Standardization training program Q30 discipline: Dependability

28/06/2016

ESTEC-NL

Copyright

COPYRIGHT NOTICE:

By using the ECSS Training material, developed by ESA, you agree to the following conditions:

1. The training shall take place at your premises and shall be addressed to your staff (internal participants);

2. In case of a training to be given to external participants, the prior ESA written authorisation shall be requested;

3. The ESA Copyright shall always be mentioned on all Training Material used for the purpose of the training and participants shall acknowledge the ESA ownership on such a Copyright;

4. The Training material shall not be used to generate any revenues (i.e. the training and Training Material shall be "free of charge" excl. any expenses for the training organisation);

5. Only non-editable PDF files of the Training Material can be distributed to the participants (nor power point presentations);

6. Any deficiency identified in the Training Material shall be reported to the ECSS secretariat;

7. If the Training Material is modified or translated, the ESA Copyright on such edited Training Material shall be clearly mentioned. A copy of the edited Training Material shall be delivered to ESA for information.

8. You shall always hold harmless, indemnify and keep ESA indemnified against any and all costs, damages and expenses incurred by ESA or for which ESA may become liable, with respect to any claim by third parties related to the use of the Training Material.

Introduction

❑ 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

❑ 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

❑ Consider relevant interfaces to other disciplines (such as quality assurance, software product assurance, configuration management, safety, risk management, ...) and ECSS standards

Contents

❏ Introduction to dependability basic concepts

❏ Introduction to and overview of ECSS-Q-ST-30C

❏ Detailed contents of ECSS-Q-ST-30C and practical considerations

❏ Time for questions

Introduction to dependability
What is dependability ?

Standardization
training program
Q30 discipline:
Dependability
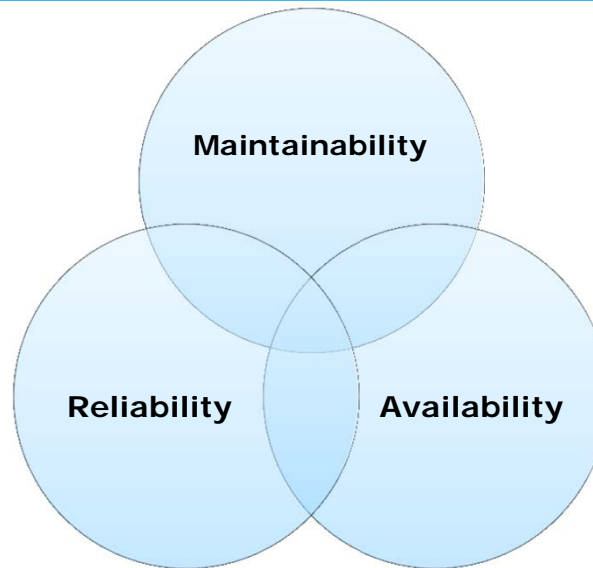
Dependability

"The collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance".

Note: Dependability is used only for general descriptions in non quantitative terms". [ECSS-P-001B, Glossary of Terms]

Dependability is also addressed by the acronym RAM (Reliability, Availability and Maintainability)

Introduction to dependability
What is dependability ? (cont.)

Standardization
training program
Q30 discipline:
Dependability

- 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"
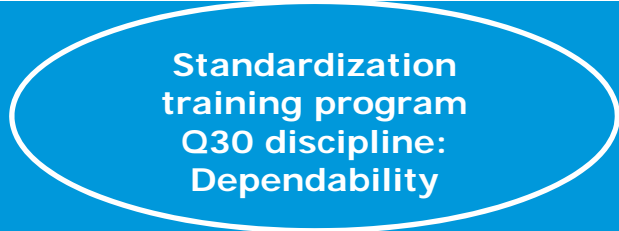
Introduction to dependability
What is dependability ? (cont.)

Standardization
training program
Q30 discipline:
Dependability

❑ **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 !

Introduction to dependability
Why is dependability important ?

Standardization
training program
Q30 discipline:
Dependability

- ❑ **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, …)

❑ 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 ?
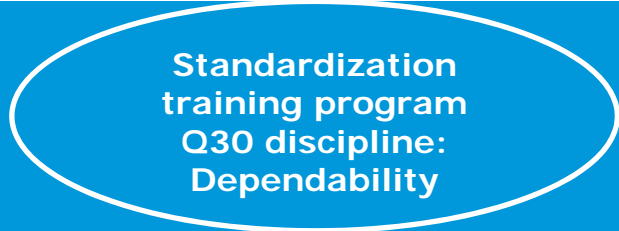
❑ **Qualitative requirements**

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

Introduction to dependability
Dependability engineering

Standardization
training program
Q30 discipline:
Dependability

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

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.

Make use of it!

Introduction to dependability
Dependability assurance basic principles and objectives

Standardization
training program
Q30 discipline:
Dependability

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 ?

❏ ECSS-Q-ST-30C 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
6 March 2009

EUROPEAN COOPERATION
ECSS
FOR SPACE STANDARDIZATION

Space product assurance

Dependability

ECSS Secretariat
ESA-ESTEC
Requirements & Standards Division
Noordwijk, The Netherlands

ECSS-Q-ST-30C

What is ECSS-Q-ST-30C ? (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 (6 March 2009)

ECSS-Q-ST-30C
6 March 2009

EUROPEAN COOPERATION
FOR SPACE STANDARDIZATION
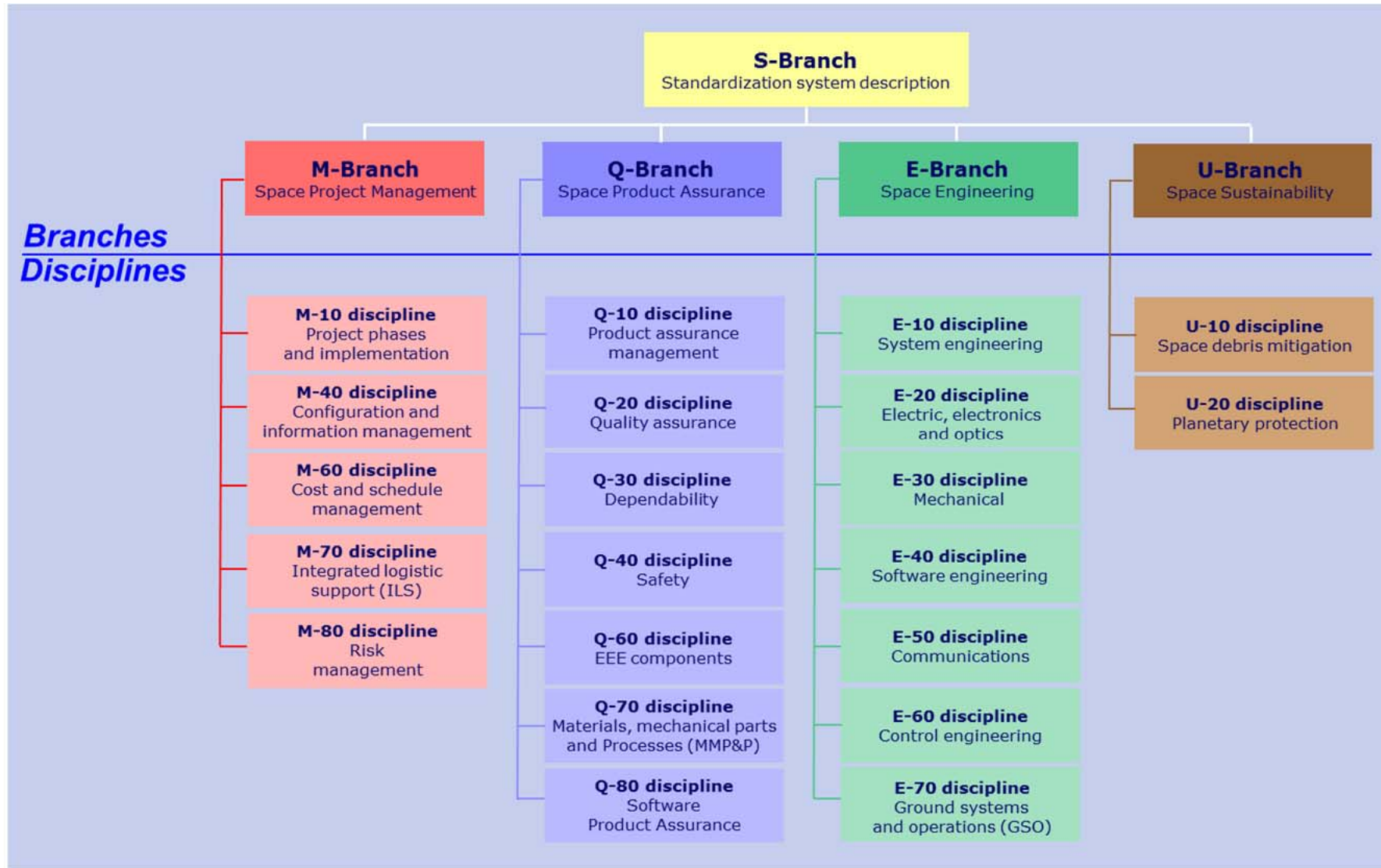
Space product assurance

Dependability

ECSS Secretariat
ESA-ESTEC
Requirements & Standards Division
Noordwijk, The Netherlands

ECSS-Q-ST-30C

Introduction to and overview of ECSS-Q-ST-30C

Overview of ECSS-Q-ST-30C

Standardization
training program
Q30 discipline:
Dependability

Introduction to and overview of ECSS-Q-ST-30C
Overview of ECSS-Q-ST-30C (cont.)

Standardization
training program
Q30 discipline:
Dependability

Structure of ECSS-Q-ST-30C

ECSS-Q-ST-30C

- 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

- Annexes

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

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

ECSS-Q-ST-30C

- 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

- Annexes

→

- ❑ Foreword
- ❑ 1 Scope
- ❑ 2 Normative references

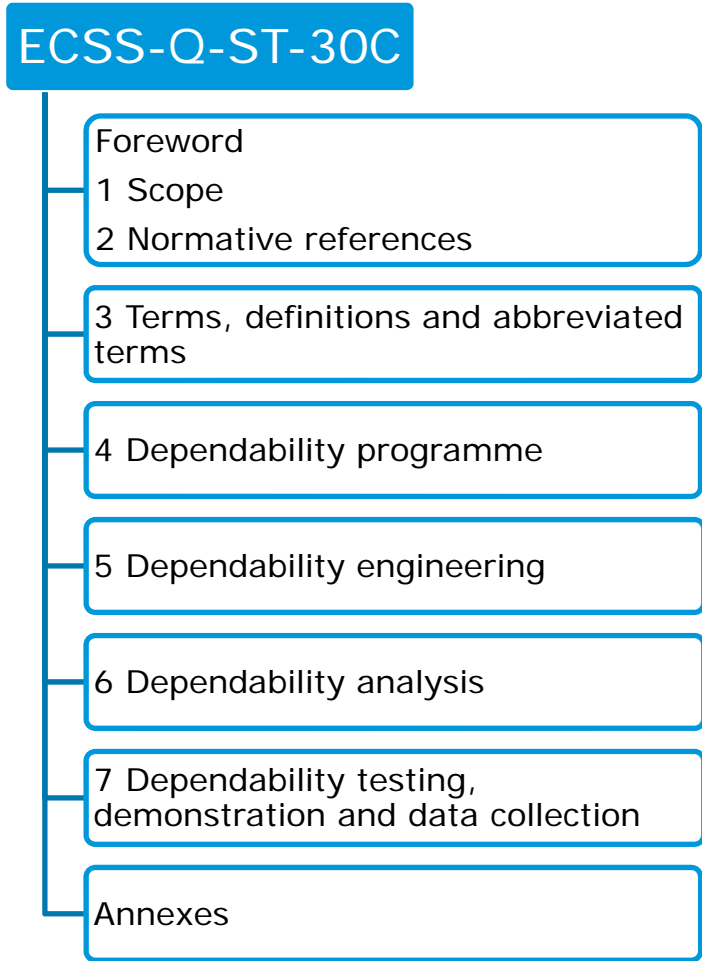**Introduction to and overview of ECSS-Q-ST-30C**
Overview of ECSS-Q-ST-30C (cont.)

Standardization
training program
Q30 discipline:
Dependability

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

ECSS-Q-ST-30C

- Foreword
  1 Scope
  2 Normative references

- 3 Terms, definitions and abbreviated terms → ❑ 3 Terms, definitions and abbreviated terms

- 4 Dependability programme

- 5 Dependability engineering

- 6 Dependability analysis

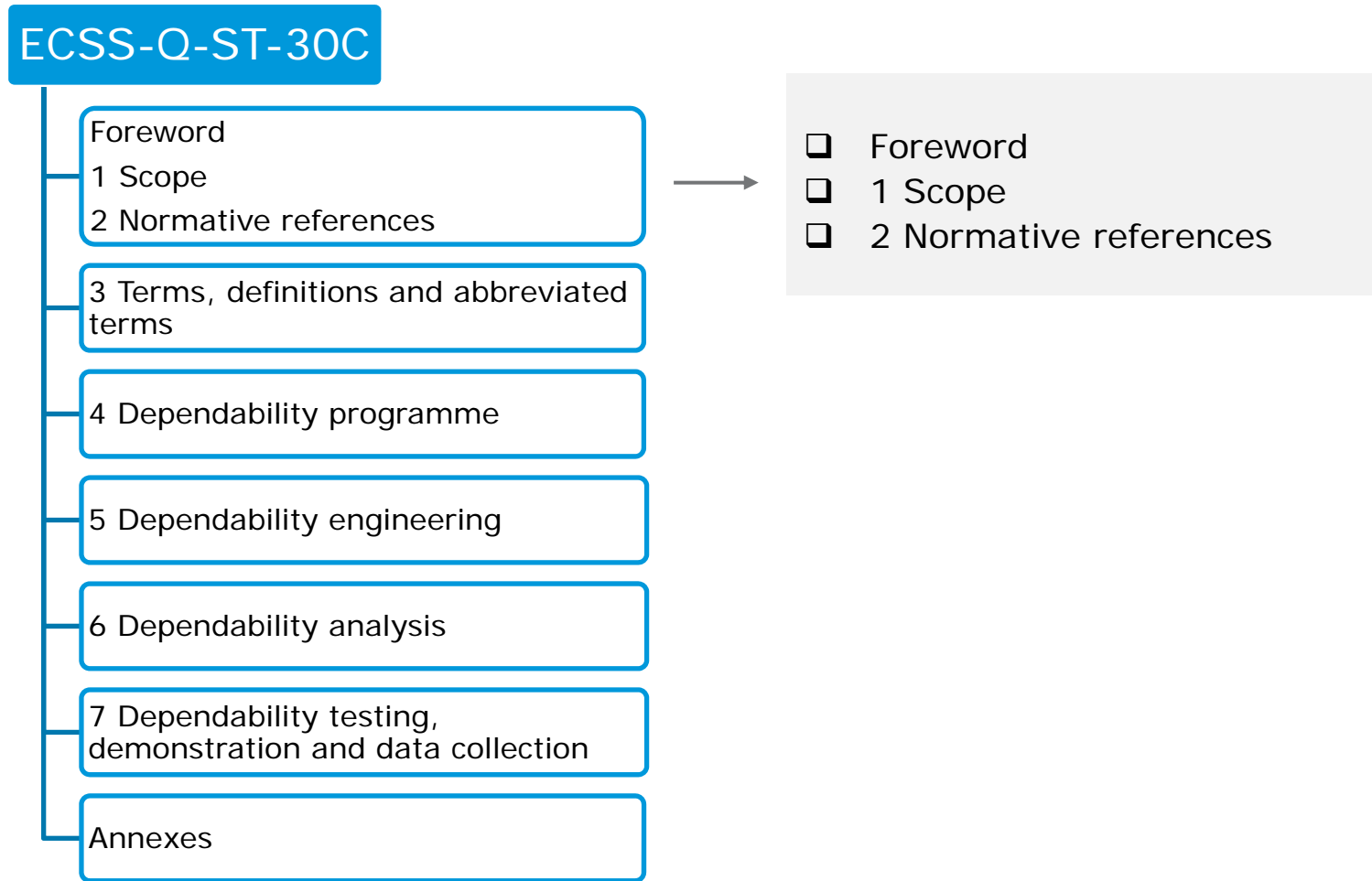- 7 Dependability testing, demonstration and data collection

- Annexes

Introduction to and overview of ECSS-Q-ST-30C
Overview of ECSS-Q-ST-30C (cont.)

Standardization training program Q30 discipline: Dependability
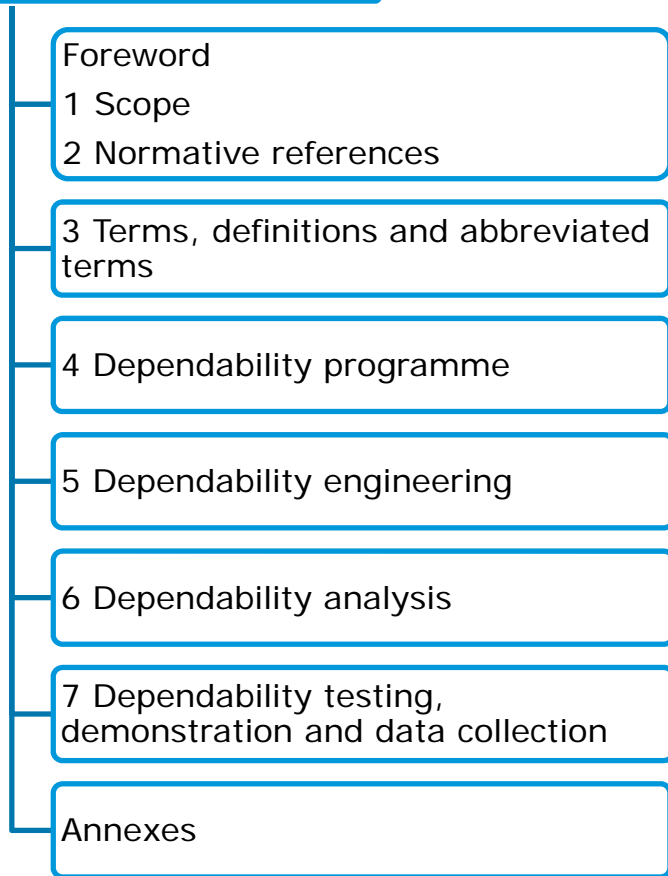
What are the contents of ECSS-Q-ST-30C ?

ECSS-Q-ST-30C

- 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

- 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

Introduction to and overview of ECSS-Q-ST-30C
Overview of ECSS-Q-ST-30C (cont.)

Standardization training program Q30 discipline: Dependability

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

ECSS-Q-ST-30C

- 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

- 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 Classification of critical functions and products
  - ▪ 5.5 Involvement in testing process
  - ▪ 5.6 Involvement in operational aspects
  - ▪ 5.7 Dependability recommendations

Introduction to and overview of ECSS-Q-ST-30C
Overview of ECSS-Q-ST-30C (cont.)

Standardization training program Q30 discipline: Dependability

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

ECSS-Q-ST-30C

- 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

- 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 List

Introduction to and overview of ECSS-Q-ST-30C
Overview of ECSS-Q-ST-30C (cont.)

Standardization training program Q30 discipline: Dependability

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

ECSS-Q-ST-30C

- 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 →

- Annexes

❑ 7 Dependability testing, demonstration and data collection
  - 7.1 Reliability testing and demonstration
  - 7.2 Availability testing and demonstration
  - 7.3 Maintainability demonstration
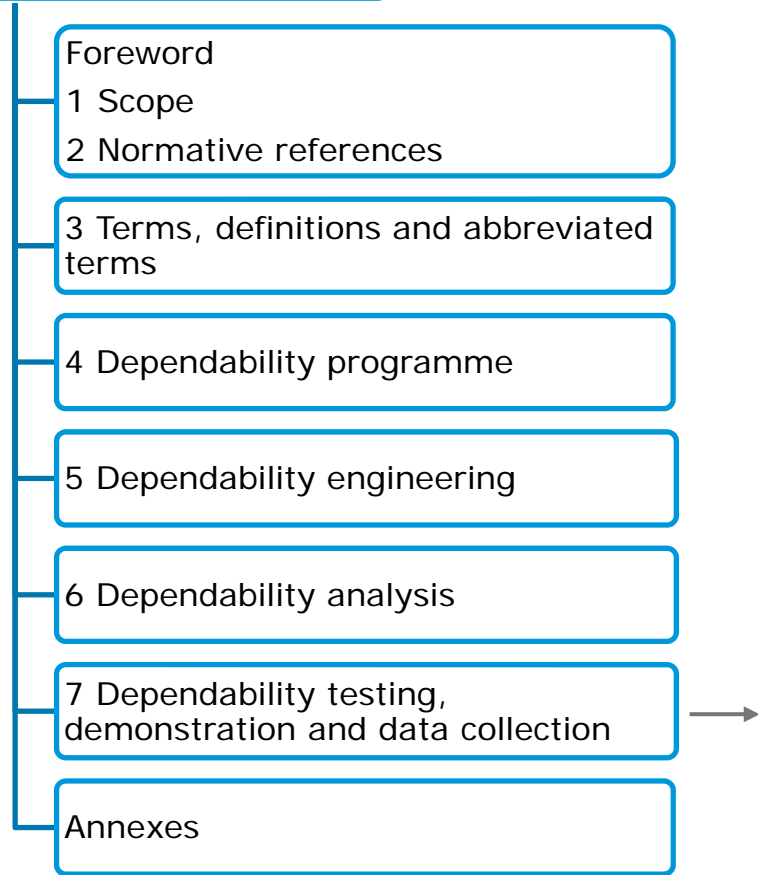 - 7.4 Dependability data collection and dependability performance monitoring
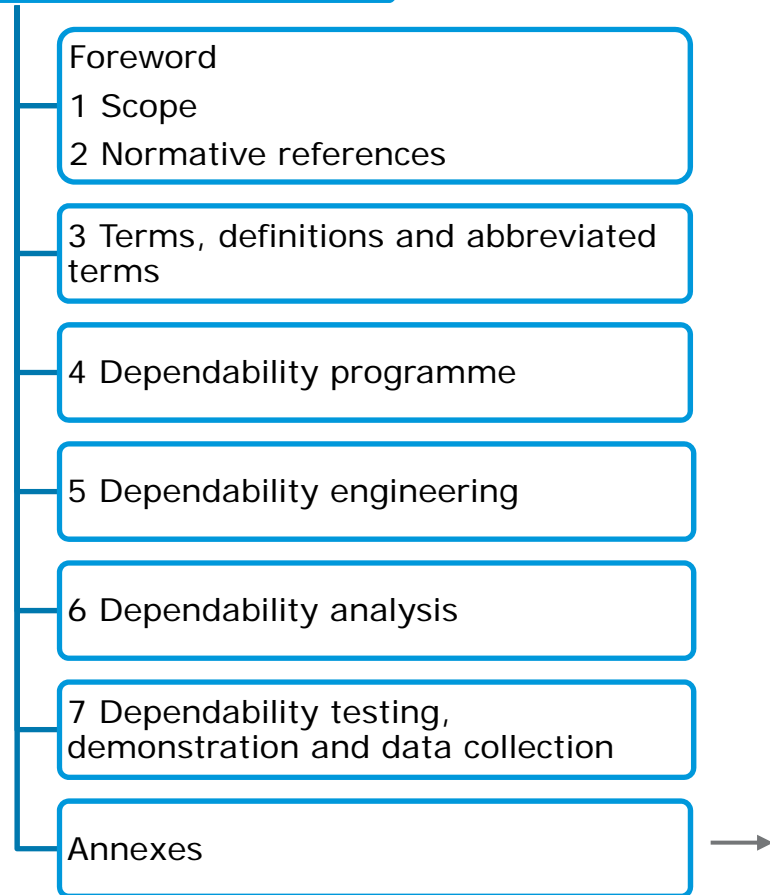
Introduction to and overview of ECSS-Q-ST-30C
Overview of ECSS-Q-ST-30C (cont.)

Standardization
training program
Q30 discipline:
Dependability

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

ECSS-Q-ST-30C

- 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

- Annexes →

- ❑ Annex A (informative) Relationship between dependability activities and project phases
- ❑ Annex B (informative) Document requirement list (DRL)
- ❑ 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 (informative) Analyses applicability matrix
- ❑ Annex L (informative) Common-cause check lists
- ❑ Bibliography

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

Standardization training program Q30 discipline: Dependability

This training session provides:

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

What does ECSS-Q-ST-30C start with?

ECSS-Q-ST-30C

- 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

- Annexes

→

- ❏ Foreword
- ❏ 1 Scope
- ❏ 2 Normative references

Detailed contents and practical considerations
Foreword

Standardization
training program
Q30 discipline:
Dependability

The foreword of ECSS-Q-ST-30C:

❑ 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 and B (change log)

Detailed contents and practical considerations
1 Scope

Standardization
training program
Q30 discipline:
Dependability

The scope of ECSS-Q-ST-30C 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

Detailed contents and practical considerations
What should be noted on section 1?

Standardization
training program
Q30 discipline:
Dependability

Some practical remarks and considerations on the "scope" of ECSS-Q-ST-30C 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

ECSS-Q-ST-30C 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

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

ECSS-Q-ST-30C

- Foreword
  1 Scope
  2 Normative references

- 3 Terms, definitions and abbreviated terms → ❑ 3 Terms, definitions and abbreviated terms

- 4 Dependability programme

- 5 Dependability engineering

- 6 Dependability analysis

- 7 Dependability testing, demonstration and data collection
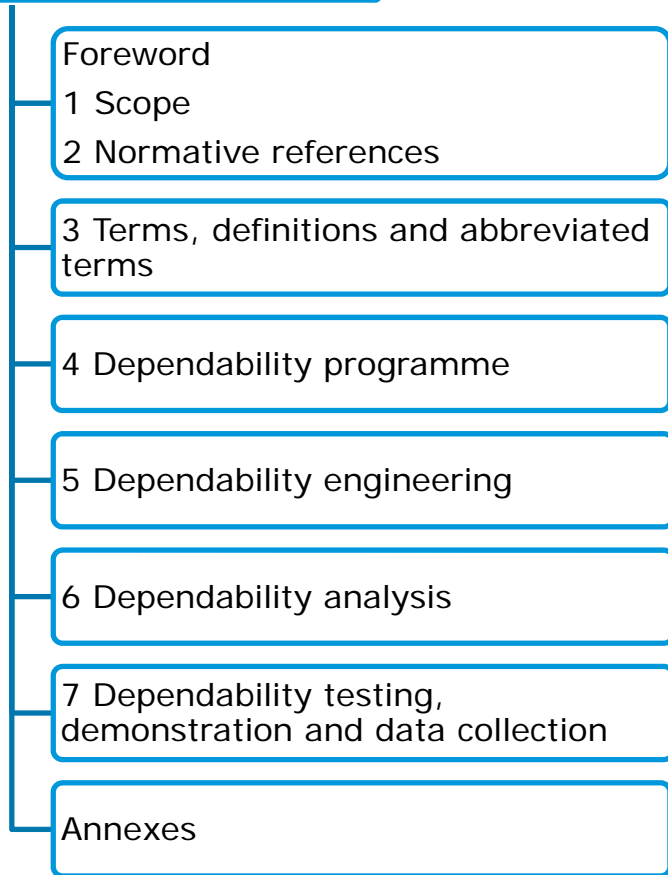
- Annexes

Detailed contents and practical considerations
3 Terms, definitions and abbreviated terms (cont.)

Standardization
training program
Q30 discipline:
Dependability

ECSS-Q-ST-30C 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
- ❑ **Space element:** product intended to be operated in space (adapted from ECSS-ST-00-01B)
- ❑ **Space segment:** one or more space elements
- ❑ **Limited-life item:** item 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

All other definitions are given in the ECSS glossary of terms (ECSS-ST-00-01B)
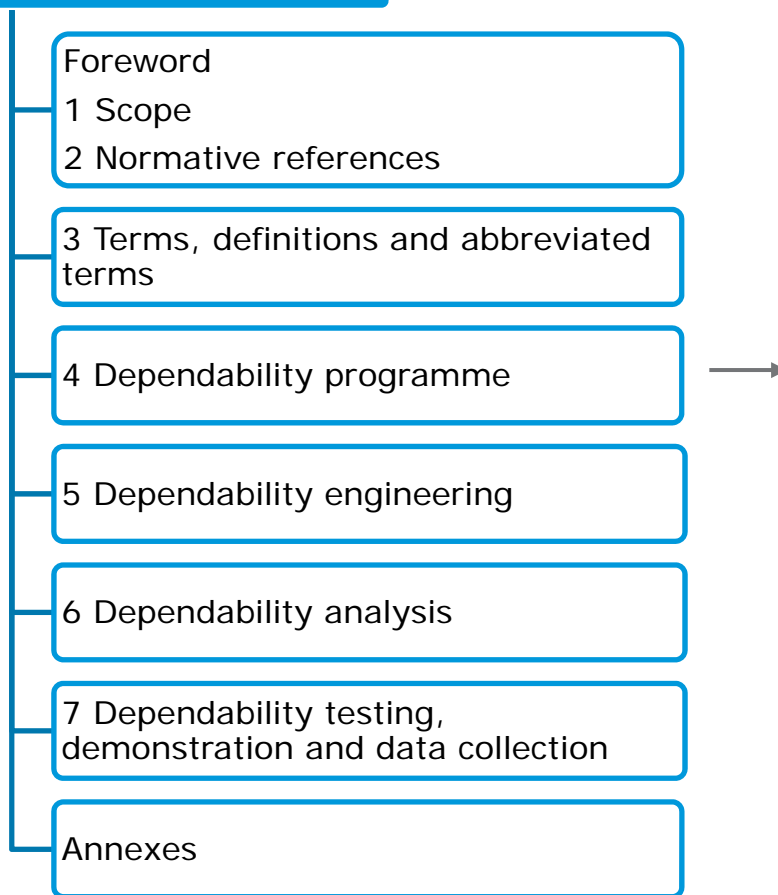
Detailed contents and practical considerations
4 Dependability programme

Standardization
training program
Q30 discipline:
Dependability

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

ECSS-Q-ST-30C

Foreword
1 Scope
2 Normative references

3 Terms, definitions and abbreviated terms

4 Dependability programme $\rightarrow$

5 Dependability engineering

6 Dependability analysis

7 Dependability testing, demonstration and data collection

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

Detailed contents and practical considerations
4 Dependability programme (cont.)

Standardization
training program
Q30 discipline:
Dependability

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

Detailed contents and practical considerations
What should be noted on section 4?

Standardization
training program
Q30 discipline:
Dependability

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

Detailed contents and practical considerations
5 Dependability engineering

Standardization
training program
Q30 discipline:
Dependability

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

ECSS-Q-ST-30C

- 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

- 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 Classification of critical functions and products
  ▪ 5.5 Involvement in testing process
  ▪ 5.6 Involvement in operational aspects
  ▪ 5.7 Dependability recommendations

Detailed contents and practical considerations
5 Dependability engineering (cont.)

**Standardization
training program
Q30 discipline:
Dependability**

What are the key ingredients of dependability engineering ?

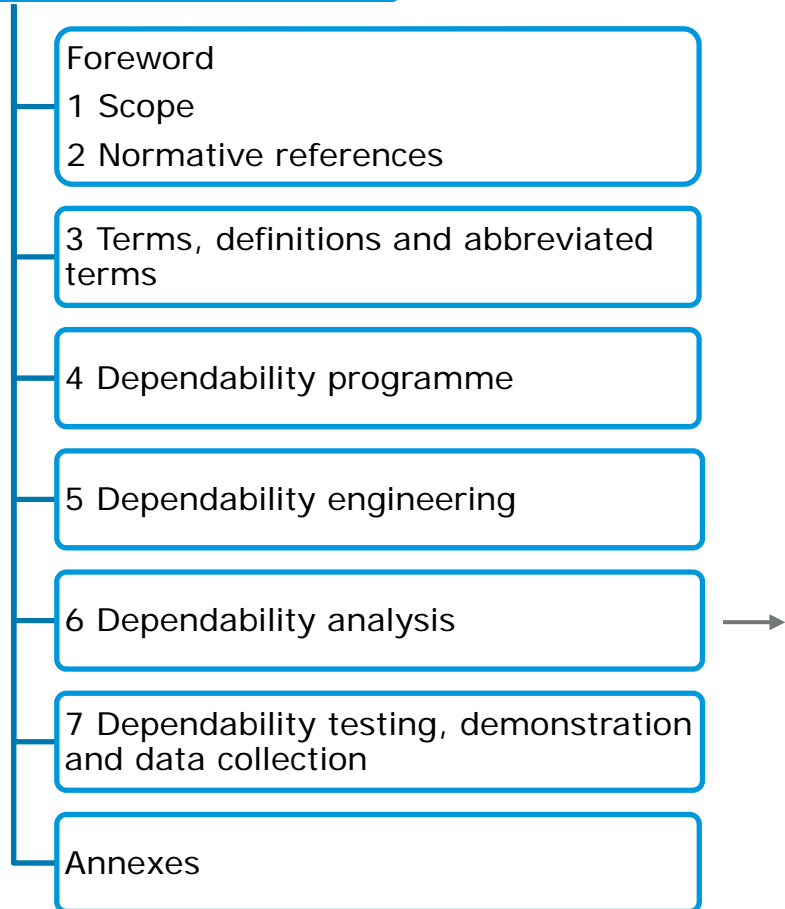Dependability engineering involves and is based on:

- ❑ Integration of dependability in the project

- ❑ Dependability requirements in technical specifications

- ❑ Dependability design criteria including:
    - ❑ mission success criteria
    - ❑ design approach
    - ❑ failure tolerance requirements
    - ❑ severity classification

- ❑ Classification of critical functions and products

- ❑ Involvement in test definition and operational aspects

- ❑ Dependability recommendations in support of the risk reduction process

Detailed contents and practical considerations
What should be noted on section 5?

Standardization training program Q30 discipline: Dependability

Some practical remarks and considerations on the "dependability engineering" requirements of ECSS-Q-ST-30C 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) !

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

ECSS-Q-ST-30C

- 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
- 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 List

Detailed contents and practical considerations
6 Dependability analyses (cont.)

Standardization
training program
Q30 discipline:
Dependability

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 analysis and objectives

❑ Identification and listing of dependability critical items

  ❑ The dependability critical items shall be documented in conformance with ECSS-Q-ST-10-04

Detailed contents and practical considerations
6 Dependability analyses (cont.)

Standardization
training program
Q30 discipline:
Dependability

What are the dependability analysis requirements and methods ?

The ECSS Dependability analyses and methods comprise:

- Reliability analyses

- Maintainability analyses

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

Detailed contents and practical considerations
6 Dependability analyses (cont.)

Standardization
training program
Q30 discipline:
Dependability

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

❑ **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-30-02C is specifically dedicated to these analyses

❑ **Hardware Software Interaction Analysis (HSIA)**
   ❑ ECSS-Q-ST-30-02C contains a section dedicated to this analysis

❑ **Contingency analysis**

❑ **Fault Tree Analysis (FTA)**
   ❑ ECSS-Q-ST-40-12 is a guideline for this analysis

Detailed contents and practical considerations
6 Dependability analyses (cont.)

Standardization
training program
Q30 discipline:
Dependability

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

❑ **Common-cause analysis**

    ❑ An example of check list of generic common-cause parameters is provided in Annex L of ECSS-Q-ST-30C

❑ **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

Detailed contents and practical considerations
What should be noted on section 6?

Standardization
training program
Q30 discipline:
Dependability

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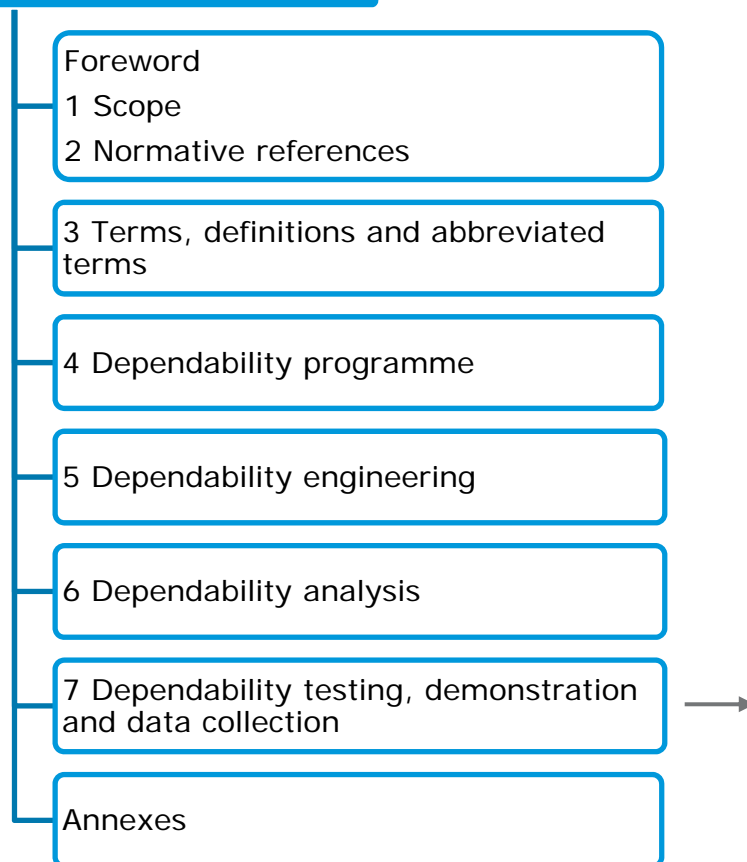
What does ECSS-Q-ST-30C require on testing, demonstration and data collection ?

ECSS-Q-ST-30C

- 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 →

- 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

Detailed contents and practical considerations
7 Dependability testing, demonstration and data collection (cont.)

Standardization training program Q30 discipline: Dependability

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)

Detailed contents and practical considerations
What should be noted on section 7?

Standardization
training program
Q30 discipline:
Dependability

Some practical remarks and considerations on the "dependability testing, demonstration and data collection" requirements of ECSS-Q-ST-30C 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

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

ECSS-Q-ST-30C

- 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

- Annexes →

❑ Annex A (informative) Relationship between dependability activities and project phases
❑ Annex B (informative) Document requirement list (DRL)
❑ 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 (informative) Analyses applicability matrix
❑ Annex L (informative) Common-cause check lists
❑ Bibliography

Detailed contents and practical considerations

Annexes (cont.)

Standardization
training program
Q30 discipline:
Dependability

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

Informative

- ❑ Relationship between dependability activities and programme phases
- ❑ Document requirement list
- ❑ Analyses applicability matrix
- ❑ Common-cause check lists

Normative (DRDs)

- ❑ dependability plan
- ❑ contingency analysis
- ❑ reliability prediction
- ❑ failure detection identification and recovery
- ❑ zonal analysis
- ❑ maintainability analysis
- ❑ common-cause analysis
- ❑ worst case analysis

Detailed contents and practical considerations
What should be noted on the Annexes?

Standardization
training program
Q30 discipline:
Dependability

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
  ❑ analyses applicability matrix to support project reviews
  ❑ design requirements (common-cause checklist)

Thank you for your attention !

Are there any questions ?