**编号：CGC-R49016：2014**

# 功能安全认证实施规则

# 过程工业自动控制系统

（显示仪表系统、控制/调节仪表系统、工业过程自动控制报警装置系统、基地式仪表、自动化控制成套设备、工业控制用计算机/系统、巡回检测装置、远动装置等产品）

本资料版权为北京鉴衡认证中心所有，且受版权法和国 际公约保护。如未获得本中心许可，任何单位和个人不 得以任何形式或任何方法复制本资料及其任何部分用于 任何目的。鉴衡认证中心保留依法追究侵权责任的权利。

**北京鉴衡认证中心**

2014年01月26日

**目录**

[1. 适用范围 4](#_Toc379894696)

[2. 认证依据 4](#_Toc379894697)

[3. 认证模式 4](#_Toc379894698)

[4. 认证申请 4](#_Toc379894699)

[4.1 申请认证产品的基本要求 4](#_Toc379894700)

[4.2 申请单元划分 4](#_Toc379894701)

[4.3 申请认证提交材料 4](#_Toc379894702)

[5. 设计评估 5](#_Toc379894703)

[5.1 资料审查 5](#_Toc379894704)

[5.2 文档评估 7](#_Toc379894705)

[6. 型式试验 7](#_Toc379894706)

[6.1 样品要求 7](#_Toc379894707)

[6.1.1 一般要求 7](#_Toc379894708)

[6.1.2 抽样和送样要求 7](#_Toc379894709)

[6.2 型式试验 7](#_Toc379894710)

[6.2.1 试验内容和要求 8](#_Toc379894711)

[6.2.2 试验方法和要求 8](#_Toc379894712)

[6.2.3 型式试验时限 8](#_Toc379894713)

[6.2.4 型式试验报告 8](#_Toc379894714)

[6.2.1 型式试验评估 8](#_Toc379894715)

[7. 初始工厂审查 8](#_Toc379894716)

[7.1 审查内容 8](#_Toc379894717)

[7.1.1 工厂质量保证能力审查 8](#_Toc379894718)

[7.1.2 产品一致性检查 8](#_Toc379894719)

[7.2 初始工厂审查时间 9](#_Toc379894720)

[8. 认证结果评价与批准 9](#_Toc379894721)

[9. 获证后监督 9](#_Toc379894722)

[9.1 监督检查的频次 9](#_Toc379894723)

[9.2 监督的内容 9](#_Toc379894724)

[9.2.1 工厂质量保证能力复查 9](#_Toc379894725)

[9.2.2 产品一致性检查 10](#_Toc379894726)

[9.3 产品抽样检检测 10](#_Toc379894727)

[9.4 获证后监督结果的评价 10](#_Toc379894728)

[10. 复审 10](#_Toc379894729)

[11. 认证证书 10](#_Toc379894730)

[11.1 认证证书的保持 10](#_Toc379894731)

[11.1.1 证书的有效性 10](#_Toc379894732)

[11.2 认证产品的变更 10](#_Toc379894733)

[11.2.1 变更的申请 10](#_Toc379894734)

[11.2.2 变更评价和批准 10](#_Toc379894735)

[11.2.3 认证证书覆盖产品的扩展 10](#_Toc379894736)

[11.3 认证范围的扩大 11](#_Toc379894737)

[11.4 认证范围的缩小 11](#_Toc379894738)

[11.5 认证证书的暂停、注销和撤销 11](#_Toc379894739)

[11.5.1 暂停认证的条件 11](#_Toc379894740)

[11.5.2 注销认证的条件 11](#_Toc379894741)

[11.5.3 撤销认证的条件 12](#_Toc379894742)

[12. 认证标志的使用 12](#_Toc379894743)

[12.1 准许使用的标志样式 12](#_Toc379894744)

[12.2 变形认证标志的使用 12](#_Toc379894745)

[12.3 加施方式 12](#_Toc379894746)

[12.4 加施位置 12](#_Toc379894747)

[13. 认证收费 12](#_Toc379894748)

1. **适用范围**

本认证实施规则适用于过程工业自动控制系统的认证，包括显示仪表系统、控制/调节仪表系统、工业过程自动控制报警装置系统、基地式仪表、自动化控制成套设备、工业控制用计算机/系统、巡回检测装置、远动装置等产品。

1. **认证依据**

GB/T 21109.1-2007 过程工业领域安全仪表系统的功能安全 第1部分：框架、定义、系统、硬件和软件要求。

1. **认证模式**

设计评估+产品型式试验+初始工厂审查+获证后监督。

认证的基本环节包括：

·认证的申请与受理

·设计评估

·型式试验

·初始工厂审查

·认证结果评价与批准

·获证后监督

1. **认证申请**
	1. **申请认证产品的基本要求**

申请认证的过程工业自动控制系统的产品主要零部件、原材料以及安装时使用的零配件都应是安全的、可靠的。

申请认证的企业应具备完善的质量管理体系，并配备所需的生产设备、检验设备和型式试验设备。

* 1. **申请单元划分**

原则上按产品品种、型式规格、工作原理、安全结构和对产品性能有重要影响的零部件的不同划分申请单元。同一制造商、同一产品规格/型号，不同生产场地生产的产品应作为不同的申请单元。

* 1. **申请认证提交材料**

申请认证需提交的资料如下：

a）书面的认证申请书；

b）注册营业执照的复印件；

c）生产厂质量手册和程序文件目录；

d）产品外形照片及内部结构照片；

e）产品认证涉及的企标或技术条件；

f）已经获得的认证证书和认证报告(适用时)。

如果需要在认证证书上体现产品的商标，则需提供注册商标证书的复印件。

1. **设计评估**

设计评估包括资料审查和文档评估两部分。

* 1. **资料审查**

申请者提供的资料应包括整体安全生命周期、E/E/PES安全生命周期、软件安全生命周期各个阶段要求的相关文档，不同的文档可以组成文档、文档集、文档包或文档包组，申请者应提供的资料包括：

1）整体安全生命周期阶段

1. 概念：总体概念描述
2. 整体范围定义：整体范围定义描述
3. 危险和风险分析：危险和风险分析描述
4. 整体安全要求：整体安全要求规范（包括整体安全功能和整体安全完整性）
5. 安全要求分配：安全要求分配描述
6. 整体操作和维护计划编制：整体操作和维护计划
7. 整体安全确认计划编制：整体安全确认计划
8. 整体安装和试运行计划编制：整体安装计划、整体试运行计划
9. 实现：E/E/PE安全相关系统的实现过程相关资料（见2）和3））
10. 整体安装和试运行：整体安装报告、整体试运行报告
11. 整体安全确认：整体安全确认报告
12. 整体操作和维修：整体操作和维护日志
13. 整体修改和改型：整体修改请求、整体修改和改型影响分析报告、整体修改和改型日志
14. 停用或处理报告：整体停用或处理影响分析报告、整体停用或处理计划、整体停用或处理日志
15. 所有有关阶段：安全计划、验证计划、验证报告、功能安全评估计划、功能安全评估报告

2）E/E/PES安全生命周期阶段

1. E/E/PES安全要求：E/E/PES安全要求规范（包括安全功能和安全完整性）
2. E/E/PES安全确认计划编制：E/E/PES安全确认计划
3. E/E/PES设计和开发——E/E/PES结构：结构设计描述（包括硬件结构和软件结构）、可编程电子集成测试规范、对可编程电子和非可编程电子硬件的集成测试规范
4. E/E/PES设计和开发——硬件结构：硬件结构设计描述、硬件结构集成测试规范
5. E/E/PES设计和开发——硬件模块设计：硬件模块设计规范、硬件模块测试规范
6. E/E/PES设计和开发——部件构建和采购：部件的构建和采购记录
7. E/E/PES设计和开发——硬件模块测试报告
8. 可编程电子集成：可编程电子和软件集成测试报告
9. E/E/PES集成：可编程电子和其它硬件集成测试报告
10. E/E/PES操作和维护规程：用户说明书、操作和维护说明书
11. E/E/PES安全确认：E/E/PES安全确认报告
12. E/E/PES修改：E/E/PES修改规程说明书、E/E/PES修改要求、E/E/PES修改影响分析报告、修改日志
13. 所有有关阶段：E/E/PES安全计划、E/E/PES验证计划、E/E/PES验证报告、E/E/PES功能安全评估计划、E/E/PES功能安全评估报告

3）软件安全生命周期阶段

1. 软件安全要求：软件安全要求规范（包括软件安全功能和软件安全完整性）
2. 软件确认计划编制：软件安全确认计划
3. 软件设计和开发——软件结构：软件结构设计描述（见2）中的E/E/PES结构设计描述）、软件结构集成测试规范、可编程电子和软件集合测试规范
4. 软件设计和开发——软件系统设计：开发工具和编码手册说明书、软件系统设计描述、软件系统集成测试规范
5. 软件设计和开发——软件模块设计：软件模块设计规范、软件模块测试规范
6. 软件设计和开发——编码：源代码表
7. 软件模块测试：软件模块测试报告、代码复审报告
8. 软件集成：软件系统集成测试、软件结构集成测试
9. 可编程电子集成：可编程电子和软件集成测试报告
10. 软件操作和维护规程：用户说明书、操作和维护说明书
11. 软件安全确认：软件安全确认报告
12. 软件修改：软件更新程序说明书、软件更新要求、软件更新影响分析报告、软件更新日志
13. 所有有关阶段：软件安全计划、软件验证计划、软件验证报告、软件功能安全评估计划、软件功能安全评估报告
	1. **文档评估**

文档评估为申请单元功能安全认证的主要工作，通过文档评估可得到相应安全功能达到的安全完整性等级（SIL）。文档评估的内容包括：

——概念评估；

——整体范围定义评估；

——危险与风险分析评估；

——安全要求评估；

——安全要求分配评估；

——硬件安全生命周期评估；

——软件安全生命周期评估；

——SIL评估；

——安装和试运行评估；

——安全确认评估；

——操作及维护评估；

——修改和改型评估；

——停用或处理评估；

——所有有关阶段（安全计划、验证和功能安全评估）评估；

1. **型式试验**
	1. **样品要求**
		1. **一般要求**

试验样品，在特性、特征、制造质量上应能够代表或覆盖申请认证的产品或系列产品，并应是以规定用于产品生产过程的方法和手段制造的。

试验样品应按照确定的试验方案进行检测。如果某项试验，包括许可的复验结果或所产生的现象已足以判定产品不符合认证条件时，则CGC可以终止试验并通知厂方负责人或其代表。申请人如仍希望获得认证，应在3个月内提交关于就导致不符合认证条件的原因进行调查和采取纠正措施的书面说明，经CGC研究后决定是否：规定某些附加条件和要求；再次进行有关试验；中止此次认证。

* + 1. **抽样和送样要求**

申请者应为型式试验机构提供安装调试完毕、能够正常进行型式试验的样品。每个申请单元应至少提供一个样品。

* 1. **型式试验**
		1. **试验内容和要求**

申请单元的型式试验的内容应符合相关产品型式试验标准的规定，并满足相关标准要求。

* + 1. **试验方法和要求**

申请者应在CGC认可的检测机构，依据申请单元的相关型式试验标准的要求进行型式试验；经CGC同意，申请者可利用自有检测资源进行型式试验，利用自有检测资源进行试验时应有CGC认证人员现场监督。

* + 1. **型式试验时限**

一般为30个工作日，从收到样品和检测费用算起。

* + 1. **型式试验报告**

型式试验结果的评价按认证产品执行的标准判定的规定执行。型式试验报告应按规定的格式出具。

* + 1. **型式试验评估**

CGC评估型式试验报告中的试验方法和试验结果，验证型式试验报是否满足相关标准的要求。CGC可针对申请者提供的试验报告中缺少的相关部分与申请者进行沟通，以使得申请者对相关试验进行完善。

1. **初始工厂审查**
	1. **审查内容**

工厂审查的内容为工厂质量保证能力和产品一致性检查。

* + 1. **工厂质量保证能力审查**

由CGC派审查员对生产厂按照“产品认证工厂质量保证能力要求”进行工厂质量保证能力审查。同时，还应按照“过程工业自动控制系统功能安全认证工厂质量控制检测要求”进行核查。

* + 1. **产品一致性检查**

工厂审查时，应对申请认证的产品进行一致性检查。若认证单元覆盖多个型号时，则一致性检查应从每单元产品中至少抽取一个覆盖型号；若认证单元中覆盖有多个系列的产品,则一致性检查应从认证单元的每个系列产品中至少抽取一个覆盖型号。重点核实以下内容:

1）认证产品的铭牌和包装箱上所标明的产品名称、规格型号与型式试验检测报告上所标明的应一致；

2）认证产品的结构应与型式试验检测时的样机或检测报告上所标明的一致；

3）认证产品所用关键零部件（元器件）及其制造商应与申报并经认证确认的一致；

4）认证产品质量与认证产品标准的要求一致，抽取样品进行现场见证试验。

工厂质量保证能力审查应覆盖申请认证产品的所有加工场所，产品一致性检查应覆盖申请认证产品，审查时，认证产品应在生产。

* 1. **初始工厂审查时间**

一般情况下，型式试验合格后，再进行初始工厂审查。根据需要，型式试验和工厂审查也可以同时进行。

工厂审查时间根据所申请认证产品的单元数量和工厂的生产规模确定，一般每个加工场所为2-3个人日。

1. **认证结果评价与批准**

CGC负责组织对认证结果进行综合评价，评价合格后，对申请人颁发认证证书/符合证明。设计评估和型式试验结果的评价按指定标准和适用技术条件合格判定的规定进行。

初始工厂审查的评价：

* 如果整个审查过程中未发现不符合项,则审查结论为合格；

· 如果发现轻微的不符合项，工厂应在规定的时间内采取纠正措施，报审查组确认其措施有效后，则审查结论为合格；

* 如果发现严重不符合项，或工厂的质量保证能力不具备生产满足认证要

求的产品量，则可终止审查。

认证结论评价、批准时间以及证书制作时间一般不超过5个工作日。

1. **获证后监督**
	1. **监督检查的频次**

一般情况下，在初次审查后的第12个月，对获证企业进行监督复查，在随后的 监督复查中两次监督复查时间间隔不应超过 12个月。

若发生下述情况可增加监督频次：

1) 获证产品出现严重质量问题或用户提出质量方面的投诉，并经查实,为持证人责任的；

2) 认证机构有足够理由对获证产品与标准要求的符合性提出质疑时；

3) 有足够信息表明生产制造商、生产厂因变更组织机构、生产条件、质量管理体系等，从而可能影响产品符合性或一致性时。

* 1. **监督的内容**

获证后监督的方式采用工厂产品质量保证能力的复查+认证产品一致性检查。必要时，抽取样品或其重要零部件送检测机构检验。

* + 1. **工厂质量保证能力复查**

由认证机构根据工厂质量保证能力要求，对工厂进行监督复查。

工厂质量保证能力复查的时间每个加工场所一般为1-2个人日。

* + 1. **产品一致性检查**

从获证起,按本规则7.1.1及7.1.2条的规定进行，检查样品主要以新增认证单元的产品为主，并保证四年覆盖所有认证单元。

* 1. **产品抽样检检测**

需要时，对获证产品进行抽样检测，抽样检测由CGC指定的检测机构负责，抽样范围为已生产的产品，抽样形式为随机抽样。

认证检测采用的标准或相关部门发布的技术条件所规定的项目均可作为抽样检测项目。

CGC可针对不同产品的不同情况，以及其对产品性能的影响程度，进行部分或全部项目的检测。每次监督检查应至少抽取1个认证单元中的1个型号的产品进行检测，通常抽样产品应在认证周期内覆盖所有认证单元。

* 1. **获证后监督结果的评价**

监督复查合格后，可以继续保持认证资格、使用认证标志。对监督复查时发现的不符合项应在3个月内完成纠正措施。逾期将撤消认证证书、停止使用认证标志，并对外公告。

1. **复审**

复审时应进行产品检验和工厂审查。产品检验由申请人按CGC的要求送样，进行部分项目检测，必要时进行全项目检测。复审工厂审查按照初审要求进行。

1. **认证证书**
	1. **认证证书的保持**
		1. **证书的有效性**

证书有效期为四年,有效期内，证书的有效性依据CGC的定期监督获得保持。证书有效期满前6个月企业应申请复审，通过后由CGC换发证书。

* 1. **认证产品的变更**
		1. **变更的申请**

认证后的产品，如果其产品中属于零部件的规格、型号、生产厂或涉及安全性能的设计、机构发生变更时，应向认证机构提出申请。

* + 1. **变更评价和批准**

CGC根据变更的内容和提供的资料进行评价，确定是否可以变更或需送样品进行检测，如需送样试验，检测合格后方能进行变更。

* + 1. **认证证书覆盖产品的扩展**

认证证书持有者需要增加与已获得认证产品为同一单元内的产品认证范围时，应从认证申请开始办理手续，CGC应核查扩展产品与原认证产品的一致性, 确认原认证结果对扩展产品的有效性，针对差异做补充检测或检查。CGC确认扩展产品符合要求后，根据具体情况，向认证证书持有者颁发新的认证证书或补充认证证书，或仅作技术备案、维持原证书。产品抽样检测按照本规则的9.3的要求执行。

* 1. **认证范围的扩大**

根据本规则4.2节所规定的认证单元划分原则，认证证书持有者在原有认证单元基础上增加新的认证单元，应提出正式书面申请。

认证证书持有者提交正式的申请文件，经认证机构确认，可安排工厂审查或样品检测。

* 1. **认证范围的缩小**

当认证证书持有者提出不再保留某个已认证单元的认证资格时属缩小认证产品范围，原则上应提出书面申请，经确认后注销相应的认证单元。认证证书持有者应退还认证证书，同时停止在该认证单元的产品上使用认证标志。

* 1. **认证证书的暂停、注销和撤销**
		1. **暂停认证的条件**

当出现下列情况之一时暂停证书，认证部用挂号信或等效方式书面通知认证证书持有者暂停使用认证证书和认证标志。

1）企业质量保证能力因变化而达不到认证的要求；

2）产品性能下降，达不到标准要求及其补充技术条件；

3）用户投诉，并经查实确属质量问题，达不到认证的要求；

4）认证证书持有者未按期交纳认证费用；

5）认证证书持有者未经CGC同意不接受CGC对生产厂的监督复查；

6）获证企业有误用认证标志或涉及认证虚假行为的；

7）对一年内未生产获证产品；

8）发生当认证要求更改时，未按CGC-QP-V07《自愿性产品认证 认证变更程序》 的相应要求办理相关手续；

9）产品获证后，如果图纸、技术文件、工艺规程或质量控制体系有较大改变，并未应征得CGC同意；

10）企业提出暂停要求的。

* + 1. **注销认证的条件**

出现下列情况之一时注销认证证书，认证部用挂号信或等效方式书面通知认证证书 持有人停止使用认证证书和认证标志：

1）由于认证标准或其补充条件的内容发生较大变化，证书持有者认为达不到变化的要求时，不再申请认证；

2）认证证书到期，证书持有者未提出延证申请；

3）企业不再生产认证产品；

4）证书的颁发有错误。

* + 1. **撤销认证的条件**

出现下列情况之一时撤销认证证书，认证部用挂号信或等效方式书面通知认证证书 持有人停止使用认证证书和认证标志。

1）接到CGC暂停使用认证证书和认证标志的通知后，不能按期改正其存在的问题的；

2）由于产品存在严重不安全问题且造成严重后果的；

3）使用弄虚作假或其它不正当手段骗取认证证书者；

4）伪造、转让、滥用认证证书或认证标志的；

5）拒不缴纳认证费用的。

1. **认证标志的使用**

证书持有者必须遵守认证机构CGC-XZ-V02《自愿性产品认证 认证标志管理细则》的规定。

* 1. ******准许使用的标志样式**
	2. **变形认证标志的使用**

本规则覆盖的产品不允许加施任何形式的变形认证标志。

* 1. **加施方式**

可以采用认证机构统一印制的标准规格标志（标签））、模压式或铭牌印刷三种方式中的任何一种。

* 1. **加施位置**

应在产品本体和/或其包装物的明显位置上加施认证标志。

1. **认证收费**

认证收费由认证机构按国家有关规定统一收取。