SLOVENSKI STANDARD
SIST CR 954-100:2002

01-september-2002

Varnost strojev - Z varnostjo povezani deli krmilnih sistemov - 100. del: Vodilo za uporabo in izvedbo EN 954-1:1996

Safety of machinery - Safety-related parts of control systems - Part 100: Guide on the use and application of EN 954-1:1996

Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 100: Leitfaden für Benutzung und Anwendung der EN 954-1:1996

Sécurité des machines - Parties des systèmes de commande relatives a la sécurité - Partie 100: Guide d'utilisation et d'application de l'EN 954-1:1996

Ta slovenski standard je istoveten z: **CR 954-100:1999**

ICS:

13.110	Varnost strojev	Safety of machinery

SIST CR 954-100:2002 **en**

CEN REPORT

RAPPORT CEN

CEN BERICHT

CR 954-100

August 1999

ICS

English version

Safety of machinery - Safety-related parts of control systems - Part 100: Guide on the use and application of EN 954-1:1996

Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 100: Guide d'utilisation et d'application de l'EN 954-1:1996

Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 100: Leitfaden für Benutzung und Anwendung der EN 954-1:1996

This CEN Report was approved by CEN on 10 March 1999. It has been drawn up by the Technical Committee CEN/TC 114.

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

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

Central Secretariat: rue de Stassart, 36 B-1050 Brussels

Ref. No. CR 954-100:1999 E

Foreword

This CEN Report has been prepared by Joint Working Group 6 (JWG 6) of CEN Technical Committee 114, the secretariat of which is held by DIN. It is offered for all to see because JWG 6 is concerned that EN 954-1: 1996 is at times being incorrectly used and interpreted.

JWG 6 is preparing an Amendment to EN 954-1:1996 to incorporate the ideas in this CEN Report together with some additional points.

0 Introduction

EN 954-1 was published in 1996 and from experience gained it is clear that there have been difficulties in understanding how this standard is to be used. This CEN Report gives advice on how to avoid misinterpretations.

EN 954-1:1996 gives guidance on the principles to be followed in:

– designing safety-related parts of control systems (EN 954-1:1996, clause 4);

– the characteristics of safety functions (EN 954-1:1996, clause 5);

– the requirements for the categories of safety-related parts of control systems (EN 954-1:1996, clause 6).

Feedback from users indicates that the scope of EN 954-1:1996 is not fully understood. Therefore it must be emphasised that the standard does not give guidance on:

– the systematic application of the risk reduction process to the selection of the categories of safety-related parts of the control system;

– the application of the risk reduction process to the overall safety requirements of the machine (see EN 954-1:1996, step 2 in figure 1);

– the detailed implementation of safety-related parts utilising different technologies and in particular when different technologies are combined within one safety function.

1 Purpose

This CEN Report provides guidance on the appropriate use and interpretation of EN 954-1 : 1996. It also gives further information on the following topics:

– how the control system contributes to reducing risk in the machine;
– what is meant by the safety-related parts of the control system in relation to safety functions;
– the proper selection and use of categories;
– the role of annex B of EN 954-1:1996.

2 Normative references

Not appropriate. For references referred to within this CEN Report, see annex A.

3 Correct use of EN 954-1:1996

The issues presented in EN 954-1:1996 are complex. The clauses of the standard are interrelated and cannot be used alone. It is therefore necessary to take into account ALL clauses of the standard.

4 Explanation of the design procedures

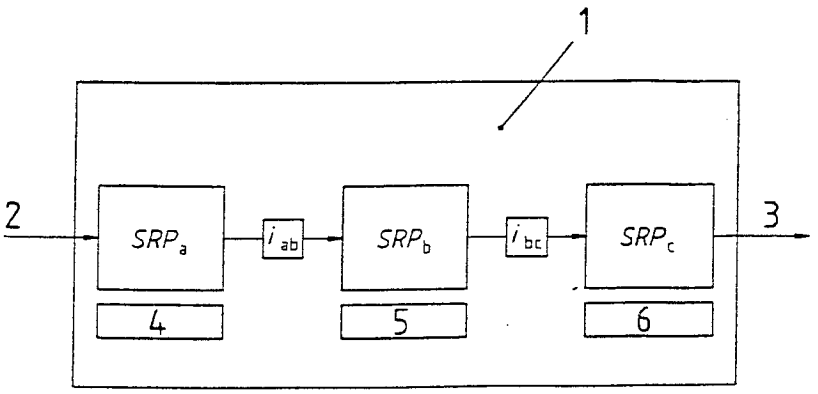
The overall design procedure is given in EN 292-1 : 1991, clause 5. Part of this process is a risk assessment , the principles of which are given in EN 1050. This risk assessment covers the whole machine life cycle. If it is found that there are risks which must be reduced, then appropriate measures must be chosen. EN 292-2 : 1991 gives guidance on the measures for risk reduction.

Part of the risk reduction process is to determine the safety functions (see EN 292-1 : 1991, 3.13) of the machine. This will include the safety functions of the control system, e.g. emergency stop function, start and restart (see EN 954-1 : 1996, clause 5).

A safety function may be implemented by one or more safety-related parts of the control system. The designer may use any of the technologies available, singularly or in combination. A safety function can also be an operational function, e.g. a two-hand control as a means of cycle or process initiation.

A typical safety function is given in figure 1 showing safety-related parts (SRP) for:

- input (SRP_a);
- logic/processing (SRP_b);
- output/power control elements (SRP_c);
- interconnecting means (i_{ab}, i_{bc}), e.g. electrical, optical.



1 Typical safety function
2 Initiation means, e.g. manual actuation, other signals
3 Machine actuators, disconnecting means, brakes
4 Input
5 Logic
6 Output

Figure 1: Diagramatic presentation of a combination of safety-related parts for processing a typical safety function

NOTE 1: Safety-related parts consist of one or more components; components consist of one or more elements.

NOTE 2: All interconnecting means are included in the safety-related parts.

NOTE 3: An example of a safety function is shown in figure 2 and the associated text.

Each safety-related part of the safety function may be made from different technologies. Different technologies may be used for implementing within each safety-related part, e.g. an input comprising a mechanical actuator linked to a light-activated signal converter.

Having established the safety functions of the control system, it is then necessary to identify the safety-related parts of the control system (see EN 954-1 : 1996, 3.1 and clause 8) and then decide how important the contribution is to the risk reduction process. The protective measures provided by the control system depend on this contribution and not directly on the overall risk reduction for the hazard being considered.

NOTE 4: The loss of a safety function does not lead automatically to an injury or a damage to health if other effective protective (safety) measures have been taken.

The greater the reduction of risk is dependent on the safety-related parts of control systems, then the ability of those parts to resist faults is required to be higher (according to EN 954-1 : 1996, 4.2). Therefore protective measures to reduce the risk must be taken, principally:

– **Reducing the probability of faults at the component level.** The aim is to reduce the probability of faults or of failure modes which affect the safety function. This can be made by increasing the reliability of components, e.g. by selection of well-tried components and/or applying well-tried safety principles, in order to exclude critical faults or failure modes. EN 954-1 : 1996 does not give a systematic view on reliability requirements.

– **Improving the structure of the system.** The aim is to avoid the dangerous effect of a fault. Some faults may be detected and a redundant and/or monitored structure may be needed.

Both measures can be used separately or in combination. With some technologies, the required risk reduction can be achieved by selecting reliable components and by fault exclusions, but with other technologies, risk reduction may require a redundant and/or monitored system with two or more parts. In addition, common cause failures should be taken into account. One way of describing these measures is to use the system of five categories established in EN 954-1 : 1996, clause 6.

5 Categories

Categories (for definition see EN 954-1 : 1996, 3.2) are intended to classify safety-related parts of the control system which carry out a safety function, on the basis of their performance in case of fault. These parts may be used singly or in combination. The categories should be considered as reference points for the performance of a safety-related part of a control system with respect to the occurrence of faults (see EN 954-1 : 1996, clause 0). Categories cannot and never should be considered as having accurately delineated limits because the assessment of the parameters being considered can be subjective.

The common conception that the categories of EN 954-1 : 1996 always or alone correspond to levels of risk is not correct.

In choosing a category, the designer must also consider the safety performance to be achieved and this will depend upon both the structure and the reliability of those safety-related parts. EN 954-1 : 1996 does not fully specify reliability requirements.

Therefore all that can be said about the safety performance for a given technology is:

1) Categories 1, 2, 3 and 4 are all better than Category B;
2) In categories B, 1 and 2 a single fault can lead to the loss of the safety function;
3) Categories 3 and 4 will not fail due to a single fault (common mode faults are considered as a single fault);
4) Category 4 has the best performance as regards to fault tolerance because an accumulation of faults is considered.

Control systems employing certain technologies cannot always be designed to satisfy every category, e.g. a mechanical link which meets the requirements of Category 1 but which cannot meet the requirements of Categories 3 or 4. However, the expectation that the safety function will be performed can be equal to, or higher than, that of some other systems which meet Categories 2, 3 or 4.

When a safety function is implemented by several safety-related parts of the control system, three possibilities can occur:

a) each of the safety-related parts has the same category and can be assigned the same overall category;

b) safety-related parts to different categories but used in combination in such a way that an overall category is assigned;

c) an overall category cannot be assigned because the technologies used cannot be designed to satisfy every category.

Detection of a fault by the control system in a Category 3 is not always necessary when a fault is self evident, e.g. when the machine itself reveals the fault by not allowing a start or restart.

Type-C standard writers and designers should be aware of the limitations of setting out the performance of the safety function in terms of an overall category because of the limitations in the category requirements, particularly for reliability.

6 Selection of categories

When selecting categories for the safety-related parts which carry out the safety function(s) (see EN 954-1 : 1996, clause 6), faults which can occur in those parts must be considered under two aspects :

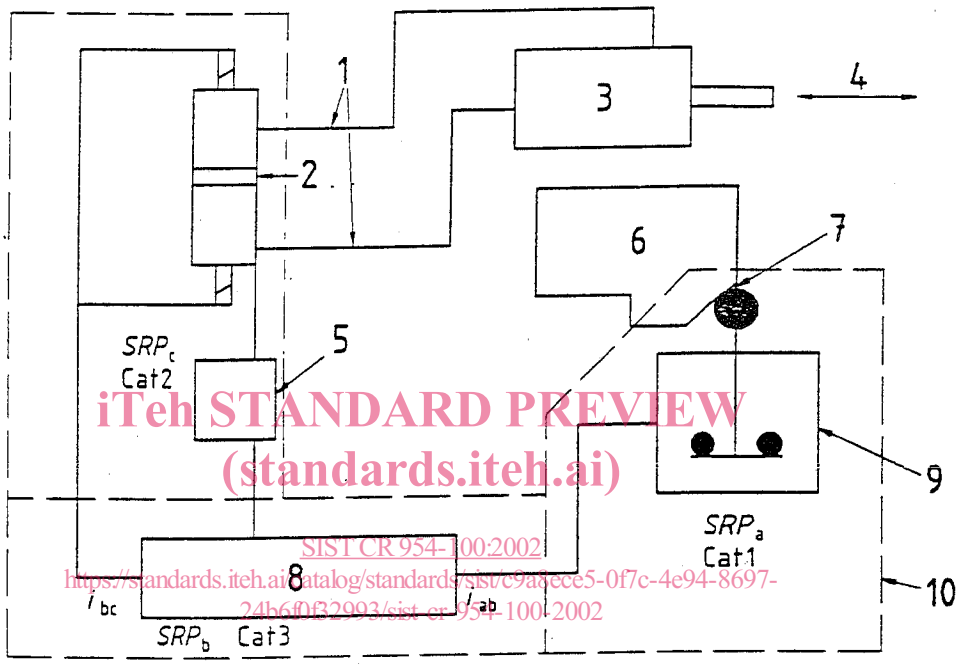
– evaluating the probability of failure or effect of a fault in those parts;
– considering the effect of failure or a fault in those parts on the safety function.

The required performance of the safety function depends upon the level of risk; if the risk is high, the required performance is high and vice versa. When determining the performance, the essential safety and health requirements of directive(s) must be followed. The relevant harmonised standards reflect the state of the art in various applications and this information should be taken into account when selecting categories.

The probability of occurrence of faults is usually established by qualitative estimation, because there is seldom enough data to give a basis for quantitative procedures. This means that in most cases Failure Mode and Effects Analysis (FMEA - see IEC 60812) or similar methods should be used. All relevant faults and/or failure modes should be considered and the actual performance of the safety function in case of a fault should be checked against the required performance.

Some faults or failure modes can be excluded if the probability of their occurrence is very low. This probability depends upon the application conditions. One important consideration is the frequency of demands on the safety function which can vary enormously (from infrequent, e.g. emergency stop device, to continuous, e.g. control of moving machine parts). Because of this, average values or estimates of acceptable failure rates cannot usually be given.

After the whole procedure of risk reduction, a validation (see EN 954-1 : 1996, clause 8) should be made. This validation is part of the validation of the whole machine system.



1 Output signal
2 Fluidic directional valve
3 Fluidic actuators
4 Hazardous movement
5 Checking function
6 Guard
7 Input signal
8 Electronic control logic
9 Position device
10 Scope of EN 954-1

NOTE: The stop and start functions have been omitted to keep the example simple.

Figure 2: Example to explain the use of categories

Figure 2 is a schematic diagram of the safety-related parts to provide one of the functions to control a machine actuator. **This is not a functional/working diagram and is included only to demonstrate the principle of combining categories and technologies in this one function.**

The control is provided through an electronic control logic and a fluidic directional valve checked at suitable intervals (see EN 954-1 : 1996, 6.2.3). The risk is reduced by an interlocking guard which prevents access to the hazardous situation when the guard is closed and prevents start-up of the fluidic actuator when the guard is open.

For this example, the combined safety-related parts of the control system begins at point 7 and ends at point 1 (see figure 2).

The safety-related parts which provide the safety function are: guard cam, position device, electronic control logic, fluidic directional valve and the interconnecting means.

These combined safety-related parts provide a stop function (see EN 954-1 : 1996, 5.2) as a safety function (for definition see EN 954-1 : 1996, 3.6). As the guard opens, the contacts in the position device open and the electronic control logic provides a signal to the fluidic directional valve to stop the fluidic flow as the output of the safety-related parts of the control system. At the machine, this stops the hazardous movement of the actuator.

This combination of safety-related parts creates a safety function to demonstrate the categorisation based on the requirements of EN 954-1 : 1996, clause 6. It considers the possibility and the probability of the faults that can occur which may affect the ability of those combined parts to perform the safey function. Using these principles, the safety-related parts shown in figure 2 can be categorised as follows:

– Category 1 for the electro-mechanical position device.
To reduce the probability of faults this device is comprised of well-tried components applied using well-tried safety principles, e.g. positive opening operation, over-dimensioning (see EN 954-1 : 1996, clause 3 and 6.2.2);

– Category 3 for the electronic control logic.
To increase the level of safety performance of this electronic control logic, the structure of this safety-related part of the control system is designed so that it is able to detect most single faults, e.g. redundancy (see EN 954-1 : 1996, 6.2.4);

– Category 2 for the checked fluidic directional valve.
To achieve the required level of safety performance, this safety-related part uses components which are periodically checked, e.g. monitoring, in order to detect the faults which have not been avoided using well-tried safety principles (see EN 954-1 : 1996, 6.2.3).

NOTE: The position, size and layout of the interconnecting means have also to be taken into account.

The overall objective is that each of the safety-related parts achieves a similar level of safety performance so that the contribution of the safety-related parts of the control system provides the required reduction in risk. Therefore the reliability and structure within the safey-related parts of the control system have both to be considered.

7 The role of annex B in EN 954-1

When evaluating risks, the procedures given in EN 1050 must be followed. The advice given in EN 954-1 : 1996, annex B is for information only.

Annex A (informative)

Bibliography

EN 292-1 : 1991
Safety of machinery - Basic concepts, general principles for design - Part 1: Basic terminology, methodology

EN 292-2 : 1991/A1 : 1995
Safety of machinery - Basic concepts, general principles for design - Part 2: Technical principles and specifications

EN 954-1 : 1996
Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design

EN 1050
Safety of machinery - Principles for risk assessment

IEC 60812
Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)