DIN EN 16602-40:2018-07 (E)

Space product assurance - Safety; English version EN 16602-40:2018

Inhalt

Seite

European Foreword 7

1 Scope 9

2 Normative references 10

3 Terms, definitions and abbreviated terms 11

3.1 Terms from other standards 11

3.2 Terms specific to the present standard 11

3.3 Abbreviated terms 13

3.4 Nomenclature 14

4 Safety principles 15

4.1 Objective 15

4.2 Policy 15

4.2.1 General 15

4.2.2 Implementation 15

4.3 Safety programme 16

5 Safety programme 17

5.1 Scope 17

5.2 Safety programme plan 17

5.3 Conformance 18

5.4 Safety organization 18

5.4.1 Safety manager 18

5.4.2 Safety manager access and authority 18

5.4.3 Safety audits 19

5.4.4 Approval of documentation 19

5.4.5 Approval of hazardous operations 19

5.4.6 Representation on boards 19

5.4.7 Safety approval authority 20

5.5 Safety risk assessment and control 20

5.6 Safety critical items 20

5.7 Project phases and safety review cycle 20

5.7.1 Safety program tasks and reviews 20
5.7.2 Progress meetings 24
5.7.3 Safety reviews....24
5.8 Safety compliance demonstration 25
5.9 Safety training....25
5.9.1 General....25
5.9.2 Product specific training 25
5.9.3 General awareness briefings....26
5.9.4 Basic technical training 26
5.9.5 Training records 26
5.10 Accident-incident reporting and investigation 26
5.11 Safety documentation 26
5.11.1 General....26
5.11.2 Safety data package 27
5.11.3 Safety deviations and waivers....27
5.11.4 Safety lessons learned....28
5.11.5 Documentation of safety critical items 28
6 Safety engineering 29
6.1 Overview 29
6.2 Safety requirements identification and traceability 29
6.3 Safety design objectives 29
6.3.1 Safety policy and principles....29
6.3.2 Design selection....29
6.3.3 Hazard reduction precedence 30
6.3.4 Environmental compatibility....32
6.3.5 External services....32
6.3.6 Hazard detection - signalling and safing....32
6.3.7 Space debris mitigation....33
6.3.8 Atmospheric re-entry....33
6.3.9 Safety of Earth return missions 33
6.3.10 Safety of human spaceflight missions 34
6.3.11 Access 34
6.4 Safety risk reduction and control....34
6.4.1 Severity of hazardous event and function criticality 34
6.4.2 Failure tolerance requirements....36
6.4.3 Design for minimum risk....37
6.4.4 Probabilistic safety targets 38

6.5 Identification and control of safety-critical functions 39
6.5.1 Identification 39
6.5.2 Inadvertent operation 39
6.5.3 Status information 39
6.5.4 Safe shutdown and failure tolerance requirements 39
6.5.5 Electronic, electrical, electromechanical components 40
6.5.6 Software functions 40
6.6 Operational Safety 42
6.6.1 Basic requirements 42
6.6.2 Flight operations and mission control 42
6.6.3 Ground operations 43

7 Safety analysis requirements and techniques 46
7.1 Overview 46
7.2 General 46
7.3 Assessment and allocation of requirements 47
7.3.1 Safety requirements 47
7.3.2 Additional safety requirements 47
7.3.3 Define safety requirements - functions 47
7.3.4 Define safety requirements - subsystems 47
7.3.5 Justification 47
7.3.6 Functional and subsystem specification 47
7.4 Safety analyses during the project life cycle 47
7.5 Safety analyses 48
7.5.1 General 48
7.5.2 Hazard analysis 48
7.5.3 Safety risk assessment 49
7.5.4 Supporting assessment and analysis 49

8 Safety verification 53
8.1 General 53
8.2 Hazard reporting and review 53
8.2.1 Hazard reporting system 53
8.2.2 Safety status review 53
8.2.3 Documentation 53
8.3 Safety verification methods 54
8.3.1 Verification engineering and planning 54
8.3.2 Methods and reports 54
8.3.3 Analysis 54

8.3.4 Inspections 54
8.3.5 Verification and approval 55
8.4 Verification of safety-critical functions 55
8.4.1 Validation 55
8.4.2 Qualification 55
8.4.3 Failure tests 56
8.4.4 Verification of design or operational characteristics 56
8.4.5 Safety verification testing 56
8.5 Hazard close-out 56
8.5.1 Safety assurance verification 56
8.5.2 Hazard close-out verification 57
8.6 Declaration of conformity of ground equipment 57

Annex A (informative) Analyses applicability matrix 58

Annex B (normative) Safety programme plan - DRD 60
B.1 DRD identification 60
B.1.1 Requirement identification and source document 60
B.1.2 Purpose and objective 60
B.2 Expected response 60
B.2.1 Contents 60
B.2.2 Special remarks 61

Annex C (normative) Safety verification tracking log (SVTL) DRD 62
C.1 DRD identification 62
C.1.1 Requirement identification and source document 62
C.1.2 Purpose and objective 62
C.2 Expected response 62
C.2.1 Contents 62
C.2.2 Special remarks 64

Annex D (normative) Safety analysis report including hazard reports - DRD 66
D.1 DRD identification 66
D.1.1 Requirement identification and source document 66
D.1.2 Purpose and objective 66
D.2 Expected response 66
D.2.1 Contents 66
D.2.2 Special remarks 67

Annex E (informative) Criteria for probabilistic safety targets 68

E.1 Objectives of probabilistic safety targets 68
E.2 Criteria for probabilistic safety targets 68

Annex F (informative) Applicability guidelines 69

Annex G (informative) European legislation and 'CE' marking 75

G.1 Overview 75
G.2 CE mark 75
G.3 Responsibility of the design authority 75
G.4 Declaration of conformity 76
G.5 References 76

Bibliography 78

Figures

Figure C-1 : Safety verification tracking log (SVTL) 65

Tables

Table 6-1: Severity categories 36
Table 6-2: Criticality of functions 36
Table 6-3: Criticality category assignment for software products vs. function criticality 41

Table A-1 : Safety deliverable documents 59