SLOVENSKI STANDARD

SIST-TP CLC/R0BT-004:2004

september 2004

Direktive ES, funkcionalna varnost in vloga standardizacije CENELEC

EC Directives, functional safety and the role of CENELEC standardization

ICS 01.120; 13.110

Referenčna številka
SIST-TP CLC/R0BT-004:2004(en)

CENELEC **R0BT-004**

REPORT October 2001

English version

EC Directives, functional safety and the role of CENELEC standardization

This CENELEC Report has been prepared by the CENELEC BTWG 99-2, "Functional safety". It was approved for publication by the CENELEC Technical Board on 2000-04-01.

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

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Ref. No. R0BT-004:2001 E

Foreword

This CENELEC Report on functional safety has been prepared by CENELEC BTWG 99-2, Functional safety.

This report provides a definition of functional safety and considers the relationship between functional safety and CENELEC standards including those that have been harmonized under relevant EC directives e.g. the LVD, ATEX, MDD, MD, EMC.

The text of the draft was approved by the CENELEC Technical Board for final editing and publication on 2000-04-01.

1 Task

Arising from the background given in annex A, CENELEC BTWG 99-2 was asked to prepare a report on functional safety which addressed:-

- the definition of functional safety;
- the way in which functional safety is being handled, from a CENELEC standardization viewpoint, under various EC Directives but specifically those relevant for the electrotechnical field such as the LVD, ATEX, MDD, MD, EMC.;
- the implications of functional safety related to safety-related EMC-immunity within the scope of the Low Voltage Directive and other EC Directives from a CENELEC standardization viewpoint.

2 Functional safety

2.1 Definition of functional safety

Functional safety is, for the purpose of this Report, defined as:-

"Part of the overall safety relating to the equipment and its associated control system which depends on the correct functioning of electrical, electronic, programmable electronic (E/E/PE) safety-related systems, other technology safety related systems", external risk reduction facilities.

This definition is based on IEC 61508-4 (see Annex B for an overview of IEC 61508).

2.2 What is functional safety?

The key to understanding functional safety is the concept of a safety-related system. The term 'safety related' is used to describe those systems (i.e. a safety-related system) which are required to perform a specific function or functions (i.e. safety functions) to reduce risks to a level which is considered tolerable.

The key to the understanding of safety-related systems is the concept that a safety-related system carries out safety functions and that a safety function should be specified both in terms of its functionality (what the function does) and its safety integrity (the probability of a safety function being performed satisfactorily).

Safety-related systems may be implemented in any technology, but in the context of CENELEC standardisation the primary concern are those which are implemented in E/E/PE technologies.

The following are examples of E/E/PE safety-related systems:

- an emergency shut-down system in a hazardous chemical process plant;
- a crane safe load indicator;
- a railway signalling system;

- guard interlocking systems and emergency stopping systems for machinery and household appliances;
- a variable speed motor drive used to control a restricted speed as a means of protection;
- the system for interlocking and controlling the exposure dose of a medical radiotherapy machine.
- the indicator lights, anti-lock braking, and engine-management systems on a motor car.

It should be noted that an E/E/PE safety-related system covers all parts of the system that implements the safety function (i.e. from sensor, control logic, communication systems through to the final actuator).

2.3 Safety integrity

The specification for safety integrity is derived by undertaking a risk analysis and determining the necessary risk reduction that the safety function is required to achieve. The general principle is that more rigour is required in the engineering of safety-related systems at higher levels of safety integrity in order to achieve the necessary lower failure rates.

To ensure that the safety integrity of the safety functions is adequate for the specific application, the safety-related system has to be designed taking into account the many failure causes which might arise from:

- incorrect specifications of the system and/or hardware and/or software.

- omissions in the safety requirements specification (eg. failure to develop all relevant safety functions during different modes of operation);
- random hardware failure mechanisms;
- systematic hardware failure mechanisms;
- software errors;
- environmental influences (e.g. electromagnetic, temperature, mechanical phenomena);
- supply system voltage disturbances (loss of supply; reduced voltages; re-connection of supply).

The key requirements for the achievement of adequate safety integrity comprise requirements for:

- hardware safety integrity (i.e. random hardware failures);
- systematic safety integrity comprising:
  - requirements for the avoidance (prevention) of systematic failures;
  - requirements for the control of systematic failures.

Systematic failure causes, which are relevant to both hardware and software, are of key concern in complex electronic systems, such as programmable electronic systems, since the failure modes of such systems are complex and for most practical purposes cannot be fully determined.

Any strategy for the achievement of functional safety must include the achievement of an adequate level of safety integrity.

An example of functional safety is given in annex C.

3 Concept for a coherent set of standards for functional safety

In IEC, work on functional safety has led to the publication of IEC 61508, "Functional safety of electrical, electronic, programmable safety-related systems". The scope of this seven part standard covers all safety-related systems which are electrotechnical in nature (electro-mechanical systems; solid state electronic systems; computer based systems). An overview of IEC 61508 is provided in annex B.

IEC 61508 is generic and can be used directly by industry (as a “standalone” standard) and also by standards writers as a basis for the development of sector standards (e.g. for the machinery sector; for the process sector; for the nuclear sector). IEC 61508 will therefore influence the development of E/E/PE safety-related systems across all sectors. IEC 61508, or one of its sector implementations, may be used to facilitate the development of product standards.

IEC 61508 has already been used to influence a number of developments and work is in progress to develop sector implementations.

Generally, the significant hazards for a product have to be identified by the manufacturer via a hazard analysis. If this analysis identifies that functional safety is necessary in order to have adequate protection against a significant hazard, for the product in question, then it has to be taken into account in an appropriate manner in the product design. Similarly, standards writers need to address functional safety in their safety standard (see ISO/IEC Guide 51) if the hazard analysis carried out by a TC identifies that functional safety is necessary in order to have adequate protection against a significant hazard. Since IEC 61508 has a safety pilot function, according to Guide 104, the requirements specified in safety standards shall be in accordance with the requirements in IEC 61508.

4 Functional safety and EC Directives

In order to remove barriers to trade and to ensure the free trade of products within the European Union, the Council adopts EC directives based on Article 100(a) of the EU treaty. Most of these EC directives focus on certain products and deal with safety aspects (e.g. ATEX, LVD, MD, MDD).

Such product directives are “total safety” directives since they cover all relevant safety aspects of a product including, where relevant, functional safety. Some directives specify the requirements in a very detailed way (e.g. the MD) other directives specify the requirements in a more abstract manner (e.g. the LVD).

Although the LVD has been in force for more than 25 years there still exists the misunderstanding that it only covers electrical safety. However, Annex 1 of the LVD listing the relevant safety requirements leaves no doubt that the LVD deals with safety of electrotechnical products and not with electrical safety of products. In order to clarify this misunderstanding the European Commission has explicitly confirmed the total safety approach of the LVD in their Guidelines on the Application of Council Directive 73/23/EEC (item 10).

Although the LVD does not explicitly use the term functional safety, the following requirements of Annex 1, Clauses 2(c) and 3(b) of the LVD are relevant:

> "2. Protection against hazards arising from the electrical equipment:
>
> (a) .....
>
> (b) .....
>
> (c) Persons, domestic animals and property must be adequately protected against non-electrical dangers caused by the electrical equipment which are revealed by experience.
>
> 3. Protection against hazards which may be caused by external influences on the electrical equipment
>
> (a) .....
>
> (b) The electrical equipment must be resistant to non-mechanical influences in the expected environmental conditions, in such a way that persons, domestic animals and property are not endangered.
>
> (c) ....."

It can be argued that 2(c) covers functional safety in general and that 3(b) covers functional safety in the context of safety-related EMC – immunity in particular and other environmental influences.

As mentioned above, other EC directives specify more precisely that functional safety has to be observed. For example, Article 1.2 of Annex 1 of the MD requires that controls must be designed and constructed so that they are safe and reliable.

Accordingly, it will be incumbent on the writers of standards to consider the inclusion of the above-mentioned procedures regarding hazard analysis and functional safety when establishing or revising the relevant product (or family product) standards including those covered by other EC directives covering safety aspects (e.g. ATEX, MD, MDD).

5 EMC and functional safety

If a product is insufficiently immune against electromagnetic disturbances then a failure of the safety-related function can cause a hazardous condition for persons or properties etc and in such a case safety-related EMC-immunity1 is a relevant aspect in the context of functional safety.

[1)] In the context of this report, EMC-immunity describes immunity from electromagnetic disturbances.

In other cases, where insufficient EMC immunity leads to a reduction of performance (e.g. flicker of a TV screen or a non-hazardous failure of control equipment) but not to dangerous failures, then EMC is not part of the functional safety but part of performance related EMC. Only these latter aspects are covered by the EMC Directive.

If the hazard analysis carried out by a TC identifies that functional safety is relevant and necessary in order to have adequate protection against a significant hazard, then safety-related EMC-immunity will need to be addressed and requirements included in relevant safety standards. If a safety-related EC directive exists for this product this standard has to be offered to the European Commission for listing in the OJEC under this safety-related EC directive but not under the EMC Directive.

Within IEC, a Technical Specification (IEC 61000-1-2) has been developed to deal with the achievement of adequate EMC-immunity with regard to functional safety. The document should provide essential support for IEC 61508.

6 Summary

In summary:

1. *The definition of functional safety in IEC 61508 provides a sound technical basis for future CENELEC standardization activity;*

2. *Functional safety is within the scope of "total safety" directives such as ATEX, LVD, MD, MDD.;*

3. *IEC 61508 provides a basis for dealing with the functional safety of E/E/PE safety-related systems;*

4. *The Technical Specification IEC 61000-1-2 is very important for standardization activities since it will be of value to all Technical Committees who have to set requirements for the achievement of adequate EMC-immunity with regard to functional safety. However, co-ordination of safety-related EMC-immunity levels will need to be addressed.*

5. *For E/E/PE safety-related systems, not covered by an EC "total safety" directive IEC 61508 provides a standardization route for achieving functional safety including aspects relating to safety-related EMC-immunity*

6. *IEC 61508 provides a basis for establishing a coherent set of standards for functional safety at generic, sector and product levels. As far as is possible, CENELEC should not seek to develop its own approach to functional safety by developing its own standards but should support, according to the Dresden Agreement, IEC activities. This would also be in the spirit of the WTO-TFB Agreement.*