ISO 14620-1:2018 (E)

Space systems — Safety requirements — Part 1: System safety

Contents

Foreword

Introduction

1 Scope

1.1 General
1.2 Field of application
1.3 Tailoring

2 Normative references

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions
3.2 Abbreviated terms

4 System safety programme

4.1 Scope
4.2 Safety organization
4.2.1 General
4.2.2 Safety representative
4.2.3 Reporting lines
4.2.4 Safety integration
4.2.5 Coordination with others
4.3 Safety representative access and authority
4.3.1 Access
4.3.2 Delegated authority to reject — stop work
4.3.3 Delegated authority to interrupt operations
4.3.4 Conformance
4.3.5 Approval of reports
4.3.6 Review
4.3.7 Representation on boards
4.4 Safety risk management
4.4.1 Safety risks
4.4.2 Hazard assessment
4.4.3 Preferred measures
4.5 Project phases and safety review cycle
4.5.1 Progress meetings
4.5.2 Project reviews
4.5.2.1 General
4.5.2.2 Mission definition review
4.5.2.3 Preliminary requirements review
4.5.2.4 System requirements review
4.5.2.5 Preliminary design review
4.5.2.6 Critical design review
4.5.2.7 Qualification review
4.5.2.8 Acceptance review
4.5.2.9 Flight readiness review
4.5.2.10 Operational readiness review
4.5.2.11 Launch commitment meeting
4.5.2.12 In orbit test review
4.5.2.13 End-of-life assessment
4.5.3 Safety programme review
4.5.4 Safety data package
4.6 Safety programme plan
4.6.1 Implementation

4.6.2 Safety activities
4.6.3 Definition
4.6.4 Description
4.6.5 Safety and project engineering activities
4.6.6 Supplier and sub-supplier premises
4.6.7 Conformance
4.7 Safety certification
4.8 Safety training
4.8.1 Overall training
4.8.2 Participation
4.8.3 Detailed technical training
4.8.4 Product specific training
4.8.5 Records
4.8.6 Identification
4.9 Accident/incident reporting and investigation
4.10 Safety documentation
4.10.1 General
4.10.2 Customer access
4.10.3 Supplier review
4.10.4 Documentation
4.10.5 Safety data package
4.10.6 Safety deviations and waivers
4.10.6.1 Request for deviation
4.10.6.2 Description, analysis and rationale
4.10.6.3 Identification and review
4.10.6.4 Assessment of deviation
4.10.6.5 Review and disposition
4.10.6.6 Certification authority approval
4.10.7 Verification tracking log
4.10.8 Lessons-learned file

5 Safety engineering

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

6 Safety analysis requirements and techniques

6.1 General
6.2 Assessment and allocation of requirements
6.2.1 Safety requirements
6.2.2 Additional safety requirements
6.2.3 Define safety requirements — functions
6.2.4 Define safety requirements — subsystems
6.2.5 Justification
6.2.6 Functional and subsystem specification
6.3 Safety analysis
6.3.1 General
6.3.2 Mission analysis
6.3.3 Feasibility
6.3.4 Preliminary definition
6.3.5 Detailed definition, production and qualification
6.3.6 Utilization
6.3.7 Disposal
6.4 Specific safety analysis
6.4.1 General
6.4.2 Hazard analysis
6.4.3 Safety risk assessment
6.4.4 Safety analysis for hardware-software systems
6.4.4.1 Safety critical function
6.4.4.2 Requirements definition phase
6.4.4.3 Architectural and detailed design phase
6.4.4.4 Software code
6.4.4.5 Space debris mitigation
6.5 Supporting assessment and analysis
6.5.1 General
6.5.2 Warning time analysis
6.5.3 Caution and warning analysis
6.5.4 Common cause and common mode failure analysis
6.5.4.1 Multiple failures
6.5.4.2 Identification of requirements and scope
6.5.4.3 Identification of common cause failures
6.5.4.4 Analysis of common mode failures
6.5.4.5 Integration of results
6.5.5 Fault tree analysis
6.5.6 Human dependability analysis
6.5.7 Failure modes, effects and criticality analysis
6.5.8 Sneak analysis
6.5.8.1 Applicability
6.5.8.2 Use of results
6.5.9 Zonal analysis
6.5.9.1 Definition
6.5.9.2 Redundancy and objectives
6.5.10 Energy trace analysis

7 Safety verification

7.1 General
7.2 Tracking of hazards
7.2.1 Hazard reporting system
7.2.2 Status
7.2.3 Safety progress meeting
7.2.4 Review and disposition
7.2.5 Documentation
7.2.6 Mandatory inspection points
7.3 Safety verification methods
7.3.1 Verification engineering and planning
7.3.2 Methods and reports
7.3.3 Verification requirements
7.3.4 Analysis
7.3.5 Inspections

7.3.6 Tests
7.3.7 Verification and approval
7.4 Qualification of safety critical functions
7.4.1 Verification
7.4.2 Qualification
7.4.3 Failure tests
7.4.4 Verification of design or operational characteristics
7.4.5 Safety verification testing
7.5 Hazard close-out
7.5.1 Safety assurance verification
7.5.2 Safety approval authority
7.6 Residual risk reduction

8 Operational safety

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

Page count: 36