



SLOVENSKI STANDARD
SIST EN 14738:2004
01-september-2004

Zagotavljanje varnih proizvodov v vesoljski tehniki – Analiza nevarnosti

Space product assurance - Hazard analysis

Raumfahrtproduktsicherung - Gefahrenanalyse

Assurance produit des projets spatiaux - Analyse des dangers

Ta slovenski standard je istoveten z: EN 14738:2004

[SIST EN 14738:2004](https://standards.iteh.ai/catalog/standards/sist/50f263ad-c569-4fe8-834b-b948f3d6cf6f/sist-en-14738-2004)

<https://standards.iteh.ai/catalog/standards/sist/50f263ad-c569-4fe8-834b-b948f3d6cf6f/sist-en-14738-2004>

ICS:

49.140 Vesoljski sistemi in operacije Space systems and operations

SIST EN 14738:2004

en

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 14738:2004

<https://standards.iteh.ai/catalog/standards/sist/50f263ad-c569-4fe8-834b-b948f3d6cf6f/sist-en-14738-2004>

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 14738

March 2004

ICS 49.140

English version

Space product assurance - Hazard analysis

Assurance produit des projets spatiaux - Analyse des dangers

Raumfahrtproduktsicherung - Gefahrenanalyse

This European Standard was approved by CEN on 2 February 2004.

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 Central Secretariat 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 Central Secretariat has the same status as the official versions.

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

STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 14738:2004
<https://standards.iteh.ai/catalog/standards/sist/50f263ad-c569-4fe8-834b-b948f3d6c6ff/sist-en-14738-2004>



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

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

Contents

	page
Foreword.....	3
1 Scope	5
2 Normative references	5
3 Terms, definitions and abbreviated terms	5
4 Principles of hazard analysis.....	7
5 Objectives of hazard analysis.....	11
6 Hazard analysis requirements and process.....	12
7 Hazard analysis implementation	20
Annex A (informative) Examples of generic hazards.....	22
Annex B (normative) Hazard report — Document requirements definition (DRD).....	24
Annex C (informative) Background information	30
Bibliography	32

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN 14738:2004](https://standards.iteh.ai/catalog/standards/sist/50f263ad-c569-4fe8-834b-b948f3d6cf6f/sist-en-14738-2004)

<https://standards.iteh.ai/catalog/standards/sist/50f263ad-c569-4fe8-834b-b948f3d6cf6f/sist-en-14738-2004>

Foreword

This document (EN 14738:2004) has been prepared by CEN/CS.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by September 2004, and conflicting national standards shall be withdrawn at the latest by September 2004.

It is based on a previous version¹⁾ originally prepared by the ECSS Product Assurance Panel and approved by the ECSS Steering Board. The European Cooperation for Space Standardization (ECSS) is a cooperative effort of the European Space Agency, national space agencies and European industry associations for the purpose of developing and maintaining common standards.

This European Standard is one of the series of space standards intended to be applied together for the management, engineering and product assurance in space projects and applications.

Requirements in this European Standard are defined in terms of what shall be accomplished, rather than in terms of how to organize and perform the necessary work. This allows existing organizational structures and methods to be applied where they are effective, and for the structures and methods to evolve as necessary without rewriting the standards.

The formulation of this European Standard takes into account the existing EN ISO 9000 family of documents.

The annexes A and C are informative. Annex B is normative.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

¹⁾ ECSS-Q-40-02A.

EN 14738:2004 (E)

Introduction

Safety analysis comprises hazard analysis, safety risk assessment and supporting analyses as defined in EN ISO 14620-1. The objective of safety analysis is to identify, assess, reduce, accept, and control safety hazards and the associated safety risks in a systematic, proactive, complete and cost effective manner, within overall risk management. Safety analysis can be implemented through an iterative process, with iterations being determined by the project progress through the different project phases, and by changes to a given project baseline.

Hazard analysis comprises the identification classification and reduction of hazards. Hazard analysis can be implemented at each level of the customer-supplier network. Hazard analysis activities at lower level can contribute to system level safety analysis. System level safety analysis can determine lower level hazard analysis activities.

Hazard analysis interfaces with dependability analysis, in particular FMECA. Hazard analysis also establishes the basis for safety risk assessment.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN 14738:2004](#)

<https://standards.iteh.ai/catalog/standards/sist/50f263ad-c569-4fe8-834b-b948f3d6cf6f/sist-en-14738-2004>

1 Scope

This European Standard specifies the hazard analysis requirements of EN ISO 14620-1:2002, 6.4.2; it specifies the principles, process, implementation, and requirements of hazard analysis.

It is applicable to all European space projects where during any project phase there exists the potential for hazards to personnel or the general public, space flight systems, ground support equipment, facilities, public or private property or the environment.

2 Normative references

This European Standard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text, and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this European Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies (including amendments).

EN 13290-5:2001, *Space project management — General requirements — Part 5: Configuration management*.

EN 13701:2001, *Space systems — Glossary of terms*.

EN ISO 14620-1:2002, *Space systems — Safety requirements — Part 1: System safety (ISO 14620-1:2002)*.

EN ISO 17666:2003, *Space systems — Risk management (ISO 17666:2003)*.

SIST EN 14738:2004

<https://standards.iteh.ai/catalog/standards/sist/50f263ad-c569-4fe8-834b-738-2004>

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this European Standard, the terms and definitions given in EN 13701:2001 together with the following apply.

3.1.1

consequence tree

set of hazard scenarios leading to the same safety consequence

3.1.2

detection time

time span between the occurrence of the initiator event and its detection through the observable symptoms

3.1.3

hazard

existing or potential condition of an item that can result in a mishap
[ISO 14620-2:2000]

NOTE 1 This condition can be associated with the design, fabrication, operation, or environment of the item, and has the potential for mishaps.
[ISO 14620-2:2000]

NOTE 2 Hazards are potential threats to the safety of a system. They are not events, but the prerequisite for the occurrence of hazard scenarios with their negative effects on safety in terms of the safety consequences.

EN 14738:2004 (E)

3.1.4**hazard acceptance**

decision to tolerate the consequences of the hazard scenarios when they occur

3.1.5**hazard analysis**

systematic and iterative process of the identification, classification and reduction of hazards

3.1.6**hazard control**

preventive or mitigation measure, associated to a hazard scenario, which is introduced into the system design and operation to avoid the events or to interrupt their propagation to consequence

3.1.7**hazard elimination**

removal of a hazard from a particular hazard manifestation

3.1.8**hazard manifestation**

presence of specific hazards in the technical design, operation and environment of a system

3.1.9**hazard minimization**

substitution of a hazard in the hazard manifestation by another hazard of the same type but with a lower potential threat

EXAMPLE

High toxicity to low toxicity.

ITeH STANDARD PREVIEW
(standards.iteh.ai)

3.1.10**hazard reduction**

process of elimination or minimization and control of hazards

3.1.11**hazard scenario**

sequence of events leading from the initial cause to the unwanted safety consequence

NOTE

The cause can be a single initiating event, or an additional action or a change of condition activating a dormant problem.

3.1.12**hazard tree**

set of hazard scenarios originating from the same set of hazard manifestations

3.1.13**hazardous**

property of an item and its environment which provides the potential for mishaps [ISO 14620-2:2000]

3.1.14**observable symptoms**

evidence that indicates that an undesirable event has occurred

NOTE

Observable symptoms appear during the scenario propagation time.

3.1.15**reaction time**

time span between the detection and the occurrence of the consequence

NOTE

This is the time span available for mitigating actions after detection of the occurrence of the initiator event.

3.1.16**residual hazard**

hazard remaining after implementation of hazard reduction

3.1.17**resolved hazard**

hazard that is reduced, the reduction verified and the hazard considered acceptable

NOTE Resolved hazards are submitted for formal acceptance.

3.1.18**scenario propagation time**

time span between the occurrence of the initiator event and the occurrence of the consequence

3.1.19**severity of safety consequence**

measure of the gravity of damage with respect to safety

3.2 Abbreviated terms

The following abbreviated terms are defined and used within this European Standard.

CC&M common cause and common failure mode analysis

DRD document requirements definition

ECSS European Cooperation for Space Standardization

FMECA failure modes, effects and criticality analysis

GSE ground support equipment

OHA operating hazard analysis

PHA preliminary hazard analysis

SHA system hazard analysis

SSHA subsystem hazard analysis

4 Principles of hazard analysis**4.1 Hazard analysis concept**

Hazard analysis is based on the following hazard analysis concept, which is depicted in Figures 1 to 4.

Hazards, which are present through hazard manifestations in the system, are activated if initiating events (i.e. cause) occur. Hazard scenarios reflect the system behaviour to the activated hazards in terms of event propagation from causes to safety consequences, as depicted in Figure 1. The occurrence of events is coupled to observable symptoms in the system. Safety consequences are characterized by their severity.

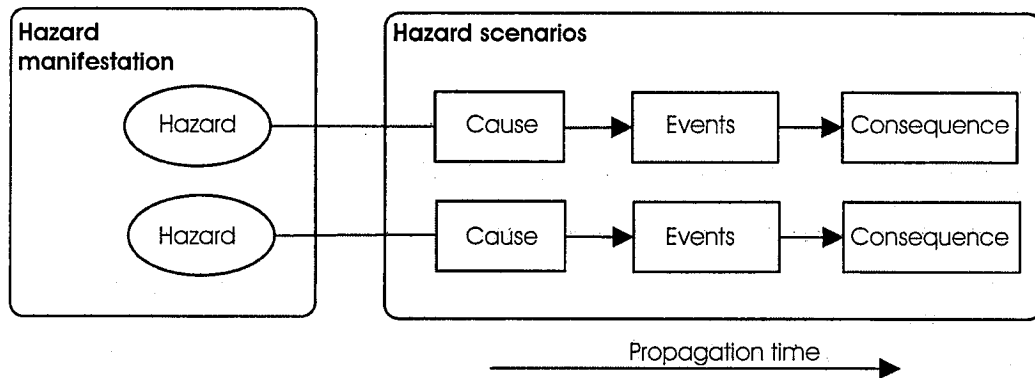


Figure 1 — Hazard and hazard scenarios

Different hazard scenarios can originate from the same hazard. Furthermore, different hazard scenarios can lead to the same safety consequence. For an example, see Table 4. The collection of hazard scenarios originating from the same hazard manifestation is collated into a hazard tree, as illustrated in Figure 2. The collection of hazard scenarios leading to the same safety consequence is collated into a consequence tree, as illustrated in Figure 3.

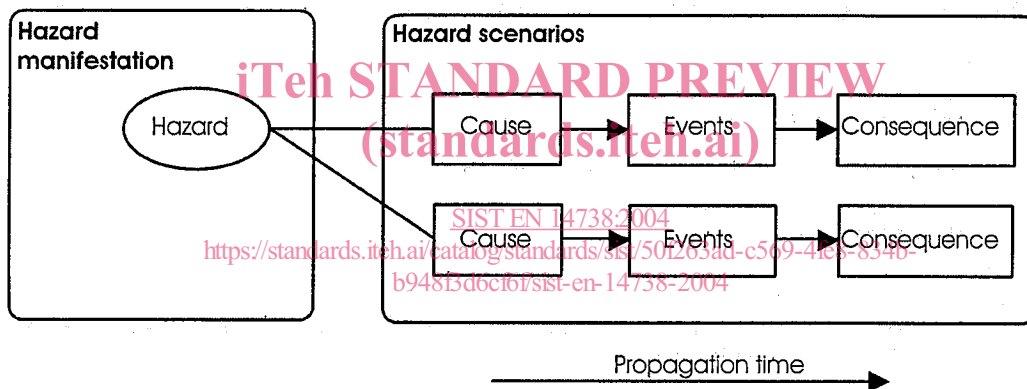


Figure 2 — Example of a hazard tree

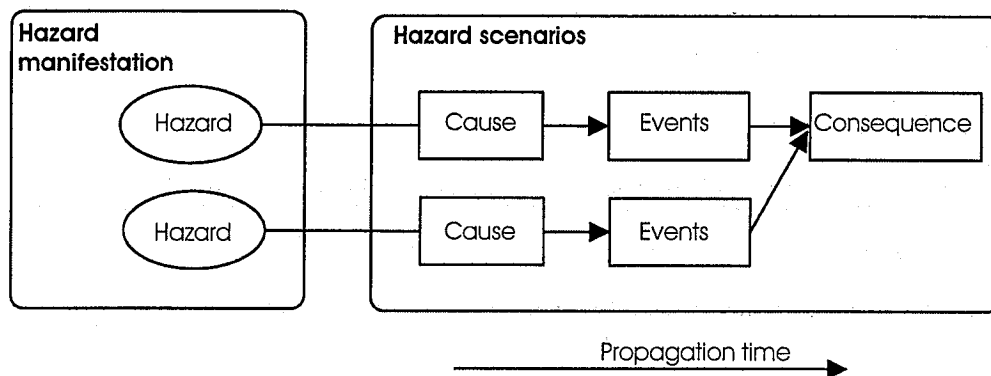


Figure 3 — Example of a consequence tree

Hazards are reduced by either eliminating them or, if this is not possible, by minimizing and controlling them, as shown in Figure 4. Hazards are eliminated through the removal of specific potentially safety threatening

system characteristics. Hazards are minimized through reducing the level or amount of specific potentially safety threatening system characteristics. Hazards are controlled through the prevention of the occurrence or reduction of the likelihood and mitigation of the effects of events. Occurrence of the events can be detected through their observable symptoms.

EXAMPLE A hazard to driving a car is "poor weather conditions", and the hazard is manifested by "ice on the road". The cause "rapid change of direction" can lead to the event "loss of control of the car" and "running of the road", and finally to the consequence "death of driver". Hazard elimination can be achieved by "delaying the journey", and hazard minimization by "gritting the road". There are various methods for hazard control which impact on different parts of the process: "driving slowly" impacts on the cause; "using snow-chains" impacts on the link between cause and event; "fitting airbag" impacts on the link between event and consequence.

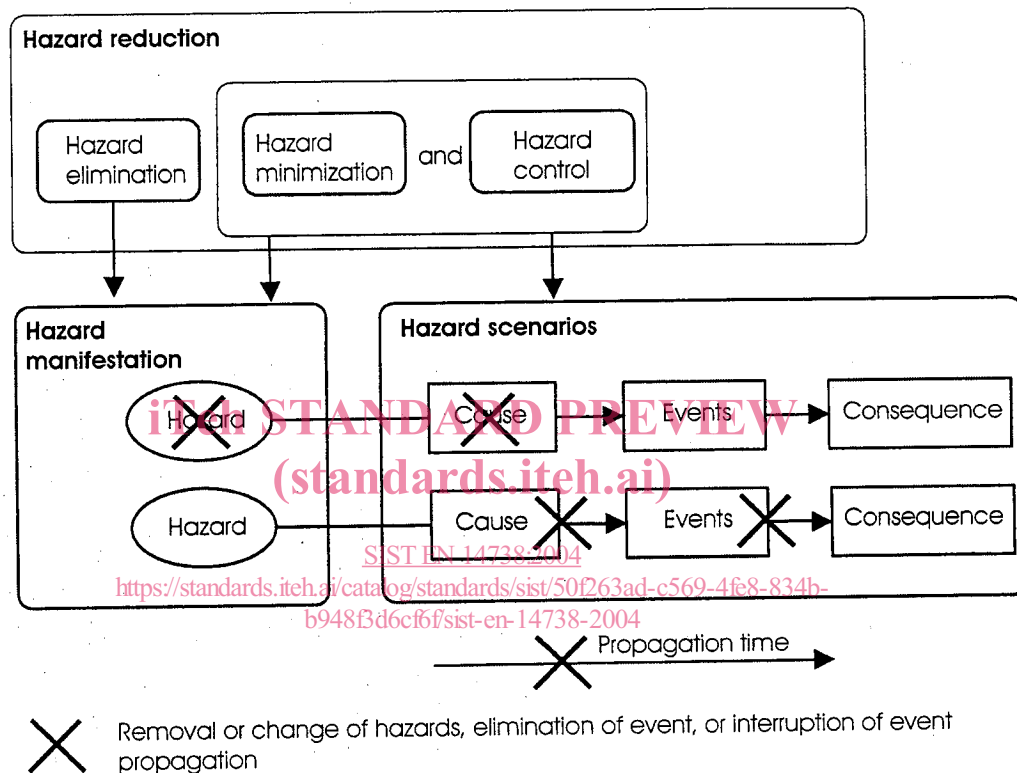


Figure 4 — Reduction of hazards

Failure causes as identified through FMECA and other analyses, such as common cause and common failure mode analysis (CC&M), can represent causes of hazard scenarios, as depicted in Figure 5.

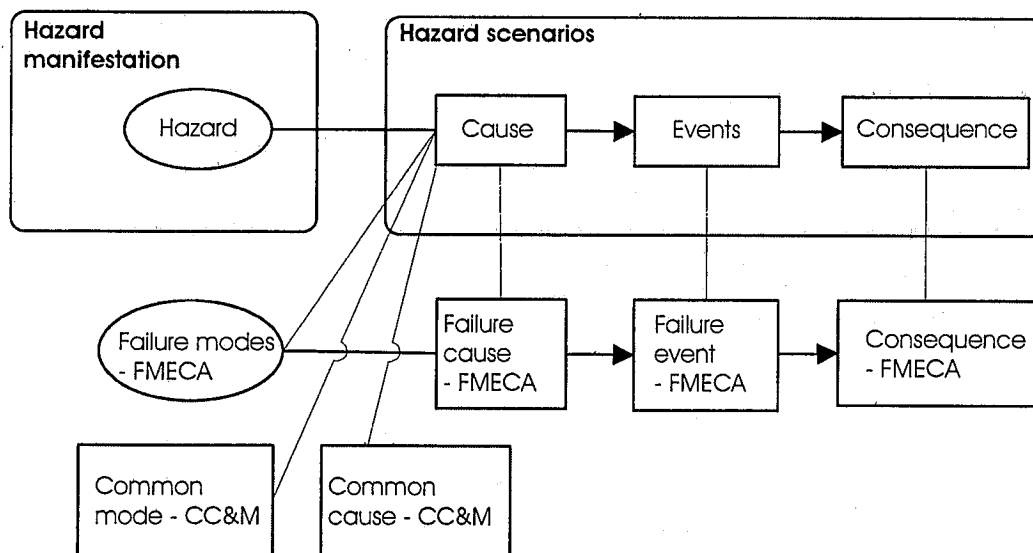


Figure 5 — Interface to FMECA and CC&M analysis

4.2 Role of hazard analysis

Hazard analysis is the principal deterministic safety analysis, which assists engineers and managers in including safety aspects in the engineering practices and the decision-making process throughout the project life cycle in design, construction, testing, operation, maintenance, and disposal, together with their interfaces.

Hazard analysis provides essential input to the safety risk assessment for a system.

4.3 Hazard analysis process

The hazard analysis process comprises the steps and tasks necessary to identify and classify hazards, to achieve hazard reduction. The basic steps are:

- Step 1: define the hazard analysis implementation requirements;
- Step 2: identify and classify the hazards;
- Step 3: decide and act on the hazards;
- Step 4: track, communicate and accept the hazards.

The process of hazard analysis, including iteration of its tasks, is summarized in Figure 6.