ECSS-Q-ST-40-12C
31 July 2008

EUROPEAN COOPERATION
ECSS
FOR SPACE STANDARDIZATION

Space product assurance

Fault tree analysis – Adoption notice ECSS/IEC 61025

ECSS Secretariat
ESA-ESTEC
Requirements & Standards Division
Noordwijk, The Netherlands

Foreword

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

This Standard has been prepared by the ECSS Executive Secretariat, endorsed by the Document and Discipline Focal points, and approved by the ECSS Technical Authority.

Disclaimer

ECSS does not provide any warranty whatsoever, whether expressed, implied, or statutory, including, but not limited to, any warranty of merchantability or fitness for a particular purpose or any warranty that the contents of the item are error-free. In no respect shall ECSS incur any liability for any damages, including, but not limited to, direct, indirect, special, or consequential damages arising out of, resulting from, or in any way connected to the use of this Standard, whether or not based upon warranty, business agreement, tort, or otherwise; whether or not injury was sustained by persons or property or otherwise; and whether or not loss was sustained from, or arose out of, the results of, the item, or any services that may be provided by ECSS.

Published by: ESA Requirements and Standards Division
ESTEC, P.O. Box 299,
2200 AG Noordwijk
The Netherlands

Change log

ECSS-Q-40-12A 14 October 1997	First issue
ECSS-Q-40-12B	Never issued
ECSS-Q-ST-40-12C 31 July 2008	Second issue Minor editorial changes to conform with ECSS drafting rules, new ECSS template and with the renumbering of ECSS standards.

Table of contents

1 Scope

This Standard defines requirements for the performance of Fault Tree Analysis (FTA) on space projects and incorporates the IEC 61025 standard into the ECSS system.

With effect from the date of approval, this Standard announces the adoption of the external document on a restricted basis for use in the European Cooperation for Space Standardization (ECSS) system.

This standard may be tailored for the specific characteristic and constraints of a space project in conformance with ECSS-S-ST-00.

2
Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this ECSS Standard. For dated references, subsequent amendments to, or revisions of any of these publications do not apply. However, parties to agreements based on this ECSS Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references the latest edition of the publication referred to applies.

ECSS-S-ST-00-01	ECSS system – Glossary of terms
ECSS-Q-ST-30	Space product assurance – Dependability
ECSS-Q-ST-40	Space product assurance – Safety
IEC 61025 (1990-10)	Fault tree analysis (FTA)

3
Terms, definitions and abbreviated terms

3.1 Terms defined in other standards

For the purpose of this Standard, the terms and definitions from ECSS-S-ST-00-01 apply, in particular for the following terms:

dependability

3.2 Abbreviated terms

For the purpose of this Standard, the abbreviated terms from ECSS-S-ST-00-01 and the following apply:

Abbreviation	**Meaning**
ECSS	European Cooperation for Space Standardization
IEC	International Electrotechnical Commission
FT	fault tree
FTA	fault tree analysis
NUREG	U.S. Nuclear Regulatory Commission, Washington, DC

4 Principles

The standard IEC 61025 (1990-10) titled “Fault tree analysis (FTA)” defines basic principles, provides the steps necessary to perform an analysis, identifies appropriate assumptions, events and failure modes, and provides identification rules and symbols.

5 Requirements

5.1 ECSS usage restriction

5.1.1 Applicability

a. The supplier shall use the FTA as defined in ECSS-Q-ST-30 and ECSS-Q-ST-40.

b. The supplier shall perform a FTA for:

1. selected undesirable events which could have catastrophic, critical or major consequences;

   NOTE For definition for the scale of severity, refer to ECSS-Q-ST-30.

2. support of failure;

3. accident investigations.

   NOTE This is to limit the amount of effort in performing the analysis.

c. The supplier shall agree with the customer on the content of the FTA.

d. The supplier shall provide the FTA for customer review.

e. Where FTA is used in failure or accident investigations, the supplier shall agree with the relevant Review Board on the depth of the FTA.

5.1.2 Procedure

a. The supplier shall perform the FTA in conformance with the methodology and symbols described in IEC 61025.

NOTE 1 IEC 61025 uses general terms to describe the FTA process, including preparations for the FTA, the procedure itself and the output report.

NOTE 2 Users are encouraged to make sure that they have a clear understanding and interpretation of these general terms when taken in the context of the space system under analysis.

NOTE 3 The informative reference, NUREG 0492 (1991) “Fault Tree Handbook” can be used as a comprehensive reference work to complement this ECSS Standard.

5.1.3 Software tools supporting FTA

a. When using a computer program to support the FTA, the supplier shall use a computer program which fulfils the following criteria:

1. it supports the functionality which is necessary to perform the FTA;
2. it is compatible with project requirements for electronic data transfer and the interchange of data between interacting programs or tools.

NOTE Although there are several proprietary software programs available for various platforms designed to assist the FT analyst, this ECSS Standard does not endorse any particular product.

Bibliography

ECSS-S-ST-00	ECSS system – Description, implementation and general requirements
NUREG 0492 (1991)	Fault Tree Handbook - Reliability and Risk Analysis, Norman J McCormick, Academic Press