

ISO 14620-1:2002-12 (E)

Space systems - Safety requirements - Part 1: System safety

Contents		Page
Foreword		vii
Introduction		viii
1	Scope	1
1.1	General	1
1.2	Field of application	2
1.3	Tailoring	2
2	Normative references	2
3	Terms, definitions and abbreviated terms	2
3.1	Terms and definitions	2
3.2	Abbreviated terms	7
4	System safety programme	7
4.1	Scope	7
4.2	Safety organization	8
4.2.1	General	8
4.2.2	Safety representative	8
4.2.3	Reporting lines	8
4.2.4	Safety integration	8
4.2.5	Coordination with others	8
4.3	Safety representative access and authority	8
4.3.1	Access	8
4.3.2	Delegated authority to reject - stop work	8
4.3.3	Delegated authority to interrupt operations	8
4.3.4	Conformance	8
4.3.5	Approval of reports	9
4.3.6	Review	9
4.3.7	Representation on boards	9
4.4	Safety risk management	9
4.4.1	Risks	9
4.4.2	Hazard assessment	9
4.4.3	Preferred measures	9
4.5	Project phases and safety review cycle	9
4.5.1	Progress meetings	9
4.5.2	Project reviews	10
4.5.3	Safety programme review	12
4.5.4	Safety data package	12
4.6	Safety programme plan	12
4.6.1	Implementation	12
4.6.2	Safety activities	12
4.6.3	Definition	12
4.6.4	Description	13
4.6.5	Safety and project engineering activities	13
4.6.6	Supplier and sub-supplier premises	13
4.6.7	Conformance	13
4.7	Safety certification	13
4.8	Safety training	13
4.8.1	Overall training	13
4.8.2	Participation	14

4.8.3	Detailed technical training	14
4.8.4	Product specific training	14
4.8.5	Records	14
4.8.6	Identification	14
4.9	Accident/incident reporting and investigation	14
4.10	Safety documentation	14
4.10.1	General	14
4.10.2	Customer access	14
4.10.3	Supplier review	14
4.10.4	Documentation	15
4.10.5	Safety data package	15
4.10.6	Safety deviations and waivers	15
4.10.7	Verification tracking log	16
4.10.8	Lessons-learned file	16
5	Safety engineering	16
5.1	Safety engineering policy	16
5.1.1	General	16
5.1.2	Elements	16
5.1.3	Lessons learned	16
5.2	Safety design principles	17
5.2.1	Human life consideration	17
5.2.2	Design selection	17
5.2.3	System safety order of precedence	17
5.2.4	Environmental compatibility	18
5.2.5	Safe without services	18
5.2.6	Fail safe design	18
5.2.7	Hazard detection - Signalling and safing	18
5.2.8	Access	19
5.3	Safety risk reduction and control	19
5.3.1	Severity	19
5.3.2	Failure tolerance requirements	21
5.3.3	Design for minimum risk	22
5.3.4	Probabilistic safety targets	22
5.4	Identification and control of safety critical functions	23
5.4.1	Identification	23
5.4.2	Inadvertent operation	23
5.4.3	Provisions	23
5.4.4	Safe shutdown and failure tolerance requirements	23
5.4.5	Electronic, electrical, electromechanical	23
6	Safety analysis requirements and techniques	24
6.1	General	24
6.2	Assessment and allocation of requirements	24
6.2.1	Safety requirements	24
6.2.2	Additional safety requirements	24
6.2.3	Define safety requirements - functions	24
6.2.4	Define safety requirements - subsystems	24
6.2.5	Justification	24
6.2.6	Functional and subsystem specification	25
6.3	Safety analysis	25
6.3.1	General	25
6.3.2	Mission analysis	25
6.3.3	Feasibility	25
6.3.4	Preliminary definition	25
6.3.5	Detailed definition, production and qualification	25
6.3.6	Utilization	25
6.3.7	Disposal	25
6.4	Specific safety analysis	25
6.4.1	General	25
6.4.2	Hazard analysis	26
6.4.3	Safety risk assessment	26

6.4.4	Safety analysis for hardware-software systems	27
6.5	Supporting assessment and analysis	27
6.5.1	General	27
6.5.2	Warning time analysis	27
6.5.3	Caution and warning analysis	28
6.5.4	Common cause and common mode failure analysis	28
6.5.5	Fault tree analysis	29
6.5.6	Human dependability analysis	29
6.5.7	Failure modes, effects and criticality analysis	29
6.5.8	Sneak analysis	29
6.5.9	Zonal analysis	30
6.5.10	Energy trace analysis	30
7	Safety verification	30
7.1	General	30
7.2	Tracking of hazards	31
7.2.1	Hazard reporting system	31
7.2.2	Status	31
7.2.3	Safety progress meeting	31
7.2.4	Review and disposition	31
7.2.5	Documentation	31
7.2.6	Mandatory inspection points	31
7.3	Safety verification methods	31
7.3.1	Verification engineering and planning	31
7.3.2	Methods and reports	31
7.3.3	Verification requirements	32
7.3.4	Analysis	32
7.3.5	Inspections	32
7.3.6	Tests	32
7.3.7	Verification and approval	32
7.4	Qualification of safety critical functions	32
7.4.1	Validation	32
7.4.2	Qualification	32
7.4.3	Failure tests	33
7.4.4	Verification of design or operational characteristics	33
7.4.5	Safety verification testing	33
7.5	Hazard close-out	33
7.5.1	Safety assurance verification	33
7.5.2	Safety approval authority	33
7.6	Residual risk reduction	33
8	Operational safety	34
8.1	Basic requirements	34
8.2	Flight operations and mission control	34
8.2.1	Launcher operations	34
8.2.2	Contamination	34
8.2.3	Flight rules	34
8.2.4	Hazardous commanding control	34
8.2.5	Mission operation change control	35
8.2.6	Safety surveillance and anomaly control	35
8.3	Ground operations	35
8.3.1	Applicability	35
8.3.2	Initiation	35
8.3.3	Review and inspection	35
8.3.4	Hazardous operations	35
8.3.5	Launch and landing site requirements	36
8.3.6	GSE requirements	36
	Bibliography	37