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

Page

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 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.

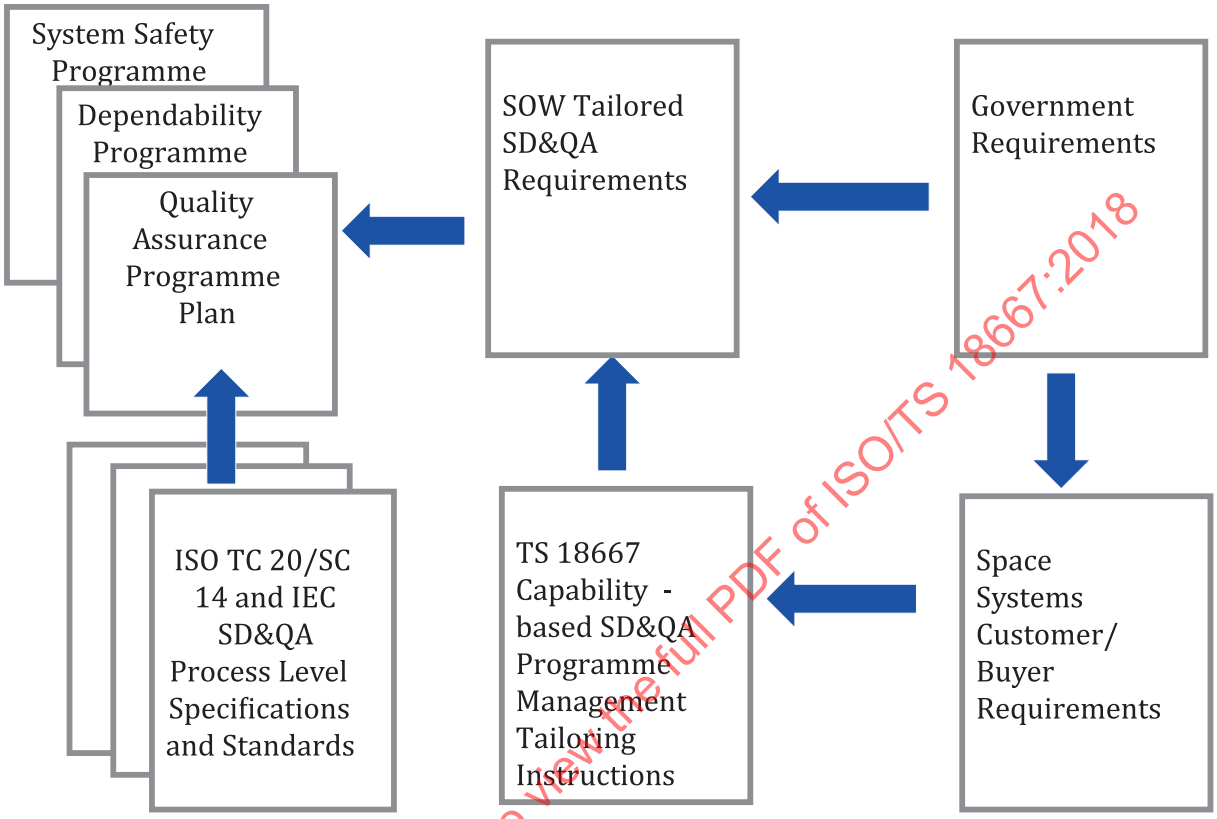


Figure 1 — Example Capability-based SD&QA programme planning flow diagram

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.

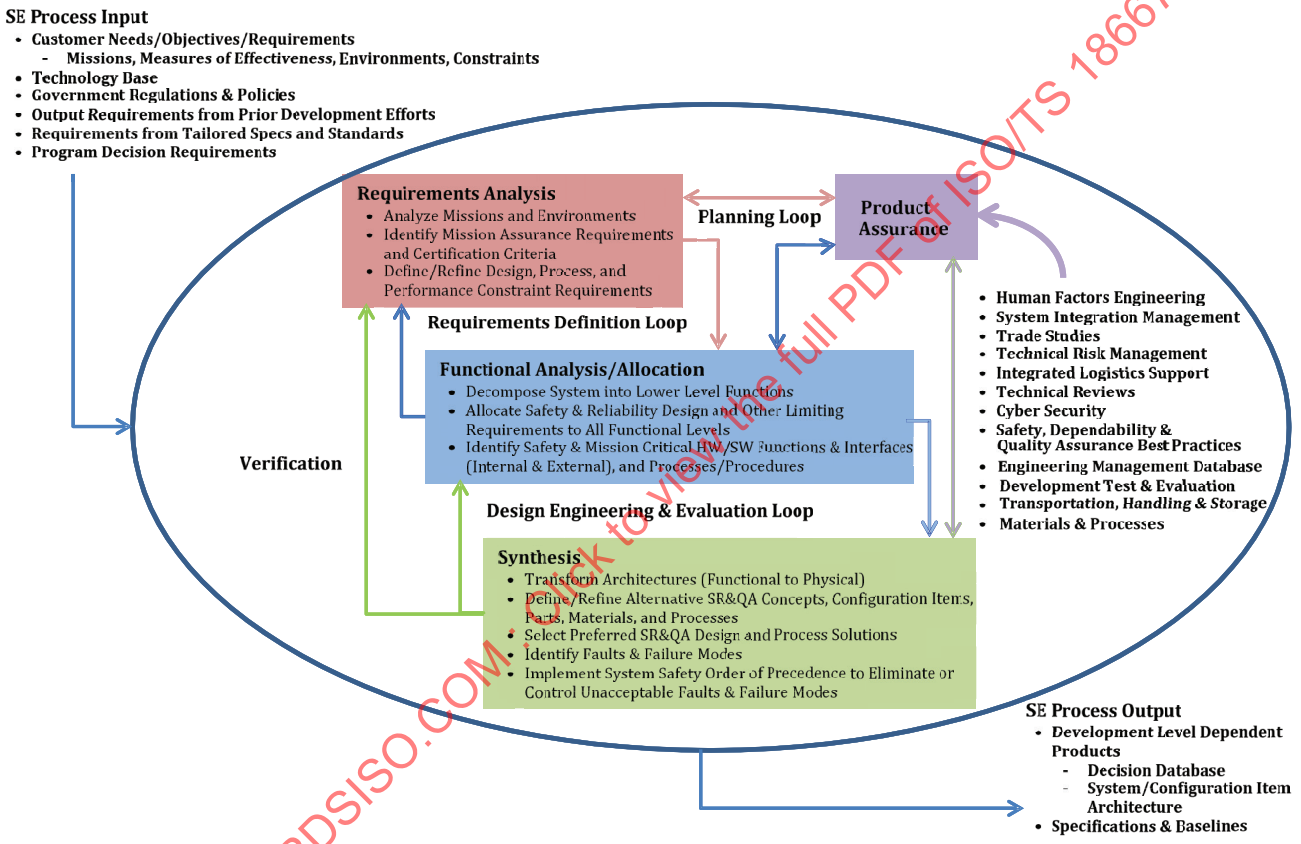


Figure 2 — Example systems engineering process flow

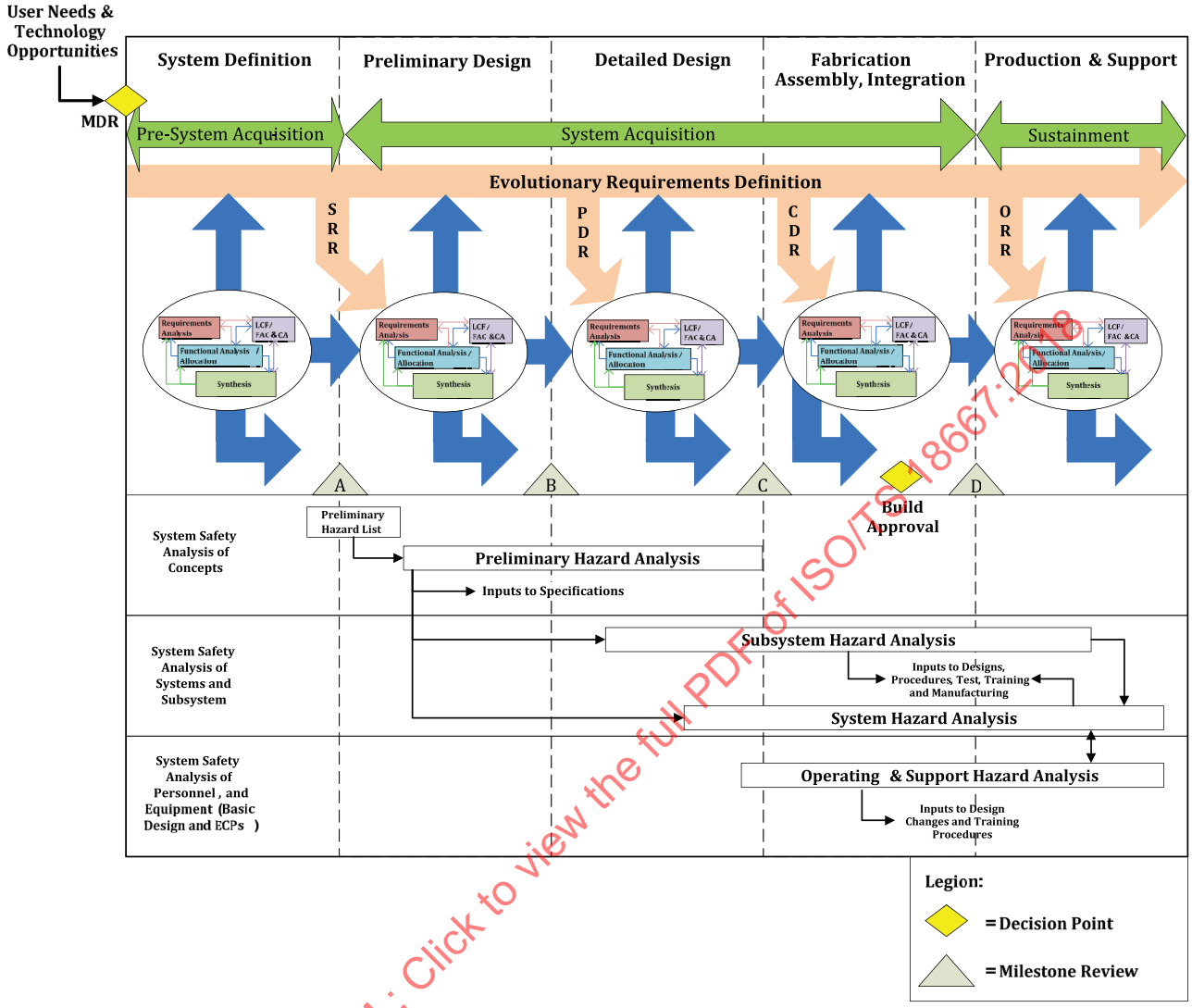


Figure 3 — Example systems engineering process life cycle implementation

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.

5.2.2 Safety programme

The Safety programme lead is assigned responsibility to identify and assess hazards during the design, manufacture, assembly, testing, transportation, and operational phases of the space system or system of systems. Furthermore, the system safety lead is authorized to:

1) ensure all Environment, Safety, and Occupational Health (ESOH) requirements are met;

2) evaluate potential ESOH hazards throughout the space system's life cycle, as applicable; and

3) implement identified operating, manufacturing, and maintenance safety procedures.

5.2.3 Dependability programme

The Dependability programme lead is assigned responsibility to evaluate potential failure modes during the design, manufacture, assembly, testing, transportation, and operational phases of the space system or system of systems. Furthermore, the Dependability programme lead is authorized to:

1) ensure all reliability, maintainability, and availability risks are balanced within the project's objectives, constraints, and budget;

2) assess potential failure modes throughout the space system's life cycle, as applicable; and

3) predict the inherent and operational reliability of the space system or system of systems.

5.2.4 Quality Assurance (QA) programme

The QA programme lead is assigned responsibility to proactively prevent anticipated processing errors during the design, manufacturing, testing, transportation, integration, and operations phases of the space system or system of systems. Furthermore, the QA programme is authorized to ensure all QA requirements are met throughout the space system's life cycle.

5.2.5 Assign qualified managers, leads, engineers, and technicians to SD&QA programme

For Capability Level 3 or higher SD&QA programme, qualification requirements are established for all individuals assigned to the SD&QA programme as managers, leads, engineers, or technicians. The qualification requirements include, but are not limited to, verifiable experience or training necessary to properly develop/acquire and manage/monitor a SD&QA programme plan that is consistent with the instructions in this document.

5.2.6 Continuously improve the SD&QA process

For Capability Level 5 SD&QA programme, an approach is establish to continuously improve the SD&QA processes. The continuous improvement approach includes, but is not limited to the following activities:

— instituting procedures to facilitate the proactive identification and implementation of needed improvements in SD&QA processes;

— periodically training management and engineering personnel in the use of SD&QA tools and the cost-effective implementation of SD&QA processes; and

— integration of SD&QA lessons learned into the training materials. (See ISO 16192).

5.3 Define/identify, assess, and flow down the SD&QA requirements

Define/identify and assess space systems SD&QA requirements that are consistent with the contractual requirements and this document, and flow them down to all affiliated subcontractors. The space

systems SD&QA requirements shall be categorized as design, procedural, or operational. The most typical SD&QA requirements applied to commercial space systems are the following:

— Design:
  — mission reliability;
  — safety-critical/mission-critical item reliability;
  — orbital explosion probability;
  — mean mission duration;
  — launch reliability;
  — LEO/GEO collision probability;
  — disposal manoeuvre reliability;
  — unusually hazardous risks;
— Procedural:
  — safety-critical/mission-critical item control;
— Operational:
  — operational dependability; and
  — re-entry casualty expectation.

Guidelines for defining system safety requirements for space systems are found in ISO 14620-1; guidelines for defining dependability requirements for space systems are found in ISO 23460 and IEC 60300-3-4:2007; and guidelines for defining quality assurance requirements for space systems are found in ISO 27025.

For Capability Level 2 or higher SD&QA programme, the defined/identified SD&QA requirements are documented in an approved SD&QA programme plan. For Capability Level 3 or higher SD&QA programme, the identified SD&QA requirements are assessed using System Requirements Hazard Analysis (SRHA), or an equivalent methodology, to determine the risk of conflicting requirements, requirements creep, requirements falsification, and other undesirable conditions caused by unintended or bad requirements.

5.3.1 Flow down the essential SD&QA requirements

The following SD&QA requirements are considered essential and are flowed and are down to all affiliated subcontractors:

— identify design and process conditions that are unacceptable for safety-critical and mission-critical items;

— mitigate/correct unacceptable design and process conditions or verify acceptability of the associated mishap/failure risk;

— use quantitative risk assessment approaches to verify mission-critical functions for High I unit-value/criticality and above space systems are single-fault tolerant against loss or degradation due to:
  1) a single hardware or software component failure/fault;
  2) propagating failure mode; or
  3) human error;

— use quantitative risk assessment approaches to verify safety-critical functions for High III unit-value/criticality and above space systems are dual-fault tolerant against loss or degradation due to:

  1) dual independent hardware or software component failures/faults;

  2) dual independent human errors; or

  3) a combination of a component failure/fault and a human error;

— use quantified risk assessment approaches to verify High III unit-value/criticality systems do not generate hazardous radiation or energy, when no provisions have been made to protect personnel or sensitive subsystems/components from damage or adverse effects;

— use quantified risk assessment approaches to verify that there is an acceptable level of risk that no packaging, handling or storage procedures will cause a catastrophic accident/mishap for which no controls have been provided to protect personnel or safety-critical/mission-critical equipment;

— identify any SD&QA requirements that can be verified by existing analyses, inspections, test reports, or data products. For Capability Level 2 or higher SD&QA programme, document these requirements and verification methods in approved SD&QA programme plans.

5.3.2 Conflicting SD&QA requirements disposition criteria

Note for cases of conflicting SD&QA requirements, the issue is resolved using the following order of precedence:

1) system safety requirements;

2) availability requirements;

3) reliability requirements; and

4) maintainability and testability requirements.

The order of precedence for SD&QA requirements is based on hierarchical "tiers" of influence each requirement has on the others requirements. System safety requirements are in tier 1 because they drive availability and testability requirements. Availability requirements are in tier 2 because they drive reliability and maintainability requirements. Reliability requirements are in tier 3 because they drive maintainability and testability requirements. Finally, maintainability and testability requirements are in tier 4.

5.4 Planning the SD&QA programme

5.4.1 General

Planning for the SD&QA programme is in accordance with the groups of pre-tailored processes shown in Figures 4, 5 and 6, the Product Unit-Value/Criticality definitions in Figure 1, and the five SD&QA programme capability levels defined in Annex B. Additional guidance for planning the SD&QA programme is found in ISO 14620-1, ISO 23460, ISO 27025, and IEC 60300-3-1:2003.

		Product Unit-Value/Criticality				
	System Safety Programme Processes	**Low**	**Medium**	**High I**	**High II**	**High III**
Safety Programme	System Safety Programme Planning	√	√	√	√	√
	Hazard Analysis	√	√	√	√	√
	Product Safety Testing	√	√	√	√	√
	System Safety Programme Working Group (Includes Data Product Peer Reviews)		√	√	√	√
	Subcontractor and Supplier System Safety Programme Management			√	√	√
	Fault Tree Analysis			√	√	√
	Event Tree Analysis			√	√	√
	Human Reliability Analysis				√	√

Figure 4 — Example pre-tailored system safety programme for space systems (See ISO 14620-1)

		Product Unit-Value/Criticality				
	Quality Assurance Programme Processes	**Low**	**Medium**	**High I**	**High II**	**High III**
Quality Assurance Programme	Quality Assurance Programme Planning	√	√	√	√	√
	Quality Control	√	√	√	√	√
	Configuration Management	√	√	√	√	√
	Failure Reporting, Analysis & Corrective Action System / Non-Conformance Control System	√	√	√	√	√
	Failure Review Board / Non-Conformance Review Board	√	√	√	√	√
	Component Engineering	√	√	√	√	√
	Environmental Stress Screening	√	√	√	√	√
	Critical Item Risk Management		√	√	√	√
	Material Review Board			√	√	√
	Subcontractor and Supplier Quality Assurance Programme Management			√	√	√
	Project SD&QA Database System			√	√	√
	Quality Assurance Programme Working Group (Includes Data Product Peer Reviews)			√	√	√
	Fishbone Analysis				√	√
	Design of Experiments					√

Figure 5 — Example pre-tailored Quality Assurance programme for space systems (See ISO 27025)

		Product Unit-Value Criticality				
	Dependability Programme Processes	**Low**	**Medium**	**High I**	**High II**	**High III**
Dependability Programme	Dependability Programme Planning	√	√	√	√	√
	Functional Diagram Modeling	√	√	√	√	√
	Product Failure Mode, Effects, and Criticality Analysis	√	√	√	√	√
	Component Reliability Predictions	√	√	√	√	√
	Software Component Reliability Predictions		√	√	√	√
	Design Concern Analysis		√	√	√	√
	Worst Case Analysis		√	√	√	√
	Environmental Event/Survivability Analysis		√	√	√	√
	System Reliability Modeling		√	√	√	√
	Maintainability Predictions		√	√	√	√
	Subcontractor and Supplier Dependability Programme Management			√	√	√
	Anomaly Detection and Response Analysis			√	√	√
	Operational Availability Modeling			√	√	√
	Similarity and Allocations Analysis			√	√	√
	Stress and Damage Simulation Analysis			√	√	√
	Structural and Thermal Stress Analysis			√	√	√
	Component Reliability Life Testing			√	√	√
	Dependability Working Group (Includes Data Product Peer Reviews)			√	√	√
	Sneak Circuit Analysis				√	√
	Reliability, Maintainability, and Availability Demonstration Testing				√	√
	Process Failure Mode, Effects, and Criticality Analysis				√	√
	Probabilistic Risk Assessment					√
	Reliability Growth Testing					√
	Ongoing Reliability Testing (ORT)					√

Figure 6 — Example pre-tailored dependability programme for space systems (See ISO 23460)

5.4.2 Select SD&QA processes based on Product Unit-Value/Criticality Categories

Select a group of SD&QA processes that are commensurate with the space system's unit-value/criticality, life cycle phase, and availability/maturity of SD&QA analyses input data.

5.4.3 Define SD&QA process implementation phasing based on systems engineering life cycle phases/milestones

Define the following space system project characteristics:

1) SD&QA activities to be performed in each systems engineering life cycle phase;

2) key inputs of each SD&QA activity, and the source of each key input;

3) key outputs of each SD&QA activity, and the uses of each key output;

4) estimated-time-to-complete (ETC) or level-of-effort (LOE) in hours for each SD&QA activity;

5) key milestones of the SD&QA programme in each systems engineering life cycle phase; and

6) project-wide SD&QA risk management approach, i.e. the methods for monitoring, evaluating, reporting, and responding to anticipated and unanticipated problems. Identify unacceptable product deficiencies mutually with the customer in the SD&QA programme plan.

The following product characteristics are considered unacceptable deficiencies for Category 3 and above space systems, unless quantitative risk assessment methods verify the risk of failure is acceptable:

a. Single point failure modes, common cause failure modes, human errors, or design features which could cause a mishap of catastrophic or critical severity.

b. Human factor hazards involving procedures, component designs or locations that fail to address human physical, anthropometrics, physiological and perceptual-cognitive capabilities or limitations. For example, a design that is conducive to error, such as, controls that are difficult to read, are confusing, or create excessive cognitive demands on the users.

c. Other safety or reliability design conditions that are specified as unacceptable in the contract.

Seamlessly integrate the SD&QA programme with the systems engineering process in a cost-effective manner that achieves an optimum set of SD&QA processes that minimizes duplication in effort. For Capability Level 2 or higher SD&QA programme, document the descriptions of the selected processes in an approved SD&QA programme plan.

Consider the following factors during the selection of SD&QA process activities:

— unit-value criticality of the end product based on the product unit-value/criticality categories defined in Table 1 (or provide rationale for placing a particular class of product in a different unit-value/criticality category);

— applicable product life cycle phases;

— output data requirements, i.e. the required outputs of each SD&QA activity;

— types of input data available for SD&QA analyses;

— applicability of capability level growth, with respect to maturation of the available SD&QA analysis input data;

— types of product deficiencies addressed by SD&QA processes;

— assessment of capability of SD&QA processes to achieve specific SD&QA requirements;

— cost-effectiveness of integration of SD&QA processes with other Systems Engineering processes; and

— avoidance of duplication of effort.

Table 1 — Example Product Unit-Value/Criticality Category Definitions

High III Unit-Value/Criticality Category 5	High II Unit-Value/Criticality Category 4	High I Unit-Value/Criticality Category 3	Medium Unit-Value/Criticality Category 2	Low Unit-Value/Criticality Category 1
— Defence spacecraft — Launch vehicles — Long-range missiles — Nuclear powered space vehicles — Flight termination hardware/software components — Commercial /military manned spacecraft	— Commercial/ communications spacecraft — Experimental manned spacecraft — Short-range missiles/ rockets — Low Earth orbit passenger spacecraft — Safety-critical hardware/ software components — Satellite ground control stations — Radiation hardened spacecraft electronics — Spacecraft explosive devices	— Science/research spacecraft — Small satellites — CubeSats (debris threat) — Mission-critical hardware/software components — Satellite communication ground relay stations — Military computers/ peripherals — Military grade spacecraft electronics — Spacecraft structures /mechanisms — Spacecraft pressure vessels — Landers on comet/planet	— CubeSats micro satellites (non-debris threat) — Industrial grade spacecraft electronics — Industrial computers/ peripherals — Industrial computers/ peripherals — Space experiment equipment — Spacecraft status monitoring hardware/ software components — Computer operating system software programs — Prototype spacecraft systems/ components	— Motorized/manual spacecraft assembly tools — Spacecraft insulation materials — Computer application software programs

Specific SD&QA processes are implemented throughout the space system life cycle to eliminate or mitigate specific SD&QA risks or issues. Table 2 provides an example of the applicability of the SD&QA process capability levels in the space system life cycle.

Table 2 — Example space systems SD&QA process capability level life cycle matrix

Space Systems Unit-Value/ Criticality Level	Life Cycle Phase				
	Conceptual Systems Definition Phase	Preliminary Design Phase	Detailed Design Phase	Fabrication, Assembly, Integration and Test Phase	Delivered Product Operation and Service Phase
Low	Capability Level 1 Processes	Capability Level 1 Processes	Capability Level 1 Processes	Capability Level 1 Processes	Capability Level 1 Processes (*)
Medium	Capability Level 1 Processes	Capability Level 2 Processes	Capability Level 2 Processes	Capability Level 2 Processes	Capability Level 2 Processes (*)
High I	Capability Level 1 Processes	Capability Level 2 Processes	Capability Level 3 Processes	Capability Level 3 Processes	Capability Level 3 Processes (*)
High II	Capability Level 1 Processes	Capability Level 2 Processes	Capability Level 4 Processes	Capability Level 4 Processes	Capability Level 4 Processes (*)
High III	Capability Level 1 Processes	Capability Level 2 Processes	Capability Level 4 Processes	Capability Level 5 Processes	Capability Level 5 Processes (*)

(*) indicates that the process capability level only apply to changes that occur during the space system's life cycle phase.

5.4.4 Identify the SD&QA guidance sources

For Capability Level 2 or higher SD&QA programme, identify the documents used as guidance for the SD&QA programme, including industry standards and enterprise-level documented practices. Other sources of guidance include best practices and design rules that are recommended by technical papers and books published by engineering experts.

5.4.5 Establish the Technical Performance Metrics

For Capability Level 2 or higher SD&QA programme, establish Technical Performance Metrics (TPMs) for the purpose of tracking and reporting the progress of each SD&QA programme.

5.5 Coordinate the SD&QA processes with other product assurance processes

5.5.1 General

The SD&QA programme leads or their representative participate in product design reviews, technical interchange meetings, management status reviews, working group meetings, and any other meetings held by the project that may be germane to system safety, dependability, or quality assurance.

5.5.2 Coordinate Project's and Subcontractor's SD&QA Activities

The SD&QA progrmme leads coordinate the project's and subcontractor's SD&QA activities during product design, manufacture, test, inspection, shipping, storage, operation, sustainment, and disposal.

For Capability Level 2 or higher SD&QA programme, the SD&QA programme plans define the essential elements of each SD&QA activity/method based on the product's unit-value/criticality, life cycle

milestones/phases, output data requirements, and types/maturity of available input data. This information provides the basis for establishing a SD&QA Integrated Master Schedule (IMS), which is essentially a comprehensive predecessor and successor dataflow matrix for planning and tracking SD&QA activities. The IMS is used to the greatest extent practical to schedule and track planned SD&QA risk management activities across the project.

For Capability Level 3 or higher SD&QA programme, the SD&QA programme leads ensure that the project and its subcontractors provide SD&QA data products in predefined formats to facilitate integrating and processing large amounts of data for component, assembly, subsystem, and system level SD&QA analyses, tests, and inspections.

5.5.3 Establish, utilize, and maintain a project SD&QA database system

For Capability Level 3 or higher SD&QA programme, an integrated project-wide SD&QA database system is established, utilized, and maintained. The database contains all the key SD&QA requirements and data products, has data change control and tracking features; and can automatically generate SD&QA programme plans and reports, e.g. a computerized evaluation of the SD&QA programme plan with regard to a measure of comprehensiveness. The SD&QA lead ensures timely utilization of the SD&QA database system to the greatest extent practical by the project functions, such as, Design, Manufacturing, Test, and Risk Management. The reports generated by the database include the results of hazard analyses, FMECAs, FTAs, and ETAs.

5.6 Apply engineering and evaluation methods to identify system and process deficiencies

5.6.1 General

Apply validated engineering and evaluation principles and techniques to identify existing and potential system and process deficiencies, including unacceptable safety design or reliability design conditions as instructed in 5.3.2e. Identify practical methods for avoiding, eliminating, or controlling unacceptable safety or reliability design conditions, and for verifying that the implemented mitigation/disposition methods are successful.

The prerequisite for performing a thorough and accurate failure mode, effects, and criticality analysis, or hazard analysis (FMECA/Hazard Analysis), is to first understand how the system operates and its mission success criteria. The SD&QA lead ensures that the project's SD&QA engineers are provided with detailed and comprehensive functional diagram models for all indenture levels of the system.

The contractor and customer mutually establishes the unacceptable design criteria. The unacceptable design criteria are determined from special studies, analyses, simulations, historical data, and test results. The unacceptable design criteria are used to further evaluate requirements and designs to see if they are acceptable.

5.6.2 Define the system failure criteria and identify failure modes

Define the system failure criteria. For Capability Level 2 or higher SD&QA programme, document the failure criteria in an approved SD&QA programme plan. Assign a severity category to each identified failure mode or hazard based on the worst case end effects on the system or mission. Estimate the probability of occurrence as either a quantitative or qualitative value. Quantitative probability values are actually ranges that are relative to (i.e. a percent of) the accepted overall probability of failure (POF) of the space system. For example, if a satellite's required design reliability is 0,85, then its acceptable probability of failure is 0,15. The rationale for selecting a qualitative probability value is documented in sufficient detail by the subject matter expert (SME) to allow other people that independently assess the same SD&QA risk to at least understand the logical flow of the SME's decision-making process. Examples of failure mode severity categories and probability levels are provided in Table 3.

In the absence of data to perform a quantitative probability analysis, it may be necessary to determine qualitative probability values that are based solely on engineering judgment or a best guess. Whenever

engineering judgment or a best guess is used to justify accepting a high or serious residual risk, then the source(s) of that engineering judgment or best guess is documented in the risk acceptance memorandum, along with a statement of the number of years of verified experience with reliability assessments on similar space systems, equipment, or processes.

Table 3 — Example failure mode severity categories and probability levels

Category/Level	Example of quantitative probability level thresholds	Example of qualitative probability level ranges	Safety severity categories (according to ISO 14620-1	Dependability severity categories (according to ISO 23460)	Example of dependability severity categories for redundant items
1	(E) FREQUENT The probability of occurrence value is greater than or equal to 10^{-1}. $X > 10^{-1}$	(E) FREQUENT The probability of occurrence value's range is greater than 10 % of the acceptable overall system probability of failure (POF) during a specified operating time interval or number of operating cycles.	CATASTROPHIC Loss of life, life-threatening or permanently disabling injury or occupational illness, loss of an element of an interfacing manned flight system loss of launch site facilities or loss of system; severe detrimental environmental effects.	CATASTROPHIC Complete loss of mission: complete loss of primary mission capability.	
2	(D) PROBABLE The probability of occurrence value is less than 10^{-1} but greater than or equal to 10^{-2}. $10^{-1} > X > 10^{-2}$	(D) PROBABLE A probability of occurrence value's range is between 1.0 % and 10 % of the acceptable overall system POF, during a specified operating time interval or number of operating cycles.	CRITICAL Temporarily disabling but not life-threatening injury, or temporary occupational illness; major damage to flight systems or loss or major damage to ground facilities; major damage to public or private property; or major detrimental environmental effects.	CRITICAL Major loss or degradation of the primary mission: capability to complete some mission objectives (or all at a degraded level) with immediate loss of a critical science instrument; or loss of a major amount of critical science data; or major reduction in life of the primary mission; or loss of spacecraft function resulting in loss of opportunity for obtaining critical science data.	
3	(C) OCCASIONAL The probability of occurrence value is less than 10^{-2} but greater than or equal to 10^{-3}. $10^{-2} > X > 10^{-3}$	(C) OCCASIONAL The probability of occurrence value's range is between 0,1 % and 1,0 % of the acceptable overall system POF, during a specified operating time interval or number of operating cycles.	MARGINAL Minor injury, minor occupational illness, or minor system or environmental damage.	MAJOR Minor loss or degradation of the primary mission: minor loss of spacecraft or instrument function leading to loss of a minor amount of critical science data; or a significant reduction in life of the primary mission; or loss or major degradation of an ancillary mission.	1R - Loss or degradation of a redundant subsystem or science instrument, which would result in a severity category 4 if remaining redundancy is lost.

Table 3 *(continued)*

Category/Level	Example of quantitative probability level thresholds	Example of qualitative probability level ranges	Safety severity categories (according to ISO 14620-1	Dependability severity categories (according to ISO 23460)	Example of dependability severity categories for redundant items
4	(B) REMOTE The probability of occurrence value is less than 10^{-3} but greater than or equal to 10^{-6}. $10^{-3} > X > 10^{-6}$	(B) REMOTE The probability of occurrence value's range is between 0,01 % and 0,1 % of the acceptable overall system POF, during a specified operating time interval or number of operating cycles	NEGLIGIBLE Less than minor injury, occupational illness, or less than minor system or environmental damage.	MINOR/NEGLIGIBLE Potential for less than minor loss or degradation of spacecraft or performance: no immediate impact on spacecraft or primary mission, but potential exists for future loss, at severity levels 3 to 5, due to induced failure or resulting from the conjunction of this anomaly with a future event; or potential for cumulative major loss of a mission-critical function over a long period of time; or spacecraft or primary mission loss or significant degradation, at severity level 4, would occur if adequate redundancy, alternatives, or compensating measures are not implemented; or minor degradation of an ancillary mission.	2R - Loss or degradation of a redundant subsystem or science instrument, which would result in a severity category 3 if the remaining redundancy is lost.
5	(A) IMPROBABLE/NON-CREDIBLE The probability of occurrence value is less than 10^{-6}. $10^{-6} > X$	(A) IMPROBABLE / NON-CREDIBLE The probability of occurrence value's range is less than 0,01 % of the acceptable overall system POF during a specified operating time interval or number of operating cycles.			3R - Loss or degradation of a redundant subsystem or science instrument, which would result in a severity category 2 if the remaining redundancy is lost.
NOTE When several severity categories can be applied to the system or system component, the highest severity takes priority.					

5.6.3 Assess maturity of key input data, constraints, ground rules, and analytical assumptions

For Capability Level 4 or higher SD&QA programme, evaluate the maturity of the input data used for SD&QA analyses (e.g. analytical assumptions, constraints, and ground rules) in the context of the Systems Engineering Plan (SEP) and the Table 4 criteria.

Table 4 — Example SD&QA engineering and evaluation input data maturity rating criteria

HIGH	MEDIUM	LOW
Based on statistically significant field, test, or simulation data	Based on averaged field, test, or simulation data	Based on handbook data or engineering judgment

5.7 SD&QA risk assessment and control

5.7.1 Integrate SD&QA with programme-wide technical risk management processes

Integrate the SD&QA processes with the project-wide, closed-loop risk management process shown in Figure 7 in accordance with this document and ISO 17666. The main steps in this process are risk identification, risk mitigation, risk tracking, and risk acceptance. Unacceptable risks are identified, analysed, and tracked throughout the product life cycle until mitigated or controlled to an acceptable level.

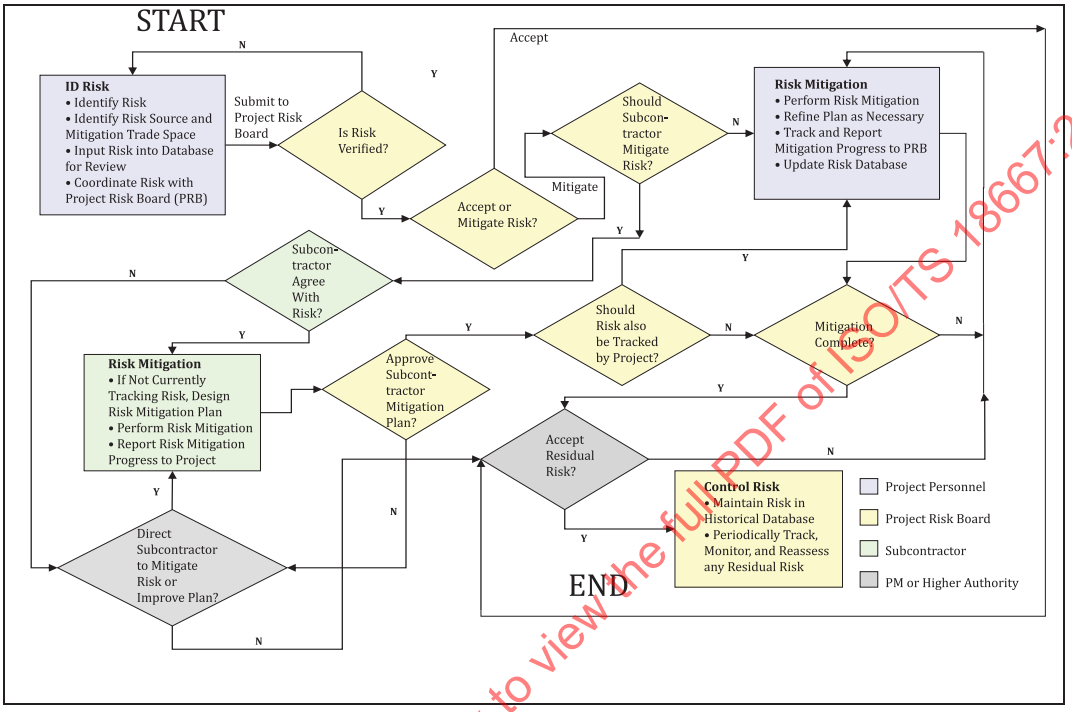


Figure 7 — Example closed-loop risk management process

5.7.2 SD&QA risk management responsibilities

The SD&QA risk management responsibilities defined in this subclause facilitate establishing a uniform and repeatable approach to identify, flow up, mitigate or control, and track significant project risks. Each SD&QA risk is assessed with respect to severity of potential failure cause/hazard, probability of occurrence, worst case end effects/mishaps, and system or process related residual risks. All high and serious risks are accepted by the appropriate level of authority. The risk management responsibilities of the SD&QA programme leads include, but are not be limited to, the following activities:

— ensuring the approach for SD&QA risk management is documented in the contractor's internal SD&QA standards and the project's risk management plan (RMP);

— ensuring the management of SD&QA risk is appropriately addressed in the project's RMP;

— providing guidance to project personnel for performing initial risk assessments using qualitative methodologies when quantitative probability data are not available;

— appointing SD&QA representatives in accordance with ISO 14300-2 who are qualified by training or experience to perform SD&QA functions (see safety representative qualification requirements in ISO 14620-1:2002, 4.2.2);

— identifying and reporting instances of significant residual risk to project management;

— translating all risk matrices to 5x5 for reporting purposes if the risks are not already being managed in that format;

— identifying and managing safety-critical and mission-critical items;

— monitoring the SD&QA processes to ensure they are performed in accordance with the Integrated Master Schedule (IMS) and the project's budget; and

— assisting the identification and avoidance of anticipated or unplanned events that may affect the product's safety/reliability design or the project's schedule/budget.

5.7.3 SD&QA Programme Self-Inspections

For Capability Level 4 or higher SD&QA programme, perform a self-inspection at least annually using the criteria in Table 5:

Table 5 — Example SD&QA Programme Self-Inspection Criteria

SD&QA PROGRAMME ESSENTIAL ELEMENTS	SELF-INSPECTION CRITERIA
Programme authorization	Does the contractor have an industry acknowledged basis for authorizing its Safety, Dependability and Quality Assurance (SD&QA) Programme?
	Are the SD&QA programme authorized to interface with outside industry organizations and working groups whose charter/goal is to continuously improve industry recognized Safety, Dependability and Quality Assurance practices?
	Does the contractor have the necessary resources on hand to facilitate effective execution of the SD&QA programme in a cost-efficient manner?
	Does the contractor have empowering policies in place that facilitate efficient execution of the SD&QA programme?
Requirements definition	Are all SD&QA requirements identified in the contractor requirement documents?
	Has the contractor demonstrated a thorough understanding of all SD&QA requirements?
	Are there any SD&QA process which may have requirements that duplicate, contradict, overlap, supersede, or circumvent requirements of another SD&QA process?
	Are overlooked or missing SD&QA requirements identified and reported as residual risks?
Planning (including SD&QA test plans)	Are all applicable SD&QA requirements and self-imposed objectives identified in the SD&QA programme plans?
	Are all of the measureable and level-of-effort (LOE) SD&QA tasks that are associated with each SD&QA requirement and self-imposed objective identified in the Product Assurance Plan or Integrated Master Schedule (IMS), and the SD&QA programme plans?
	Are all of key outputs/artifacts identified for each SD&QA task throughout the space system's life cycle?
	Are overlooked, missing, or deficient tasks identified and reported as residual risks?
Programme coordination	Are customer submittals and internal exchange data products identified and mapped to giver and receiver organizations and individuals?
	Are system safety inputs to customer submittal data products properly developed, approved, coordinated, distributed, and maintained?
	Are all stakeholders provided with checklists that enhance mishap avoidance?
	Are stakeholders monitored to ensure they properly apply the checklists?

Table 5 *(continued)*

SD&QA PROGRAMME ESSENTIAL ELEMENTS	SELF-INSPECTION CRITERIA
Engineering and evaluation	Does system safety and reliability engineering participate early and proactively in the system design or modification process?
	Are the appropriate system safety engineering methods selected to achieve all of the design safety and operational safety requirements?
	Are the appropriate reliability engineering methods selected to achieve all of the design reliability, operational reliability, and reliability growth requirements?
	Are the selected engineering methods validated to be effective means of achieving the design requirements prior to use?
	Are the input data and assumptions used in engineering assessments evaluated for accuracy prior to application?
Risk assessment and tracking	Are risk assessment metrics identified and within compliance of requirements?
	Is the appropriate approval authority for high and serious risks identified?
	Is the risk mitigation/control order of precedence defined, implemented, and tracked (including hazardous material controls)?
	Are all high and serious residual risks identified and properly reported?
Verification (including SD&QA Testing)	Have applicable military, federal, national, international, and industry safety standards and codes been identified and have the approach for verifying compliance with each been defined and concurred with by the customer?
	Have the test, demonstration, analysis, or inspection approach for verifying compliance with each system safety, mission reliability, and quality assurance requirement been defined and concurred with by the customer?
	Have all SD&QA requirements verification plans and reports been properly documented, approved, implemented, and tracked?
	Are SD&QA requirements verification results evaluated in terms of meeting requirement thresholds and determining residual risks?

5.7.4 SD&QA risk identification

The project-wide identification of SD&QA risks is coordinated by SD&QA leads by providing project personnel with technical assistance, training, and checklists. SD&QA risk identification is performed within the context of the project's overall risk taxonomy. An example of a project's overall risk taxonomy is provided in Table 6.

Table 6 — Example risk taxonomy for a space system development

Technical risks
— Technology maturation
— Systems engineering & integration
— Requirements analysis
— Functional analysis/allocations
— Synthesis
— Product assurance
— Engineering databases
— Technical Performance Measures
— Environment, Safety, and Occupational Health (ESOH)
— Reliability, Availability & Maintainability (RAM)
— Quality Assurance (QA)
— System security/cybersecurity
— Human Systems Integration (HSI)
— Interoperability
— Test & evaluation
— Manufacturing
— Supportability
Programmatic Risks
— Estimates
— Programme planning
— Programme execution
— Communication
— Contract structure/provisions
— Schedule
Business (external)
— Dependencies
— Resources
— Priorities
— Regulations/laws
— Market
— Customer
— Weather

SD&QA risk identification is focused on the following areas of technical risk: Environment, Safety and Occupational Health (ESOH); Mission Success (MS); and Quality Assurance (QA). SD&QA risk assessment is focused on identifying the sources of SD&QA risks, such as, part failure modes, conflicting or missing requirements, design weaknesses, and hazardous processes and procedures. The results of these assessments are captured in FMECA, Hazard Report (HR), and similar fault/failure analysis reports. Typical SD&QA risk sources included in these assessments are:

— suppliers/vendors;

— immature technology;

— extreme operating environment (space, desert, etc.);

— new design/process;

— high level of design complexity/skill level;

— tight tolerance requirements;

— new operational requirements (customer needs);

— new SD&QA requirements (safety, reliability, maintainability, availability, or quality assurance);

— changing requirements;

— engineering change proposals (ECPs), specification change notices (SCNs), software problem reports (SPRs), and requests for deviations and waivers;

— cost and schedule estimating assumptions;

— resource availability (people, materials, facilities, tools, etc.);

— under-qualified personnel (design, engineering, production, etc.);

— SD&QA technique/method/process is not a best technical practice; and

— limited SD&QA programme capability.

The SD&QA leads monitor project personnel to ensure they regularly practice the following risk assessment activities:

1) Review pertinent Lessons Learned Logs to identify any associated failure causal factors (i.e. hazards) that are not addressed by programme planning.

2) Review programme generated documents in a timely manner to identify any potential failures, deficiencies, accidents, and incidents whose associated hazards are not addressed by programme planning.

3) Review closed failure, deficiency, accident, incident, and non-conformance reports to identify any associated hazards that are not addressed by programme planning.

4) Assess the hazard's potential impacts on programme domains (i.e. safety, performance, cost, schedule, technology, and data) for all identified hazards that are not addressed by programme planning.

5) Ensure a FMECA record, or similar documented record, exists for each identified High and Serious hazard risk.

6) Provide a documented record of each identified SD&QA risk to the SD&QA lead for entering into the project's risk management database or hazard tracking log.

5.7.5 Qualitative SD&QA risk likelihood assessment

Qualitative risk source likelihood scales similar to the examples shown in Table 7, are used for initial SD&QA risk assessments where the risk source is known but insufficient data are available to develop a quantitative probability of occurrence. The technical risk assessment process is an iterative process where the maturity of the probability factor is low at the beginning of the product development phase and increases in accuracy at a rate commensurate with the progress made in the systems engineering process.

Table 7 — Example of Qualitative Probability Indicators for Programme Functions

Probability Level	Risk Sources						
	Requirements	**Technology**	**Resources**	**Designs**	**Processes and Plans**	**Integration**	**System/Data Security**
Frequent (1) (>30 %)	No validation by customers or users and no allocations	New technology with uncharacterized performance and producibility	Required staffing and facilities undefined; Required staffing and facilities unavailable	Commercial off-the-shelf (COTS) components and assemblies with standardized integration or recommended applications	Few or no critical processes, plans, and associated metrics for compliance verification are appropriately defined/ documented	Experienced with systems that are not similar and most or all of the interfaces are different	No audits, inspections, or training to verify personnel understand security requirements and are managing risks
Probable (2) (>20 % to <30 %)	Incomplete validation by users or customers and/or incomplete allocations	Significant modifications to existing technology with only partially characterized performance and producibility	Required staffing and facilities incompletely defined; Availability of staffing and facilities undetermined	COTS components and assemblies with minor modifications to standardized integration or recommended applications	Most critical processes, plans, and associated metrics for compliance verification are appropriately defined/ documented	Experienced with systems that are somewhat similar but many or most of the interfaces are different	No audits and very infrequent inspections/ training to verify personnel understand security requirements and are managing risks
Occasional (3) (>10 % to <20 %)	System requirements validated by users or customers but flowdown incomplete	Moderate modifications to existing technology with performance characterized, but producibility only partially characterized	Required staffing and facilities incompletely defined; Staffing and facilities available with shortfalls	COTS components and assemblies with major modifications to standardized integration or recommended applications	All critical processes, plans, and associated metrics for compliance verification are appropriately defined/ documented	Experienced with similar systems but some of the interfaces are different	Bi-annual audit/ inspection/training minimally to verify personnel understand security requirements and are managing risk
Remote (4) (>1 % to <10 %)	Requirements documented and validated by users and customers and allocated to interfaces and major programme elements	Minor modifications to existing technology with conservative performance and producibility characterization	Required staffing and facilities completely defined; Staffing and facilities available with shortfalls	New components or assemblies with fully characterized performance and manufacturability	All critical processes, plans, and associated metrics for compliance verification are appropriately defined/ documented, and reviews indicate successful results	Experienced with similar systems that have similar interfaces	Annual audits minimally and occasional inspections/training to verify personnel understand security requirements and are managing risk

Table 7 *(continued)*

Probability Level	Risk Sources						
	Requirements	**Technology**	**Resources**	**Designs**	**Processes and Plans**	**Integration**	**System/Data Security**
Improbable (5) (<1 %)	Requirements documented and validated by users and customers and flowed down to major subsystems/ components	Off-the-shelf or minor modifications to technology successfully applied in previous programs	Required staffing and facilities completely defined; Staffing and facilities available without shortfalls	New components or assemblies with uncharacterized performance or manufacturability	All critical processes, plans, and associated metrics for compliance verification are appropriately defined/ documented, and trending indicates successful results	Experienced with very similar systems that have very similar or identical interfaces	Semi-annual audits minimally and frequent inspections to verify personnel understand security requirements and are minimizing risk

5.7.6 Quantitative SD&QA risk likelihood assessment

Initial assessments of high and serious SD&QA risks are periodically updated until high fidelity quantitative risk likelihood data can be fully developed. Quantitative risk likelihood scales similar to the examples shown in Table 8, are used for final risk assessments of high and serious SD&QA risks where the risk source is known and sufficient data are available to develop a quantitative probability of occurrence.

Table 8 — Example of Fixed Quantitative Probability Levels for Programme Domains

	Rating	Technical Risks	Performance Risks	Safety Risks	Cost/ Schedule Risks
Likeli-hood	5 - Improbable	<0,1 %	<1 %	<0,000 1 %	<1 %
	4 - Remote	0,1 % to 1 %	1 % to 10 %	0,000 1 % to 0,1 %	1 % to 10 %
	3 - Occasional	1 % to 10 %	10 % to 20 %	0,1 % to 1 %	10 % to 20 %
	2 - Probable	10 % to 20 %	20 % to 30 %	1 % to 10 %	20 % to 30 %
	1 - Frequent	>20 %	>30 %	>10 %	>30 %

5.7.7 SD&QA risk mitigation assessment

Apply the following risk mitigation order of precedence when selecting SD&QA failure/hazard risk mitigation or control methods:

1) **Eliminate faults through design selection.** Ideally, the risk of a failure mode is eliminated. This elimination is often accomplished by selecting a design alternative that removes the fault altogether;

2) **Reduce risk through design alteration.** If the risk of a failure mode cannot be eliminated by adopting an alternative design or alternative material, consider design changes that reduce the severity and/or the probability of a failure mode;

3) **Incorporate engineered features or devices**. If the risk of a failure mode is unable to be eliminated or adequately mitigated through a design alteration, reduce the risk using an engineered feature or device. In general, engineered features actively interrupt the failure mechanism sequence and devices reduce the risk of a failure mode;

4) **Provide warning devices.** If engineered features and devices do not adequately lower the risk of the failure mode, include a detection and warning system to alert personnel to the presence of a faulty condition or occurrence of an undesirable latent event.

5) **Develop procedures and training.** Where other risk reduction methods cannot adequately mitigate the risk from a failure mode, incorporate special procedures and training. Procedures may prescribe the collection of diagnostics or prognostics data. Warnings, cautions, and other written advisories are not the only risk reduction method used for high and serious initial risk levels.

5.7.8 SD&QA risk tracking

Beginning with the start of the system definition phase, and continuing throughout all subsequent product life cycle phases, the SD&QA programme leads periodically review the open SD&QA risks to assess status of risk mitigation efforts. They also assess the impact of changes in the Work Breakdown Structure (WBS) budget or Integrated Master Schedule (IMS) which they are responsible for managing.

5.7.9 SD&QA risk level assessment

5.7.9.1 General

Following determination of the likelihood level and consequence category of the risk, use the ISO 17666 compliant 5x5 risk matrix in Figure 8 and plug in the probability and severity values to assess the criticality of the risk (i.e. Green = LOW, Yellow = MEDIUM, Red = HIGH).

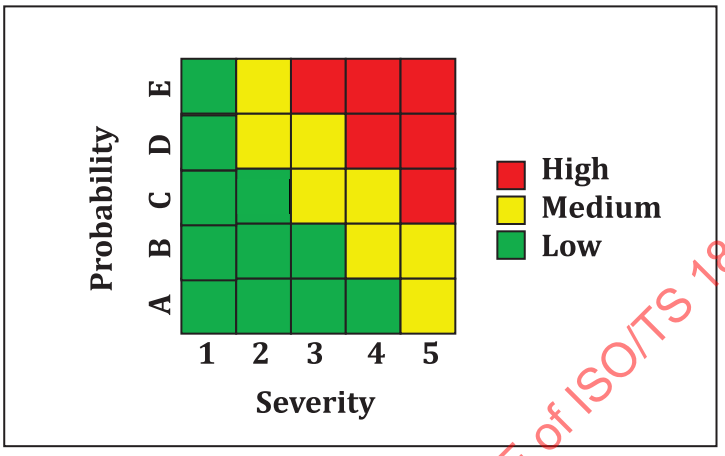


Figure 8 — Example ISO 17666 compliant 5x5 risk matrix

5.7.9.2 High risk

If a risk is determined to be High or Red then a detailed risk assessment is performed. The type and depth of this risk assessment may vary based on the project domain affected and the data collected. The kinds of results obtained from a detailed risk assessments include:

— finer resolution of likelihood and consequence estimates;

— ability to expose and rank specific contributions to the risk;

— an opportunity to express the uncertainty in these estimates explicitly, and to identify a means of reducing these uncertainties; and

— an opportunity to break down the likelihood and consequences into their constituents, enabling a better understanding of the composition of the risk and an improved ability to develop mitigation plans.

The results of the detailed risk assessments are documented formally in the project's risk database by the Project Risk Management Board (PRMB). The topics covered in the formal documentation are include the risk management scope, purpose, objectives, approach, results, and conclusions. The conclusions include a comparison of the estimated cost and schedule impacts on the overall project if the risk were to be realized and if it is mitigated. If the status of the risk changes due to new data being collected after completion of the detailed risk assessment, then the risk is reassessed by the risk owner and resubmitted to the PRMB for review and concurrence.

5.7.9.3 Medium risk

A preliminary risk assessment is performed on Medium or Yellow risks. The type and depth of this risk assessment is determined by the risk owner. The kinds of results obtained from a preliminary risk assessment include:

— gross resolution of likelihood and consequence estimates;

— ability to identify and rank generic contributions to the risk;

— an expression of likelihood in terms of point estimates and identification of means of determining uncertainties; and

— an engineering estimate of the composition of the risk to allow development of mitigation plans.

As in the cases of High and Serious risks, the results of all preliminary risk assessments are documented formally by the PRMB in the risk management database.

5.7.9.4 Low risk

Low or Green risks are considered insignificant risk drivers. These risks represent hazards, faults, or failure modes that have little or no adverse impact and/or probability of occurrence. No risk assessments are conducted or mitigation plans developed for low risks. Low risks are archived by the PRMB in the risk database and reviewed periodically, e.g. quarterly to ensure that new data has not been collected that would warrant changing the status of the risk. Should the risk status change, the risk items are reassessed by the risk owner and resubmitted to the PRMB for review and concurrence.

5.7.10 Separate ESOH/system safety risk management

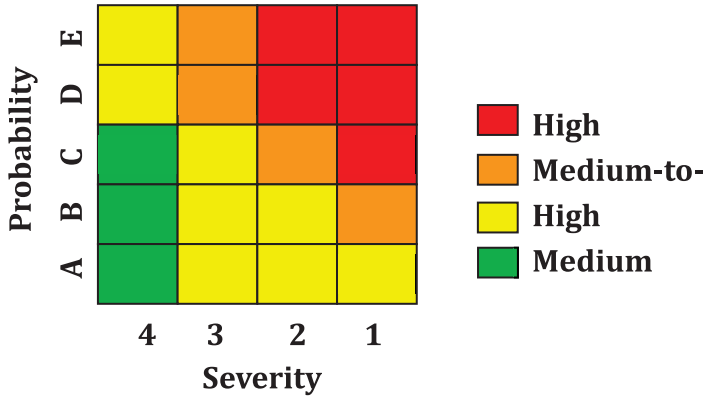
The management of Environment, Safety, and Occupational Health (ESOH)/system safety risks has some unique requirements imposed by a number of government instructions, policies, laws, and regulations. As a result of these requirements, the contractor may be required to manage ESOH/system safety risks separately from all other project domain risks. In cases where system safety risks are managed separately from all other programmatic risks, e.g. in accordance with the ISO 14620-1 methodology, the project manager (PM) provides a direct line of communication to the system safety lead to ensure safety risks receive proper attention. Safety risks that represent a significant cost or schedule risk are captured in the programme risk management database.

ESOH/system safety risks are analysed, mitigated or controlled, and tracked throughout the product life cycle in the same manner as the other SD&QA risks. Also, the ESOH/system safety risks and the other SD&QA risks are reported at all major project reviews and to the customer using the ISO 17666 5x5 risk matrix.

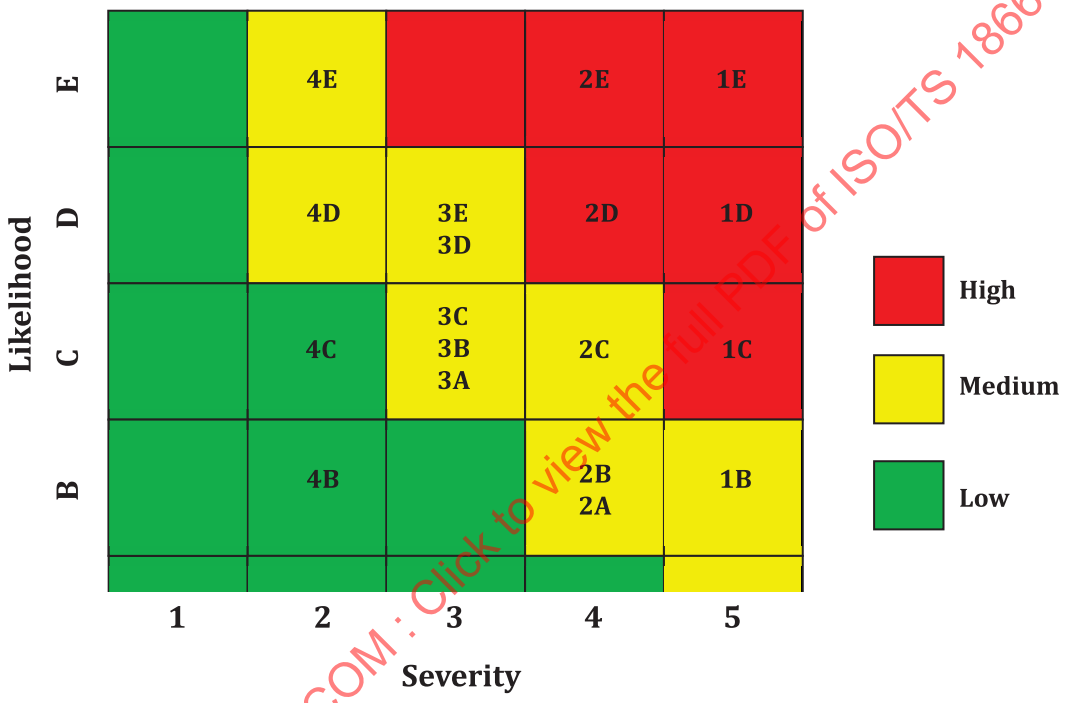
5.7.11 Present SD&QA risk status using a single risk matrix format

For Capability Level 4 or higher SD&QA programme, the project manager (PM) presents all high and medium risks that were assessed using the ISO 17666 risk assessment methodology, as a part of all major milestone reviews, along with the corresponding risk mitigation plans for each risk. All high and medium risks that were assessed using the ISO 14620-1 hazard severity assessment methodology or the ISO 23460 event severity assessment methodology, are translated from the 4x5 risk matrix format to the 5x5 risk matrix format described in ISO 17666 prior to being reported by the PM. Figure 9 provides an example of a template used to translate a 4x5 risk matrix to a 5x5 risk matrix.

Figure 10 provides an example of a risk prioritization approach for determining the order in which risks are addressed when limited funds are available to handle/mitigate risks. This risk prioritization approach is implemented by replacing the 'A' thru 'E' likelihood designations of the ISO 17666 risk matrix with '1' through '5', and then assigning sequential numbers from '1' through '25' to each block in the ISO 17666 risk matrix. The lowest level risk block is located in the bottom left corner of the ISO 17666 risk matrix (i.e. likelihood × severity = 1 × 1 = 1). This block is assigned the lowest rank value of '1'. The next lowest level risk block is located directly above the '1' block (i.e. likelihood × severity = 2 × 1 = 2), and it is assigned the rank value of '2'. Continuing this procedure, the next lowest level risk block is directly adjacent to the '1' block (i.e. likelihood × severity = 1 × 2 = 2), and it is assigned the rank value of '3'. Note even though the likelihood and severity products of blocks '2' and '3' are both equal to 2, the risk level of block '3' is ranked a higher than block '2' because the severity of block '3' is higher, i.e. its severity level is 2 versus severity level 1 of block '2'. This block numbering schema is continued until all 25 blocks in the risk matrix are assigned a unique number.



a) Example ISO 23460 and ISO 14620-1 compliant 4x5 risk matrix



b) Example ISO 17666 compliant 5x5 risk matrix

Figure 9 — Example ISO 23460 or ISO 14620-1 to ISO 17666 risk matrix translation matrix

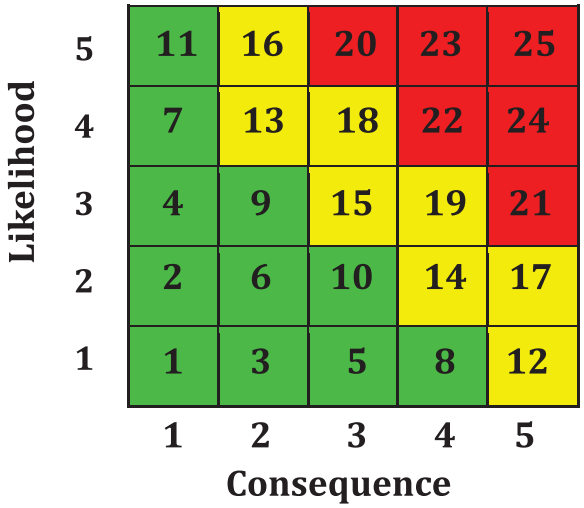


Figure 10 — ISO 17666 risk prioritization matrix

An example application of the Risk Matrix Translation Matrix in Figure 9 is provided below. In this example, the Risk Matrix Translation Matrix in Figure 9 is applied to the ISO 17666 Risk Prioritization Matrix in Figure 10. The result is the following ranking of ISO 23460 and ISO 14620-1 risk matrix blocks from highest to lowest.

25 – 1E
24 – 1D
23 – 2E
22 – 2D
21 – 1C
20 –
19 – 2C
18 – 3E
3D
17 – 1B
16 – 4E
15 – 3C
3B
3A
14 – 2B
2A
13 – 4D
12 – 1A
11
10
09– 4C
08
07
06 – 4B
05
04
03 – 4A
02
01

5.7.12 Perform structured SD&QA reviews

For Capability Level 5 SD&QA programme, develop and apply a structured review process (e.g. a formal peer review working group) to aid thorough evaluation of the SD&QA data products in all product life cycle phases. The peer review team includes personnel who are cognizant of events that led to failures in systems similar to the one being developed. Product-based and process-based lessons learned that are relevant to the system being developed are gathered from across the enterprise and used to develop review checklists that support timely implementation of the structured review process and updating of the SD&QA programme. The review checklists reflect the technical knowledge, insights, design rules, application data, and other clues that help uncover latent deficiencies.

5.7.13 Apply SD&QA lessons learned

Proposed lessons learned are evaluated for quality, prioritized, and forwarded to the Lessons Learned Approval Authority for appropriate action. The contractor takes steps to ensure that proposed lessons learned are documented and reviewed in a timely manner, and the related recommendations are infused throughout the project, the stakeholder organizations, and as necessary, enterprise-wide using the appropriate systems. The project's SD&QA database system includes a field that allows an authorized person to tag particular data as a proposed lessons learned. A positive indication in the lessons learned field generates a notification to the Lessons Learned Review Committee, or similar approval authority, regarding the data's candidacy. Further guidance for processing lessons learned is found in ISO 16192.

For Capability Level 3 or higher SD&QA programme, describe in an approved plan how existing SD&QA data/reports will be reviewed for applicable product-based[2)] and process-based[3)] lessons learned. Existing lessons learned are reviewed to identify possible deficiencies or needed process improvements, such as, improved procedures or training materials.

For Capability Level 4 or higher SD&QA programme, describe in an approved plan how SD&QA lessons learned will be exchanged with other projects throughout the enterprise, e.g. the project will transmit approved SD&QA lessons learned to other projects for information and comments.

For Capability Level 5 SD&QA programme, describe in an approved plan how non-proprietary lessons learned data will be exchanged with other organizations, e.g. the enterprise will enter into data exchange agreements and employ safeguards to protect security classified, International Traffic in Arms Regulations (ITAR)-restricted, proprietary, or other sensitive data. The received data will be reviewed by an enterprise-level Lessons Learned Board to identify significant findings that are implemented in a project.

5.8 Verify SD&QA requirements are met

Document verification of each quantitative and qualitative SD&QA requirement. The project manager or chief engineer is to choose one or more of the following methods to verify each SD&QA requirement:

— test;

— demonstration;

— analysis;

— inspection;

— simulation; and

— similarity.

For a Capability Level 3 or higher SD&QA programme, the planning for validating SD&QA requirements is documented in a Requirements Verification Plan (RVP), and includes descriptions of the verification methods to be applied. The Space Systems Safety-critical and Mission-critical Unacceptable Conditions Checklist in Annex D is used to aid in the development of a RVP that is commensurate with the unit-value criticality of the space system. The results of the RVP are documented in a Requirements Verification Report (RVR) that is provided to the customer for review.

2) For this document, a product-based lesson learned is important information created, documented, and retrieved according to a system or device life cycle specific functional or physical descriptor.

3) For this document, process-based lesson learned is important information created, documented, and retrieved according to a process or procedure descriptor.

Annex A
(informative)

Fundamental SD&QA Processes

When using the SD&QA processes named in this annex to plan the SD&QA programme, integrate them as necessary with the management, engineering, and test functions in the project. The SD&QA processes are the fundamental building blocks of the SD&QA programme. Annex C provides a brief definition of each SD&QA process with regard to its purpose and functional description.

SD&QA Management Process Group:

1) SDS&QA programme planning;
2) Subcontractor and supplier SD&QA programme management;
3) SD&QA programme working groups;
4) Failure reporting, analysis, and corrective action system;
5) Failure review board/non-conformance review board;
6) Critical item risk management;
7) Project SD&QA database system;
8) Quality control;
9) Configuration management; and
10) Material review board.

SD&QA Engineering Process Group:

1) Functional Diagram Modelling;
2) System Reliability Modelling;
3) Component Reliability Predictions;
4) Product Failure Mode, effects, and Criticality Analysis;
5) Sneak Circuit Analysis;
6) Design Concern Analysis;
7) Structural and Thermal Stress Analysis;
8) Worst Case Analysis;
9) Human Reliability Analysis;
10) Environmental Event Survivability Analysis;
11) Anomaly, Detection, and Response Analysis;
12) Maintainability Predictions;
13) Operational Availability Modelling;

14) Hazard Analysis;

15) Software Component Reliability Predictions;

16) Process Failure Mode, Effects, and Criticality Analysis;

17) Event Tree Analysis;

18) Fault Tree Analysis;

19) Fishbone Analysis;

20) Similarity and Allocations Analysis;

21) Component Engineering;

22) Stress and Damage Simulation Analysis; and

23) Probabilistic Risk Assessment.

SD&QA Test Process Group:

1) Environmental Stress Screening;

2) Reliability Growth Testing;

3) Reliability, Maintainability, and Availability Demonstration Testing;

4) Component Reliability Life Testing;

5) Design of Experiments;

6) Ongoing Reliability Testing; and

7) Product Safety Testing.

Annex B
(informative)

Capability-based Safety, Dependability and Quality Assurance Programme tailoring requirements template

B.1 The Capability Level 1 Safety, Dependability and Quality Assurance (SD&QA) Programme include the following activities.

B.1.1 Authorization of the contractor's SD&QA organizations which are assigned the responsibility and authority for meeting the SD&QA requirements and objectives. The following independent programme are authorized at a minimum: a Safety programme, a Dependability programme, and a Quality Assurance (QA) programme.

— Assign qualified management and engineering personnel, and obtain the tools needed to cost-effectively implement the SD&QA programme. Use validated methods to identify and eliminate or control of unacceptable deficiencies, as required.

B.1.2 Identification of appropriate SD&QA requirements. The SD&QA requirements are consistent with the contractual requirements and this document. At a minimum, define and flow down to all affiliated subcontractors that produce safety-critical and mission-critical items the following essential SD&QA requirements:

— the design conditions that are considered unacceptable;

— mitigate/correct unacceptable design conditions or verify acceptability of the mishap/failure risk levels associated with the unacceptable design conditions;

— verify mission-critical functions are single-fault tolerant against loss or degradation due to a single hardware or software component failure/fault, propagating failure, or human error; or verify acceptability of the risk of loss or degradation of the mission-critical functions using quantified risk assessment approaches;

— verify safety-critical functions for High III unit-value/criticality products are dual-fault tolerant against loss or degradation due to dual independent hardware or software component failures/faults, dual independent human errors, or a combination of a component failure/fault and a human error; or verify acceptability of the risk of loss or degradation of the safety-critical functions using quantified risk assessment approaches;

— verify the system does not generate hazardous radiation or energy, when no provisions have been made to protect personnel or sensitive subsystems/components in High III unit-value/criticality products from damage or adverse effects;

— verify, via quantified risk assessment approaches, that there is an acceptable level of risk that no packaging, handling or storage procedures will cause a catastrophic accident/ mishap for which no controls have been provided to protect personnel or safety-critical/ mission-critical equipment;

— identify any SD&QA requirements which may be satisfied by an existing analysis, inspection, test report, or data product from a similar project, product, or process. For Capability Level 2 or higher SD&QA programme, document these requirements in approved SD&QA programme plans.

B.1.3 In lieu of formally approved project SD&QA programme plans, use this document and ISO 14300 to define a set of Capability Level 1 SD&QA processes which comprise the "basic" SD&QA programme that is tailored to achieve the minimum acceptable level of SD&QA risk.

NOTE The basic SD&QA programme constitutes the minimum effort required to eliminate or mitigate specific technical risks for a specific systems engineering life cycle phase of a low unit-value product.

B.1.4 Coordination of SD&QA activities with other functions in the project's Product Assurance process.

NOTE Coordinate the interactions required for successful implementation of each SD&QA process.

B.1.5 Implementation of the Capability Level 1 SD&QA programme, which represents the minimum effort required to eliminate, mitigate, or accept specific technical risks of a low unit-value/criticality system/product, during specific phases of its life cycle. The following activities are included, at a minimum, in the Capability Level 1 SD&QA programme:

a) Construction of detailed and comprehensive functional diagram models of the system;

b) Definition of the system's failure criteria; and

c) Identification of the system's failure modes and their qualitative probabilities of occurrence.

B.1.6 Implementation of product and process risk management principles that are consistent with this document and ISO 17666.

B.1.7 Identification of formal and informal methods which will be used to verify the SD&QA requirements are met. The formal verification methods involve review and concurrence by the customer. Product Safety Testing is performed in a formal manner. The informal verification methods involve review and concurrence by internal management only.

B.1.8 Documentation of all applicable SD&QA requirements and the associated assessment results in a single report for each SD&QA process that is implemented.

NOTE The SD&QA assessment reports are updated on an "as required" or "as needed" basis. "As required" updates are triggered by scheduled events, e.g. is contractually required delivery times. "As needed" updates are triggered by unscheduled events, e.g. changes made to the system or project which affect the integrity of data in the report.

B.2 The Capability Level 2 SD&QA programme include all the tasks in the Capability Level 1 SD&QA programme plus the following at a minimum.

B.2.1 Change B.1.5 to, "Implementation of the Capability Level 2 SD&QA programme, which represents the minimum effort required to eliminate, mitigate, or accept specific technical risks of a medium unit-value/criticality system/product, during specific phases of its life cycle. The following activities are included, at a minimum, in a Capability Level 2 SD&QA programme".

B.2.2 Development of the SD&QA programme plans, which are formally approved by internal management and the customer, and include but is not limited to the following topics:

— unit-value/criticality of the end product based on the product unit-value/criticality categories defined in Table 1;

— product's life cycle phases;

— all applicable SD&QA requirements;

— types of hazards and failure modes associated with product;

— SD&QA assessment method(s) to be used to verify each SD&QA requirement;

— objectives and approach of each planned SD&QA process;

— input data sources and output data users for each SD&QA process;

— estimated time to complete (ETC) or level of effort (LOE) to complete each SD&QA process;

— applicability of capability level growth, with respect to maturation of the SD&QA input data commensurate with progression of the Systems Engineering process; and

— identification of applicable standards, guides, and enterprise-level command media which govern the contractor's SD&QA programme(s).

B.2.3 Integration of the SD&QA programme plans with the contractor's Systems Engineering Plan (SEP) or Product Assurance Management Plan (PAMP) to establish the SD&QA organization's infrastructure, and the management personnel's authority, accountability, and responsibilities.

NOTE The SD&QA programme plans are updated on an "as required" or "as needed" basis. "As required" updates are triggered by contractually required delivery times. "As needed" updates are triggered by changes to the system or project which affect the integrity of information in the plan.

B.2.4 Distribution of each SD&QA assessment report to the customer(s) for review.

B.2.5 Establishment of Technical Performance Metrics for purposes of tracking and reporting the progress of each SD&QA programme.

B.2.6 Oversee the SD&QA activities of subcontractors during product manufacture, test, inspection, or shipping.

B.3 The Capability Level 3 SD&QA programme include all the tasks in the Capability Level 2 SD&QA programme plus the following.

B.3.1 Change B.2.1 to, "Implementation of the Capability Level 3 SD&QA programme, which represents the minimum effort required to eliminate, mitigate, or accept specific technical risks of a High I unit-value/criticality system/product, during specific phases of its life cycle. The following activities are included, at a minimum, in a Capability Level 3 SD&QA programme".

B.3.2 Assessment of the identified SD&QA requirements using System Requirements Hazard Analysis, or an equivalent methodology, to determine the risk of conflicting requirements, requirements creep, requirements falsification, and other undesirable conditions caused by unintended or bad requirements.

Note for cases of conflicting SD&QA requirements the issue is resolved using the following order of precedence:

1) System safety requirements;

2) Availability requirements;

3) Reliability requirements; and

4) Maintainability and testability requirements.

B.3.3 Change B.1.5 c to "Identification of the system's hazards and failure modes and their quantitative probabilities of occurrence."

B.3.4 Establishment, utilization, and maintenance of a project SD&QA database system that:

1) provides seamless interfaces among SD&QA processes and other project functions, such as, design, manufacturing, and testing;

2) contains all the key SD&QA requirements and data products;

3) has data change control and tracking procedures;

4) can automatically generate SD&QA programme plans and reports that are commensurate with the product's unit value/criticality and systems engineering life cycle data content/maturity; and

5) can be used to automatically evaluate SD&QA programme plans and reports with regard to compliance with requirements and appropriateness of verification artifacts.

B.3.5 Assurance that other project functions utilize SD&QA analysis results/data to the greatest extent practical.

B.3.6 Collection, review, and utilization of existing SD&QA lessons learned, as applicable.

B.3.7 Evaluation of all aspects of the SD&QA programme to identify and approve new product and process based lessons learned.

B.4 The Capability Level 4 SD&QA programme include all the tasks in the Capability Level 3 SD&QA programme plus the following.

B.4.1 Change B.3.1 to, "Implementation of the Capability Level 4 SD&QA programme, which represents the minimum effort required to eliminate, mitigate, or accept specific technical risks of a very-High I unit-value/criticality system/product, during specific phases of its life cycle. The following activities are included, at a minimum, in a Capability Level 4 SD&QA programme".

B.4.2 Change B.2.5 to, "Oversee the SD&QA activities of subcontractors, such that, major subcontractors provide SD&QA data products in predefined formats that facilitate integrating component level SD&QA data products with assembly, subsystem, or system level analyses, tests, or inspections".

B.4.3 Evaluation of the maturity of the input data used for SD&QA analyses (e.g. constraints, ground rules, and analytical assumptions) in the context of the Project Management Plan (PMP) or Systems Engineering Plan (SEP) and the Input Data Maturity Rating Criteria defined in this document.

B.4.4 Acquisition of validated computerized SD&QA tools and integrate them with the Project SD&QA Database System.

B.4.5 Establishment of channels to exchange approved lessons learned with similar projects throughout the enterprise.

B.4.6 Integration of all SD&QA risk assessments with a single project-wide Risk Management Process to ensure all risks associated with identified hazards and failure modes are properly reported within the contractor's organization and to the customer in a timely manner. At a minimum, this approach includes the following objectives:

— establishment of minimum qualifications for performing all experience-intensive or training-intensive activities;

— reporting of all incidents of significant residual risk to the appropriate risk acceptance authorities;

— proper management of all safety-critical and mission-critical items;

— assurance that all SD&QA milestones and deliverables are included in the project's Integrated Master Schedule (IMS) and can be accomplished within the project's allocated budget; and

— assurance that all anticipated undesirable events will be prevented and the impact of unanticipated undesirable events will be minimized.

B.5 The Capability Level 5 SD&QA programme include all the tasks in the Capability Level 4 SD&QA programme plus the following.

B.5.1 Change B.4.1 to, "Implementation of the Capability Level 5 SD&QA programme, which represents the minimum effort required to eliminate, mitigate, or accept specific technical risks of an High III unit-value/criticality system/product, during specific phases of its life cycle. The following activities are included, at a minimum, in a Capability Level 5 SD&QA programme".

B.5.2 Performance of formal peer reviews to evaluate the SD&QA programme outputs.

B.5.3 Continuous improvement of the overall SD&QA programme by:

— instituting processes that facilitate individuals and teams proactively identifying and assessing SD&QA hazards and failure modes; and

— periodically training management and technical personnel how to properly use cost-effective SD&QA tools and processes, or exposing them to new SD&QA lessons learned.

B.5.4 Sharing of approved SD&QA lessons learned with external enterprises and organizations.

Annex C
(informative)

Safety, Dependability and Quality Assurance (SD&QA) programme and Process Definitions

C.1 System Safety Programme (SSP)

The contractor assigns a system safety manager with verifiable experience or training necessary to properly develop/acquire and manage/monitor a System Safety Programme that is consistent with the requirements in this document, ISO 14620-1, ISO 14300-2, and any other system safety standards (e.g. MIL-STD-882E) or guides referenced in the Statement of Work (SOW). The system safety manager establishes internal reporting procedures for the investigation and disposition of product related hazards and safety incidents, including potentially hazardous conditions not yet involved in a mishap/incident.

C.1.1 System Safety Management Processes

A. System Safety Programme Planning

Purpose:

To identify the activities essential in assuring the System Safety tasks required to identify, evaluate, and eliminate or control hazards, or to reduce the residual hazard risk to a level acceptable throughout the system life cycle. The approved System Safety Programme Plan (SSPP) demonstrates that the project manager fully understands his/her system safety obligations to the customer and to the contractor, and that the resources necessary to fulfil this obligation are allocated. For the customer, the SPPP provides the means for understanding how the programme accomplishes its system safety responsibilities, as called out in the programme statement of work (SOW) or this document.

Process Description:

The SPP ensures safety design risks are balanced against project constraints and objectives through a comprehensive effort that will contribute to system safety over the product life cycle. The SPP is developed as part of the initial planning for all product development programme. The SPP includes descriptions of the following:

— the responsibilities of the system safety organization;

— the system safety responsibilities of key individuals and organizations outside the system safety organization;

— how the safety programme will be established and implemented consistent with contractual requirements;

— how system safety standards and guidance will be provided to all programme disciplines consistent with contractual requirements;

— the single Point of Contact (POC) for all system safety matters pertaining to the programme, the customer, the subcontractors, and the contractor;

— how all reasonable and prudent hazard risks will be assessed, and eliminated, controlled, or accepted during all phases of the programme;

— how the flow down of system safety requirements to subcontractors will be consistent with contractual requirements;

— how product and operational safety issues will be brought to the attention of the project manager in a timely manner;

— how the generation and delivery of system safety documents, and other items related to system safety contractual deliverables, will be consistent with contractual requirements;

— how system safety engineers will participate in technical reviews, design change reviews, and trade studies to ensure compliance with applicable system safety requirements;

— how system safety audits and reviews, if contractually required, will be conducted to ensure compliance with system safety policies, procedures, and functional performance requirements; and

— how the resources needed to accomplish the safety programme tasks will be ensured.

B. Subcontractor and supplier safety management

Purpose:

To identify sources of products and services that may be used to satisfy system safety requirements, and manage the pertinent activities of subcontractors and suppliers to minimize risk of hazardous conditions. Also, to ensure system safety activities of subcontractors are consistent with the overall safety programme through verification of compliance or conducting surveillance of their system safety activities.

Process description:

Exercise monitoring and control of subcontractor and supplier system safety activities; ensure System Safety Programme Plans (SSPPs) are complete and executable; exchange applicable system safety lessons learned; and if necessary, assist in development of their system safety capabilities. All system safety deliverables expected from the subcontractor are called out in contractual agreements with the subcontractor.

C. Safety programme working group

Purpose:

To conduct formal and informal technical reviews, determine the status of a safety programme, and work system safety risks and issues to closure.

Process description:

System safety engineers meet to review status of planned system safety activities, significant hazard risks, and any mishaps which may have occurred. The group also ensures appropriate follow-up actions or corrective actions are taken in a timely manner, and are properly implemented, verified, and documented.

C.1.2 System safety engineering tasks

A. Hazard Analysis

Purpose:

To identify hazardous conditions and risks for purpose of elimination and/or control. Hazard analysis is performed to examine the system, subsystems, components, and their interrelationships, as well as logistic support, training, maintenance, operational environments, and system/component disposal plans to:

— Identify hazards and recommend appropriate corrective action.

— Assist the individual(s) actually performing the analysis in evaluating the safety aspects of a given system or element.

— Provide managers, designers, test planners, and other decision makers with the information and data needed to permit effective trade-offs.

— Demonstrate compliance with given safety-related technical specifications, operational requirements, and design objectives.

Process description:

The timely identification of unacceptable hazards is the first activity in assuring proper safety provisions.

— Identification involves determining the severity or magnitude, importance, and frequency or likelihood of the worst-case mishap caused by the hazard at every system indenture level.

— Timely evaluation of unacceptable hazards involves determining the appropriate corrective action to eliminate or control unacceptable hazards and avoid the postulated mishaps of catastrophic or critical severity.

— Timely communication of the hazard evaluation results to individuals with decision-making authority to implement corrective actions.

— Needed safety design changes are identified and completed early in the system's life cycle to minimize the impact on cost and schedule.

B. Fault Tree Analysis

Purpose:

To systematically examine a potential system failure by creating a graphical representation of the system using deductive logic. The fault tree represents system relationships and fault paths, and provides a means for qualitative or quantitative system evaluation. Fault Tree Analysis (FTA) is a deductive, top-down method used to determine how a given system failure can occur. A system's top undesired event is either identified or postulated, and the analysis attempts to find out what contributes to this undesirable event.

Process description:

The FTA begins with a top event, establishes the component-level to which each system-level fault is examined, and determines the immediate causes for each fault at progressively lower levels until a component-level fault is reached. The FTA determines the various ways in which a particular type of top event or failure could occur. All of the possible system contributing factors and their relationships are established and, if possible, a top probability of occurrence calculated.

The primary output of FTA is the fault tree structure, which allows for qualitative or quantitative evaluation of a system failure. FTA is particularly useful in the examination of functional paths of high complexity, in which the outcome of one or more combinations of non-critical basic events may produce an undesirable system failure. Typical candidates for FTA are functional paths or interfaces that could have impact on flight safety, munitions handling safety, safety of operating and maintenance personnel, and probability of error-free command in automated systems in which a multiplicity of redundant and overlapping outputs may be involved. The fault tree is an analysis tool that provides a way to combine all contributing failures, events, and conditions that can lead to the occurrence of an undesired top event.

For the case of a system with mission-critical design requirements, FTA is used to identify unacceptable conditions where single component failure, common mode failure, human error, or a design weakness could cause a mishap of Catastrophic or Critical mishap severity category.

For the case of a system with safety-critical design requirements, FTA is used to identify unacceptable conditions where dual independent component failures, dual independent human errors, or a combination of a component failure and a human error involving safety-critical command and control

functions could cause a mishap of Catastrophic or Critical mishap severity category. Guidelines for FTA are in IEC 61025.

C. Event Tree Analysis

Purpose:

To systematically examine various possible outcomes of a given initiating event and create a graphical model of the system logic. The event tree represents system relationships and accident paths and provides a means for qualitative or quantitative system evaluation. Event Tree Analysis (ETA) is an inductive process that shows all possible outcomes (end states) resulting from an initiating event, and can expand accidental events into scenarios that take into account all safety mitigation measures whether functioning or not and additional factors impacting the outcomes.

ETA can be used to identify all possible accident scenarios and sequences of events in a complex system allowing for identification of the system's design and operational weaknesses. This can lead to improvements in system safety functions and result in lowering the operational risks of technologically advanced systems.

Process description:

ETA is an accident propagation analysis tool. The analysis is conducted in the form of a decision tree and is based on a binary logic distinction between success and failure. It begins with an initiating event (the root of the tree) and follows it through the system to determine a range of its potential outcomes (end states). The logic describes the states in which an event either has or has not occurred or a component has or has not failed. This corresponds to the functions or subsystems and their success or failure of being activated given the existing conditions. Each branch of the ET includes probability of success or failure. Such accident sequences allow using the Boolean logic for quantification of system risks.

The primary output of ETA is the event tree structure, which allows for qualitative or quantitative evaluation of a range of possible accident end states. ETA is particularly useful in the examination of accident propagation paths of highly complex designs, in which the failure of one or more combinations of mitigating events may produce undesirable consequences. Typical candidates for ETA are functional paths or interfaces that could impact flight safety, munitions handling safety, safety of operating and maintenance personnel, and probability of error free command in automated systems in which a multiplicity of redundant and overlapping outputs may be involved. Event tree analysis in combination with fault tree analysis is an analysis tool that provides a way to combine all contributing failures, events, and conditions that can lead to either success or failure of a complex system. Guidelines for ETA are in IEC 62502:2010.

D. Human Reliability Analysis

Purpose:

To perform user/operator level reliability predictions and assessments based on a critical-function analysis that characterizes human performance capabilities, historical performance data, and operator interfaces with the system design. This task aids in evaluating the reliability of users/operators, and provides key input to system reliability modelling/predictions.

Process description:

Develop a mathematical model to estimate the failure rate or hazard rate of the user/operator. The model represents:

1) historical operator error rates versus skill levels;

2) critical-function procedures;

3) error mitigation features;

4) training effectiveness; and

5) hazard assessment of operator interfaces.

Guidelines for human reliability analysis are in IEC 62508:2010.

E. Probabilistic Risk Assessment (PRA)

Purpose:

PRA is a comprehensive, structured, and logical analysis methodology aimed at identifying and assessing risks in complex technological systems for the purpose of cost-effectively improving their safety and performance.

Process Description:

A PRA characterizes risk in terms of three basic questions:

(1) What can go wrong?

(2) How likely is it?

(3) What are the consequences?

The PRA process answers these questions by systematically identifying, modelling, and quantifying scenarios that can lead to undesired consequences, considering uncertainties in the progression of such scenarios due to both variations of, and limited knowledge about, the system and its environment. The PRA integrates models based on systems engineering, probability and statistical theory, reliability and maintainability engineering, physical and biological sciences, decision theory, and expert elicitation. The collection of risk scenarios allows the dominant contributors to risk and areas of uncertainty about risk to be identified. Guidelines for PRA are in ISO 11231.

C.1.3 Safety testing tasks

A. Product Safety Testing (PST)

Purpose:

Tests are defined during the Engineering and Manufacturing Development Phase to validate selected safety features of the system or product. Safety critical equipment is tested to determine mishap severity or to establish the margin of safety of the design.

Process description:

The contractor implements demonstrate the acceptability of safety critical equipment, inducing or simulating failure modes. When it cannot be analytically determined whether the corrective action will adequately control a hazard, safety tests will be conducted to evaluate the effectiveness of the controls. Safety testing is integrated into system test and demonstration plans to the maximum extent possible. Guidelines for safety testing are in ISO 14620-2.

C.2 Dependability Programme

C.2.1 General

The contractor assigns a dependability manager/lead with verifiable experience or training necessary to properly develop/acquire and manage/monitor a detailed Dependability Programme Plan that is consistent with the requirements in this document, ISO 23460, and ISO 14300-2.

C.2.2 Dependability management tasks

A. Dependability Programme Planning (See IEC 60300-1:2014; IEC 60300-3-1:2003)

Purpose:

To identify those activities and designs essential in assuring product reliability, maintainability, availability and dependability performance.

Process description:

The supplier establishes a Dependability Programme Plan (DPP) that is integrated with the overall Product Assurance Plan. The DPP describes how reliability engineering contributes to the total product design, and the level of authority and constraints on the Dependability discipline. The DPP identifies the sources of the reliability engineering methodologies, reliability design guidelines, and reliability design review checklists that will be utilized.

The DPP identifies the product reliability requirements, the reliability activities, the inputs each activity needs (including inputs that are needed from operation and support experience with a predecessor item or items), the sequence of events required to achieve the product reliability requirements, and the method to be used to verify how each product reliability requirement will be met. The DPP encompasses a core set of reliability activities that include the allocation of product reliability requirements, the analysis of failure modes and effects, the identification and control of reliability critical items, the estimation of component level failure/hazard rates, the development of a product level reliability model, and the implementation of a failure recurrence prevention process to ensure all verified failures are adequately closed.

The DPP describes the method by which the reliability requirements are disseminated internally to designers and other product stakeholders, and externally to subcontractors and major suppliers. The DPP includes a schedule of each activity, with estimated start and completion points. The DPP describes the procedures for evaluating the status and control of each reliability activity, and identify the organizational unit or individual with the authority and responsibility for executing each reliability activity. The DPP describes the interrelationships of Dependability activities and how these activities interface with the activities of other product assurance processes. For example, single-fault versus dual-fault tolerance design trade-offs may be driven by overlap between mission reliability requirements and safety design requirements.

Necessary reliability engineering resources are identified in the DPP. The reliability engineering skill requirements and associated reliability activity coordination skill requirements are identified in the DPP.

The DPP may require revision as product development progresses, in response to improved risk understanding and the availability of evaluation results. In which case, revisions to the DPP are managed under the supplier's existing document control policy.

B. Subcontractor and supplier dependability management

Purpose:

Identify sources of products and services used to satisfy reliability, maintainability, and availability requirements, and manage the pertinent activities of subcontractors and suppliers to minimize risk of latent deficiencies. Assure Dependability activities of the subcontractor or supplier are consistent with the overall Dependability programme, through verification of compliance, or surveillance of their reliability, maintainability, and availability activities.

Process description:

Monitor and control of subcontractor and supplier reliability engineering activities; ensure that their reliability programme plans are complete and executable; exchange applicable reliability lessons learned; and if necessary, assist in development of their reliability capabilities. All reliability deliverables expected from the subcontractor are called out in contractual agreements with the subcontractor.

C. Dependability working group

Purpose:

To conduct formal and informal technical reviews, determine the status of the Dependability programme, and work reliability, maintainability, and availability risks and issues to closure.

Process description:

Engineers cognizant of the project's Dependability requirements meet to review the status of planned reliability activities, significant failure mode risks, and any verified test failures. The group also ensures required follow-up actions or corrective actions are taken in a timely manner, and are properly implemented, verified, and documented.

C.2.3 Dependability engineering tasks

A. Functional Diagram Modelling (FDM)

Purpose:

To develop graphical representations of the system's functional interrelationships. The primary output of FDM is a graphical diagram that represents detailed design information with regard to the functional characteristics of each system element. FDM assists in achieving a common understanding, in a functional sense, of the system or system of systems among all product assurance processes. The FDM, also referred to as a Functional Block Diagram (FBD), can be thought of as a "bridge", serving as the link between the technical engineering documentation such as drawings, ICDs, and so forth, to the Failure Mode, Effects and Criticality Analysis (FMECA).

Process description:

Collect, process, and evaluate detailed system design information to develop a graphical representation of the system that consists of:

— the system's functional elements, including inputs and outputs of each functional element;

— the system's functional paths (e.g. wiring, tubing, logic flow, operator actions, power, signals, electromagnetic waves, forces, pressures, and mechanical motions); and

— references to a description of the system's modes of operation (e.g. mission timeline, states, transitions, switching, timing, and phases).

B. Product Failure, Mode, Effects and Criticality Analysis (FMECA)

Purpose:

To identify effects of potential failure modes, system redundancy features, responses to system failures, single point failure modes, and critical items which require special controls during processing.

Process description:

An FMEA/FMECA is prepared whenever a system functional block diagram is available, and is updated throughout the system development cycle. The FMEA/FMECA process is used to identify credible single-point failure modes and feed into the critical items controls process to eliminate or control their effects. See Figure C.1 for a flow depiction for the FMEA/FMECA and Critical Items List (CIL) analysis process.

FMEA: Perform a systematic analysis of local and system effects of specific component failure modes. Guidelines for FMECA are in IEC 60812:2006.

FMECA: Evaluate mission criticality of each failure mode. Criticality analysis is applied to the design process to eliminate safety critical flaws in the system or mitigate those failures, by actions such as providing redundant features or identifying operator actions which can be taken. Also, FMECA can be used to identify failures of a less critical nature, but which are determined to be maintainability drivers.

Critical Items List (CIL): Provides a summary of selected hardware related items whose related failure modes can result in serious injury, loss of life (flight or ground personnel), loss of vehicle, or loss of one or more mission objectives.

C. Component Reliability Predictions

Purpose:

To perform part and component level reliability predictions and assessments. This task aids in evaluating the reliability of similar components, and provides key input to system reliability modelling.

Process description:

Develop a mathematical model to estimate the failure rate or hazard rate of the component for a given operating mode, operating cycles, and under specified operating conditions. The model provides insight into component level redundant functions. Guidelines for reliability predictions are in IEC 60605-4:2001, IEC 60605-6:2007, IEC 61650:1997.

D. System Reliability Modelling

Purpose:

To perform assembly through system level reliability predictions, allocations, and assessments. Aids in evaluating reliability of competing designs, and provides key input to availability and sparing assessments.

Process description:

Develop a hierarchical mathematical model to estimate the probability of the system successfully performing its intended functions for a given period of time or operating cycles, and under specified operating conditions. The model accounts for initial system reliability, which includes the cumulative effects of functional testing, storage, handling, packaging, transportation, assembly, and maintenance on the ability of the system to meet its operational reliability requirements. The model provides insight into assembly through system level redundant functions. Guidelines for reliability modelling are in IEC 61165:2006, and IEC 61649:2008.

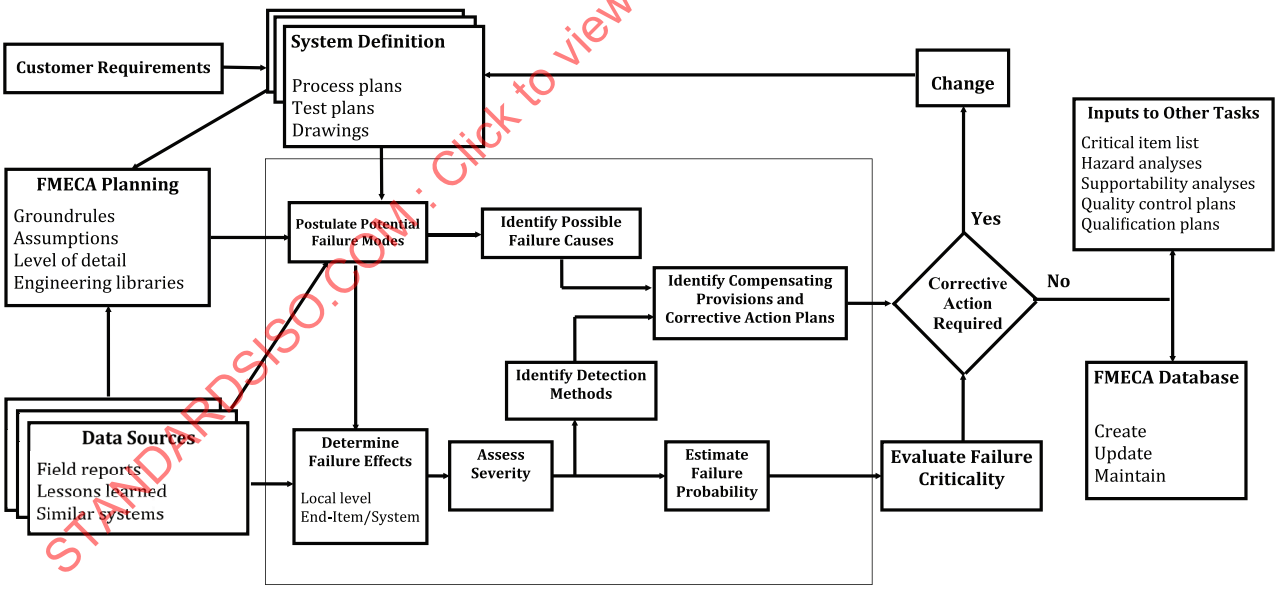


Figure C.1 — Example FMEA/FMECA and Critical Item List (CIL) analysis process

E. Design Concern Analysis (DCA)

Purpose:

To ensure a safe and reliable product by designing-in special features that prevent, tolerate, or recover from failures, compensate for potential design weaknesses, or mitigate risk.

Process description:

Design rules and guidelines may be used upfront to ensure a degree of product durability by avoiding specific types of design weaknesses. Or, perform an analysis on an existing design to identify where special features are needed to mitigate a design weakness. Some of these special features include redundancy, fault tolerance, fail-safe, and design margin.

F. Worst Case Analysis (WCA)

Purpose:

To ensure that all circuits will perform within specifications over a given lifetime while experiencing the worst possible variations of electrical piece parts and environments.

Process description:

During preliminary design, evaluate circuit performance assuming maximum part parameter variations and extreme operating conditions, e.g. long use life, high temperature, radiation, shock, etc.

G. Environmental Event/Survivability Analysis

Purpose:

To ensure the system will physically survive its natural operating environmental by one or more of the following methods:

1) Performing a environmental hazard analysis to verify the probability of environmentally induced damage is non-credible (i.e. $<10^{-6}$),

2) Showing proper electromagnetic interference (EMI) margin exists for all components susceptible to anticipated single event upsets (SEUs),

3) Using commercial products that meet Federal Communications Commission (FCC), or European Union electromagnetic compatibility (EMC) requirements, or MIL-STD-461C requirements, and,

4) Showing that system functionality will be restored following the occurrence of environmentally induced damage.

Process description:

Identify environmental hazards and develop a mathematical model to estimate the failure rate or hazard rate associated with environmental event susceptible parts. The model represents the following:

— historical failures of similar systems in similar operating environments;

— components susceptible to environment induced damage;

— environmental damage mitigation features; and

— assessment of the system restoration capability.

H. Software Component Reliability Predictions (S-102.2.15)

Purpose:

To quantify the probability or frequency of a software component's functional success or failure. Predictions are expressed as a statistical life distribution that represents the probability of a software component functioning during a particular time period. This task aids in ensuring software design reliability, and it provides key input to system reliability modelling/predictions.

Process description:

Develop mathematical or simulation models which represent the following software component attributes:

— architecture;

— application;

— use environment;

— operating profile; and

— failure modes, mechanisms, and causes.

Criteria for a capability-based Software Component Reliability Predictions (SCRP) process are defined in the S-102.2.15, *Capability-based Software Reliability Predictions Standard*, which requires an organization, company, group, or individual to be capable of performing SCRP in a manner that is commensurate with the product's unit-value/criticality and systems engineering life cycle data content/maturity. Guidelines for software reliability analysis are in IEC 62628:2012.

I. Maintainability Predictions

Purpose:

To perform probabilistic estimates of failure maintenance times based on maintenance time-study data, diagnostics capability of the design, and accessibility of failed components. Maintainability predictions are performed to aid:

1) Defining/meeting repair time requirements;

2) Identifying where design features are needed to reduce the repair time; and

3) Ensuring all repair actions are characterized and repeatable.

The output of maintainability predictions is primarily used to support integrated logistics support (ILS) assessments. This task aids in ensuring maintenance training and skill levels are compatible with system design, and it provides key input to system availability modelling/predictions.

Process description:

Perform maintainability predictions to support system availability modelling/predictions, and ILS assessments, as required. Guidelines for maintainability requirements are in IEC 60706-2:2006, and for maintainability predictions are in IEC 60300-3-10:2001 and IEC 60706-6.

J. Anomaly Detection and Response (ADR) Analysis

Purpose:

To develop identification and response methods for system anomalies or faults which pose an unacceptable risk. The response methods can range from manual Test, Analyse, and Fix (TAAF) procedures, to automated fault isolation and recovery software. Depending on how it is performed, ADR analysis can be used to develop different types of ADR systems. The primary output of ADR analysis is Functional Failure Analysis (FFA) worksheets, which systematically identify the detection and response methods for functional failure modes that require such actions, as defined by FMECA, system tests, test deficiency reports, failure analyses, hazard analyses, or risk assessments.

Process description:

Perform an analysis to design system functions for detecting, verifying, isolating, and responding to a specified set of functional failure modes. The ADR analysis process includes the following tasks:

— defining ADR system requirements and design criteria which meet the user's needs;

— establishing ADR analysis technical performance metrics (TPMs);

— collecting and evaluating engineering information needed to perform the analysis (e.g. signal lists, specs, interface control drawings (ICDs), test data, operational data, schematics, and product FMECA);