Standardization training program
Q30 discipline:
Dependability

19/06/2017

ESTEC-NL

Introduction

Standardization training program Q30 discipline: Dependability

- Trainer
- Course Objectives
- Course Contents

Trainer

Name: Antonio HARRISON SANCHEZ
Education: MS Aerospace Engineering (Reliability Engineering Option), 2006
The University of Arizona, Tucson, USA

Relevant Work Experience

2005-2006	The University of Arizona, Tucson, USA Graduate Research Assistant Deterministic & Probabilistic Design Optimization Group
2006-2008	European Space Agency, ESTEC, Noordwijk, NL Young Graduate Trainee Dependability and Safety Assurance Section
2008-2015	TERMA B.V., Leiden, NL Product Assurance Engineer ESTEC On-site contractor
2015-today	European Space Agency, ESTEC, Noordwijk, NL Dependability and Safety Engineer Dependability and Safety Assurance Section

Objectives

Standardization training program Q30 discipline: Dependability

- Familiarize with dependability basic concepts
- Have an overview of the most important principles to “design & operate” a dependable system
- Understand the dependability program & requirements defined in ECSS-Q-ST-30C Rev. 1
- Consider relevant interfaces to other disciplines (such as quality assurance, software product assurance, configuration management, safety, risk management, …) and ECSS standards

Contents

Standardization training program Q30 discipline: Dependability

- Introduction to dependability basic concepts
- Introduction and overview of ECSS-Q-ST-30C Rev. 1
- Detailed contents of ECSS-Q-ST-30C Rev. 1 and practical considerations
- Time for questions

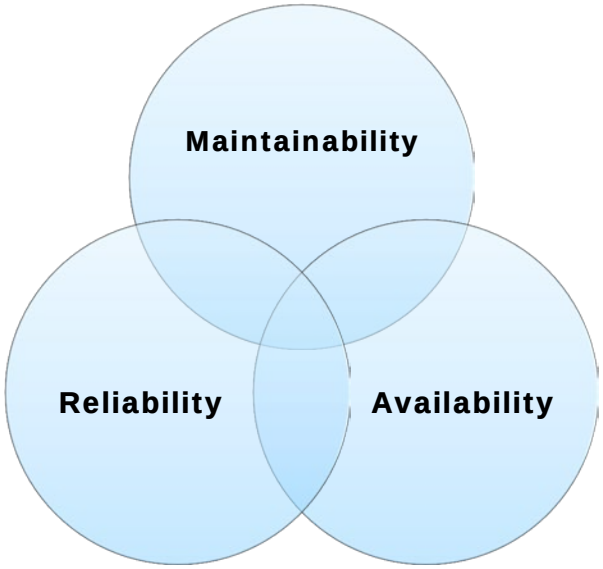
What is dependability ? [ECSS-S-ST-00-01]

The extent to which the fulfilment of a required function can be justifiably trusted

Reliability: the ability of an item to perform a required function under given conditions for a given time interval

Maintainability: ease of performing maintenance on a product. Maintainability can be expressed as the probability that a maintenance action on a product can be carried out within a defined time interval, using stated procedures and resources.

Availability: ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided



Main components of dependability: Reliability, availability and maintainability. Dependability is also addressed by the acronym **RAM**.

Dependability shall be considered in conjunction with safety.

What is dependability ? (cont.)

- Dependability should be seen as the capability to provide the required functionalities at a performance level sufficient to achieve the mission objectives
- Dependability is a capability/performance characteristic and not a functionality. It cannot be implemented by a dedicated subsystem/item but it is an inherent characteristic of each item/function
- Dependability is a “built-in” design characteristic that is traded off with the other item characteristics (mass, volume, complexity, cost, etc.). It is implemented by the design engineer together with the dependability engineer to find the optimum solution for the implementation of the required function while assuring the required dependability performance
- Dependability applies to systems, products or services. It applies to hardware, software and human
- Dependability focuses on failures, failure prevention and on the reduction of the consequences of failure (life, cost, schedule, availability of service, etc.)
- Dependability risks are related to the potential loss or degradation of the required technical performance that affects the attainment of “mission objectives”

What is dependability ? (cont.)

- **Example 1:** Driving a car
  - Safety risk of getting injured or even killed in an accident / totalling the car
  - Dependability risks of having a breakdown on the highway (reliability), not having the car (availability) while its being fixed or maintenance that takes much longer than expected (maintainability)
- **Example 2:** Designing & operating a spacecraft & Moon base
  - Safety risk of loss of an astronaut, spacecraft or Moon base due to accident
  - Dependability risks: Complete failure of an experiment ORU (reliability), shut down of an ORU (availability), and ORU repair or replacement problem (maintainability)

Mission failures are always more costly than proactive investments into safety and dependability assurance !

Why is dependability important ?

- **Example 1:** Driving a car
  - The implications of a car accident can be catastrophic for your family (loss of a family member, financial loss, …)
  - The implications of a car breakdown can be severe (delays, loss of driving pleasure, loss of reputation of car manufacturer, higher life-cycle costs, …)
- **Example 2:** Designing & operating a spacecraft & Moon base
  - The implications of a major accident can be catastrophic for the customer organisation (loss of life, destruction of premises, consequences to the environment , loss of reputation & credibility and funding, …)
  - The implications of a loss or degradation of a mission can be very “expensive” (no scientific return of a “one chance only mission”, need to rebuild system, …)

How do dependability and safety interact ?

- A safe system is not necessarily a dependable system, a dependable system is not necessarily a safe system
- An increase of safety can decrease the reliability and vice versa
- “Dependability & safety” needs to be integrated and optimised during the design & operation development process

How do dependability and safety interact ? (cont.)

- **Example 1:** Driving a car
  - Safety features ABS, VSC, airbag, … can decrease the reliability of the car (increased failure rate of added electronics). A fire extinguisher poses a safety hazard (pressure vessel) but decreases the fire safety risk
- **Example 2:** Designing & operating a spacecraft & Moon base
  - Redundancy in the propulsion system can increase the reliability but also the chance of leaks
  - Increase of environmental shielding can require more transportation flights to the Moon base, which increase the overall launch risks and introduce additional costs

How is dependability performance expressed ?

- **Qualitative requirements**

  e.g. “No single failure in the monitoring function shall cause the loss of the monitored function.”

- **Quantitative requirements**

  e.g. “The launcher shall have a reliability of no less than 0.98 for successfully inserting the payload in its target orbit with the specified separation performance.”

Only meaningful together with specified environmental and operational conditions !

How is dependability achieved / enhanced ?

- **Reliability**
  - De-rating
  - Use of redundancy
  - Design diversity
  - Effects limitation
- **Maintainability**
  - Modularity
  - Accessibility
  - Failure Detection
  - Tools and skills to perform maintenance
- **Availability**
  - Optimization of reliability and maintainability balance

Dependability engineering

1. Aims at the integration and prioritisation of dependability in project activities

- Involves the application of dependability design & operation principles and requirements such as the “failure tolerance”, “fail safe”, “emergency, caution & warning”, “failure detection, isolation & recovery”, …

- Involves the identification & control of “dependability critical functions”

- Is based on the application of dependability analyses as design & operation drivers through the identification, reduction and control of dependability risks

Dependability engineering during life cycle

Standardization training program Q30 discipline: Dependability

Phase A
- Establishment of the dependability policy and initial conceptual trade offs

Phase B
- Definition of project specific failure effect severity categories and preliminary dependability analyses to support design trade offs

Phase C/D
- Detailed analyses down to the lowest design level as verification of the defined design to comply with the applicable dependability requirements
- Support to the definition, execution and evaluation of tests and simulations for the verification of compliance with the applicable dependability requirements

Phase E/F
- Support of in-flight anomaly investigations and resolutions and collection of dependability data from operational and anomaly data.

A detailed list of dependability activities along the different phases is provided in ECSS-Q-ST-30C Rev. 1

Make use of it!

Dependability assurance basic principles and objectives

What is dependability assurance?

Dependability assurance as part of product assurance & safety management is a continuous and iterative process throughout the project life cycle devoted to study, plan and implement activities intended to minimise dependability risks of a system within the project constraints

What is the need for dependability assurance?

Dependability assurance ensures that all dependability risks are adequately identified, assessed, minimised, controlled and finally accepted as part of project risk management

Dependability assurance ensure conformance to dependability requirements through the implementation of a dependability assurance programme

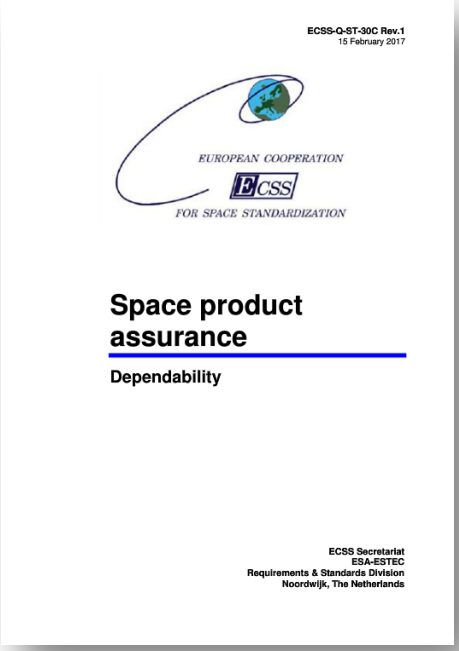
Dependability assurance basic principles and objectives (cont.)

What are the main objectives of dependability assurance ?

- assure that the system is reliable, available, maintainable
- support trade-offs and system engineering
- prevent that “something goes wrong”
- get it right the first time
- learn from mistakes
- investigate failures and resolve problems
- make sure that only known risks are accepted

What is ECSS-Q-ST-30C Rev. 1 ?

- ECSS-Q-ST-30C Rev. 1 is the ECSS level 2 standard on "dependability"
  - Dependability comprises reliability, availability and maintainability
    - Reliability is the ability to perform a required function
    - Availability is the ability to be in a state to perform a required function
    - Maintainability is the ability to be retained in or restored to a state in which an item can perform the required function
- Defines dependability assurance program and requirements for space systems
  - Program and requirements are applied to hardware, software and human of a space system



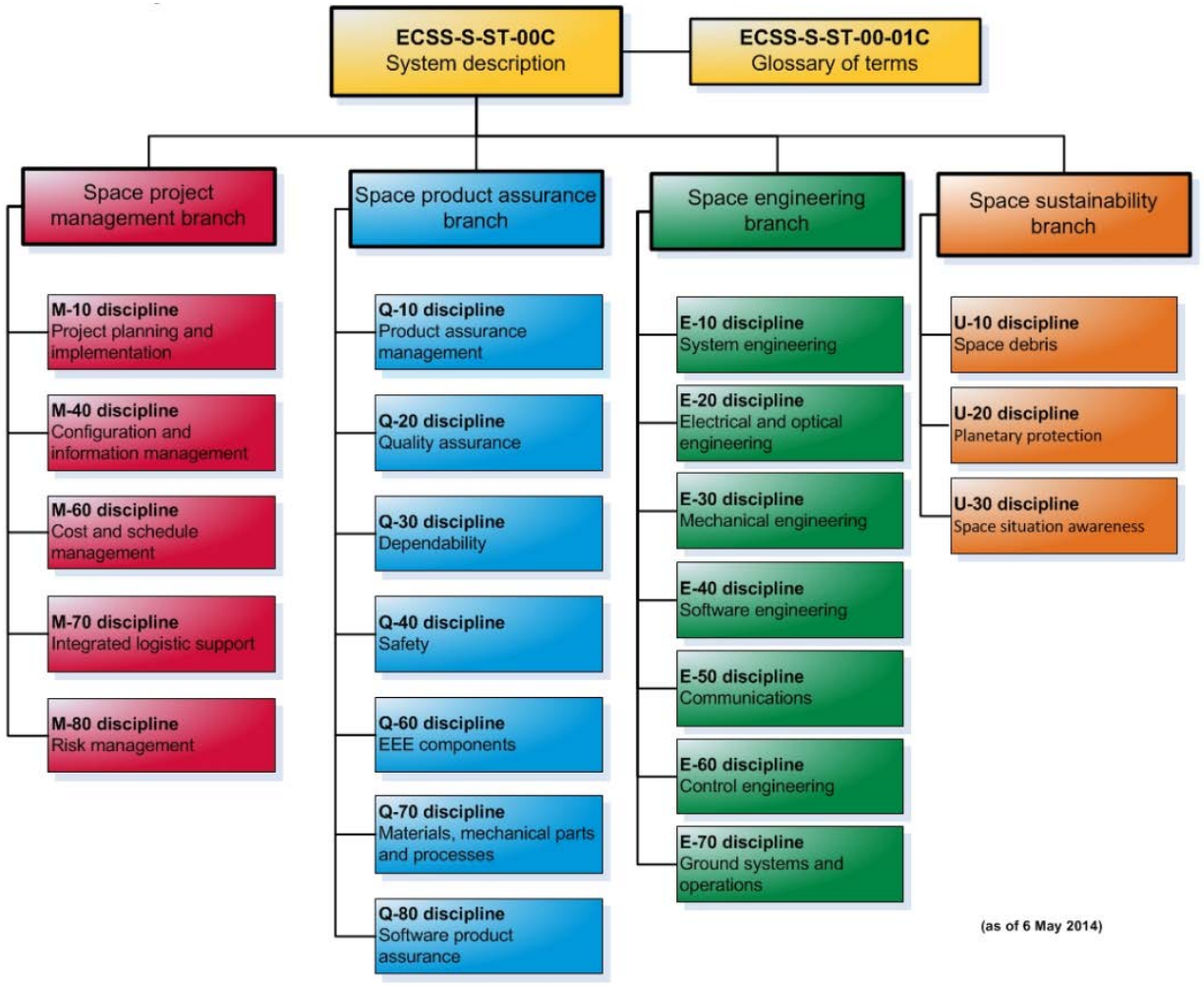
ECSS-Q-ST-30C Rev. 1

What is ECSS-Q-ST-30C Rev. 1 ? (cont.)

- Identifies dependability requirements for functions implemented in software and the interaction between hardware and software
- Interfaces with other ECSS standards of the Q (product assurance), M (project management) and E (engineering) series
- Applies to all European space projects and to all projects phases
- Is currently in version C Rev. 1 (2017)

ECSS-Q-ST-30C Rev. 1

Overview of ECSS-Q-ST-30C



Overview of ECSS-Q-ST-30C Rev. 1 (cont.)

Structure of ECSS-Q-ST-30C Rev. 1

- ECSS-Q-ST-30C Rev. 1
  - Foreword
    1 Scope
    2 Normative references
  - 3 Terms, definitions and abbreviated terms
  - 4 Dependability programme
  - 5 Dependability engineering
  - 6 Dependability analyses
  - 7 Dependability testing, demonstration and data collection
  - 8 Pre-tailoring matrix per product types
  - Annexes

Overview of ECSS-Q-ST-30C Rev. 1 (cont.)

What are the contents of ECSS-Q-ST-30C Rev. 1 ?

- ECSS-Q-ST-30C Rev. 1
  - Foreword
    1 Scope
    2 Normative references
  - 3 Terms, definitions and abbreviated terms
  - 4 Dependability programme
  - 5 Dependability engineering
  - 6 Dependability analyses
  - 7 Dependability testing, demonstration and data collection
  - 8 Pre-tailoring matrix per product types
  - Annexes

→

- Foreword
  - 1 Scope
  - 2 Normative references

Overview of ECSS-Q-ST-30C Rev. 1 (cont.)

What are the contents of ECSS-Q-ST-30C Rev. 1 ?

ECSS-Q-ST-30C Rev. 1

- Foreword
  1 Scope
  2 Normative references
- 3 Terms, definitions and abbreviated terms
- 4 Dependability programme
- 5 Dependability engineering
- 6 Dependability analysis
- 7 Dependability testing, demonstration and data collection
- 8 Pre-tailoring matrix per product types
- Annexes

→

- 3 Terms, definitions and abbreviated terms
  - 3.1 Terms from other standards
  - 3.2 Terms specific to the present standard
  - 3.3 Abbreviated terms
  - 3.4 Nomenclature

Overview of ECSS-Q-ST-30C Rev. 1 (cont.)

What are the contents of ECSS-Q-ST-30C Rev. 1 ?

ECSS-Q-ST-30C Rev. 1

- Foreword
  1 Scope
  2 Normative references
- 3 Terms, definitions and abbreviated terms
- 4 Dependability programme
- 5 Dependability engineering
- 6 Dependability analyses
- 7 Dependability testing, demonstration and data collection
- 8 Pre-tailoring matrix per product types
- Annexes

→

- 4 Dependability programme
  - 4.1 General
  - 4.2 Organization
  - 4.3 Dependability programme plan
  - 4.4 Dependability risk assessment and control
  - 4.5 Dependability critical items
  - 4.6 Design reviews
  - 4.7 Dependability Lessons learnt
  - 4.8 Progress reporting
  - 4.9 Documentation

Overview of ECSS-Q-ST-30C Rev. 1 (cont.)

What are the contents of ECSS-Q-ST-30C Rev. 1 ?

ECSS-Q-ST-30C Rev. 1

- Foreword
  1 Scope
  2 Normative references
- 3 Terms, definitions and abbreviated terms
- 4 Dependability programme
- 5 Dependability engineering
- 6 Dependability analyses
- 7 Dependability testing, demonstration and data collection
- 8 Pre-tailoring matrix per product types
- Annexes

→

- 5 Dependability engineering
  - 5.1 Integration of dependability in the project
  - 5.2 Dependability requirements in technical specification
  - 5.3 Dependability design criteria
  - 5.4 Criticality classification
  - 5.5 Involvement in testing process
  - 5.6 Involvement in operational aspects
  - 5.7 Dependability recommendations

Overview of ECSS-Q-ST-30C Rev. 1 (cont.)

What are the contents of ECSS-Q-ST-30C Rev. 1 ?

ECSS-Q-ST-30C Rev. 1

- Foreword
  1 Scope
  2 Normative references
- 3 Terms, definitions and abbreviated terms
- 4 Dependability programme
- 5 Dependability engineering
- 6 Dependability analyses
- 7 Dependability testing, demonstration and data collection
- 8 Pre-tailoring matrix per product types
- Annexes

→

- 6 Dependability analyses
  - 6.1 Identification and classification of undesirable events
  - 6.2 Assessment of failure scenarios
  - 6.3 Dependability analyses and the project life cycle
  - 6.4 Dependability analyses – methods
  - 6.5 Dependability Critical Items Criteria

Overview of ECSS-Q-ST-30C Rev. 1 (cont.)

What are the contents of ECSS-Q-ST-30C Rev. 1 ?

ECSS-Q-ST-30C Rev. 1

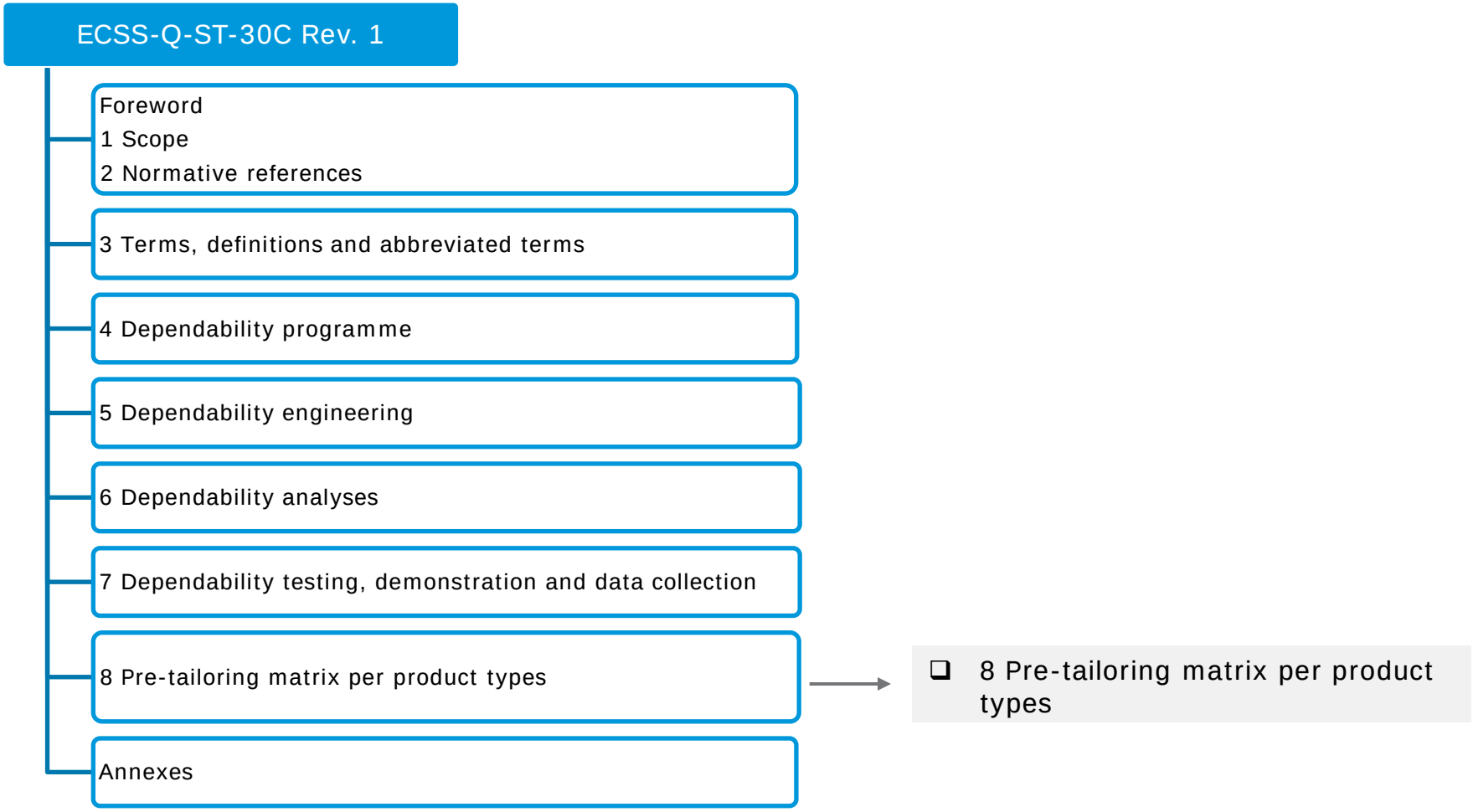
- Foreword
  1 Scope
  2 Normative references
- 3 Terms, definitions and abbreviated terms
- 4 Dependability programme
- 5 Dependability engineering
- 6 Dependability analyses
- 7 Dependability testing, demonstration and data collection
- 8 Pre-tailoring matrix per product types
- Annexes

→

- 7 Dependability testing, demonstration and data collection
  - 7.1 Reliability testing and demonstration
  - 7.2 Availability testing and demonstration
  - 7.3 Maintainability demonstration
  - 7.4 Dependability data collection and dependability performance monitoring

Overview of ECSS-Q-ST-30C Rev. 1 (cont.)

What are the contents of ECSS-Q-ST-30C Rev. 1 ?



Overview of ECSS-Q-ST-30C Rev. 1 (cont.)

What are the contents of ECSS-Q-ST-30C Rev. 1 ?

ECSS-Q-ST-30C Rev. 1

- Foreword
  1 Scope
  2 Normative references
- 3 Terms, definitions and abbreviated terms
- 4 Dependability programme
- 5 Dependability engineering
- 6 Dependability analyses
- 7 Dependability testing, demonstration and data collection
- 8 Pre-tailoring matrix per product types
- Annexes →

Annex A (informative) Relationship between dependability activities and project phases

- ❑ Annex B (informative) Dependability documents delivery per review
- ❑ Annex C (normative) Dependability plan – DRD
- ❑ Annex D (normative) Contingency analysis – DRD
- ❑ Annex E (normative) Reliability prediction – DRD
- ❑ Annex F (normative) Failure Detection Identification and Recovery – DRD
- ❑ Annex G (normative) Zonal analysis – DRD
- ❑ Annex H (normative) Maintainability analysis – DRD
- ❑ Annex I (normative) Common-cause analysis – DRD
- ❑ Annex J (normative) Worst Case Analysis – DRD
- ❑ Annex K DELETED
- ❑ Annex L (informative) Common-cause check lists
- ❑ Bibliography

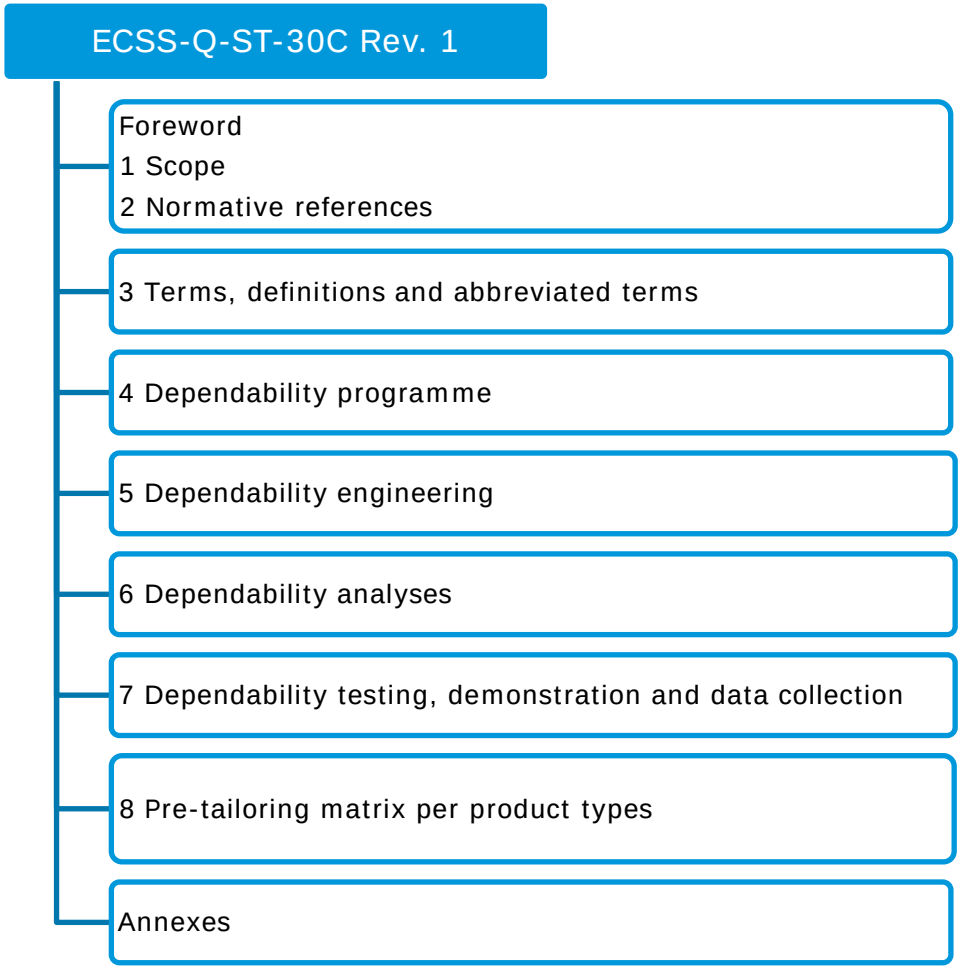
How is the detailed contents of ECSS-Q-ST-30C Rev. 1 presented ?

This training session provides:

- A summary of the chapters of ECSS-Q-ST-30C Rev. 1
- Some practical remarks and considerations

Foreword and first two sections

What does ECSS-Q-ST-30C Rev. 1 start with?



- Foreword
  - 1 Scope
  - 2 Normative references

Foreword

The foreword of ECSS-Q-ST-30C Rev. 1:

- Gives an explanation of what ECSS standards are
- Points out that the requirements deal with the “what is to be accomplished” rather than with the “how to organize and perform the tasks”
- Provides an overview of the changes to the previous versions A, B, and C (change log)

1 Scope

The scope of ECSS-Q-ST-30C Rev.1 comprises the:

- Dependability assurance program definition
- Dependability requirements definition (including identification of requirements for functions implemented in software)
- Link to software product assurance and to ECSS-Q-ST-80
- Link to risk management process and to ECSS-M-ST-80
- Applicability to all European space projects
- Applicability to all project phases
- Tailoring principles

What should be noted on section 1?

Some practical remarks and considerations on the “scope” of ECSS-Q-ST-30C Rev. 1 are:

- Dependability policy is applied by implementing a dependability assurance programme
- Dependability assurance is a continuous and iterative process throughout the project life cycle
- Dependability requirements for functions implemented by software are defined and the link to software product assurance is given
- Pre-tailoring table according to product type is given in clause 8

2 Normative references

ECSS-Q-ST-30C Rev.1 makes references to ECSS documents and requirements in the areas of:

- product assurance management
- critical item control
- FMEA/FMECA
- EEE components derating
- glossary of terms

3 Terms, definitions and abbreviated terms

What are the terms, definitions and abbreviated terms used in ECSS-Q-ST-30C Rev. 1 ?

ECSS-Q-ST-30C Rev. 1

- Foreword
  1 Scope
  2 Normative references
- 3 Terms, definitions and abbreviated terms
- 4 Dependability programme
- 5 Dependability engineering
- 6 Dependability analyses
- 7 Dependability testing, demonstration and data collection
- 8 Pre-tailoring matrix per product types
- Annexes

→

- 3 Terms, definitions and abbreviated terms
  - 3.1 Terms from other standards
  - 3.2 Terms specific to the present standard
  - 3.3 Abbreviated terms
  - 3.4 Nomenclature

3 Terms, definitions and abbreviated terms (cont.)

ECSS-Q-ST-30C Rev. 1 provides definitions of terms which are specific to this standard such as:

- **Failure scenario:** conditions and sequence of events, leading from the initial root cause, to an end failure
- **Limited-life product:** product with useful life duration or operating cycles limitation, prone to wear out, drift or degradation below the minimum required performance in less than the storage and mission time
- **Criticality (function, software, hardware, operation):** Classification of a function or of a software, hardware or operation, according to the severity of the consequences of its potential failures
- **Criticality (failure, failure mode):** Classification of a failure or failure mode according to a combination of the severity of the consequences and its likelihood or probability of occurrence

All other definitions are given in the ECSS glossary of terms (ECSS-ST-00-01)

4 Dependability programme

What does ECSS-Q-ST-30C Rev. 1 require on dependability programme ?

ECSS-Q-ST-30C Rev. 1

- Foreword
  1 Scope
  2 Normative references
- 3 Terms, definitions and abbreviated terms
- 4 Dependability programme
- 5 Dependability engineering
- 6 Dependability analyses
- 7 Dependability testing, demonstration and data collection
- 8 Pre-tailoring matrix per product types
- Annexes

→

- 4 Dependability programme
  - 4.1 General
  - 4.2 Organization
  - 4.3 Dependability programme plan
  - 4.4 Dependability risk assessment and control
  - 4.5 Dependability critical items
  - 4.6 Design reviews
  - 4.7 Dependability Lessons learnt
  - 4.8 Progress reporting
  - 4.9 Documentation

4 Dependability programme (cont.)

What are the key ingredients of a dependability program?

Dependability programme management of a project includes:

- Implementation of dependability assurance as part of product assurance
- Dependability programme planning and implementation
- Dependability risk assessment and control
- Dependability critical item identification and control
- Participation to design reviews
- Collection of dependability lessons learnt
- Supplier control, progress reporting and documentation

What should be noted on section 4?

Some practical remarks and considerations on the "dependability programme" requirements of ECSS-Q-ST-30C are:

- Dependability assurance is a systematic process for specifying dependability requirements and demonstrating their achievement
- The supplier is responsible for the development, maintenance and implementation of a dependability plan for all project phases (DRD is provided in Annex C of the standard)
- The dependability engineer is responsible for the identification and reporting of dependability associated risks
- The design and all the design changes are assessed for their impact on dependability

5 Dependability engineering

What does ECSS-Q-ST-30C Rev. 1 require on dependability engineering?

ECSS-Q-ST-30C Rev. 1

- Foreword
  1 Scope
  2 Normative references
- 3 Terms, definitions and abbreviated terms
- 4 Dependability programme
- 5 Dependability engineering
- 6 Dependability analyses
- 7 Dependability testing, demonstration and data collection
- 8 Pre-tailoring matrix per product types
- Annexes

→

- 5 Dependability engineering
  - 5.1 Integration of dependability in the project
  - 5.2 Dependability requirements in technical specification
  - 5.3 Dependability design criteria
  - 5.4 Criticality classification
  - 5.5 Involvement in testing process
  - 5.6 Involvement in operational aspects
  - 5.7 Dependability recommendations

5 Dependability engineering (cont.)

What are the key ingredients of dependability engineering ?

Dependability engineering involves and is based on:

- Integration of dependability in the project
- Dependability requirements in technical specifications
- Dependability design criteria including:
  - mission success criteria
  - design approach
  - failure tolerance requirements
  - Severity category
- Criticality classification (functions, hardware and operations, software criticality category)
- Involvement in test definition and operational aspects
- Dependability recommendations in support of the risk reduction process

What should be noted on section 5?

Some practical remarks and considerations on the "dependability engineering" requirements of ECSS-Q-ST-30C Rev. 1 are:

- Dependability characteristics are traded off with other attributes such as mass, size, cost and performance
- Dependability requirements are specified as part of the overall project requirements
- Dependability is apportioned in a top-down process to establish dependability requirements for lower level elements
- Failure tolerance should never be directly translated into redundancy and only implemented using the results of dependability (& safety) analyses
- "Mission success " criteria shall be defined (at each level) !

6 Dependability analyses

What does ECSS-Q-ST-30C Rev. 1 require on dependability analyses ?

ECSS-Q-ST-30C Rev. 1

- Foreword
  1 Scope
  2 Normative references
- 3 Terms, definitions and abbreviated terms
- 4 Dependability programme
- 5 Dependability engineering
- 6 Dependability analyses
- 7 Dependability testing, demonstration and data collection
- 8 Pre-tailoring matrix per product types
- Annexes

→

- 6 Dependability analyses
  - 6.1 Identification and classification of undesirable events
  - 6.2 Assessment of failure scenarios
  - 6.3 Dependability analyses and the project life cycle
  - 6.4 Dependability analyses – methods
  - 6.5 Dependability Critical Items Criteria

6 Dependability analyses (cont.)

What are the dependability analysis requirements and methods?

The ECSS dependability analysis requirements address the:

- Assessment of failure scenarios (identification and classification of undesirable events)
- Implementation of the analyses throughout the project life cycle
- Purpose of the analyses and objectives
- Definition of the dependability critical items criteria

6 Dependability analyses (cont.)

What are the dependability analysis requirements and methods ?

The ECSS Dependability analyses and methods comprise:

- Reliability analyses
- Maintainability analyses
- Availability analysis

  ECSS-Q-ST-30-09 is specifically dedicated to this analysis

6 Dependability analyses (cont.)

What are the reliability analyses addressed in ECSS-Q-ST-30C Rev. 1?

- **Reliability prediction**
  - ECSS-Q-HB-30-08 (currently obsolete) is mentioned as a guideline for the selection of reliability data sources and their use
- **Failure Mode Effects (and Criticality) Analysis (FMEA/FMECA)**
  - ECSS-Q-ST-30-02 is specifically dedicated to these analyses
- **Hardware Software Interaction Analysis (HSIA)**
  - ECSS-Q-ST-30-02 contains a section dedicated to this analysis
- **Contingency analysis**
- **Fault Tree Analysis (FTA)**
  - ECSS-Q-ST-40-12 is a guideline for this analysis

6 Dependability analyses (cont.)

What are the reliability analyses addressed in ECSS-Q-ST-30C Rev. 1?

- **Common-cause analysis**
  - An example of check list of generic common-cause parameters is provided in Annex L of ECSS-Q-ST-30C Rev. 1
- **Worst Case Analysis (WCA)**
  - ECSS-Q-HB-30-01 describes the analysis methodology
- **Part stress analysis**
  - Part derating shall be implemented in conformance with ECSS-Q-ST-30-11 to assure that the stress level applied to all the EEE parts are within the limits
- **Zonal analysis**
- **Failure Detection Isolation and Recovery (FDIR) analysis**
  - ECSS-E-ST-70-11 provides the description of the FDIR process

What should be noted on section 6?

Some practical remarks and considerations on the “dependability analysis” requirements of ECSS-Q-ST-30C are:

- Dependability (& safety) analyses are the main design & operation drivers with respect to safety & mission success
- The results of dependability (& safety) analyses are used to define, optimise, justify, implement and verify dependability (& safety) requirements
- Dependability (& safety) analyses need to be used as drivers and not for verification only
- Dependability analyses provide input to safety analyses (e.g. FMEA/FMECA to hazard analysis, reliability prediction to safety risk assessment)

7 Dependability testing, demonstration and data collection

What does ECSS-Q-ST-30C Rev. 1 require on testing, demonstration and data collection ?

ECSS-Q-ST-30C Rev. 1

- Foreword
  1 Scope
  2 Normative references
- 3 Terms, definitions and abbreviated terms
- 4 Dependability programme
- 5 Dependability engineering
- 6 Dependability analyses
- 7 Dependability testing, demonstration and data collection
- 8 Pre-tailoring matrix per product types
- Annexes

→

- 7 Dependability testing, demonstration and data collection
  - 7.1 Reliability testing and demonstration
  - 7.2 Availability testing and demonstration
  - 7.3 Maintainability demonstration
  - 7.4 Dependability data collection and dependability performance monitoring

7 Dependability testing, demonstration and data collection (cont.)

Dependability testing, demonstration and data collection comprise:

- Validation or verification of dependability analyses, requirements and data (with test data)
- Data collection from system developments and dependability trend identification
- Monitoring of dependability performances in the field (in-orbit data)

What should be noted on section 7?

Some practical remarks and considerations on the “dependability testing, demonstration and data collection” requirements of ECSS-Q-ST-30C Rev. 1 are:

- Dependability testing and demonstration should be integrated with related safety verification activities
- Demonstration of the dependability of critical items is possible or meaningful primarily when critical items are physical system constituents
- Dependability data provide diagnostic support during operations

8 Pre-tailoring matrix per product types

1. What does ECSS-Q-ST-30C Rev. 1 require on pre-tailoring matrix per product types?

ECSS-Q-ST-30C Rev. 1

- Foreword
  1 Scope
  2 Normative references
- 3 Terms, definitions and abbreviated terms
- 4 Dependability programme
- 5 Dependability engineering
- 6 Dependability analyses
- 7 Dependability testing, demonstration and data collection
- 8 Pre-tailoring matrix per product types → ❑ 8 Pre-tailoring matrix per product types
- Annexes

8 Pre-tailoring matrix per product types (cont.)

- The Matrix of Table 8-2 presents the pre-tailoring of this ECSS Standard per space product type
- There are nine product types, one per column

Space system	Space segment element and sub-system	Launch segment element and sub-system	Ground segment element and sub-system	Space segment equipment	Launch segment equipment	Ground segment equipment	Ground support equipment	Software

- For each product type the possible values for each requirement are:
  - "X" when applicable
  - "-" when not applicable
  - "//" when pre-tailoring applicability not definable - to be determined during tailoring
  - "X#" when requirement is applicable except in a specific case
  - "//#" when pre-tailoring applicability not definable – however supplementary indications regarding applicability are given
- A requirement is considered applicable for a product type if it is verified on this product type

Annexes

What does ECSS-Q-ST-30C Rev. 1 require on the Annexes ?

ECSS-Q-ST-30C Rev. 1

- Foreword
  1 Scope
  2 Normative references
- 3 Terms, definitions and abbreviated terms
- 4 Dependability programme
- 5 Dependability engineering
- 6 Dependability analyses
- 7 Dependability testing, demonstration and data collection
- 8 Pre-tailoring matrix per product types
- Annexes →

- ❑ Annex A (informative) Relationship between dependability activities and project phases
- ❑ Annex B (informative) Dependability documents delivery per review
- ❑ Annex C (normative) Dependability plan – DRD
- ❑ Annex D (normative) Contingency analysis – DRD
- ❑ Annex E (normative) Reliability prediction – DRD
- ❑ Annex F (normative) Failure Detection Identification and Recovery – DRD
- ❑ Annex G (normative) Zonal analysis – DRD
- ❑ Annex H (normative) Maintainability analysis – DRD
- ❑ Annex I (normative) Common-cause analysis – DRD
- ❑ Annex J (normative) Worst Case Analysis – DRD
- ❑ Annex K DELETED
- ❑ Annex L (informative) Common-cause check lists
- ❑ Bibliography

Annexes (cont.)

There are two types of annexes, i.e. informative and normative plus bibliography

Informative

- Relationship between dependability activities and programme phases
- Dependability documents delivery per review
- Common-cause check lists

Normative (DRDs)

- Dependability plan
- Contingency analysis
- Reliability prediction
- Failure Detection Identification and Recovery Analysis
- Zonal analysis
- Maintainability analysis
- Common-cause analysis
- Worst Case Analysis

What should be noted on the Annexes?

Some practical remarks and considerations on the Annexes are:

- Normative annexes provide DRD's of the required plan or analysis
  - Each DRD includes scope and applicability, description and purpose, application and interrelationships, and content
- Informative annexes provide inputs for the definition of project specific requirements on:
  - dependability activities to be performed throughout the project phases
  - DRL
  - design requirements (common-cause checklist)

End of dependability session

Standardization training program Q30 discipline: Dependability

Thank you for your attention !

Are there any questions ?