BS EN 9320:2014

BSI Standards Publication

Aerospace series — Programme Management — General guidelines for acquisition and supply of open systems

National foreword

This British Standard is the UK implementation of EN 9320:2014.

The UK participation in its preparation was entrusted to Technical Committee ACE/1, International and European Aerospace Policy and Processes.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 83573 5

ICS 35.080; 49.020

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2014.

Amendments issued since publication

Date	Text affected

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 9320

December 2014

ICS 35.080; 49.020

English Version

Aerospace series - Programme Management - General guidelines for acquisition and supply of open systems

Série aérospatiale - Management de Programme - Recommandations générales pour l'acquisition et la fourniture de systèmes ouverts

Luft- und Raumfahrt - Programm-Management - Allgemeiner Leitfaden für Erwerb und Lieferung von offenen Systemen

This European Standard was approved by CEN on 28 June 2014.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 9320:2014 E

Contents

Page

Foreword

This document (EN 9320:2014) has been prepared by the Aerospace and Defence Industries Association of Europe - Standardization (ASD-STAN).

After enquiries and votes carried out in accordance with the rules of this Association, this Standard has received the approval of the National Associations and the Official Services of the member countries of ASD, prior to its presentation to CEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by June 2015, and conflicting national standards shall be withdrawn at the latest by June 2015.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

1 Scope

These general guidelines cover the open system acquisition and supply processes.

There is an increasing requirement for systems designed and produced by industry, particularly in the aeronautic, space and defence fields, to be used with other systems designed, produced, acquired and operated independently.

The concept of open systems is touched upon in many systems engineering documents. This document deals specifically with this subject. To this end, through the various processes applied, it provides information to stakeholders (buyers, suppliers, designers, subcontractors, supervisors, etc.) on the best practice to be adopted.

The specific nature of openness for a system is defined by all the following properties:

- Interchangeability,
- Interoperability,
- Upgradability,
- Reusability,
- Reversibility,
- Flexibility,
- Affordability.

These properties are defined in the glossary for these general guidelines.

These general guidelines are largely based on the structure and system life cycle processes described in standard ISO/IEC 15288:2008.

The characteristics of openness also relate to:

- The products or services offered by the company (target systems resulting from use of company processes).
- The company's processes (project systems). Several stakeholders, with their own assignments, cultures, jobs and geographical locations, different working methods, modelling frameworks, standards, tools and aids, etc. are involved in the activities, which are sometimes multidisciplinary, of the internal and external processes of a company. These diverse elements are not necessarily all suited to working together without causing certain risks, a loss of autonomy, effectiveness and/or efficiency, etc. A company must, for example, develop its ability and capacity in terms of interoperability both internally (between the systems of which it is made) and externally (with other partners), including, by way of an example:
  - Ability of each stakeholder and each department involved to maintain efficient and trusting relationships with other stakeholders, taking into account deadline, cost and quality objectives,
  - Ability to exchange, communicate and use the necessary flows (data, information, knowledge, materials, energy) autonomously, without error and dynamically throughout the life cycle of the target system,
  - Ability to coordinate, synchronise and manage common tasks and share and use resources (human, machine or application) and services efficiently and appropriately.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 9001:2008, *Quality management systems — Requirements*

ISO 9241-210:2010, *Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems*

ISO 10007:2003*, Quality management systems — Guidelines for configuration management*

ISO 10303-1:1994, *Industrial automation systems and integration — Product data representation and exchange — Part 1: Overview and fundamental principles*

ISO/IEC 15288:2008, *Systems and software engineering — System life cycle processes*

ISO/IEC 9126-1:2001, *Software engineering — Product quality — Part 1: Quality model*

IEEE 830:1998, *IEEE Recommended Practice for Software Requirements Specifications*

IEEE 1471:2000, *IEEE Recommended Practice for Architectural Description for Software — Intensive Systems*

3 Terms and definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1
affordability
ability of a system to have acceptable operational performance for an acceptable cost of ownership, resulting from a compromise after negotiation between the Parties

[SOURCE: IEEE 1471:2000]

3.1.2
architecture
fundamental organisation of a system described by its components, the relationship between these components and with the environment, and the principles guiding its representation and its development. The relationships between the components are described in the interfaces

3.1.3
capacity
capacity is represented by the consistent integration of a Policy, an Organisation, human resources, training, Support and Equipment

3.1.4
component
product that cannot be broken down from the point of view of a specific application

[SOURCE: ISO 10303-1:1994]

3.1.5
flexibility
ability of a system to continue to fulfil its mission by dynamically or statically adapting to anticipated or foreseeable changes that may occur in its environment

3.1.6
interchangeability
ability of a hardware or software component to be replaced, with no change to the components connected to it, by another that meets the same requirements

3.1.7
interface
an interface is the part of a system or piece of equipment that communicates with another system or piece of equipment

3.1.8
interoperability
interoperability can be defined as the ability of systems to exchange, with no loss or ambiguity, various object flows (data, information, knowledge, materials, energy, etc.), then to be capable of using these objects independently to fulfil their own assignments or to fulfil a shared assignment for a given purpose with no change to their structure, behaviour or operation

3.1.9
key interface
the interface of a module that needs to be interoperable, easy to change, replaced or isolated due to its complexity, obsolescence or the costs involved

3.1.10
operational assignment
operational assignments are the parts of department activities that may be repetitive, planned and of limited duration

3.1.11
product life cycle
this covers all the situations the product goes through during its life from statement of requirement to withdrawal from whatever service is provided

[SOURCE: NF X 50-100:1996]

3.1.12
reusability
for a hardware or software component, ability to be used, unchanged, in a system or subsystem other than the one for which it was originally developed

For a system or subsystem, ability to use, unchanged, hardware or software components which were not originally developed for it

3.1.13
reversibility
ability of a system, subsystem or component to be modified and updated by a manufacturer other than the one that produced it

3.1.14
open system
assembly including software and hardware elements and operating procedures, designed by humans. These elements interact to satisfy the requirements (including interface requirements) defined, published and maintained by general consensus by a group

Modular construction created so that its modules are defined precisely and have public interfaces allowing independent suppliers to provide new capacities and innovative modules

[Modular Open System Architecture]

3.1.15
openness
the characteristic of openness for a system is defined by all the following properties:

- Interchangeability,
- Interoperability,
- Upgradability,
- Reusability,
- Reversibility,
- Flexibility,
- Affordability.

3.1.16
system of systems (SoS)
the characteristics of a system of systems are:

- Operational independence of the systems,
- Managerial independence of the systems,
- Emergence of new services,
- Upgradable configurations,
- Geographic distribution of the systems,

3.1.17
technical facts
key technical event, anticipated or unexpected, in the life cycle of a product

3.1.18
upgradability
potential ability of a system, subsystem or component to respond to changes in operational requirements and anticipated or foreseeable technical changes without affecting the basis of its structure

3.1.19
validation
comparative assessment to confirm that the requirements of stakeholders are properly satisfied. If discrepancies are found, they are recorded and lead to corrective action. Validation is ratified by the stakeholders

[SOURCE: ISO/IEC 15288:2008]

3.1.20
verification
demonstration, through assessment of the product, that the system has been designed correctly, i.e. that it complies with the specifications according to which the product was made

[SOURCE: ISO/IEC 15288:2008]

3.2 List of abbreviations

NCOIC	Network Centric Operations Industry Consortium
OTS	Off-The-Shelf
IADT	Inspection Analysis Demonstration Test
OS	Open System
MMI	Man Machine Interface
SoS	System of Systems
SMART	Specific, Measurable, Achievable, Realistic and Time-constrained.
STEP	Standard for the Exchange of Product model data
TRL	Technology Readiness Level
IRL	Integration Readiness Level
SCOPE	Systems Capabilities, Operations, Programmes and Enterprises
UML	Unified Modelling Language
SysML	System Modelling Language

4 Acquisition process

The organisations are producers and consumers of systems, which may make products or perform services. These systems are produced by some or implemented or consumed by others within the context of the relationship between buyers (those who purchase and consume or use) and suppliers (those who produce and sell). Buyer/supplier relations are maintained through contracts. Acquisition of an open system requires specific activities to be carried out to optimise signature of contracts to obtain a product/service that satisfies the openness requirements.

The purpose of the process described in this chapter is to characterise these activities. The level of detail of each activity depends on the complexity of the system to be acquired.

4.1 An acquisition strategy is established

4.1.1 Define an openness strategy

Define the openness level required depending on, for example, the maturity scale defined using the SCOPE model developed by the NCOIC. To establish this openness level, it is important to:

- Be aware of the operational environment into which the system to be acquired will be integrated, exhaustively and explicitly identify the systems of the operational environment with which the system to be acquired should interoperate, characterise the flows between these systems.
- List the rules and standards applied by the technical systems of this operational environment.
- Define the openness objectives.
- Rate these openness objectives for the system to be acquired in accordance with the environment.

4.1.2 Define an acquisition strategy

The way in which the system is acquired (related to the quantity and/or the complexity of the system in question) can have a direct effect on the system openness. A short-term acquisition for a system with a short life cycle may be unique. On the other hand, acquisition in stages or long-term acquisition for a system with a long life cycle entails requirements in terms of openness, including upgradability, and can cause openness problems linked to changes in the environment in which it is integrated, for example unplanned changes to the other systems in its environment. It is therefore necessary to establish an acquisition strategy depending on the system life cycle model and the changes anticipated in the system environment (regular upgrades, midlife upgrades, etc.).

It is necessary to:

- Define the life cycle model.
- The more important the openness characteristics, for example interoperability, the more complex the system's life cycle will be.
- Describe the acquisition increments leading to the solution.
- The acquisition increments must be organised depending on the openness requirements identified (for example planning the main changes anticipated taking into account the maturity of the technology implemented – TRL).

Contractual requirements specific to reversibility will be defined when the acquisition strategy is defined.

4.2 A supplier is selected and the selection justified

4.2.1 Define selection criteria

To facilitate the production of an open system, the prime contractor (supplier) should have experience in the design of open systems. The selection criteria proposed may be:

- the maturity of the supplier (according to SCOPE).
- a scale based on the supplier's experience:
- 0: no open system design listed,
  - 1: design of open systems in a different field,
  - 2: design of open systems in the field,
  - 3: recognised as an open system manufacturer (several references in several fields).
- The quality of presentation of the response to the call for tenders (structured presentation promoting a systems engineering strategy, etc.)
- The open systems of the suppliers are certified (for example by the NCOIC).

4.2.2 Justify the choice of supplier

Each supplier is assessed/graded in accordance with predefined criteria. Within the context of an open system, as well as the cost/performance aspects, the supplier's experience must also be taken into consideration.

4.3 Communication with the supplier is maintained

Continuously discuss the open system requirements and its interfaces (external and internal).

The needs of the Client in terms of the requirements for the system openness aspects that the Industrial Contractor must satisfy and apply during production and industrialisation of the system should therefore be stipulated in detail in the contract. This may relate to current and future operational changes to be taken into account, predicted technical developments and changes to OTS components.

4.4 A contract is drawn up

4.4.1 State the acceptance criteria for openness

The open system level, in terms of interoperability, upgradability, interchangeability, reusability, flexibility, reversibility and affordability, must be clearly defined in the form of requirements and acceptance criteria must be formulated for each of these requirements. The contract must refer to these requirements associated with openness, in line with the predefined acquisition strategy. A requirement must be Measurable, Useful, Simple and Traceable (MUST). To define these requirements, a detailed description of the system's operational environment will be used (current operational environment and probable future operational environment). To encourage interoperability, the system's interfaces with its environment must be precisely characterised from an operational and functional point of view. If rules, standards or OTS components need to be used, they need to be characterised:

- Either define a catalogue of rules, standards and OTS components to be used and keep it up-to-date,
- Or draw up the requirements relating to the use of rules, standards and OTS components with an associated priority: critical, essential, important, useful, optional, etc. (see essential, important, desirable or IEEE 830:1998 essential, conditional and optional).

4.4.2 Stipulate the legal conditions

From an architectural point of view, the openness is characterised by the use of product rules and standards and OTS components. To ensure that the openness requirements expressed by the Client comply with Industrial Contractor and third party intellectual property rights, a strategy on the choice of these rules, standards and OTS components must be defined in close collaboration with legal experts: rules, public or proprietary standards, free of charge or chargeable, etc.

For a SoS, every effort will be made to ensure a certain level of consistency between the various contracts. This means that the systems to be integrated into the SoS must comply with the interoperability rules and that the partners (Client and Prime Contractor) of the different SoS must exchange both technical and non-technical information (coordination between programmes, agreement between partners) and follow standardised systems engineering processes and activities when they are called upon to collaborate.

Of the various openness characteristics, reversibility is not a technical characteristic but a contractual and legal aspect. The guidelines present reversibility within the framework of French law. They will need to be adapted for other jurisdictions.

The contractual clauses relating to reversibility will be negotiated. Reversibility may be dealt with in a conditional part of contracts.

Particular attention will be paid to determining the elements of contracts specific to reversibility:

- a duration,
- advance notification of enforcement of the reversibility clause,
- a **reversibility plan** set up as soon as service provision commences and which must be updated regularly (similar to the service continuity plan in the banking field),

- the transfer of **intellectual property rights** (patents, drawings, models, etc.), copyright for software,
- the scope of the actions in relation to reversibility,
- gradual stoppage of services,
- maintenance or gradual reduction of performance commitments,
- transfer of information and data on maintenance history (reliability, failure rate),
- transfer of spare parts management: parts inventory, list of orders in progress, stock rotation management rules,
- expertise (know-how, etc.).
- skills transfer,
- transmission of written procedures, condition of installations,
- Staff re-employment,
- Training.
- Reversibility acceptance phase,
- Contractual guarantees,
- Payment of price.

4.4.3 Define the means for checking openness characteristics

The requirements of the openness tests to be performed must be laid down in a contract and their results produced in the presence of both parties. The following methods can be used:

- The development of scenarios by simulation and/or experimentation,
- The assessment methods based on inspection, analysis, demonstrations and tests (IADT),
- Operational acceptance tests and verification of service rendered.

These methods are cross-functional and apply to models, prototypes, demonstration models, first-offs and so on. Resources, such as test benches, simulation environments and scenarios, must be specified.

4.5 A product or service conforming to the contract terms is accepted

If the openness characteristics have been demonstrated and validated (performance of the activities defined in 4.4.3) and the product/service delivered satisfies all the requirements laid down in the contract, it can be contractually accepted.

The penalties associated with the non-conformity of an openness characteristic are dealt with in the same way as the other penalties. Depending on the ranking of the openness objectives laid down by the buyer, the penalties will be defined in the contract.

It is worth noting that defining guarantee criteria for system openness is not necessarily easy as the openness characteristics of a product/service depend on the products/services with which it interacts. Thus, the interoperability of a system is closely linked to the technological stability of the operational environment. Alternatively, it needs to be looked at in terms of risk. The instability of the environment will be managed by change requests and addenda to the original contract.

4.6 The contract is closed

Ownership of the system is transferred when the contract is closed. In the end, the reversibility clause may be invoked, as long as it has been clearly defined in the contract and is not unfair.

5 Supply process

The organisations are producers and consumers of systems, which may make products or perform services. Within this context, the supply process from the supplier side mirrors the acquisition process from the buyer side.

The purpose of the process described in this chapter is to characterise these activities. The level of detail of each activity depends on the complexity of the system to be supplied.

5.1 A buyer or a market for a product/service is identified and a proposal made

More and more systems must have good openness properties in order to be marketable. It is therefore important to have good knowledge of the environment of the product/service when conducting market research: operational environment, industry practice, standards. It is then possible to work out a project strategy which will provide answers to the following questions: What is the target market (mass production or confidential), what is the market segment (quasi-monopoly or highly competitive), what do customers and prospects want in terms of openness, what is the capacity for interoperability with existing and planned systems and what is the system's life cycle (upgradability)?

The architectural choices for meeting the openness requirements must be financially assessed (definition of the openness quality/cost ratio) which must take into account customer requirements, market volume, competitor position, market trends and so on.

5.2 A contract is drawn up and communication maintained

Within the context of an open system, the Prime Contractor defines in a contract the means in place to guarantee the openness characteristics required by the Client (rules/standards employed, tests performed, details of the results). It also establishes the performance schedule consistent with the life cycle model established by the Client.

The supplier must ensure the feasibility of the required openness level. Should a requirement associated with the openness poses a risk (irrelevant requirement given the technical or operational environment, difficult and/or onerous design, etc.), the Prime Contractor must offer to conduct an openness requirements review for the Client.

5.3 A product or service conforming to the contract terms is provided

The supplier should provide all relevant information in the documentation so as to enable the scope of the system openness supplied to be defined. The quantity and level of detail may vary depending on the complexity of the system but the supplier should provide the client with at least the following information:

- a list of the external interfaces and their characteristics (functional and technical),
- a list of OTS components (such as consumables or components with life cycles shorter than the cycle of the system acquired) and the method for procuring them,
- a list of standards (de jure/de facto) used,
- compliance with the standards and any deviations must be traced.

To check the reversibility and/or upgradability characteristics of the system, the supplier may also be required to characterise the internal system interfaces.

5.4 Ownership is transferred to the client

Depending on the terms of the contract, the supplier shall indicate, as a minimum, the components for which a licence is required (usage/operation/modification rights, etc.). Within this context, it is possible to implement the reversibility clauses, upon request from the client.

5.5 The contract is closed

The supplier will establish a period during which it guarantees the openness capacities of its system or any limitations.

6 Life cycle model management process

6.1 The strategy and the processes required for managing the life cycle model are defined

To implement the requirements of this standard, the life cycle policies of the systems, the systems engineering processes and the associated procedures, which must comply with the strategic and business plans of the organisation, need to be defined within the organisation.

The actual extent and details of integration of a life cycle into a project will depend on the requirements in terms of openness of the target system, the complexity of the work, the methods for demonstrating satisfaction of the requirements used and the core skills and training of the staff involved in carrying out the work. Therefore, if an upgradability requirement is expressed, this requirement needs to be translated in terms of life cycle, taking into account the main changes anticipated in each life cycle phase and the implications for the technical and project processes. A project adapts the policies and procedures to its requirements and needs. The appropriate procedures and policies include risk management, quality management and personnel management.

The system openness characteristics for the life cycle relate to all life cycle phases. However, their impact is mainly seen during the operation and maintenance phases. A method for gathering operator feedback needs to be created and made available, particularly for the flexibility, upgradability, interoperability and interchangeability characteristics.

This has repercussions on both architecture and processes. Indeed, procedures for gathering information from operators need to be put in place for project ownership and/or project management.

The interoperability characteristics may have consequences for the life cycle. This will be all the more complex (V, W, spiral cycle, etc.) if the system in question needs to be interoperable with many different systems that change through their own life cycles.

The life cycle model must be defined depending on the organisation’s openness strategy and the operational constraints of the future system.

7 Infrastructure management process

The aim of this infrastructure management process is to provide systems and services for the project to uphold the objectives of the programme throughout the life cycle of the system.

Here, the guidelines apply in particular to the project systems where several stakeholders (client and contractors) are involved. Indeed, they must implement standardised processes and activities and exchange information (which is also standardised), and hence the tools must be collaborative and interoperable.

8 Budget management process

8.1 The opportunities, investments or requirements of the investment plan are defined, prioritised and selected

New growth markets, projects or other commitments need to be identified, prioritised, selected and traced in accordance with the business strategy and the organisation's action plans. Project performance thresholds then need to be defined.

The strategy for openness systems created by the Company must be compatible with the financial requirements (affordability).

Anything to do with reversibility must be budgeted for from the pre-contract stages of the project. This budget must include the cost of drawing up and maintaining the reversibility plan and the financing thereof.

8.2 Resources and budgets are identified and allocated for each project

All multi-project interfaces that have to be managed or maintained by the project need to be identified. This includes the "project systems" and the components of systems common to several projects.

For an open system, a risk budget needs to be allocated to cover the impact of risks associated with demonstration of the system openness to be designed, for example delayed provision of the other system or systems with which the open system must interoperate for the integration and/or verification phases.

Resources and a budget also need to be allocated to contribute to standardisation activities in the organisations affected by the system (e.g. ETSI).

For a system contributing to a SoS, and for the SoS itself, the updates and anticipated changes required for the target system to protect its ability to interoperate with the other SoS systems need to be provided for. The accounts to which these updates and changes are to be allocated should be determined as soon as possible.

9 Resource management process

9.1 The core skills required by the projects are identified

Identify the core skills requirements based on current and planned projects. These are technical, financial and legal skills (e.g. reversibility).

For open systems, it is recommended to appoint managers for each of the openness characteristics to be dealt with, for example the manager of interfaces within the context of interoperability, and to establish the scope of their responsibility. Their assignments are, not exclusively, as follows:

- to ensure that the requirements relating to these openness characteristics are correctly formulated and validated by the stakeholders who expressed them,
- to ensure that information is correctly circulated between the various lots or with the systems identified as stakeholders,
- to ensure that the functional and physical architecture solutions satisfy the requirements relating to these openness characteristics,
- to ensure that the system openness characteristics match their definition.

9.2 The necessary human resources are provided for the projects

- Predict and anticipate core skills gaps by recruiting or training qualified personnel.

- Predict project task allocations for training the team for project requirements.

For a system contributing to a SoS, and for the SoS itself, human and organisational resources need to be provided for updating and making the anticipated changes required for the target system to protect its ability to interoperate with the other SoS systems.

9.3 Staff core skills are developed, maintained or enhanced

Identify and record staff core skills.

Draw up the core skills development plan.

- This plan includes the types and levels of training, personnel categories, schedules, personnel requirements and training needs.

Obtain or develop training, resource training.

- These resources include the teaching aids developed by the organisation or by external parties, the training sessions, computer instruction, etc.

Plan skills development.

For an open system, it may be necessary to train the interface manager in the challenges of the openness and to make sure that he is competent in management and implementation of the standards in the field. It is also desirable to raise awareness amongst the other parties involved with definition of the system on the concepts of integration, interfaces, standards, etc.

To sustain the “open system” vision within an organisation, it may be helpful to promote the skills in the interfaces field.

9.4 Conflicts in multi-project resource demands are resolved

Coordinate multi-project management interfaces to resolve foreseeable conflicts:

- with ability (aptitude) in terms of resources and organisation infrastructure to support current projects,

- with overload of work for the project teams.

9.5 Individual knowledge, information and core skills are pooled, shared, reused and improved throughout the organisation

Keep the skills development plan up-to-date.

Establish and maintain the infrastructure for sharing general and field-specific information within the organisation.

Select an appropriate knowledge management strategy.

Enter and make information accessible to the organisation in line with its strategy.

In the absence of an “interfaces” stream, it may be helpful to create a “community of interest” within the organisation to improve the methods and processes associated with the definition, characterisation and design of interfaces, etc.

10 Quality management process

The aim of this process is to provide products and services that meet the quality objectives set by the organisation and satisfy customer requirements.

Not specific to openness.

11 Project planning process

This process determines the scope of project and technical activity management, identifies the output of processes, the tasks and project deliverables, draws up project task coordination schedules, including the performance criteria and the resources necessary for accomplishing these tasks and steers performance of the project plan.

11.1 The project plan is available

Project definition:

1 Identify project objectives and constraints.

- Objectives and constraints include performance and all other aspects relating to quality, cost, lead time and the satisfaction of the stakeholders. Each objective is identified in sufficient detail to be able to adjust and integrate appropriate selection of processes and activities.

- The openness characteristics must be identified as project objectives.

With regard to open systems, constraints associated with the provision of third party systems for the design, integration, verification and validation of the system to be designed (interoperability) need to be taken into account.

2 Define the scope of the project in accordance with the terms of contract.

- The project includes all the appropriate activities required to satisfy economic decision-making criteria and to make the project a success. A project may be responsible for one or more phases in the life cycle of the whole installation. The schedule shows all the appropriate actions for maintaining the project plan and assessing and coordinating the project.

For the open systems, the project interfaces consistent with the technical interfaces need to be defined.

For a system contributing to a SoS, and for the SoS itself, the respective scopes and responsibilities of the project teams, according to the scopes of the SoS systems, need to be defined.

3 Define and maintain a life cycle model made up of phases, based on the life cycle model defined within the organisation.

4 Establish a tasks tree based on the upgradable architecture of the system.

- Each aspect of the system architecture, each process and each appropriate action is described with a level of detail suitable for the project and the risks identified.

5 Define and maintain a programme schedule based on the objectives of the project and the work assessments.

- This includes definition of the length, the connections, the dependencies within the project and also with third party projects and the sequencing of project activities, the accomplishment milestones, the resources allocated and the reviews necessary for adequate completion of the project.

6 Define the project accomplishment criteria for the life cycle phase decision grids, the delivery dates and the major dependencies on external input or output.

- The frequency of internal project reviews is defined in line with the organisation policy based on criteria such as the criticality of contracts and product criticality, schedule and technical risks.

7 Formulate and communicate a plan for technical management of the project, including reviews.

8 Draw up a Project Quality Plan.

- This includes the definition and documentation of the project's quality objectives to guarantee the company's quality objectives as well as the company's quality management objectives, policies and procedures (in accordance with ISO 9001:2008 or other).

9 Identify the project costs and plan a budget.

- Costs are identified, in particular, using the programme schedule, work assessments, infrastructure costs, refuelling items, estimation of service purchases and project systems, as well as budget reserves for risk management [particularly project risks associated with third party systems (see budget process)].

10 Draw up a reversibility plan and an associated budget.

11.2 Stakeholders, responsibilities and authorities are identified

1 Establish the structure of authorities and project work responsibilities.

- This requires project organisation, human resources, development of staff core skills and team operation methods to be defined. They include the efficient use of human resources divided amongst the functions of the organisation to contribute to all phases in the system's life cycle. The structure of authority is defined, i.e. the individual responsibilities and legal authorities as appropriate, for example the design authority, security authority, certification or accreditation levels.

2 Define the infrastructure and the services required by the project.

- This requires the abilities required, their availability and their allocation to project tasks to be defined. The installations, tools and technical communication and information means are also included. Requirements associated with the "project systems" required in each life cycle phase within the scope of the project are also indicated.

For open systems, project interface managers need to be identified (communication with third party systems).

3 Plan the acquisition of outsourced equipment, goods and services.

- This includes, as required, subcontracting forecasts, supplier selection, acceptance, contract administration and contract closure. Contract processes are used for projected purchases.

Not specific to openness.

11.3 The resources and services required for project completion are formally requested

1 Submit the requests to obtain the resources necessary for project completion.

12 Project control and assessment process

This process assesses, periodically and for major events, progress and accomplishment compared to requirements, project plans and all contract objectives. If significant discrepancies are found, the information provided relating to these discrepancies results in managerial actions being taken (e.g. an exemption request). This process also involves redefining the activities and tasks of the project, if necessary, in order to rectify any discrepancies and deviations due to project management or technical processes. This may lead to the schedule being revised.

Not specific to openness.

13 Decision-making process

This process is in response to a decision needing to be made during the system's life cycle, regardless of its nature or source, in order to achieve indicated, desirable or optimised results. Alternative actions are analysed and a course of action is chosen and directed. The decisions and their justifications are recorded to support future decision-making.

This process is comparable with the risk and opportunity management process.

Not specific to openness.

14 Risk management process

The risk management process is an ongoing process to systematically tackle risk throughout the life cycle of a system, a software product or a service. It may be applied to risks associated with procurement, development, maintenance and implementation of a system and with its withdrawal from service.

Each aspect of openness is prone to risk and opportunity.

For example, only having one supplier for an OTS component is a risk if component interchangeability is required. Similarly, the absence of a publicly recognised and adopted standard is a risk where a system has to interoperate with various different systems within a SoS, insofar as it would be necessary to develop specific interfaces for each of the different systems. However, implementing a formalised iterative and incremental strategy within a contractual framework is an opportunity when, later on, upgradability proves necessary. Care should be taken with compatibility between the standards of various interfacing systems.

The reader should refer to RG.Aéro 000 39B for more details on management of programme risks (only available in French, currently).

14.1 The scope of risk management is determined

By definition, an open system is directly affected by the slightest change in its environment (interoperability). Risk analysis for an open system must be extremely thorough:

1 Define the risk management policies.

2 Document the risk management process to be applied.

3 Identify the parties responsible, their roles and the scope of their responsibilities.

4 Provide the responsible parties with the appropriate resources for risk management.

5 Define the process for evaluation and improvement of the risk management process (measurement of process maturity) and review it regularly to assess its effectiveness and results.

6 Define and document the context of the risk management process.

This includes a description of the prospects of the stakeholders, the risk categories and a description (perhaps by reference) of the objectives, hypotheses and technical and managerial constraints.

7 Take feedback from similar programmes into account, see Table 1.

The main types of risks/opportunities to be taken into account for openness are:

Table 1 — Types of risks/opportunities

Field		Type of Risk (R) / Opportunity (O)
Environment	R	Unexpected changes to the operational, technical, administrative, legal and/or political environment.
	R	Unavailability of interoperating third party systems.
	O	Emergence of opportunities in the operational, technical, administrative, legal and/or political environment.
Normative	R	Inadequacy of the standards adopted.
	R	Insufficient maturity of prospective or adopted standards.
	O	Opportunities of change to emerging, then recognised, standards.
	O	Sustainability of the standards of the field chosen for the target system.
OTS component/technology	R	Uncertain future of the OTS component supplier.
	R	Unwanted change in the OTS component.
	R	Uncertain sustainability of the component.
	R	Insufficient robustness of the OTS component under system use conditions.
	R	Technological emergence.
	R	Technology readiness and in-house expertise in this technology (TRL, IRL).
	O	Changes to the OTS component encouraging of the system openness.
	O	Plurality and diversity of the range of OTS components; ability to diversify supply.
Organisational	R	Failure to manage critical skills.
	R	No economic and technical monitoring of suppliers, technology, etc.
	O	Training and circulation of best practice.
	O	Call for standardised processes dealing with the problems involved with openness.
Functional	R	Over or under-specification of the openness requirement.
	R	Allocation of functions to various components.
	R	Level of interface control too macroscopic.
	R	Level of interface control too microscopic.
	O	Reuse of components.
	O	Loose coupling of the functional architecture.
Financial	R	Over-specification of the openness requirement beyond the values covered by the supply.
	R	Openness testability cost.
	O	Emergence of a less expensive OTS that meets the openness requirement.
	O	Sustainability of provisions allocated to the openness characteristics.

14.2 Appropriate risk and opportunity management strategies are defined and implemented

1 Define and document the thresholds and the risk conditions under which a level of risk may be accepted; for example, only having one supplier when component interchangeability is required.

2 Define and document the conditions under which opportunities are exploited.

3 Define the process for evaluating and improving the risk and opportunity management process.

- This includes processing of information gained through feedback and experience.
- Gather risk and opportunity proposals from all stakeholders.

14.3 Risks and opportunities are identified as soon as they emerge, managed until a conclusion is reached and funded

1 Establish and maintain a portfolio of risks and opportunities, see Table 2.

The risks and opportunities portfolio includes:

- the context for risk and opportunity management;
- a record of the status of each risk and/or opportunity including its probability, its impact and the thresholds of each risk or opportunity;
- the priority of each risk and opportunity based on criteria provided by the stakeholders;
- the action requests with their status.

The portfolio of risks and/or opportunities is updated when the status of a risk or opportunity changes.

Each risk/opportunity identified must have its own sheet so it can be monitored throughout the life cycle of the system.

Table 2 — Management of risks/opportunities

Information	Description of the information required
Identifier	Each risk/opportunity must have a unique identifier so unambiguous reference can be made to it in other documents.
Creation date	The date the risk or opportunity is created.
Description	Description of the risk or opportunity.
Initial clearance date	The projected date for the risk to be cleared or the opportunity taken.
Final clearance date	The actual date the risk is cleared or the opportunity taken.
Type	The type of risk or opportunity.
Criticality / Probability	− risk criticality = Severity × probability − opportunity benefit = Positive impact × probability
Development	How the risk or opportunity develops (increase, steady, decrease).
Description of the impact	− Description of the consequences if the risk is realised. − Description of the impact of the opportunity if it is taken: benefits and secondary effects.
Cost of the impact	− Cost of the consequences if the risk is realised. − Financial assessment of the benefits.
Action(s) for reduction / support	Description of actions likely to: − reduce the probability or the cost of the risk. − encourage the opportunity to be taken.
Action(s)	− Description of emergency actions. (Risks only). − Description of opportunity-taking actions. (Opportunities only).
Budget / Funding	Describe the budgets corresponding to the action plans.

Continuously monitor the system throughout its life cycle to detect any new risks and/or opportunities and their origin.

14.4 Risks and opportunities are analysed and their priority (for allocation of resources) is determined

1 Identify the risks and opportunities in the categories described within the context of risk and opportunity management.

2 Estimate the probability of each risk and opportunity identified emerging and the consequences thereof.

3 Regularly send the relevant extract of the risks and opportunities portfolio to the stakeholders as required.

4 Continuously monitor all risks and opportunities and changes in context and reassess them when their status has changed.

14.5 Risk management/opportunity exploitation measures are defined, implemented and evaluated to determine changes in the risk/opportunity status and the progress of activities to deal with them

1 Once a decision has been made on how to handle a risk/opportunity, carry out implementation actions according to the project control activities in 5.4.3.3 and 6.4.2.3 of ISO/IEC 15288:2008.

2 Apply and monitor handling of the risk/opportunity to evaluate its effectiveness.

3 Throughout the life cycle, gather together information on the risk/opportunity to improve the risk/opportunity management process and generate feedback.

- The information on risk and opportunity sheets includes the risks or opportunities identified, their origins, handling thereof and the success of the handling methods selected.
- Keep the history of risk and opportunity sheets that have been closed.
- To successfully manage risks and opportunities, it is recommended to keep the history of risk and opportunity sheets that have been closed, as risks and opportunities can sometimes re-emerge following an unexpected event. In addition, this history is valuable for other similar projects. It is often very useful to take feedback from other projects into account.

4 Monitor closure of risk/opportunity sheets.

14.6 The appropriate action is taken to integrate the opportunity into the project

Opportunity management goes hand in hand with risk management.

The aim of opportunity handling however, unlike risk handling, is to maximise the level of opportunity for the programme by seeking to increase the likelihood of occurrence of the opportunity and/or its impact (see RG.Aéro 000 39B).

15 Configuration management process

The purpose of the configuration management process is to establish and maintain the integrity of all identified outcomes of a project or to handle them and make them available to interested parties.

15.1 A configuration management strategy is defined

15.2 Define a configuration management strategy

This includes:

- the definition of authorities for registration, access, publication and control of changes to configuration items;
- the definition of storage locations and conditions, their environment and, in the case of information, the storage media in accordance with the designated levels of integrity, safety and security;
- the definition of the criteria or events to initiate configuration management and maintain the guidelines for configuration changes;
- the definition of the audit strategy and the responsibilities for ensuring continuous and secure integrity of configuration definition information.

  Configuration management activities should be compatible with the guidance provided by ISO 10007:2003. The types of configuration items include, amongst other things, the frames of reference (needs, requirements, models of different levels, including study models, test protocols, etc.), the target system, the enabling systems (including those that enable to target system qualification).

On the subject of openness, Configuration Management must relate to the following items in particular:

1 external interfaces,

2 internal interfaces,

3 technical and functional characteristics of component openness,

4 characteristic of a language, of a code and of a process.

Thorough configuration management is essential for establishing and protecting the openness properties over time.

The configuration management strategy must also keep up-to-date the frame of reference of interface standards (and rules) used within the context of system design.

During regular reviews, the impact of changes to standards on openness is to be defined.

15.3 The items requiring configuration management are defined

Identify the items that are subject to configuration management.

- The items are differentiated using unique, lasting identification or marking. The marks comply with the appropriate standards and the conventions of the product field, so that the items covered by configuration management are clearly linked to their specifications or an equivalent, documented description.

15.4 Configuration references are established

1 Ensure that the configuration information enables upward and downward traceability for other configuration statuses.

2 Keep the information on the configurations with an appropriate level of integrity and security.

  - The nature of the items covered by configuration management needs to be taken into account. The description of configurations conforms, as far as possible, to the product or technology standards. Record each configuration change, the rational for it and the associated authorisations in a configuration reference database.

3 Consolidate the configuration status of the items for which the configuration changes to form a documented and time-marked or detailed reference. Record the rational for the changes and the associated authorisations in a configuration reference database. This reference must enable the interoperability level to be reassessed.

15.5 The configuration of configuration items is managed

1 As soon as an impact on interoperability with third party systems is identified, a way of notifying stakeholders needs to be provided.

2 Ensure that changes to configuration references are correctly identified, recorded, assessed, recognised, integrated and verified.

3 Carry out audits to check compliance of the product with the specifications, plans, interface management documents and other contractual requirements.

15.6 The status of configuration items is available throughout the life cycle

1 Keep configuration records during the system life cycle and archive them according to agreements, relevant legislation or best industry practice.

2 Manage recording, recovery and consolidation of the current configuration status and the status of all previous configurations to confirm the accuracy, opportunity, integrity and security of the information.

The availability of configuration information is essential for reversibility.

16 Information management process

This process generates, gathers, transforms, maintains, recovers, circulates and deletes information. It manages information, including technical, project, organisational, contractual or user information.

16.1 The information to be managed is identified

1 Define the information to be monitored during the system life cycle and afterwards, in accordance with organisation policy or legislation in force.

2 Assign the authorities and the responsibilities for initiation, design, reproduction, distribution, archiving and destruction of information.

3 Define the rights, duties and clauses relating to transmission of and access to information.

- Pay attention to legislation on information and data, associated with security and privacy, and image reproduction rights, contractual restrictions, access rights, intellectual property and patents. Where there are restrictions or constraints, information is identified as a result. Staff with knowledge of such information is notified of its commitments and responsibilities, including legal ones.

For a system for which interoperability is required, or for a system contributing to a SoS and for a SoS itself, technical and non-technical project information needs to be sent to the projects managing the third party systems with which interoperability is required. This is all the more necessary as there are no rules or standards in the protocols, in exchange semantics, in configuration management and in man machine interfaces, which is a significant risk factor.

It is particularly important to notify project teams designing third party systems of any changes to the system during its life cycle in order to maintain the required level of interoperability.

16.2 Information formalism is defined

1 Define the semantics, the formats and the means for representing, storing, sending and extracting information.

- Information may come in and may be sent in any form and may be stored, processed, reproduced and sent using any means.
- Pay attention to organisational constraints, for example the infrastructure, inter-organisation communication methods and the distribution of roles and responsibilities for the project. Information, including rules, is stored, transformed and circulated and the appropriate presentation conventions are used in accordance with policy, agreements and legislative constraints.

With regard to the system's interoperability criterion, the formalism must be chosen in accordance with the formalism used by the project teams designing the other systems.

This results in the use of a standardised, widely adopted formalism, such as UML, SysML or STEP (ISO 10303-1:1994).

With regard to the system's upgradability criterion, the formalism must be chosen to support this system upgradability. This may relate to the semantics of the formalism which must be extendable while maintaining semantic consistency with what was created before (upward and downward compatibility). This may also relate to the formalism's ability to be transformed and used where another, more encompassing one is needed.

With regard to interchangeability, the selected formalism must enable the maintenance engineer and the user to compare the system in question with the systems with which it can be interchanged. This requires a unique description of the functionalities, the interfaces and the metrics associated with them.

With regard to reversibility (a non-technical criterion), this criterion may affect formalism selection, with this formalism needing to be publicly known and information provided.

Finally, with regard to reusability, the selected formalism must be usable (accessible, legible, comprehensible) by project teams who need to reuse the system in question. A publicly recognised formalism for which information is provided must be implemented.

16.3 Information is modified to suit requirements

1 Obtain the information identified.

- This may include producing information or gathering it from the appropriate sources.

In this case, the changes made must be systematically documented and communicated to the stakeholders, particularly the project teams for other systems or teams that have to reuse the system in question.

16.4 Information is kept available

1 Define the measures for keeping the information.

- This includes status reviews of the integrity, validity and availability of the information stored and any requirements for reproduction or transformation to another format. In light of technological changes, either the infrastructure for reading the information needs to be maintained or the information should be transcribed into a format for the new technology (electronic format, operating system, application).

16.5 Information is up-to-date, complete and valid

1 Keep and store information records in accordance with integrity, security and confidentiality requirements.

- Record the status of information items, for example the version description, distribution record, degree of classification. The information should be legible and stored and maintained in such a way that it is easily accessible and that damage, deterioration and loss are prevented.

2 Store the designated information for audit and feedback requirements.

- Select the format, the locations and the means for protecting the information in accordance with the storage and recovery frequencies and the organisation's policy, contracts and legislation.

3 Delete unwanted, invalid or non-verifiable information in accordance with the organisation's policy and confidentiality requirements (security and personal protection).

Information management, maintenance and storage actions must take into account the openness criteria. Therefore, before deleting any information, you should check that no other project team needs it.

16.6 Information is made available to the designated parties

1 Retrieve and circulate information to designated parties in accordance with the requirements of agreed schedules or defined circumstances.

- The information is provided to the designated parties in a suitable format.

2 Provide the regulatory documentation to the stakeholders involved.

- Regulatory documentation includes, for example, certification and accreditation documentation, pilot's licences and assessment rates.

Updated information must be circulated to the stakeholders as required, particularly the project teams designing the systems with which the system in question must interoperate.

16.7 Information is made available to the designated parties whenever changes are made

1 The information in question relates, in particular, to interface standard modifications.

Information must be circulated to the stakeholders involved whenever changes are made.

17 Measuring process

The aim of the measuring process is to gather, compile, analyse and reproduce measurement data relating to the products developed and the processes implemented in the organisations (client or contractors). This is done to maintain efficient management of the processes and to objectively demonstrate product quality.

17.1 Information requirements for the technical and management processes are identified

Not specific to openness.

17.2 An appropriate set of assessment measurements, based on information requirements, is identified and/or developed.

1 Define the collection of data, analysis and the notification procedures.

2 Define the criteria for evaluating information products and the measurement process.

3 Identify, approve and supply the resources required for measurement processing.

4 Acquire and deploy support tools.

5 Integrate data production, collection, analysis and notification procedures into the appropriate processes.

The metrics, (project and technical) specific to the system's openness characteristics, need to be integrated. Try to take into account the quality attributes applicable to open systems (ISO/IEC 9126-1:2001, *Software engineering — Product quality — Part 1: Quality model*).

17.3 Assessment activities are identified and planned

There are several architecture assessment methods. As an example, these guidelines suggest the ATAM method ("ATAM ^{SM} Method for Architecture Evaluation"). See the document in the Appendices presenting ATAM ^{SM} implementation for the problem of the openness and interoperability of systems.

This may be component replacement scenarios.

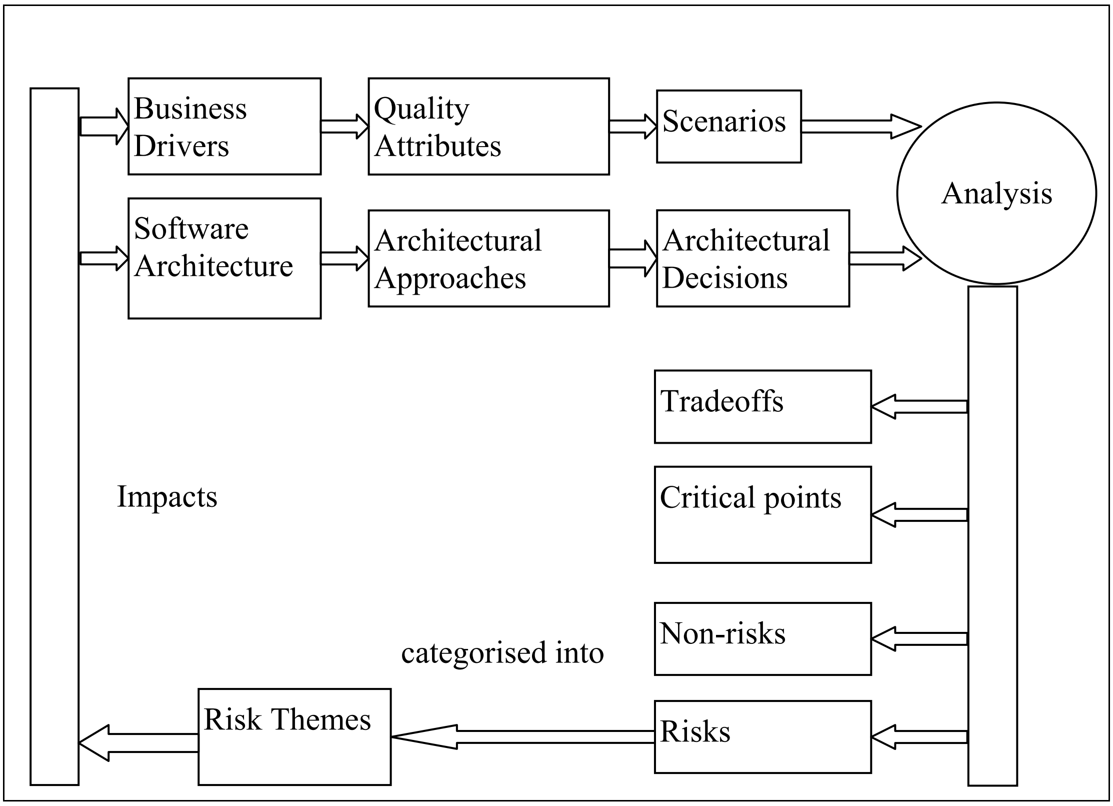

Figure 1 — ATAM© Block Diagram (Source SEI)

The architecture evaluation process is an iterative process. Using, on the one hand, business objectives, hence the requirement and, on the other hand, the system architecture, hence the solution, the dimensioning attributes of the quality model (interchangeability, interoperability, upgradability, etc.) and the attributes directing the architectural approach, the scenarios and the architectural decisions are obtained respectively.

These are the input for the analysis, the results of which are a list of risks, a list of non-risks, the tradeoffs and the sensitivity points, enabling these requirements to be met.

The risks are categorised. Their impacts on business drivers and on the system architecture are evaluated.

17.4 The required data is compiled, stored, analysed and the results interpreted

1 Compile, store and check the data.

2 Analyse the data and develop information products.

17.5 Information products are used to uphold decisions and provide an objective basis for communication

Document and communicate the results to measurement users.

17.6 The measuring process and the measurements are evaluated

Evaluate the information products and the measuring process.

17.7 Improvements are communicated to measuring process managers

Identify potential improvements.

17.8 Appendix: ATAM ("Method for Architecture Evaluation")

The evaluation approach

To analyse an architecture, the suggested methodology examines the architectural approaches used. The architectural approaches are the major decisions taken with regard to the architecture for the interfaces, the measurements taken to deal with system growth, the responses to changes, the integration with other systems, the main architectural patterns, the use of OTS, etc.

1 Identify and prioritise the quality attributes to evaluate (including those associated with the openness). They must draw attention to the aspects of the architecture that are most critical for the success of the system. Reiterate the critical requirements and the associated measurements and the standards, models, etc. to satisfy them.

2 Select scenarios showing the quality attributes to evaluate. Divided into three main categories: usage scenario (typical usage - nominal, degraded - of the existing system), growth scenario (modifications, changes, performance or reliability improvement, etc.) and exploratory scenario (extreme cases, or limit, of growth such as gaining an order of magnitude of performance), they may be based on operational scenarios created in the "Identify the operational requirement" activity and on the outcome of the "Define the critical requirements for openness" activity. Scenario structure must be built on the stimulus - environment - response principles. The scenarios must show the degree of architecture openness. For example, the scenarios associated with flexibility must show that the system architecture supports the addition or withdrawal of hardware or software components without there being any major impact on the architectural approaches. The priority and the risk or difficulty of each scenario must be identified.

3 Present the system from the point of view of business challenges and the main objectives, its main functions, the main abstractions from the system, their dependencies, the flows and the technical constraints (operating system, the hardware and middleware required for use thereof, the OTS components that have to be used, the hardware and software platforms required, the reuse of codes, existing applications or existing hardware, the other systems with which the system interacts or communicates or which it uses, together with the approaches, the architectural styles and patterns used), and management, economic or political constraints. This part will be based on the views created in all activities of the "Definition and analysis of requirements" process and those resulting from the "model architectures" activity.

4 Examine the suitability of the quality attributes for the architectural approaches. On this occasion, the risks, non-risks, critical points or tradeoffs made to satisfy quality requirements on the chosen characteristics are listed for each scenario. The process involves showing how architectural decisions allow top priority scenarios to be respected. If a scenario cannot be satisfied, this represents a major risk. It is used to come up with a list of components involved in the scenario and the effects (potential) on critical system requirements, an evaluation sheet for each scenario and a reasoned summary of the correspondence between the scenarios and the architectural approaches.

The method may be used from the start of the acquisition process as well as in a development phase. It is, however, recommended to use it as early as possible in the life cycle.

Interoperability

Interoperability is not synonymous with openness but it is the main attribute of it. It is necessary, during evaluation, to examine the scenarios that implement the various interfaces of the system with the external systems with which they interoperate. These scenarios must allow interoperability to be evaluated under four dimensions (‘PAID’). The procedures (P) dimension is important for exchanges, especially from the point of view of their security, their confidentiality and possibly their authentication. The applications (A) dimension is important from the point of view of sharing applications (if required). The infrastructure (I) dimension is particularly important from the point of view of standards and OTS components. Finally, the data (D) dimension is important from the point of view of changes to exchange formats, upgradability (addition of new messages for example) and the consistency of the semantics for data common to several applications.

It is also necessary to think about the mechanisms implemented to ensure the upward compatibility of interfaces, particularly those for which it is known that the standard on which they are implemented or the technology that they use are likely to develop quickly.

Checklists

A few key questions:

- What security requirements affect the openness?
- Have all the key interfaces been identified?
- Are the standards used overwhelmingly recognised?
- Have the critical requirements with regard to the openness been fully identified?
- What new functionalities are anticipated in the future?
- How are changes to any OTS components used taken into account?
- What fast-moving technology is used?
- For which components (hardware/software) are multiple supply sources needed?
- Which components are critical from a logistical point of view?
- Which components must be replaceable in operation?
- Which components are likely to be subject to reversibility?
- Which interfaces/components are critical from the point of view of dependability and personal safety?

18 Requirement establishment and analysis process

18.1 Establishment of stakeholder requirements

18.1.1 Define the requirement

The requirement corresponds to the first statement of definition of a system (what is it used for, who is it used for, in what context is it used, what is its purpose, what is its operating duration, etc.). From a customer request, the following is to be defined:

- the known or probable future environments of the system,
- the operational assignments (explained using projected and representative scenarios in the operational environment),

- the functional definition in terms of scope, objectives, expected behaviour and performance and required properties.

18.1.2 Identify the stakeholders

In addition to identifying people or groups of people who have a legitimate interest in the system during its life cycle, the stakeholders involved with third party systems (present and future) with which the system must interoperate need to be listed.

18.1.3 Identify the requirements and constraints of the openness

They may correspond to expected requirements of the system (interoperability, upgradability, etc.) but also those imposed either by practices in the operational environment (standards, industry rules) or by the designer's work methodology (mainly for aspects relating to pooling of system design: interchangeability, reusability, flexibility, etc.). It is worth noting that the openness level of the system to be designed will depend on cost of ownership requirements. It is also recommended to identify the rules and standards applicable to the system domain.

Method:

the following (non-exhaustive) list of questions to ask can be used. For each response identified, the corresponding requirements in terms of interoperability, modularity, flexibility, interchangeability, etc. need to be stated:

- What functions/services have to be used by a third party system (for interoperability)?
- What functions/services are affected by rapid development from the point of view of use or a technological point of view (for flexibility and upgradability)?
- What functions/services need to have several supply sources (for interchangeability)?
- Which functions/services can be reused within the system?
- Which functions/services can be assumed to be sustainable and which are expected to need to be upgradable?
- Which hardware/software dependencies are critical in terms of cost, maintainability, support, etc. (for general modularity)?
- If the acquisition strategy is incremental, which functions/services are affected by the increments?
- Which requirements and constraints relating to the project system (e.g. organisation to be put in place for collaboration, necessary skills)?
- What budgets are in place for the system at each stage of its life cycle (for affordability)?

N.B.: These questions may be applied to the components when they are imposed.

18.2 Definition of stakeholder requirements

18.2.1 Establish usage scenarios

The usage scenarios are used to analyse the use of the system in its environment and to identify the requirements that have not already specified by the stakeholders. The openness characteristics need to be highlighted by describing the operational scenarios that show the chaining of system functions, both internally and using an external flow.

Method:

- Business Process Modelling (BPM),
- Analysis of usage scenarios,
- Operational views of architecture frameworks.

18.2.2 Characterise the operational flows and list the interfaces of the target system

For each of these different usage scenarios, it is necessary to identify and characterise (type, format, etc.) each incoming and outgoing flow (information, flow/electric signals, fluids, etc.) and the interfaces with the external systems that support these flows.

These components are essential for subsequent identification of the rules and standards to use, the reusable components, the critical interfaces and for creating an open architecture and characterising the degree of system openness.

18.2.3 Characterise the interfaces and define the openness requirements for the interfaces

Definition of the functional and non-functional interfaces is essential for systems with open architecture that are required to evolve and interoperate with other systems in a SoS environment. With each flow (information, electric flows/signals, fluids, etc.) passing through an interface, this is identified using the flow diagrams above.

The requirements associated with interface modularity (to encourage system interoperability), interface upgradability (to encourage system upgradability) and rules, regulations and standards imposed on the interfaces will be defined.

Method:

Coupling matrix (or N^2 matrices).

18.2.4 Highlight the services that the system must provide

The view of services is a description of the services that the system must provide to third party systems to create usage scenarios, regardless of the way in which these services are produced. Each service groups together a coherent set of functions that it carries out.

Method:

- Service view of architecture frameworks,
- Analysis of usage scenarios.

18.2.5 Define the functions that the system must carry out

Identify the functions that perform the services. According to the openness requirements requested by the stakeholders (upgradability, interchangeability, etc.), it is also necessary to identify and characterise the internal flows as well as the functional and non-functional interface constraints.

Method: Functional breakdown (for prioritising the functions and contributing to internal flow characterisation).

18.2.6 Define the requirements that may restrict architectural choices

The openness characteristics of a system generate technical constraints and have a direct influence over the architectural choices. Indeed, the main principles on which the architecture of an open system is based are: the modular design, the identification of key interfaces and the use of standards. Thus, to encourage interoperability, some technological choices may be imposed according to rules, standards and regulations in the operational environment. The same goes for the other openness characteristics (upgradability, reversibility, reusability, etc.) and the choice of certain components or certain internal interfaces may be imposed or restricted.

Requirements resulting from interoperability:

Interoperability may therefore be seen as a requirement that covers requirements relating to compatibility (rather static and often handled like a regulatory and/or technical requirement), interoperation (dynamic as changing and may be temporarily non-compliant with, in this case, potential well-known and unforeseen effects on the two systems) and ability to revert to the previous configuration (dynamic as changing here as well over time and stipulating the possibility for the interactive systems to return to their state, considered as original, before their interaction).

The required level of interoperability for the system results in requirements that can be divided into four dimensions: procedures, applications, infrastructures, data.

Procedures:

For each flow identified (mainly data streams), it will be necessary to define transfer procedures, which results in requirements relating to frequency, volumes and/or flow. These procedures cover operational, functional and technical aspects as well as standards for architectures (software, hardware, data, etc.).

Applications:

It is then necessary to ensure that data exchanges are interpreted by both the system to be designed and the third party systems, which results in requirements relating to processing of the transferred flow, implementing, for example, adaptors.

Infrastructures:

It is necessary to manage dependability associated with the flow transfer, which results in the specification of requirements in terms of security and protection of flows, particularly when operations are carried out through a single interface but on different networks (public, restricted or classified).

Interoperability of a system also results in requirements for its component applications. The level of sophistication of an application will be directly linked to its gradation in the interoperability levels.

The infrastructure affects everything to do with the connections between systems and/or applications and everything that establishes, affects and facilitates interaction between systems (“middleware”). Interoperability of the system is accompanied by requirements for the infrastructure that can be broken down into five sub-domains:

- Communication and network requirements (cable between two machines, LAN, WAN, WiFi, satellites, etc.),
- System service requirements,
- Hardware requirements (use of standards, OTS components, etc.),
- Security equipment requirements (encryption hardware, firewall, multi-level gateways, etc.),
- Dependability requirements.

Data:

The data domain groups together all the information used and processed by the system from the point of view of data format (its syntax) but also its meaning (its semantics). This includes all forms of data that support each level of the system’s operations from the operating system and the communication infrastructure to all the end user applications. It is therefore necessary to mention requirements for standards on file formats and databases and for the precise semantics of the data, particularly for data exchanges between applications or systems.

Methods:

- Many methods, such as LISI (Level of Information Systems Interoperability) and NATO C2 Maturity Level (NML) defined in NNEC (NATO Network Enabled Capability),
- Service, system and technical views in architectural frameworks.

Requirements resulting from upgradability:

The requirements associated with the upgradability of a system relate to both changes to operational capacities, technology, rules and standards, as well as to management of hardware and software obsolescence. Indeed, changes in capacities and technological developments cannot be considered independently as an expected technological change may, for example, allow a capacity change that would otherwise be impossible.

Capacity-related requirements will allow the type of growth and exploratory scenarios which must be looked at in architectural evaluation to be determined.

Technological requirements may be closely linked to the technological readiness milestones highlighted in the “prospective” part.

Upgradability requirements must be defined taking into account the life cycle of the system. They should therefore be time-marked.

Method: Technological watch, TRL

Requirements resulting from interchangeability:

The interchangeability of a component imposes, for system architecture, the loose coupling of the component with the components to which it is interconnected. This characteristic also results in requirements in terms of rules, regulations and standards to be used for the interface or interfaces that the component provides and requires. It is necessary to express the interchangeability requirements at least for the components the lifespan (calendar or cyclical) of which is not compatible with that of the system (obsolescence handling).

Requirements resulting from reusability:

They relate to the requirements (or constraints) generated by the use of existing (OTS) hardware or software components that may be integrated into the system without modification or, if they are configurable, with a configuration adjustment. In order to identify these requirements for the system it is essential to characterise the prospective OTS components and to take into account any changes to them during the life cycle of the system.

Method:

- Characterise the prospective OTS components,
- Define the resulting requirements for the system.

18.2.7 Identify the openness characteristics associated with the MMI

When different systems interoperate, this lead the users of these systems to exchange, communicate and coordinate. The MMIs of the different systems must allow them to share a common understanding of the situation, the status and their environment. It is necessary to identify what information users need for this. Therefore, to aid interoperability of the system to be designed, it becomes necessary to create an MMI consistency guide.

It is also necessary to define the openness characteristics specific to the MMI. Depending on the upgradability of the system, its MMI should itself be upgradable. Reusability, reversibility and interchangeability may also be characteristics specific to the MMI.

In any case, the creation, modification or development of the MMIs must be evaluated (functionality, impact on the working environment of operators, etc.) and validated by prototyping, with the users.

Method:

- MMI consistency guide,
- Human-centred design principles (see standard ISO 9241-210:2010).

18.2.8 Define the requirements which have inevitable consequences for contracts and technical or project decisions

Generally speaking, any requirement has consequences for contracts, technical decisions or projects, whether they are budgetary, schedule-related, strategic, etc.

With regard to interoperability requirements, the systems contributing to a SoS and the SoS itself, the exchange of information between partners and the supply of planned developments have consequences for contracts, the budget, the schedule of major changes and so on.

Requirements resulting from reversibility:

This openness characteristic involves requirements in terms of implementation which must not depend on specific technology of the industrial contractor who designed the first version. Reversibility will be facilitated by the use of rules and standard, where this is possible, and by the use of technology widely distributed for performance.

Furthermore, reversibility involves specific requirements for contractors in relation to intellectual property rights and licences. These requirements will be dealt with during the contract signature phase.

Method:

- Use non-proprietary components,
- Define the system’s property transfer requirements enabling partial or total reversibility of the system.

18.2.9 Formulate the Manufacturing, Integration and Transition requirements specific to the openness

- Define the manufacturing constraints for system components that have an impact on the openness characteristics,
- Define the requirements for integration of the components into the system to be designed (accessibility of components involved in reusability, upgradability, interchangeability, etc.) particularly for OTS components,
- Define the requirements relating to the system’s transition with third party systems that ensure interoperability (sizing, specific requirements, etc.).

18.2.10 Formulate Verification and Validation requirements

Just like many so-called non-functional requirements (portability, maintainability, usability, reliability, etc.), requirements relating to the openness are difficult requirements to check due to their imprecision if they are not expressed and formulated correctly, or due to the potential cost of testing and they are, as a result, often under-evaluated. It is, however, essential to define requirements in terms of methods, means and expected results which enable evaluation of the technical completion of the system and the achievement of objectives, particularly associated with openness. Whether the interoperability and upgradability requirements are defined in terms of quality or quantity, it is necessary to associate evaluation metrics, the sensitivity of which depends on the present or future operational environment of the system (growth capacity of x% in y years, interoperability with a system about which there is little information, etc.).

18.2.11 Prepare the information to be provided with regard to the operational openness requirement in the various documents at the beginning of the design phase

Particular attention shall be paid to information regarding interfaces (internal and external) and OTS components. For the latter, it is necessary to ensure that each OTS component is or will be adequately described to characterise, verify and validate its operation within the system and during the life cycle of the system. It is preferable to have the following information:

- Supplier's references;
- Basic OTS component characteristics;
- Any associated rules or standards;
- The necessary hardware configuration;
- Any software necessary;
- The conditions for use;
- The qualification and/or certification conditions;
- The robustness;
- The performances;
- The associated documentation;
- The licences and property rights;
- The functional capacities;
- The interfaces required;
- The versions;
- The usage restrictions.

18.3 Analysis of stakeholder requirements

18.3.1 Analyse all requirements obtained

- Check the impact of requirements associated with openness on the other functional or non-functional requirements (portability, maintainability, ease of use, reliability, etc.),
- Identify and prioritise the requirements and identify conflicts and missing, incomplete, ambiguous, contradictory, incongruous or unverifiable requirements,
- Resolve the problems identified above (in consultation with the stakeholders),
- Check the integrity of the system requirements to make sure that each requirement or group of requirements ensure the overall integrity of the system.

18.3.2 Select the critical requirements with regard to openness

The selection of the critical requirements with regard to openness depends on the openness criteria priorities. In accordance with their contribution to satisfaction of the operational requirement, a prioritised list is thus established by classifying the requirements according to three categories: essential, important or desirable. The aim of this list is not to do away with certain requirements but to look for a strategy to handle them better. It will mainly be used for evaluation of an open architecture and for value analysis.

18.3.3 Validate the specification of requirements with the stakeholders

It needs to be established with the stakeholders involved that the system requirements specification created correctly reflects their requirements and their desires but also the constraints resulting from the system characteristics (like the openness). It should, in particular, be confirmed that:

- the requirements can be understood by the stakeholders who created the requirement,
- the resolution of conflicts in the requirements has not corrupted or deviated the objectives of the stakeholders,
- the specification that results from it satisfies, necessarily and adequately, the requirements of the stakeholders (level of openness compliant with expectations),
- the specification represents a necessary and adequate entry to the other processes, in particular the architectural design process.

18.3.4 Trace the requirements in a way appropriate to management of requirements

The requirement specification document serves as a reference base for requirement traceability throughout the life cycle of the product. It is therefore necessary to identify (label) the requirements in a practical form so they can be managed. The requirements associated with the openness must also be recorded and labelled (in particular the requirements resulting from reversibility). During the life cycle of the system, any change requirement (whether operational, technological or for handling obsolescence) will be analysed compared to this reference base.

18.4 Requirement monitoring throughout the system life cycle

18.4.1 Continue monitoring requirements during the whole life cycle of the system

Requirements management is an essential condition to guarantee the openness characteristics, particularly interoperability and upgradability. Every change to requirements during the system's life cycle must be traced with the associated rational (origin of requirement, objectives, justification, etc.), the decisions and the corresponding hypotheses. The requirements specification may be reviewed at key points in the system life cycle to ensure that changes to operational requirements are taken into account and that the system is compliant with the established objectives.

Requirements monitoring is a source of knowledge for establishing requirements for future systems with which the target system should interoperate or for systems of the same type as the target system.

19 Architecture design process

The purpose of this process is to design one or more prospective architectures that satisfy the requirement expressed and open architecture principles, to optimise these architectures according to various criteria (functional efficiency, cost, risk, ability to be produced and maintained, TRL), to compare, check and validate them in order to implement one of them.

The design requirements specification resulting from this process is used as the basis for designing an integration, verification and validation strategy for the system produced.

As the purpose of this document is openness, within this context the architecture design activities involve:

- Describing and modelling prospective architectures, staying with what is necessary for openness analysis,
- Defining, documenting and managing the architectures, mainly the interfaces, of the system,
- Comparing the prospective architectures and selecting the one that best meets the openness criteria,
- Checking and validating the openness characteristics of the architecture and certifying the interfaces.

Depending on the projects, it is sometimes necessary to study several alternative architectures, to compare them and to select the most suitable one with regard to the criteria defined. The approach adopted here involved designing prospective architectures then comparing them to select the one that best meets the requirement and the openness criteria.

19.1 Describe and model prospective architectures

As open systems are complex, their engineering is made easier by the use of models.

The architecture of the system to be studied is described so as to apply the following open architecture principles:

- Functional modularity: The modular design allows system expansion or reconfiguration to be anticipated by the incorporation of replaceable components. The first stage in the design of a system is to segment the system into subsystems or components and to identify the parts that have to be modular. The modular design involves the iterative succession of:

- Breakdown into subsystems or high-level components, then in turn into low-level components;

- The identification of interfaces (internal and external);

- The allocation of performance to the components from the highest level down to the lowest.

The breakdown of the system into subsystems is based on the functional analysis approach using input documents that are the functional specifications, the activity analyses to identify the usage scenarios, the description of the context and the environment, the standards to be applied and the allocation of services and interfaces.

The modularity is characterised by:

- Loose coupling of the components; the objective is to limit interdependence of the functions and components to facilitate future modifications by reducing their architectural impact, throughout system life cycle (e.g. addition of modules or replacement of physical modules by other, compatible ones);

- A high consistency of components; the objective is to group functions and components together that:

  - are closely related to each other (coupled) in the same module in order to facilitate integration, testing and maintenance to aid interchangeability;

  - have consistent sustainability (obsolescence management).

- The key interfaces: These are identified during the “Define and document the system’s internal and external interfaces” activity. They are the interfaces of the various modules. They must be modelled logically and physically on the systems and subsystems that support them. These interfaces must be characterised in terms of services provided and in terms of performance (service quality). In addition, this characterisation of services and performances must be independent, insofar as is possible, of the technologies implemented by the modules to perform them. Finally, the characterisation of these services and these performances must be published so that the other modules can “familiarise” themselves with it (concept of discovery in the field of service-oriented architecture). This publication may be in the form of a “yellow pages” type of services catalogue or even through a services broker who plays the role of a trusted third party.

- The separation of concerns, also known as separation of “aspects”), in an aspect-oriented architecture approach. It involves separating everything that comes under functions and services from everything that comes under other dimensions, such as ease of use (usability), security, maintainability and portability. The objective of such a separation of concerns approach is to limit dependency between functional modules and non-functional modules.

- The standards: They must be stated for all interfaces that can be standardised.

The descriptions used must comply, insofar as is possible, with the selected architecture framework.

19.2 Define, document and manage the architectures, mainly the interfaces, of the system

Interface definitions must be documented and available to stakeholders who need them (i.e. those who develop systems/subsystems that interface with the systems/subsystems in question). These definitions also include the limitations imposed by intellectual property rights.

These interface definitions are managed in configuration, taking into account any changes that may occur.

If the use of OTS components is anticipated, it is necessary to check that they satisfy the design and interface criteria identified above.

19.3 Compare the prospective architectures and select the one that best meets the requirement and the openness criteria

Comparing the prospective architectures allows one to be selected that best meets the requirement and the openness criteria. It may implement a multi-criteria analysis, including a weighting of the openness criteria depending on the requirement expressed.

19.4 Check and validate the openness characteristics of the architecture and certify the interfaces

The verification and validation activity may draw inspiration from the Software Engineering Institute's ATAM method ("Architecture Trade off Analysis Method"). It involves determining the main quality attributes to be evaluated and, potentially, establishing priorities between these attributes. The quality attributes associated with the openness are interoperability, interchangeability, requirement upgradability, technology upgradability, reusability, reversibility, flexibility and affordability.

All verification and validation means may be implemented (inspection, simulation, demonstration, testing) depending on the types of architecture and interface dealt with.

Interoperability is not synonymous with openness but it is the main attribute of it. It is necessary, during evaluation, to examine the scenarios that implement the various interfaces of the system with the external systems with which they interoperate. These scenarios must allow interoperability to be evaluated under four dimensions (PAID) (see "requirements resulting from interoperability").

It is also necessary to define the mechanisms in place to ensure upward compatibility of interfaces.

Interfaces are certified by a trusted third party who checks the compliance of the interfaces compared with the architecture standard and the characterisation of services and performances.

20 Execution process

There are no specific openness and interoperability requirements in this process.

21 Integration process

The integration process consists of assembling the different components of the system to form complete or partial system configurations to produce a product that meets the specified system requirements. No specific method has been identified for integration of the components of a system with one or more openness characteristics, but there are complementary actions that come under interoperability and system openness.

The system verification stages must be performed (see verification process) at the same time as the integration process, then validation is carried out (see validation process). If the design has not taken into account the openness and interoperability criteria, the integration cannot be performed successfully.

21.1 Establish an integration strategy

The integration strategy must reduce the risks of integrating system components as much as possible. Within the context of an open system, the assembly sequences may be created so as to meet an incremental verification requirement, either of functionalities, physical modules or a combination of the two.

The integration strategy must also ensure that the integration of additional modules does not affect the system's openness characteristics (using a non-regression approach).

One rule to be applied is to integrate the various validated components as soon as possible and not wait until all the components are ready and tested (suitable integration platform).

For a system contributing to a SoS, the integration strategy must take into account not just the integration of system components but also the integration of the target system in the SoS. This strategy must be consistent with the integration strategy of the SoS itself.

21.2 Define the design constraints resulting from the integration

The integration generates design constraints. These constraints mainly relate to:

- system modularity,
- the integration means and the associated validation tests,
- the interfaces/interconnections required for assembly of the intermediate and future configurations and for test performance,
- the interfaces with the other contributing systems (including those for maintenance and built-in logistical support).

22 Verification process

The verification process answers the question "Are we making the product correctly?": it confirms with tangible proof that the requirements of quality, compliance with standards and design and development methods have been properly respected. The verification may cover activities such as comparative analysis and documentary reviews and provides essential information for corrective action to resolve non-conformities with regard to design and development standards and methods.

22.1 Establish a verification strategy

The verification strategy must, in particular, highlight:

- the correct formulation of the requirements in relation to systems engineering criteria (SMART requirements),
- compliance with architectural standards, frameworks and patterns,
- compliance of the actual, allocated architecture with the architecture description,
- the integrity and completeness of the parts list (particularly for interfaces and OTS components),
- compliance of the components with standards used or rules established,
- traceability (particularly for openness, traceability relating to interfaces, OTS components and standards).

Method: For each type of verification, the IADT method (Inspection, Analysis, Demonstration, Test) may be used, taking into account the associated cost and the criticality of the property being tested.

22.2 Define the design constraints so the system can be verified

Verification generates design constraints. These constraints mainly relate to:

- the physical accessibility of the components to check (connections and probes as well as documentation, etc.),
- the suitability of the available means of measurement for the parameters to check,
- the reliability of the verification and measurement means,
- the loose coupling between the verification means (system contributing to verification) and the system to be checked.

22.3 Check the openness characteristics

Open system is verified by analysis of its architectural characteristics, i.e.:

- **system modularity**: does the system design satisfy the characteristics and apply the openness quality metrics identified through the measuring process? Example of questions: what are the coupling and aggregation levels of the components? Does the system allow physical or functional components to be added or removed?
- **the components used**: what type of components are used (specific, OTS)? What is the level of technological readiness of the components? What level of information is available on each component (bundle or source code available, proprietary or public components, etc.)?
- **the key interfaces**: what type are the internal and external interfaces (specific, de jure standards, de facto standards, proprietary, free, etc.)?

Method:

1 ATAM methodology (“Architecture Trade off Analysis Method”, see measuring process),

2 Procedure, application, infrastructure and data views (PAID of the LISI “Levels of Information Systems Interoperability”).

22.4 Identify and correct non-conformities

Data produced during the verification process must be recorded and the non-conformities corrected. Non-conformities that can alter the system openness properties are:

- An incomplete list of requirements, for example unidentified or incorrectly identified openness requirements, particularly visible in the integration phase,
- A list of untraced or poorly traced requirements,
- An incomplete architecture description,
- A discrepancy between a produced component and its description, particularly for interfaces,
- A discrepancy with production and integration of system components compared to the recommended architecture (modularity not respected, access to interfaces difficult, integration not enabling addition of future components, etc.),
- Corrupted or incomplete information relating to the parts list (particularly interfaces and OTS components),
- Poor implementation of standards compared to the rules (normative or usage rules).

23 Validation process

The validation process answers the question “Are we making the right product?” it uses tangible proof to demonstrate that the requirements for a specific use or planned application have been satisfied. In other words, validation must demonstrate that the use of the system meets expectations for the whole life cycle, particularly in the planned operational environment, and that the system satisfies its requirements.

23.1 Establish a validation strategy

The validation strategy must, in particular, highlight:

- the compliance of requirements with stakeholder needs,
- the compliance of the design with the requirements,
- the compliance of the actual architecture with the architecture description,
- the compliance of the constituents with the architecture description (particularly interfaces and OTS components),
- the compliance of the product produced with the specified standards and rules,
- the compliance of the documentation with the product (specifications, definition file, user manual, etc.).

Method: For each type of validation, the IADT method (Inspection, Analysis, Demonstration, Test) may be used, taking into account the associated cost and the criticality of the property being tested.

23.2 Define the constraints resulting from validation

In terms of design, the major constraint for openness, specific to validation, lies in the testability of the system. Thus, interoperability may call for validation beyond the scope of nominal or contractual use (refuelling of an aeroplane in flight, etc.).

Within the context of an open system, validation also imposes constraints in terms of project organisation. Openness requires, in addition to validation means, associated equipment and trained operators:

- the provision of third party systems or a representative model,
- the involvement of third party system stakeholders.

23.3 Validate the openness characteristics

In the validation process, scenarios of usage of the system in its operational environment are used. These scenarios must highlight one or more openness characteristics:

- **interchangeability** can be demonstrated by the replacement of one component by another that has the same functions,
- **interoperability** can be demonstrated by the extent and the quality of cooperation with third party systems or their simulators and/or models,
- **upgradability** can be demonstrated by the addition, modification or withdrawal of one or more components or functions within the context of an adjustment of operational requirements and/or the technologies used in the operational environment,
- **reusability** can be demonstrated by the insertion of the component(s) of the system into another system,
- **reversibility** can be demonstrated by documentary analysis of the component from both a technical (level of information) and legal (intellectual property) point of view,

- **flexibility** can be demonstrated by the deployment of the system (generally accompanied by the addition, modification and/or withdrawal of one or more components or functions) in a different operational environment and/or in a modified (degraded) operational environment.

The system as a whole is declared validated when the specified performances (metrics), including openness performances, are satisfied.

Method: Verification of service provided

23.4 Identify and correct nonconformities

Data produced during the validation process must be recorded and the nonconformities corrected. Non-conformities that can alter the system openness properties include:

- Openness requirements not covered,

- Requirements not complying with needs (over or under-specification, etc.),

- An architecture that does not meet requirements (lack of modularity, etc.),

- A poorly designed interface (the projected nominal flow cannot pass through),

- A discrepancy between the environment identified during transition preparation and the actual operational environment of the system (identification error).

24 Qualification process

Qualification (NF L 00-007B)

All of the tasks that contribute to providing evidence, based on theoretical and experimental justifications, that the defined product meets the specified requirement and is producible.

The qualification decision is the document by which the client issuing the technical requirement specification (TRS) declares, based on theoretical and experimental justifications, that the defined product, identified by the definition file, satisfies all the requirements of the TRS and is producible.

This process is not specific to openness.

However, requirements specific to interoperability can be identified that form an interoperability frame of reference. From this point of view, there is therefore a specificity regarding the object but not the process itself.

25 Operating process

This process defines the activities necessary for the implementation and monitoring of system services and performances from commissioning until withdrawal from service. In order to support the services, it identifies and analyses the operational problems and gives an account of any changes to the operational requirement (capacity or technological change in the operational environment).

25.1 Prepare a strategy for operation

Generally speaking, the operating strategy must take into account:

- the implementation of the system in its projected operational environment, or even in an operational environment that was not envisaged originally (new operational assignments),

- feedback on changes in the operational environment (including new assignments and changes to use policies),

- feedback on problems encountered by operators implementing the system (inadequacy of the system for the actual operational context),

- communication about any changes to operational requirements,

For an open system, feedback about changes to the operational environment and the problems encountered by operators will be decisive when it comes to triggering changes to the system in question.

Feedback may be provoked by or depend on:

- the operating time of the system. If the operating time is long, the system in question should evolve in line with the changes to the operational context, be interoperable with third party systems not designed at the time of its manufacture and so on,

- the changeability of the operational environment (new threats, new devices, for example improvised explosive devices, new device use policies, etc.),

- the upgradability of the technological aspect of its components (obsolescence management, emergence of technological opportunities, etc.),

- the provisions allowing the system to interoperate with a future third party system at a given time,

- the planned provisions, or absence thereof, for changes to the system’s capacity requirement.

The openness characteristics in question are:

- interoperability, when the system is required to interoperate with third party systems or to be integrated into a SoS,

- security, when new security policies are adopted, when new threats are identified or when new stakeholders (all those involved in crisis management) come along,

- upgradability, when new operational requirements (new threats, new policies, etc.) are issued or even when new technologies are likely to be introduced,

- interchangeability, when technological components need to be changed and to coexist alongside other components with the same function,

- reusability, when the system or its components will be reused in another, higher level system,

- flexibility, when operational requirements change by a small amount, needing the system to take them into account without an engineering and design cycle being required.

25.2 Monitor the level of openness of the system throughout its operating cycle

The level of openness of a system may deteriorate for one of the reasons above.

In order to maintain or adjust open system characteristics, it is essential to constantly monitor the operational environment in which the system is operated. Any change to this environment calls for analysis in order to identify the adaptations or changes to be made to the system to guarantee the system openness level.

More generally, each time changes are made, the openness level needs to be checked to make sure it has stayed the same.

26 Maintenance process

This process defines the activities necessary for maintenance of system services and performances from commissioning until withdrawal from service. These activities are defined in order to maintain a level of service availability that meets user expectations. No complementary action or specific method has been identified for maintenance of the components of a system with one or more openness characteristics.

Due to its physical characteristics (in particular its modularity), maintenance of an open system will be easier than for an integrated system. Generally speaking, to guarantee availability of the services provided by the system, the maintenance strategy must particularly take into account:

- The logistics necessary for maintenance (supply of spare parts, infrastructures, test benches),
- Obsolescence management.

The openness has no impact on corrective and preventive maintenance but it does on upgrade maintenance. Like in the operating process, the impact of changes on system openness should be monitored.

Interchangeability is the openness characteristic directly affected by the maintenance process and this must be prepared for as from the early phases of projects.

27 Withdrawal from service process

This process defines the activities necessary for deactivation, disassembly and recycling or destruction of system components. No complementary action or specific method has been identified for withdrawal from service of the components of a system with one or more openness characteristics.

Generally speaking, the withdrawal from service strategy must take into account:

- The means necessary for withdrawal of the system or its components from service,
- The life cycle of each system component,
- The system for processing disassembled components (disposal, recycling),
- The traceability of withdrawal from service operations.

It is worth noting that, because of its physical characteristics, withdrawal from service of an open system will be easier than for an integrated system. Disassembly is of course facilitated by the modular architecture of the system and recycling aided by the use of OTS components that can be reconditioned and reused in other systems.

This process is not specific to openness.

Bibliography

[1] NF L 00-007B, *Aerospace industry — Vocabulary — General terms*

[2] NF X 50-100:1996, *Functional analysis — Basic requirements*

[3] RG.Aéro 000 39B, *Programme management — Guide for the risk control*

[4] ISO 16290:2013, *Space systems — Definition of the Technology Readiness Levels (TRLs) and their criteria of assessment*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™