PROJECT FINAL REPORT

JU Grant Agreement number: ***100204***

Project acronym: ***pSHIELD***

Project title: ***pilot embedded Systems arcHItecturE for multi-Layer Dependable solutions***

Date of latest version of Annex I against which the assessment will be made:

Period covered: from 01.06.2010 to 31.12.2011

Name, title and organisation of the scientific representative of the project's coordinator[1]:

Dr. Josef Noll (MOVATION)

Tel: +47 9083 8066

E-mail: josef.noll@movation.no

Project website[2] address: http://www.pshield.eu

[1] Usually the contact person of the coordinator as specified in Art. 8.1. of the grant agreement

[2] The home page of the website should contain the generic European Emblem and the Joint Undertaking's logo which are available in electronic format at the Europa website (logo of the European flag: http://europa.eu/abc/symbols/emblem/index_en.htm ; logo of the Joint Undertaking: http://www.artemis-ju.eu. The area of activity of the project should also be mentioned.

4.1 Final publishable summary report

pSHIELD Major Achievements

The pSHIELD project represents the first step of the SHIELD Roadmap, planned in the scope of the ARTEMIS-JU. This roadmap foresees two phases: the first one is supposed to be a preliminary investigation of the innovative solutions proposed by the consortium, while the second phase will take care of their actual development and implementation. This report presents the results achieved at the end of phase one.

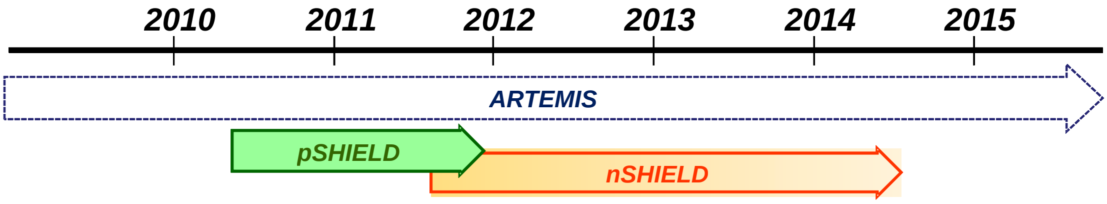

FIGURE 1- SHIELD ROADMAP

Since the pSHIELD project was supposed to be a proof of concept, at first it is useful mentioning what kind of concepts have been identified:

C1. Demonstrate **composability** of Security, Privacy and Dependability (SPD) technologies
C2. Develop **new** SPD **technologies**
C3. Assure **modularity** and **expandability** of the proposed solution
C4. Design an **architectural framework**
C5. Define proper SPD **metrics**
C6. Demonstrate results into an **application scenario** relevant in an industrial perspective

The strategy (in terms of work packages) to address these concepts was the following:

WP1. Project Management
WP2. SPD Metrics, requirements and system design
WP3. SPD Node
WP4. SPD Network
WP5. SPD Middleware & Overlay
WP6. Platform integration, validation & demonstration
WP7. Knowledge exchange and industrial validation

The mapping between concepts and activities is reported in the table 1 and will be useful to analyze the project results.

SHIELD		Activities						
		WP1	WP2	WP3	WP4	WP5	WP6	WP7
Concepts	Composability	X	X			X		
	new technologies	X		X	X	X		
	modularity expandability	X	X			X		
	architectural framework	X	X				X	
	Metrics	X	X					
	application scenario	X					X	X

TABLE 1 MAPPING OF SHIELD ACTIVITIES VS CONCEPT

In particular, at the end of the project, **tangible assets** have been produced to sustain the proof of concepts. They are:

- 28 official **deliverables** (plus 6+2 additional deliverables)
- A dozen of **prototypes**
- Several **papers**, Ph.D. and master thesis
- Targeted industrial, Scientific and public **dissemination**

But the pSHIELD biggest outcomes, that enrich the value of the paperwork, HW and SW produced so far, are the "**ideas**" behind those outputs, and the "**perspectives**" that they have opened: these constitute the pSHIELD major achievements (and heritage of phase 2 nSHIELD).

With respect to the above mapping table, the major achievements described in the following will be listed, WP by WP, and grouped in three areas:

- Consortium and **management** activities (WP1)
- **Scientific** and **technological** achievements (WP2, WP3, WP4, WP5, WP6)
- **Impact**, visibility and business opportunities (WP7)

Among the achievements, particular attention will be devoted to those results that constitute a real breakthrough either in scientific, technological or impact perspective.
For all the mentioned achievements, an indication of the measurable outcome will be provided, as an objective mean of verification of the work carried out.

a. Consortium and management activities

Workpackage 1 was in charge to manage project and partners so as to build an effective team able to realize the SHIELD roadmap. This activity has been really challenging due to external factors:

- The recent economic crisis, that obliged some partners to work without national funding
- The uncertainty in the finalization of national contracts due to internal inertia

Nevertheless, the team succeeded in completing the work and producing results (in some cases with its own resources only), thus demonstrating the clear commitment of industrial and academic players into the SHIELD roadmap.

Major Achievements:

- Clear definition and agreement of roles and responsibilities
- Sharing and capitalization of knowledge coming from consortium members
- Liaison with the second phase thanks to the involvement of nSHIELD coordinator
- Continuity between Phase 1 and Phase 2 assured by the presence of key personnel

Breakthroughs:

- The SHIELD "Team" has been built

Measurable outcomes:

- Consolidation and intensive use of collaborative tools (Wiki, SVN, …)
- Delivery of all documents
- Project completion in time (after the re-focus)

b. Scientific and Technological Achievements

Workpackage 2 was in charge to formalize the pSHIELD Architecture, requirements and, above all, metrics (that constitute the key enabling technology for the SPD-driven composability). The biggest contribution in this perspective has been done by the adoption of the Common Criteria standard as main inspiration for the definition of the SPD metrics.

Major Achievements:

- Identification and formalization of a coherent SPD Metrics
- Formalization of two methodologies to compose the SPD Metrics
- Compliance with the existing standard Common Criteria

Breakthroughs:

- Compliance with the existing standard Common Criteria (ISO 15408)
- Consistently measured, without subjective criteria
- Expressed as a cardinal number
- Context specific, relevant enough to make decisions

Measurable Outcomes:

- D2.2.1-2 pSHIELD SPD Metrics
- Implementation of one of these methodologies into WP5 prototypes with the semantically-enabled metrics composition

Workpackage 3 was responsible for the technical and scientific achievements in terms of innovative SPD technologies at node level. This activity has produced some of the most significant pSHIELD prototypes, by delivering concrete hardware platforms.

Achievements:

- Design of *generic conceptual model* of a pSHIELD node for all node types, which can be implemented in different architectures, providing different functionalities, different SPD compliance levels and different services, depending on the type of node and application field. Three node types represent very different devices but they share the same conceptual model, enabling a seamless composability.
- Power Node PCB Layout design
- Study on cryptographic solution for all kinds of nodes with limited resources
- Design and implementation of a protection circuit for a power supply (dependable power supply)
- Development of a new cryptographic key exchange protocol (The major finding is that with this protocol it is possible to increase the lifetime of the cryptographic keys during a session and greatly increase the strength of the underlying cryptographic algorithm against cryptanalytic attacks while keeping the computational overhead to minimal levels).

Breakthroughs:

- Node secure and dependable by construction
- Development and implementation of Partial Reconfigurable Node based on FPGA Programmable Reconfigurable Device (PRD) concept
- pSHIELD node installation was the first on a real M2M platform

Measurable Outcomes:

- D3.1-2-3-4
- pSHIELD SPD FPGA Power Node prototype

- Protection board prototype
- Integration with Telenor Shepherd® Platform
- Connectivity with Shepherd® Platform
- Prototype of cryptographic algorithms into a micro node (TelosBmote)
- Partial Reconfigurable Trans-/Receiver FSK node

Workpackage 4 was responsible of the advances in Network technologies, with the aim of formalizing the innovative pSHIELD Network. The key technology in this perspective is the cognitive radio that allows the *cognitiveness* of the whole network.

Achievements:

- Development of a real Cognitive Radio Node software that is able to automatically detect the presence of a threat and adjust internal radio transmission parameters accordingly
- Establishment of communication across heterogeneous platforms, thus preparing for *security interworking*
- ETSI M2M platform functionality TS102.690 supported by the access to the telecom platform
- Realization and adaptation of HW and SW of multicore platform for the cognitive algorithm validation on embedded system
- Implementation of a Cognitive Radio Node software simulator
- Identification of spectrum sensing features for Cognitive Radio analysis
- Adaptation of sensing part of the Cognitive Radio simulator for pSHIELD
- Study of the requirements for lightweight link-layer secure communication in wireless sensor network scenarios and the design and development of proper schemes focusing on confidentiality. More specifically, intrusion detection systems (IDS) have been studied.
- Study of the resource footprint (energy consumption among them) and its impact on performance on some commercially available devices
- Studies on the setup of a general framework for secure communications within heterogeneous networks comprising resource-limited devices

Breakthroughs:

- Miniaturization of Cognitive Radio Technologies

Measurable Outcomes:

- D4.1-2
- Network prototypes (miniaturized SDR node)
- Innovative approaches for SPD driven transmissions and Trusted and dependable connectivity
- Spectrum Sensing for SPD driven transmissions and Trusted and dependable connectivity
- Physical layer Techniques enabling SPD driven transmissions and Trusted and dependable connectivity

Workpackage 5 has represented the key technological workpackage, in charge of producing the SHIELD enablers at Middleware level. pSHIELD Middleware is the glue that allows the composition of pSHIELD elements, properly described by the pSHIELD Semantic Model.

Achievements:

- Drawing of an original pSHIELD ontology
- Semantic model compliant with defined metrics

- Design and implementation of a reduced but significant “working” example of the pSHIELD Middleware and Overlay. This Middleware is able to discover and compose SPD functionalities to achieve the desired SPD level.
- Technological Assessment of the Policy Based Management for Security applications and preliminary feasibility analysis with respect to pSHIELD
- Formulation of an innovative model to represent (composable) Embedded Systems based on the theory of Hybrid Automata. Thanks to this formulation it has been possible to apply some closed-loop control algorithms (like MPC) to optimize the SPD composability in a context-aware way.

Breakthroughs:

- Definition and implementation of an original ontological model of ESs, including the semantic characterization of the system and inferential engine features (based on specific metrics) to face the SPD composability problem
- Harmonization of control algorithms, Policy Based Management and Common Criteria approaches in the Security Agent architecture

Measurable Outcome:

- D5.1-2-3-4
- A prototype owl file with the pSHIELD Ontology has been obtained
- A prototype of a reasoner has been integrated into the pSHIELD Middleware emulator
- An OSGI prototype of the pSHIELD middleware performing composability tasks in collaboration with CS nodes is available for demonstration
- D5.2 Analysis on Policy Based Management
- Closed-loop algorithms simulations

Workpackage 6 had the responsibility of integrating the pSHIELD technologies and testing them into an application scenario relevant in an industrial perspective. The environment selected for the pilot project was the railways application domain, and in particular the management of freight trains transporting hazardous materials.

Achievements:

- Identification and test of two platforms suitable for the integration with the pSHIELD key functionalities for the final demonstrator in the railways scenario: These platforms were provided by Movation, in collaboration with Telenor and the Norwegian Rail Authorities (JBV), and Ansaldo, in collaboration with University of Naples.
- Definition of the use case environment in the form of freight trains transporting hazardous material
- Demonstration of the usability and transmission of data produced by sensors, in the service of specific use case scenarios as critical infrastructure protection
- Exploration of the platform’s synthetic capability and composability, through possible synergies and fusion/cooperation of components

Breakthroughs:

- Identification of several additional prototypal demonstrators to show the interoperation among different (composed) technologies and the possibility of realizing SPD functionalities

Measurable Outcomes:

- D6.1-2-3-4
- Prototypal Demonstrators
- Architecture, analysis and tests performed by ASTS
- Architecture and analysis performed by Movation

- On site and on track trial with the Norwegian and Italian Railways

In particular, the prototypal demonstrators are (with the indication of the addressed functionality):

- ✓ **FPGA Power node prototype** (SPD)
  SPD metrics, Self-recovery from hardware transient faults (through fault injection), Auto reconfiguration, Data encryption, Provision of security and privacy services, Hardware data encryption/decryption
- ✓ **Cognitive Radio prototype** (SPD)
  Threats tolerant transmission
- ✓ **Middleware prototype for composability** (SPD)
  SPD Audit, Cryptographic Support, Identification and Authentication, Protection of the SPD functionalities, Security Management
- ✓ **Heterogeneous Platform prototype** (SPD)
  Auto start up on power failure, Auto reconfigurable on software failure, Auto synchronization on software failure, End-to-end secure communication, Mal-user detection, Access control for accessing sensor data
- ✓ **Rail car monitoring system** (SPD)
  Intrusion awareness, fault-tolerance, data redundancy and diversity

c. Impact, visibility and business opportunity

Workpackage 7 was the interface between the project and the outside world, in charge of dissemination and exploitation activities of the project. The strong exploitation of project results into industrial context (and with the active collaboration of external industrial partners) has been one of the most valuable results of pSHIELD.

Achievements:

- Targeted dissemination at top level, including telecom actors (Telenor), industrial actors (ABB) and security research institutes (Norwegian Defense Research Establishment)
- Real world interworking of sensors on the measurement locomotive of the Norwegian Rail Authorities and Telenor Objects
- pSHIELD implementation in place in an electrical motorcycle at the showroom of Telenor, the Innovation Fair at Fornebu
- Foundation of IoT/Future Internet *Value Network* for Industrial Ecosystem

Breakthroughs:

- Awareness of the IoT Ecosystem for semantic-based security

New Challenges:

- Scalability: Transformation from SPD sensor to SPD application

Measurable Outcome:

- Dissemination and Exploitation reports
- Field trials

✓ pSHIELD references

Here follows the list of all beneficiaries with the corresponding contact name and associated coordinates as well as the address of the public Website of the Project and other relevant contact details:

- SESM S.c.a.r.l (IT) adimarzo@sesm.it
- Acorde (ES) silvia.mier@acorde.com
- Ansaldo STS (IT) antonio.ruggieri@ansaldo-sts.com
- Critical Software (PO) jverissimo@criticalsoftware.com
- Selex Elsag (ex Elsag Datamat) (IT) elisabetta.campaiola@selexelsag.com
- EuroTech (IT) p.azzoni@ethlab.com
- Hellenic AeroSpace Industry (GR) PAPPAS.Nikolaos@haicorp.com
- Selex Elsag (ex Selex Communication) (IT) marco.cesena@selexelsag.com
- THYA (SL) sdrakul@thyia.si
- TRS (IT) gabriele.natoli@trs.it
- Movation (NO) josef.noll@movation.no
- European Software Institute (ES) Inaki.Eguia@tecnalia.com
- Center for Wireless Innovation (NO) zahid.iqbal@unik.no,
- ATHENA (GR) stefanidis@ece.upatras.gr
- Mondragon Goi Eskola Politeknikoa (ES) info@mondragon.edu
- Università Sapienza di Roma (IT) vincenzo.suraci@dis.uniroma1.it
- Università Genova (IT) mlucio@dibe.unige.it
- WEBSITE and collaborative tools WIKI www. http://pshield.unik.no
- PSHIELD website http://www.pshield.eu/

✓ Conclusions

By exploring all the material produced during the pSHIELD project, the following conclusions can be drawn:

- It is possible to define the characteristics of a pSHIELD component and of the pSHIELD system (Design Architectural Framework)
- It is possible to quantify security, privacy and dependability (Define metrics)
- It is possible to improve SPD technologies (Develop new technologies)
- It is possible to compose SPD technologies according to the selected metrics (Demonstrate composability)
- The composability mechanism is independent to the number and type of underlying technologies (Assure Modularity and expandability)
- It is possible to provide enriched services and application to relevant application scenarios with SPD requirements (Demonstrate into an Application scenario)

Furthermore, a list of open issues and new challenges has been identified: this will constitute the basis of the work to be done in nSHIELD.

Management challenges

- Perform a seamless handover towards nSHIELD
- Share the background with the new partners so that they can enrich the consortium capabilities

Scientific/Technical challenges

- Extend and enrich the Common Criteria composition approach to capture the complexity of systems
- Composability between pSHIELD nodes and pSHIELD network
- Cover the whole chain to certify the Softcore of an Embedded Node (never certified before)
- Implementation of Cognitive Network Functionalities: cognitive resource management, spectrum-aware routing, …
- Enrich and refine the semantic model to reinforce the composability mechanism
- Replicate this environment on a real world middleware
- Improve the overlay behavior by enabling interaction between Security Agents
- Enrichment of control algorithms (i.e. DES Theory)
- Address nSHIELD new scenarios and technologies

4.2 Use and dissemination of foreground

Section A (public)

Dissemination Activities

pSHIELD project promoted dissemination activities towards the following main areas:

- Targeted Industrial Dissemination
- Scientific dissemination
- Industrial publications
- Workshops and Exhibitions

Industrial Contacts

This text summarises the feedback provided from companies and public organisations after meetings with pSHIELD participants. These meetings are established to either discuss technology, applications or aspects of the eco-system for secure sensor information. From the Norwegian side, the main focus is on bringing pSHIELD sensors into a standardised machine-to-machine (M2M) and machine-to-business (M2B) environment. Movation is member of ETSI and Artemisia, and through these ones fosters interoperability as e.g. ETSI TS102.690 "Functional architecture for an M2M platform". Movation has the main focus on bringing pSHIELD results to the sensor and Telecom industry in Norway. A close cooperation of the pSHIELD partners Movation and CWIN is established with Telenor Objects, resulting in the first implementation of a mobile IoT platform foreseen for demonstrations with the Norwegian Rail Authorities. CWIN concentrates on the extensions of the platform towards sensor description and access, both based on semantic technologies. From Slovenian side, the main focus is on the next generation networks (NGNs) in which the pSHIELD SPD networks like SPD-WSNs will take part for many application scenarios, like critical infrastructure protections, smart grids, intelligent transportation and social mobility networking. The SPD-WSNs are the main research focus area of THYIA. As member of WWRF forum, Artemisia, Net!Works (before e-Mobility TP), member of security steering board TMGS TA2, HLG KETs, Artemis TP Slovenia, ICT TM Slovenia, THYIA widely disseminated the pSHIELD concepts and results. In parallel, THYIA’s national project TITRES (Technology Innovation in Telecommunications for Rational Ecological Systems) included smart grid concepts and SPD features for the next smart devices that THYIA is developing for the European market. Additional, THYIA is contributing with innovative SPD concepts in ME3GAS JU ARTEMIS project which addressed smart metering, M2M devices and smart grid infrastructures. THYIA has contributions on the national workshops organised by industrial partners and Slovenian’s Government where they demonstrated the pSHIELD advantages and new concepts for ESs.

Scientific dissemination

Here after the full white papers and scientific papers list PSHIELD related.

- Mariana Esposito, Inaki Eguia, Francesco Flammini, Alfio Pappalardo and Erkuden Rios, "Formalizing SPD metrics for Embedded Systems Multilayer approach" Second Eastern European and Mediterranean Software Process Improvement Conference (EuroMed SPI II), Zamudio, Spain, October 6-7, 2011.
- Josef Noll, "Security, Privacy and Dependability in the Internet of Things (IoT)", WWRF#27, invited paper to WG7, 18.-20. October 2011.

- Josef Noll, Zahid Iqbal and Mohammad M.R. Chowdhury, "Integrating context- and content-aware mobile services into the cloud", CWI/CTIF seminar on Mobile Cloud Computing and wireless applications, 24.-25. October 2011, Aalborg University in Copenhagen.
- V. Voyiatzis, K. Stefanidis and D. N. Serpanos: "Increasing Lifetime of Crypto Keys on Smartphone Platforms with the Controlled Randomness Protocol", In Proceedings of 6th Workshop on Embedded Systems Security WESS 2011, October 2011.
- Iñaki Garitano, Roberto Uribeetxeberria and Urko Zurutuza, "Review of SCADA Anomaly Detection Systems", Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011, Salamanca (Spain) in April, 2011, ISBN 9783642196447.
- Urko Zurutuza , Enaitz Ezpeleta, Álvaro Herrero and Emilio Corchado "Visualization of Misusebased Intrusion Detection: Application to Honeynet Data", Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011,Salamanca (Spain) in April, 2011, ISBN 9783642196447.

- Ekhiotz Jon Vergara, Simin Nadjm-Tehrani, Mikael Asplund and Urko Zurutuza, "Resource Footprint of a Manycast Protocol Implementation on Multiple Mobile Platforms", Fifth International Conference on Next Generation Mobile Applications, Services and Technologies,NGMAST 2011, Cardiff, Wales, UK, 14-16 September 2011.
- Fiaschetti A., Lavorato F., Suraci V., Palo A., Taglialatela A., Morgagni A., Baldelli A., Flammini F., "On the use of semantic technologies to model and control Security, Privacy and Dependability in complex systems" Proc. Of 30th International Conference on. Computer Safety, Reliability and Security (SAFECOMP'11), Sep. 2011. Naples, Italy.
- Sarfraz Alam, Mohammad M. R. Chowdhury, Josef Noll, "Interoperability of Security-enabled Internet of Things", to appear in Wireless Personal Communication Special Issue on "Internet of Things and Future Applications", Springer-Netherland, 2011.
- Mohammad M. R. Chowdhury, Josef Noll, "Securing Critical Infrastructure: A Semantically Enhanced Sensor Based Approach", 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic System Technology, WiRELESS ViTAE 2011, Chennai, India, Feb. 28-March 2011.
- K. Stefanidis, A. V. Voyiatzis and D. N. Serpanos: "Performance of the Controlled Randomness Protocol on .NET Compact Framework Embedded Systems", In Proceedings of 4th IFIP International Conference on New Technologies, Mobility and Security, Paris, France, February 2011.
- Bixio, M. Ottonello, M. Raffetto, and C.S. Regazzoni, "Comparison among Cognitive Radio Architectures for Spectrum Sensing," EURASIP Journal on Wireless Communications and Networking, vol. 2011, Article ID 749891, 18 pages, 2011. doi:10.1155/2011/749891
- L. Bixio, L. Ciardelli, M. Ottonello, M. Raffetto, C. S. Regazzoni, Sk. S. Alam and C. Armani, "A Transmit Beamforming Technique for MIMO Cognitive Radios,", Wireless Innovation Forum Conference on Communications Technologies and Software Defined Radio, SDR'11 -WInnComm - Europe, Brussels, Belgium, June 22-24, 201
- Sk.S. Alam, L. Marcenaro and C.S. Regazzoni, "Opportunistic Spectrum Sensing and Transmissions", in Cognitive Radio and Interference Management: Technology and Strategy, Meng-Lin Ku and Jia-Chin Lin eds, IGI Global, 2012
- Sarfraz Alam, "A Security Proxy for User-centric Internet of Things", Wireless World Research Forum (WWRF) #25, Kingston, UK, 16.-18. November 2010
- Sarfraz Alam, Mohammad M. R. Chowdhury, Josef Noll, "An Event-driven Sensor VirtualizatiApproach for Internet of Things", *poster*, VERDIKT conference, Oslo, 1.-2. November 2010

Industrial publication

- Giuseppe Martufi, Fabrizio de Seta, "pSHIELD for Embedded System Security", EDlink 37 (Elsag Datamat Company Magazine), Rome, 2010.

Workshops and Exhibitions

- Valentina Casola, Mariana Esposito, Francesco Flammini, and Nicola Mazzocca, "Monitoring railway infrastructures, a case-study for the pShield project" The 2nd International Workshop on Mobile Commerce, Cloud Computing, Network and Communication Security 2012 at IMIS 2012.(UNDER REVISION)
- Josef Noll, "Security challenges in the Internet of Things" (Media:CoSummit-SecurityInIoTOct2011.pdf),[ARTEMIS/ITEA2Co-Summit 2011], Panel on Trends in ICT Security, 24-26 October2011, Helsinki,Finland
- Josef Noll (Movation AS), Przemyslaw Osocha (SESM), "pSHIELD project - demonstration of SPD prototypes", Exhibition, 24-26 October 2011, Helsinki, Finland
- Przemyslaw Osocha, João Carlos Cunha, "SPD Power Node ES solution in pSHIELD framework", ERCIM/EWICS/Cyberphysical Systems Workshop at SAFECOMP 2011, 22 September 2011, Naples, Italy
- Przemyslaw Osocha, "Standardization of future European Embedded Systems solutions", Marie Curie Researchers Symposium SCIENCE – Passion, Mission, Responsibilities", Polish Presidency of the EU Council, 25-27 September 2011, Warsaw, Poland
- Przemyslaw Osocha (SESM), Yen Pham (CWIN), "pSHIELD-pilot embedded Systems arcHItecturE for multi-Layer Dependable solutions", ARTEMIS Spring Event at Embedded World 2011, 1-3 March 2011, Nuremberg, Germany
- Przemyslaw Osocha (SESM), Yen Pham (CWIN), "Demonstrating Security, Privacy and Dependability for Sensors to Systems", ARTEMIS IA Co-summit 2010 Project Exhibition, 26-27 October 2010, Ghent, Belgium
- "pSHIELD and security in embedded systems", Internal Seminar, Critical Software, 08 October 2010, Coimbra, Portugal
- Spase Drakul, "Strategic Vision of the TITRES project," National Workshop, Ministry of Economy Republic of Slovenia, October 2010, Ljubljana, Slovenia.