DIN EN 16602-80:2019-02 (E)

Space product assurance - Software product assurance; English version EN 16602-80:2018

Table of contents

European Foreword 7

1 Scope 8

2 Normative references 9

3 Terms, definitions and abbreviated terms 10

3.1 Terms for other standards 10

3.2 Terms specific to the present standard 10

3.3 Abbreviated terms 16

3.4 Nomenclature 18

4 Space system software product assurance principles 19

4.1 Introduction 19

4.2 Organization of this Standard 20

4.3 Tailoring of this Standard 22

5 Software product assurance programme implementation 23

5.1 Organization and responsibility 23

5.1.1 Organization 23

5.1.2 Responsibility and authority 23

5.1.3 Resources 24

5.1.4 Software product assurance manager/engineer 24

5.1.5 Training 24

5.2 Software product assurance programme management 25

5.2.1 Software product assurance planning and control 25

5.2.2 Software product assurance reporting 26

5.2.3 Audits 27

5.2.4 Alerts 27

5.2.5 Software problems 27

5.2.6 Nonconformances 28

5.2.7 Quality requirements and quality models 29

5.3 Risk management and critical item control 29
5.3.1 Risk management 29
5.3.2 Critical item control 29
5.4 Supplier selection and control 30
5.4.1 Supplier selection 30
5.4.2 Supplier requirements 30
5.4.3 Supplier monitoring 30
5.4.4 Criticality classification 31
5.5 Procurement 31
5.5.1 Procurement documents 31
5.5.2 Review of procured software component list 31
5.5.3 Procurement details 32
5.5.4 Identification 32
5.5.5 Inspection 32
5.5.6 Exportability 32
5.6 Tools and supporting environment 32
5.6.1 Methods and tools 32
5.6.2 Development environment selection 33
5.7 Assessment and improvement process 34
5.7.1 Process assessment 34
5.7.2 Assessment process 34
5.7.3 Process improvement 35

6 Software process assurance 37

6.1 Software development life cycle 37
6.1.1 Life cycle definition 37
6.1.2 Process quality objectives 37
6.1.3 Life cycle definition review 37
6.1.4 Life cycle resources 37
6.1.5 Software validation process schedule 38
6.2 Requirements applicable to all software engineering processes 38
6.2.1 Documentation of processes 38
6.2.2 Software dependability and safety 39
6.2.3 Handling of critical software 41
6.2.4 Software configuration management 43
6.2.5 Process metrics 45
6.2.6 Verification 46
6.2.7 Reuse of existing software 49

6.2.8 Automatic code generation....52
6.3 Requirements applicable to individual software engineering processes or activities....53
6.3.1 Software related system requirements process....53
6.3.2 Software requirements analysis....53
6.3.3 Software architectural design and design of software items....55
6.3.4 Coding....56
6.3.5 Testing and validation....57
6.3.6 Software delivery and acceptance....62
6.3.7 Operations....63
6.3.8 Maintenance....64
7 Software product quality assurance....66
7.1 Product quality objectives and metrication....66
7.1.1 Deriving of requirements....66
7.1.2 Quantitative definition of quality requirements....66
7.1.3 Assurance activities for product quality requirements....66
7.1.4 Product metrics....66
7.1.5 Basic metrics....67
7.1.6 Reporting of metrics....67
7.1.7 Numerical accuracy....67
7.1.8 Analysis of software maturity....68
7.2 Product quality requirements....68
7.2.1 Requirements baseline and technical specification....68
7.2.2 Design and related documentation....69
7.2.3 Test and validation documentation....69
7.3 Software intended for reuse....70
7.3.1 Customer requirements....70
7.3.2 Separate documentation....70
7.3.3 Self-contained information....70
7.3.4 Requirements for intended reuse....70
7.3.5 Configuration management for intended reuse....70
7.3.6 Testing on different platforms....71
7.3.7 Certificate of conformance....71
7.4 Standard ground hardware and services for operational system....71
7.4.1 Hardware procurement....71
7.4.2 Service procurement....71
7.4.3 Constraints....72

7.4.4 Selection 72
7.4.5 Maintenance 72
7.5 Firmware 72
7.5.1 Device programming 72
7.5.2 Marking 73
7.5.3 Calibration 73

Annex A (informative) Software documentation 74

Annex B (normative) Software product assurance plan (SPAP) - DRD 80
B.1 DRD identification 80
B.1.1 Requirement identification and source document 80
B.1.2 Purpose and objective 81
B.2 Expected response 82
B.2.1 Scope and content 82
B.2.2 Special remarks 86

Annex C (normative) Software product assurance milestone report (SPAMR) - DRD 87
C.1 DRD identification 87
C.1.1 Requirement identification and source document 87
C.1.2 Purpose and objective 88
C.2 Expected response 88
C.2.1 Scope and content 88
C.2.2 Special remarks 89

Annex D (normative) Tailoring of this Standard based on software criticality 90
D.1 Software criticality categories 90
D.2 Applicability matrix 91

Annex E (informative) List of requirements with built-in tailoring capability 102

Annex F (informative) Document organization and content at each milestone 103
F.1 Introduction 103
F.2 ECSS-Q-ST-80 Expected Output at SRR 103
F.3 ECSS-Q-ST-80 Expected Output at PDR 105
F.4 ECSS-Q-ST-80 Expected Output at CDR 110
F.5 ECSS-Q-ST-80 Expected Output at QR 112
F.6 ECSS-Q-ST-80 Expected Output at AR 113

F.7 ECSS-Q-ST-80 Expected Output not associated with any specific milestone review 115

Bibliography 117

Figures

Figure 4-1: Software related processes in ECSS Standards 20

Figure 4-2: Structure of this Standard 21

Figure A-1 : Overview of software documents 74

Tables

Table A-1 : ECSS-E-ST-40 and ECSS-Q-ST-80 Document requirements list (DRL) 75

Table B-1 : SPAP traceability to ECSS-E-ST-40 and ECSS-Q-ST-80 clauses 80

Table C-1 : SPAMR traceability to ECSS-Q-ST-80 clauses 87

Table D-1 : Software criticality categories 90

Table D-2 : Applicability matrix based on software criticality 91