

Table of contents

| | |
|--|-----------|
| European Foreword | 6 |
| 1 Scope | 7 |
| 2 Normative references | 8 |
| 3 Terms, definitions and abbreviated terms | 9 |
| 3.1 Terms from other standards..... | 9 |
| 3.2 Terms specific to the present standard | 9 |
| 3.3 Abbreviated terms..... | 10 |
| 3.4 Nomenclature | 11 |
| 4 Dependability programme | 12 |
| 4.1 General..... | 12 |
| 4.2 Organization | 12 |
| 4.3 Dependability programme plan | 12 |
| 4.4 Dependability risk assessment and control | 13 |
| 4.5 Dependability critical items | 13 |
| 4.6 Design reviews | 14 |
| 4.7 Dependability Lessons learnt..... | 14 |
| 4.8 Progress reporting | 14 |
| 4.9 Documentation | 14 |
| 5 Dependability engineering | 15 |
| 5.1 Integration of dependability in the project..... | 15 |
| 5.2 Dependability requirements in technical specification | 15 |
| 5.3 Dependability design criteria | 16 |
| 5.3.1 General | 16 |
| 5.3.2 Consequences | 16 |
| 5.3.3 Failure tolerance | 17 |
| 5.3.4 Design approach..... | 18 |
| 5.4 Criticality classification..... | 19 |
| 5.4.1 Classification of critical functions, hardware and operations..... | 19 |
| 5.4.2 Assignment of software criticality category | 20 |
| 5.5 Involvement in testing process..... | 21 |

| | | |
|------------------------------|--|-----------|
| 5.6 | Involvement in operational aspects | 21 |
| 5.7 | Dependability recommendations | 22 |
| 6 | Dependability analyses | 23 |
| 6.1 | Identification and classification of undesirable events | 23 |
| 6.2 | Assessment of failure scenarios | 23 |
| 6.3 | Dependability analyses and the project life cycle | 23 |
| 6.4 | Dependability analyses - methods | 24 |
| 6.4.1 | General | 24 |
| 6.4.2 | Reliability analyses | 25 |
| 6.4.3 | Maintainability analyses | 28 |
| 6.4.4 | Availability analysis | 28 |
| 6.5 | Dependability Critical Items Criteria | 29 |
| 7 | Dependability testing, demonstration and data collection | 30 |
| 7.1 | Reliability testing and demonstration | 30 |
| 7.2 | Availability testing and demonstration | 30 |
| 7.3 | Maintainability demonstration | 30 |
| 7.4 | Dependability data collection and dependability performance monitoring | 31 |
| 8 | Pre-tailoring matrix per product types | 32 |
| Annex A (informative) | Relationship between dependability activities and project phases | 41 |
| A.1 | Mission analysis / Needs identification phase (phase 0) | 41 |
| A.2 | Feasibility phase (phase A) | 41 |
| A.3 | Preliminary definition phase (phase B) | 41 |
| A.4 | Detailed definition and production/ground qualification testing phases (phase C/D) | 42 |
| A.5 | Utilization phase (phase E) | 42 |
| A.6 | Disposal phase (phase F) | 43 |
| Annex B (informative) | Dependability documents delivery per review | 44 |
| Annex C (normative) | Dependability plan - DRD | 47 |
| C.1 | DRD identification | 47 |
| C.1.1 | Requirement identification and source document | 47 |
| C.1.2 | Purpose and objective | 47 |
| C.2 | Expected response | 47 |
| C.2.1 | Scope and content | 47 |
| C.2.2 | Special remarks | 48 |

| | |
|---|-----------|
| Annex D (normative) Contingency analysis – DRD | 49 |
| D.1 DRD identification | 49 |
| D.1.1 Requirement identification and source document | 49 |
| D.1.2 Purpose and objective..... | 49 |
| D.2 Expected response | 49 |
| D.2.1 Scope and content | 49 |
| D.2.2 Special remarks | 49 |
| Annex E (normative) Reliability prediction – DRD | 51 |
| E.1 DRD identification | 51 |
| E.1.1 Requirement identification and source document..... | 51 |
| E.1.2 Purpose and objective..... | 51 |
| E.2 Expected response | 52 |
| E.2.1 Scope and content | 52 |
| E.2.2 Special remarks | 52 |
| Annex F (normative) Failure Detection Identification and Recovery Analysis – DRD | 53 |
| F.1 DRD identification | 53 |
| F.1.1 Requirement identification and source document..... | 53 |
| F.1.2 Purpose and objective..... | 53 |
| F.2 Expected response | 53 |
| F.2.1 Scope and content | 53 |
| F.2.2 Special remarks | 54 |
| Annex G (normative) Zonal analysis – DRD | 55 |
| G.1 DRD identification | 55 |
| G.1.1 Requirement identification and source document..... | 55 |
| G.1.2 Purpose and objective..... | 55 |
| G.2 Expected response | 55 |
| G.2.1 Scope and content | 55 |
| G.2.2 Special remarks | 55 |
| Annex H (normative) Maintainability analysis – DRD | 56 |
| H.1 DRD identification | 56 |
| H.1.1 Requirement identification and source document..... | 56 |
| H.1.2 Purpose and objective..... | 56 |
| H.2 Expected response | 56 |
| H.2.1 Scope and content | 56 |
| H.2.2 Special remarks | 57 |

| | |
|---|-----------|
| Annex I (normative) Common-cause analysis – DRD | 58 |
| I.1 DRD identification | 58 |
| I.1.1 Requirement identification and source document | 58 |
| I.1.2 Purpose and objective | 58 |
| I.2 Expected response | 58 |
| I.2.1 Scope and content | 58 |
| I.2.2 Special remarks | 58 |
| Annex J (normative) Worst Case Analysis – DRD | 59 |
| J.1 DRD identification | 59 |
| J.1.1 Requirement identification and source document | 59 |
| J.1.2 Purpose and objective | 59 |
| J.2 Expected response | 59 |
| J.2.1 Scope and content | 59 |
| J.2.2 Special remarks | 59 |
| Annex K <<deleted>> | 61 |
| Annex L (informative) Common-cause check lists..... | 62 |
| Bibliography..... | 65 |
| Tables | |
| Table 5-1: Severity categories | 17 |
| Table 5-2: Criticality of functions..... | 19 |
| Table 5-3: Criticality category assignment for software products vs. function criticality | 20 |
| Table 8-1: Definitions of the columns of Table 8-2..... | 33 |
| Table 8-2: Pre-Tailoring matrix per “Space product types” | 34 |
| Table B-1 : Dependability deliverable documents per project review | 45 |
| Table L-1 : Common cause check list example for design | 62 |
| Table L-2 : Common cause check list example for design (continued) | 63 |
| Table L-3 : Common cause check list example for environment | 64 |
| Table L-4 : Common cause check list example for unexpected operations..... | 64 |