ISO 14620-1:2026-08 (E)

Space systems - Safety requirements - Part 1: System safety

Contents

Page

Foreword vi

Introduction vii

1 Scope 1

2 Normative references 1

3 Terms,definitionsandabbreviatedterms 1
3.1 Terms and definitions 1
3.2 Abbreviated terms 4

4 System safety programme 4
4.1 Scope 4
4.2 Safety organization 5
4.2.1 General 5
4.2.2 Safety representative 5
4.2.3 Reporting lines 5
4.2.4 Safety integration 5
4.2.5 Coordination with others 5
4.3 Safety representative access and authority 5
4.3.1 Access 5
4.3.2 Delegated authority to reject -- Stop work 5
4.3.3 Delegated authority to interrupt operations 6
4.3.4 Conformance 6
4.3.5 Approval of reports 6
4.3.6 Review 6
4.3.7 Representation on boards 6
4.4 Safety risk management 6
4.4.1 Safety risks 6
4.4.2 Hazard assessment 6
4.4.3 Preferred measures 7
4.5 Project phases and safety review cycle 7
4.5.1 Progress meetings 7
4.5.2 Project reviews 7
4.5.3 Safety programme review 9
4.5.4 Safety data package 9
4.6 Safety programme plan 10
4.6.1 Implementation 10
4.6.2 Safety activities 10
4.6.3 Definition 10
4.6.4 Description 10
4.6.5 Safety and project engineering activities 10
4.6.6 Supplier and sub-supplier premises 10
4.6.7 Conformance 11
4.7 Safety approval process 11
4.8 Safety training 11
4.8.1 Overall training 11
4.8.2 Participation 11
4.8.3 Detailed technical training 11
4.8.4 Product specific training 11
4.8.5 Records 11
4.8.6 Identification 12

4.9 Accident and incident reporting and investigation 12
4.10 Safety documentation 12
4.10.1 General 12
4.10.2 Customer access 12
4.10.3 Supplier review 12
4.10.4 Documentation 12

4.10.5 Safety data package 12
4.10.6 Safety deviations and waivers 13
4.10.7 Safety Verification tracking log 13
4.10.8 Lessons-learned file 13

5 Safety engineering 14
5.1 Safety engineering objectives 14
5.1.1 General 14
5.1.2 Elements 14
5.1.3 Lessons learned 14
5.2 Safety design principles 14
5.2.1 Human life consideration 14
5.2.2 Design selection 14
5.2.3 System safety order of precedence 14
5.2.4 Environmental compatibility 15
5.2.5 Safe without services 15
5.2.6 Fail safe design 16
5.2.7 Hazard detection -- Signalling and safing 16
5.2.8 Access 16
5.2.9 Safety risk reduction and control 16
5.3 Failure tolerance requirements 19
5.3.1 Basic requirements 19
5.3.2 Software 19
5.3.3 Payload interface 19
5.3.4 Redundancy separation 19
5.3.5 Failure propagation 20
5.3.6 Design for minimum risk 20
5.3.7 Probabilistic safety targets 20
5.4 Identification and control of safety-critical functions 21
5.4.1 Identification 21
5.4.2 Flow-down of safety-critical functions 21
5.4.3 Inadvertent operation 21
5.4.4 Provisions 21
5.4.5 Shutdown and failure tolerance requirements 22
5.4.6 Electronic, electrical, electromechanical 22

6 Safety analysis requirements and techniques 22
6.1 General 22
6.2 Assessment and allocation of requirements 22
6.2.1 Safety requirements 22
6.2.2 Additional safety requirements 23
6.2.3 Define safety requirements -- Functions 23
6.2.4 Define safety requirements -- Subsystems 23
6.2.5 Justification 23
6.2.6 Functional and subsystem specification 23
6.3 Safety analysis 23
6.3.1 General 23
6.3.2 Mission analysis 23
6.3.3 Feasibility 23
6.3.4 Preliminary definition 23
6.3.5 Detailed definition, production and qualification 23
6.3.6 Utilization 24
6.3.7 Disposal 24
6.4 Specific safety analysis 24
6.4.1 General 24

6.4.2 Hazard analysis 24
6.4.3 Safety risk assessment 25
6.4.4 Safety analysis for hardware-software systems 25
6.5 Supporting assessment and analysis 26
6.5.1 General 26

6.5.2 Warning time analysis 26
6.5.3 Caution and warning analysis 26
6.5.4 Common cause and common mode failure analysis 27
6.5.5 Fault tree analysis 27
6.5.6 Human dependability analysis 27
6.5.7 Failure modes, effects and criticality analysis 27
6.5.8 Hardware-software interaction analysis (HSIA) 27
6.5.9 Sneak analysis 28
6.5.10 Zonal analysis 28
6.5.11 Energy trace analysis 29

7 Safetyverification 29
7.1 General 29
7.2 Tracking of hazards 29
7.2.1 Hazard reporting system 29
7.2.2 Status 29
7.2.3 Safety progress meeting 29
7.2.4 Review and disposition 29
7.2.5 Documentation 29
7.2.6 Mandatory inspection points (MIPs) 30
7.3 Safety verification methods 30
7.3.1 Verification engineering and planning 30
7.3.2 Methods and reports 30
7.3.3 Verification requirements 30
7.3.4 Analysis 30
7.3.5 Inspections 30
7.3.6 Tests 30
7.3.7 Verification and approval 31
7.4 Qualification of safety-critical functions 31
7.4.1 Verification 31
7.4.2 Qualification 31
7.4.3 Failure tests 31
7.4.4 Verification of design or operational characteristics 31
7.4.5 Safety verification testing 31
7.5 Hazard close-out 31
7.5.1 Safety assurance verification 31
7.5.2 Safety approval authority 32
7.6 Residual risk reduction 32

8 Operational safety 32
8.1 General 32
8.2 Basic requirements 32
8.3 Flight operations and mission control 32
8.3.1 Launcher operations 32
8.3.2 Contamination 33
8.3.3 Flight rules 33
8.3.4 Hazardous commanding control 33
8.3.5 Mission operation change control 33
8.3.6 Safety surveillance and anomaly control 33
8.4 Ground operations 33
8.4.1 Applicability 33
8.4.2 Initiation 34
8.4.3 Review and inspection 34
8.4.4 Hazardous operations 34
8.4.5 Launch and landing site requirements 34
8.4.6 GSE requirements 34

Bibliography 35