



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 16855.1-2018

**Safety of machinery -- Safety-related parts of control systems --
Part 1: General principles for design**

Issued on: December 28, 2018

Implemented on: July 1, 2019

Issued by: SAMR; SAC

Table of Contents

Foreword...	4
Introduction...	6
1 Scope...	9
2 Normative References...	10
3 Terms, Definitions, Symbols and Abbreviated Terms...	10
3.1 Terms and definitions...	10
3.2 Symbols and abbreviated terms...	17
4 Design Considerations...	19
4.1 Safety objectives in design...	19
4.2 Strategy for risk reduction...	20
4.3 Determination of required performance level (PLr)...	24
4.4 Design of SRP/CS...	25
4.5 Evaluation of the achieved performance level PL and relationship with SIL	26
4.6 Software safety requirements...	34
4.7 Verification that achieved PL meets PLr.....	41
4.8 Ergonomic aspects of design...	41
5 Safety Functions...	41
5.1 Specification of safety functions...	41
5.2 Details of safety functions...	45

Foreword

GB/T 16855 Safety of Machinery - Safety-Related Parts of Control Systems consists of the following two parts.

--- Part 1.General Principles for Design.

--- Part 2.Validation.

This Part is Part 1 of GB/T 16855.

This Part was drafted as per the rules specified in GB/T 1.1-2009.

This Part replaced GB/T 16855.1-2008 Safety of Machinery - Safety-Related Parts of Control Systems - Part 1.General Principles for Design. Compared with GB/T 16855.1-

2008, this Part has the major technical changes besides the editorial modifications as follows.

- Modify the standard name into Safety of Machinery - Safety-Related Parts of Control Systems - Part 1.General Principles for Design;
- Delete the Table 1 in the Introduction (see Introduction of 2008 Edition);
- Modify the term "system failure" into "systematic failure" (see 3.1.7 of this Edition;

3.1.7 of 2008 Edition);

- Modify the term "mean time to dangerous failure" into "mean time between failure"; and modify its abbreviation into "MTTFD" (see 3.1.25 of this Edition;

3.1.25 of 2008 Edition);

- Add the terms "high demand and continuous mode" and "proven in use", and their definitions (3.1.38 and 3.1.39 of this Edition);
- Modify the Figure 1 (see Figure 1 of this Edition; Figure 1 of 2008 Edition);
- Add the requirements of SRP/CS output part as per category description (see

4.5.5 of this Edition);

- Modify the calculation or estimation of the MTTFD value of a single component (see Appendix C of this Edition; Appendix C of 2008 edition);
- Re-draft Appendix I (see Appendix I of this Edition, Appendix I of 2008 edition).

This Part uses translation method to equivalently adopt ISO 13849-1.2015 Safety of Machinery - Safety-Related Parts of Control Systems - Part 1.General Principles for Design.

The Chinese documents that have a consistent correspondence with the international documents in the normative references of this Part are as follows.

- GB 28526-2012 Electrical Safety of Machinery - Functional Safety of Safety-Related Electrical, Electronic and Programmable Electronic Control Systems (IEC 62061.2005, IDT);
- GB/T 30175-2013 Safety of Machinery - Guidance on the Application of GB/T

16855.1 and GB 28526 in the Design of Safety-Related Control Systems

(ISO/TR 23849.2010, IDT).

This Part made the following editorial modifications.

--- Modify the editorial errors in Table 1; modify "Table 3" into "Table 2"; modify "Table 4" into "Table 3", modify "Table 7" into "Table 6".

This Part was proposed by and under the jurisdiction of National Technical Committee for Standardization of Machinery Safety (SAC/TC 208).

Drafting organizations of this Part. Pilz Electronics (Changzhou) Co., Ltd.; China Productivity Center for Machinery; Anhui Leku Intelligent Parking Equipment Co., Ltd.; Suzhou Angoey Smart Safety Technologies Limited Inc.; Xiamen Rituo Electrical Technology Co., Ltd.; Nanan Zhongji Institute of Standardization Co., Ltd.; Fujian MinXuan Technology Co., Ltd.; Mesnac Co., Ltd.; China Software Test Center; Anshineng (Shanghai) Mechanical & Electrical Commerce and Trade Co., Ltd.; Center Testing International Group Co., Ltd.; Nanjing University of Science and Technology; Xi'an Xumai Smart Home Appliance Technology Co., Ltd.; Nanjing Forestry University/National-Provincial Joint Engineering Research Center of Electrometrical Product Packaging; Nanan Testing Institute of Quality and Metrology; Lihong Safety Engineering (Shanghai) Co., Ltd.; and Zhejiang Ptarmigan Supply China Management Co., Ltd.

Chief drafting staffs of this Part. Zhang Xiaofei, Huang Zhijiong, Li Qing, Zhu Bin, Sun Zhenchao, Li Liyan, Zhao Yangyang, Wang Baozhen, Yu Mingjin, Liu Fawang, Lu Xiaoguang, Guo Yongzhen, Liu Panchao, Ju Likai, Cheng Hongbing, Bai Honghai, Ju Ronghua, Ji Kun, Hou Hongying, Huang Dongsheng, Yin Zhiyao, Fu Huiqing, Liu Ying, Chen Zhuoxian, Li Zhong, Liu Zhiyong, Song Xiaoning, Li Yali, and Zhou Aiping.

The historical editions replaced by this Standard are as follows.

--- GB/T 16855.1-1997, GB/T 16855.1-2005, GB/T 16855.1-2008.

1 Scope

This Part of GB/T 16855 provides safety requirements and guidance on the principles

for the design and integration of safety-related parts of control systems (SRP/CS), including the design of software. For these parts of SRP/CS, it specifies characteristics that include the performance level required for carrying out safety functions.

2 Normative References

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this document.

GB/T 2900.13-2008 Electrotechnical Terminology - Dependability and Quality of Service [IEC 60050(191).1990, IDT]

3 Terms, Definitions, Symbols and Abbreviated Terms

State of an item characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

Use of a machine in a way not intended by the designer, but which may result from readily predictable human behavior.

4 Design Considerations

The purpose in following the overall design procedure for the machine is to achieve the safety objectives (see 4.1). The design of the SRP/CS to provide the required risk reduction is an integral subset of the overall design procedure for the machine.

5 Safety Functions

Where necessary, the requirements for characteristics and safety functions shall be adapted for use with different energy sources.

The structure of an SRP/CS is a key characteristic having great influence on the PL. Even if the variety of possible structures is high, the basic concepts are often similar. Thus, most structures which are present in the machinery field can be mapped to one of the categories.