework – Version 1	4000	BOSCH	P	CO	2011-03-31	Yes	2011-06-01	
D4.3.2	Implementation of software framework	4000	BOSCH	P	CO	2011-06-30	Yes	2011-11-17	Version 1.1: 2011-11-20
D4.4.1	Test specification	4000	EURE-COM	R	CO	2010-12-31	Yes	2011-05-12	
D4.4.2	Test results	4000	EURE-COM	R	PU	2011-06-30	No	2012-02-15	
D5.1.1	On-board communication demonstrator specification	5000	ES-CRYPT	R	RE	2010-12-31	Yes	2010-12-30	Version 1.0: 2011-08-18
D5.1.2	On-board communication demonstrator	5000	ES-CRYPT	D	PU	2011-12-31	No	2012-02-15	

2.2 Milestones

Table 2 lists all milestones based on the revised Description of Work and indicates whether they have been actually achieved.

Table 2 List of milestones

Milestone no.	Milestone name	Due achievement date from Annex I	Achieved Yes/No	Actual/forecast achievement date	Comments
M1	Requirements available	2009-03-31	Yes	2009-03-31	
M2	Security and trust model and secure on-board architecture available	2010-02-28	Yes	2010-03-11	
M3	Protocol specification and model-based verification available	2010-09-30	Yes	2010-12-30	
M4	FPGA prototype, basic software, and security software framework available	2011-06-30	Yes	2011-11-23	
M5	Final validation and demonstrator available	2011-12-31	Yes	2011-11-23	

3 Project management

3.1 Management achievements

What has been achieved?

- A quarterly progress report including a person-month overview per beneficiary and work package for July–September 2011 has been compiled and sent to the European Commission.
- A quarterly cost overview for July–September 2011 has been compiled for internal use by the EVITA Steering Committee.

3.2 Project meetings

Table 3 lists the physical meetings of the project partners within the reporting period.

Table 3 Physical project meetings within the reporting period

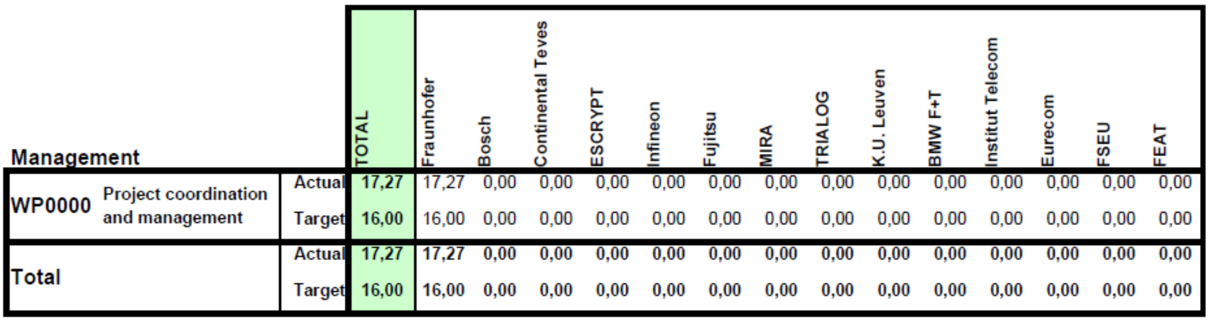
Meeting	Date	Venue
Integration Workshop	2011-10-25/26	Munich, Germany
Review Preparation Meeting	2011-11-22	Langenselbold, Germany
Final Review and Public Workshop	2011-11-23	Erlensee, Germany

3.3 Person-month overview

Table 4 through Table 7 give a tabular overview of target person-months over the entire project duration and actual person-months spent so far per beneficiary and per work package. The target person-months are taken from the revised Annex I of the Grant Agreement.

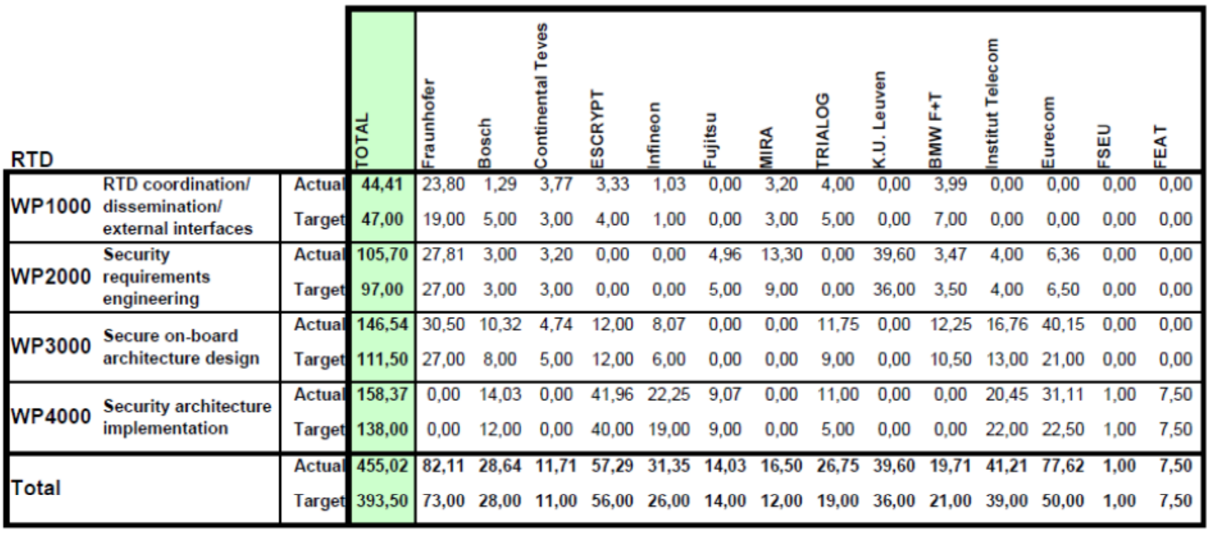
The project budget is based on the targeted person-months and conservative estimates of the costs per person-months. The actual costs per person-month may be slightly lower than the estimates. In that case, more person-months than targeted are within the budget. The actual costs per person-months will be determined for the periodic report.

Table 4 Person-month overview for management activities



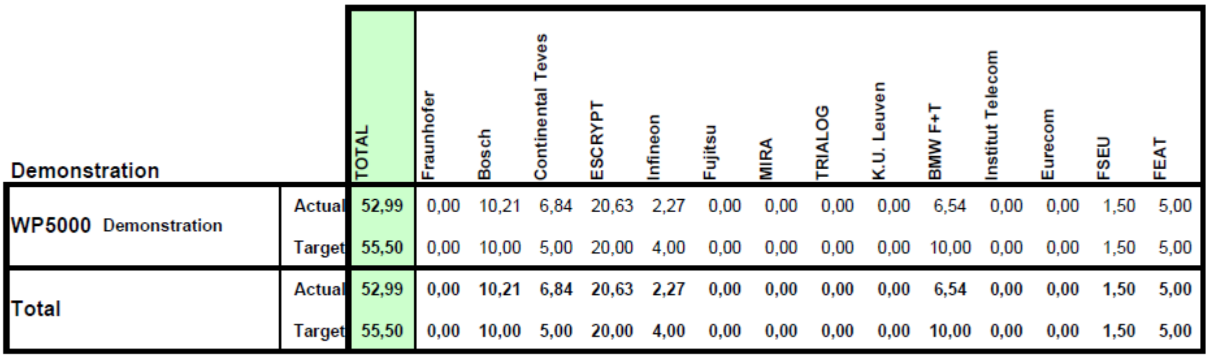
Management			TOTAL	Fraunhofer	Bosch	Continental Teves	ESCRYPT	Infineon	Fujitsu	MIRA	TRIALOG	K.U. Leuven	BMW F+T	Institut Telecom	Eurecom	FSEU	FEAT
WP0000	Project coordination and management	Actual	17,27	17,27	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		Target	16,00	16,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Total		Actual	17,27	17,27	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		Target	16,00	16,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00

Table 5 Person-month overview for RTD activities



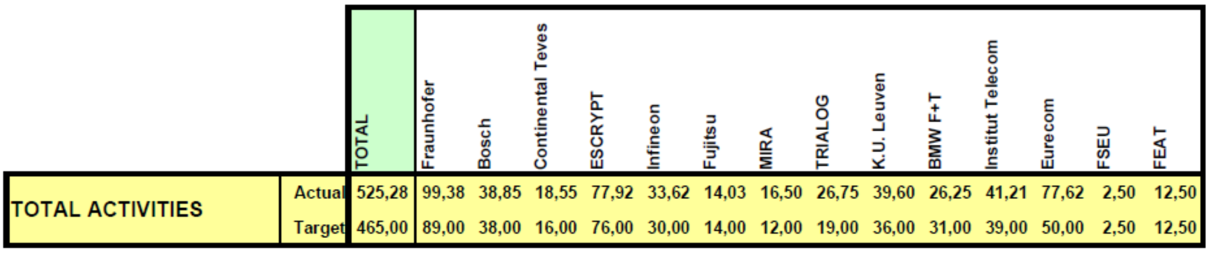
RTD			TOTAL	Fraunhofer	Bosch	Continental Teves	ESCRYPT	Infineon	Fujitsu	MIRA	TRIALOG	K.U. Leuven	BMW F+T	Institut Telecom	Eurecom	FSEU	FEAT
WP1000	RTD coordination/ dissemination/ external interfaces	Actual	44,41	23,80	1,29	3,77	3,33	1,03	0,00	3,20	4,00	0,00	3,99	0,00	0,00	0,00	0,00
		Target	47,00	19,00	5,00	3,00	4,00	1,00	0,00	3,00	5,00	0,00	7,00	0,00	0,00	0,00	0,00
WP2000	Security requirements engineering	Actual	105,70	27,81	3,00	3,20	0,00	0,00	4,96	13,30	0,00	39,60	3,47	4,00	6,36	0,00	0,00
		Target	97,00	27,00	3,00	3,00	0,00	0,00	5,00	9,00	0,00	36,00	3,50	4,00	6,50	0,00	0,00
WP3000	Secure on-board architecture design	Actual	146,54	30,50	10,32	4,74	12,00	8,07	0,00	0,00	11,75	0,00	12,25	16,76	40,15	0,00	0,00
		Target	111,50	27,00	8,00	5,00	12,00	6,00	0,00	0,00	9,00	0,00	10,50	13,00	21,00	0,00	0,00
WP4000	Security architecture implementation	Actual	158,37	0,00	14,03	0,00	41,96	22,25	9,07	0,00	11,00	0,00	0,00	20,45	31,11	1,00	7,50
		Target	138,00	0,00	12,00	0,00	40,00	19,00	9,00	0,00	5,00	0,00	0,00	22,00	22,50	1,00	7,50
Total		Actual	455,02	82,11	28,64	11,71	57,29	31,35	14,03	16,50	26,75	39,60	19,71	41,21	77,62	1,00	7,50
		Target	393,50	73,00	28,00	11,00	56,00	26,00	14,00	12,00	19,00	36,00	21,00	39,00	50,00	1,00	7,50

Table 6 Person-month overview for demonstration activities



Demonstration			TOTAL	Fraunhofer	Bosch	Continental Teves	ESCRYPT	Infineon	Fujitsu	MIRA	TRIALOG	K.U. Leuven	BMW F+T	Institut Telecom	Eurecom	FSEU	FEAT
WP5000	Demonstration	Actual	52,99	0,00	10,21	6,84	20,63	2,27	0,00	0,00	0,00	0,00	6,54	0,00	0,00	1,50	5,00
		Target	55,50	0,00	10,00	5,00	20,00	4,00	0,00	0,00	0,00	0,00	10,00	0,00	0,00	1,50	5,00
Total		Actual	52,99	0,00	10,21	6,84	20,63	2,27	0,00	0,00	0,00	0,00	6,54	0,00	0,00	1,50	5,00
		Target	55,50	0,00	10,00	5,00	20,00	4,00	0,00	0,00	0,00	0,00	10,00	0,00	0,00	1,50	5,00

Table 7 Overall person-month overview



		TOTAL	Fraunhofer	Bosch	Continental Teves	ESCRYPT	Infineon	Fujitsu	MIRA	TRIALOG	K.U. Leuven	BMW F+T	Institut Telecom	Eurecom	FSEU	FEAT
TOTAL ACTIVITIES	Actual	525,28	99,38	38,85	18,55	77,92	33,62	14,03	16,50	26,75	39,60	26,25	41,21	77,62	2,50	12,50
	Target	465,00	89,00	38,00	16,00	76,00	30,00	14,00	12,00	19,00	36,00	31,00	39,00	50,00	2,50	12,50

3.4 Project status

The project is finished and has achieved its main objectives.