Project no: 269317

nSHIELD

new embedded Systems arcHItecturE for multi-Layer Dependable solutions

Instrument type: Collaborative Project, JTI-CP-ARTEMIS

Priority name: Embedded Systems

D1.2 Quality Control Guidelines

Due date of deliverable: M3 – 2011.11.30

Actual submission date: M7 – 2012.03.21

Second submission date: M24 – 2013.08.31

Start date of project: 01/09/2011 Duration: 36 months

Organisation name of lead contractor for this deliverable:

Selex ES, SES

Revision [4]

Project co-funded by the European Commission within the Seventh Framework Programme (2007-2012)		
Dissemination Level		
PU	Public	
PP	Restricted to other programme participants (including the Commission Services)	X
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)	

Document Authors and Approvals

Authors		Date	Signature
Name	**Company**		
Cennamo Francesco	Selex Galileo	21/03/2012	
-	Hellenic Aerospace Industry		
-	Selex-Elsag		
-	THYIA		
Cecilia Coveri	Selex ES	22/05/2013	
Lorena de Celis	Acorde	27/06/2013	
Cecilia Coveri	Selex ES	29/07/2013	
Reviewed by			
Name	**Company**		
Roberto Uribeetxeberria	MGEP	25/06/2013	
Francesca Matarese	SESM	08/07/2013	
Elisabetta Campaiola	SES	24/07/2013	
Approved by			
Name	**Company**		

Applicable Documents

ID	Document	Description
[01]	TA	nSHIELD Technical Annex
[02]	APCA	ARTEMIS JU Projects' Consortium Agreement
[03]	D1.1	Collaborative tools and document repository
[04]	D0.0	nSHIELD-Acronyms List

Modification History

Issue	Date	Description
Draft - A	6/02/2012	First issue for comments
Issue 1	21/03/2012	Incorporate comments from draft A review
Issue 2	30/05/2013	New structure (after Artemis JU revision) for comments
Issue 3	27/06/2013	Add some comments
Issue 4	24/07/2013	Integrated contribution and revision from partners

Executive Summary

This document describes the Quality Control Process that the project team will follow to assure and control the quality of processes and outcomes produced during the course of the Collaborative Project nSHIELD.

Detailed analysis concerning the identification of obstacles is the main challenge of a collaborative project. This document lists the measures that are taken into account to deal with the identified obstacles.

The challenges inherent to the scope of the project in relationship with the risks and the contingencies of a R&D international project are evaluated.

The Quality Management System, including roles and specific boards, are described.

This document will be used as a guideline to describe and demonstrate the Quality Control Activities executed during the whole life of the project.

Contents

Figures

Tables

Glossary

Please refer to the Glossary document [04], which is common for all the deliverables in nSHIELD.

This Page is intentionally left blank

1 Introduction

1.1 Scope

These Quality Control Guidelines describe the Quality Control Process that the project team will follow to assure and control the quality of processes and outcomes produced during the course of the Collaborative Project nSHIELD.

In fact, it defines how the high level governance principles defined in the APCA [02] and in the Technical Annex [01] are enforced by procedures applicable to all daily project activities.

As an add-on, this document sets out the guidelines for the implementation of Quality Assurance (QA) of the project.

1.2 QA & QC Basic concepts

Quality Assurance (QA) and Quality Control (QC) activities are performed throughout the project. QA is a management process that is prevention-driven, while QC is a project management process that is inspection-driven.

QC is a process by which entities review the quality of all factors involved in production. This approach places an emphasis on three aspects:

- Definition and management of elements such as controls, processes and identification of bottlenecks within the collaborative environment
- Competence, such as knowledge, skills, experience, and qualifications
- Soft elements, such as personnel, integrity, confidence, organizational culture, motivation, team spirit, and relationships.

The QC system is designed to:

- Provide routine and consistence checks to ensure data integrity, correctness, and completeness;
- Identify and address errors and omissions;
- Document and archive the QC activities.

QC activities include general methods such as accuracy checks on data acquisition and calculations and the use of approved standardized procedures, measurements, estimating uncertainties, archiving information and reporting.

QA activities include a planned system of review procedures conducted by personnel not directly involved in the development process. Reviews, preferably by independent third parties, should be performed following the implementation of QC procedures. Reviews verify that data quality objectives were met and support the effectiveness of the QC programme.

QA means to introduce measures for all of the three aspects emphasized by QC.

In order to implement QA/QC activities, it is necessary to determine which methodology should be used, and where and when it will be applied. Technical and practical considerations have to be taken into account:

- Technical considerations related to the QA/QC approaches.

- Practical considerations that involve assessing different circumstances such as available resources and expertise and the particular characteristics of a collaboration project.

Typical QC elements flow is showed in the following picture.

Figure 1: Typical Quality Control elements

2 nSHIELD approach to "Quality"

QC approach in project management is usually related to inspect the accomplished work in order to be in line with the scope of the project. Thus the initial purpose of each quality control is to clearly point out the scope of the project.

The nSHIELD project aims at being a pioneering investigation to address Security, Privacy and Dependability in the context of Embedded Systems (ESs) as "built in" rather than as "add-on" functionalities, proposing and perceiving, with this strategy, the first step toward SPD certification for future ES. The leading concept is to demonstrate composability of SPD technologies.

So the aim of nSHIELD includes the following items:

- How can we demonstrate composability of SPD technologies?
- How can we document the achievements in a sufficient manner?

The following diagram represents the high-level structure describing the quality guidelines for nSHIELD.

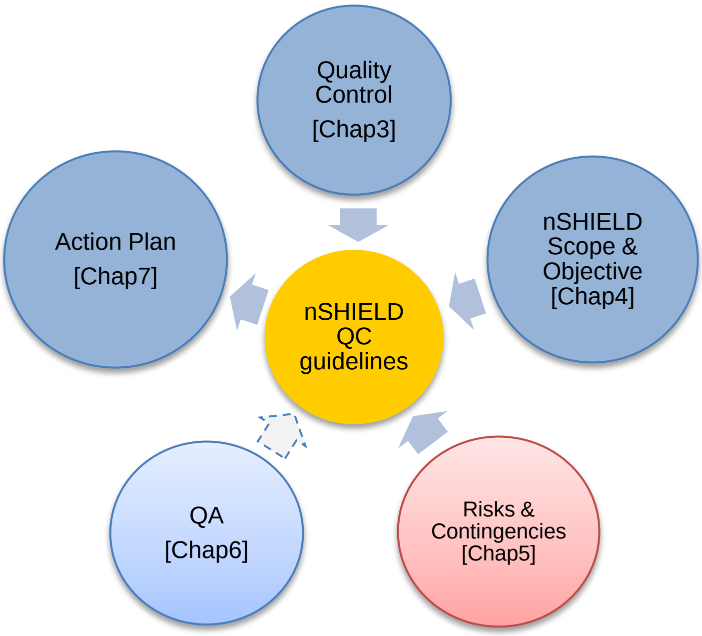


Figure 2: Elements of the Quality Control in nSHIELD

nSHIELD is a collaborative project aiming at creating an innovative, modular, composable, expandable and high-dependable architectural framework and common SPD metrics capable of measuring the overall SPD level in any specific application domain, with minimum engineering effort.

For this reason, the standard elements, concurring to QC guidelines definition of nSHIELD, are considered slightly differently from the standard ones, ref fig.1. The risks and the contingencies that could emerge in the development of such kind of project must be emphasized in the QC guidelines definition respect to the QA requirements. This is due to the fact that QA definitions are generally more applicable to a product than to a technological demonstrator.

In the next paragraphs are reported the concepts of QC and QA in general terms and how these are to be specialized in relation to a collaborative project.

3 Quality Control

QC includes all the operational techniques and activities that are used to fulfil requirements for quality. The focus of QC is principally addressed on the deliverables of the project. As project move through phases, at major milestones, and finally at project completion, scope verification must be performed to ensure that the work is of quality and that the project is aligned with the project consortium expectation.

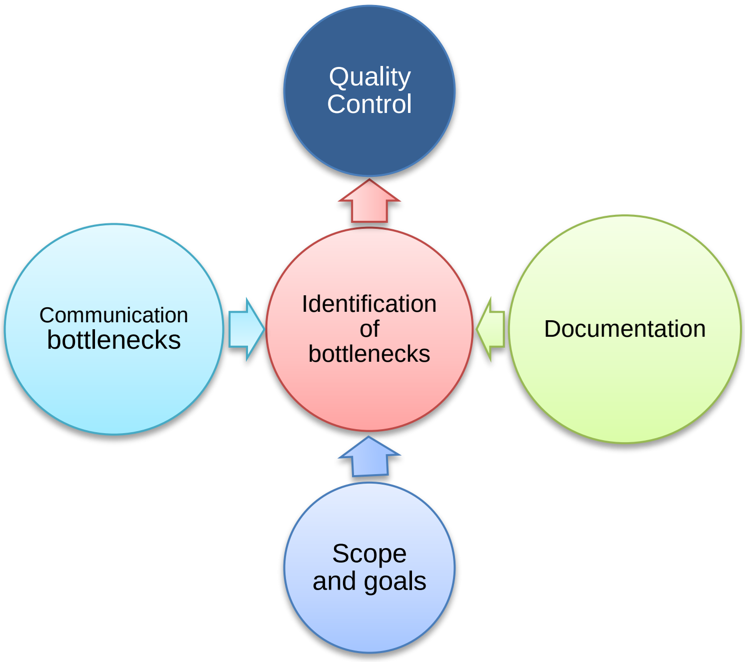
The identification of obstacles is the main challenge of a collaborative project.

Figure 3: nSHIELD QC development and implementation phase

The light blue balls concern three areas strictly connected each other, including culture, competency, and language. In fact, in a collaborative research project, people don't work in the same location, they don't see each other on a regular basis, and the companies, they are working for, might have diverging goals. And even worse, these company's goals might not be in-line with the project goals.

The green balls could be considered more linked with the control processes to be used during the development of the project.

3.1 Identification of bottlenecks



The major source of misunderstanding is due to communication. *Exchange of information* and *information flow* are considered the core assets for a successful project

Identification of bottlenecks includes the three areas

- Communication bottlenecks
- Scope and goals
- Documentation

Figure 4: Identification of bottlenecks

Communication is based on language, culture, medium and topic. *Language* is the most obvious bottleneck and is complicated by the fact that participants to nSHIELD project often talk about a specific topic, which might have a very distinct meaning in the language of the different partners. Additionally, the usage of terms might be subjected to the culture of the company (or of the country). During call conferences, voice quality is often reduced, participants might be difficult to be understood and the level of incoming loudness is quite different.

In research projects there is always a substantial time delay between the time of writing the proposal and the time of executing the activities. This time delay, and the fact that the office in charge of the proposal might not be identical to that performing the work, is a major source of misunderstanding. Though the aim and goals of the project might be clear for the ones who have written them, the description might be somewhat blurry or remains on high-level to ensure flexibility in executing the project. Aim and goals, which are described just on a high level, are a bottleneck for the execution or the project.

The starting point of every project is the Technical Annex that describes in detail the work packages tasks and the expected outcomes in deliverables. The Technical Annex is used in different way by the partners, being followed word by word by someone, or seen as a guideline only, by others. The deliverables are the means to present work towards the JU, project partners, collaborating projects and the public. Unfortunately, some deliverables are often produced after the completion of the task of reference.

The major challenge, identified in bottlenecks related to documentation, is due to the fact that documentation is not synchronous to on-going developments and discussions. Handling documentation is not easy.

The following measures are taken into account to deal with the identified bottlenecks:

a. Support audio conferences with written agenda and minutes available as soon as possible after the meeting
b. Give space to physical meetings such that partners can meet, exchange information and familiarize, thus enhancing the understanding of other cultures

c. Audio conference length no more than 60 minutes
d. Establish measurable outcomes
e. Establish sub-goals for each task, when possible
f. Definition on how the Technical Annex should be used according to JU
g. Use of deliverables as mean of documenting work, but choice of on-line collaboration tools for information exchange
h. Use of common collaboration tools to share the result of the discussions.

Collaborative tools and document repository for the nSHIELD project are described in [03].

3.2 Competency and knowledge

This section will look into the competence of the partners and the results, as compared to the state of technology, on the QC point of view.

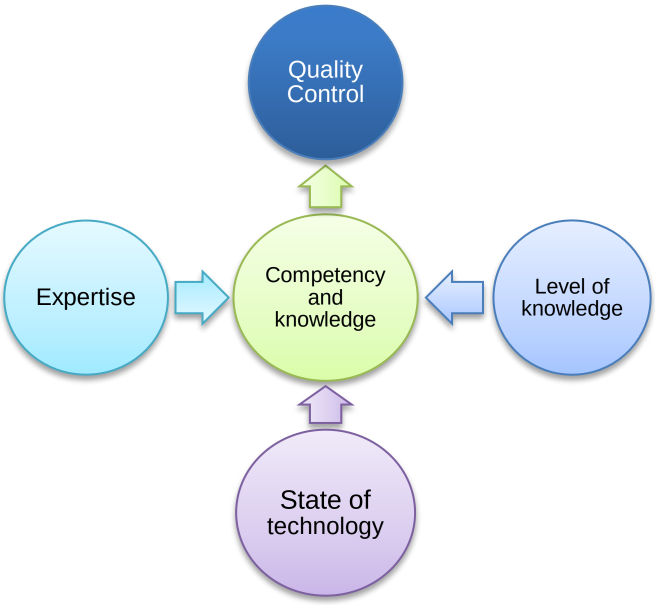


Figure 5: Competency and knowledge

The following figure indicates the challenges related to competency, and especially points out that competency and knowledge have to be compared to the state of technology. Though the wording "state of technology" is commonly used, it might not mean the same thing for participating people. A business-oriented person will always relate the results as how they can be brought to the market, while a research oriented person will always challenge himself as compared to other research results.

The measures in the competency and knowledge area may include:

- Level of knowledge
- Experts in this field
- Comparison to state of technology

The measures taken into account to deal with the identified competency and knowledge bottlenecks are:

a. improvement of internal knowledge exchange by means of training session
b. subgroups of experts (in certain fields) definition
c. definition of the state of technology to be reached: e.g. algorithm development, prototype development.

3.3 Soft elements

Under *soft elements* we mean the personalities of the engaged people, the managerial structures that people find in their respective organization, and the relationships of people. Project participants might be used to take leadership, depending on the culture of the person, of the company, or of the area.

Some cultures tend to have a more collaborative approach, while other cultures prefer a more dominant leadership. While the dominant leader may be perfect for a dissemination and exploitation of results, he might not have the same understanding within the project. A project based on experts needs to look for collaborative leaderships.

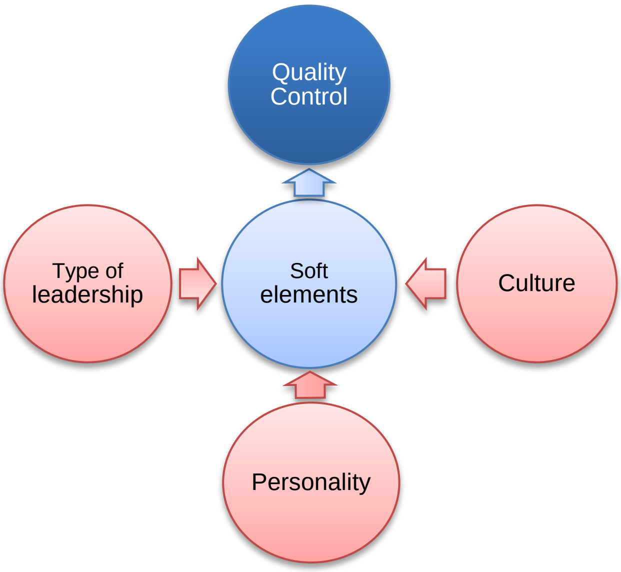


Figure 6: Soft elements that may influence the project

In companies, project participants often go through the process of getting known to each other. They meet each other on daily basis and thus get used to the personality of their co-workers. This is not the case in an international research project.

The countermeasures and the stage for successful collaborative project may include:

a. A collaborative leadership structure built on the expertise of experts in each domain
b. Open meeting allowing cultural exchange and common understanding
c. Leadership shared among participants.

3.4 Errors and omissions identification

nSHIELD is devoted to the demonstrators development and their implementation, so the first step is to identify and address eventual errors and omissions as defined for a basic QC system. Errors and omissions may be caused by incorrect or inaccurate use of information shared with the partners or by data that are inadequately documented for effective use by the consortium.

A detailed errors and omissions map provides a summation and analysis of the information gathered through an identification process, that could be summarized in:

- Reviews of all available information, internal reports, minutes, external reports.
- Questionnaires to be distributed to a few key personnel in the project team to obtain critical information.
- Targeted interviews to round out the information already gathered, in particular to the End User and Advisory Board
- Errors and omissions gap analysis by reviewing the reports through a spiral approach, in order to identify potential gaps and overlaps.

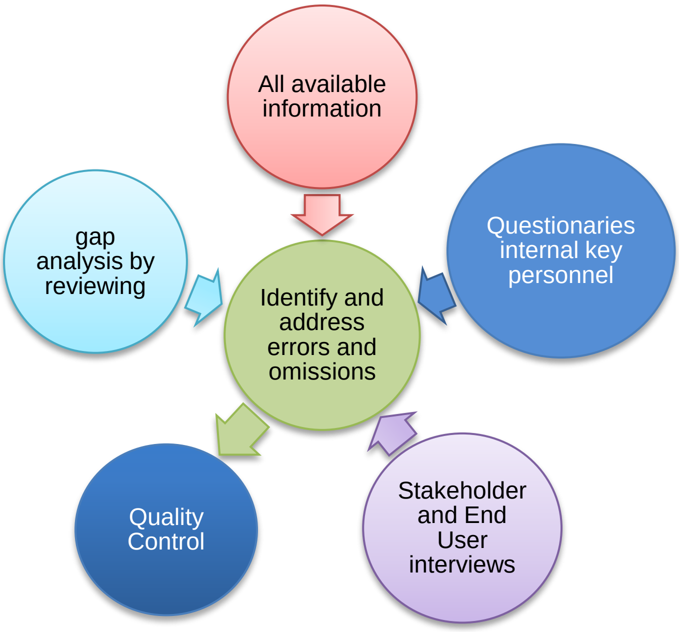


Figure 7: Errors and omissions identification map

Attention is focused on techniques used in particular activities, or stages of Errors and Omissions processes, including:

a. Identifying and mitigating E&O as early as possible, including immediate engagement of partners in addressing the problem;

b. Properly evaluating the nature and impacts of E&O.

3.5 Routine and consistence checks

In computer science, data validation is the process of ensuring that a program operates on clean, correct and useful data. It uses routines, often called "validation rules" or "check routines", that check for correctness, meaningfulness, and security of data that are input to the system. The rules may be implemented through the automated facilities of a data dictionary, or by the inclusion of explicit application program validation logic.

The system nSHIELD aims to establish a modular and scalable SPD framework applicable to different scenarios. Due to this reason it is necessary to define procedures and design routines to preserve the consistency of the program and consistency with the proposed objectives.

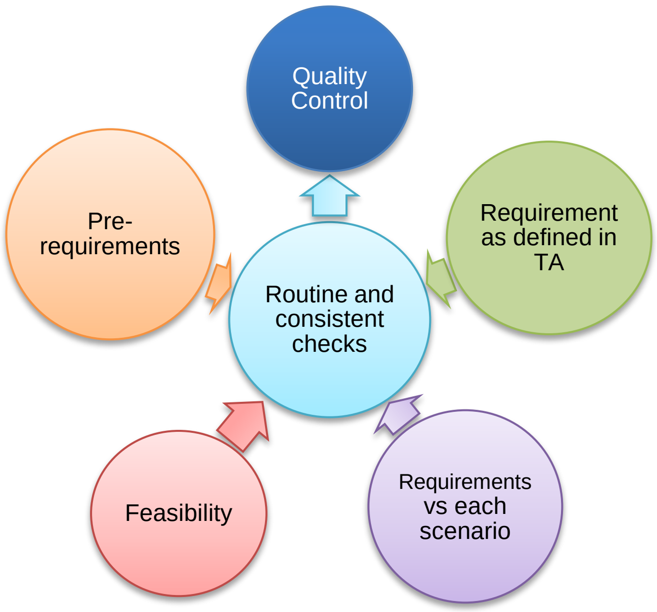


Figure 8: Routine and consistence checks

This process occurs through:

- Verify the consistency of requirements against the Technical Annex
- Verify the consistency of requirements through the different scenarios
- Verify the validity of assumption in each scenarios
- Verify the feasibility of implementation for each scenarios

3.6 QC activities documents and archive

The Quality documentation describes or references the processes, including the roles, responsibilities, and authorities of management and team, for:

Figure 9: QC activities documents and archive

- identifying quality-related documents and records requiring control;
- preparing, reviewing for conformance to technical and quality system requirements, approving, issuing, using, authenticating, and revising documents and records;
- ensuring that records and documents accurately reflect completed work;
- maintaining documents and records including transmittal, distribution, retention, access, preservation, traceability, retrieval, removal of obsolete documentation.

4 nSHIELD scope and objective

This chapter defines challenges with respect to the scope of the nSHIELD project. We understand that the scope of a research project is to establish state-of-the-art developments, to support new technologies, and to document the achievements.

The nSHIELD project is the opening investigation towards the realization of the SHIELD Architectural Framework for Security, Privacy and Dependability (SPD).

As defined in the Technical Annex and illustrated in the following figure, the nSHIELD project is focused on the seven principal aspects related to SPD.

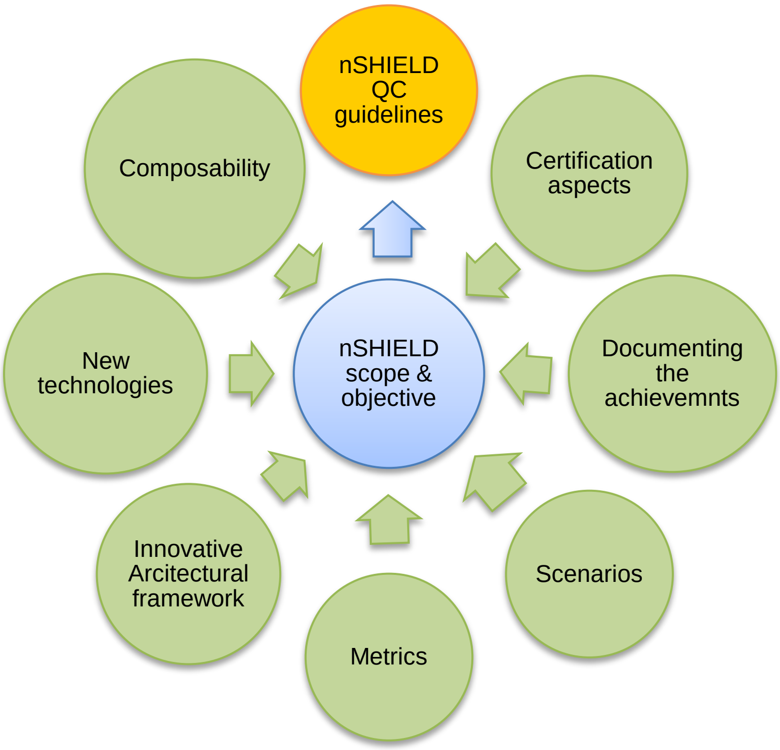


Figure 10 Categories contributing to SHIELD scope and objectives

4.1 Composability

According to the TA, the leading concept of nSHIELD is to demonstrate composability of SPD technologies. It means the ability to derive instantiations of architecture from a generic platform that support the constructive composition of large systems, out of components and sub-systems, without uncontrolled emergent behaviour or side effects.

Composability of SPD functionalities at different layers among different technologies will be refined and developed, taking into account performances and dynamic composability of any kind of technologies, present in the project.

nSHIELD will approach SPD at 4 different levels: node, network, middleware and overlay. For each level, the state of the art in SPD of individual technologies and solutions should be improved and integrated.

4.2 New technologies

A wide set of technologies will be used to realize SPD functionalities; design guidelines will be provided to make any “nSHIELD compliant technology” composable with the others. The SPD technologies will be, then, enhanced with the “composability” functionality that is being studied and designed in nSHIELD, in order to fit in the SHIELD architectural framework.

nSHIELD will select the most appropriate SPD algorithms, technologies and procedures, will improve them and develop the missing ones, and will integrate and harmonize them in a modular, composable, expandable and high-dependable architectural framework.

4.3 Innovative architectural framework

The nSHIELD approach is based on modularity and expandability, and can be adopted to bring built-in SPD solutions in all the strategic sector of ARTEMIS, such as transportation, communication, urban environment. To achieve these challenging goals the project aims at creating an innovative, modular, composable, expandable and high-dependable architectural framework and common SPD metrics capable of measuring the overall SPD level in any specific application domain, with minimum engineering effort.

nSHIELD will refine and develop the framework in complex scenarios.

4.4 Metrics

A complete exhaustive set of metrics for SPD description will be refined and consolidated in the nSHIELD project and used to validate the whole functionalities of the framework.

In the framework of nSHIELD, the developed SPD-based solutions will be proved in a set of ambitious application scenarios, aiming at verifying the achieved SPD performance, measured in terms of properly defined SPD metrics.

In this respect, a first fundamental step will be the definition of SPD metrics and their ontological description. Homogeneous metrics will make easier the monitoring of the current SPD levels of the various layers and of the overall system, as well as the assessment of the various SPD levels.

4.5 Scenarios

The SHIELD General Framework consists of four layered system architecture and Application Layer in which three complex scenarios are considered:

1. Railway,
2. Voice/Facial Recognition,
3. Dependable Avionic Systems

The project will validate the nSHIELD architectural framework by means of three (complex) scenarios relevant in an industrial perspective and one feasibility study concerning Social Mobility and Networking.

The proposed ambitious application scenarios correspond to future product and services markets that are expected to exhibit fast growth rates due to socio-economic trends.

4.6 Documenting the achievements

The scope of the project includes the documentation of achievements through targeted dissemination, scientific dissemination, internal dissemination, and deliverables.

In section 3.2, it has been identified the value of internal trainings, in order to bring participants on to the same level of understanding. Such internal dissemination should include hands on experience in order to achieve a better learning. However, trainings are not the only way of internal dissemination. They should go ahead with living documentation, which is nowadays often achieved through a Wiki-based collaboration platform, as for the pilot project.

Last but not least, the project should create deliverables. A good way of documenting the achievements is through collaborative platforms and prototypes. A collaborative platform will allow acting as a living document, where ideas and discussions can be contributed at any time. However the challenge of a collaborative platform is often that the content turns into an unstructured cloud of information. Thus the challenge is to generate the structure in a collaborative platform.

Prototypical developments might be in the form of software or instant form of hardware. These developments should be taken up to the point where they can prove certain theory, rather than trying to develop market solutions, out of nSHIELD scope.

4.7 Certification aspects

The nSHIELD project aims at addressing SPD in the context of ESs as “built in” functionalities, proposing and perceiving with this strategy the first step towards SPD certification for future ESs.

The integrated use of SPD metrics in the framework will have impact on the development cycles of SPD in ESs because the qualification, (re-)certification and (re-)validation process of a SHIELD framework instance will be faster, easier and widely accepted.

The definition of semantic enabled SPD metrics and the development of proper tools for the management of SPD lifecycle, pertain to the ESs’ development cycles improvement and will ease the qualification and certification of the generated system. SPD metrics in particular are considered the indispensable basement for building standardized methods and industry-wide accepted parameters for certificability in Security, Privacy and Dependability fields.

5 Risk and contingency

A precondition to risk assessment is establishment of objectives that shall be identified in the TA and in the Quality Control document. Risk assessment is the identification and analysis of relevant risks to achieve the stated objectives, and forms the basis for determining how the Consortium will manage the risks.

Different types of risks and crisis have to be contemplated. The general rule is that the Project Manager/Coordinator will be in charge of early crisis detection, in order to search for the first informal solution; when not possible, the problem will be submitted to the Task Force (Steering Committee) debating in an urgency mode.

Figure 11: nSHIELD Risks assessment

Several of these potential risks can be assessed concerning their probability and level of (negative) impact. Risks with a high probability and a severe impact are handled with particular caution during the project. The following measures are foreseen to cope with those risks:

- Potential Risks will be identified and analysed in detail.
- For the ones with medium to high probability and severe impact, countermeasures and contingency plans are discussed, and they will be flagged throughout the execution of the project as “risk items”. This ensures that all levels of the project take special care of those items.
- For the ones with low probability or low impact, and for the ones that cannot be foreseen at this stage, the Technical Management Committee will ensure that such risks are identified in an early phase, and that necessary countermeasures are taken.

General causes of crises envisaged are in particular:

- Research and technological risks as failure in the execution of a critical task;
- Economic and exploitation risks as default of confidence between partners. In case the defaulting partner is the Coordinator, then a specific procedure is foreseen in the Consortium document for replacing it;
- Organization risks as IPR or confidentiality issue not well addressed;
- Investment related risks (e.g. financial crisis of any partner or increases of costs);
- Methodological risks as failure of one or more partners in delivering their output and deliverables in due time or within an agreed delay.

5.1 Research and technological risks

Due to the high number of SPD technologies that will be developed and integrated in the nSHIELD system, for the sake of simplicity, instead of listing all the risks associated to each technology, two macro-risks have been identified, see applicable document [01].

Risk 1. A technology development at node, network or middleware layer delays

Probability: [Medium]. nSHIELD aims to enhance more than 30 SPD technologies at all levels of an ES. It is possible that one or more of challenging technologies can require more effort to be enhanced to match the specifications. However as shown in section 5.3 for each technology at least two partners are involved in its development and approx. the 2/3 of the consortium is always involved in R&D activities. So, in the case one of the technologies is delaying, the other partners can provide technical assistance or some more effort.

Gravity: [Medium/High]. The delay of one or more technologies can cause a delay in the delivery of a prototype and thus the entire project can be delayed.

Contingency plan*:* If a critical delay occurs in one or more of the SPD technologies, two main countermeasures can be taken. First of all the technology can be used at the state of the art, without enhancement, and adapted to be composable with the rest of the architecture. Secondly, taking advantage from the composability feature of the nSHIELD system, it can be replaced by other available SPD solutions (even if with less performance).

Risk 2. The composability concept fails

Probability: [Low/Medium]. The leading nSHIELD concept is to demonstrate the composability of heterogeneous SPD technologies. It can occur the case that this innovative concept once deployed produced less benefit than the effort it requires to operate, even if the current research literature seems to demonstrate the contrary[1]. Moreover the nSHIELD work plan has been organized to check continuously (through integration, validation and verification processes) the achievements of the project milestones and results.

Gravity: [Medium]. If the static and dynamic composability concept fails, the added value brought by the project is limited to the evolution of the single SPD technologies in ESs and to the simplification of (re-) certification processes.

Contingency plan: To mitigate the effects of this risk, as soon as one of the checks fails (during the integration, the validation or the verification processes) less strict requirements and specifications and a more efficient system design can be studied, in order to improve the nSHIELD performances with the minimum effort.

5.2 Standardization and exploitation risks

Risk 3. Products appear on the market before the project work is completed

Probability: [Low]. The key players in this market are embedded system manufacturers, integrators and their suppliers, of which several major ones are in the consortium. Whilst partners are aware of on-going work on small-scale single-technology, proprietary solutions, they are aware that especially from 2001 the SPD topics have become a worldwide priority. However, they have no knowledge of a similar activity to nSHIELD that takes such holistic approach to SPD, where a composable convergent over-layer can guarantee efficiency, reliability, adaptability, resiliency over different networked ES technologies.

[1] "*A top-down, multi-abstraction layer approach for embedded security design reduces the risk of security flaws, letting designers maximize security while limiting area, energy, and computation costs.*". Source: D. D. Hwang, P. Schaumont, K. Tiri and I. Verbauwhede, "Securing Embedded Systems", published by the IEEE computer society, IEEE security & privacy, 2006.

Gravity: [Medium/High]. If a product will appear on the market before the project work is completed then this would be a serious situation that might have impact on the project.

Contingency plan: If a seemingly competing product came to the market during the project's lifetime, it would have to be examined carefully. It is highly unlikely that all the types of technological advances proposed by nSHIELD with respect to the standard integrated SPD solution would be covered, or that all the features and functions of nSHIELD could be included in any product that could emerge within the next couple of years. Rather than closing the project, a realistic contingency plan would be to work together with the manufacturer to enhance their product with nSHIELD aspects that they do not have.

Risk 4. Standards emerge that prevent the deployment of the results, or lead towards a different solution to that being developed in the project

Probability: [Low]. Some key players in standardization groups are present in the nSHIELD consortium. They are expected to be aware of the work in relevant standards organizations.

Gravity: [High]. If standards did emerge that prevented the deployment of the results, or led towards a different solution to that being developed in the project then this would be a serious situation that might impact heavily on the project.

Contingency plan: If a standard emerged to handle ES SPD in all layers in a different manner, it might still be feasible to adapt the nSHIELD infrastructure to the new standard. The nSHIELD components are very modular and composable, and the necessary adaptations may be largely a case of modifying the external interfaces.

5.3 Organizational risks

Risk 5. Withdrawal of a key partner

Probability: [High]. In a project with more than 20 partners lasting 3 years, the chances are high that at least one partner will have to leave the project due to an event such as major internal re-organization or takeover. Alternatively, a partner may find itself unable to complete its allocated responsibilities, due to the transfer of key personnel within, or outside, the company, financial problems, etc. In both cases it will be necessary to find a replacement partner.

Key partners are considered those with management roles (Coordinator, WP leaders), and those that provide node or network technologies not provided by other partners.

Gravity: [Medium]. Thanks to the good balance of the composition of the project consortium, a complete collapse of the project is highly unlikely, even if a key partner withdraws. Monitoring procedures will be put in place to detect early any under-achieving partner and the project will encourage open and honest reporting of problems, so that solutions can be found as soon as possible.

Contingency plan: The consortium comprises major companies, who have expertise in several areas relevant to nSHIELD, and a transfer of resources to an existing partner, of the same country, would be the first choice for a replacement. Given the overwhelming interest expressed to be part of this consortium, if no replacement could be found internally, it is expected to be simple to find an external replacement organization to take over the work at relatively short notice.

Risk 6. Since WP6 builds on all other work packages, the main risk identified is the delaying of components delivery.

Probability: [Medium]. Because of the number and variety of components to be integrated onto the platform, there is a chance of not being able to produce working demonstrations of all expected features coping with the challenging scenarios addressed in WP7. nSHIELD has continuous verification mechanism that helps to identify potential delays and to react in time.

Gravity: [Medium].

Contingency plan: Measures can be taken to minimize the risks if there's some foreseen delay; for example some components can be replaced with older versions or components already developed in other projects, so that a single delay should not compromise the final demonstration.

5.4 Methodological risks

These risks are related primarily to the need to merge research results from different organizations, with a potentially large degree of difference in methods, terminology, and outputs.

Risk 7. The consortium fails to deliver proper models and tools

Probability: [Medium]. The complexity and innovation of nSHIELD conceptual framework and related tools can lead to unforeseen design deadlocks.

Gravity: [Medium]. This methodological risk causes problems to system development.

Contingency plan: Contingency plans of the consortium foresee that, in such a case, the parameterization and configuration of the field test will be solely based on the extensive experience of the project partners in development of SPD systems and technologies. Drawbacks of this measure are that the evaluation of progress beyond the state-of-the-art cannot be executed at the quality intended and in a reproducible manner.

Risk 8. The consortium fails to deliver prototypes according to the specifications and requirements

Probability: [Medium]. To enable composability of SPD functionalities, nSHIELD requirements and specifications should be applied strictly. It is possible that one or more prototypes fail to respect the specifications.

Gravity: [Medium]. This methodological risk causes problems to the platform integration and the field tests.

Contingency plan: In this situation, a minimal combination of industrial partner existing products would provide a substitution for the prototype. Yet the results of such a substitution would not be able to provide all the functionalities of the project prototype. Therefore, the gravity of this risk is rated medium.

5.5 Investment related risks

Risk 9. Low or negative investment return

Probability: [Medium]. This is a sensitive issue for all participants since all investments need to be related to a return plan. Participants believe that potential benefits identified during the project definition phase are sufficient to guarantee valuable returns. However, the outcome of the project may be subject to re-definitions or deviations thus altering the initial expectations of the respective partners with respect to resources necessary to accomplish a certain task and wide-scale applicability of results.

Gravity: [High].

Contingency plan: To enhance the possibility that investments bring a positive outcome to the project, acceptance preparation activities will be conducted starting from the beginning of the project.

6 Quality Assurance

The focus of Quality Assurance is on the processes used in the project. Quality Assurance ensures that project processes are used effectively to produce quality project deliverables. It involves following and meeting standards, continuously improving project work, and correcting project defects.

Good practice for QA procedures requires an objective review to assess the quality of the project, and also to identify areas where improvements could be made.

The project may be reviewed as a whole or in parts. The objective in QA implementation is to involve reviewers that can conduct an unbiased review of the project.

It is good practice to use QA reviewers that have not been involved in same project. Preferably these reviewers would be independent experts from other agencies or a national or international expert or group not closely connected with project activities. Where third party reviewers outside the project are not available, staff not directly involved in the activities being reviewed can also fulfil QA roles.

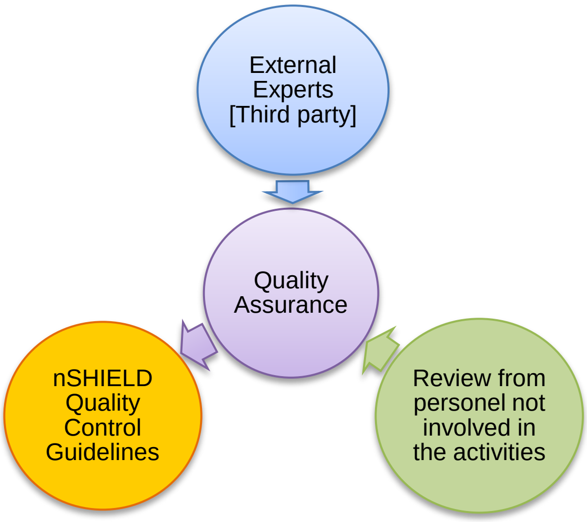


Figure 12: Quality Assurance

7 Action Plan

The goal of this section is to establish an action plan and identify which actions have to be taken in order to have a successful quality management in the project. The previous sections have identified all the input to take into account in the nSHIELD project, identifying several implementation phases, project scope and objectives, and performing the risk analysis.

Generally speaking, the action plan summarizes the quality control guidelines, the priorities evidenced by partners and by stakeholders and the background as showed in the following figure.

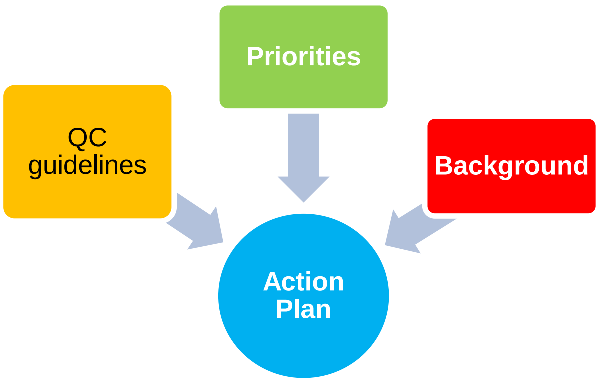


Figure 13: Action Plan input

The action plan describes what the project involves in terms of resources, time, money and technologies in order to execute activities as meeting, workshops, sharing of information, developing of common technical solution where partners, stakeholders, decision makers and external resources are involved. The action plan impact can be summarized in three steps:

- Short term - learning about problems and misunderstanding
- Medium term – action and decision for the selection of the suitable solution
- Long term impact – solution and methodologies for collaborative research.

nSHIELD action plan will guide the project to be developed according to the following criteria:

- Contribution to the project objectives;
- Correspondence of solutions with ARTEMIS expectations;
- Accuracy and meaningfulness of the outputs;
- Respect of time and cost constraints planned for the project.

A preliminary analysis of nSHIELD indicates that the overall progress is good, and that only a limited number of areas require further attention in the quality management. In particular this aspect is related to the areas of information, structure, procedures, and tools. This need is due to the structure of the consortium that is composed by more than 20 partners from 6 different European countries.

The Quality Control reports, D1.6 and D1.9, will provide additional information on how the project is performed.

8 nSHIELD Quality Management System

A quality management system (QMS) can be expressed as the organizational structure, procedures, processes and resources needed to implement quality management [R1].

Quality management is performed throughout the project lifecycle with special attention to:

- Quality Planning – primarily during the project planning process (Chap. 6)
- Quality Assurance (QA) – primarily during the project execution process (Chap.7).
- Quality Control (QC) – primarily during the project monitoring and controlling process (Chap.3).

The goals for quality management of R&D projects are to assure:

- Project deliverables meet their stated requirements.
- Project management processes are appropriately followed.

8.1 Deliverables requirements

Each deliverable responsible, supported by the Project Coordinator, establishes and defines the needed controls in order to:

- ensure that documents of external origin and Classified documents (i.e.: confidential, etc.) are identified, filed, reproduced and their distribution is controlled;
- approve documents for adequacy prior to issue;
- review, update (as necessary) and re-approve documents;
- ensure that changes and the current revision status of documents are identified;
- ensure that relevant versions of applicable documents are available at points of use;
- ensure that documents remain legible and readily identifiable;
- prevent the unintended use of obsolete documents and identify them if they should be used for any purpose.

A template with a logo dedicated to the nSHIELD project is available as common structure for all the deliverables, in the wiki [http://nshield.unik.no/wiki/Deliverables]

8.2 Project Management roles & processes

The successful management of the project and consortium will be also based on the experience, capability and motivation of the Project Coordinator (Coordinator) as well as of the Technical Manager. Project Coordinator and Technical Manager are indicated as Project Management.

The Project Coordinator, the Technical Manager and the WPs responsible must ensure that the nSHIELD requirements are defined and met, with the aim of achieving the objectives of the project through the guidelines of these Quality Control Guidelines.

The Project Management commitments must be summarized as in the following:

- establishing the quality and environmental policy;
- ensuring that the quality objectives have been established;
- conducting reviews;
- ensuring the availability of resources.

Additionally, the Project Management has to:

- identify the processes needed for the Quality Management System and their application throughout the project;
- determine the sequence and interaction of these processes;
- determine criteria and methods needed to ensure that both the operation and control of these processes are effective;
- ensure the availability of resources and information necessary to support the operation and monitoring of these processes;
- establish methods to monitor, measure and analyse these processes;
- implement actions necessary to achieve planned results and continuous improvement of these processes.

8.2.1 Roles in nSHIELD

The Project Coordinator is MOVATION (NO) and the Technical Manager is SES (IT). The Project Management is leaded by SES.

8.2.1.1 WP Responsibility

The project is structured in eight work packages (WP). WPs responsible are listed in the following table.

Table 8-1: nSHIELD WPs Responsibility

WP	Title	Partner Responsibility
1	Project Management	SES (*Cecilia Coveri*)
2	SPD Metrics Requirements and system design	TECNALIA (*Inaki Eguia*)
3	SPD Node	ISD (*George Dramitinos*)
4	SPD Network	SES (*Marco Cesena*)
5	SPD Middleware and Overlay	SES (*Andrea Morgagni*)
6	Platform integration, validation and demonstration	HAI (*Nikolaos Pappas*)
7	SPD Application	MAS (*Josef Noll*)
8	Knowledge exchange and industrial validation	MGEP (*Roberto Uribeetxeberria*)

8.2.1.2 Technical Task Force

A Technical Task Force which works as horizontal coordination body for all work packages has been instituted. The partners involved on the Technical Task Force will meet typically every two weeks, or when necessary, depending on the amount of work. Each meeting can be held by call conferences, Webex or Skype, depending on the suitable media selected by the partners day by day.

The members of the Technical Task Force are listed in the following table.

Table 8-2: nSHIELD Technical Task Force members

Partners	Participant
SES	Elisabetta Campaiola, Marco Cesena, Cecilia Coveri, Andrea Morgagni, Massimo Traversone
MAS	Josef Noll
SEARCH-LAB	Balazs Berkes, Ezster Kerezsi
ISD	George Dramitinos
UNIROMA1	Andrea Fiaschetti
TECNALIA	Inaki Eguia
UNIGE	Lucio Marcenaro, Kresimir Dabcevic
HAI	Nikolaos Pappas
MGEP	Roberto Uribeetxeberria

8.2.1.3 Technical Management Committee

Additionally, the Design Authority is represented by a group of partner representatives of the major industries and of research institutes that are part of the Technical Management Committee (TMC).

In particular, the TMC is in charge of the approval of all kind of amendments required by the Consortium to the Technical Annex.

The members of the TMC are listed in the following table.

Table 8-3: nSHIELD TMC members

Partners	Participant
SES	Elisabetta Campaiola, Cecilia Coveri, Andrea Morgagni, Marco Cesena
ASTS	Francesco Flammini
HAI	Nikolaos Pappas
ETH	Paolo Azzoni
TECNALIA	Inaki Eguia
ISD	George Dramitinos
MAS	Josef Noll
UNIROMA1	Andrea Fiaschetti

8.2.1.4 Demonstrators Scenarios responsibility

The responsible for the coordination of the scenarios demonstrator is MOVATION (Josef Noll)

The responsible for each scenario are listed in the following table.

Table 8-4: nSHIELD Scenario responsibility

Scenario	Partners
T7.1 Railways Security	ASTS (Francesco Flammini)
T7.2 Voice/Facial Recognition	ETH (Paolo Azzoni)
T7.3 Dependable Avionic System	SES (Massimo Traversone)
T7.4 Social Mobility Networking	MAS (Josef Noll)

The Technical Annex document identifies detailed responsibilities and authorities for each task, activity and deliverable.

8.2.2 Plan-Do-Check-Act

The downstream focus of the R&D activities is the "life motif" guiding the management in every aspect concerning the nSHIELD project. The Quality Management System of nSHIELD is based on the PDCA; Plan – Do – Check – Act/Adjust, addressing the applicable parts of this methodology to the R&D project.

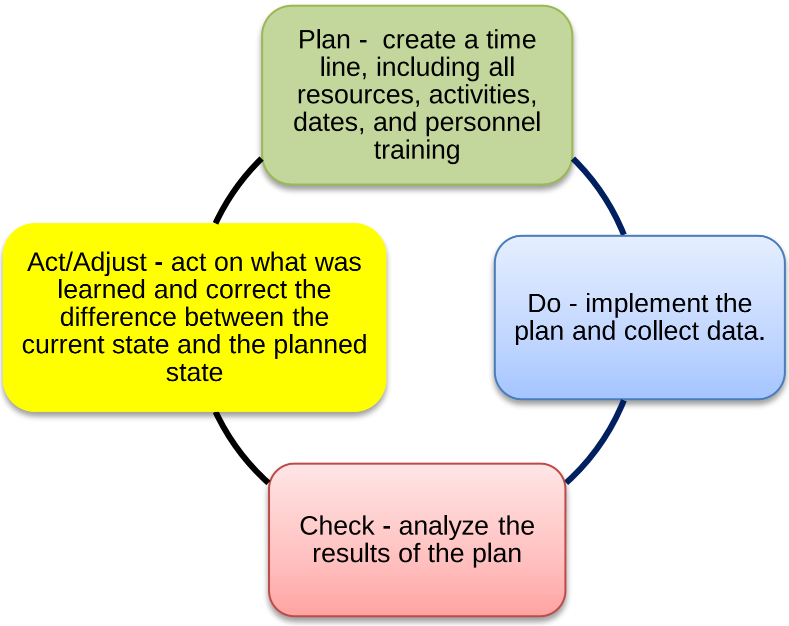


Figure 14: Quality Management System steps

8.2.2.1 Plan

The Project Management and the WP leaders establish quality objectives, including those needed to meet requirements for nSHIELD objective, at all relevant functions and levels within the consortium. The quality objectives are measurable and consistent with the quality policy.

8.2.2.2 Do - Project Implementation and data collection

The Project Management and the WP leaders have to define the resource requirements to implement and maintain the Quality of the project and continually improve the Quality Plan effectiveness.

The personnel, involved in the nSHIELD activities, performing work affecting quality of the nSHIELD project, will be competent based upon appropriate education, training, skills and experience.

The following processes:

- Design and Development
- Testing and Validation
- Technical-Qualitative metrics.

are agreed and monitored by the Project Management, the WPs leaders and the Technical Task Force.

Common technical features, strictly connected to the scenarios, can be discussed at Demonstrators scenario responsibility board, first.

When planned results are not achieved, appropriate actions are taken to correct the non-conforming process implementation. The TMC must be aware of the changes, because some of them could be required to be evaluated and then approved by the TMC.

8.2.2.3 Check

The Project Management and the WP leaders perform a review of the entire quality system annually, as a minimum, to ensure its continuous suitability, adequacy and effectiveness.

Review Input

As a minimum, the input to the management review meeting includes information on:

- results of internal technical semi-annual meeting
- ARTEMIS-JU feedback;
- monitoring and measurement results of the processes;
- status of preventive and corrective actions;
- follow-up actions from previous management reviews;
- changes that could affect the quality management system;
- recommendations for improvement to the quality management system.

Review Output

The output of the review meeting includes, as a minimum, any decisions and actions related to:

- improvement of the effectiveness of the quality management system;
- the quality policy observance;
- improvement of the effectiveness and the efficiency of the processes;
- improvement of achieving objectives;
- human, infrastructure and environmental resource needs;
- quality and environmental targets assigned to each partner.

Preventive Actions

Project Management conducts review meetings to determine actions needed to eliminate the causes of potential non conformities in order to prevent their occurrence.

Data analysis

The Project Management and the WP leaders determine, collect and analyse appropriate data to demonstrate the suitability and effectiveness of the quality management system and to evaluate where continual improvement of the effectiveness of the quality management system can be made.

Concerning a R&D project, the analysis of data provides information relevant to conformity and trend of nSHIELD processes and solution. Each WP leader analyses own data and, if necessary, promotes (defines) the actions to improve own processes and solution.

The results from the above analysis will be reviewed during the Management Review meetings

8.2.2.4 Act/Adjust

Every time “non-conformities” occur on documentation and deliverables (SW/HW solution for nSHIELD objective), they will be investigated for:

- determining the causes of non-conformities;
- evaluating the need for action to ensure that non conformities do not occur;
- determining and implementing action needed;
- recording of the results of action taken;
- reviewing corrective action taken;
- taking specific actions where timely and/or effective corrective actions are not achieved.

The TMC is required to approve changes or adjustments, when necessary.

9 Conclusions

For defining quality control guidelines it is important to:

- Clearly outline the scope of the project, including detailed sub-goals for work packages, tasks and deliverables
- Identify risks in the project and establish a contingency plan
- Identify potential hurdle of a collaborative project
- Document and archive all QC activities
- Establish an action plan
- Apply the nSHIELD Quality Management System

The following picture summarizes the QC guidelines described in the document.

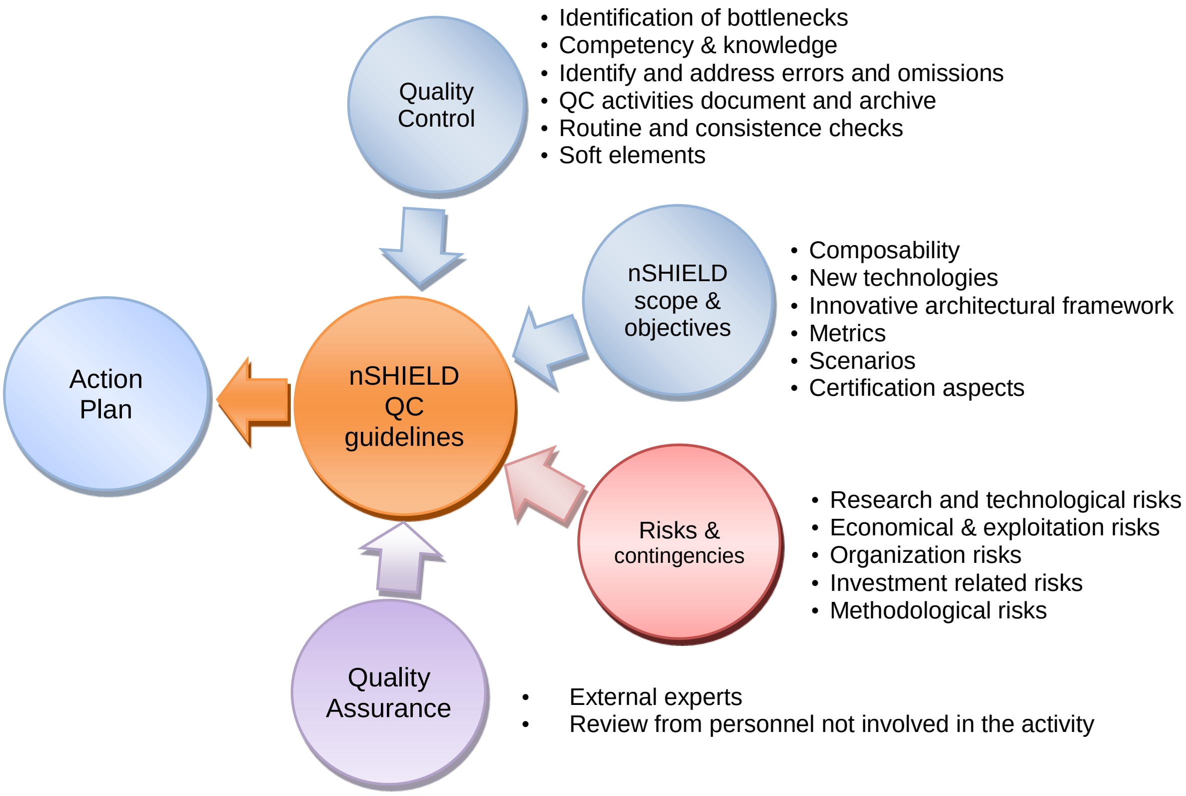


Figure 15: nSHIELD QC Guidelines summary

This document has performed a detailed analysis of nSHIELD project quality management. In the following the measures for potential hurdles has been provided in a tabular form.

Table 9-1: List of potential bottlenecks in nSHIELD

Topic	Action	Relevance (+,0,-)	Achieved (Yes, no, partly)
3.1a Language and topic language	Support audio conferences with written agenda and minutes available as soon as possible after the meeting	+	Yes
3.1b Exchange of information	Give space to physical meetings such that partners can meet, exchange information and familiarize, thus enhancing the understanding of other culture	0	Partly
3.1c Audio conferences	Audio conference length no more than 60 minutes	0	Yes
3.1d Unclear descriptions	Establish measurable outcomes	+	Partly
3.1e High level scopes not broken down	Establish sub-goal for each task, when possible	+	Partly
3.1f Technical Annex	Definition on how the TA should be used according to JU	0	No
3.1g Deliverables	Use of deliverables as mean of documentation of work, but choice of on-line collaboration tools for information exchange	-	Yes
3.1h Tools	Use of common collaboration tools to share the result of the discussions	0	Partly
3.2a Level of knowledge	Improvement of internal knowledge exchange by means of training session	+	Partly
3.2b Expert in this field	Subgroups of experts (in certain fields) definition	0	Yes
3.2c Comparison to state of technology	Definition of the state of technology to be reached: e.g. algorithm development, prototype development	+	Partly
3.3a Type of leadership	A collaborative leadership structure built on the expertise of experts in each domain	+	Partly
3.3b Culture	Open meeting allowing cultural exchange and common understanding	+	Partly
3.3c Personality	Leadership shared among participants	0	Partly
3.4a Errors and Omissions finding	Identifying and mitigating E&O as early as possible, including immediate engagement of partners in addressing the problem	+	No
3.4b Errors and Omission mitigation	Properly evaluating the nature and impacts of E&O	+	No

Risk Management is taken care of, risks are identified, and the contingency plan is established, accordingly with what was already outlined in the Technical Annex.

As it is still relevant to answer the questions of the risk assessment, it has been repeated and summarized here:

- Have research and technological risks been properly identified?
- Have economic and exploitation risks been properly identified?
- Have organizational risks been properly identified?
- Have methodological risks been properly identified?
- Have Investment related risks been properly identified?

The project management approach proposed for nSHIELD provides mechanisms to identify and resolve potential risks. The tight control both at the WP and project management level ensures that risks are identified.

The Project manager (PM) will ensure that risks management is an essential part of the regular project management phone conferences.

When it comes to the action plan, we have addressed the areas of information, structure, procedures, and tools as being the most relevant ones for nSHIELD. Our major concern was how to achieve living information, which was (partly) achieved through the use of a collaboration platform based on a Semantic MediaWiki.

10 References

[R1] Wikipedia Quality Management - http://en.Wikipedia.org/Wiki/Quality_management

[R2] Data Validation - http://en.Wikipedia.org/Wiki/Data_validation