FROM HAZARD ANALYSIS TO SAFETY RISK ASSESSMENT AND FURTHER: THE NEW EUROPEAN SPACE STANDARDS ON HAZARD ANALYSIS AND SAFETY RISK ASSESSMENT

R. Tuominen[1/], T. Bedford[2/], G. Canepa[3/], I. Jenkins[4/], J. Lenic[5/], G. Morelli[6/], P. Pearson[7/], C. Preyssl[8/] & M. Stamatelatos[9/ *]

[1/] VTT Industrial Systems, Reliability and Risk Management
PO Box 1609, FIN-33101 Tampere, Finland
Tel: +358 3 316-3269, E-mail: Risto.Tuominen@vtt.fi

[8/] ESA Quality, Dependability and Safety Division, ESTEC
PO Box 299, 2200 AG Noordwijk, The Netherlands
Tel: +31 71 565-4476, E-mail: Christian.Preyssl@esa.int

ABSTRACT

This paper addresses two new safety standards on hazard analysis and safety risk assessment. As part of the process of updating existing European standards it became clear that the standards relating to safety could be improved. The ECSS-Q-40 working group identified the need for review of the lower level standards. The subsequent lower level working group reviewed the existing situation and identified that separate hazard analysis and safety risk assessment standards were necessary.

The present paper briefly discusses the perspective and the intented role of the two new safety standards. The members of the ECSS-Q-40-02/03 working group have jointly prepared the paper.

INTRODUCTION

In the framework of the European Co-operation for Space Standardisation (ECSS), the ECSS-Q-40 Space Safety standard was established and contains requirements on Safety Analysis as part of a systematic safety program. Hazard Analysis and Safety Risk Assessment constitute the backbone of Safety Analysis and are addressed in two new standards, namely ECSS-Q-40-02 and ECSS-Q-40-03. Both standards have been prepared by the same ECSS working group, in close co-operation with the ECSS-Q-40 working group.

The approaches adopted to Hazard Analysis and Safety Risk Assessment are fully in line with and support the ECSS Risk Management process defined in the management standard ECSS-M-00-03. The approach emphasises the importance and application of the risk management process applied to Safety, a process being emphasised throughout the subject of Safety & Dependability. The intent is to establish an integral relationship between Dependability and Safety.

OVERVIEW OF THE INTEGRATED HAZARD ANALYSIS AND SAFETY RISK ASSESSMENT PROCESS

Safety analysis comprises hazard analysis, safety risk assessment and supporting analyses as defined in ECSS-Q-40 and as depicted in Figure 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. It takes into account the project's technical and programmatic constraints. Safety analysis can be implemented through an iterative process. Cycles of the safety analysis process are iterated during the different project phases and evolution of system design & operation.

The purpose of hazard analysis is to identify, classify and propose the means to reduce hazards in a deterministic manner. The purpose of safety risk assessment is to determine the overall safety risks induced by hazards and to rank the risk contributors. Risk assessment is based on a probabilistic analysis, in that the risk ranking is jointly dependent on the consequences and on the likelihood of those consequences occurring.

Authors' affiliations:
[2/] University of Strathclyde, Scotland; [3/] Alenia Aerospazio, Italy; [4/] Astrium, Germany; [5/] DLR, Germany; [6/] Galileo Avionica, Italy; [7/] Astrium, England; [9/] NASA Headquarters, USA.

Proceedings of Joint ESA-NASA Space-Flight Safety Conference, ESTEC, Noordwijk (NL), 11-14 June 2002 (ESA SP-486, August 2002)

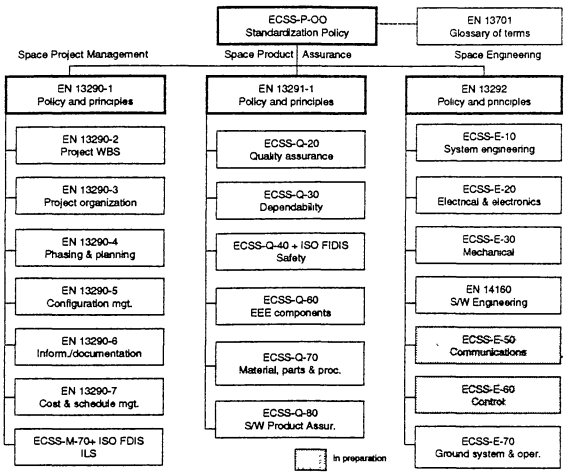

Figure 1 ECSS document architecture
Source: ECSS Secretariat

The analyses can be implemented at each level of the customer-supplier chain. The activities at lower level contribute to system level safety assessments. On the other hand, system level safety analyses can be used to determine lower level activities.

Hazard analysis and safety risk assessment interrelate with Dependability (i.e., Reliability, Availability and Maintainability (RAM)). Hazard analysis is linked in particular to FMECA. Safety risk assessment is linked closely to reliability analysis but extends to outside the confines of the system by looking also at system vulnerability to external insults and other initiators not usually covered in traditional reliability analysis.

As part of normal engineering practices, managers and engineers will use both of these techniques to assist in the decision-making process for project risk management. Ranking of safety risks, according to their criticality for the project success, allows management to direct its attention to the essential safety issues, as part of the major objectives of risk management.

HAZARD ANALYSIS PROCESS

Hazard analysis aims at:

- identifying the hazards posing a threat to safety, and the associated hazard scenarios,
- identifying the consequence severity of each hazard scenario,
- classifying the hazards according to their consequence severity to identify hazards subject to hazard reduction, and
- identifying measures through which hazards can be eliminated, or minimized and controlled.

The above information on hazards is used to:

- assess the level of safety of a system in a deterministic way;
- increase the level of safety of a system through hazard reduction;
- use hazard reduction to drive the definition and implementation of design and operation requirements, specifications, concepts, procedures etc.;
- provide a basis for defining adequate safety requirements, determining the applicability of safety requirements, implementing safety requirements, verifying their implementation and demonstrating compliance or non-compliance;
- provide input to safety risk assessment and overall project risk management;
- support safety related project decisions;
- support safety submissions and reviews through documented evidence; and
- support safety certification of a system through documented evidence.

The hazard analysis process is summarised in Figure 2.

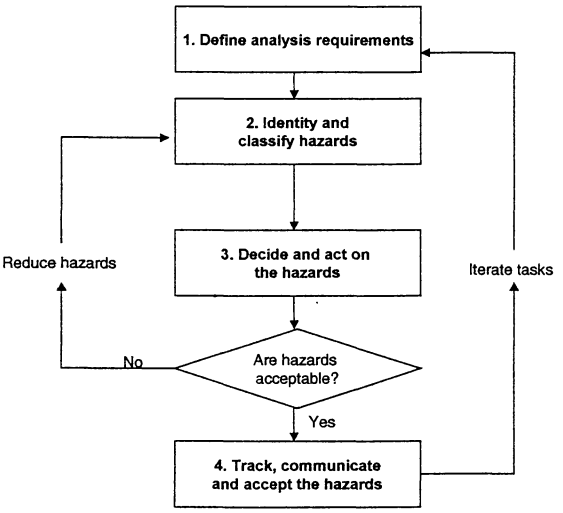

Figure 2 The process of hazard analysis

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 activities related to each step above are described in more detail within the corresponding standard ECSS-Q-40-02.

Acceptance of hazards depends on a deterministic assessment of the hazard consequence severity. Hazard reduction essentially means either the elimination of hazards through the application of design and operations or the mitigation of hazards by ensuring that more barriers are placed in the way of a hazardous consequence.

THE SAFETY RISK ASSESSMENT PROCESS

Safety risk assessment aims at:

- identifying safety risks imposed by the hazard scenarios identified in hazard analysis,
- identifying the overall safety risk,
- identifying the risk contributors,
- identifying risk reduction potential of the risk contributors,
- identifying uncertainty reduction potential of the risk contributors, and
- ranking the risk contributors.

The above information on safety risks is used to:

- assess the level of safety of a system in a probabilistic way;
- increase the level of safety of a system through safety risk reduction;
- use safety risk reduction to drive the definition and implementation of design and operation requirements, specifications, concepts, procedures etc.;
- provide a basis for defining adequate safety requirements, determining the applicability of safety requirements, implementing safety requirements, verifying their implementation and demonstrating compliance or non-compliance;
- provide input to overall project risk management;
- support safety related project decisions;
- support safety submissions and reviews through documented evidence; and
- support safety certification of a system through documented evidence.

The safety risk assessment process is summarised in Figure 3.

The safety risk assessment process comprises the steps and tasks necessary to identify and classify safety risks, to achieve safety risk reduction. The basic steps are:

- Step1: Define the safety risk analysis implementation requirements;
- Step 2: Identify and classify the safety risks;
- Step 3: Decide and act on the safety risks;
- Step 4: Track, communicate and accept the safety risks.

The activities related to each step above are described in more detail within the corresponding standard ECSS-Q-40-03.

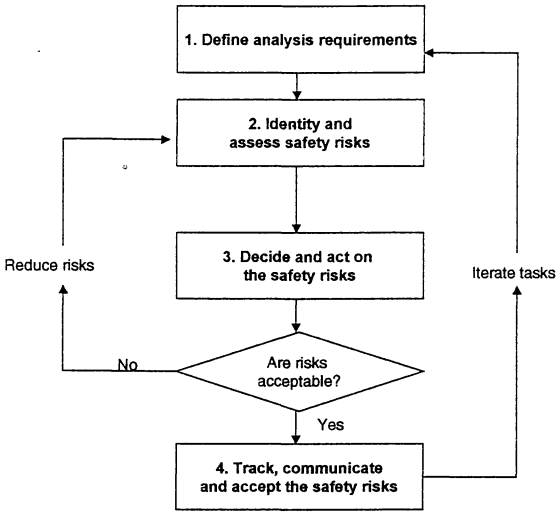

Figure 3 The process of safety risk assessment

It can be seen by comparison between Fig. 2 and 3 that the safety risk assessment process parallels the hazard analysis process. This allows a consistent approach to be applied in both cases.

Acceptance of safety risks is based however not on a ranking of the consequences, but on a joint ranking of the consequence severity and the likelihood. Hence certain risks may be accepted because their chance of occurrence is considered sufficiently low. The level of risk that is considered low enough varies from system to system (most obviously between manned and unmanned systems), and is therefore not a part of the standard.

It should be also noted that the safety risk assessment process shown in Figure 3 clearly aligns with the project risk management process defined by ECSS-M-00-03.

WHY THESE STANDARDS?

The new standards were developed in order to create a modern European standard for space safety that match the current and perceived future programs.

The new standards carry on the development started about ten years ago in ESA in the context of the PSS-

403 and PSS–404 standards for system safety, and which have been applicable on Columbus and other European space projects. The new standards were also needed to fill the gap caused by the fact that the ESA PSS-standards are no more maintained and thus no more applicable to space programs.

The new standards are most suitable to serve the needs of future manned (e.g. manned mission to Mars) and complex unmanned systems with significant safety implications (e.g. Galileo). Galileo is a new European unmanned program with important implications for safety services (eg. air traffic control). In order to certify Galileo for these services these ECSS standards can be used as an input to the Galileo safety case definition.

WHY TWO STANDARDS?

There are many cases where it is not needed to do a complete detailed safety assessment, which normally would comprise the hazard analysis and the probabilistic risk assessment. It is often appropriate to only perform a simple identification and consequence severity based ranking of hazards based on which hazard reduction can be implemented (i.e. hazard analysis). There are cases where hazard reduction can even be achieved through a simplified hazard analysis, which, for example, includes identification of hazards in a simple design but excludes identification of associated hazard scenarios.

In applications, dependent on customer requirements, one can now choose to apply either one of these standards or both in an integrated way.

ADVANTAGES OF THE NEW STANDARDS

The new ECSS hazard analysis approach constitutes an evolution of existing approaches and is considered to better reflect the European and possibly even the global needs. One of the main strengths of this new approach is the rigorous modelling and systematic distinction of hazards and scenarios, which contain events and their consequences, as shown in Figure 4.

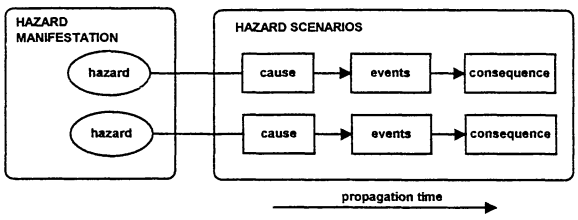

Figure 4 The concept of hazards and hazard scenarios

This differs, for example, from the NASA hazard report approach in that there is not always a proper distinction between hazards, events and consequences in the hazard titles.

Furthermore the new ECSS approach allows the construction of hazard and consequence trees, which can be used as an alternative to or in conjunction with conventional event trees and fault trees. This provides a flexible and straightforward way for the dynamic modelling of space system failures or accident scenarios without introducing a cumbersome methodological framework.

The new ECSS safety risk assessment approach constitutes an evolution, which simplifies the conventional PRA (i.e. Probabilistic Risk Assessment) approaches. These are often complex and time consuming, and are produced for an existing system rather than driving the system development. Through the use of the ECSS safety risk assessment approach, analysis costs may be reduced dramatically whilst maintaining the concept of modelling uncertainties in a rigorous way. Also, the new 'streamlined' approach should make it easier in the analyses to deal with the short cycle times and introduction of design changes typical to system development.

Both the ECSS hazard analysis and safety risk assessment approaches are process oriented and are aimed at providing analyses, which explicitly state and work towards the goals, objectives and intended use of the analysis results. Analysis results are intended to drive the design and operation through hazard and safety risk reduction, support a specific trade between e.g. two design options, show demonstration with requirements or probabilistic targets, etc.

The ECSS hazard analysis and safety risk assessment standards are not intended to be prescriptive. They only describe a general framework and a process for how to properly perform hazard analyses and safety risk assessments, not prescribe the detailed methods to be used. The actual implementation of the process can be tailored for particular user needs. The only requirements ("shall's") that are expressed in the two standards are to emphasise the implementation of the systematic analysis process, application of the hazard analysis principles and the proper documentation of the analysis and its outputs.

While specifically written for space systems the ECSS hazard analysis and safety risk assessment approaches can also be applied to non-space systems.

CONCLUSIONS

The ECSS-Q-40-02 Hazard analysis standard has completed public review and is in the process of release.

The Safety risk assessment standard ECSS-Q-40-03 is currently being drafted by the ECSS working group, and it is expected to be released for public review in year 2002.

In establishing these two standards the ECSS working group wanted to achieve, as a minimum, the following:

- a common logical approach;
- a theoretically sound and at the same time simple, easy to use methodology acceptable both to administrations and industry;
- flexibility allowing detailed analytical techniques to be applied where appropriate, or even to go to full scale PSA if needed;
- a clear interrelationship between the deterministic and probabilistic processes;
- possibility to use the hazard analysis process or both processes together.

It is believed that, from the previous figures and discussion, it is clear that this objective has been achieved.

REFERENCES

ECSS-M-00-03 Space project management – Risk management. (Available via ECSS web site http://www.ecss.nl/)

ECSS-Q-40 Space product assurance – System safety. (Available via ECSS web site http://www.ecss.nl/)

ECSS-Q-40-02 Space product assurance – Hazard analysis. To be published by ECSS.

ECSS-Q-40-03 Space product assurance – Safety risk assessment. To be published by ECSS.