PRISSMA Project
Plateforme de Recherche et d'Investissement pour la Sûreté
et la Sécurité de la Mobilité Autonome
04/2021 - 04/2024

[L8.13] REFERENCE REPORT ON SYSTEM ENGINEERING

RAPPORT DE REFERENCE INGENIERIE SYSTEME

Main authors: Emmanuel Arbaretier (APSYS), Cédric Gava (SPHEREA)

Keywords: system of interest, system of systems, traceability, requirements, verification, engineering process, logistic support analysis

Abstract.
This documents introduces the key concepts of the IEEE 15288 standard that describes processes for engineering a system to address the needs of the system's stakeholders across all the phases its lifecycle. It presents the key aspects of system of systems, which fit to the ground transportation system, and the enabling systems of a given system of interest, which encompasses the simulation and evaluation environment of an autonomous driving system. This documents also addresses the integrated logistic support stakes which addresses the operation and support of a given system.

Résumé.
Ce document présente les concepts clés de la norme IEEE 15288 qui décrit les activités d'ingénierie d'un système pour répondre aux besoins des parties prenantes du système à travers toutes les phases de son cycle de vie. Il présente les aspects clés du système de systèmes, qui s'adaptent au système de transport terrestre, et les systèmes habilitants d'un système d'intérêt donné, qui englobe l'environnement de simulation et d'évaluation d'un système de conduite autonome. Ce document aborde également les enjeux du support logistique intégré qui porte sur l'exploitation et le support d'un système donné.

Authors	Emmanuel Arbaretier (APSYS), Cédric Gava (SPHEREA), Elodie Chateauroux (TRANSPOLIS), Rafael de Sousa Fernandes (UTAC)
Document ID	PRISSMA/L8.13/V1
Date	20/10/2021
Type of document	Report
Status	Deliverable
Confidentiality	Confidential
WP allocation	WP8-T8.3
Distribution	PRISSMA partners
History	
Version 0	10/08/2021 Creation
Version 1	20/10/2021 Additional elements brought by the contributors have been added to the original version

Table of Contents

1 Introduction

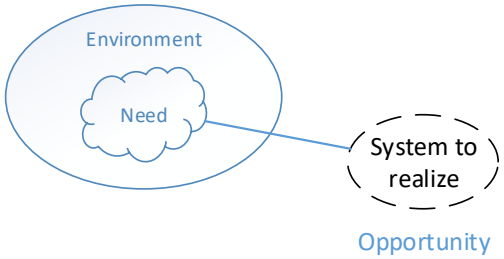
The first version of this document is released prior to the release of the other deliverables of the PRISSMA project which objectives are to define some key concepts, like the characteristics of an ODD for example. As a result, the concepts describe here might be inconsistent with the concepts described in the other deliverables and should be updated to make it consistent with the rest of the PRISSMA project.

2 Systems engineering main definitions and concepts

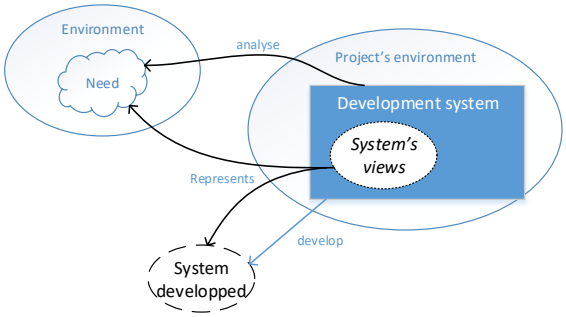
2.1 A simplified history of a system

To better understand the overall picture of system engineering, a simplified history of a designed system has been illustrated in [3]:

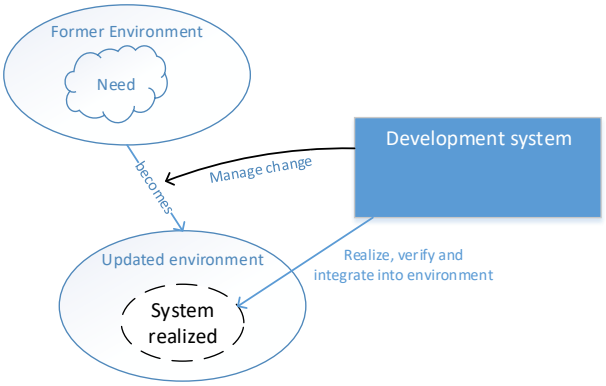
1 – The system's objective is defined: from a given need or problem in a given environment, an opportunity to realize a new system is identified to answer this need or solve the problem.



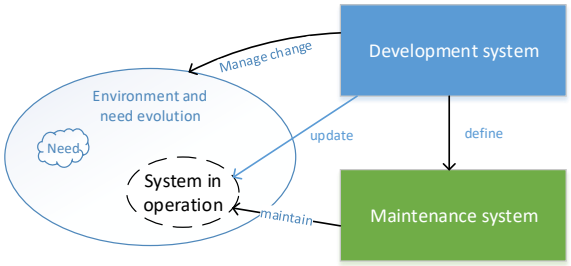
2 – The system is developed: A development system is setup to analyze the need and develop a system based on the analysis and the views of how should behave the system in its environment.
This development system can rely on one or many organizations interacting to deliver the developed system.



3 – The system is realized and placed into its environment: After being developed, the system is realized, verified and validated after its integration in its operational environment. This environment is modified by the insertion of the system.



4 – The system is operated and maintained: The development system can still be in charge of developing evolutions of the system. Another system, called maintenance system or ILS (Integrated Logistic Support) is in charge of maintaining the system in operational conditions.



This simplified history of a system leads to the concept and key points of a system based on the ISO 15288 standard [1]:

The systems considered in this International Standard are man-made, created and utilized to provide products or services in defined environments for the benefit of users and other stakeholders.

These systems may be configured with one or more of the following system elements: hardware, software, data, humans, processes (e.g., processes for providing service to users), procedures (e.g., operator instructions), facilities, materials and naturally occurring entities.

As viewed by the user, they are thought of as products or services.

The perception and definition of a particular system, its architecture and its system elements depend on a stakeholder's interests and responsibilities: One stakeholder's system-of-interest can be viewed as a system element in another stakeholder's system-of-interest.

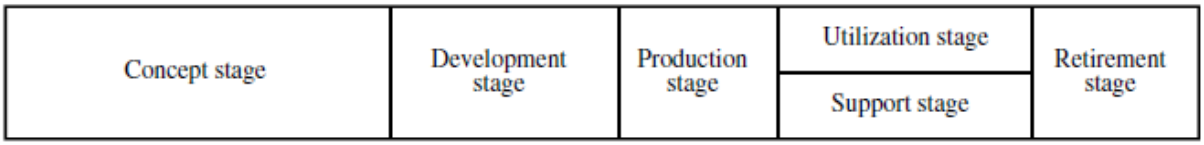
Furthermore, a system-of-interest can be viewed as being part of the environment for another stakeholder's system-of-interest.

The following are key points regarding the characteristics of a system of interest:

a. defined boundaries encapsulate meaningful needs and practical solutions;
b. there is a hierarchical or other relationship between system elements;
c. an entity at any level in the system-of-interest can be viewed as a system;
d. a system comprises an integrated, defined set of subordinate system elements;
e. humans can be viewed as both users external to a system and as system elements (i.e., operators) within a system;
f. a system can be viewed in isolation as an entity, i.e., a product; or as a collection of functions capable of interacting with its surrounding environment, i.e., a set of services.

The different stages of the life of the system from its early conceptualization to its complete retirement is called its lifecycle.

The ISO/IEC TR 24748-1 standard defines generic life cycle stages and their purpose



Life cycle stages	Purpose
Concept	Define the problem space, characterize the solution space Identify stakeholders' needs, explore idea and technologies, explore feasible concepts, propose viable solutions
Development	Define/Refine system requirements Create solution description – architecture and design Implement initial system Integrate verify and validate the system
Production	Produce the system Inspect and verify
Utilization	Operate the system to satisfy stakeholders needs
Support	Provide sustained system capability
Retirement	Store, Archive or dispose of the system

2.2 The hierarchy of a system and recursion of engineering process

A key aspect of system engineering is the decomposition of the SOI (System Of Interest) into system elements. In [1] a system element can be atomic (not decomposed at all during the lifecycle of the system) or can be considered as the SOI for a new instance of the lifecycle, and be further decomposed into further subordinate system elements.

The best practice fostered by [1] is to limit the depth of decomposition of a given system so that the decomposition remains understandable by the stakeholders, and consider the entire lifecycle of this particular decomposition.

Example (see the figure below): When one organization O had agreed to deliver the system S below and decided to decompose it into elements A, B and C, this organization will consider the whole processes without further decomposition of A, B and C and will integrate those components without considering how they are realized. Rather, during the architecture activity, the organization O will decide how each element should be made available to be assembled by this organization to deliver each instance of the system S, either by:

- Using a product already existing
- Delegating to another organization the task to consider this element has the system of interest, end restart the whole process applied to this element.

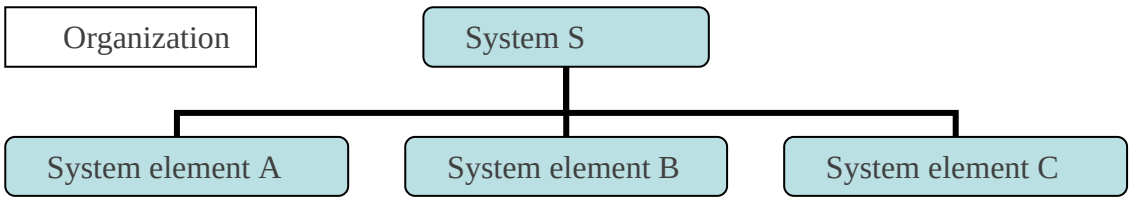


Figure 1: Example of system hierarchy

Supposing that element B and C are already existing, and element A realization is agreed to be delivered by Organization P, then the whole System S would trigger 2 separated system engineering process: one for S, and one for element A.

A chronological example of this situation is illustrated in the table below

Step	Organization O (System = S)	Organization P (System = A)
1	Agreement of supply of System S	
2	Business / Mission Analysis	
3	Stakeholder needs and Requirements Definition	
4	System Requirement Definition	
5	System Architecture Definition	
6	Agreement of Acquisition of element A	Agreement of Supply of Element A
7		System Requirement Definition
8	Acquisition of elements B and C	System Architecture Definition
9		Implementation
10		Integration
11		Verification
12	Validation of element A	
13		Production of Element A
14	Acquisition of element A	Supply of Element A
15	Integration of A, B and C	
16	Verification	
17	Validation	
18	Operation	
19	…	

Table 1: Example of life cycles of related systems

The overall picture of the system hierarchy is depicted by the figure below from [2]. The key point to observe is that the whole decomposition is not addressed by one single instance of the system engineering process described in this document.

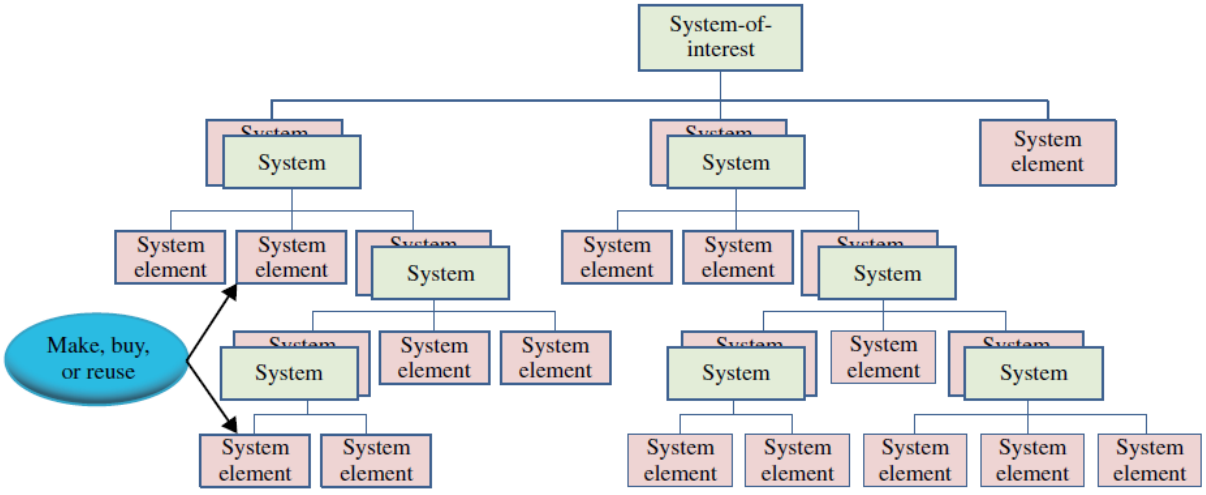


Figure 2 : Recursive hierarchy example from [3]

2.3 Systems of Systems

When the system's elements can be used in different systems at the same time, the SOI can be analyzed as a system of systems (SoS):

More precisely, the characteristics of a SoS are (Maier, 1998):

- Operational independence of constituent systems
- Managerial independence of constituent systems
- Geographical distribution
- Emergent behavior
- Evolutionary development processes

The figure below uses the air transport system as an example of SoS. The aircraft composing this system can be part of this system, but can also be part of many other systems, for example: a non-governmental system aimed at providing health support abroad, a fire management system, or a military system. The fact that an element can be part of multiple systems at the same time is an easy indicator of the need of SoS analysis instead of mere SOI analysis: the fact that a fire bomber aircraft is part of a wildfire neutralization system does not exclude it from being a water carrier system by air, thus making is also a part of the air transport SoS.

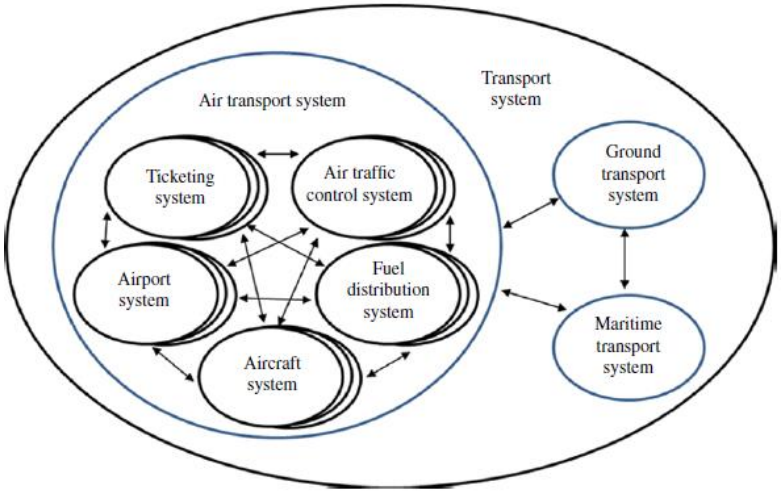


Figure 3 : Air transport system of systems example [2]

Capabilities are realized through a combination of people, processes, information as well as equipment [4];

- They are concerned with delivering outcomes, rather than outputs;
- They are enduring, with capabilities being upgraded rather than replaced; The term emerged in defense in the early 2000, however the concepts go back far earlier (Checkland, 1997).
- The concepts of Capability Systems Engineering have been used in Rail (Dogan, 2012) and Healthcare (Royal Academy of Engineering, 2017).

The concept of capability, used by PFA's automated driving safety validation proposals [10], is a pillar of the definition of a system of systems as composed by independent systems. When integrated, the independent systems can become interdependent, which is a relationship of mutual dependence and benefit between the integrated systems. Both systems and SoS conform to the accepted definition of a system in that each consists of parts, relationships, and a whole that is greater than the sum of the parts; however, although an SoS is a system, not all systems are SoS.

The system engineering's hierarchy principle detailed in the previous chapter enables to address complicated systems, which can be recursively broke down into parts until the parts are so simple that one can understand them separately and, conforming with the golden rules of system engineering process, has confidence that the assembly of the simple parts will have the expected behavior and characteristics as a whole [2].

A complex system cannot be studied this was because the emergent properties disappear when each part is studied in isolation. As a result, system engineering requires a balance of linear, procedural methods for harnessing complexity ("systemic" or systems thinking and analysis – is always required when dealing with SoS).

System of systems engineering "*deals with planning, analyzing, organizing, and integrating the capabilities of a mix of existing and new systems into an SoS capability greater than the sum of the capabilities of the constituent parts*" [DoD, 2004].

The following challenges all influence the engineering of a SoS (Dahmann, 2014):

- **SoS authorities and leadership:** In a SoS, each subsystem can have its own leading organization which objectives most probably differ from the collective objectives of the SoS. The manufacturers of different ADS are competitors and, as such, have objectives in radical opposition. Nevertheless, the ADS sharing the same infrastructure will have to cooperate to reach the objectives of the autonomous ground transportation system.
- **Constituent systems perspectives:** Some parts composing the SoS were often developed for other purposes, and should now being leveraged to meet a new or different application with new objectives. A change in management activity must be setup to deal with the evolution of these parts.
- **Capabilities and requirements [2]:** In classical system engineering, the process starts with a set of requirements of the best quality possible (see § on requirements). Since a SoS is comprised of independent systems with their own requirements, which the stakeholders attempt to interconnect to reach broader capabilities, in many situations the requirements of individual systems will not fit the objectives of the capabilities. In effect, the process consists in finding the new requirements of the existing systems with the SoS acting as a "User".
- **Autonomy, interdependencies and emergence:** The fact that each individual system can have its own evolutions can lead to unexpected or unpredictable behavior in a SoS even if the behavior of the constituent systems is well understood.
- **Testing, validation and learning:** Unlike individual systems, the SoS cannot be completely tested or validated. It is very difficult to assess the level of performances as the basis for determining the areas that need attention or to ensure users of the capabilities and limitations of the SoS.

Often, the only good way to get a good measure of SoS performance is from data collected from actual operations compared with estimations based on modeling, simulations and analysis

(in the context of PRISSMA project, this statement points at the probable need for machine learning also in the test systems).

2.4 Enabling systems

For a given system of interest, the interacting systems that are not required for the operation of the SOI are called enabling systems. These systems are used for the design (engineering tools, project system, business management systems), the testing (IVV bench, simulation environment), or the maintenance (integrated logistic support, maintenance tools and facilities).

During a stage of the system life cycle, the relevant enabling systems and the system of interest are considered together. As they are interdependent, they should be considered as part of a larger system containing both SOI and its enabling systems:

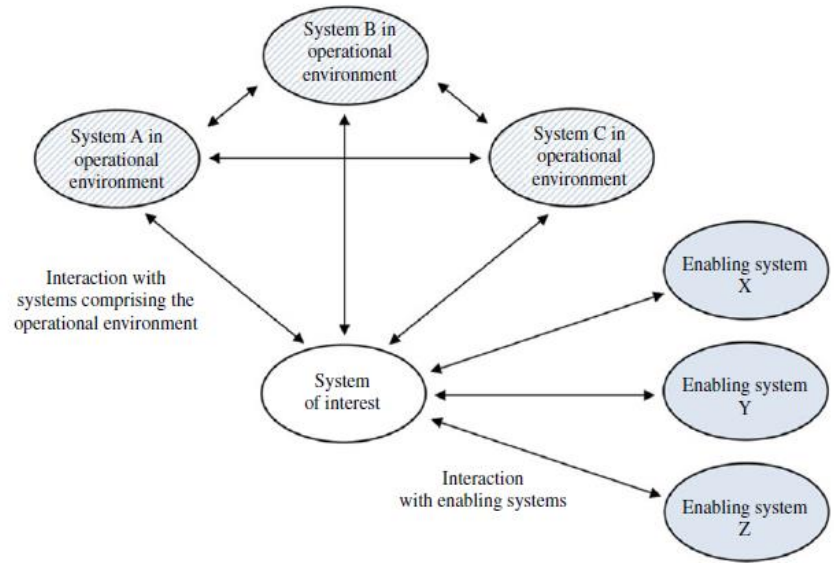


Figure 4 : Enabling systems with regard to system of interest [2]

The section 8 “Integrated Logistic Support” details the process for engineering the enabling system of systems which objective is to ensure that the system of interest meets its mission’s objectives with expected availability and level of performances for its whole operational stage.

This process is an enhancement of the system engineering process described through the sections 3 to 7 when the system of interest is a support system.

2.5 Key aspects of system engineering for dependable systems

2.5.1 Needs and Requirements

As defined by the ISO/IEC/IEEE 29148:2018 [5], a requirement is a *statement which translates or expresses a need and its associated constraints and conditions*. It's one of the fundamental pillars of the actual system engineering practice, as it scopes the intent between an acquirer and a supplier.

The System Engineering Body of Knowledge [7], describes the purpose of requirements:

- Form the basis of system **architecture** and **design** activities.
- Form the basis of system **integration** and **verification** activities.
- Act as reference for **validation** and stakeholder acceptance.
- Provide a means of **communication** between the various technical staff that interact throughout the project

Nevertheless, the quality of the requirements is a big challenge of successful system engineering projects. One of the most root cause of misunderstanding is that **the acquirer won't get what he asked for. The acquirer will get what the supplier thinks the acquirer asked for**, based on the information stated by the words and sentences of the set of requirements written by the acquirer.

This problem, so common in human relationship that each individual human does not consciously thinks about it, has been theorized by Ogden & Richards in 1923, and commonly represented as the semiotic triangle. Two human reasoning about an Object (which can be a real-life object, or a concept) actually reason on their understanding, their own Meaning, of the concept. For the same object, they never share the same meaning. The only thing they can share is their description of the Object, by words, drawing or formulas.

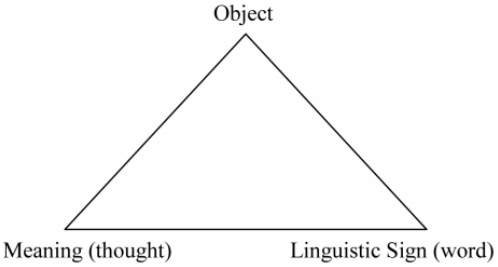


Figure 5 : The Semiotic Triangle

This representation is at the core of the Stanford University's Symbolic systems program to state a common understanding of human or computer agents based on a triptych classification:

1. Human or computer programs are **agents**.
2. Agents exchange **symbols** - words, drawings, concepts (the communication media is of lesser importance, but still necessary for the exchange).
3. The symbols they exchange is driven by the need to understand and interact with their **environment** (so the characteristics of the environment deeply constrain the symbols needed).

The agents never exchange the meaning. Whatever the representation technique used to exchange with other agents, the less formal is the relation between the symbols and the objects, the more misunderstandings will occur between agents.

Focus PRISSMA: The benefits of the symbolic systems principles are multiple in PRISSMA:

The need for the concept of ODD is a direct illustration of these principles: we need a set of symbols to share a common understanding of operational environment both between humans during the design phase and by the autonomous vehicle and drivers during operation.

As stated in PFA's document [10]: *Understandability of autonomous driving functionalities (ODDs, manoeuvers) is key to safety and acceptance.*

- Understandability of ADS by humans (driver or outside the vehicle)
- Understandability between ADS: how to assess, at development and design stage, how different two particular ADS systems understand the same situation? How will they exchange this information is the situation requires decision (like 2 or more ADS systems triggering MRM). A solution would probably be that the ADS system should broadcast their decision and scenario based on a common language, standardized, with a formal semantic like ontologies. With AI, V2X aspects should encompasses more than data or information, it should address also semantics. This standard shall be enforced by authorities, to be also updated by ADS.

Since requirements are sentences, their quality is then at the core of the delivery of the expected system. The S.M.A.R.T. acronym has been a first step towards principles for assessing the quality of requirements [Doran 1981]:

- Specific: the requirement targets a specific area
- Measurable: the requirement quantifies or, at least suggests, an indicator of progress
- Assignable: the requirements specify who will do it
- Realistic: the requirements state what results can realistically be achieved, given available resources
- Time-related: the requirements specify when the result(s) can be achieved

Unfortunately, these simple rules are not enough for ensuring proper quality. The INCOSE had issued a guide for writing requirements which brings more formal criteria to evaluate requirement quality [8]:

> *[...] Even though natural language can be an imperfect way of expression, textual forms of communication remain the only universal means of expression that covers the wide variety of concepts that must to be communicated throughout a system life cycle.*
>
> *Text is not the only medium by which needs and requirements can be expressed. Alternatives to writing textual statements for expression include:*
>
> - *operational scenarios, use cases, and user stories (as used as part of Agile development methodologies, or epics, features and stories in the SAFe Framework);*
> - *prototypes, such as used in production-driven and rapid application development methodologies;*

- *diagrams as part of a modeling approach with well-defined semantics, such as UML for software and SysML for generic systems; and*

- *tabular formats that provide template structures to collect and present requirements, such as Tom Gilb's Planguage (Gilb, T., 2005) or David Parnas's SCR (Heitmeyer el al., 1997).*

Just as there are issues with any form of technical communication, these other approaches can also be imperfect as they do not yet cover the wide range of concepts needed and have their own presentational, traceability, and management challenges.

- *Problem statements, operational scenarios, use cases and user stories are written from the perspective of the user's (actor's) interaction with other actors and the system under development rather than the perspective of what the system under development must do in order for the users to interact with the System of Interest (SOI) in the way they expect, as defined by the use cases. While use cases are an excellent conceptual tool for stakeholder expectation analysis to help understand the features and associated functionality and performance expected by the stakeholders of the system of interest, they do not always effectively replace well-formed, text-based stakeholder needs and requirements for all the various ideas and concepts that must be communicated, especially non-functional needs and requirements.*

- *As an alternate form to communicate stakeholder needs and requirements, use cases, diagrams, and other model forms do not have the characteristics of well-formed statements as defined in this Guide that are necessary to communicate clearly the broad spectrum of needs and requirements into a language that can be clearly understood by all parties (stakeholders, developers, testers) over time.*

A distinction is therefore made between **concepts**, **needs** and **requirements**:

***Concepts** are typically **narrative descriptions** of ways in which the organization (and entities within an organization) expects to manage, acquire, develop, operate, support, and retire the business capability.*

***Needs** are **formal statements** of expectations for an entity **stated in the language and perspective of stakeholders**. Needs are transformed into requirements through a process of requirements analysis (which is also called business analysis or mission analysis at the higher levels)—there may be more than one requirement defined for any need.*

Requirements are formal textual statements that communicate what an entity must do to realize the intent of the needs.

In summary, concepts are informal and narratives, needs are formal and stated in the perspective of stakeholders, and requirements are formal and state what an entity must do to realize the needs.

Which is formalized by the following definitions:

*An **entity** is a single thing to which a concept, need or requirement applies: an enterprise, business unit, service, system, or system element (which could be a product, process, human, or organization).*

*A **concept** is a written or graphic representation that concisely expresses how an entity will satisfy the problem or opportunity it was defined to address within specified constraints with acceptable risk.*

*A **need statement** is the result of a formal transformation of one or more concepts into an agreed-to expectation for an entity to perform some function or possess some quality (within specified constraints with acceptable risk).*

*A **requirement statement** is the result of a formal transformation of one or more needs or parent requirements into an agreed-to obligation for an entity to perform some function or possess some quality (within specified constraints with acceptable risk).*

These definitions lead to characteristics of **well formed-requirements** based on the two main aspects of a requirement statement:

Formal Transformation: *Given the need and requirement is a result of a formal transformation, the following characteristics of a well-formed need or requirement have been derived:*

C1 - Necessary: *The need or requirement defines an essential capability, characteristic, constraint, or quality factor needed to satisfy a concept, need or parent requirement.*

C2 - Appropriate: *The specific intent and amount of detail of the need or requirement is appropriate to the level of the entity to which it refers.*

C5 - Singular: *The stakeholder need or requirement statement should state a single capability, characteristic, constraint, or quality factor.*

C8 - Correct: *The need must be an accurate representation of the concept from which it was transformed. A requirement must be an accurate representation of the need from which it was transformed.*

C9 - Conforming: *The individual needs and requirements should conform to an approved standard pattern and style guide or standard for writing and managing needs and requirements.*

Agreed-to Obligation: *Since the need and requirement is to be a part of a fair agreement to meet an obligation, the following characteristics of a need or requirement have been derived.*

C3 - Unambiguous: *Need statements must be written such that the stakeholder intent is clear. A requirement is stated in such a way that it can be interpreted in only one way by all the intended readers.*

C4 - Complete: *The requirement sufficiently describes the necessary capability, characteristic, constraint, or quality factor to meet the entity need without needing other information to understand the requirement.*

C6 - Feasible: *The need or requirement can be realized within entity constraints (for example: cost, schedule, technical, legal, ethical, safety) with acceptable risk.*

C7 - Verifiable: *The requirement is structured and worded such that its realization can be proven (verified) to the customer's satisfaction at the level the requirement exists.*

Interestingly, the guide defines **need set** and set of requirements, without implying the support for exchanging these sets (documents, database …):

*A **need set** is a structured set of agreed-to need expressions for the entity and its external interfaces captured in an Entity (Enterprise/Business Unit/System/System Element/Process) Needs Document or equivalent electronic representation of the set of needs.*

*A **set of requirements** is a structured set of agreed-to requirement expressions for the entity and its external interfaces documented in an Entity (Enterprise/Business Unit/System/System Element/Process) Requirements Specification (Document). A set of requirements results from the formal transformation of the set of needs that represents an agreed-to obligation for the entity.*

***Formal Transformation:** Given the set of needs and requirements is the result of a formal transformation, the following characteristics of the need and requirement set have been derived:*

***C10 - Complete:** The need or requirement set for a given SOI stands alone such that it sufficiently describes the necessary capabilities, characteristics, constraints, interfaces, standards, regulations, and/or quality factors to meet the needs without requiring other sets of needs or requirements at the appropriate level of abstraction.*

***C11 - Consistent:** The set of needs contains individual needs that are unique, do not conflict with or overlap with other needs in the set, and the units and measurement systems they use are homogeneous. The language used within the set of needs is consistent (i.e., the same words are used throughout the set to mean the same thing).*

***Agreed-to Obligation:** Since the set of need and requirements is to be a result of a fair agreement to meet an obligation, the following characteristics of the set have been derived:*

***C12 - Feasible:** The sets of needs and requirements can be realized within entity constraints (cost, schedule, technical, legal and regulatory l) with acceptable risk.*

***C13 - Comprehensible:** The set of need statements and resulting requirement statements must be written such that it is clear as to what is expected of the entity and its relation to the system of which it is a part.*

***C14 - Able to be validated:** It must be able to be proven that the set of needs will lead to the achievement of the product goals and objectives, stakeholder expectations, risks, and concepts within the constraints (such as cost, schedule, technical, legal and regulatory compliance) with acceptable risk.*

This guide gives some practical rules to assess if the requirement has the characteristic

Accuracy
R1 – Use the form of a complete sentence: subject, verb, object.
R2 - Use the active voice in the main sentence structure with the responsible entity clearly identified as the subject.
R3 - Ensure the subject and verb are appropriate to the level to which the need or requirement refers.
R4 - Define terms in a glossary, data dictionary, etc.
R5 - Use definite article "the" rather than the indefinite article "a."
R6 - Use appropriate units when stating quantities. All numbers should have units of measure explicitly stated.
R7 - Avoid the use of vague terms such as "some", "any", "allowable", "several", "many", "a lot of", "a few", "almost always", "very nearly", "nearly", "about", "close to", "almost", and "approximate".
R8 - Avoid escape clauses such as such as "so far as is possible", "as little as possible", "where possible", "as much as possible", "if it should prove necessary", "if necessary", "to the extent necessary", "as appropriate", "as required", "to the extent practical", and "if practicable..
R9- Avoid open-ended clauses such as "including but not limited to", "etc." and "and so on.".

Concision
R10 - Avoid superfluous infinitives such as ".. be designed to …", "…be able to …..", "…be capable of…".
R11 - Use a separate clause for each condition or qualification.

Non-ambiguity
R12, 13, 14 - Use correct grammar, spelling, punctuation.
R15 - Use a defined convention to express logical expressions such as "[X AND Y]", "[X OR Y]", [X XOR Y]", "NOT[X OR Y]".
R16 - Avoid the use of "not."
R17 - Avoid the use of the oblique ("/") symbol except in units, i.e. Km/hr

Singularity
R18 - Write a single sentence that contains a single thought conditioned and qualified by relevant sub-clauses.
R19 - Avoid combinators that join clauses, such as "and", "or", "then", "unless", "but", "as well as", "but also", "however", "whether", "meanwhile", "whereas", "on the other hand", and "otherwise."
R20 - Avoid phrases that indicate the purpose of the requirement.
R21 - Avoid parentheses and brackets containing subordinate text.
R22 - Enumerate sets explicitly instead of using a group noun to name the set.
R23 - When a need or requirement is related to complex behavior, refer to the supporting diagram or model.

Completeness
R24 - Avoid the use of pronouns and indefinite pronouns.
R25 - Avoid relying on headings to support explanation or understanding of the requirement.

Realism
R26 - Avoid using unachievable absolutes such as 100% reliability or 100% availability.
R27 - State applicability conditions explicitly.
R28 - Express the propositional nature of a condition explicitly for a single action instead of giving lists of actions for a specific condition.

Uniqueness
R29 - Classify the need and requirement according to the aspects of the problem or system it addresses.
R30 - Express each need and requirement once and only once.

Abstraction
R31 - Design inputs avoid stating a solution unless there is rationale for constraining the design. Focus on the problem "what" rather than the solution "how."

Quantifiers
R32 - Use "each" instead of "all", "any" or "both' when universal quantification is intended
R33 - Define quantities with a range of values appropriate to the level stated.
R34 - Provide specific measurable performance targets appropriate to the level at which the requirement is stated.
R35 - Define temporal dependencies explicitly instead of using indefinite temporal keywords such as "eventually", "until", "before", "when", "after", "as", "once", "earliest", "latest", "instantaneous", "simultaneous", "while", "at last".

Uniformity of Language
R36 - Use each term consistently throughout need and requirement sets.
R37 - Use a consistent set of acronyms.
R38 - Avoid the use of abbreviations.
R39 - Use a project-wide style guide for individual needs and requirements and for sets of needs and requirements.

Modularity
R40 - Group related requirements together.
R41 – Conform to a defined structure or template for sets of needs and requirements

Figure 6 : rules for needs and requirements statements [8]

Finally, the guide gives a list of possible attributes to manage the stakes of needs and requirements along their lifecycle (* indicates mandatory attributes).

Attributes to Help Define the Requirement and its Intent
A1 - Rationale*
A2 - System of Interest (SOI) Primary Verification or Validation Method*
A3 - SOI Verification or Validation Approach
A4 - Trace to Parent*
A5 - Trace to Source*
A6 - Condition of Use
A7 - States and Modes
A8 – Allocation*

Attributes Associated with the System of Interest (SOI) Verification
A9 - SOI Verification or Validation Level
A10 - SOI Verification or Validation Phase
A11 - SOI Verification or Validation Results
A12 - SOI Verification or Validation Status

Attributes to Help Maintain the Requirements
A13 - Unique Identifier*
A14 - Unique Name
A15 - Originator/Author*
A16 - Date Requirement Entered
A17 - Owner*
A18 – Stakeholders
A19 - Change Board
A20 - Change Status
A21 - Version Number
A22 - Approval Date
A23 - Date of Last Change
A24 - Stability
A25 - Responsible Person
A26 – Need or Requirement Verification Status*
A27 – Need or Requirement Validation Status*
A28 - Status (of the Need or Requirement)
A29 - Status (of Implementation)
A30 - Trace to Interface Definition
A31 - Trace to Peer Requirements
A32 - Priority*
A33 – Criticality or Essentiality*
A34 – Risk (of Implementation)*
A35 – Risk (Mitigation)
A36 - Key Driving Need or Requirement (KDN/KDR)
A37 - Additional Comments
A38 - Type/Category

Attributes to Show Applicability and Allow Reuse
A39 - Applicability
A40 - Region
A41 - Country
A42 - State/Province
A43 - Application
A44 - Market Segment
A45 - Business Unit
A46 - Business (Product)Line

Figure 7 : attributes for needs and requirements statements [8]

This guide covers the foundational aspects for writing needs and requirements in a way that it improves the probabilities of providing to an acquirer what is expected. The quality of requirements used for any part of the AD System of Systems has a central aspect for the safety and the security of the overall transportation system involving AD systems and their environment.

The usage of ontologies has been in constant evolution for better formalizations of symbolic representations, whatever its graphical or textual nature, in order to reduce the possible misunderstandings between agents, whatever their human or non-human nature.

Ontologies are used for automatically assessing the characteristics of requirements and set of requirements based on [8].

FOCUS PRISSMA: Shouldn't ontologies be an outcome of PRISSMA to sustain common representations of rules and scenarios of AD System in order to improve understandability between the different agents involved in the AD System of systems?

2.5.2 Verification and Validation

Another key aspect of system engineering is on verification and validation, which are also dedicated activities in the ISO 15288 process (see §4.9 and §4.11).

This standard states the definition of these two concepts by complementing definitions coming from the ISO9000:2015

> ***validation:*** *confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled*
>
> *Note 1: Validation in a system life cycle context is a set of activities ensuring and gaining confidence that a system is able to accomplish its intended use, goals and objectives. The right system has been built.*

> ***verification:*** *confirmation, through the provision of objective evidence, that specified requirements have been fulfilled*
>
> *Note 1: Verification in a system life cycle context is a set of activities that compares a product of the system life cycle against the required characteristics for that product. This may include, but is not limited to, specified requirements, design description and the system itself. The system has been built right.*

The guide for writing requirements [8] provides additional precisions regarding verification and validation:

> *The true meaning of the concepts "Verification" and "validation" are often misunderstood, and the terms are often used interchangeably without making clear the context in which they are used resulting in ambiguity. To avoid this ambiguity, each term needs to be preceded by a modifier (i.e., the subject) which clearly denotes the proper context in which the term is being used, specifically need verification or validation; requirement verification or validation; design verification or validation; system verification or validation [...]. The following definitions of these terms are included in terms of a product life cycle:*
>
> ***Need Validation:*** *confirmation that the needs and set of needs clearly communicate the concepts from which they were transformed in a language understood by the requirement writers. The focus is on the message the needs and set of needs are communicating.*
>
> *"Do the needs and set of needs clearly and correctly communicate the agreed-to concepts, constraints, and stakeholder expectations?" or "Have we correctly and completely captured what the system needs to do?*
>
> ***Requirement Validation:*** *confirmation that the requirements and requirement set is an agreed-to transformation that clearly communicates the needs in a language understood by the developers.*
>
> *The focus is on the message the requirements and set of requirements are communicating. "Do the requirements and requirements set clearly and correctly*

communicate the intent of the need set?" "Are we doing the right things?" or "Are we building the right thing [as defined by the requirement set]?"

Need or Requirement Verification: *the process of ensuring the need or requirement meets the rules and characteristics defined for writing well-formed need or requirement statements. The focus is on the quality (wording and structure) of the need or requirement statements. "Is the need or requirement statement worded or structured correctly in accordance with the organization's standards, guidelines, rules, and checklists?" These standards, guidelines, rules, and checklists would be developed at the business management and operations levels.*

2.5.3 Traceability

The whole technical process of system engineering relies on traceability.

Traceability in system engineering is the capability (and implementation) of keeping track of a given set or type of information to a given degree, or the ability to chronologically interrelate uniquely identifiable entities in a way that is verifiable.

The traceability should be applied to most of the elements of concerns of system engineering, for example:

- From a product to its configuration information
- A requirement of system element to requirements of a parent element
- An allocation of a requirement to a system component
- A change request to the configuration item it targets

Ideally a good traceability shall enable to trace back any component or any managed changed of a particular product to all of its information along the whole life-cycle of the product: from its early concept phase, to its disposal. The traceability between definition information is a key to their verification: conformance of the design with its requirements, or coverage and consistency of the requirements of the system with the stakeholders needs.

FOCUS PRISSMA: As expected from Europe with IA Act, traceability is key from the conception phase to the end of the AI/ADS system life cycle.T raceability is state-of-the art in the transportation industry but this traceability shall also be enforced on the enabling systems and their associated development projects. The audits and qualification tests of an IA based AD system should encompass both the system and its test enabling system: a flaw or default on an AD system should have traceability up to the configuration (see §5.5) of the test systems (simulation, closed road or open road) thus including their complete configuration information.

2.5.4 Configuration management

Configuration management is another pillar of dependable systems engineering. Its concepts are detailed in §5.5.

2.6 PRISSMA Context

2.6.1 Shuttle use case analysis

The analysis of autonomous driving systems (AD Systems) falls in the category of systems of systems (SoS): the configuration of the whole system is constantly changing. Moreover, given the nature and environment of the autonomous driving system, its system's view can be very complex to describe, thus even more complex to prescribe.

Let's consider the first example of an autonomous shuttle on a dedicated road.

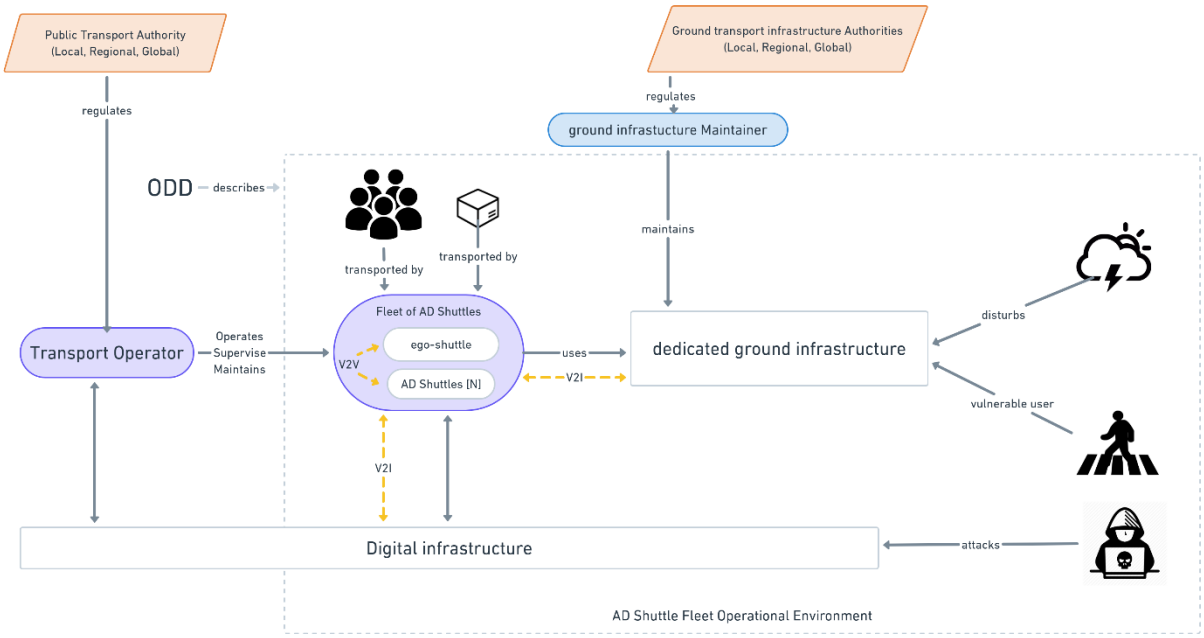


Figure 8 : AD shuttle on dedicated infrastructure operational system view

A **Transport Operator** remotely operates a **Fleet of AD Shuttles** which transports People or Cargo on a **dedicated ground infrastructure**, where most of the paths of the shuttles are dedicated to the shuttles, but there is a risk that some **vulnerable user** can be present on the path. This infrastructure might be equipped with connections for V2I exchanges with the shuttles. It is likely, but not necessarily mandatory, that the shuttles also implement V2V exchanges between them.

Alongside the road is the **digital infrastructure**, used for the connection of all the vehicles with communication networks. The digital infrastructure is targeted by potential attacks from hackers.

The operational environment states can change because of various event (weather, traffic accident, etc, etc). This environment and its different states are described by an ODD (Operational Design Domain), along with the states of the shuttles.

The organizational stakeholders (The transport Operator, the road infrastructure maintainer or the Police) are regulated by legal authorities, constrained at different localization levels. For France vehicle, for instance:

- Global regulation is made by United Nations
- European regulations are made by European Union
- French states add particular regulations for France, with specific organizations for autonomous driving system like STRMTG

Now let's consider the shuttles are operating on predefined paths, but on open roads. Although it is simpler that a complete open roads AD vehicle, yet the vehicles have to adapt to considerably changing environment.

The **Operational Environment** of this fleet has **other vehicles, autonomous or not.** Some vehicle might not have V2I connectivity, nor V2V connectivity with the shuttles. This environment is vulnerable to much more hazards than the dedicated ground infrastructure previously stated.

Since the autonomous driving shuttle might cross some borders, it has to comply with different regulations given its localization, which makes the legal context of this kind of autonomous vehicle more complex.

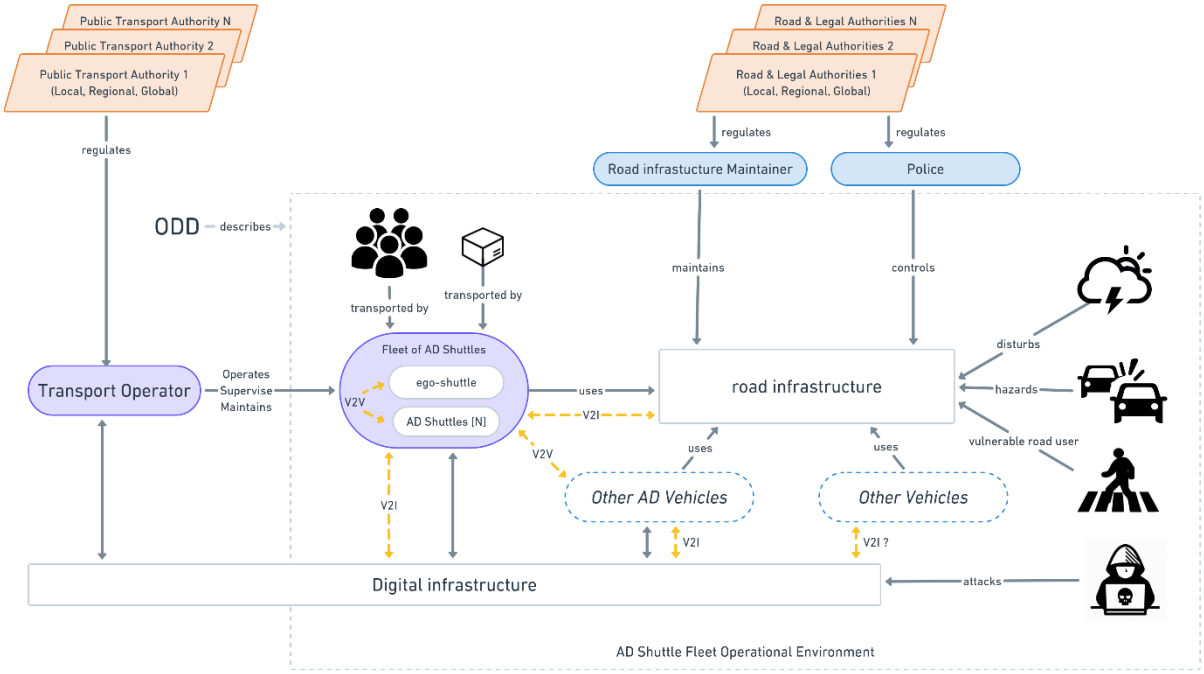


Figure 9 : AD shuttle operational system view

During design phase, the Shuttle Manufacturer is responsible for designing, producing and testing the shuttle fleet. This shuttle fleet and the Shuttle manufacturer are control by public safety authorities.

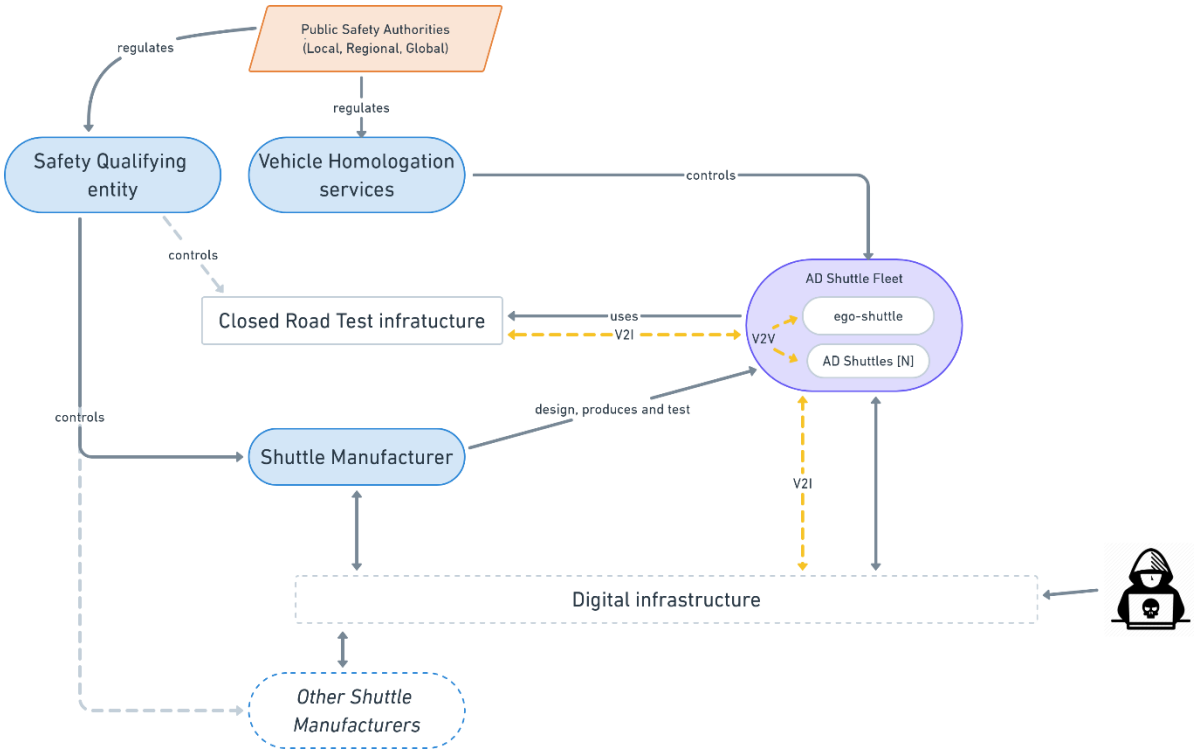


Figure 10 : AD shuttle design system view

2.6.2 Generic autonomous driving system analysis

An example generic view of the AD system of system context is deduced from the previous examples to sustain further analysis of AD systems.

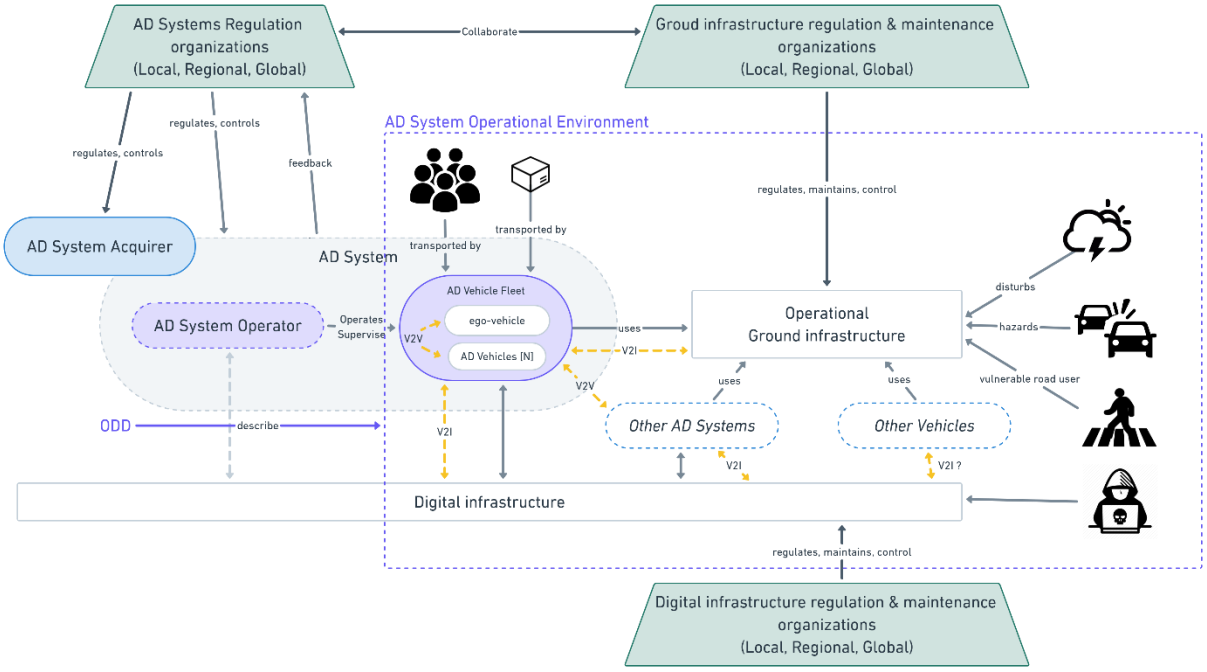


Figure 11 : Generic AD system operational view

The **AD system** is composed of:

- An **ADS Fleet** of **N AD vehicles**, with a particular one named **ego vehicle** if it's necessary to address one particular AD vehicle the **ADS Fleet**.
- An optional AD system operator, which is also a system involving organizations and means to operate the AD System.

It is supposed the AD vehicles transport **cargo payload** or **Non Driver passengers**, it can also have a **local operator** (a driver).

The ADS Operational environment is a group of systems:

The **ADS Fleet** shares **the operational ground infrastructure** (roads, rails and associated enabling systems) with **Other AD Systems**, **Non ADS vehicle**, **and vulnerable users**. The **ground infrastructure** may be subjects to hazards modifying or influencing it in wide range (from mere rain or animal crossing to storm or general failure of traffic lights).

It is supposed that at least one **Ground transportation regulation & maintenance organization** is responsible from stating the rules and norms of the Ground transportation system but, in practice, many should be considered (one for each country or area which defines specific rules for ground transportation system). This organization encompasses law enforcements, road maintenance companies, road manufacturing companies.

It is supposed also that dedicated organizations rules and monitor AD systems during their operations. Those organizations are also supposed to regulates activities of the AD System's acquirer (with dedicated driving licenses for individuals, or special requirements for public

transport companies). All the regulation organizations have dedicated scope of authority that may overlap given the nature of the AD System from local to global requirements. As detailed in the previous section, an AD system bound to a dedicated closed road is obviously easier to design than an AD system for open roads.

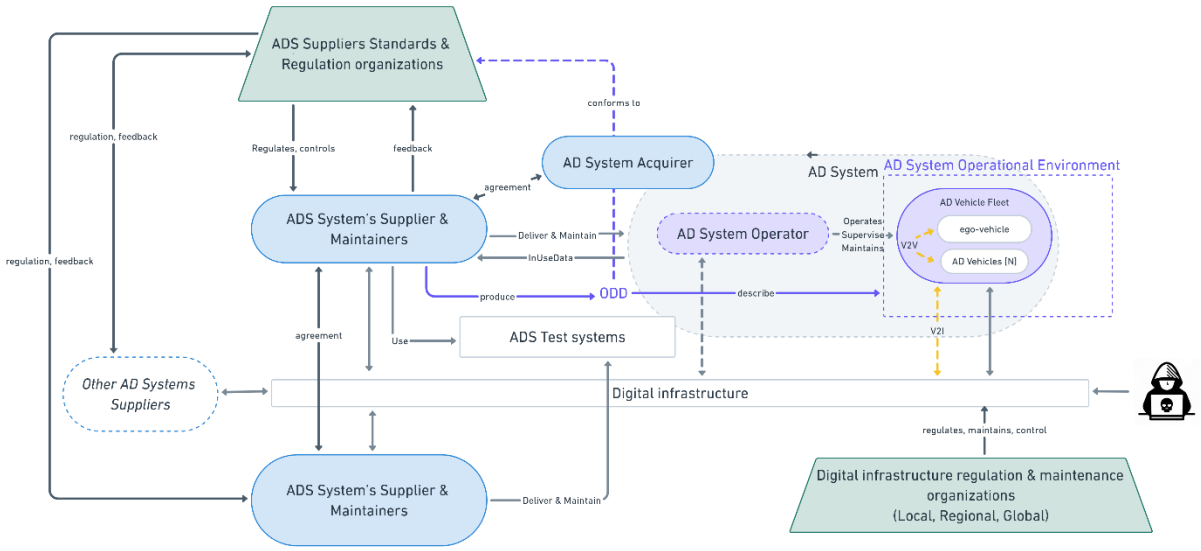


Figure 12 : AD system of systems example

The **AD system** is developed, validated, produced and maintained by ADS System's Supplier & Maintainer organization, which can be one or more probably many companies.*

The regulation authorities ruling the AD systems supplier can play here an additional value by merging the feedbacks from multiple AD system providers, and supplying, in return, common **ADS Missions** and ADS Operational environment models to force the different AD system providers to take into account the feedbacks from all the AD system providers to increase safety when the different fleets will share the same ground transportation systems.

3 Systems engineering process overview

The ISO 15288 standard [1] classifies each process into one of the following categories:

- Organizational Project-Enabling Processes
- Agreement Process
- Technical Management Processes
- Technical Processes

The determination of the life cycle processes in this International Standard is based upon three basic principles [1].

- Each life cycle process has strong relationships among its outcomes, activities and tasks.
- The dependencies among the processes are reduced to the greatest feasible extent.
- A process is capable of execution by a single organization in the life cycle.

Each process of this standard is described in terms of the following attributes:

- The title conveys the scope of the process as a whole;
- The purpose describes the goals of performing the process;
- The outcomes express the observable results expected from the successful performance of the process;
- The activities are sets of cohesive tasks of a process;
- The tasks are requirements.

To summarize each process, the INCOSE system engineering handbook [2] pictures each process using IPO diagram (Input/Process/Output):

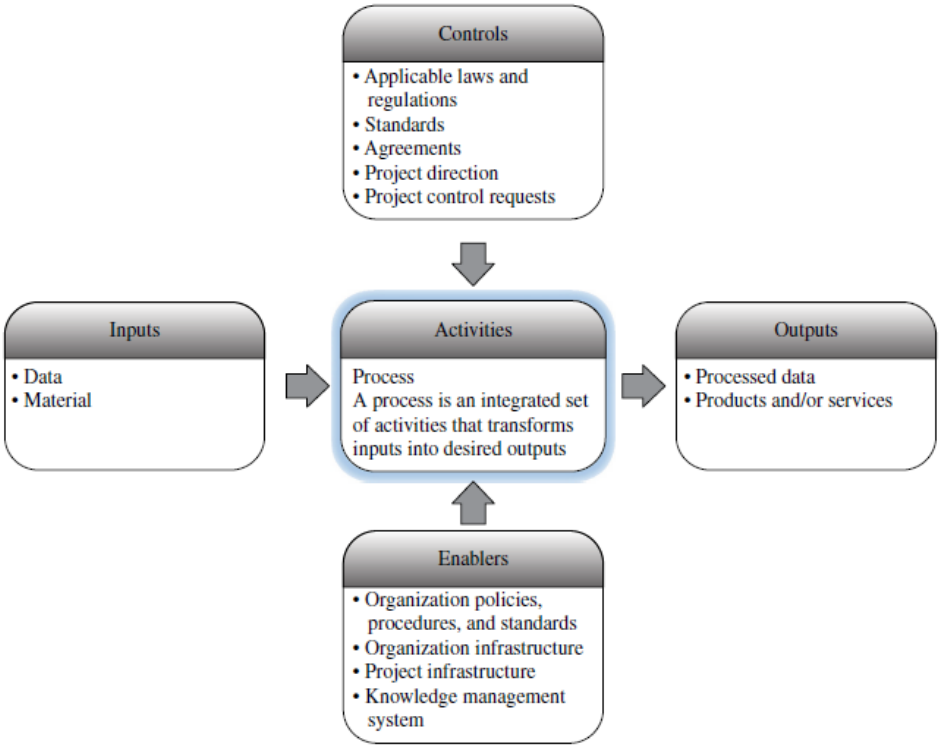


Figure 13 : IPO (Input /Process/Output) diagrams principles

4 Technical process

The Technical Processes are used to define the requirements for a system, to transform the requirements into an effective product, to permit consistent reproduction of the product where necessary, to use the product to provide the required services, to sustain the provision of those services and to dispose of the product when it is retired from service. [1]

The technical processes are often pictured on the V model, extended right part to locate the operation, maintenance and disposal. The Production is not part of ISO 15288, but is an important process that occurs after the development. The importance of traceability is underlined by the red lines showing that:

- The validation of the SOI is linked with the stakeholder requirements, which are often the acquirer requirements
- The verification of the SOI is linked with the system requirements
- The integration of the SOI is linked with the architecture definition

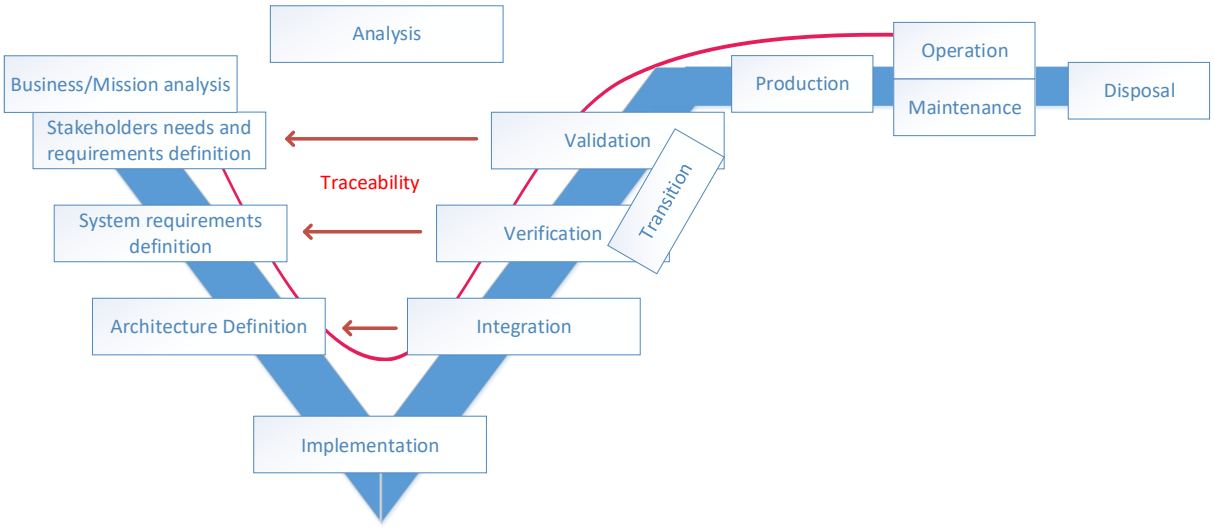


Figure 14 : V cycle display of ISO 15288 processes

A multidisciplinary approach leads to an evolution of this simple V model to a more complete vision of interleaved V cycles for interdisciplinary system engineering:

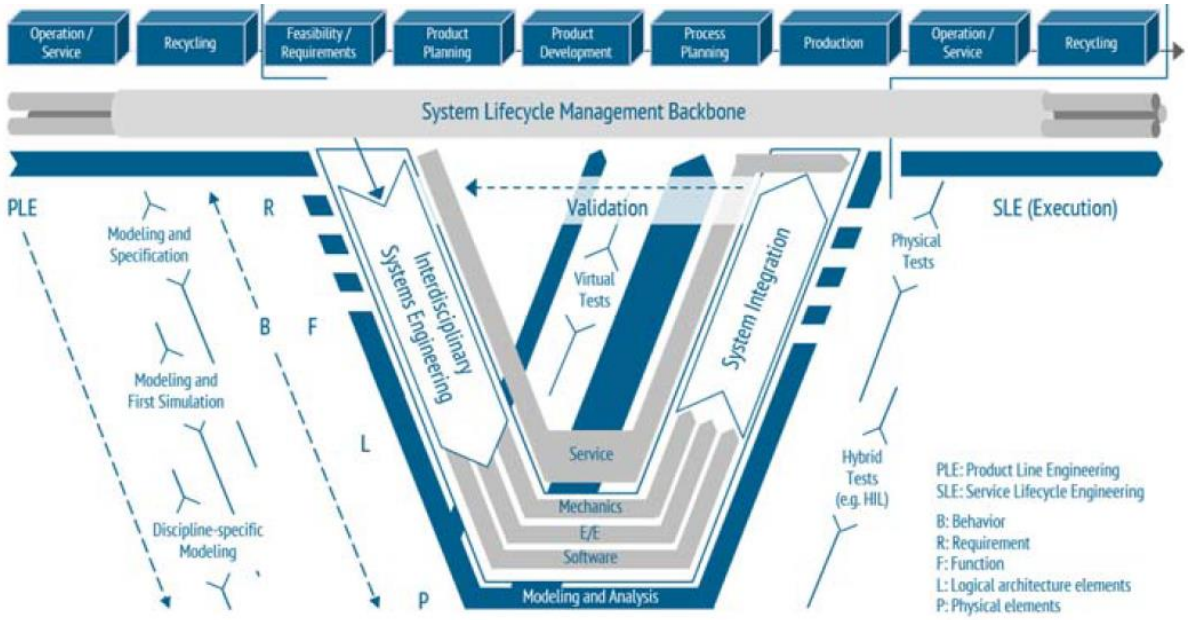


Figure 15 : MPVE V cycle

In this view of the V cycle, the models of the system can have their own V cycle when considered as the product which can be verified and validated. But since this model is an abstraction of the real system, its V cycle is interleaved with the system's V cycle, and can share some artefacts with the real systems:

- Requirements
- Validation elements
- Test systems

FOCUS PRISSMA: The transition from pure simulation to closed road, and open road testing should consider the AD system's model's lifecycle at the same time with AD system itself.

In addition, as any enabling system, the test systems used in the V process of the AD system are considered as the SOI when it comes to design and produce them.

4.1 Business or Mission Analysis

FOCUS PRISSMA: The PRISSMA project itself is part of the Business analysis of deploying AD SoS at large scale (it is the part of the task 8.4 to link the validation framework to the economic efficiency).

The purpose of the Business or Mission Analysis process is to define the business or mission problem or opportunity, characterize the solution space, and determine potential solution class(es) that could address a problem or take advantage of an opportunity [1].

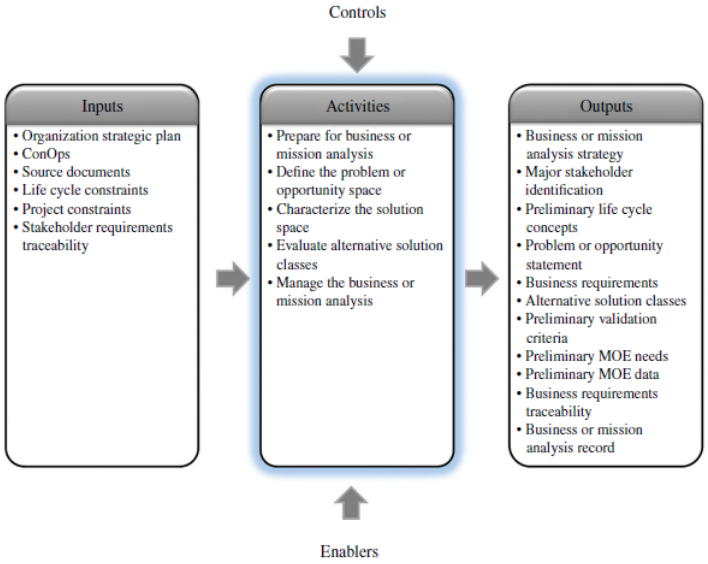


Figure 16 : Business or Mission Analysis IPO diagram [2]

4.2 Stakeholder Needs and Requirements Definition Process

FOCUS PRISSMA: The statement of all the stakeholders' needs and requirements is at the core of the system verification and system validation activities (see §4.9 and §4.11 for these activities). The quality of the statements of the needs and requirements (see §2.5.1) and the completeness of identification of the stakeholders of AD System of System (see §3) will be a key factor for the success of the development of the framework for the safety of AI based AD systems.

When considering a test system as a system of interest, the best stakeholder needs definition is a complete test campaign definition of the system under test. The completeness and the quality of the definition of the tests carried out with the test system, along with the system under test requirements to be tested, is a key factor in the delivery of the test system that fit the need.

The purpose of the Stakeholder Needs and Requirements Definition process is to define the stakeholder requirements for a system that can provide the capabilities needed by users and other stakeholders in a defined environment.

It identifies stakeholders, or stakeholder classes, involved with the system throughout its life cycle, and their needs. It analyzes and transforms these needs into a common set of stakeholder requirements that express the intended interaction the system will have with its operational environment and that are the reference against which each resulting operational capability is validated. The stakeholder requirements are defined considering the context of the system-of-interest with the interoperating systems and enabling systems. [1]

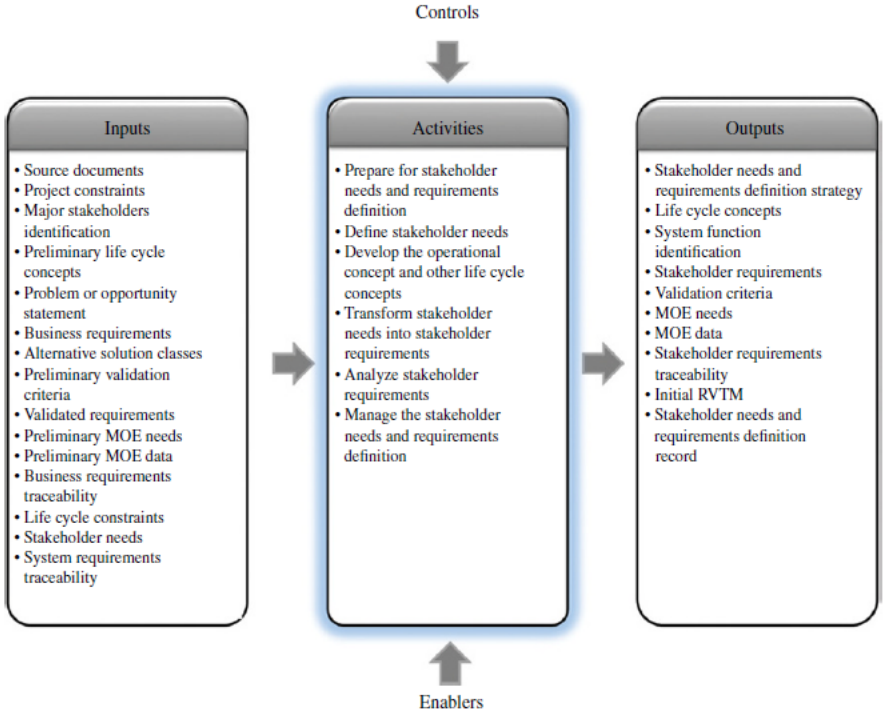


Figure 17 : Stakeholder Needs and Requirements Definition Process [2]

4.3 System Requirements Definition Process

FOCUS PRISSMA: As with the stakeholder needs and requirements definition process (§4.2) a good definition of system requirements is a key to the verification and validation of a dependable system capabilities, including its safety and securities performances.

The assertion of the quality of the system requirements, using precise rules like the writing guide [INCOSE-TP-2010-006-03 - Guide for writing requirements] is key to the success of the system.

The purpose of the System Requirements Definition process is to transform the stakeholder, user-oriented view of desired capabilities into a technical view of a solution that meets the operational needs of the user.

This process creates a set of measurable system requirements that specify, from the supplier's perspective, what characteristics, attributes, and functional and performance requirements the system is to possess, in order to satisfy stakeholder requirements. As far as constraints permit, the requirements should not imply any specific implementation. [1]

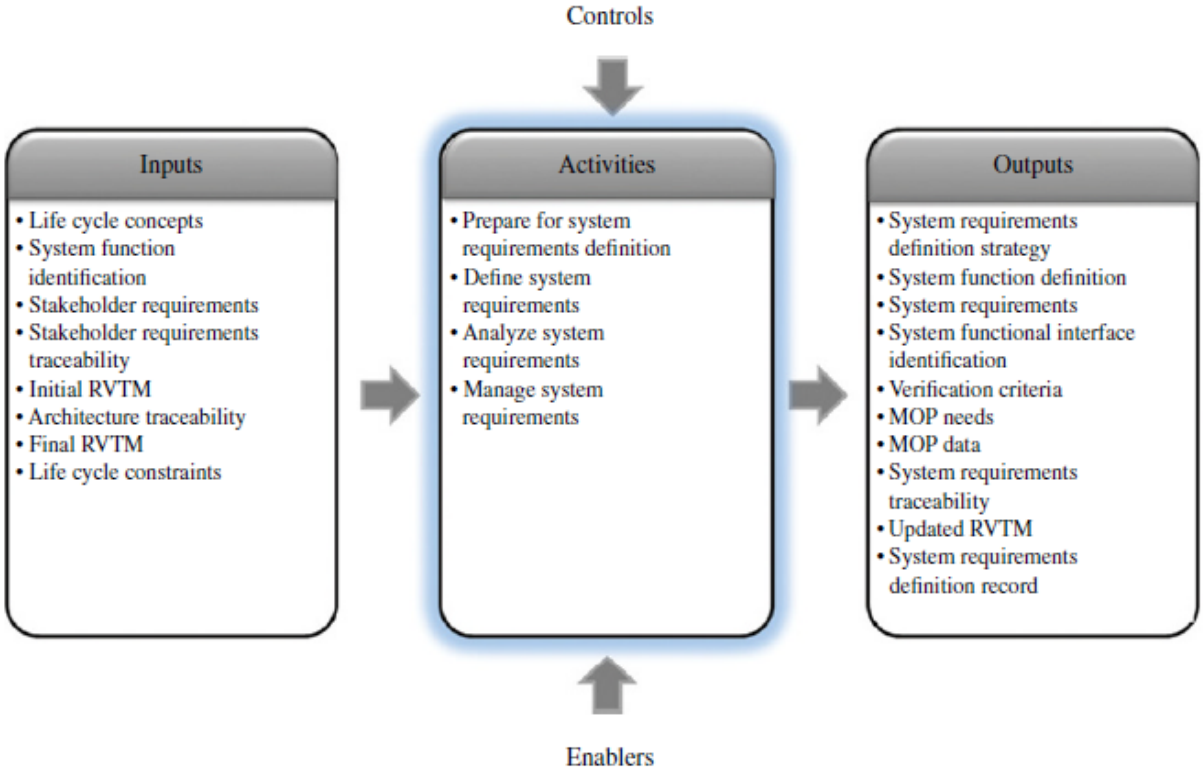


Figure 18 : System Requirements Definition Process [2]

4.4 Architecture Definition Process

FOCUS PRISSMA: The architecture of the AD system is out of scope of the PRISSMA project. The architecture under concern is the architecture of the test system: which components can be used to meet the test system requirements.

The purpose of the Architecture Definition process is to generate system architecture alternatives, to select one or more alternative(s) that frame stakeholder concerns and meet system requirements, and to express this in a set of consistent views.

Iteration of the Architecture Definition process with the Business or Mission Analysis process, System Requirements Definition process, Design Definition process, and Stakeholder Needs and Requirements Definition process is often employed so that there is a negotiated understanding of the problem to be solved and a satisfactory solution is identified. The results of the Architecture Definition process are widely used across the life cycle processes. Architecture definition may be applied at many levels of abstraction, highlighting the relevant detail that is necessary for the decisions at that level.

NOTE 1: System architecture deals with fundamental principles, concepts, properties, and characteristics and their incorporation into the system-of-interest. Architecture definition has more uses than as merely a driver (or part of) design. Refer to ISO/IEC/IEEE 42010:2011 for more information about architecture description and the uses and nature of architecture.

NOTE 2: The Architecture Definition process supports identification of stakeholders and their concerns. As the process unfolds, insights are gained into the relation between the requirements specified for the system and the emergent properties and behaviors of the system that arise from the interactions and relations between the system elements. The Design Definition process (see subclause 6.4.5), on the other hand, is driven by requirements that have been vetted through the architecture and more detailed analyses of feasibility. Architecture focuses on suitability, viability, and desirability, whereas design focuses on compatibility with technologies and other design elements and feasibility of construction and integration. An effective architecture is as design-agnostic as possible to allow for maximum flexibility inthe design trade space. An effective architecture also highlights and supports trade-offs for the Design Definition process and possibly other processes such as Portfolio Management, Project Planning, System Requirements Definition, and Verification.

NOTE 3: In product line architectures, the architecture is necessarily spanning across several designs. The architecture serves to make the product line cohesive and helps ensure compatibility and interoperability across the product line. Even for a single product system, the design of the product will likely change over time while the architecture remains constant. [1]

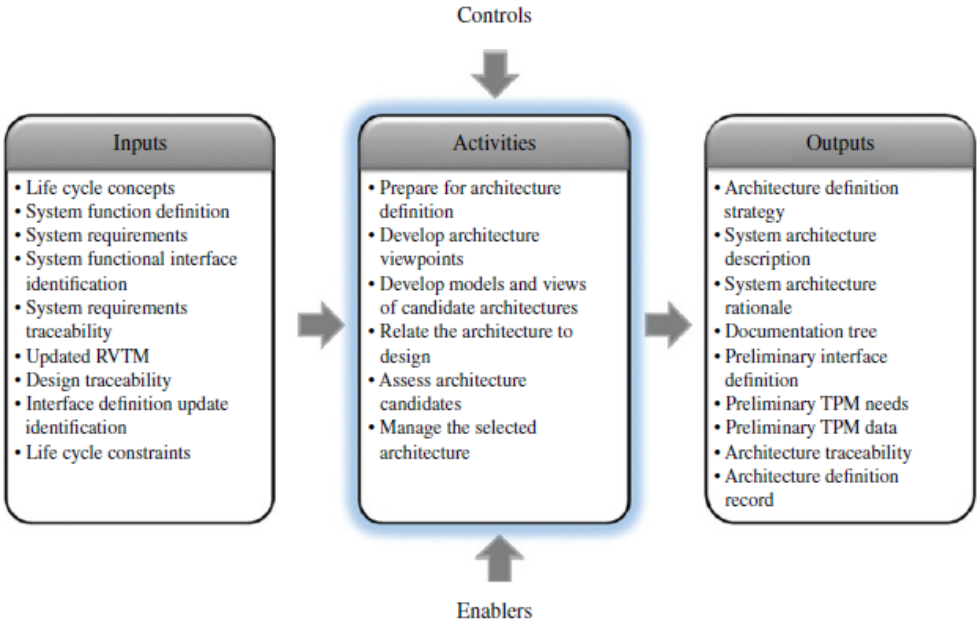


Figure 19 : Architecture Definition Process [2]

Some tools are dedicated to the architecture process. The Capella MBSE tool is an implementation of the Arcadia methodology constraining the architect to follow strict allocations rules. One key aspect of defining candidate's architectures that meet the system requirements is the proper allocation of system requirements and functions to system elements that will jointly fulfill the requirement or function of the system. The Capella MBSE tool brings a simple constraint: if a system function F needs 2 system elements for being fulfilled by the system, then this function F needs to be split in at least 2 function F' and F", each of this function being allocated exclusively and entirely to system component.

In the figure below, the function F2 defined at "Functional & Functional Need" abstraction level, is decomposed into F21 and F22 at subsequent levels.

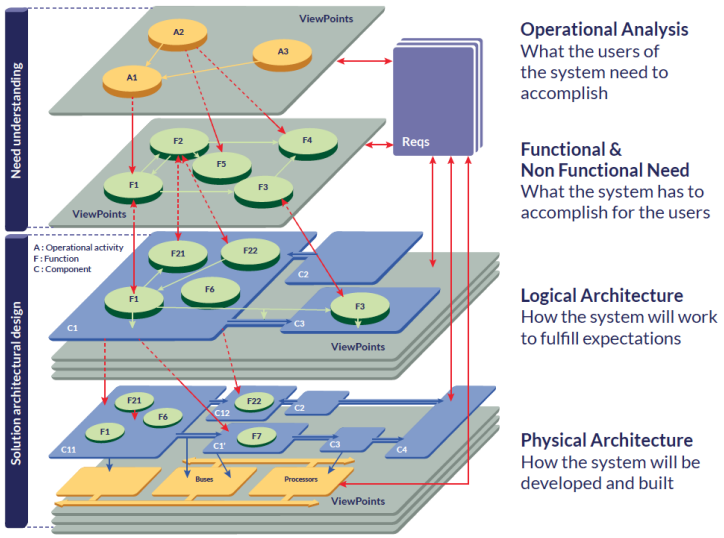


Figure 20 : Arcadia system engineering process illustrated

4.5 Design Definition Process

FOCUS PRISSMA: The complete set of requirements for the test system derived from the safety and security constraints of the system under test should have already been provided during the stakeholder needs and requirements definition process (see 4.2). Nevertheless, since the design definition brings to the architecture process additional constraints arose by the system elements, one particular components of the test system needs specific considerations in the scope of PRISSMA:

One of the main goal of the PRISSMA project is to assess the impact of using AI based component in the test system?

The purpose of the Design Definition process is to provide sufficient detailed data and information about the system and its elements to enable the implementation consistent with architectural entities as defined in models and views of the system architecture.

NOTE 1: The Architecture Definition process, supports identification of stakeholders and their concerns. Through the use of the process, insights are gained into the relation between the requirements specified for the system and the emergent properties and behaviors of the system that arise from the interactions and relations between the system elements. The Design Definition process, on the other hand, is driven by requirements that have been vetted through the architecture and more detailed analyses of feasibility. Architecture focuses on suitability, viability, and desirability, whereas design focuses on compatibility with technologies and other design elements and feasibility of construction and integration.

An effective architecture is as design-agnostic as possible to allow for maximum flexibility in the design trade space.

NOTE 2: Design definition considers any applicable technologies and their contribution to the system solution. Design provides the 'implement-to' level of the definition, such as drawings and detailed design descriptions.

NOTE 3: This process provides feedback to the system architecture to consolidate or confirm the allocation, partitioning and alignment of architectural entities to system elements that compose the system. [1]

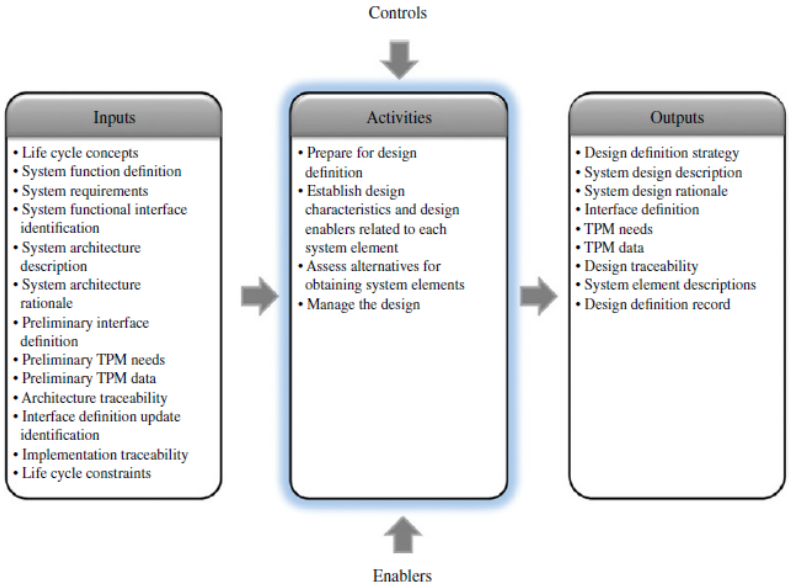


Figure 21 : Design Definition Process IPO from [2]

4.6 System Analysis Process

FOCUS PRISSMA: This process gathers all the analysis required by the other processes. Always present in a system engineering project, there is nothing special for the PRISSMA project, unless to state that any required analysis shall be conducted to meet the project's mission's goals.

4.7 Implementation Process

FOCUS PRISSMA: This process is out of scope of PRISSMA.

4.8 Integration Process

FOCUS PRISSMA: The integration of a given set of elements of a system needs some particular tests to be taken to assess the capabilities of this set regarding system's requirements. Depending on the system of interest, the scope of the tests to be taken should be analyzed properly:

* AD vehicle: the SOI is one vehicle. The integration of some components, including AI components, is a state-of-the art activity in system engineering: the context of these components are simulated. As mentioned in §5.5, the configuration management of the set of these system's element AND its test system should be done carefully.

* AD system of system: one AD system is a part of the AD system of systems. Even if this AD system comprising the AD vehicle fleet and possible remote supervision has been validated, the operation of the first vehicles in the Road is an integration for the AD system of system. The transition from validation to operation of a given AD system should be ruled and audited by authoritative organizations.

The purpose of the Integration process is to synthesize a set of system elements into a realized system (product or service) that satisfies system requirements, architecture, and design.

This process assembles the implemented system elements. Interfaces are identified and activated to enable interoperation of the system elements as intended. This process integrates the enabling systems with the system-of-interest to facilitate interoperation.

NOTE 1: For a given level of the system hierarchy, this process iteratively combines implemented system elements to form complete or partial system configurations in order to build a product or service. It is used recursively for successive levels of the system hierarchy.

NOTE 2: The interfaces are defined by the Architecture Definition and Design Definition processes. This process coordinates with these other processes and checks to make sure the interface definitions are adequate and that they take into account the integration needs. [1]

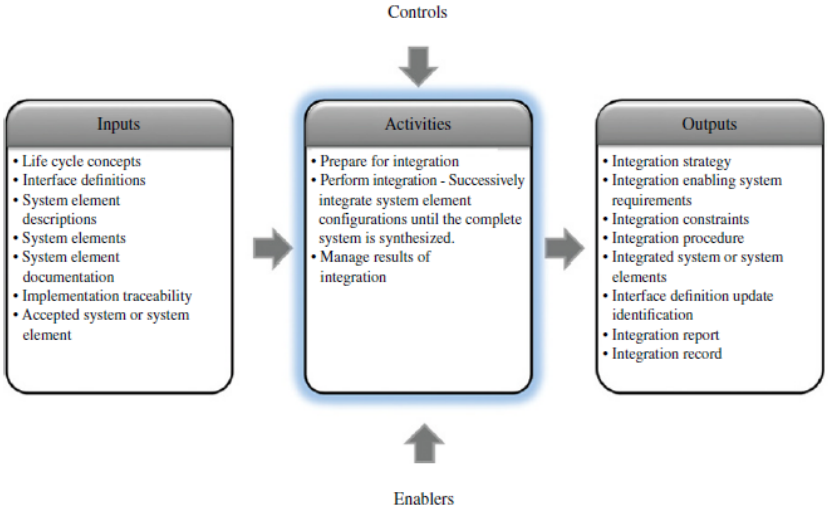


Figure 22 : Integration Process IPO from [2]

4.9 Verification Process

As mentioned in §2.5.2, the verification principle should have a subject. This process targets all the subject under verification (requirements, need, design or system).

The purpose of the Verification process is to provide objective evidence that a system or system element fulfils its specified requirements and characteristics.

The Verification process identifies the anomalies (errors, defects, or faults) in any information item (e.g., system requirements or architecture description), implemented system elements, or life cycle processes using appropriate methods, techniques, standards or rules. This process provides the necessary information to determine resolution of identified anomalies.

NOTE: The Verification process determines that the "product is built right". The Validation process determines that the "right product is built". [1]

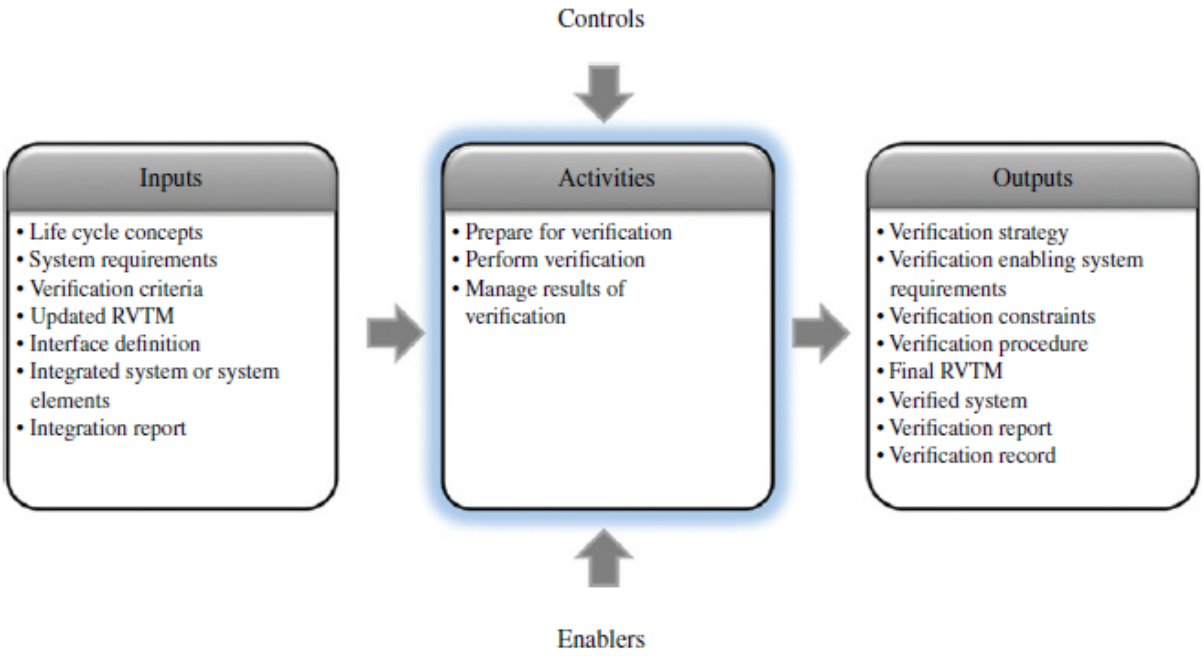


Figure 23 : Verification Process IPO from [2]

FOCUS PRISSMA: The PRISSMA project focus on some particular verification activities: the tests that can be taken on an AD system (simulation test, closed road or open road tests).

Since the verification scope is to verify a system against its requirements, and not the stakeholder's needs it fulfills, the quality of the requirements will have a particularly strong impact on the seamless transition of the verification success to the validation success: if the system has good requirements, then a successful verification will enable a successful validation. But if the system requirements definition process has flaw, then the delivered system fulfilling its requirements will probably won't fill the stakeholders' needs.

4.10 Transition Process

FOCUS PRISSMA: As stated in §4.8, the transition of some systems during their lifecycle can arise some particular troubles. For an AD system, its transition from validation (maybe in closed road) to operation (possibly in open road) should be planned, along with the transition for the enabling systems that will guarantee its security.

These questions are typically core questions of the PRISSMA project.

The purpose of the Transition process is to establish a capability for a system to provide services specified by stakeholder requirements in the operational environment.

This process moves the system in an orderly, planned manner into the operational status, such that the system is functional, operable and compatible with other operational systems. It installs a verified system, together with relevant enabling systems, e.g., planning system, support system, operator training system, user training system, as defined in agreements. This process is used at each level in the system structure and in each stage to complete the criteria established for exiting the stage. It includes preparing applicable storage, handling, and shipping enabling systems.

NOTE: In the case of system upgrades, the transition activities need to be accomplished with minimal disruption to ongoing operations. [1]

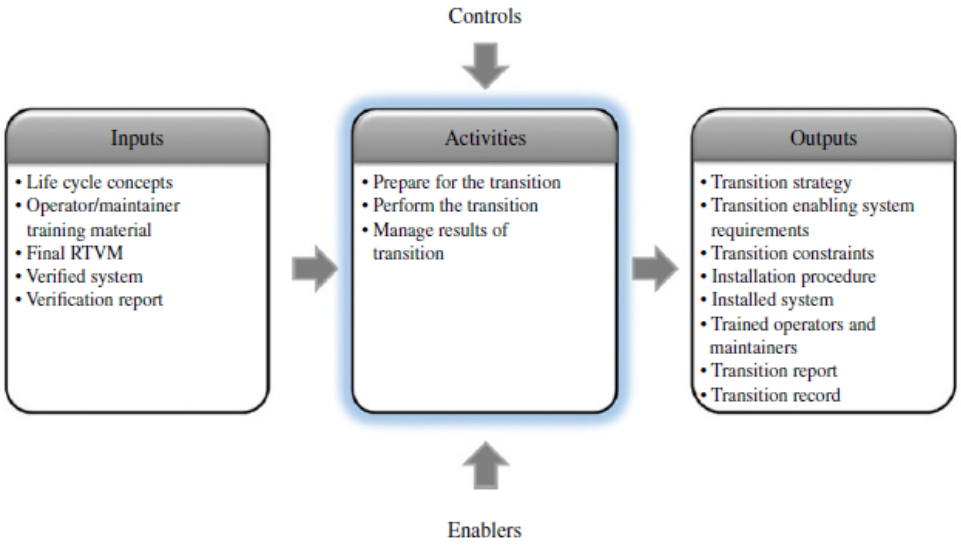


Figure 24 : Transition Process IPO from [2]

4.11 Validation Process

FOCUS PRISSMA: This process is key for the PRISSMA project. The good definition of stakeholder needs and requirements is a key factor of success in traditional engineering projects, and will also be the case with AI AD system: what environment is enough for validation, what are all the stakeholders involved for a particular AD system are typical questions relative to validation that should be addressed.

Indeed, the question of the environment for the evaluation of an AI system is essential.

For example, validating an AI system according to a protocol proposed by the manufacturer in the ODD defined for the system could be a first step.

In a second step, we would push the system to its limits with RODs (Restricted Operational Domain) in "edge cases" to test the limits of the AI system. The use of the OEDR (Object and Event Detection and Response) will also foster specific activities for the validation of the ADS.

The purpose of the Validation process is to provide objective evidence that the system, when in use, fulfills its business or mission objectives and stakeholder requirements, achieving its intended use in its intended operational environment.

The objective of validating a system or system element is to acquire confidence in its ability to achieve its intended mission, or use, under specific operational conditions. Validation is ratified by stakeholders. This process provides the necessary information so that identified anomalies can be resolved by the appropriate technical process where the anomaly was created.

NOTE 1: The validation process determines that the "right product is built". The verification process determines that the "product is built right".

NOTE 2: Validation is also applicable to the engineering artifacts (viewed as system elements) produced in the definition and realization of the system. [1]

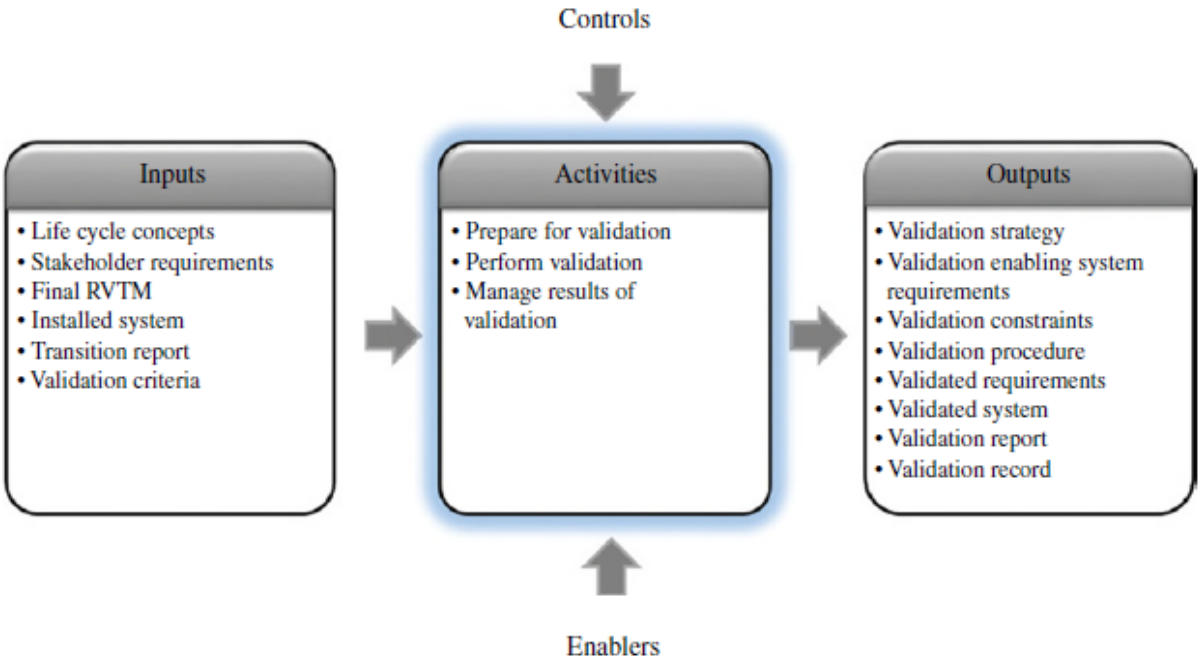


Figure 25 : Validation Process IPO from [2]

4.12 Operation Process

Although the operation process is part of the IEC 15288 standard, it is addressed in deeper viewpoint by the Integrated Logistic Support detailed in the section 8.

The purpose of the Operation process is to use the system to deliver its services. This process establishes requirements for and assigns personnel to operate the system, and monitors the services and operator-system performance. In order to sustain services it identifies and analyzes operational anomalies in relation to agreements, stakeholder requirements and organizational constraints.

NOTE ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013), provides requirements for establishing a service management system, which supports the Operation process to achieve its purpose.[1]

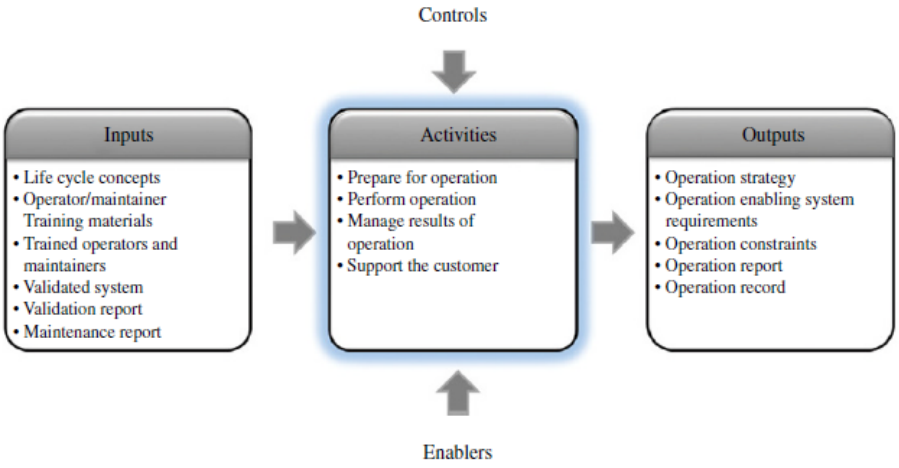


Figure 26 : Operation Process IPO from [2]

4.13 Maintenance Process

Although the maintenance process is part of the IEC 15288 standard, it is addressed in deeper viewpoint by the Integrated Logistic Support detailed in the section 8.

4.14 Disposal Process

FOCUS PRISSMA: This process is out of scope of PRISSMA.

5 Technical Management process

The Technical Management Processes are used to establish and evolve plans, to execute the plans, to assess actual achievement and progress against the plans and to control execution through to fulfillment. Individual Technical Management Processes may be invoked at any time in the life cycle and at any level in a hierarchy of projects, as required by plans or unforeseen events. The Technical Management Processes are applied with a level of rigor and formality that depends on the risk and complexity of the project.

The scope of a technical management process is the technical management of a project or its products, to include the system.

NOTE: This set of technical management processes are performed so that system-specific technical processes can be conducted effectively. They do not comprise a management system or a comprehensive set of processes for project management, as that is not the scope of this standard.

5.1 Project planning process

FOCUS PRISSMA: This process is out of scope of PRISSMA.

5.2 Project assessment and control process

FOCUS PRISSMA: This process is out of scope of PRISSMA.

5.3 Decision management process

FOCUS PRISSMA: In such new technological field as IA based AD system, any decision regarding the development and maintenance of the AD system should be aggregated correctly for feedback and problem solving as stated by IA Act.

The purpose of the Decision Management process is to provide a structured, analytical framework for objectively identifying, characterizing and evaluating a set of alternatives for a decision at any point in the life cycle and select the most beneficial course of action.

NOTE 1: This process is used to resolve technical or project issues and respond to requests for decisions encountered during the system life cycle, in order to identify the alternative(s) that provides the preferred outcomes for the situation. The methods most frequently used for Decision Management are the trade study and engineering analysis. Each of the alternatives is assessed against the decision criteria (e.g., cost impact, schedule impact, programmatic constraints, regulatory implications, technical performance characteristics, critical quality characteristics, and risk). Results of these comparisons are ranked, via a suitable selection model, and are then used to decide on an optimal solution. Key study data, (e.g., assumptions and decision rationale) are typically maintained to inform decision-makers, and support future decision-making.

NOTE 2: When it is necessary to perform a detailed assessment of a parameter for one of the criteria, the System Analysis process is employed to perform the assessment. [1]

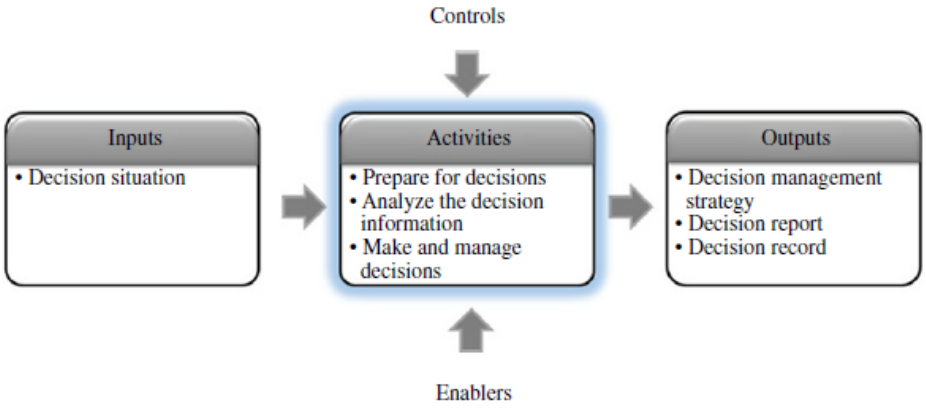


Figure 27 : Decision management process IPO from [2]

FOCUS PRISSMA: This activity is generally not considered enough in a result-oriented implementation of this system engineering process, where the delivery of acknowledged work products matter more than rationale of past decisions.

In this new field of IA, tracking the alternatives and decisions in all the organizations involved in the ADS providing system will be a key for improvement in case of undesired behavior of the ADS system.

5.4 Risk management process

FOCUS PRISSMA: The risk management process is at the core of safety and security and is emphasized in many working groups and projects about AI based systems.

The purpose of the Risk Management process is to identify, analyze, treat and monitor the risks continually. The Risk Management process is a continual process for systematically addressing risk throughout the life cycle of a system product or service. It can be applied to risks related to the acquisition, development, maintenance or operation of a system.

NOTE Risk is defined in ISO Guide 73:2009 as "The effect of uncertainty on objectives". This has an attached NOTE 1, "An effect is a deviation from the expected — positive and/or negative." A positive risk is sometimes commonly known as an opportunity, and addressed within the risk management process.

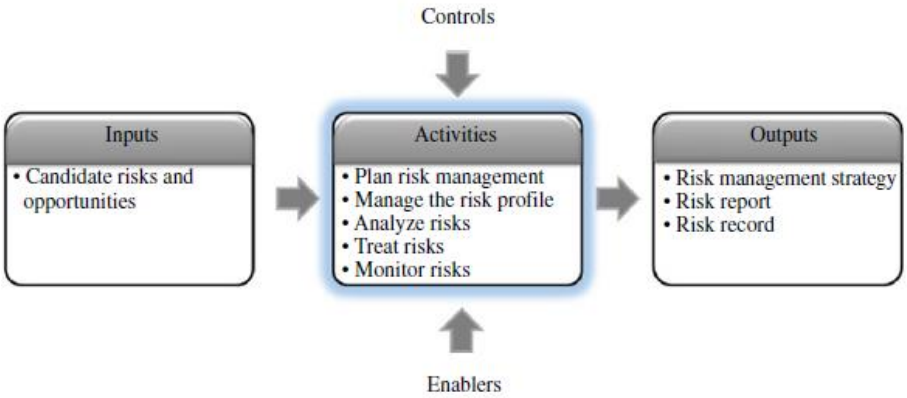


Figure 28 : Risk management process IPO from [2]

5.5 Configuration management process

The purpose of Configuration Management (CM) is to manage and control system elements and configurations over the life cycle. CM also manages consistency between a product and its associated configuration definition. [1]

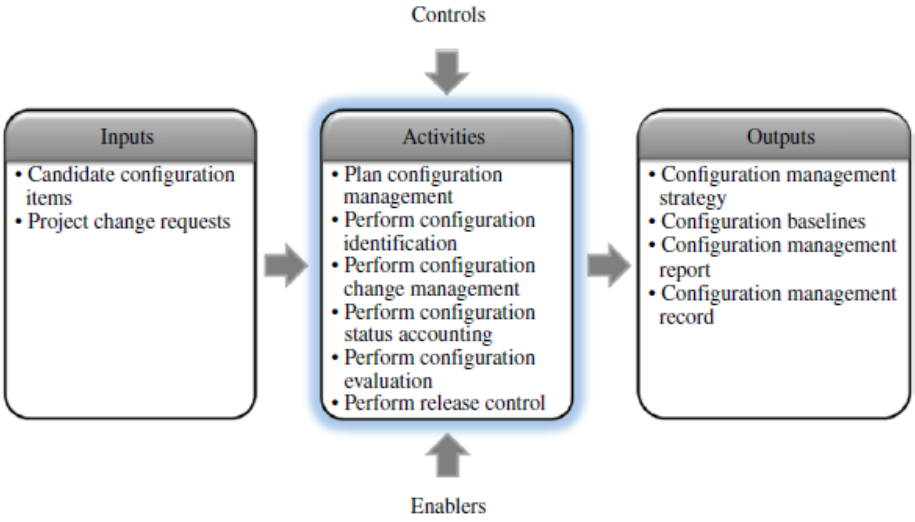


Figure 29 : Configuration management process IPO from [2]

So based on IEC 15288[1] the configuration has two main goals:

1. Manage and control system elements and configurations over the lifecycle: this goal deals with the products themselves
2. Manage consistency between a product and its associated configuration definition: this goal focus on the information about a product, and the consistency between the product and these information.

The [EIA-649C] standardize the activities to establish, perform, evaluate or improve Configuration Management (CM) processes.

When appropriately and effectively applied, CM provides a positive impact on every aspect of the product life cycle. CM is a comprehensive process for establishing and maintaining consistency of any product's performance, functional and physical attributes with its requirements, design, and operational information.

Even if configuration management of automotive or dependable systems in general is extremely well managed, given their ROI when system's data are analyzed after crashes, this configuration management tends to be less and less important along the chain of enabling systems (the SOI depends on enabling systems, which depend on their enabling systems, and so on). A successful program, may rely for its maintenance, on a software running on a 20 years PC, which sources are only kept on a developer's backup SSD next to his last holidays photo. Since certification activities only covers the safety of the SOI and quality insurance of the SOI's development process, this kind of flaw cannot be detected.

All the information of a given product is defined by the product configuration information:

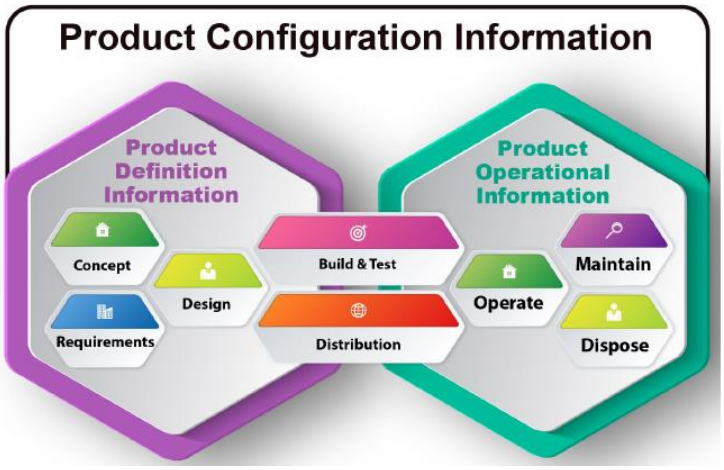


Figure 30 : Product Configuration Information

The configuration management relies on the 6 activities described in both the IEC 15288[1] and the [EIA-649C]:

1. Plan configuration management
2. Perform configuration identification
3. Perform configuration change management
4. Perform configuration status accounting
5. Perform configuration evaluation
6. Perform release control

The configuration management relies on the concept of configuration item which is uniquely identified for being managed:

The identification of the configuration of each configuration item of a system along its lifecycle is scoped by the baseline concept:

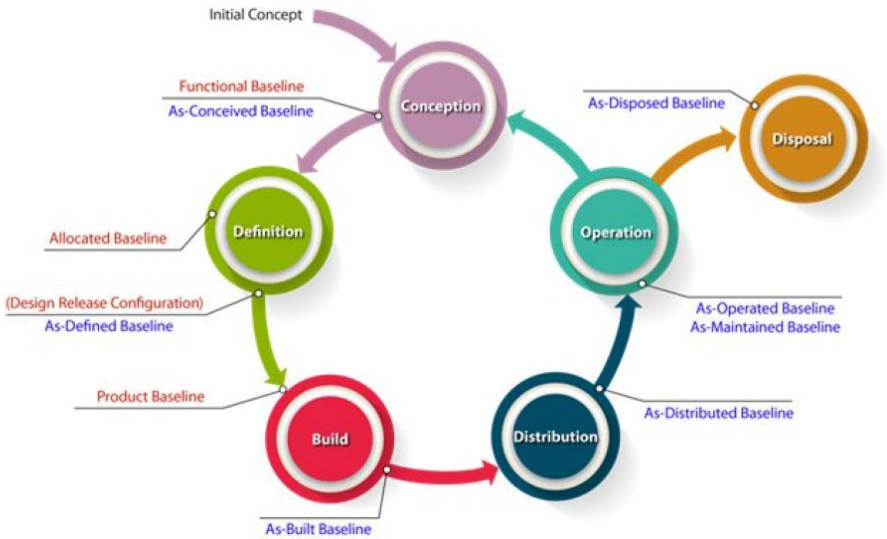


Figure 31 : Configuration baseline along the system lifecycle

FOCUS PRISSMA: Attention should be paid to the configuration management of the configuration management process should be carefully applied to the enabling systems and components:

* Identifying the baselines of system of system elements: the AD System along with its test system should be identified jointly when taking tests. A rule of thumb is to enforce standards at 3 levels:

1 - The system of interest (the ADS System)

2 - The direct enabling systems of the SOI (test systems, maintenance systems)

3 - The enabling systems of the direct enabling systems

* Simulation models and verification activities: asserting the validity of the results of a particular verification campaign made on a particular set of simulation models interaction. What is the validity of test campaign conduced on the AD vehicle's model in version x, interacting with environmental model version y and mission's model version z? When one configuration of one of these models is updated, what can be stated about the results of previous test campaign?

* The current state of the art regarding IA configuration management in ADS is to forbid the learning of the IA after being deployed. Currently, the idea of a fleet of vehicles with different levels of AI software is not considered and learning should be done in a disembarked way to ensure an equivalent level of performance and expectations in the whole fleet of the manufacturer for a given ODD.

5.6 Information management process

FOCUS PRISSMA: As mentioned in §2.5.2, human and IA based systems can be viewed as agents interacting with their environment. The use of ontologies has been widely used to gather concepts and definitions into reasonable structures both for human and computer.

In addition, some information regarding the security of operating AD systems should be transmitted by a given AD systems operator to disseminate potential knowledge across the different stakeholders of the AD systems, including the organizations developing and maintaining those AD systems.

The purpose of the Information Management process is to generate, obtain, confirm, transform, retain, retrieve, disseminate and dispose of information, to designated stakeholders.

Information management plans, executes, and controls the provision of information to designated stakeholders that is unambiguous, complete, verifiable, consistent, modifiable, traceable, and presentable. Information includes technical, project, organizational, agreement, and user information. Information is often derived from data records of the organization, system, process, or project. [1]

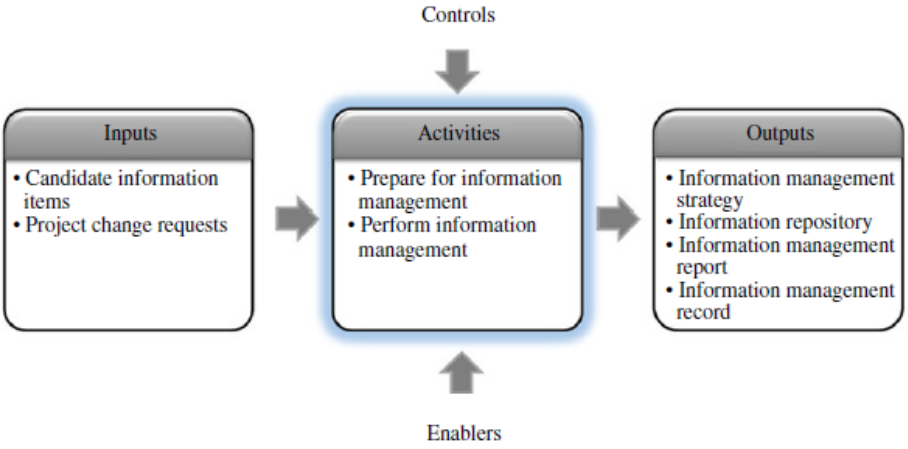


Figure 32 : Information management process IPO from [2]

5.7 Measurement process

FOCUS PRISSMA: The assertion of the security of AI based AS system will probably involve some KPI evaluating the quality of the tests taken on AD systems. Should the statement of these KPI be part of the PRISSMA project?

The choice of KPIs must be consistent with the ODD or ROD chosen for the test. In the case where the test procedure is proposed by the AI system manufacturer, an evaluation of the protocol and the chosen metrics will be essential.

The purpose of the Measurement process is to collect, analyze, and report objective data and information to support effective management and demonstrate the quality of the products, services, and processes.

NOTE 1: ISO/IEC 15939 (IEEE Std 15939-2007) provides a more detailed set of measurement activities and tasks that are aligned with the activities and tasks shown below.

NOTE 2: Clause 8 of ISO 9001:2008 specifies Quality Management System requirements for measurement and monitoring of processes and products.

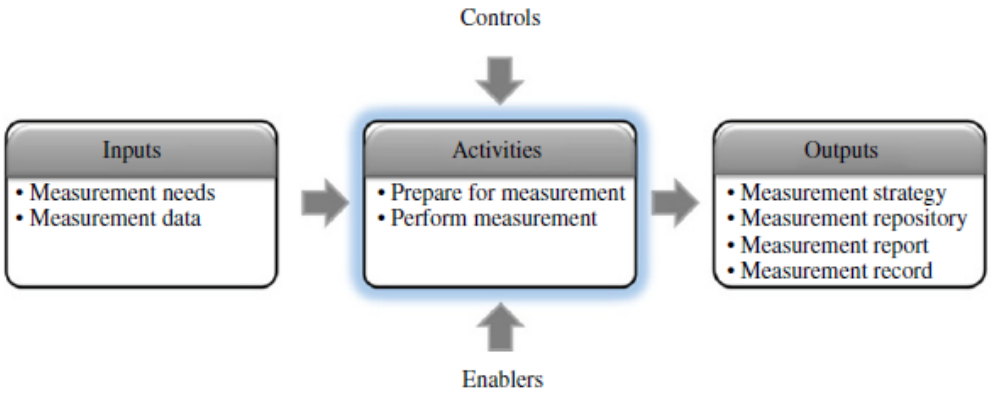


Figure 33 : Measurement process IPO from [2]

5.8 Quality assurance process

The purpose of the Quality Assurance process is to help ensure the effective application of the organization's Quality Management process to the project.

Quality Assurance focuses on providing confidence that quality requirements will be fulfilled. Proactive analysis of the project life cycle processes and outputs is performed to assure that the product being produced will be of the desired quality and that organization and project policies and procedures are followed.

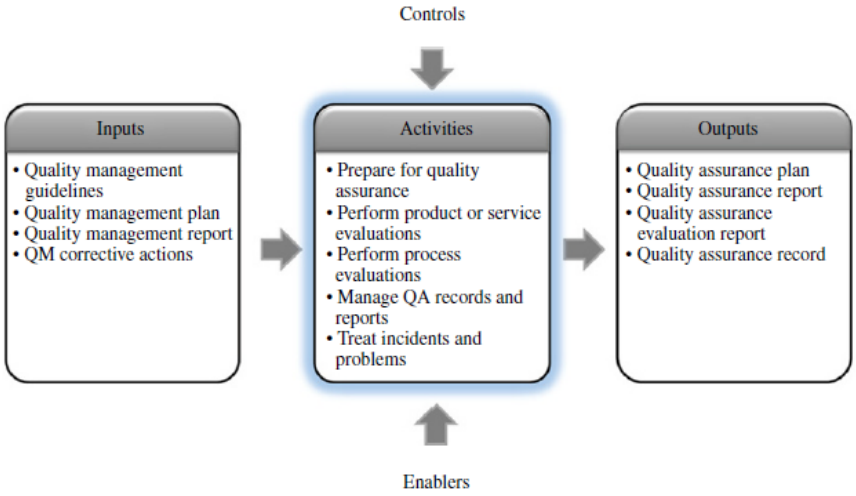


Figure 34 : Quality assurance process IPO from [2]

FOCUS PRISSMA: The quality assurance process is key to the success of AD systems. Can it be addressed inside the PRISSM project, or will it be a continuation.

6 Organizational Project-Enabling Process

The Organizational Project-Enabling Processes help ensure the organization's capability to acquire and supply products or services through the initiation, support and control of projects. These processes provide resources and infrastructure necessary to support projects and help ensure the satisfaction of organizational objectives and established agreements. They are not intended to be a comprehensive set of business processes that enable strategic management of the organization's business.[1]

6.1 Life cycle model management process

The purpose of the Life Cycle Model Management process is to define, maintain, and assure availability of policies, life cycle processes, life cycle models, and procedures for use by the organization with respect to the scope of this International Standard.

This process provides life cycle policies, processes, models, and procedures that are consistent with the organization's objectives, that are defined, adapted, improved and maintained to support individual project needs within the context of the organization, and that are capable of being applied using effective, proven methods and tools. [1]

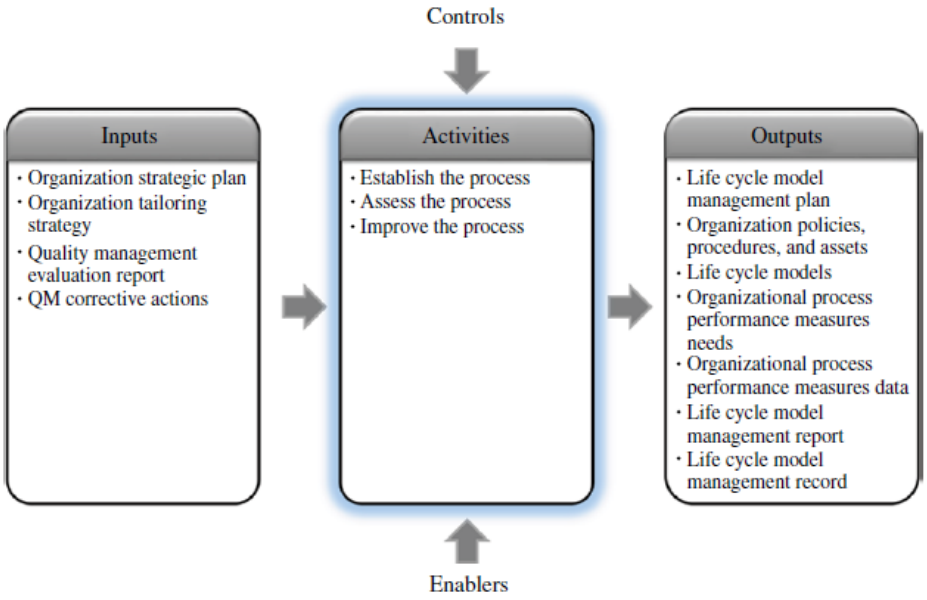


Figure 35 : Life cycle management process IPO from [2]

FOCUS PRISSMA: Do AI add specific life cycle stages to the systems?

6.2 Infrastructure management process

The purpose of the Infrastructure Management process is to provide the infrastructure and services to projects to support organization and project objectives throughout the life cycle.

This process defines, provides and maintains the facilities, tools, and communications and information technology assets needed for the organization's business with respect to the scope of this International Standard. [1]

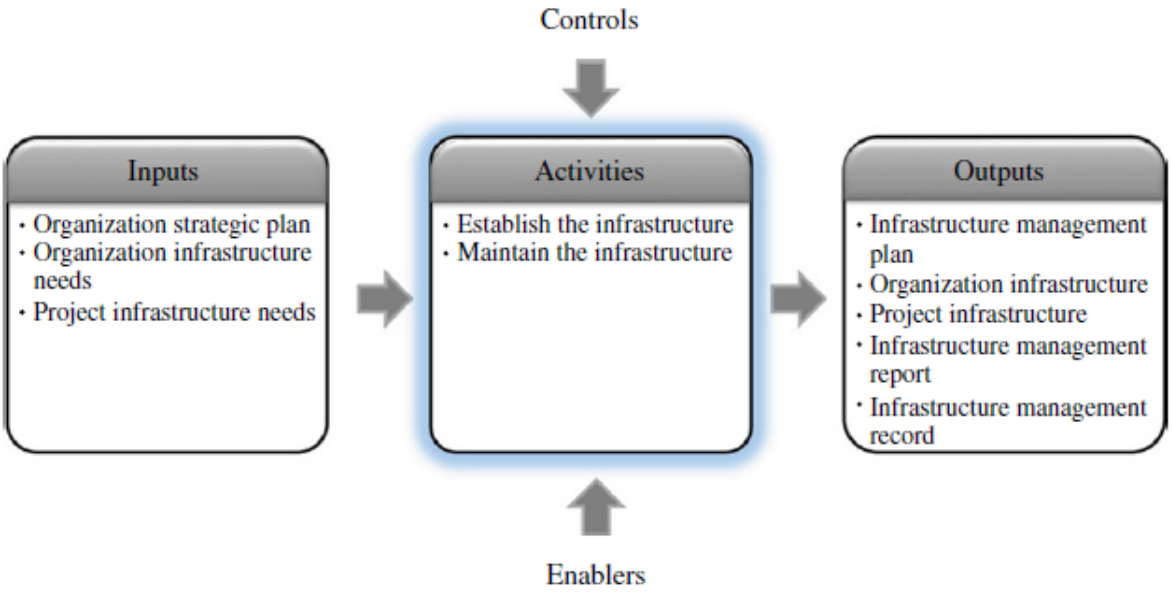


Figure 36 : Infrastructure management process IPO from [2]

6.3 Portfolio management process

The purpose of the Portfolio Management process is to initiate and sustain necessary, sufficient and suitable projects in order to meet the strategic objectives of the organization.

This process commits the investment of adequate organization funding and resources, and sanctions the authorities needed to establish selected projects. It performs continued assessment of projects to confirm they justify, or can be redirected to justify, continued investment. [1]

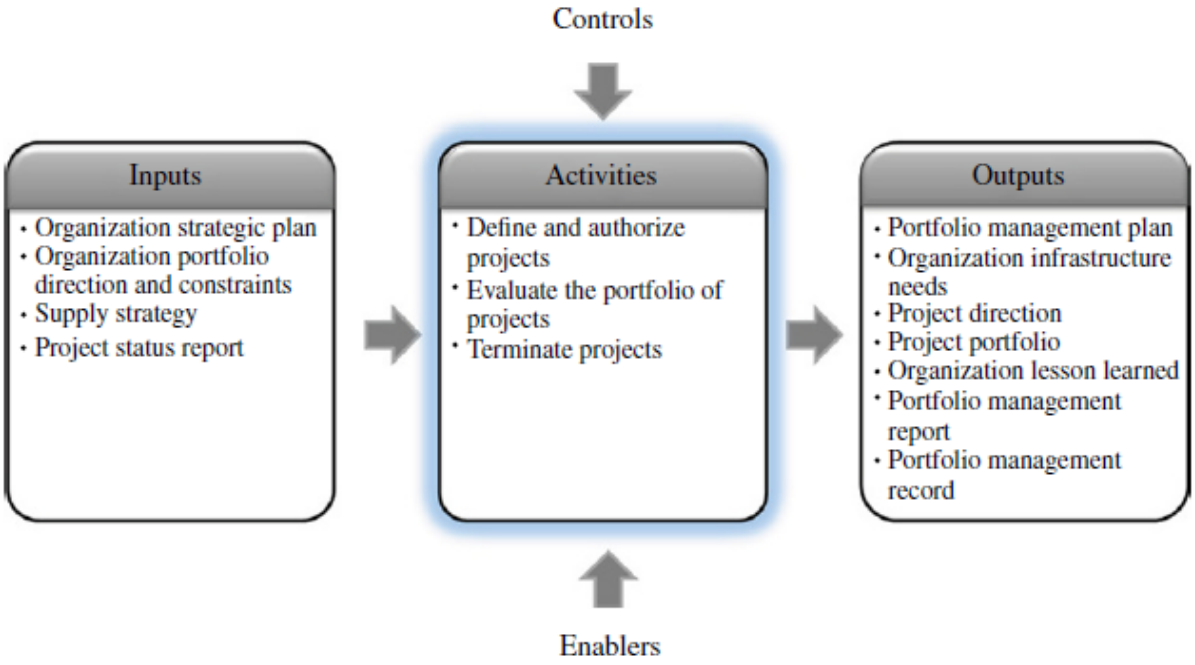


Figure 37 : Portfolio management process IPO from [2]

6.4 Human resource management process

The purpose of the Human Resource Management process is to provide the organization with necessary human resources and to maintain their competencies, consistent with business needs.

This process provides a supply of skilled and experienced personnel qualified to perform life cycle processes to achieve organization, project, and stakeholder objectives. [1]

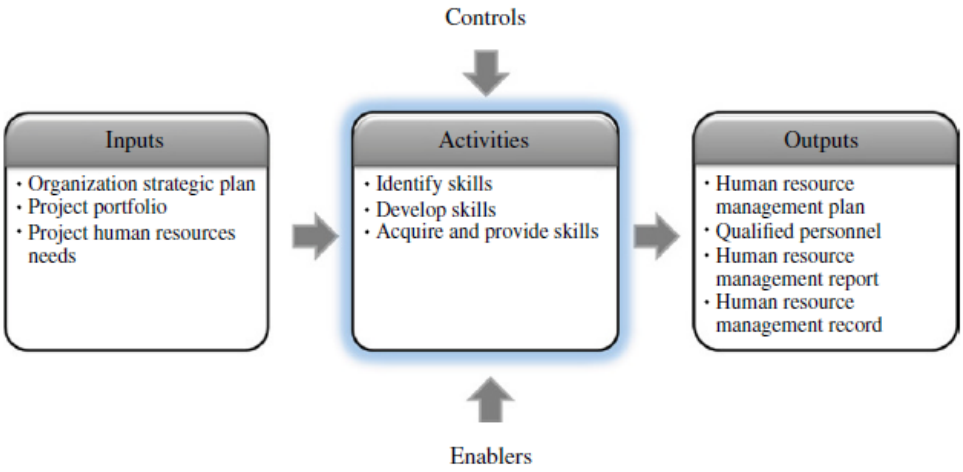


Figure 38 : Human resource management process IPO from [2]

6.5 Quality management process

The purpose of the Quality Management process is to assure that products, services and implementations of the quality management process meet organizational and project quality objectives and achieve customer satisfaction.

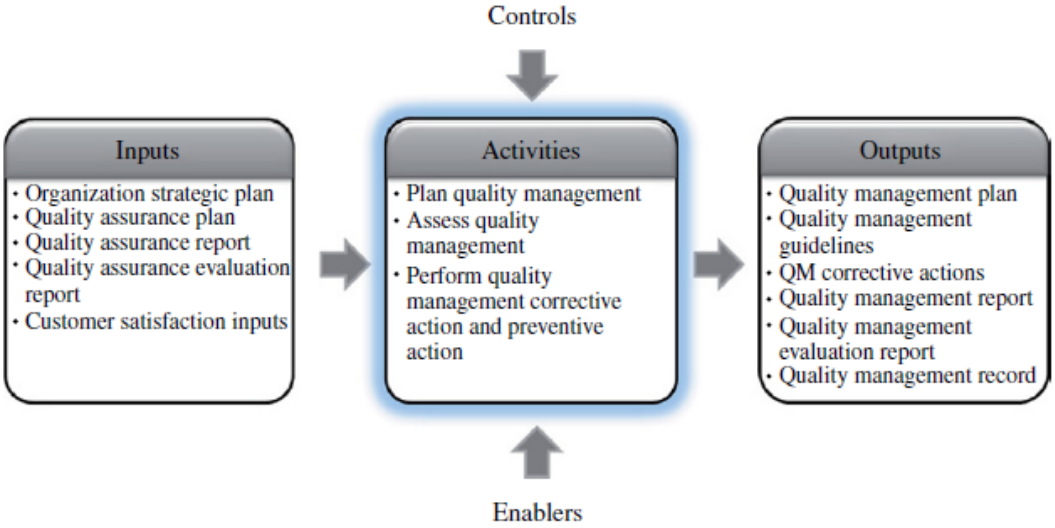


Figure 39 : Quality management process IPO from [2]

6.6 Knowledge management process

The purpose of the Knowledge Management process is to create the capability and assets that enable the organization to exploit opportunities to re-apply existing knowledge.

This encompasses knowledge, skills, and knowledge assets, including system elements. [1]

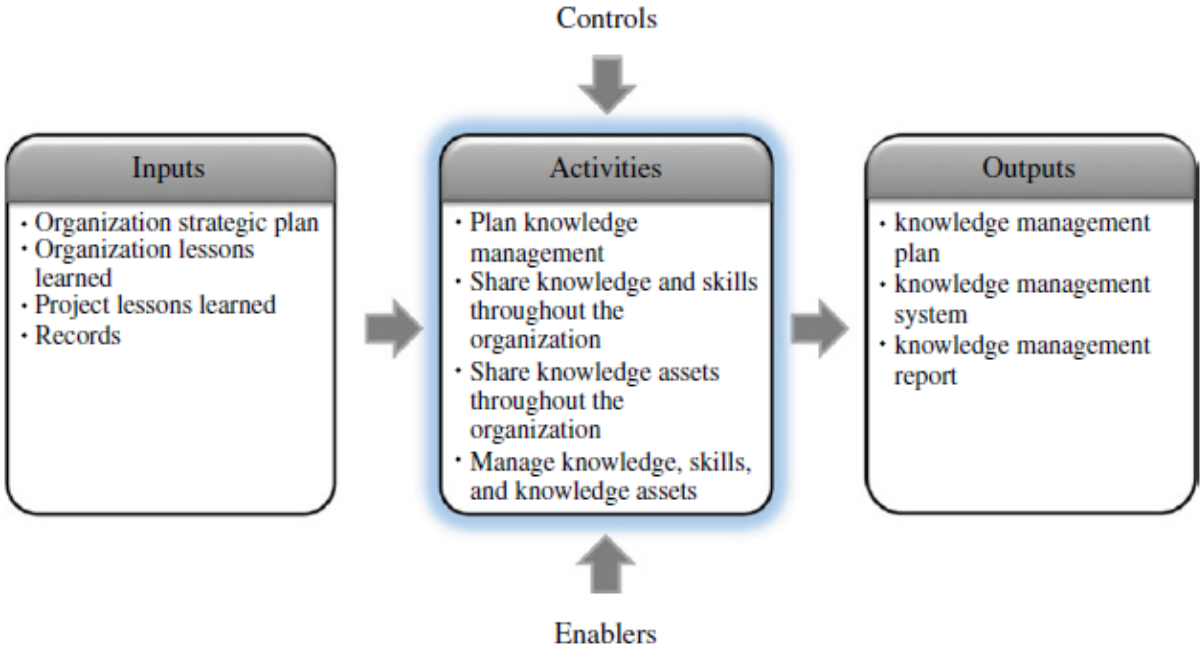


Figure 40 : Knowledge management process IPO from [2]

7 Agreement process

These processes [Acquisition process, Supply process] define the activities necessary to establish an agreement between two organizations. If the Acquisition process is invoked, it provides the means for conducting business with a supplier. This may include products that are supplied for use as an operational system, services in support of operational activities, or elements of a system being provided by a supplier. If the Supply process is invoked, it provides the means for an agreement in which the result is a product or service that is provided to the acquirer.

NOTE: Security is an increasing concern in systems engineering. See ISO/IEC 27036, Security techniques — Information security for supplier relationships, for requirements and guidance for suppliers and acquirers on how to secure information in supplier relationships. Specific aspects of information security supplier relationships are addressed in Parts 3 and Part 4. [1]

FOCUS PRISSMA: as noted in the introduction note of this process, asserting the security for the supply chain is key in the security of the system as a whole. The establishment and monitoring of the agreement with the supplier shall include the security, including cyber security, of the whole **AD system** and its associated **ADS supplying system**.

7.1 Acquisition process

The purpose of the Acquisition process is to obtain a product or service in accordance with the acquirer's requirements.

NOTE: As part of this process, the agreement is modified when a change request is agreed to by both the acquirer and supplier [1]

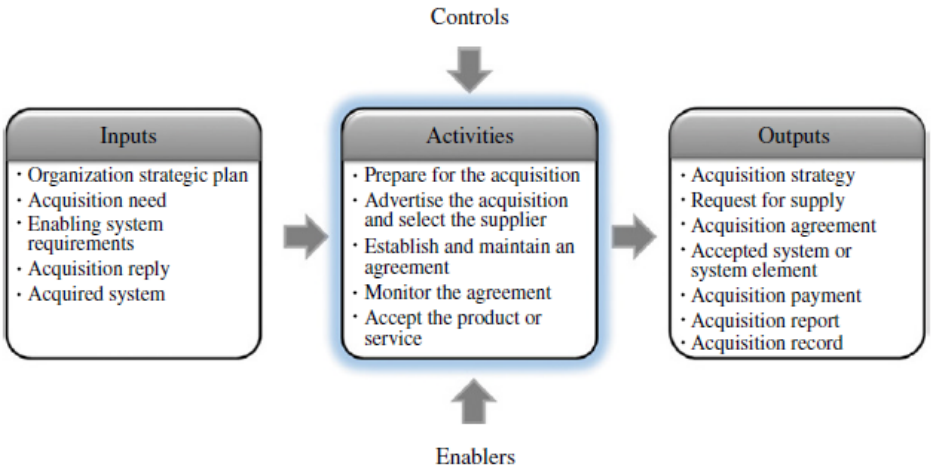


Figure 41 : Acquisition process IPO from [2]

7.2 Supply process

The purpose of the Supply process is to provide an acquirer with a product or service that meets agreed requirements.

NOTE As part of this process, the agreement is modified when a change request is agreed to by both the acquirer and supplier [1]

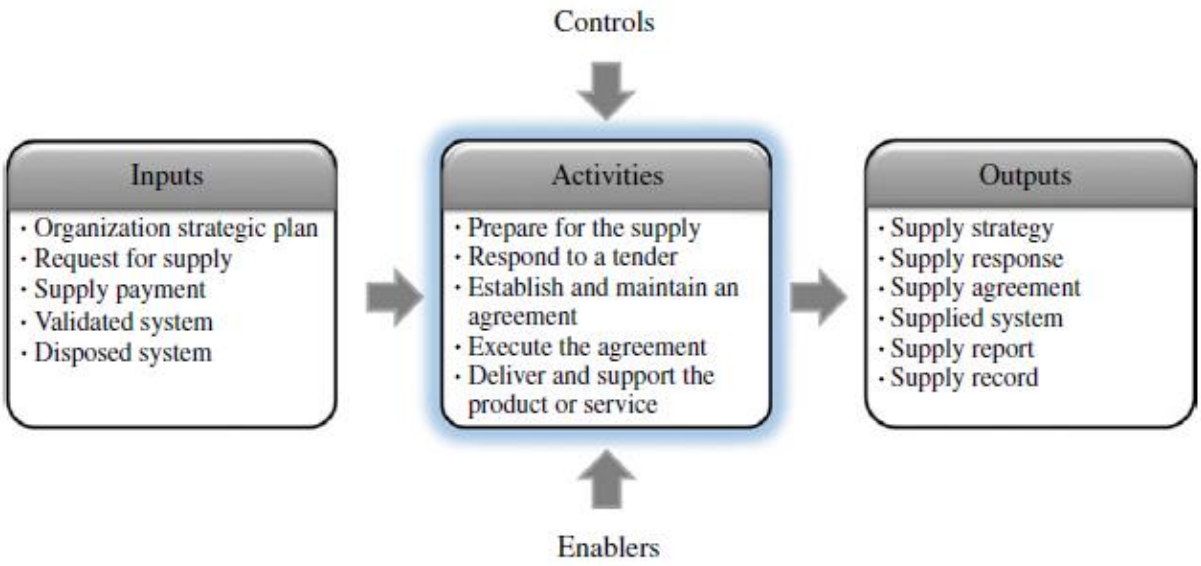


Figure 42 : Supply process IPO from [2]

8 Integrated Logistic Support

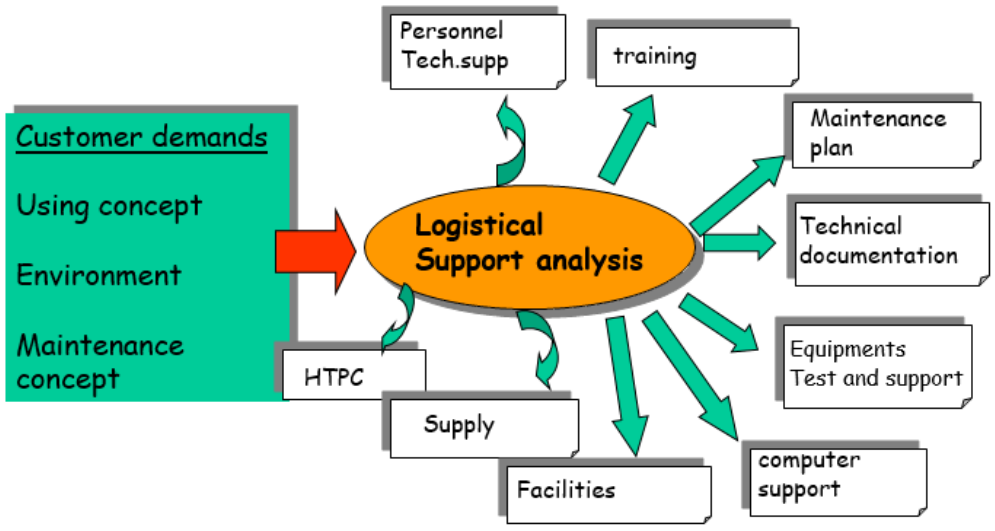
8.1 Foreword

This development handles with Logistic Support Analysis and Optimization, as integrated with System Engineering framework to which it is associated: it is widely inspired from MIL-STD-1388-1A issue which explains how to optimize the different logistic elements to reach best system performances, generally measured in terms of operational availability, in the minimum Life Cycle Cost. Then other standards are presented which have helped to propagate this engineering concept throughout the whole industrial community.

8.1.1 LSA process in System Engineering

Logistic Support Analysis process is an approach to consider as a real product the support system associated to a main system and which includes all logistics physical elements and strategies to help main system maintain its performance and operational availability during its whole life cycle.

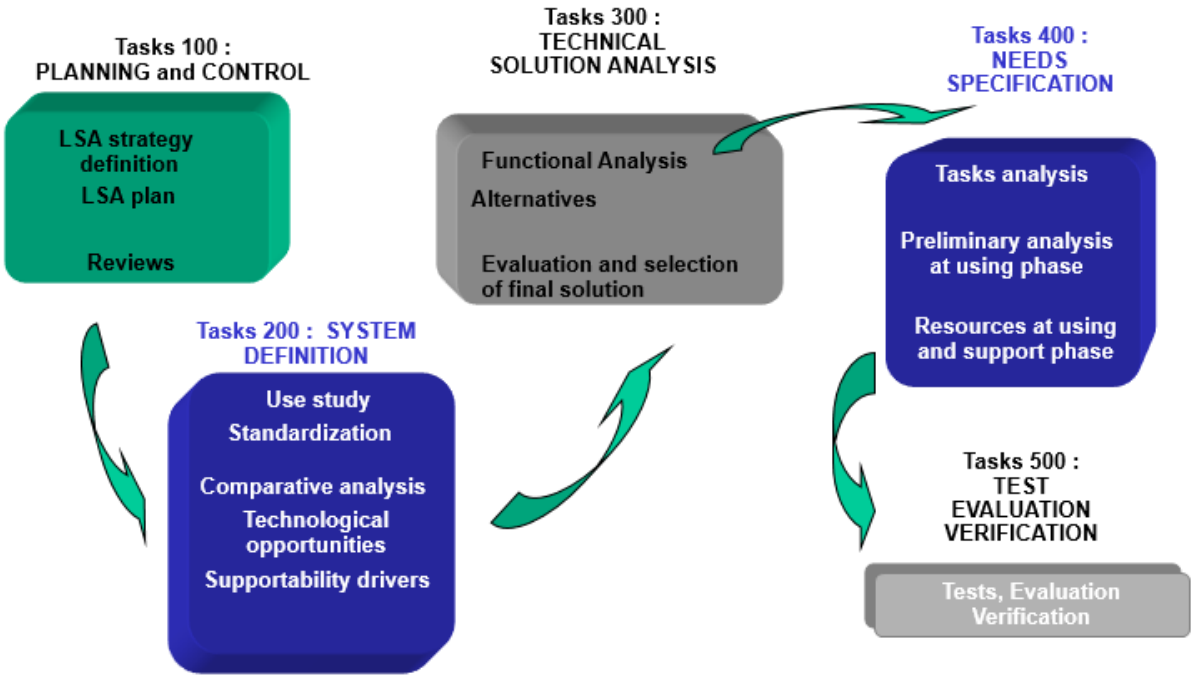
For this purpose, a systematic and comprehensive analysis has to be conducted on an iterative basis through all phases of the system/equipment life cycle to satisfy supportability (supportability includes all elements of ILS required to operate and maintain the system/equipment) objectives. The level of detail of the analyses and the timing of task performance shall be tailored to each system/equipment and shall be responsive to program schedules and milestones. Figure 1 depicts the major LSA process objectives by program phase.



8.1.2 Project interface

Maximum use has to be made of analysis and data resulting from requirements of other system engineering programs to satisfy LSA input requirements. Tasks and data required by this standard, which are also required by other standards and specifications, shall be coordinated and combined to the maximum extent possible. LSA data shall be based upon, and traceable to, other system engineering data and activities where applicable. Design and performance information shall be captured, disseminated, and formally controlled from the beginning of the design effort to serve as the design audit trail for logistic support resource planning, design tradeoff study inputs, and LSA documentation preparation.

8.1.3 LSA tasks



The LSA tasks are divided into five general sections:
- Section 100, Program Planning and Control;
- Section 200, Mission and Support Systems Definition;
- Section 300, Preparation and Evaluation of Alternatives;
- Section 400, Determination of Logistic Support Resource Requirements;
- Section 500, Supportability Assessment.

Table I identifies the general purpose of each section, the individual tasks contained in each section, and the general purpose of each task and subtask.

Each individual task is divided into four parts:
- purpose,
- task description,
- task input,
- task output.

The purpose provides the general reason for performing the task. The task description provides the detailed subtasks which comprise the overall task. It is not intended that all tasks and/or subtasks be accomplished in the sequence presented. The sequence of task and subtask accomplishments should be tailored to the individual acquisition program. Where applicable, the subtasks are organized to correspond with relative timing of performance during the acquisition process. Consequently, for some tasks, all subtasks may not be required to be performed for a given contract period. In these cases, the SOW shall specify the applicable subtask requirements.

8.1.4 LSA documentation and information system

LSA documentation shall consist of all data resulting from analysis tasks conducted under this standard, and shall be the primary source of validated, integrated design, related supportability data pertaining to an acquisition program.

LSA documentation shall be developed and maintained commensurate with design, support, and operational concept development, and shall be updated to reflect changes or availability of better information based on testing, configuration changes, operational concept changes, and support concept changes during the acquisition process.

Accumulated LSA documentation shall provide an audit trail of supportability and supportability related design analyses and decisions, and shall be the basis for actions and documents related to manpower and personnel requirements, training programs, provisioning, maintenance planning, resources allocation, funding decisions, and other logistic support resource requirements.

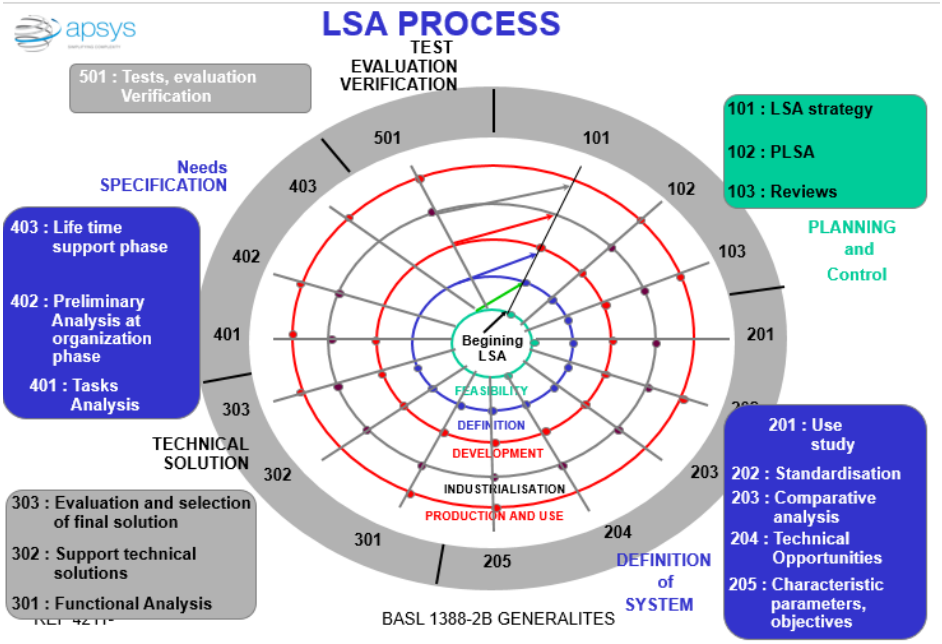
Configuration control procedures shall be established over LSA documentation updates to assure proper coordination among other system engineering programs, the LSA program, and the development of ILS documents using LSA data.

Deliverable documentation shall be as specified in applicable data item descriptions cited on contract data requirements list (CDRL), DD Form 1423. When the requiring authority desires delivery of the task outputs, as described in paragraph 5 of this standard, for LSA tasks or subtasks cited in the SOW, then appropriate data item descriptions and delivery information must be included in the CDRL.

8.1.5 LSA Data Base

The logistic support analysis record (LSAR) is a subset of LSA documentation and LSAR data elements shall conform to the requirements of MIL-STD-1388-2B.

Deliverable LSAR data shall be as specified in data item descriptions cited on the CDRL (Contractual Data Requirement List).



8.1.6 LSA Management

Management procedures shall be established to assure continuing assessment of analysis results and to allow for system/equipment design and LSA program adjustments as required. Feedback and corrective action procedures shall be established which include controls to assure that deficiencies are corrected and documented. Assessments, validations, and verifications shall be conducted throughout the system/equipment life cycle to demonstrate, within stated confidence levels, the validity of the analyses performed and the products developed from the analyses, and to adjust the analysis results and products as applicable.

8.2 LSA Tasks

8.2.1 General

The LSA tasks are divided into five general sections:
- Section 100, Program Planning and Control;
- Section 200, Mission and Support Systems Definition;
- Section 300, Preparation and Evaluation of Alternatives;
- Section 400, Determination of Logistic Support Resource Requirements;
- Section 500, Supportability Assessment.
-

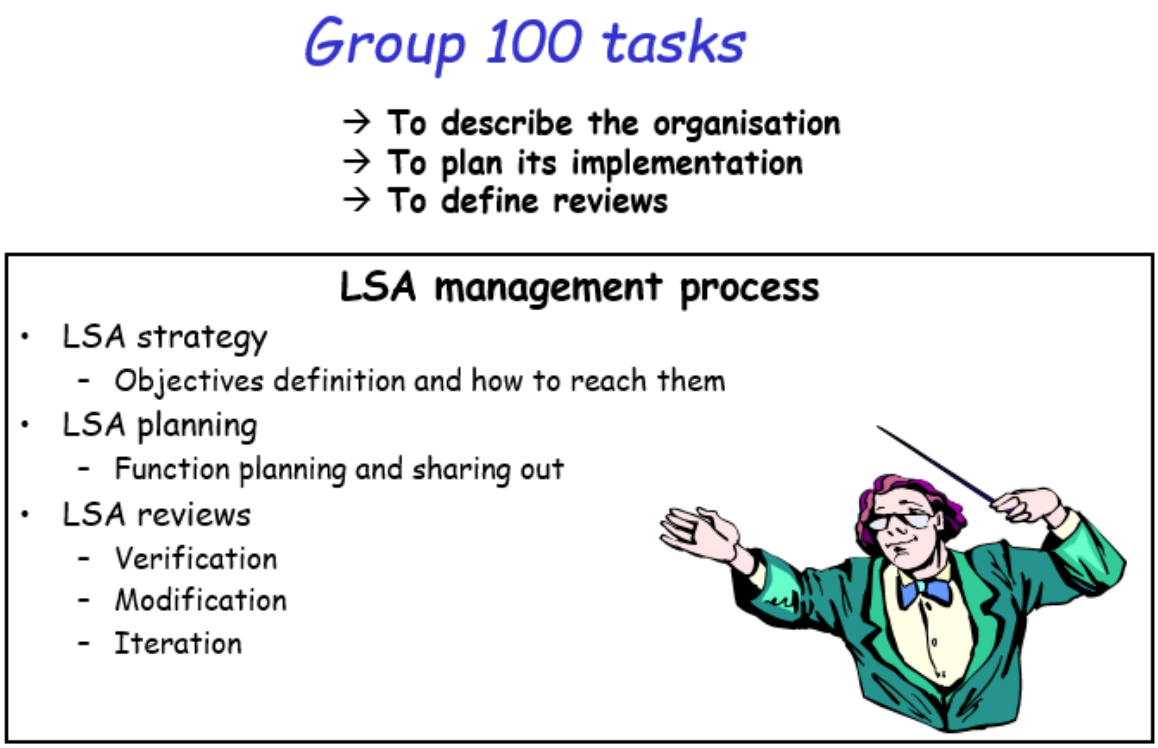
Table I identifies the general purpose of each section, the individual tasks contained in each section, and the general purpose of each task and subtask.

Each individual task is divided into four parts: purpose, task description, task input, and task output. The purpose provides the general reason for performing the task. The task description provides the detailed subtasks which comprise the overall task. It is not intended that all tasks and/or subtasks be accomplished in the sequence presented.

The sequence of task and subtask accomplishments should be tailored to the individual acquisition program. Where applicable, the subtasks are organized to correspond with relative timing of performance during the acquisition process.

Consequently, for some tasks, all subtasks may not be required to be performed for a given contract period. In these cases, the SOW shall specify the applicable subtask requirements (see the section 8.1.3)

8.3 LSA Tasks 100: Program Planning and Control



8.3.1 Task 101: development of an early logistic support analysis strategy

Main objective is to develop a proposed LSA program strategy for use early in an acquisition program, and to identify the LSA tasks and subtasks which provide the best return on investment.

Task 101 consists in preparing potential supportability objectives for the new system/equipment, identify and document the risk of accomplishing these objectives, and identify proposed LSA tasks and subtasks to be performed in each phase of the acquisition program. Identify the organizations to perform each task and subtask.

The proposed supportability objectives and analysis tasks and subtasks shall be based on the following factors:
a). The probable design, maintenance concept, and operational approaches for the new system/equipment and gross estimates of the reliability and maintainability (R&M), O&S costs, logistic support resources, and readiness characteristics of each design and operational approach.
b). The availability, accuracy, and relevance of readiness, O&S cost, and logistic support resource data required to perform the proposed LSA tasks and subtasks.
c). The potential design impact of performing the LSA tasks and subtasks.

Estimate the cost to perform each task and subtask identified under 101.2.1 and the cost effectiveness of performing each, given the projected costs and schedule constraints.

Update the LSA strategy as required based on analysis results, program schedule modifications, and program decisions.

8.3.2 Task 102: LSA plan

Main objective is to develop a Logistic Support Analysis Plan (LSAP) which identifies and integrates all LSA tasks, identifies management responsibilities and activities, and outlines the approach toward accomplishing analysis tasks.

Task 102 consists in preparing an LSAP which describes how the LSA program will be conducted to meet program requirements. The LSAP may be included as part of the Integrated Support Plan (ISP) when an ISP is required.
The LSAP shall include the following elements of information, with the range and depth of information for each element tailored to the acquisition phase:

a). A description of how the LSA program will be conducted to match the system and logistic requirements defined in the applicable program documents.

b). A description of the management structure and authorities applicable to LSA. This includes the interrelationship between line, service, staff, and policy organizations.

c). Identification of each LSA task that will be accomplished and how each will be performed. Identification of the major tradeoffs to be performed under Subtask 303.2.3, when applicable.

d). A schedule with estimated start and completion points for each LSA program activity or task. Schedule relationships with other ILS program requirements and associated system engineering activities shall be identified.

e). A description of how LSA tasks and data will interface with other ILS and system oriented tasks and data. This description will include consideration of nuclear hardness criticality and required analysis and data interfaces with the following programs, as applicable:

(1) System/Equipment Design Program.
(2) System/Equipment Reliability Program.
(3) System/Equipment Maintainability Program.
(4) Human Engineering Program.
(5) Standardization Program.
(6) Parts Control Program.
(7) System Safety Program.
(8) Packaging, Handling, Storage, and Transportability Program.
(9) Initial Provisioning Program.
(10) System/Equipment Testability Program.
(11) Survivability Program.
(12) Technical Publications Program.
(13) Training and Training Equipment Program.
(14) Facilities Program.
(15) Support Equipment Program.
(16) Test and Evaluation Program.

f). Work Breakdown Structure (WBS) identification of items upon which LSA will be performed and documented. Identification of an LSA candidate list, and LSA candidate selection criteria. The list shall include all items recommended for analysis, items not recommended and the appropriate rationale for selection or non-selection.

g). Explanation of the LSA control numbering system to be used.

h). The method by which supportability and supportability related design requirements are disseminated to designers and associated personnel.

i) The method by which supportability and supportability related design requirements are disseminated to subcontractors and the controls levied under such circumstances.

j) Government data to be furnished to the contractor.

k). Procedures for updating and validating of LSA data to include configuration control procedures for LSA data.

l.) LSA requirements on Government furnished equipment/materiel (GFE/GFM) and subcontractor/vendor furnished materiel including end items of support equipment.

m).The procedures (wherever existing procedures are applicable) to evaluate the status and control of each task, and identification of the organizational unit with the authority and responsibility for executing each task.

n). The procedures, methods, and controls for identifying and recording design problems or deficiencies affecting supportability, corrective actions required, and the status of actions taken to resolve the problems.

o). Description of the data collection system to be used by the performing activity to document, disseminate, and control LSA and related design data.

p). A description of the LSAR ADP system to be used and identification of the validated status when independently developed LSAR ADP software is recommended.

Update the LSAP as required, subject to requiring authority approval, based on analysis results, program schedule modifications, and program decisions.

8.3.3 Task 103: program and design reviews

Main objective is to establish a requirement for the performing activity to plan and provide for official review and control of released design information with LSA program participation in a timely and controlled manner, and to assure that the LSA program is proceeding in accordance with the contractual milestones so that the supportability and supportability related design requirements will be achieved.

Task 103 consists in establishing and documenting design review procedures (where procedures do not already exist) which provide for official review and control of released design information with LSA program participation in a timely and controlled manner. These procedures shall define accept/reject criteria pertaining to supportability requirements, the method of documenting reviews, the types of design documentation subject to review, and the degree of authority of each reviewing activity.

Formal review and assessment of supportability and supportability related design contract requirements shall be an integral part of each system/equipment design review (e.g., system design review (SDR), preliminary design review (PDR). critical design review (CDR), etc.) specified by the contract.
The performing activity shall schedule reviews with subcontractors and suppliers, as appropriate, and inform the requiring authority in advance of each review. Results of each system/equipment design review shall be documented. Design reviews shall identify and discuss all pertinent aspects of the LSA program.

Agendas shall be developed and coordinated to address at least the following topics as they apply to the program phase activity and the review being conducted:

a). LSA conducted by task and WBS element.

b). Supportability assessment of proposed design features including supportability, cost, and readiness drivers and new or critical logistic support resource requirements.

c). Corrective actions considered, proposed, or taken, such as:

(1) Support alternatives under consideration.
(2) System/equipment alternatives under consideration.
(3) Evaluation and tradeoff analysis results.
(4) Comparative analysis with existing systems/equipment.
(5) Design or redesign actions proposed or taken.

d). Review of supportability and supportability related design requirements (with review of specifications as developed).

). Progress toward establishing or achieving supportability goals.

f) LSA documentation required, completed, and scheduled.

g). Design, schedule, or analysis problems affecting supportability.

h). Identification of supportability related design recommendations to include a description of the recommendation; whether or not it has been approved or is pending; rationale for approval (e.g., cost savings, maintenance burden reductions, supply support reductions, reliability improvements, safety or health hazard reduction etc.).

i). Other topics and issues as appropriate.

Formal review and assessment of supportability and supportability related design contract requirements shall be an integral part of each system/equipment program review specified by the contract. Program reviews include, but are not limited to,

- ILS management team meetings,
- reliability program reviews,
- maintainability program reviews,
- technical data reviews,
- test integration reviews,
- training program reviews,

- human engineering program reviews,
- system safety program reviews
- supply support reviews.
-

The performing activity shall schedule program reviews with subcontractors and suppliers, as appropriate, and inform the requiring authority in advance of each review. Results of each system/equipment program review shall be documented. Program reviews shall identify and discuss all pertinent aspects of the LSA program.

The LSA program shall be planned and scheduled to permit the performing activity and the requiring authority to review program status.
The status of the LSA program shall be assessed at LSA reviews specified by the contract.
The performing activity shall schedule LSA reviews with subcontractors and suppliers, as appropriate, and inform the requiring authority in advance of each review.
Results of each LSA review shall be documented.
LSA reviews shall identify and discuss all pertinent aspects of the LSA program to a more detailed level than that covered at design and program reviews.

LSA guidance conferences shall be planned and scheduled to permit the performing activity and the requiring authority to formally assess the relationship of the LSA documentation, task milestones and funding levels contractually required.
The performing activity shall schedule a LSA guidance conference with the subcontractors and suppliers, as appropriate, and inform the requiring authority in advance of each conference.
Results of each LSA guidance conference shall be documented.
Additional functional area guidance conferences shall be held as part of the LSA guidance conference or scheduled to occur after the LSA guidance conference.
A requirement for the additional conferences to be held shall be scheduled during the LSA guidance conference or as part of the LSA plan.

A list of candidate conferences is as follows:

a). Provisioning Guidance Conference.
b). Provisioning Preparedness Review Conference.
c). Long Lead Time Item Provisioning Conference.
d). Provisioning Conference.
e). Interim Support Items Conference.
f). General Conference.

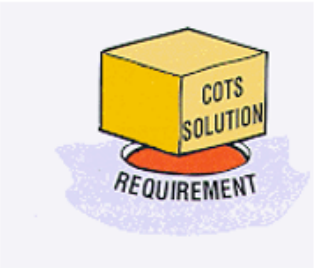
8.4 LSA TASKS 200 : MISSION AND SUPPORT SYSTEM DEFINITION

Group 200 tasks(1/2)

→ To set support capacity objectives
→ To set study aims, limits and constraints (comparison with current systems)
→ To analyse support capacity factors

SYSTEM CHARACTERISTICS

- Constraints (context study)
  - Users
  - Environment
- Factors (standardization study)
  - Of support capacity
  - Of cost
  - Of availability



Group 200 tasks(2/2)

SYSTEM CHARACTERISTICS

- Factors classification and properties (comparative analysis)
- Technological data integration (technological opportunities)
- Main factors selection (parameters, characteristics, objectives)
  - Of support capacity
  - Of cost
  - Of availability

8.4.1 TASK 201: use definition

Main objective is to identify and document the pertinent supportability factors related to the intended use of the new system/equipment.

Task 201 consists in identifying and documenting the pertinent supportability factors related to the intended use of the new system/equipment. Factors to be considered include mobility requirements, deployment scenarios, mission frequency and duration, basing concepts, anticipated service life, interactions with other systems/end items, operational environment, and human capabilities and limitations. Both peacetime and wartime employment shall be considered, in identifying the supportability factors. Previously conducted mission area and weapon system analyses which quantified relationships between hardware, mission, and supportability parameters and which are pertinent to the new system/equipment shall be identified and documented.

Quantitative data must be considered in developing support alternatives and conducting support analyses. This data would include but not be limited to the following:

a). Operating requirements, consisting of the number of missions per unit of time, mission duration, and number of operating days, miles, hours, firings, flights, or cycles per unit of time.
b). Number of systems supported.
c). Transportation factors (e.g., mode, type, quantity to be transported, destinations, transport time and schedule).
d). Allowable maintenance periods.
e). Environmental requirements to include hazardous materials, hazardous waste, and environmental pollutants.
f). Number of operator, maintainer, and support personnel available to support the requirements of the new system.

One shall conduct field visits to operational units and support activities which most closely represent the planned operational and support environment for the new system/equipment.

One will have to prepare a use study report and update the use study report as more detailed information on the intended use of the new system/equipment becomes available.

8.4.2 TASK 202: mission hardware, software, and support system standardization

Main objective is to define supportability and supportability related design constraints for the new system/equipment based on existing and planned logistic support resources which have benefits due to cost, manpower, personnel, readiness, or support policy considerations, and to provide input into mission hardware and software standardization efforts.

Task 202 consists in:

- Identifying existing and planned logistic support resources which have potential benefits for use on each system/equipment concept under consideration. All elements of ILS shall be considered. Define in quantitative terms supportability and supportability related design constraints for those items which should become program

constraints due to cost, manpower, personnel, readiness, or support policy considerations and benefits.
- Providing supportability, cost, and readiness related information into mission hardware and software standardization efforts. This input shall be provided to a level commensurate with the level of mission hardware and software standardization being pursued.
- Identifying recommended mission hardware and software standardization approaches which have utility due to cost, readiness, or supportability considerations and participate in the system/equipment standardization effort. This task shall be performed to a level of indenture commensurate with the design development.
- Identifying any risks associated with each constraint established. For example, known or projected scarcities, and developmental logistic support resources would represent possible risk areas when establishing standardization constraints.

8.4.3 TASK 203: comparative analysis

Main objective is to select or develop a Baseline Comparison System (BCS) representing characteristics of the new system/equipment for: - projecting supportability related parameters, making judgments concerning the feasibility of the new system/equipment supportability parameters, and identifying targets for improvement,
- determining the supportability, cost, and readiness drivers of the new system/equipment.

Task 203 consists in:

- Identifying existing systems and subsystems (hardware, operational, and support) useful for comparative purposes with new system/equipment alternatives. Different existing systems shall be identified when new system/equipment alternatives vary significantly in design, operation, or support concepts, or where different existing systems are required to adequately compare all parameters of interest.
- Selecting or developing a BCS for use in comparative analyses and identifying supportability, cost, and readiness drivers of each significantly different new system/equipment alternative. A BCS may be developed using a composite of elements from different existing systems when a composite most closely represents the design, operation, and support characteristics of a new system/equipment alternative. Different BCS's or composites may be useful for comparing different parameters of interest. Previously developed BCS's shall be assessed to determine the extent to which they can fill the need for the new system/equipment.
- Determining the O&S costs, logistic support resource requirements, reliability and maintainability (R&M) values, and readiness values of the comparative systems identified. Identify these values at the system and subsystem level for each BCS established. Values shall be adjusted to account for differences between the comparative system's use profile and the new system/equipment's use profile where appropriate.
- Identifying qualitative environmental, health-hazard, safety and supportability problems on comparative systems which should be prevented on the new system/equipment.
- Determining the supportability cost, and readiness drivers of each comparative system or BCS. These drivers may come from the design, operating, or support characteristics of the comparative systems and represent drivers for the new system/equipment. For example, repair cycle time may be the prime readiness driver, a particular hardware

subsystem may be the prime manpower driver, or energy cost may be the prime cost driver.
- Identifying and documenting any supportability, cost, or readiness drivers for the new system/equipment resulting from subsystems or equipment in the new system for which there are no comparable subsystems or equipment in comparative systems.
- Updating the comparative systems, their associated parameters, and the supportability, cost, and readiness drivers as the new system/equipment alternatives become better defined or as better data is obtained on the comparative systems and subsystems.
- Identifying and documenting any risks and assumptions associated with the comparative systems, and their associated parameters and drivers, such as a low degree of similarity between the new system/equipment and existing systems or the lack of accurate data on existing systems.

8.4.4 TASK 204: technological opportunities

Main objective is to identify and evaluate design opportunities for improvement of supportability characteristics and requirements in the new system/equipment.

Task 204 consists in establishing design technology approaches to achieve supportability improvements on the new system/equipment over existing systems and subsystems. These design approaches shall be established through the following:
a). Identifying technological advancements and other design improvements which can be exploited in the new system/equipment's development and which have the potential for reducing logistic support resource requirements, reducing costs, reducing environmental impact, improving safety, or enhancing system readiness.
b). Estimating the resultant improvements that would be achieved in the supportability, cost, environmental impact, safety, and readiness values.
c). Identifying design improvements to logistic elements (such as support equipment and training devices) that can be applied during the new system/equipment's development to increase the effectiveness of the support system or enhance readiness.

One shall update the design objectives as new system/equipment alternatives become better defined.

One will have to identify any risks associated with the design objectives established, any development and evaluation approaches needed to verify the improvement potential, and any cost or schedule impacts to implement the potential improvements.

8.4.5 TASK 205: supportability and supportability related design factors

Main objective is to establish:
- quantitative supportability characteristics resulting from alternative design and operational concepts,
- supportability and supportability related design objectives, goals and thresholds, and constraints for the new system/equipment for inclusion in program approval documents, system/equipment specifications, other requirements documents, or contracts as appropriate.

Task 205 consists in identifying the quantitative operations and support characteristics resulting from alternative design and operational concepts for the new system/equipment. Operational characteristics shall be expressed in terms of crew size per system, aptitude and skill requirements of each job in the crew, and performance standards for each task. Supportability characteristics shall be expressed in terms of feasible support concepts, estimates of manpower requirements, aptitude and skill requirements for each job associated with the system, performance standards for each task, R&M parameters, system readiness, O&S cost, and logistic support resource requirements. Both peacetime and wartime conditions shall be included.

In the framework of task 205 one shall as well:

a) Conduct sensitivity analysis on the variables associated with the supportability, cost and readiness drivers identified for the new system/equipment.

b) Identify any hardware or software for which the Government will not or may not have full design rights due to constraints imposed by regulations or laws limiting the information the contractor must furnish because of proprietary or other source control considerations. Include alternatives and cost, schedule and function impacts.

c) Establish supportability, cost, environmental impact, and readiness objectives for the new system. Identify the risks and uncertainties involved in achieving the objectives established. Identify any risks associated with new technology planned for the new system/equipment.

d) Establish supportability and supportability related design constraints for the new system/equipment for inclusion in specifications, other requirements documents, or contracts as appropriate. The design constraints will address, but are not limited to, those constraints related to hazardous material, hazardous waste, and environmental pollutants. These constraints shall include both quantitative and qualitative constraints. Document the quantitative constraints in the LSAR or equivalent format approved by the requiring authority.

e) Identify any constraints that preclude adoption of a NATO system/equipment to satisfy the mission need.

f) Update the supportability, cost, and readiness objectives and establish goals and thresholds as new system/equipment alternatives become better defined.

8.5 LSA TASKS 300: PREPARATION AND EVALUATION OF ALTERNATIVES

Group 300 tasks

→ To optimise support system for new equipment
→ To develop system which ensure best balance between cost - delays - performances and support capacity

POTENTIAL SOLUTIONS- OPTIMISATION

- Identification of maintenance tasks
- Potential Solutions for le support system
- Optimisation

8.5.1 TASK 301: functional requirements identification

Main objective is to identify the operations, maintenance, and support functions that must be performed in the intended environment for each system/equipment alternative under consideration and then to identify the human performance requirements for operations, maintenance and to document those requirements in a task inventory.

Task 301 consists in

- Identifying and documenting the functions that must be performed for the new system/equipment to be operated and maintained in its intended operational environment for each design alternative under consideration. These functions shall be identified to a level commensurate with design and operational scenario development, and shall include both peacetime and wartime functions (in case of a military system). Identify hazards, including hazardous material, hazardous waste, and environmental pollutants associated with those functions identified.

- Identifying those functional requirements which are unique to the new system/equipment due to new design technology or operational concepts, or which are supportability, cost, or readiness drivers. Identify hazards, including hazardous material, hazardous waste, and environmental pollutants associated with those functions identified.

- Identifying any risks involved in satisfying the functional requirements of the new system/equipment.

In the framework of this task 301, a task inventory shall be prepared for the new system/equipment or facility being acquired. This task inventory shall identify all tasks that operators, maintainers, or support personnel must perform with regard to the new system/equipment under development based on the mission analysis, scenarios/conditions and the identified functional requirements (i.e. functional analysis).
Task shall be identified to a taxonomic level commensurate with design and operational scenario development. The task inventory shall be organized in terms of a task taxonomy which defines mission, scenario/conditions, function, job, duty, task, subtask and task elements, as defined in the glossary.

The task inventory shall be composed of task descriptions, each of which consists of:
a. An action verb which identifies what is to be accomplished in the task.
b. An object which identifies what is to be acted upon in the task.
c. Qualifying phrases needed to distinguish the task from related or similar tasks.

Task descriptions shall be clear, concise, relevant, and written in operator or maintainer language. Hazardous materials, generation of waste, release of air and water pollutants, and environmental impacts associated with each task shall be identified. Where the same task appears in the duty of more than one job and is therefore identified as a collective task for training purposes, it will be identified as such within the task inventory. All verbs shall be unambiguously defined within the taxonomy. A list of preferred verbs is provided in MIL-STD-1388-2.
Task descriptions may be supplemented by graphical displays or time line charts. Task descriptions shall be limited to information germane to the task, not the qualifications of personnel involved, necessary tools, or job aids. Operations, preventive maintenance, corrective maintenance, and other support tasks such as preparation for operation, post operation, calibration, and transportation shall be identified by the following methods:

The results of the failure modes, effects, and criticality analysis (FMECA), or equivalent analysis, shall be analyzed to identify and document corrective maintenance task requirements. The FMECA or equivalent, shall be documented on system/equipment hardware and software and to the indenture level consistent with the design progression and as specified by the requiring authority. The LSAR, or equivalent format approved by the requiring authority, shall be used for the FMECA documentation.

Preventive maintenance task requirements shall be identified by conducting a reliability centered maintenance (RCM) analysis in accordance with the detailed guidelines provided by the requiring authority. The RCM analysis shall be based on the FMECA data and documented in the LSAR or equivalent format approved by the requiring authority.

Operations, maintenance, and other support tasks shall be identified through analysis of the functional requirements of the new system/equipment taking into account mission analysis, and scenarios/conditions under which the new system/equipment will be operated. The analysis shall examine each system function allocated to personnel and determine what operator or support personnel tasks are involved in the performance of each system function.

One will have to participate in formulating design alternatives to correct design deficiencies uncovered during the identification of functional requirements or operations and maintenance task requirements. Design alternatives which reduce or simplify functions shall be analyzed.

One shall update as well the functional requirements and operations and maintenance task requirements as the new system/equipment becomes better defined and better data becomes available.

8.5.2 TASK 302: support system alternatives

Main objective is to establish viable support system alternatives for the new system/equipment for evaluation, tradeoff analysis, and determination of the best system for development.

Task 302 consists in developing and documenting viable alternative system level support concepts for the new system/equipment alternatives which satisfy the functional requirements of the new system/equipment within the established supportability and supportability related design constraints. Each alternative support concept shall be developed to a level of detail commensurate with the hardware, software, and operational concept development, and shall address all elements of ILS.
The same support concept may be applicable to multiple new system/equipment design and operational alternatives. Support concept alternatives shall be prepared to equivalent levels of detail to the degree possible for use in the evaluation and tradeoff of the alternatives.
The range of support alternatives considered shall not be restricted to existing standard support concepts but shall include identification of innovative concepts which could improve system readiness, optimize manpower and personnel requirements, or reduce O&S costs. Contractor logistic support (total, in part, or on an interim basis) shall be considered in formulating alternative support concepts.

In the framework of task 302, one shall as well:

- Update the alternative support concepts as system tradeoffs are conducted and new system/equipment alternatives become better defined. Alternative support concepts shall be documented at the system and subsystem level, and shall address the supportability, cost, and readiness drivers and the unique functional requirements of the new system/equipment.

- Develop and document viable alternative support plans for the new system/equipment to a level of detail commensurate with the hardware, software, and operational scenario development.

- Update and refine the alternative support plans as tradeoffs are conducted and the new system/equipment's design and operational scenario become better defined.

- Identify risks associated with each support system alternative formulated.

8.5.3 TASK 303: evaluation of alternatives and tradeoff analysis

Main objective is to determine the preferred support system alternative(s) for each system/equipment alternative and to participate in alternative system tradeoffs to determine the best approach (support, design, and operation) which satisfies the need with the best balance between cost, schedule, performance, readiness, and supportability.

In task 303, for each evaluation and tradeoff to be conducted under-this task, one shall:

a). Identify the qualitative and quantitative criteria which will be used to determine the best results. These criteria shall be related to the supportability, cost, environmental impact, and readiness requirements for the system/equipment.

b). Select or construct analytical relationships or models between supportability, design, and operational parameters and those parameters identified for the evaluation criteria. In many cases, the same model or relationship may be appropriate to perform a number of evaluations and tradeoffs. Parametric and cost estimating relationships (PER/CER) may be appropriate for use in formulating analytical relationships.

c). Conduct the tradeoff or evaluation using the established relationships and models and select the best alternatives) based upon the established criteria.

d). Conduct appropriate sensitivity analyses on those variables which have a high degree of risk involved or which drive supportability, cost, or readiness for the new system.

e). Document the evaluation and tradeoff results including-any risks and assumptions involved.

f). Update the evaluations and tradeoffs as the system/equipment becomes better defined and more accurate data becomes available.

g). Include both peacetime and wartime considerations in the analyses.

h). Assess the impact on existing or planned weapon, supply, maintenance, and transportation systems based on the tradeoff decision. i. Assess life cycle support considerations to include post production support.

In the framework of task 303, one shall as well:

- Conduct evaluations and tradeoffs between the support system alternatives identified for each system/equipment alternative (Task 302). For the selected support system alternative(s), identify and document any new or critical logistic support resource requirements. Any restructured personnel job classification shall be identified as a new resource.

- Conduct evaluations and tradeoffs between design, operations, and support concepts under consideration.

- Evaluate the sensitivity of system readiness parameters to variations in key design and support parameters such as R&M, spares budgets, resupply time, and manpower and personnel skill availability.

- Estimate and evaluate the manpower and personnel implications of alternative system/equipment concepts in terms of total numbers of personnel required, job classifications, skill levels, and experience required. This analysis shall include organizational overhead requirements, error rates, and training requirements.

- Conduct evaluations and tradeoffs between design, operations, training, and personnel job design to determine the optimum solution for attaining and maintaining the required

proficiency of operating and support personnel. Training evaluations and trades shall be conducted and shall consider shifting of job duties between job classifications, alternative technical publications concepts, and alternative mixes of formal training, on-the-job training, unit training, and use of training simulators.

- Conduct level of repair analysis (LORA) in accordance with MIL-STD-1390, commensurate with the level of design, operation, and support data available. Identify Source, Maintenance, and Recoverability (SMR) characteristics from the LORA for those items identified as provisioned item candidates.

- Evaluate alternative diagnostic concepts to include varying degrees of built-in-test (BIT), off-line-test, manual testing, automatic testing, diagnostic connecting points for testing, and identify the optimum diagnostic concept for each system/equipment alternative under consideration.

- Conduct comparative evaluations between the supportability, cost, and readiness parameters of the new system/equipment and existing comparative systems/equipment. Assess the risks involved in achieving the supportability, cost, and readiness objectives for the new system/equipment based upon the degree of growth over existing systems/equipment.

- Conduct evaluations and tradeoffs between system/equipment alternatives and energy requirements. Identify the petroleum, oil, and lubricant (POL) requirements for each system/equipment alternative under consideration and conduct sensitivity analyses on POL costs.

- Conduct evaluations and tradeoffs between system/equipment alternatives and survivability and battle damage repair characteristics in a combat environment.

- Conduct evaluations and tradeoffs between system/equipment alternatives and transportability requirements. Identify the transportability requirements for each alternative under consideration and the limiting constraints, characteristics, and environments on each of the modes of transportation.

- Conduct evaluations and tradeoffs between system/equipment alternatives and support facilities (including power/utilities and pavements) requirements. Identify the facility requirements for each support system alternative under consideration and the limiting constraints, characteristics, and environment on each type of facility.

8.6 LSA TASKS 400: DETERMINATION OF LOGISTIC SUPPORT RESOURCE REQUIREMENTS

Group 400 tasks

→ To Identify logistic support resource requirements for the system, in its operational environment
→ To Develop plans for contractual (post-production) support

SELECTED SOLUTION DESCRIPTION

- Detailed description of maintenance tasks
- Starting up phase support
- Using phase support

8.6.1 TASK 401: task analysis

Main objective is to analyze required operations and maintenance tasks for the new system/equipment to:
a). Identify logistics-support resource requirements for each task..
b). Identify new or critical logistic support resource requirements.
c). Identify transportability requirements.
d). Identify support requirements which exceed established goals, thresholds, or constraints.
e). Provide data to support participation in the development of design alternatives to reduce O&S costs, optimize logistic support resource requirements, or enhance readiness.
f) Provide spirce data for preparation of required ILS documents (technical manuals, training programs, manpower and personnel lists, etc).

Task 401 will consist in conducting a detailed analysis of each operation, maintenance and support task contained in the task inventory (Task 301) and determine the following:

a). Logistic support resources required (considering all ILS elements) to perform the task.
b).Task frequency, task interval, elapsed time, and man-hours in the system/equipment's intended operational environment and based on the specified annual operating base.
c). Maintenance level assignment based on the established support plan (Task 303).
d). Environmental impact of the tasks including use of hazardous materials, generation of hazardous waste, and release of air and water pollutants.

In the framework of task 401, one shall as well:

- Document the results in the LSAR (Logistic Support Analysis Record or LSA Data Base) or equivalent format approved by the requiring authority.

- Identify new or critical logistic support resources required to perform each task, and hazardous materials, hazardous waste, and environmental impact requirements associated with these resources. New resources are those which require development to operate or maintain the new system/equipment. These can include support and test equipment, facilities, new or special transportation systems, new computer resources, and new repair, test., or inspection techniques or procedures to support new design plans or technology. Critical resources are those which are not new but require special management attention due to schedule constraints, cost implications, or known scarcities. Unless otherwise required, document new and modified logistic support resources in the LSAR, or equivalent documentation approved by the requiring authority, to provide a description and justification for the resource requirement.

- Based upon the identified task procedures and personnel assignments, identify training requirements and provide recommendations concerning the best mode of training (formal classroom, on-the-job, or both) and the rationale for the recommendations. Document the results in the LSAR or equivalent format approved by the requiring authority.

- Analyze the total logistic support resource requirements for each task and determine which tasks fail to meet established supportability or supportability related design goals or constraints for the new system/equipment. Identify tasks which can be optimized or simplified to reduce O&S costs, optimize logistic support resource requirements, reduce environmental impact including use of hazardous materials, generation of hazardous waste, release of air and water pollutants, and environmental impact, or enhance readiness. Propose alternative designs and participate in the development of alternative approaches to optimize and simplify tasks or to bring task requirements within acceptable levels.

- Based upon the identified new or critical logistic support resources, determine what management actions can be taken to minimize the risks associated with each new or critical resource. These actions could include development of detailed tracking procedures, or schedule and budget modifications. Managers and program decision authorities shall consider the desirability and effectiveness of integrating Spares Acquisition Integrated with Production (SAIP) when the end item is, or will be, in production.

- Conduct a transportability analysis on the system/equipment and any sections thereof when sectionalization is required for transport. When the general requirements of MIL-STD-1366 limitations are exceeded, document the transportability engineering characteristics in the LSAR, or equivalent format approved by the requiring authority. Participate in the development of design alternatives when transportability problem areas are surfaced.

-

8.6.2 Task 402: early fielding analysis

Main objective is to assess the impact of introduction of the new system/equipment on existing systems, identify sources of manpower and personnel to meet the requirements of the new system/equipment, determine the impact of failure to obtain the necessary logistic support resources for the new system/equipment, and determine essential logistic support resource requirements for a combat environment.

Task 402 will consist in:

- Assessing the impact on existing systems (weapon, supply, maintenance, transportation) from introduction of the new system/equipment. This assessment shall examine impacts on depot workload and scheduling, provisioning and inventory factors, automatic test equipment availability and capability, manpower and personnel factors, training programs and requirements, POL requirements, and transportation systems, and shall identify any changes required to support existing weapon systems due to new system/equipment requirements.

- Analyzing existing manpower and personnel sources to determine sources to obtain the required manpower and personnel for the new system/equipment. Determine the impact on existing operational systems from using the identified sources for manpower and personnel.

- Assessing the impact on system/equipment readiness resulting from failure to obtain the required logistic support resources in the quantities required. Do not duplicate analyses performed under Task 303.

- Conducting survivability analyses to determine changes in logistic support resource requirements based on combat usage. These analyses shall be based on threat assessments, projected combat scenarios, system/equipment vulnerability, battle damage repair capabilities, and component essentialities in combat. Identify and document recommended combat logistic support resources (e.g., combat supply support storage lists) and sources to satisfy the requirements. Do not duplicate analyses performed under Task 303.

- Developing plans to implement solutions to problems surfaced in the above assessments and analyses.

8.6.3 Task 403: post production support analysis

Main objective is to analyze life cycle support requirements of the new system/equipment prior to closing of production lines to assure that adequate logistic support resources will be available during the system/equipment's remaining life.

Task 403 shall consist in:

- Assessing the expected useful life of the system/equipment.
- Identifying support items associated with the system/equipment that will present potential problems due to inadequate sources of supply after shutdown of production lines.

- Developing and analyzing alternative solutions for anticipated support difficulties during the remaining life of the system/equipment.
- Developing a plan that assures effective support during its remaining life along with the estimated funding requirements to implement the plan. As a minimum, this plan shall address manufacturing, repair centers, data modifications, supply management, and configuration management.

8.7 LSA TASKS 500: SUPPORTABILITY ASSESSMENT

Group 500 tasks

→To check that specified requirements are satisfied and deficiencies are corrected

TESTS, EVALUATION, VERIFICATION

- Validation of maintenance tasks
- Validation of starting up phase support
- Validation of using phase support

8.7.1 Task 501: supportability test, evaluation and verification

Main objective is to assess the achievement of specified supportability requirements, identify reasons for deviations from projections, and identify methods of correcting deficiencies and enhancing system readiness.

Task 501 will consist in:

- Formulating a test and evaluation strategy to assure that specified supportability and supportability related design requirements are achieved, or achievable, for input into system test and evaluation plans. The test and evaluation strategy formulated shall be based upon quantified and supportability requirements for the new system/equipment; the supportability, cost, and readiness drivers; and supportability issues with a high degree of risk associated with them. Tradeoffs shall be conducted between the planned test length and cost and the statistical risks incurred. Potential test program limitations in verifying supportability objectives based on previous test and evaluation experience and the resulting effect on the accuracy of the supportability assessment shall be documented.

- Developing a System Support Package (SSP) component list identifying support resources that will be evaluated during logistic demonstration and will be tested/validated during development and operational tests.

The component lists will include:

a. Supportability test requirements.
b. Applicable Maintenance Allocation Chart (MAC).
c. Technical publications.
d. Spares and repair parts.

e. Training devices/equipment.
f. Special and common tools.
g. Test, measurement and diagnostic equipment (TMDE).
h. Operations and maintenance manpower/personnel requirements.
i. Training courses.
j. Transportation and materiel handling equipment.
k. Calibration procedures and equipment.
l. Mobile and/or fixed support facilities.
m. m. Embedded software requirements.
n Other support equipment.

In the framework of task 501, one shall also:

- Establish and document test and evaluation program objectives and criteria and identify test resources, procedures, and schedules required to meet the objectives for inclusion in the coordinated test program and test and evaluation plans. The objectives and criteria established shall provide the basis for assuring that critical supportability issues and requirements have been resolved or achieved within acceptable confidence levels.

- Analyze the test results and verify/assess the achievement of specified supportability requirements for the new system/equipment. Determine the extent of improvement required in supportability and supportability related design parameters in order for the system/equipment to meet established goals and thresholds. Identify any areas where established goals or thresholds have not been demonstrated within acceptable confidence levels. Do not duplicate analyses performed in Task 303. Develop corrections for support ability problems uncovered during test and evaluation. These could include modifications to hardware, software, support plans, logistic support resources, or operational tactics. Update the documented support plan and logistic support resource requirements as contained in the LSAR and LSAR output reports based on the test results. Quantify the effects of these updates on the projected cost, readiness, and logistic support resource parameters for the new system/equipment.

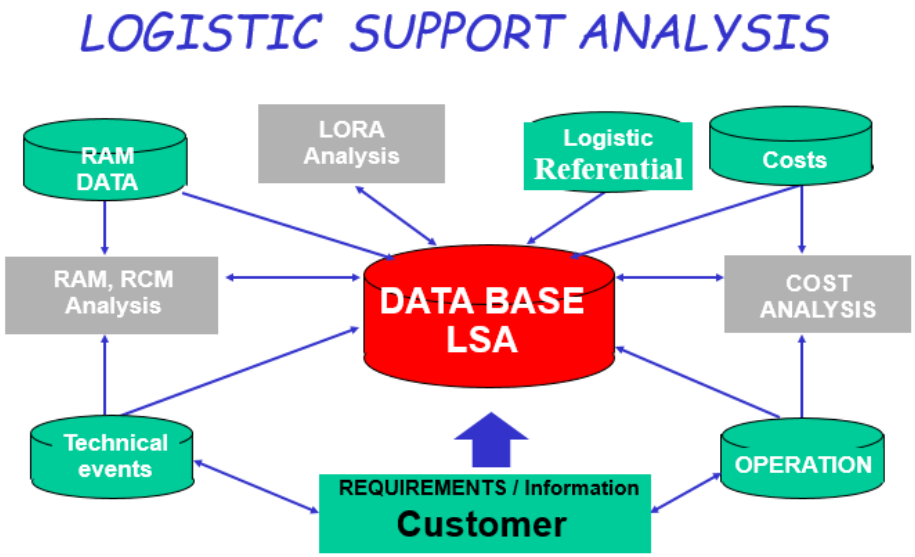
- Analyze standard reporting systems to determine the amount and accuracy of supportability information that will be obtained on the new system/equipment in its operational environment. Identify any shortfalls in measuring accomplishment against the supportability goals that were established for the new system/equipment, or in verifying supportability factors which were not tested during the acquisition phases of the item's life cycle. Develop viable plans for obtaining required supportability data from the field which will not be obtained through standard reporting systems. Conduct tradeoff analyses between cost, length of data collection, number of operational units in which to collect data, and statistical accuracy to identify the best data collection plan. Document the data collection plan selected to include details concerning cost, duration, method of data collection, operational units, predicted accuracy, and intended use of the data.

- Analyze supportability data as it becomes available from standard supply, maintenance, and readiness reporting systems and from any special data collection programs implemented on the new system/equipment. Verify achievement of the goals and thresholds established for the new system/equipment. In those cases where operational results deviate from projections, determine causes and corrective actions. Analyze

feedback information and identify areas whore improvements can be cost effectively accomplished. Document recommended improvements

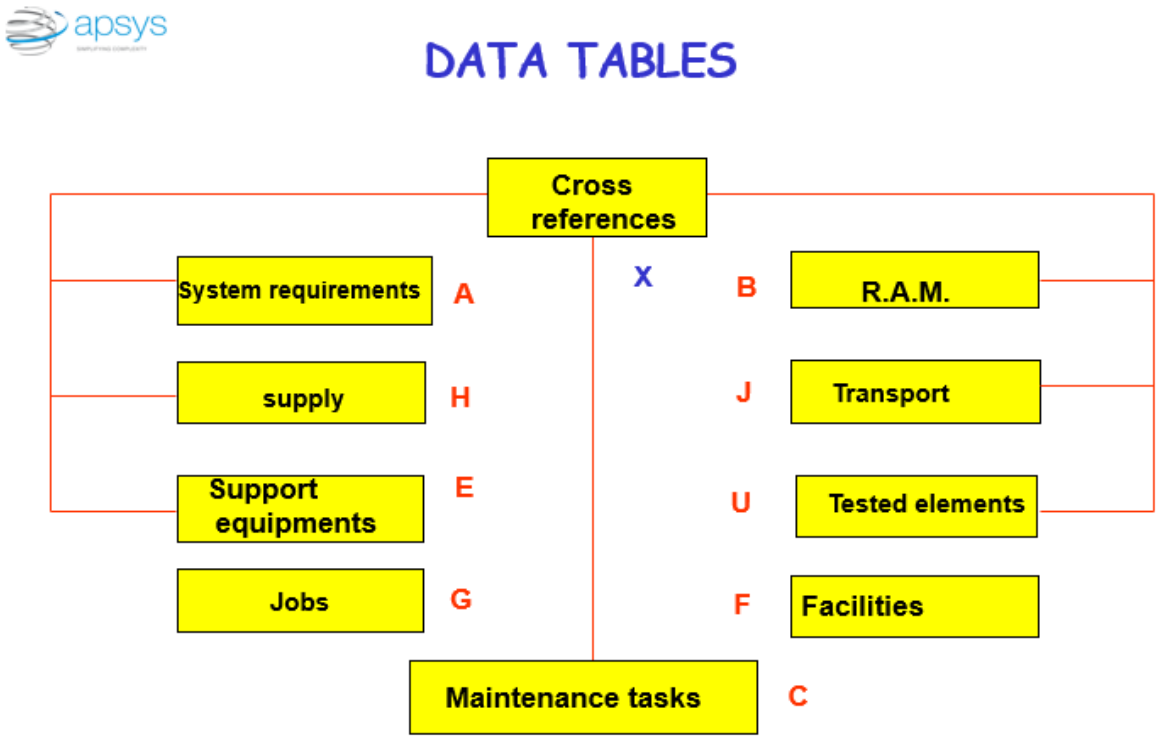
8.8 LOGISTIC INFORMATION SYSTEM STANDARD: MIL-STD-1388-2B

This standard provides a generic model of a universal logistics information system able to support LSA process described previously:

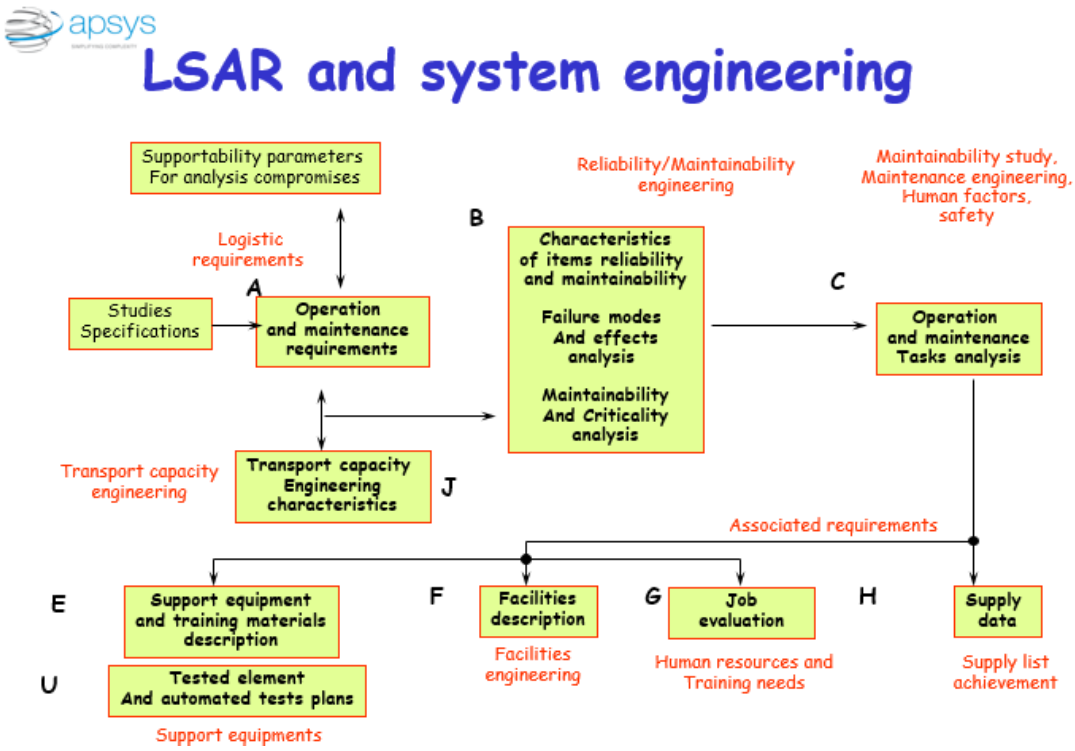


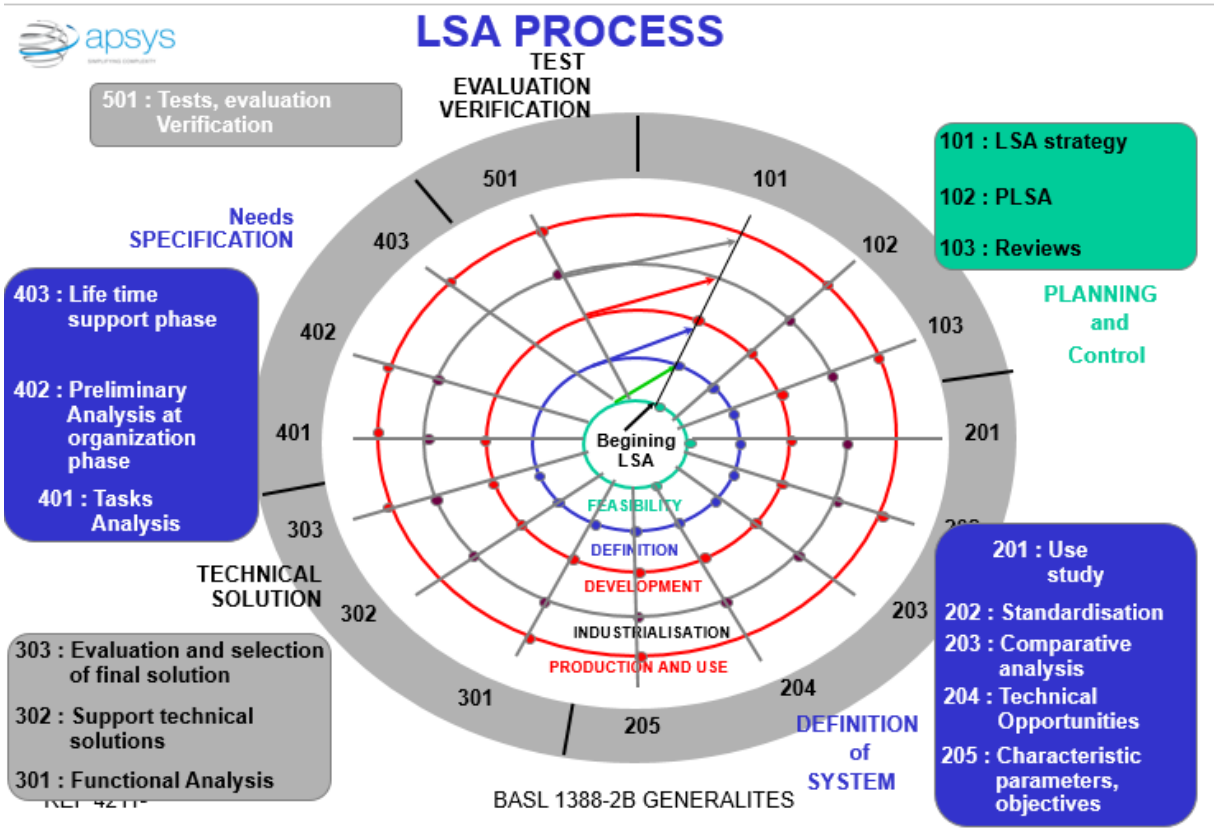
It contains:

- 518 types of data
- 9 groups of relational tables
- 104 relation tables.



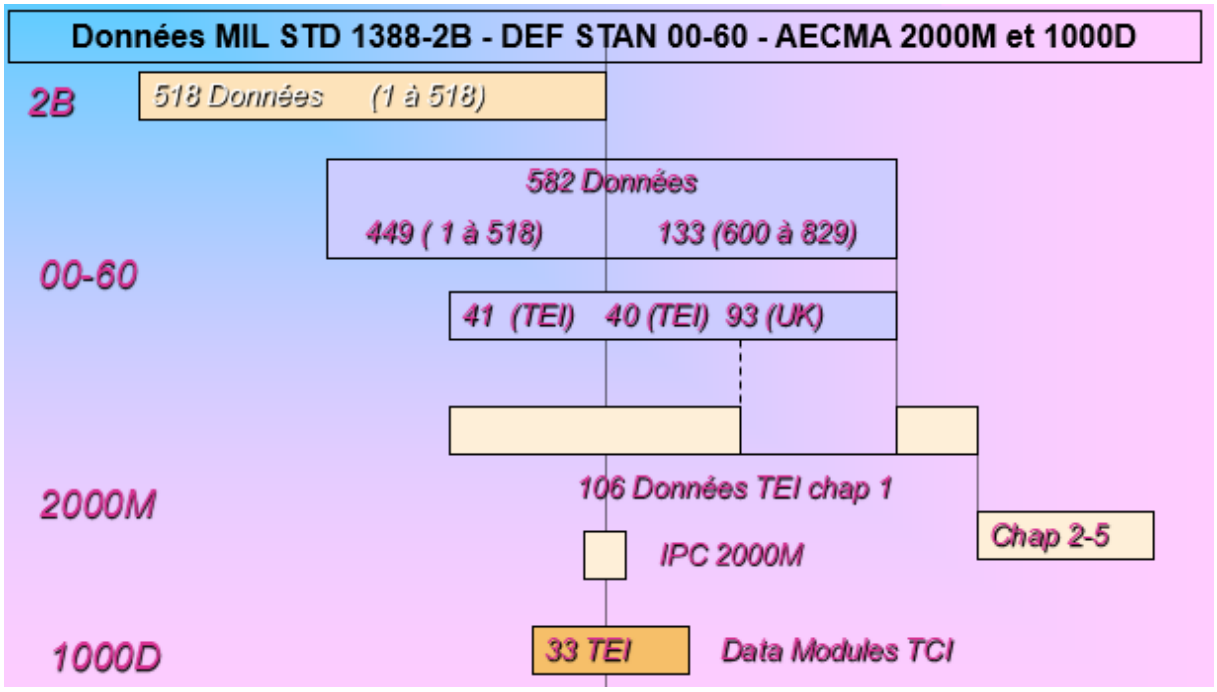
All those data and information are used and modified all along the LSA process.




LSA PROCESS
apsys
TEST
EVALUATION
VERIFICATION
501 : Tests, evaluation Verification
101 : LSA strategy
102 : PLSA
103 : Reviews
PLANNING and Control
Needs SPECIFICATION
403 : Life time support phase
402 : Preliminary Analysis at organization phase
401 : Tasks Analysis
TECHNICAL SOLUTION
303 : Evaluation and selection of final solution
302 : Support technical solutions
301 : Functional Analysis
DEFINITION of SYSTEM
201 : Use study
202 : Standardisation
203 : Comparative analysis
204 : Technical Opportunities
205 : Characteristic parameters, objectives
501
101
102
103
201
203
204
205
301
302
303
401
402
403
Begining LSA
FEASIBILITY
DEFINITION
DEVELOPMENT
INDUSTRIALISATION
PRODUCTION AND USE
BASL 1388-2B GENERALITES

8.9 VARIOUS HERITAGE FROM 1388 STANDARD: ASD-S3000L

Following graphical chart shows similarities existing between standards which have succeeded to initial LSA standard MIL-STD-13881A:



8.9.1 MIL-PRF-456

- This is the US standard which has replaced MIL-STD-1388-2B, cancelled by DoD (Department Of Defence) because it was too complicated…
- Main features :
    - Simplification of MIL STD 1388
    - Same acquisition process to collect logistic information
    - Data management tools to be proposed by client and partners
    - Flexibility, adaptability and taylorisation
    - Design information simplified

8.9.2 DEF-STAN-0060

This is a standard developed by UK MOD, very similar to MIL STD 1388.

Specific features are following :

- Some data have been removed
- Some data have been added
- Some data have been modified
- Some tables have been added (HS : crisis resupply from industry procedure, HP : design change inf., Z : Ammunition PHST requirement)
- Some AECMA 2000M data have been integrated
- Some reports have been modified

8.9.3 AECMA-2000M

This is a European standard dedicated to provisioning and exchange of electronic data about the provisioning process.

This standard has been a strong support to management and logistic support of aeronautics and military industry.

8.10 LAST HERITAGE FROM 1388 STANDARD: ASD-S3000L

8.10.1 Introduction

S3000L focuses on integrated logistic support (ILS) activities, and more strictly on logistic support analysis. It is part of a series of specifications put forward by the ASD (Aerospace and Defence Industry), which also includes S1000D, S2000M, S4000P, etc. All these specifications touch upon the design and development of complex systems and include all the elements necessary to sustain them, including operational documentation, maintenance and supply documentation, training, maintenance plans, tools, centralized database…

Thus, each one of these standards has its own specific scope of action. As for the S3000L standard, it aims to:

Regulate and document global logistic support analyses, as well as the interactions between various activities and fields by making the data exchange processes more straightforward.

Itemize the coordination of integrated logistic support activities and logistic support analysis together with other functions inherent to a company, including research and development, engineering, manufacturing, supply chain, maintenance, etc.

Provide concrete indications as to how integrated logistic support requirements can be met, particularly by suggesting several implementation models.

According to the specifications of the S3000L standard, LSA (Logistic Support Analysis) mainly aims to implement a thoroughly justified maintenance plan which strictly follows specific steps of explanation, justification, and validation based on safety assessments.

These assessments also make it possible to define the different support elements, such as technical publications to oversee maintenance tasks and all the information required in the context of training and spare parts supply (illustrated index, etc.).

Besides maintenance plans, S3000L provides ample information surrounding the product support frame of reference produced by LSA, its configuration, and its and its consistency with the main system.

It also describes the various data modules and characteristics that will sustain and feed the technical data necessary for all maintenance activities, be it from a reliability standpoint or based on design, storage, delivery, etc. All this information has become mandatory to run the more recent, increasingly complex programs.

To sum up, the S3000L specification for logistic support federates all the activities pertaining to any product or system, from its inception to the very end of its life and every single step in between, including development, operation, maintenance, optimization, improvement, and scrapping. Ultimately, S3000L deals with every element that could impact its industrial use.

For information, you have following the whole suite of S-Series ILS specifications:

- SX000i - International guide for integrated logistic support (under development)
- S1000D - International specification for technical publications using a common source database
- S2000M - International specification for materiel management - Integrated data processing
- S3000L - International specification for Logistics Support Analysis – LSA

- S4000P - International specification for developing and continuously improving preventive maintenance
- S5000F - International specification for operational and maintenance data feedback (under development)
- S6000T - International specification for training needs analysis - TNA (definition on-going)
- SX001G - Glossary for the Suite of S-specifications
- SX002D - Common Data Model

8.10.2 ASD S3000L LSA features

Thus, there exist various stages in the S3000L LSA process which come into existence through:

- The SLA Process

This process consists in a series of analyses based on data relating to operation and system support requirements, on configuration standards and on the tree structure that derives from the design.

- The Logistical Tree Structure

This tree structure is the translation of the product breakdown into a tree structure relevant to maintenance. This approach remains complicated as it shows various requirements and a different purpose in terms of conception as far as the design office is concerned.

- The Selection of the LSA Candidate

The list of LSA candidates is subjected to an action-oriented selection process based on matrices of value, depending on a number of eligibility criteria.

Within this process, value is awarded to the candidate based on support objectives and on the effort required for the analysis to be carried out.

- The Selection of the LSA Analysis Tasks

Starting from the list of successful LSA candidates, the type of analysis will need to be selected based on an index suggested by the S3000L specification logistic support solution.

A summary will be carried out, which will make it possible to assess the effort required and to determine the workload for the corresponding analysis.

- Triggering Events Analysis

At the very first stages of a system's inception, not everything is absolutely set in stone. The project could even be incomplete, which means that the maintenance plan is still in a draft state.

S3000L allows this step to affect – for each of the system's elements – one or more triggering elements or events required by the maintenance process for said element.

These triggering events can be naturally occurring ones (failure or outage, damage, preventative) or based on needs (corrective or preventive maintenance, or both) and on the origin of the analysis.

- LSA Studies

In order to carry out the analysis itself, it is necessary to define its form and its content – which is to say that document templates will need to be provided for every type of analysis –

to use the logistic tree structure selected, to identify the connection between the analyses, and to optimize efforts on value-added analyses.

- LSA Progress Conference

This is when the progress of the LSA and BLSA project is shared with the client and when the results of the analysis are consolidated within the BLSA.

8.10.3 Benefit OF ASD S3000L for technical documentation

There are multiple connections between S1000D and S3000L, although they can all ultimately be summed up quite simply:

The information provided by S3000L makes it possible to generate Procedural Data Modules automatically, be it at the level of support information (tooling, ingredients, staff, duration…), or the description of the various steps for a given task, requiring the collection of sub-tasks and their concatenation within the content.

S3000L information allows users to generate the replacement part automatically by generating IPD Data Modules in a similarly automated manner.

S3000L ensures that the coherence is maintained regarding the definition and the evolution of the tasks and the replacement information within the product's life cycle between logistical activities and support and maintenance activities.

In addition, the impact of S3000L does not only affect Tech Pub and S1000D data. It also makes it possible to store and to convey all manner of basic information, be it physical, hierarchical, about maintainability, reliability, or relating to the financial aspect of supplies used in the S2000M provisioning process.

9 References

[1] ISO/IEC/IEEE 15288

[2] INCOSE SE HANDBOOK

[3] Découvrir et comprendre l'IS AFIS

[4] Martin Eigner, Thomas Dickopf, Hristo Apostolov. The Evolution of the V-Model: From VDI 2206 to a System Engineering Based Approach for Developing Cybertronic Systems. 14th IFIP International Conference on Product Lifecycle Management (PLM), Jul 2017, Seville, Spain. pp.382-393, ff10.1007/978-3-319-72905-3_34ff. ffhal-01764166f

[5] ISO/IEC/IEEE 29148:2018

[6] [DORAN 1981] November 1981 issue of *Management Review* contained a paper by George T. Doran called *There's a S.M.A.R.T. way to write management's goals and objectives*.[1][4] It discussed the importance of objectives and the difficulty of setting them.

[7] System Engineering Body of Knowledge Version 2.4

[8] INCOSE-TP-2010-006-03 - Guide for writing requirements

[9] PFA Position paper - AD Safety WG - 2019-V1.0.pdf

[10] VMAD-05-12 AD safety validation - french views - Vdef.pdf, 2020

10 Glossary

Actual manufacturer - An individual, activity, or organization that performs the physical fabrication process that produce the deliverable part or other items of supply for the Government. The actual manufacturer must produce the part in-house. The actual manufacturer may or may not be the design control activity. Acquisition Phases

(a) Concept Exploration and Definition Phase - The identification and exploration of alternative solutions or solution concepts to satisfy a validated need.

(b) Demonstration and Validation Phase - The period when selected candidate solutions are refined through extensive study and analyses; hardware development, if appropriate; test; and evaluations.

(c) Full Scale Development Phase - The period when the system and the principal items necessary for its support are designed, fabricated, tested, and evaluated.

(d) Production and Deployment Phase - The period from production approval until the last system is delivered and accepted.

(e) Operations and Support - The Period following fielding of initial systems which is used to ensure systems continue to provide the capabilities required to meet the identified mission need.

ADS: Autonomous Diving System

Availability - A measure of the degree to which an item is in an operable and committable state at the start of a mission when the mission is called for at an unknown (random) time.

DoD: Department of Defense

capability: Ability to achieve a desired effect under specified standards and conditions through combinations of ways and means to perform a set of tasks [DoD, 7].

Baseline Comparison System (BCS) - A current operational system, or a composite of current operational subsystems, which most closely represents the design, operational, and support characteristics of the new system under development.

Common and Bulk Items List (CBIL) - This list contains those items that are difficult or impractical to list on a top-down/disassembly sequence Provisioning Parts List (PPL), but for which provisioning is essential to support the operation of the end item/equipment. These items are subject to wear or failure, or otherwise required for maintenance, including planned maintenance, of the end item/equipment.

Comparability Analysis - An examination of two or more systems and their relationships to discover resemblances or differences. Computer Resources Support - The facilities, hardware, software, and manpower needed to operate and support embedded computer systems. One of the principal elements of ILS. Constraints - Restrictions or key boundary conditions that impact overall capability, priority, and resources in system acquisition.

configuration [EIA-649C]: (1) The product attributes of an existing or planned product or combination of products: the product and its product configuration information. (2) one of a series of sequentially created variations of a product.

configuration baseline [EIA-649C]: Configuration of a product, at a specific point in time, which serves as a basis for defining change, for conducting verifications, and for other management activities. For a software product, the build baseline includes the actual product.

configuration item (CI) [EIA-649C]: A product, allocated components of a product, or both, that satisfies an end use function, has distinct requirements, functionality and/or product relationships, and is designated for distinct control.

configuration management [EIA-649C]: A technical and management process applying appropriate processes, resources and controls to establish and maintain consistency between product information configuration, and the product.

Contract Data Requirements List (CDRL), DD Form 1423 Series. - A form used as the sole list of data and information which the contractor will be obligated to deliver under the contract, with the exception of that data specifically required by standard Defense Federal Acquisition Regulation (DFAR) clauses.

Contractor - Any individual, partnership, public or private corporation, association, institution, or other entity which enters into a specific contract with the government to provide supplies or services.

Contractors Procurement Schedule for SAIP - Schedule used to acquire information from contractors which will enable the Government to schedule spares procurement to coincide with the contractor's planned procurement for production.

Cost Estimating Relationship (CER) - A statistically derived equation which relates Life Cycle Cost or some portions thereof directly to parameters that describe the performance, operating, or logistics environment of a system.

Corrective Maintenance - All actions performed as a result of failure to restore an item to a specified condition. Corrective maintenance can include any or all of the following steps: Localization, Isolation, Disassembly, Interchange, Reassembly, Alignment, and Checkout.

Data Item Description (DID), DD Form 1664 - A form used to define and describe the data required to be furnished by the contractor. Completed forms are provided to contractors in support of and, for identification of, each data item listed on the CDRL.

Design Change Notice (DCN) - A formal document prepared by a contractor or a Government activity to notify the provisioning activity of changes to previously delivered provisioning lists which add to, delete, supersede or modify items which are approved for incorporation into the end item.

Design Parameters - Qualitative, quantitative, physical, and functional value characteristics that are inputs to the design process, for use in design tradeoffs, risk analyses, and development of a system that is responsive to system requirements.

Effectiveness - A measure of an items ability to meet operational requirements as a function of performance of the hardware, operator/maintainer and environment (operational, social, physical).
System effectiveness takes into account man/machine and man/man interfaces.

Enabling system [1]: system that supports a system-of-interest during its life cycle stages but does not necessarily contribute directly to its function during operation.

End Item - A final combination of end products, component parts, and/or materials which is ready for its intended use; e.g., ship, tank, mobile machine shop, aircraft.

Engineering Data for Provisioning (EDFP) - Data acquired by contract to support Logistic Support Analysis Subtask 401.2.8. This data is necessary for the assignment of Source, Maintenance, and Recoverability (SMR) codes to each Provisioning List Item Sequence Number (PLISN) on the provisioning list. EDFP is also used for assignment of Item

Management Codes, prevention of proliferation of identical items in the Government inventory, maintenance decisions, and item identification necessary in the assignment of a National Stock Number (NSN). Facilities - The permanent or semi-permanent real property assets required to support the materiel system, including conducting studies to define types of facilities or facility improvements, locations, space needs, environmental requirements, and equipment. One of the principal elements of ILS.

environment [1]: system context determining the setting and circumstances of all influences upon a system.

Failure Modes, Effects, and Criticality Analysis (FMECA) - An analysis to identify potential design weaknesses through systematic, documented consideration of the following: all likely ways in which a component or equipment can fail; causes for each mode; and the effects of each failure (which may be different for each mission phase).

Fast Track Program - An acquisition program in which time constraints require the design, development, production, testing, and support acquisition process to be compressed or overlapped.

Follow-on Test and Evaluation (FOTE) - That test and evaluation which is conducted after the production decision to continue and refine the estimates made during previous operational test and evaluation, to evaluate changes, and to evaluate the system to insure that it continues to meet operational needs and retain its effectiveness in a new environment or against a new threat.

Functional Support Requirements (FSR) - A function (transport, repair, resupply, recover, calibrate, overhaul, etc.) that the support system must perform for the end item to be maintained in or restored to a satisfactory operational condition in its operational environment.

Goals - Values, or a range of values, apportioned to the various design, operational, and support elements of a system which are established to optimize the system requirements

Government Furnished Material (GFM) - Material provided by the Government to a contractor or comparable Government production facility to be incorporated in, attached to, used with or in support of an end item to be delivered to the Government or ordering activity, or which may be consumed or expended in the performance of a contract. It includes, but is not limited to, raw and processed materials, parts, components, assemblies, tools and supplies. Material categorized as Government Furnished Equipment (GFE) and Government Furnished Aeronautical Equipment (GFAE) are included.

General Conference - A conference that may be held at any time during the life of the contract for the purpose of resolving provisioning problems.

Guidance Conference - A conference used to ensure that the contractor and the Government have a firm understanding of the contractual provisioning requirements, establish funding and task milestones, and formulate firm commitments for optional requirements in accordance with applicable data requirements.

Integrated Logistic Support (ILS) - A disciplined approach to the activities necessary to: (a) cause support considerations to be integrated into system and equipment design, (b) develop support requirements that are consistently related to design and to each other, (c) acquire the required support; and (d) provide the required support during the operational phase at minimum

cost. Interim Release - Authorization given a contractor to release support items to production or procurement prior to receipt of a provisioned item order (PIO).

Interim Support Items Conference (ISIC) - A conference for the Government to review, select and approve those items recommended for interim support (i.e. contractor supply/logistics support) by the contractor as cost effective for advance procurement prior to the time provisioning for operational requirements has been accomplished and a provisioned item order (PIO) has been provided.

Interim Support Items List (ISIL) - This list contains those support items required between operational need date and the point in time that provisioning for operational requirements has been accomplished.

lifecycle [1]: evolution of a system, product, service, project or other human-made entity from conception through retirement.

Logistic Support Analysis (LSA) - The selective application of scientific and engineering efforts undertaken during the acquisition process, as part of the system engineering and design process, to assist in complying with supportability and other ILS objectives.

Logistic Support Analysis Documentation - All data resulting from performance of LSA tasks conducted under this standard pertaining to an acquisition program.

LSA Guidance Conference - A conference used to ensure that the contractor and the government have a firm understanding of the relationship of the LSA tasks to the LSA documentation, task milestones, and funding levels contractually required. The provisioning guidance conference may be held in conjunction with or as part of the LSA guidance conference if the provisioning activity agrees

Logistic Support Analysis Record (LSAR) - That portion of LSA documentation consisting of detailed data pertaining to the identification of logistic support resource requirements of a system/equipment. See MIL-STD-1388-2 for LSAR data element definitions.

Long Lead Time Items (LLTI) - Those items which because of their complexity of design, complicated manufacturing process, or limited production capacity, cause extended production or procurement cycle which would preclude delivery in time to meet operational need date if not ordered in advance of normal provisioning.

Long Lead Time Items Provisioning Conference (LLTILC) - A conference for the Government personnel to review and select the long lead time items required for support of the end item. Interim Release Items may be reviewed during this conference.

Long Lead Time Items List (LLTIL) - A LLTIL contains those items which, because of their complexity of design, complicated manufacturing process or limited production capacity, may cause production or procurement cycles which would preclude timely and adequate delivery, if not ordered in advance of normal provisioning.

Maintainability - The measure of the ability of an item to be retained in or restored to a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair.

Maintenance Levels - The basic levels of maintenance into which all maintenance activity is divided. The scope of maintenance performed within each level must be commensurate with the personnel, equipment, technical data, and facilities provided.

Maintenance Planning - The process conducted to evolve and establish maintenance concepts and requirements for a materiel system. One of the principal elements of ILS. Manpower - The total demand, expressed in terms of the number of individuals, associated with a system. Manpower is indexed by manpower requirements, which consist of quantified lists of jobs, slots, or billets that are characterized by the descriptions of the required number of individuals who fill the jobs, slots, or billets.

Manpower and Personnel - The identification and acquisition of military and civilian personnel with the skills and the grade required to operate and support a materiel system at peacetime and wartime rates. One of the principal elements of ILS.

Objectives - Qualitative and quantitative values, or range of values, apportioned to the various design operational, and support elements of a system which represent the desirable levels of performance. Objectives are subject to tradeoffs to optimize system requirements.

ontology: representation, formal naming and definition of the categories, properties and relations between concepts, data and entities that substantiate a domain of discourse.

Operating and Support (O&S) Costs - The cost of operation, maintenance, and follow-on logistics support of the end item and its associated support systems. This term and "ownership cost" are synonymous.

Operational Concept - A statement about intended employment of forces that provides guidance for posturing and supporting combat forces. Standards are specified for deployment, organization, basing, and support from which detailed resource requirements and implementing programs can be derived.

Operational Scenario - An outline projecting a course of action under representative operational conditions for an operational system.

Optimization Models - Models which accurately describe a given system and which can be used, through sensitivity analysis, to determine the best operation of the system being modeled.

Operational Design Domain (ODD) [SAE J3016]: Operating conditions under which a given driving automation system or feature thereof is specifically designed to function, including, but not limited to, environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of traffic or roadway characteristic.

organization [1]: group of people and facilities with an arrangement of responsibilities, authorities and relationships

EXAMPLE: Company, corporation, firm, enterprise, institution, charity, sole trader, association, or parts or combination thereof.

Note 1: An identified part of an organization (even as small as a single individual) or an identified group of organizations can be regarded as an organization if it has responsibilities, authorities and relationships. A body of persons organized for some specific purpose, such as a club, union, corporation, or society, is an organization.

[SOURCE: ISO 9000:2005, modified – Note 1 has been added]

Packaging, Handling, Storage, and Transportation - The resources, processes, procedures, design considerations and methods to ensure that all system, equipment, and support items are preserved, packaged, handled, and transported properly including: environmental considerations and equipment preservation requirements for short and long term storage, and transportability. One of the principal elements of ILS.

Parametric Estimating Relationship (PER) - Statistical parametric analysis essentially involves development and application of mathematical expressions commonly called "cost estimating relationships" (CER's). Basically, CER's are developed by statistically analyzing past history to correlate cost with significant physical and functional parameters.

Performing Activity - That activity (government, contractor, subcontractor, or vendor) which is responsible for performance of LSA tasks or subtasks as specified in a contract or other formal document of agreement.

Personnel - The supply of individuals, identified by specialty or classification, skill, skill level, and rate or rank, required to satisfy the manpower demand associated with a system. This supply includes both those individuals who support the system directly (i.e., operate and maintain the system), and those individuals who support the system indirectly by performing those functions necessary to produce and maintain the personnel required to support the system directly. Indirect support functions include recruitment, training, retention, and development,

Post Conference List (PCL) - This list contains those items selected for the operations, maintenance and support of the system/end article as a result of the Provisioning Conference review. Preventive Maintenance - All actions performed in an attempt to retain an item in specified condition by providing systematic inspection, detection, and prevention of incipient failures.

Procuring Activity - The activity which awards contracts for deliverable hardware, software, firmware, courseware and/or data.

product configuration information [EIA-649C]: Information about a product consisting of product definition information and product operational information.

product definition information [EIA-649C]: Information that defines the product’s requirements, documents the product attributes including the process information, and is the authoritative sources for configuration management of the product.

product operational information [EIA-649C]: Information developed from product definition information used to test, operate, maintain and dispose of a product.

Provisioned Item Order (PIO) - A formal requirements document furnished to the contract administration activity to identify items to be bought through the provisioning process on a contract, providing the specific items to be ordered, the estimated cost, and the required delivery schedule and destination. The PIO is provided with other formal contract documentation to the contractor to place items on order. The PIO is an unpriced order.

Provisioning - The process of determining and acquiring the range and quantity (depth) of spares and repair parts, and support and test equipment required to operate and maintain an end item of materiel for an initial period of service.

Provisioning Activity (PA) - That organization of a using Military Service, or that organization delegated by a using Service, which is responsible for the selection of and the determination of requirements for provisioning items.

Provisioning Conference - A conference for reviewing PTD/EDFP, and for Government validation of support items and the assignment of technical and management codes made during the Logistics Support Analysis (LSA) process when specified by the provisioning activity. LSA is the analytical source from which provisioning decisions are made.

Provisioning methods - Method by which the Provisioning Activity (PA) will make provisioning decisions. The method will be specified in the provisioning, requirements. The following provisioning methods are applicable:

(a) **Resident Provisioning Team** (RPT) method - This method employs a Government team permanently assigned at the contractor's facility skilled in the functions of provisioning control, source, maintenance, and recoverability coding, requirements determination, cataloging, etc.

(b) **Conference team method** - This method employs Government representatives at the contractor's or vendor's facility. The conference team is not permanently assigned to the contractor's facility.

(c) **In house method** - The Government conducts provisioning at the PA or at the provisioning activity or other location specified by the prime provisioning activity. Contractor participation will be specified by the PA.

(d) **Logistic Support Analysis Record** (LSAR) method - Functions of provisioning are conducted solely during the periodic LSA reviews, to include the guidance and provisioning conference.

Provisioning Parts List (PPL) - This list structured at the end item, component, or assembly level as specified by the PA, contains the end item, component, or assembly equipment and all support items which can be disassembled, reassembled, or replaced, and which, when combined, constitute the end item, component, or assembly equipment. Provisioning Parts List Index (PPLI) - The PPLI is a listing by manufacturer's reference numbers of all items listed in the Provisioning Parts List (PPL) cross-referenced to each item's Provisioning List Item Sequence Number (PLISN). Provisioning Preparedness Review Conference - This conference is held for the Government to determine the adequacy of the provisioning documentation, facilities, and the overall preparations made by the contractor to conduct a provisioning conference.

Provisioning Technical Documentation (PTD) - PTD as used in this standard, is the generic term used to reference the various types of Provisioning Lists, This term is used by the DoD components for the identification, selection, and determination of initial requirements and cataloging of support items to be procured through the provisioning process. Applicable PTD is as follows:

(a) Provisioning Parts List (PPL)
(b) Short Form Provisioning Parts List (SFPPL)
(c) Long Lead Time Items List (LLTIL)
(d) Repairable Items List (RIL)
(e) Interim Support Items List (ISIL)
(f) Tools and Test Equipment List (TTEL)
(g) Common and Bulk Items List (CBIL)

(h) Design Change Notices (DCN)
(i) Post Conference List (PCL)
(j) System Configuration Provisioning List (SCPL) Readiness Drivers - Those system characteristics which have the largest effect on a system's readiness values. These may be design (hardware or software), support, or operational characteristics.

Reliability –
- The duration or probability of failure-free performance under stated conditions.
- The probability that an item can perform its intended function for a specified interval under stated conditions. (For non-redundant items this is equivalent to definition (1). For redundant items this is equivalent to mission reliability.)

Reliability and Maintainability Interface –
Reliability and maintainability design parameters are a key factor in the design of affordable and supportable systems. R&M parameters provide inputs into the design and LSA process that quantitatively link system readiness to the ILS elements. One of the principal elements of ILS.

Reliability Centered Maintenance - A systematic approach for identifying preventive maintenance tasks for an equipment end item in accordance with a specified set of procedures and for establishing intervals between maintenance tasks.

Repair Parts - Those support items that are an integral part of the end item or system which are coded as non-repairable.

Repairable Items List (RIL) - This list contains all support items of a repairable nature and used in or associated with the end item. Requiring Authority - That activity (government, contractor, or subcontractor) which levies LSA task or subtask performance requirements on another activity (performing activity) through a contract or other document of agreement.

requirement: statement which translates or expresses a need and its associated constraints and conditions [5]

Risks - The opposite of confidence or assurance; the probability that the conclusion reached as to the contents of a lot (number of defects or defective range) is incorrect.

Scheduled Maintenance - Preventive maintenance performed at prescribed points in the item's life.

Sensitivity Analysis - An analysis concerned with determining the amount by which model parameter estimates can be in error before the generated decision alternative will no longer be superior to others.

Short Form Provisioning Parts List (SFPPL) - This list contains only those support items which are recommended by the contractor for maintenance of the end item, i.e. only those items recommended by the contractor as procurable spares. Site Survey - An examination of potential locations and supporting technical facilities for capability to base a system.

SOI: System of Interest

Source, Maintenance and Recoverability (SMR) Codes - Uniform codes assigned to all support items early in the acquisition cycle to convey maintenance and supply instructions to

the various logistic support levels and using commands. They are assigned based on the logistic support planned for the end item and its components. The uniform code format is composed of three, two character parts: Source Codes, Maintenance Codes, and Recoverability Codes in that order.

Spares - Those support items that are an integral part of the end item or system which are coded as repairable.

Spares Acquisition Integrated with Production (SAIP) - A procedure used to combine procurement of selected spares with procurement of identical items produced for installation on the primary system, subsystem, or equipment

Special (tools, test equipment, support equipment) - Tools, test equipment, and support equipment that have single or peculiar application to a specific end item. Standardization and Interoperability.

stage [1]: period within the lifecycle of an entity that relates to the state of its description or realization

Note 1: As used in ISO 15288 standard, stages relate to major progress and achievement milestones of the entity through its lifecycle

Note 2: Stages often overlap

Standardization. The process by which member nations achieve the closest practicable cooperation among forces; the most efficient use of research, development, and production resources; and agree to adopt on the broadest possible basis the use of:

(1) common or compatible operational, administrative, and logistics procedures;

(2) common or compatible technical procedures and criteria;

(3) common, compatible, or interchangeable supplies, components, weapons, or equipment; and

(4) common or compatible tactical doctrine with corresponding organizational compatibility. Interoperability. The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together.

Statement of Prior Submission (SPS) - The SPS certifies that the contractor/subcontractor has previously furnished the Government PTD which satisfies the PTD requirements of the solicitation or the provisioning requirements submitted after award of the contract. The SPS applies to the end item or to any component thereof.

Subcontractor - A contracting entity that furnishes supplies or service to or for a prime contractor or another subcontractor.

Suitability - The degree to which a system can be satisfactorily placed in field use, with consideration being given availability, compatibility, transportability, interoperability, reliability, wartime usage rates, maintainability, safety, human factors, manpower supportability, logistics supportability, and training requirements.

Supply Support - All management actions, procedures, and techniques required to determine requirements for, acquire, catalog, receive, store, transfer, issue, and dispose of secondary items. This includes provisioning for initial support as well as replenishment supply support. One of the principal elements of ILS. Supportability - A measure of the degree to which all

resources required to operate and maintain the system/equipment can be provided in sufficient quantity. Supportability encompasses all elements of ILS, as defined in DoDI 5000.2.

Supportability Assessment - An evaluation of how well the composite of support considerations necessary to achieve the effective and economical support of a system for its life cycle meets stated quantitative and qualitative requirements. This includes integrated logistic support and logistic support resource related O&S cost considerations.

Supportability Factors - Qualitative and quantitative indicators of supportability.

Supportability Related Design Factors - Those supportability factors which include only the effects of an item's design. Examples include inherent reliability and maintainability values, testability values transportability characteristics, etc.

Support Concept - A complete system level description of a support system, consisting of an integrated set of ILS element concepts, which meets the functional support requirements and is in harmony with the design and operational concepts.

Support Equipment - All equipment (mobile or fixed) required to support the operation and maintenance of a materiel system. This includes associated multi-user end items, ground handling and maintenance equipment, tools, metrology and calibration equipment, communications resources, test equipment and automatic test equipment, with diagnostic software for both on and off equipment maintenance. It includes the acquisition of logistics support for the support and test equipment itself. One of the principal elements of ILS.

Support Items - Items subordinate to, or associated with, an end item (i.e., spares, repair parts, tools, test equipment, and sundry materials) and required to operate, service, repair or overhaul an end item.

Support Plan - A detailed description of a support system covering each element of ILS and having consistency between the elements of ILS. Support plans cover lower hardware indenture levels and provide a more detailed coverage of maintenance level functions than support concepts.

Support Resources - The materiel and personnel elements required to operate and maintain a system to meet readiness and sustainability requirements. New support resources are those which require development. Critical support resources are those which are not new but require special management attention due to schedule requirements, cost implications, known scarcities, or foreign markets.

Support System - A composite of all the resources that must be acquired for operating and maintaining a system or equipment throughout its life cycle.

system [1]: combination of interacting elements organized to achieve one or more stated purposes.

Note 1: A system is sometimes considered as a product or as the services it provides.

Note 2: In practice, the interpretation of its meaning is frequently clarified by the use of an associative noun, e.g., aircraft system. Alternatively, the word “system” is substituted simply by a context-dependent synonym, e.g., aircraft, though this potentially obscures a system principles perspective.

Note 3: A complete system includes all of the associated equipment, facilities, material, computer programs, firmware, technical documentation, services and personnel required for operations and support to the degree necessary for self-sufficient use in its intended environment.

System Configuration Provisioning List (SCPL) - This list establishes the family tree relationship of components to end item when associated PLs are developed at a component level. It also includes components which will be government furnished and separately provisioned.

System Engineering Process - A logical sequence of activities and decisions transforming an operational need into a description of system performance parameters and a preferred system configuration.

system of interest [1] (SOI): the system whose life cycle is under consideration in the context of the ISO 15288 International Standard

system of systems (SoS): set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities [DoD, 2004].