2nd Annual review
Florence 15 November 2013

Open Issues from the first Review Meeting

Responsible of the activity: nSHIELD Consortium
Presenter: Andrea Fiaschetti – Univ. "La Sapienza"

Open issue #1 - **CLOSED**

Reference	Issue 1	**Validity**	all review	**Status**	closed
Issue	Provide all deliverables both electronically and in printed form to the reviewers latest 2 weeks (14 days) before the date of the review.				
Due Date	2nd review				
Answer	The Issue has been fully addressed. In addition, for this second review a printed copy of all deliverables has been delivered directly to the reviewer				

Open issue #2 - **CLOSED**

Reference	Issue 2	**Validity**	all review	**Status**	closed
Issue	The project is kindly asked to provide printouts of the presentations at the start of the review meeting.				
Due Date	2nd review				
Answer	Printouts of the presentations provided at the beginning of the meeting				

Open issue #5 - **CLOSED**

Reference	Issue 5	**Validity**	2nd review	**Status**	closed
Issue	pSHIELD D3.2 (p. 89ff) gives an excellent treatment of the CIAA properties (Confidentiality, Integrity, Authenticity and Availability). However, two additional properties should also be handled (at least thought about in this context): Non-repudiation and traceability. These properties become very important, e.g. in the case of a railway accident with dangerous materials (= pilot applications) when actions and decisions of different parties need to be presented to an enquiry or to a court of law. nSHIELD should present a decision on this topic.				
Due Date	2nd review				
Answer	For those applications who require non repudiation and traceability we have methodologies and mechanisms (e.g. digital signatures and tamper proof audit logs) ensuring the provisioning of these qualities. However in certain systems (e.g. Oil industry) other security parameters (like latency) may prioritize other security mechanisms				

Open issue #6 - **ONGOING**

Reference	Issue 6	**Validity**	2nd review	**Status**	ongoing
Issue	Recommendation: The consortium is invited to author and publish a "nSHIELD Textbook" and publish it with a reputed publisher (e.g. Springer). This textbook should be a complete, comprehensive and consistent tutorial, providing an easy and interesting entry into the nSHIELD world for engineers and potential users				
Due Date	2nd review				
Answer	A preliminary ToC started circulating				

Open issue #7 - **CLOSED**

Reference	Issue 7	**Validity**	2nd review	**Status**	closed
Issue	nSHIELD propses a number of fragmented (?) demonstrators, each showing part of the nSHIELD achievements. nSHIELD should aim for one (or more) significantly larger and more integrated demonstrator(s). This would prove the integration efforts of the consortium and contribute to the ARTEMIS objective of reducing the ES fragmentation in today's industry. As a first step, a table or graph should be made which clearly shows which new technologies are used for which demonstrator.				
Due Date	2nd review				
Answer	A matrix that maps technologies over demonstrators is being prepared				

Open issue #8 - **CLOSED**

Reference	Issue 8	**Validity**	2nd review	**Status**	closed
Issue	Certification support during development is an important objective for nSHIELD. The project should create a liaison with the ARTEMIS-JU certification group (Contact follows from Antonio) and include the findings into the project work. Certification should be an explicit outcome of nSHIELD.				
Due Date	2nd review				
Answer	The PROSE project is closed (ended two years ago). Standardization mainly addressed and less certification. No security/privacy topics addressed in the certification field. ARTEMIS practice: - Doing certification for environment (e.g. automation, sustainable environment, …) - Doing technology/tool platforms certification (e.g. network security protocol certification 802.15.4 for security module prototype Euromils FP7 project Protection Profile (national certification authority) Ongoing certification procedure for UAV IQ Engine Kernel				

Open issue #9 - ONGOING

Reference	Issue 9	**Validity**	final review	**Status**	ongoing
Issue	Incremental certification will be one of the key cost reduction factors in future embedded systems. Some projects and groups are already working on this topic. Accepting incremental certification needs some “education” of the National authorities. nSHIELD should make contact to their respective National authorities and start discussing this topic				
Due Date	Final review				
Answer	National contacts in norway established. Focuse is on global infrastructure for Oil and Gas industry (ISO 15926)and transport (ISO 26262)				

Open issue #10 - **CLOSED**

Reference	Issue 10	**Validity**	2nd review	**Status**	closed
Issue	The proposed demonstrators are of high interest. However, it is at the time being not clear, what will really be shown in each demonstrator, i.e. which pieces of nSHIELD results will form part of the respective demonstrators. The review team would like to see either one “ultimate” demonstrator which shows in real hardware and software the most significant results and tools produced by nSHIELD. If more than one demonstrator is chosen (e.g. the UAV and the train), then please clearly indicate which technology is used in which demonstrator. Ideally, the same technology should be used in more than one demonstrator.				
Due Date	2nd review				
Answer	A matrix that maps technologies over demonstrators is being prepared				

Open issue #11 - **ONGOING**

Reference	Issue 11	**Validity**	final review	**Status**	ongoing
Issue	One risk for industry acceptance of nSHIELD methods are existing process standards, such as Autosar, IMA, ... which are very hard to change. nSHIELD should carefully study the most important development standards and compare gaps/differences and address them accordingly.				
Due Date	Final review				
Answer	Discussions with key players driving the development (e.g. ABB). Upgradeable infrastructure and modularity are the challenges for the next years Goups in Autostar and IMA working on security and safety, expecially in transport systems: Liaisons could be established by the end of nSHIELD project by TECNALIA (groups involved in Autostar and IMA) OPENCOSS Project.				

Open issue #12 - **ONGOING**

Reference	Issue 12	**Validity**	2nd review	**Status**	ongoing
Issue	nSHIELD should start early to build industry acceptance. “Measurable security” and the composition approach – this must be developed by targeted measures at an early stage (as part of the dissemination activities). For the composition approach pay explicit attention to the definition of interfaces. Please include a section on this objective & results in the dissemination plan				
Due Date	Finale review				
Answer	These topicsa re planned to be included in the dissemination plan				

Open issue #13 - **CLOSED**

Reference	Issue 13	**Validity**	2nd review	**Status**	closed
Issue	During the 1st review it was mentioned, that Finmeccanica is developing its own ES operating system (which was later weakened to “virtualization software”). The review team reminds the project that the introduction of a new OS/system software into the ES market is a major undertaking with a very high acceptance risk. If nSHIELD wants to go this route, the review team needs a good justification as part of the exploitation plan				
Due Date	2nd review				
Answer	Misconception. An internal check within Finmeccanica companies has been performed: this OS System is a Linux distribution already deveoped and tailored for Finmeccanica (internal) purposes and is out of scope for the nSHIELD project. No plan to push it on the market.				

Open issue #14 - **CLOSED**

Reference	Issue 14	**Validity**	2nd review	**Status**	closed
Issue	The work packages should be technically better coordinated: They sometimes work on individual assumptions and different models. A unified, accepted global picture is missing. Suggestion: In another project with similar challenges, the project management instituted a “Technical Task Force (TEF)” which worked as a horizontal coordination body for all work packages – with tremendous success for the consistency of the project results!				
Due Date	2nd review				
Answer	Task force stablished				

Open issue #15 - **CLOSED**

Reference	Issue 15	**Validity**	2nd review	**Status**	closed
Issue	Thyia is not performing according to their tasks defined in the TA. Thyia's effort in the reporting period is 0 MM. Their contribution to WP2 in the reporting period was nil (the contribution had to be authored by Luigi Trono). The project needs to remedy this partner situation.				
Due Date	2nd review				
Answer	An agreement has been reached between THYIA, The consortium and the Commision about its involvement in the prosecution of the project.				

Open issue #16 - **CLOSED**

Reference	Issue 16	**Validity**	2nd review	**Status**	closed
Issue	Rework D1.2 (Quality control guidelines) to really make it a binding process and metrics document and resubmit it for the 2nd review.				
Due Date	2nd review				
Answer	D1.2 re-worked according to the reviewers' indication and resubmitted for the second review meeting				

Open issue #17 - TBD

Reference	Issue 17	**Validity**	all review	**Status**	TBD
Issue	The project has been asked to improve the financial reporting, shortening the report and summarizing the figures in comprehensive tables and figures				
Action	To follow the reviewer suggestion in the preparation of the financial report.				
Due Date	2nd review				
Answer	The comment is undestood and in principle agreed. The partners should improve their efficiency in reporting activities; however some partners (e.g. UNIROMA1) are obliged to provide reports plenty of details because these reports are the mean adopted by National Evaluators to match technical activities vs involved resources: lack of details could lead to unsufficient justification of costs. In any case the consortium would appreciate if ARTEMIS could provide an example or a template of Financial reporting that is more in line with the reviewer needs				

Open issue #3 - ONGOING

Reference	Issue 3	**Validity**	2nd review	**Status**	Ongoing
Owner	Task Force	**Responsible**	Andrea F.	**Support**	ASTS, MGEP, MAS
Issue	As already mentioned in the recommendations from pSHIELD the project lacks a sufficient and consistent formal base (in the form of formal models!). This is a major divergence risk for the project. The project needs to agree on a few, basic, coordinated formal models which are binding for all work packages.				
Action	To define a formal model for some of the components presented in the project, trying to adopt the methodology suggested by the reviewer, but being much more close to the metrics rationale.				
Due Date	2nd review				
Answer	An abstraction ontology has been defined, mainly based on the attack surface metrics approach: it is expected to model in the most generic and abstract way a SHIELD component. In the prosecution of the demonstration activities formal models (e.g. SySML or UML) will be adopted to describe th edemonstrators' architecture.				

nSHIELD

Open issue #4 - **CLOSED**

Reference	Issue 4	**Validity**	2nd review	**Status**	closed
Owner	SES/ TECNALIA	**Responsible**	Renato B. Inaki E.	**Support**	-
Issue	A more formal and systematic framework is also needed for the SPD metrics. At this point there are 60 types of SPD metrics. How to make sure there are no security holes nor overlaps between metrics? How to add/remove metrics?				
Action	To provide clarification on the point raised by the reviewer. To provide a methodology for metric composition. Two methodologies currenty being taken into account				
Due Date	2nd review				
Answer	Two systematic approaches have been conceived and detailed: the multimetrics approach and the attack surface approach				