ICS 25.040.40.35.240.50
N 18

中华人民共和国国家标准

GB/T 15969.6—2015/IEC 61131-6:2012

可编程序控制器　第6部分:功能安全

Programmable controllers—Part 6:Functional safety

(IEC 61131-6:2012,IDT)

2015-12-10 发布　　2016-07-01 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

GB/T 15969《可编程序控制器》包含以下部分：

——第1部分：通用信息；

——第2部分：设备要求和测试；

——第3部分：编程语言；

——第4部分：用户导则；

——第5部分：通信；

——第6部分：功能安全；

——第7部分：模糊控制编程；

——第8部分：编程语言的应用和实现导则。

本部分为GB/T 15969的第6部分。

本部分按照GB/T 1.1—2009和GB/T 20000.2—2009给出的规则起草。

本部分使用翻译法等同采用IEC 61131-6:2012《可编程序控制器　第6部分：功能安全》。

为方便使用，本部分作了如下编辑性修改：

——删除国际标准的前言，按GB/T 1.1—2009重新编写了本部分的前言；

——正文中，凡是出现“IEC 61131-6”之处均改为本部分；

——对全文范围内列项的标点符号进行规范；

——为了保持与IEC 61131-6:2012一致性，正文中，保留不注日期的引用文件。

与本部分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 17626.2—2006　电磁兼容　试验和测量技术　静电放电抗扰度试验(IEC 61000-4-2:2001，IDT)

——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 20438.6—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)

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分由中国机械工业联合会提出。

本部分由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

本部分起草单位：机械工业仪器仪表综合技术经济研究所、北京机械工业自动化研究所、浙江大学、浙江中控科技集团有限公司、北京和利时系统工程有限公司、罗克韦尔自动化(中国)有限公司、北京国电智深控制技术有限公司、中国铁道科学研究院、重庆川仪自动化股份有限公司、江苏添福产品服务有限公司北京分公司、中科院沈阳自动化研究所、上海自动化仪表股份有限公司和西南大学。

本部分主要起草人：王春喜、高镜媚、汪烁、孙洁香、史学玲、熊文泽、罗安、周有铮、冯冬芹、田玉聪、张萍、华镕、徐皑冬、陈学军、赵勇、包伟华、裘坤、刘枫。

引　言

本部分为GB/T 15969的第6部分，针对可编程序控制器及其相关的外围设备，应与其他部分结合阅读。

作为功能安全可编程序逻辑控制器(FS-PLC)产品标准，本部分内容可认为是涵盖可编程序控制器及其相关的外围设备。

如果不能满足本部分第4章的要求，则不能声明符合GB/T 15969的第6部分。

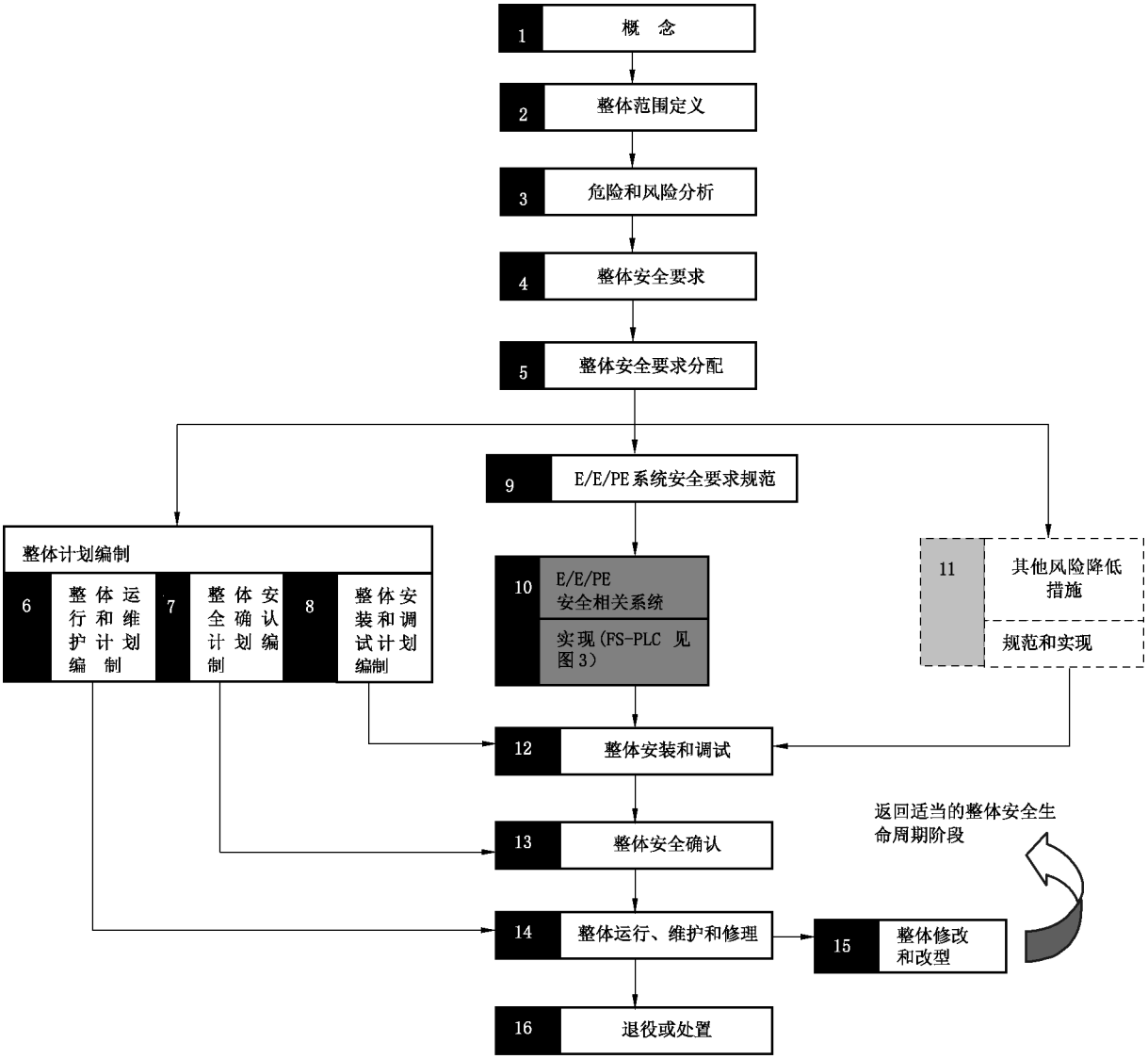
GB/T 15969的第1部分定义了通用术语。更多特定术语在各部分中进行定义。

为了与IEC 61508-1:2010的1.1保持一致，本部分包含了IEC 61508-1、IEC 61508-2和IEC 61508-3中与可编程序控制器及其相关的外围设备有关的产品特定要求。

本部分原则上是依据IEC 61508的结构。但是由于有些方面没有直接联系，因而需要不同处理。某种程度上，这是由于需要在一个单独文档中处理硬件、软件、固件等。

本部分的框架如IEC 61508-1:2010的图2，这里重新编号为图1，并对其进行了调整，以示出FS-PLC是如何用于整体E/E/PE安全相关系统安全生命周期。尽管图1方框10包含传感器、逻辑子系统和最终元件(如执行器)，但从IEC 61508-1的角度，这里通过引用图3来突出FS-PLC。

同样地，从本部分的角度来看，图1方框10的实现阶段仅体现了逻辑子系统。



注 1：为清楚起见，与功能安全验证、功能安全管理以及功能安全评估有关的活动未在图中显示，但这些都与整体的、E/E/PE 系统的和软件的安全生命周期各阶段有关。

注 2：方框 11 所表示的阶段不在本标准范围之内。

注 3：IEC 61508-2 和 IEC 61508-3 涉及方框 10(实现)，但有关部分也涉及方框 13、方框 14 和方框 15 的可编程电子方面(硬件和软件)。

注 4：见 IEC 61508-1 的表 1，描述了各方框表示的各阶段的目标和范围。

注 5：整体操作、维护、维修修改、改型及退役或处置所需的技术要求将规定为 E/E/PE 安全相关系统及其组件和元件供应商提供的信息部分。

图 1 整体 E/E/PE 安全相关系统安全生命周期各阶段中的 FS-PLC

本部分包括的范围是 FS-PLC 安全生命周期管理、功能安全要求分配和开发规划，其重点是在整体安全生命周期的实现阶段(方框 10)。本部分假设 FS-PLC 用作整体 E/E/PE 系统的逻辑子系统。

图 1 的实现(方框 10)包括：

——将 FS-PLC 的各方面安全功能分配到 FS-PLC 硬件、软件或固件、或任意组合中去；

——FS-PLC 硬件结构；

——FS-PLC 级的验证和确认活动；

——FS-PLC 修改要求；
——FS-PLC 用户使用的操作和维护信息；
——FS-PLC 制造商提供给用户的信息。

可编程序控制器　第6部分:功能安全

1　范围

GB/T 15969的本部分规定了对GB/T 15969.1定义的可编程序控制器(PLC)及其相关的外围设备的要求,其目的是用作电气/电子/可编程电子(E/E/PE)安全相关系统的逻辑子系统。符合本部分要求的可编程序控制器及其相关的外围设备认为是适用于E/E/PE安全相关系统的,称为功能安全可编程序逻辑控制器(FS-PLC)。FS-PLC通常是硬件(HW)/软件(SW)子系统。FS-PLC也可包含软件组件,如预定义的功能块。

E/E/PE安全相关系统通常包含传感器、执行器、软件和逻辑子系统。本部分是IEC 61508标准要求的产品特定实现,符合本部分就符合IEC 61508标准关于FS-PLC的所有适用的要求。IEC 61508标准是系统标准,而本部分为IEC 61508标准的原则在FS-PLC中的应用,提供了产品特定要求。

当FS-PLC用作E/E/PE安全相关系统的一部分时,本部分仅处理FS-PLC的功能安全和安全完整性要求。整体E/E/PE安全相关系统的功能安全要求和E/E/PE安全相关系统的最终应用的功能安全要求的定义不在本部分包含的范围内,但它们是本部分的输入。对于应用特定信息,读者可参考其他标准,如GB/T 21109标准、GB 28526和GB/T 16855标准。

本部分不包括FS-PLC的通用安全要求,如与GB/T 15969.2规定的电击和火灾危险相关的要求。

本部分适用于安全完整性等级(SIL)能力不高于SIL 3的FS-PLC。

本部分的目的是:

a) 建立和描述FS-PLC的安全生命周期组件,与IEC 61508-1～IEC 61508-3标识的通用安全生命周期一致;

b) 建立和描述关于E/E/PE安全相关系统的功能安全和安全完整性要求的FS-PLC硬件和软件要求;

c) 建立对FS-PLC的评估方法,依据本部分如下参数/准则:

1) FS-PLC能够达到的安全完整性等级(SIL)声明;

2) 要求时失效概率(PFD)值;

3) 每小时危险失效平均频率(PFH)值;

4) 安全失效分数(SFF)值;

5) 硬件故障裕度(HFT)值;

6) 诊断覆盖率(DC)值;

7) 验证规定的FS-PLC制造商的安全生命周期过程已就位;

8) 定义的安全状态;

9) 用于预防和控制系统性故障的措施和技术;

10) 对于本部分处理的各失效模式,失效状态下的功能行为。

d) 建立定义并标识FS-PLC及其相关的外围设备的选择和应用相关的主要特性。

本部分主要用于FS-PLC制造商。通过用户文档要求,本部分也包含了FS-PLC用户的关键角色。一些FS-PLC的用户指南可见GB/T 15969.4。