ICS 25.040
N 10

中华人民共和国国家标准化指导性技术文件

GB/Z 29638—2013/IEC/TR 61508-0:2005

电气/电子/可编程电子安全相关系统的功能安全　功能安全概念及GB/T 20438系列概况

Functional safety of electrical/electronic/ programmable electronic safety-related systems—Functional safety and GB/T 20438

(IEC/TR 61508-0:2005,IDT)

2013-07-19 发布　　2013-12-15 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　功能安全 …… 1
3.1　功能安全是什么 …… 1
3.2　安全功能及安全相关系统 …… 2
3.3　功能安全示例 …… 2
3.4　实现功能安全的挑战 …… 2
4　GB/T 20438　E/E/PE 安全相关系统的功能安全 …… 3
4.1　目的 …… 3
4.2　E/E/PE 安全相关系统 …… 3
4.3　技术方法 …… 4
4.4　安全完整性等级 …… 4
4.5　功能安全示例回顾 …… 4
4.6　GB/T 20438 框架 …… 5
4.7　GB/T 20438 作为其他标准的基础 …… 6
4.8　GB/T 20438 作为独立的标准 …… 7
4.9　更多信息 …… 7
附录 A（资料性附录）　IEC“功能安全”专区的常见问题列表 …… 8

前　言

GB/T 20438《电气/电子/可编程电子安全相关系统的功能安全》由下列7个部分构成：

——第1部分：一般要求；

——第2部分：电气/电子/可编程电子安全相关系统的要求；

——第3部分：软件要求；

——第4部分：定义和缩略语；

——第5部分：确定安全完整性等级的方法示例；

——第6部分：GB/T 20438.2和GB/T 20438.3的应用指南；

——第7部分：技术和措施概述。

本指导性技术文件，是对GB/T 20438标准的补充。它主要介绍功能安全的概念以及GB/T 20438系列标准的概况，本指导性技术文件可与GB/T 20438系列标准配套使用。

本指导性技术文件按照GB/T 1.1—2009给出的规则起草。

与本文件中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 16499—2008　安全出版物的编写及基本安全出版物和多专业共用安全出版物的应用导则(IEC Guide 104:1997,NEQ)

——GB/T 20000.4—2003　标准化工作指南　第4部分：标准中涉及安全的内容(ISO/IEC Guide 51:1999,MOD)

本指导性技术文件等同采用IEC/TR 61508-0:2005《电气/电子/可编程电子安全相关系统的功能安全　第0部分：功能安全概念及IEC 61508系列概况》。

本指导性技术文件的技术内容与IEC/TR 61508-0:2005等同，为了便于使用，做了如下编辑性修改：

——删除国际标准的前言，按GB/T 1.1—2009重新编写了本文件的前言；

——正文中，凡是出现“IEC 61508”之处均改为“GB/T 20438”；

——凡是出现“本技术报告”之处均改为“本文件”；

——根据GB/T 1.1—2009进行格式编辑性修改。

本指导性技术文件由中国机械工业联合会提出。

本指导性技术文件由全国工业过程测量和控制标准化技术委员会(SAC/TC 124)归口。

本指导性技术文件主要起草单位：机械工业仪器仪表综合技术经济研究所、上海自动化仪表股份有限公司、上海工业自动化仪表研究院、北京和利时系统工程有限公司、深圳市步科电气有限公司、北京市劳动保护科学研究所、斯堪伯奥科技(北京)有限公司、菲尼克斯电气(南京)研发工程中心有限公司、中国铁道科学研究院、中机生产力促进中心、浙江大学智能系统与控制研究所、皮尔磁工业自动化贸易(上海)有限公司、华中科技大学控制系、西门子(中国)有限公司。

本指导性技术文件主要起草人：丁露、王春喜、欧阳劲松、史学玲、孟邹清、包伟华、李佳嘉、罗安、池家武、靳江红、王海清、张龙、张萍、张晓飞、冯冬芹、褚卫中、周纯杰、李佳。

引　言

本指导性技术文件的目的是介绍功能安全的概念，并提供 GB/T 20438 系列标准的概述。

当您有如下需求时可阅读本指导性技术文件：

——判断 GB/T 20438 是否适用于您；

——参与可能涉及安全的电气/电子/可编程电子系统的开发；

——起草功能安全相关的任何其他标准。

本指导性技术文件的第 3 章给出功能安全的非正式定义，描述了安全功能、安全完整性和安全相关系统之间的关系、给出如何得出功能安全要求的示例，并列出了一些用电气/电子/可编程电子系统实现功能安全将遇到的挑战。第 4 章介绍了 GB/T 20438 的具体内容，提供了实现功能安全的方法，并描述了 GB/T 20438 的目的、技术方法和框架。它阐述了 GB/T 20438 可广泛地用于不同行业，并可作为许多其他标准的基础。

电气/电子/可编程电子安全相关系统的功能安全　功能安全概念及GB/T 20438系列概况

1　范围

本指导性技术文件介绍了功能安全的概念及GB/T 20438系列的概况。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 20438.1—2006　电气/电子/可编程电子安全相关系统的功能安全　第1部分：一般要求(IEC 61508-1:1998，IDT)

GB/T 20438.2—2006　电气/电子/可编程电子安全相关系统的功能安全　第2部分：电气/电子/可编程电子安全相关系统的要求(IEC 61508-2:2000，IDT)

GB/T 20438.3—2006　电气/电子/可编程电子安全相关系统的功能安全　第3部分：软件要求(IEC 61508-3:1998，IDT)

GB/T 20438.4—2006　电气/电子/可编程电子安全相关系统的功能安全　第4部分：定义和缩略语(IEC 61508-4:1998，IDT)

GB/T 20438.5—2006　电气/电子/可编程电子安全相关系统的功能安全　第5部分：确定安全完整性等级的方法示例(IEC 61508-5:1998，IDT)

GB/T 20438.6—2006　电气/电子/可编程电子安全相关系统的功能安全　第6部分：GB/T 20438.2和GB/T 20438.3的应用指南(IEC 61508-6:2000，IDT)

GB/T 20438.7—2006　电气/电子/可编程电子安全相关系统的功能安全　第7部分：技术和措施概述(IEC 61508-7:2000，IDT)

IEC Guide 104　安全出版物的编写及基本安全出版物和多专业共用安全出版物的应用导则(The preparation of safety publications and the use of basic safety publications and group safety publications)

ISO/IEC Guide 51　安全方面　在标准中引入安全条款的指南(Safety aspects—Guidelines for their inclusion in standards)

3　功能安全

3.1　功能安全是什么

安全是指避免会造成人体健康损害或人身损伤的不可接受风险，而这种风险是由于对财产或环境的破坏而直接或间接地导致的。

功能安全是整体安全的一部分，它依赖于一个系统或设备对其输入的正确响应。

例如，在电机绕组上装一个热传感器，可以在电机过热前实现断电的过热保护装置是功能安全的一个例子。但用特殊的隔热材料来抵御高温就不是功能安全的例子(虽然这也是实现安全的一个例子，并