



National Standards Authority of Ireland

IRISH STANDARD

I.S. EN ISO 14620-1:2002

ICS 49.140

National Standards  
Authority of Ireland  
Dublin 9  
Ireland

Tel: (01) 807 3800  
Tel: (01) 807 3838

## SPACE SYSTEMS - SAFETY REQUIREMENTS

### - PART 1: SYSTEM SAFETY

(ISO 14620-1:2002)

*This Irish Standard was published under the authority of the National Standards Authority of Ireland and comes into effect on:*

*January 24, 2003*

NO COPYING WITHOUT NSAI  
PERMISSION EXCEPT AS  
PERMITTED BY COPYRIGHT  
LAW



EUROPEAN STANDARD  
NORME EUROPÉENNE  
EUROPÄISCHE NORM

EN ISO 14620-1

December 2002

ICS 49.140

English version

Space systems - Safety requirements - Part 1: System safety  
(ISO 14620-1:2002)

Systèmes spatiaux - Exigences de sécurité - Partie 1:  
Sécurité système (ISO 14620-1:2002)

Raumfahrtsysteme - Sicherheitsanforderungen - Teil 1:  
Systemsicherheit (ISO 14620-1:2002)

This European Standard was approved by CEN on 24 June 2002.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION  
COMITÉ EUROPÉEN DE NORMALISATION  
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

## Contents

	page
<b>Foreword</b> .....	<b>5</b>
<b>Introduction</b> .....	<b>6</b>
<b>1 Scope</b> .....	<b>6</b>
<b>1.1 General</b> .....	6
<b>1.2 Field of application</b> .....	7
<b>1.3 Tailoring</b> .....	7
<b>2 Normative references</b> .....	<b>7</b>
<b>3 Terms, definitions and abbreviated terms</b> .....	<b>7</b>
<b>3.1 Terms and definitions</b> .....	7
<b>3.2 Abbreviated terms</b> .....	12
<b>4 System safety programme</b> .....	<b>12</b>
<b>4.1 Scope</b> .....	12
<b>4.2 Safety organization</b> .....	13
<b>4.2.1 General</b> .....	13
<b>4.2.2 Safety representative</b> .....	13
<b>4.2.3 Reporting lines</b> .....	13
<b>4.2.4 Safety integration</b> .....	13
<b>4.2.5 Coordination with others</b> .....	13
<b>4.3 Safety representative access and authority</b> .....	13
<b>4.3.1 Access</b> .....	13
<b>4.3.2 Delegated authority to reject - stop work</b> .....	13
<b>4.3.3 Delegated authority to interrupt operations</b> .....	13
<b>4.3.4 Conformance</b> .....	13
<b>4.3.5 Approval of reports</b> .....	14
<b>4.3.6 Review</b> .....	14
<b>4.3.7 Representation on boards</b> .....	14
<b>4.4 Safety risk management</b> .....	14
<b>4.4.1 Risks</b> .....	14
<b>4.4.2 Hazard assessment</b> .....	14
<b>4.4.3 Preferred measures</b> .....	14
<b>4.5 Project phases and safety review cycle</b> .....	14
<b>4.5.1 Progress meetings</b> .....	14
<b>4.5.2 Project reviews</b> .....	15
<b>4.5.3 Safety programme review</b> .....	17
<b>4.5.4 Safety data package</b> .....	17
<b>4.6 Safety programme plan</b> .....	17
<b>4.6.1 Implementation</b> .....	17
<b>4.6.2 Safety activities</b> .....	17
<b>4.6.3 Definition</b> .....	17
<b>4.6.4 Description</b> .....	18
<b>4.6.5 Safety and project engineering activities</b> .....	18
<b>4.6.6 Supplier and sub-supplier premises</b> .....	18
<b>4.6.7 Conformance</b> .....	18
<b>4.7 Safety certification</b> .....	18
<b>4.8 Safety training</b> .....	18
<b>4.8.1 Overall training</b> .....	18
<b>4.8.2 Participation</b> .....	19
<b>4.8.3 Detailed technical training</b> .....	19
<b>4.8.4 Product specific training</b> .....	19

4.8.5	Records .....	19
4.8.6	Identification .....	19
4.9	Accident/incident reporting and investigation .....	19
4.10	Safety documentation .....	19
4.10.1	General .....	19
4.10.2	Customer access .....	19
4.10.3	Supplier review .....	19
4.10.4	Documentation .....	20
4.10.5	Safety data package .....	20
4.10.6	Safety deviations and waivers .....	20
4.10.7	Verification tracking log .....	21
4.10.8	Lessons-learned file .....	21
5	Safety engineering .....	21
5.1	Safety engineering policy .....	21
5.1.1	General .....	21
5.1.2	Elements .....	21
5.1.3	Lessons learned .....	22
5.2	Safety design principles .....	22
5.2.1	Human life consideration .....	22
5.2.2	Design selection .....	22
5.2.3	System safety order of precedence .....	22
5.2.4	Environmental compatibility .....	23
5.2.5	Safe without services .....	23
5.2.6	Fail safe design .....	23
5.2.7	Hazard detection - Signalling and safing .....	23
5.2.8	Access .....	24
5.3	Safety risk reduction and control .....	24
5.3.1	Severity .....	24
5.3.2	Failure tolerance requirements .....	26
5.3.3	Design for minimum risk .....	27
5.3.4	Probabilistic safety targets .....	27
5.4	Identification and control of safety critical functions .....	28
5.4.1	Identification .....	28
5.4.2	Inadvertent operation .....	28
5.4.3	Provisions .....	28
5.4.4	Safe shutdown and failure tolerance requirements .....	28
5.4.5	Electronic, electrical, electromechanical .....	28
6	Safety analysis requirements and techniques .....	29
6.1	General .....	29
6.2	Assessment and allocation of requirements .....	29
6.2.1	Safety requirements .....	29
6.2.2	Additional safety requirements .....	29
6.2.3	Define safety requirements - functions .....	29
6.2.4	Define safety requirements - subsystems .....	29
6.2.5	Justification .....	29
6.2.6	Functional and subsystem specification .....	30
6.3	Safety analysis .....	30
6.3.1	General .....	30
6.3.2	Mission analysis .....	30
6.3.3	Feasibility .....	30
6.3.4	Preliminary definition .....	30
6.3.5	Detailed definition, production and qualification .....	30
6.3.6	Utilization .....	30
6.3.7	Disposal .....	30
6.4	Specific safety analysis .....	30
6.4.1	General .....	30
6.4.2	Hazard analysis .....	31
6.4.3	Safety risk assessment .....	31
6.4.4	Safety analysis for hardware-software systems .....	32
6.5	Supporting assessment and analysis .....	32

## EN ISO 14620-1:2002 (E)

<b>6.5.1</b>	<b>General.....</b>	<b>32</b>
<b>6.5.2</b>	<b>Warning time analysis .....</b>	<b>32</b>
<b>6.5.3</b>	<b>Caution and warning analysis .....</b>	<b>33</b>
<b>6.5.4</b>	<b>Common cause and common mode failure analysis .....</b>	<b>33</b>
<b>6.5.5</b>	<b>Fault tree analysis.....</b>	<b>34</b>
<b>6.5.6</b>	<b>Human dependability analysis .....</b>	<b>34</b>
<b>6.5.7</b>	<b>Failure modes, effects and criticality analysis .....</b>	<b>34</b>
<b>6.5.8</b>	<b>Sneak analysis .....</b>	<b>34</b>
<b>6.5.9</b>	<b>Zonal analysis .....</b>	<b>35</b>
<b>6.5.10</b>	<b>Energy trace analysis .....</b>	<b>35</b>
<b>7</b>	<b>Safety verification .....</b>	<b>35</b>
<b>7.1</b>	<b>General.....</b>	<b>35</b>
<b>7.2</b>	<b>Tracking of hazards .....</b>	<b>36</b>
<b>7.2.1</b>	<b>Hazard reporting system.....</b>	<b>36</b>
<b>7.2.2</b>	<b>Status .....</b>	<b>36</b>
<b>7.2.3</b>	<b>Safety progress meeting .....</b>	<b>36</b>
<b>7.2.4</b>	<b>Review and disposition .....</b>	<b>36</b>
<b>7.2.5</b>	<b>Documentation .....</b>	<b>36</b>
<b>7.2.6</b>	<b>Mandatory inspection points.....</b>	<b>36</b>
<b>7.3</b>	<b>Safety verification methods .....</b>	<b>36</b>
<b>7.3.1</b>	<b>Verification engineering and planning .....</b>	<b>36</b>
<b>7.3.2</b>	<b>Methods and reports .....</b>	<b>36</b>
<b>7.3.3</b>	<b>Verification requirements.....</b>	<b>37</b>
<b>7.3.4</b>	<b>Analysis .....</b>	<b>37</b>
<b>7.3.5</b>	<b>Inspections .....</b>	<b>37</b>
<b>7.3.6</b>	<b>Tests.....</b>	<b>37</b>
<b>7.3.7</b>	<b>Verification and approval .....</b>	<b>37</b>
<b>7.4</b>	<b>Qualification of safety critical functions .....</b>	<b>37</b>
<b>7.4.1</b>	<b>Validation .....</b>	<b>37</b>
<b>7.4.2</b>	<b>Qualification .....</b>	<b>37</b>
<b>7.4.3</b>	<b>Failure tests .....</b>	<b>38</b>
<b>7.4.4</b>	<b>Verification of design or operational characteristics.....</b>	<b>38</b>
<b>7.4.5</b>	<b>Safety verification testing .....</b>	<b>38</b>
<b>7.5</b>	<b>Hazard close-out .....</b>	<b>38</b>
<b>7.5.1</b>	<b>Safety assurance verification .....</b>	<b>38</b>
<b>7.5.2</b>	<b>Safety approval authority .....</b>	<b>38</b>
<b>7.6</b>	<b>Residual risk reduction .....</b>	<b>38</b>
<b>8</b>	<b>Operational safety.....</b>	<b>39</b>
<b>8.1</b>	<b>Basic requirements.....</b>	<b>39</b>
<b>8.2</b>	<b>Flight operations and mission control .....</b>	<b>39</b>
<b>8.2.1</b>	<b>Launcher operations .....</b>	<b>39</b>
<b>8.2.2</b>	<b>Contamination .....</b>	<b>39</b>
<b>8.2.3</b>	<b>Flight rules.....</b>	<b>39</b>
<b>8.2.4</b>	<b>Hazardous commanding control .....</b>	<b>39</b>
<b>8.2.5</b>	<b>Mission operation change control .....</b>	<b>40</b>
<b>8.2.6</b>	<b>Safety surveillance and anomaly control .....</b>	<b>40</b>
<b>8.3</b>	<b>Ground operations.....</b>	<b>40</b>
<b>8.3.1</b>	<b>Applicability .....</b>	<b>40</b>
<b>8.3.2</b>	<b>Initiation .....</b>	<b>40</b>
<b>8.3.3</b>	<b>Review and inspection .....</b>	<b>40</b>
<b>8.3.4</b>	<b>Hazardous operations .....</b>	<b>40</b>
<b>8.3.5</b>	<b>Launch and landing site requirements .....</b>	<b>41</b>
<b>8.3.6</b>	<b>GSE requirements.....</b>	<b>41</b>
	<b>Bibliography .....</b>	<b>42</b>



This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

- Looking for additional Standards? Visit Intertek Inform Infostore
- Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation