TECHNICAL SPECIFICATION

ISO/TS 18667

First edition
2018-02

Space systems — Capability-based Safety, Dependability, and Quality Assurance (SD&QA) programme management

Systèmes spatiaux — Management de programmes de sécurité, de sûreté de fonctionnement et d'assurance de la qualité (SD&QA), axé sur les capacités

Reference number
ISO/TS 18667:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html

This document was prepared by Technical Committee ISO/TC 20, *Aircraft and space vehicles*, Subcommittee SC 14, *Space systems and operations*.

Introduction

This document is intended for use in the engineering community.

The terms Safety, Dependability, and Quality Assurance (SD&QA) are often used interchangeably, but they have very different meanings. *Safety* is the system state with acceptable levels of risk for conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. *Dependability* is the ability of an item or system to perform as and when required. *Quality Assurance* is the part of quality management focused on providing confidence that quality requirements are fulfilled.

This document defines the *"what to do's"* at depths that facilitate consistency in planning and implementing SD&QA programme which identify, assess, and eliminate or mitigate technical risks using levels of effort commensurate with the product's unit-value/criticality and systems engineering life cycle data content/maturity.

The fundamental building blocks of the capability-based SD&QA programme consists of the SD&QA processes identified in Annex A and described in Annex C. The fundamental SD&QA processes are grouped programmatically according to separate SD&QA domains, and functionally according to documented management, engineering, and testing approaches. Annex B defines the tiered criteria used for rating the SD&QA risk management capability of existing SD&QA programme or for planning the desired SD&QA risk management capability of new SD&QA programme. The unique provisions of this document include the following:

— Consistent criteria (see Annex B) for rating the capability of SD&QA programme to identify, analyse, and mitigate or control, potential and existing, product and process deficiencies in a manner that is commensurate with the product's unit-value/criticality (see Table 1) and systems engineering life cycle data content/maturity (see Table 3);

— Structured planning to achieve a predefined level of SD&QA risk management capability for the overall SD&QA programme or any individual SD&QA process through a statement of work (SOW) or memorandum of agreement (MOA);

— Collecting, reviewing, and applying existing lessons learned for rating the maturity of input data used for performing SD&QA analyses;

— Creating and disseminating new lessons learned to sustain continuous improvement of the SD&QA programme through the enterprise.

Space systems — Capability-based Safety, Dependability, and Quality Assurance (SD&QA) programme management

1 Scope

This document applies to the design, development, fabrication, test, and operation of commercial, civil, and military space and ground control systems, sites/facilities, services, equipment, and computer software. Criteria is provided for rating the capability of the entire SD&QA programme or an individual SD&QA process to identify, assess, and eliminate or mitigate risks that threaten safety or mission success. The predefined capability rating criteria define the sequence of activities necessary to achieve a measurable improvement in the effectiveness of SD&QA risk management by implementing it in stages. Organizations can evaluate their existing SD&QA programme against the criteria in this document to identify the activities that need to be added, deleted, or modified to achieve the desired technical risk management effort. The phrase “desired technical risk management effort” means the activities and resources used to identify, assess, and eliminate or mitigate technical risks are commensurate with the product’s unit-value/criticality and systems engineering life cycle data content/maturity.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 10794, *Space systems — Programme management, materials, mechanical parts and processes*

ISO 10795, *Space systems — Programme management and quality — Vocabulary*

ISO 14300-2, *Space systems — Programme management — Part 2: Product assurance*

ISO 14620-1, *Space systems — Safety requirements — Part 1: System safety*

ISO 17666, *Space systems — Risk management*

ISO 23460, *Space systems — Programme management — Dependability requirements*

ISO 27025, *Space systems — Programme management — Quality assurance requirements*

ISO 9000, *Quality management systems — Fundamentals and vocabulary*

NOTE A number of process level documents that are available to aid contractors achieve their safety, dependability, and quality assurance requirements are provided in the Annex D.

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms and definitions given in ISO 10794, ISO 10795, ISO 14300-2, ISO 14620-1, ISO 17666, ISO 23460, ISO 27025, and ISO 9000 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1 Terms and definitions

3.1.1
benchmark
any standard or reference by which others can be measured

3.1.2
best technical practice
documented technique, method, procedure, or process based on a standard or guide, that was developed through experience and research, and is being used as a benchmark by multiple organizations to efficiently obtain prescribed results with consistent quality and to measure against

3.1.3
capability
ability to achieve a desired effect under specified standards and conditions

3.1.4
capability-based Safety, Dependability and Quality Assurance (SD&QA) programme
programme for space and ground control systems that consists of three groups of processes; the Safety programme; the Dependability Programme; and the Quality Assurance Programme, which are pre-tailored to efficiently identify, assess, and eliminate or mitigate specific types of technical risks throughout the product’s mission duration and post-mission disposal

3.1.5
capability-based Safety, Dependability and Quality Assurance (SD&QA) process
individual process that consists of a group of activities which are capable of efficiently identifying, assessing, and mitigating or controlling specified types of technical risks

Note 1 to entry: The list of capability levels is as follows:

— Capability Level 1 process is the minimum set or “base” activities that constitute an appropriate process for a low unit-value/criticality product;

— Capability Level 2 process includes all the Capability Level 1 activities plus additional activities for documenting a procedure, and expanding the comprehensiveness and accuracy of the process to address risks associated with a medium unit-value/criticality product.

— Capability Level 3 process includes all the Capability Level 1 and 2 activities plus additional activities for developing a database, reviewing lessons learned, verifying products and processes, and exchanging SD&QA data throughout the Systems Engineering Process.

— Capability Level 4 process includes all the Capability Level 1, 2 and 3 activities plus additional activities for generating lessons learned, improving the process, and standardizing the formats of empirical and analytical input data used for assessments.

— Capability Level 5 process includes all the Capability Level 1, 2, 3 and 4 activities plus additional activities for continuous improvement of the process.

3.1.6
capability level growth
measurable improvement in the ability of a SD&QA programme or process to support the system safety and mission success needs of a systems engineering process

EXAMPLE An increase in resources, scope of effort, or maturity of input data.

3.1.7
deficiency
amount that is lacking or inadequate

3.1.8
operational safety
level of safety risk to a system, the environment, or the occupational health of personnel caused by another system or end item when employed in an operational environment

3.1.9
product unit-value/criticality categories
five pre-defined categories of products where Category 1 is the lowest value product group and Category 5 is the highest value product group

Note 1 to entry: See Figure D.1.

3.1.10
requirements creep
discovery of one or more new requirements after start of a project, statement of work (SOW), or memorandum of agreement (MOA)

3.1.11
requirements falsification
act of creating one or more false requirements after start of a project, statement of work (SOW), or memorandum of agreement (MOA)

3.1.12
Safety, Dependability and Quality Assurance (SD&QA) programme capability levels
pre-tailored groups of processes that are capable of achieving measurable improvement in comprehensiveness, accuracy, and efficiency, with regard to technical risk identification, assessment, and mitigation, when implemented by transitioning from the lowest process group level (i.e. Capability level 1) through the process group levels (i.e. capability levels) that cumulatively involve a level of effort commensurate with the product's unit-value/criticality and systems engineering life cycle data content/maturity throughout its mission duration and post-mission disposal

Note 1 to entry: The product's unit-value/criticality is provided in Table 1.

Note 2 to entry: The systems engineering life cycle data content/maturity is provided in Table 3.

3.1.13
subject matter expert
SME
person that completed a technical education programme, was formally trained in real-world applications, and has acquired extensive experience in a technical area

3.1.14
system of systems
integration of existing and/or new systems into an over-arching system with capabilities that are greater than the sum of the capabilities of the constituent component systems

3.1.15
validation
confirmation, through objective evidence, that the requirements for a specific intended use or application have been fulfilled

Note 1 to entry: The term "validated" is used to designate the corresponding status.

Note 2 to entry: The use conditions for validation can be real or simulated.

Note 3 to entry: Validation may be determined by a combination of test, analysis, demonstration, and inspection.

3.1.16
verification
confirmation through the provision of objective evidence that specified requirements have been fulfilled

Note 1 to entry: The term "verified" is used to designate the corresponding status.

Note 2 to entry: Confirmation can be comprised of activities such as performing alternative calculations, comparing a new design specification with a similar proven design specification, undertaking tests and demonstrations, reviewing documents prior to issue.

Note 3 to entry: Verification may be determined by a combination of test, analysis, demonstration, and inspection.

3.2 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

A_O	Availability (Operational)
CA	Criticality Analysis
CIRM	Critical Item Risk Management
CDR	Critical Design Review
CN	Criticality Number
DCA	Design Concern Analysis
ESS	Environmental Stress Screening
ETA	Event Tree Analysis
ETC	Estimate to Complete
ESOH	Environment, Safety, and Occupational Health
FDM	Functional Diagram Modelling
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects, and Criticality Analysis
FRACAS	Failure Reporting, Analysis, and Corrective Action System
FRB	Failure Review Board
FTA	Fault Tree Analysis
HA	Hazard Analysis
HW	Hardware
IMS	Integrated Master Schedule
LLAA	Lessons Learned Approval Authority
LOE	Level of Effort
MCLP	Multiple Capability Level Process
MDR	Material Development Requirements
NCRB	Non-Conformance Review Board
NCCS	Non-Conformance Control System
ORR	Operational Readiness Review
PA	Product Assurance
PAP	Product Assurance Plan

PDR	Preliminary Design Review
PMP	Parts, Materials and Processes
PoF	Physics of Failure
PMP	Project Management Plan
PRR	Preliminary Requirements Review
QA	Quality Assurance
R&M	Reliability and Maintainability
RD/GT	Reliability Development/Growth Testing
RMP	Risk Management Plan
SCA	Sneak Circuit Analysis
SEP	Systems Engineering Plan
SPFM	Single Point Failure Mode
SD&QA	Safety, Dependability and Quality Assurance
SSP	System safety programme
SSPP	System safety programme plan
SW	Software
TAAF	Test, Analyse and Fix
TS	Technical Specification
WG	Working Group

4 Objectives, policy and principles — General

4.1 Objectives

The capability-based SD&QA programme is used to identify, evaluate, and eliminate or mitigate technical risks that pose a threat to system safety or mission success, throughout the product's planned mission duration and post-mission disposal. The types of deficiencies addressed include damage-threatening hazards, mission-impacting failures modes, and system performance anomalies that result from unverified requirements, optimistic assumptions, unplanned activities, ambiguous procedures, undesired environmental conditions, latent physical faults, inappropriate corrective actions, and operator errors.

4.2 Policy

The contractor and its subcontractors provide the standards, guides, resources, and training necessary to ensure the SD&QA programme is cost-effectively implemented in accordance with the mandatory SD&QA policy and this document. Optional approaches for eliminating or mitigating[1] each identified technical risk are determined by subject matter experts (SMEs), or they develop rationale for taking no action. The timing of the SD&QA programme accommodates identifying and implementing needed

1) Optional risk mitigations include verifiable controls implemented through special design features, procedures, inspections, or tests.

corrective actions in a timely manner. The data products of the SD&QA programme are made accessible to all major stakeholders. For Capability Level 3 or higher SD&QA programme:

1) establish a database system that can automatically generate a draft SD&QA assessment report; and

2) charter a Lessons Learned Approval Authority (e.g. Lessons Learned Committee) to document lessons learned associated with unacceptable deficiencies.

For Capability Level 4 or higher SD&QA programme, the format of the input and output data of SD&QA computerized tools is compatible with the format of the project SD&QA database system.

4.3 Principles

This document applies to the integration of the SD&QA programme with the project's over-arching systems engineering process. In the context of the systems engineering process, the SD&QA programme is both a "spiral" and a "vector" conglomeration of processes. It's a "spiral" in the sense that the product synthesis loop begins in the first life cycle phase and is repeated in each successive life cycle phase. It's a "vector" in the sense that at the end of each life cycle phase, artifacts and output data are produced to initiate the product synthesis loop in the next life cycle phase.

When specifying this document as a compliance document, consider also specifying other supplementary SD&QA specifications and standards, given those documents define validated methodologies which generate artifacts and data that are consistent with the artifacts and data defined in this document.

Capability-based SD&QA programme include, but are not limited, to the following essential functions:

— **Programme authorization.** Authorize and define the management responsibilities of the appointed leads of the SD&QA programme in accordance with an approved charter, which includes identification of the approval authority for each risk domain and level.

— **Requirements definition.** Internal requirements: Require the SD&QA programme to have appropriately trained, qualified, and supported managers. Require SD&QA activities to be based on best practices, i.e. industry consensus or validated practices. Customer requirements: Define/identify the SD&QA design, procedural, and operational requirements that are consistent with the customer's requirements and this document.

— **Planning.** For Capability Level 2 or higher SD&QA programme, document, approve, and flow down, as necessary, a SD&QA programme plan that identifies the quantitative and/or qualitative SD&QA requirements, the project's SD&QA compliance and guidance documents, and the processes selected to achieve the SD&QA requirements. Describe and interpret as necessary the SD&QA requirements in accordance with the contract and this document. Follow the flow diagram in Figure 1 to develop a detailed plan for each of the three top-level groups of SD&QA programme, i.e. the Safety programme, the Dependability Programme, and the Quality Assurance Programme. Plan the scope of the SD&QA programme to be commensurate with the space system's unit-value/criticality as defined in Table 1, and the space's system life cycle as defined in Table 2. Tailor the seven essential functions of the SD&QA programme to effectively and efficiently integrate with the systems engineering life cycle (see Figures 2 and 3). Identify the types of input data that are available for initiating each SD&QA process and assess its maturity in accordance with the criteria in Table 3.

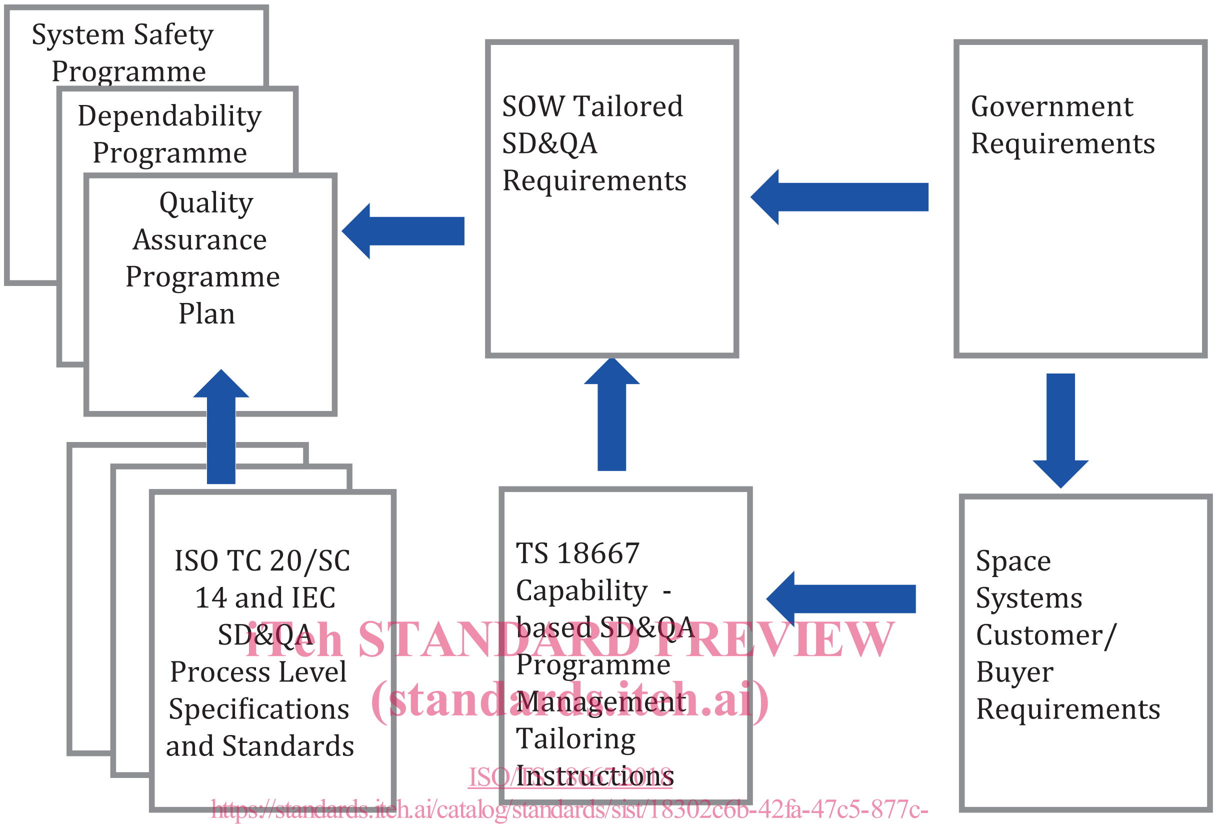

Figure 1 — Example Capability-based SD&QA programme planning flow diagram

For Capability Level 2 SD&QA programme, the SD&QA programme plan is an integral part of the Systems Engineering Plan (SEP). Establish a formal SD&QA programme plan approval process that includes customer review and concurrence. Use the space system unit-value/criticality categorizations defined in Figure D.1 to tailor an entire SD&QA programme or a single SD&QA process, or provide rationale for putting a different space system in one of the unit-value/criticality categories in Figure D.1.

For Capability Level 3 SD&QA programme, the SD&QA programme plan identifies all key inputs and outputs of each SD&QA process. Consider the applicability of process capability-level growth and maturation of analyses input data over the course of the space system's life cycle when planning the SD&QA programme. Update the SD&QA programme plan(s) on an as required or as needed basis. As required updates include those that are contractually required. As needed updates include those necessitated by changes made to the space system's design.

— **Programme coordination.** Coordinate integration of SD&QA processes within the SD&QA programme and with other processes outside of the SD&QA programme, e.g. the Design process, the Manufacturing process, and the Logistics process. Coordinate SD&QA programme planning as necessary to achieve an optimum balance among the design requirements for system safety, reliability, maintainability, operational availability, electromagnetic interference/compatibility, and product quality. Implement the SD&QA programme in a holistic manner that minimizes duplication in effort and maximizes the timely exchange of SD&QA data.

— **Engineering and evaluation.** Define analysis methods based on the space system's unit-value/criticality, the space system's life cycle, and the maturity of the analysis input data. Identify potential and existing deficiencies that pose a threat to system safety or mission success, throughout the space system's planned mission duration and post-mission disposal.

— **Risk assessment and tracking.** Assess initial, intermediate, and final risk for each of the identified deficiencies that may affect the space system's ability to achieve its specified SD&QA requirements. Identify practical mitigations or controls for all unacceptable risks, and track their implementation and verification. Document and categorized all approved residual risks for future reference.

— **Verification.** Apply consistent and measurable verification criteria for the key design parameters of items that are critical to the system safety and mission success of the space system or system of systems. Ensure SD&QA verification activities are properly planned and all applicable requirements successfully met, or instances of non-compliance documented.

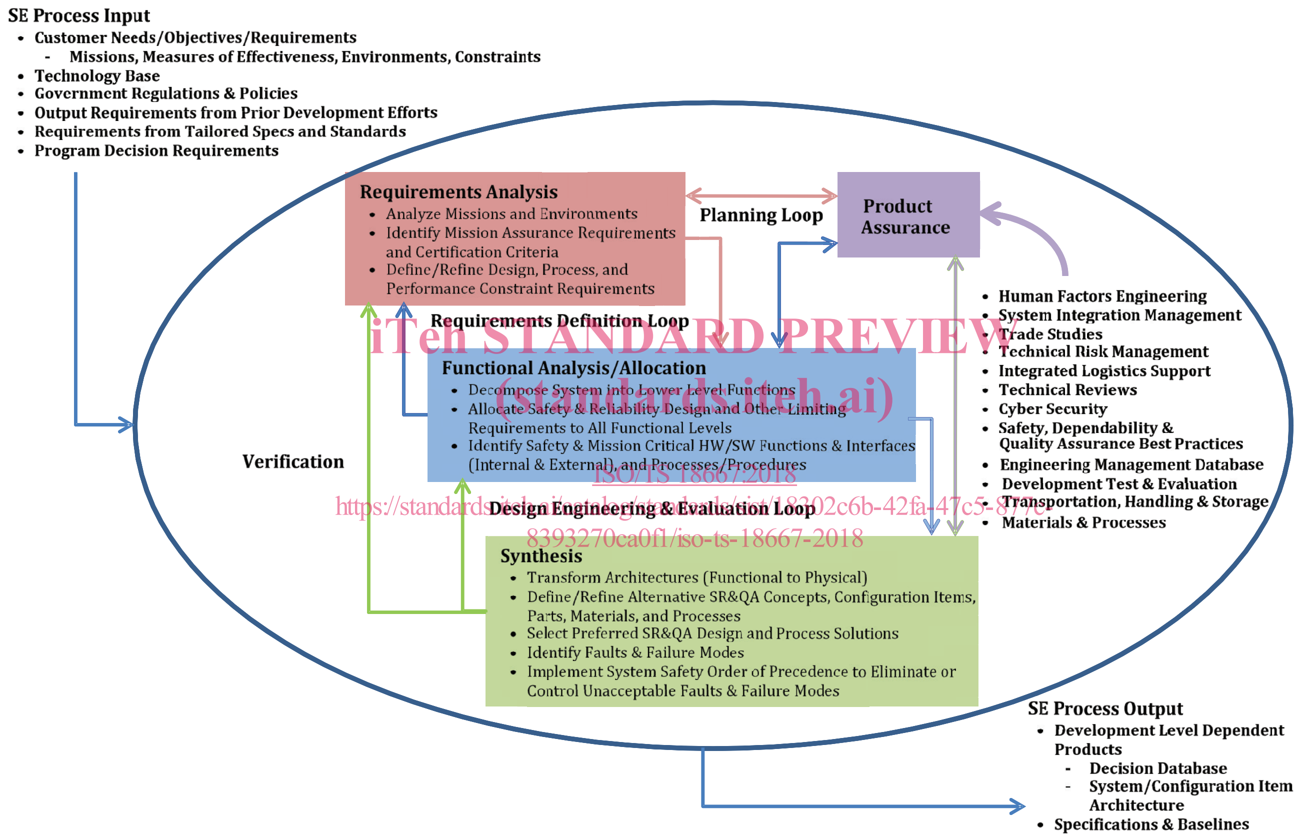

Figure 2 — Example systems engineering process flow

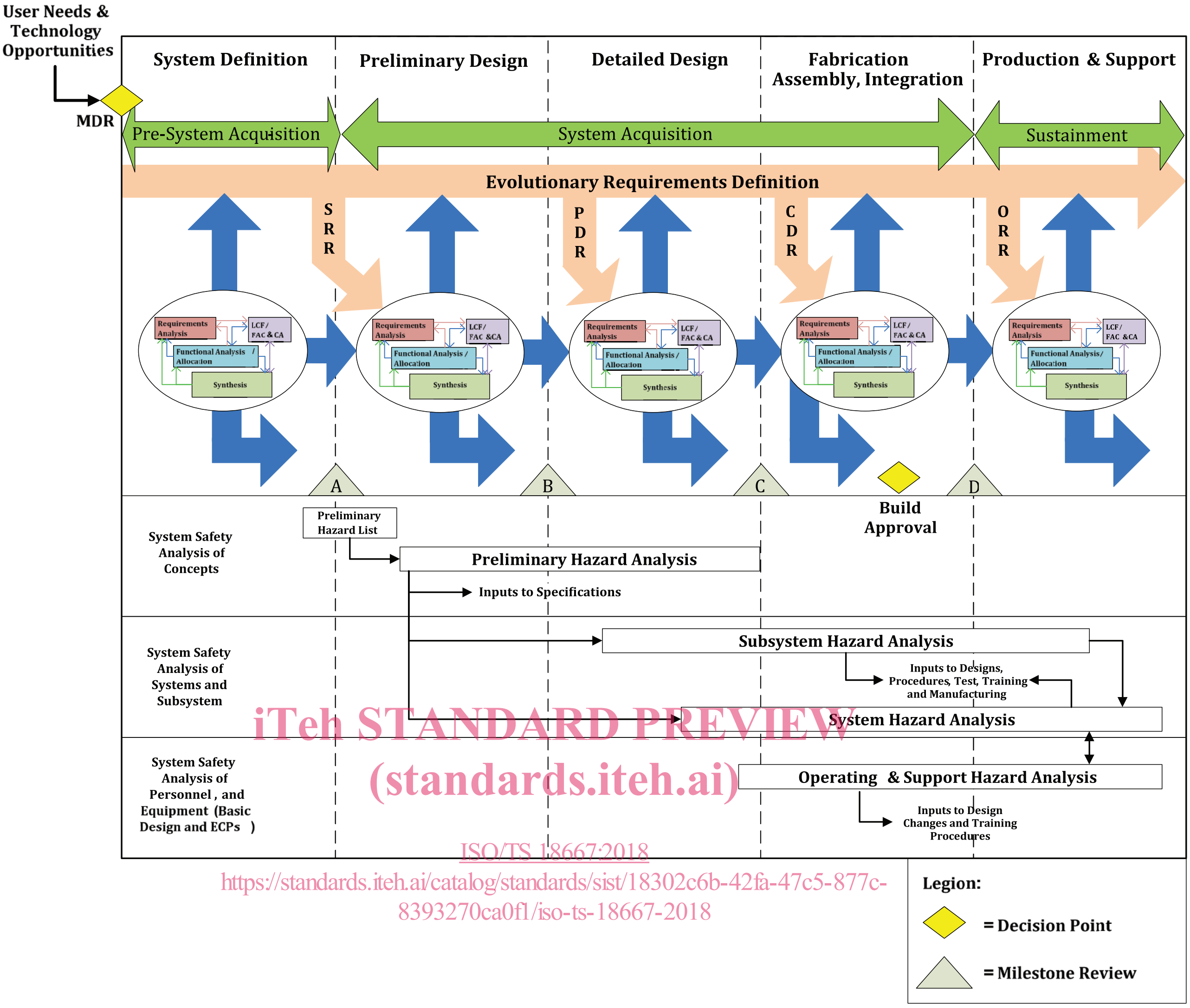

Figure 3 — Example systems engineering process life cycle implementation

5 Instructions

5.1 General

The following instructions pertain to an SD&QA programme of equivalent capability, as defined by Annex B.

5.2 Authorize SD&QA programme

5.2.1 General

For all space systems regardless of unit-value/criticality, either a contract or organizational standard authorizes the creation of a SD&QA programme for a project. The responsibility for managing the SD&QA programme is assigned by the project manager (PM). If a Safety programme, Dependability programme, or QA programme is not authorized to be created in a project, or only partially authorized in accordance with this document, then it is the responsibility of the PM to provide the customer with documented evidence that verifies only negligible or non-credible deficiencies, faults, or weaknesses will be present in the operating space system.